NATIONAL CYBER DEFENCE REFERENCE HANDBOOK II Digital Edition

▸▸ A Mandatory Disclosure

An Initiative by

National Cyber Safety and Security Standards

Institutional Members

सत्यमेव जयते

Ministry of Defence
Ministry of Commerce and Industry
Ministry of Social Justice & Empowerment
Ministry of Micro, Small & Medium Enterprises

Govt. of Andhra Pradesh

Govt. of Madhya Pradesh

Govt. of Maharashtra

Govt. of Goa

Govt. of Manipur

Department of Science & Technology
Government of Gujarat

New Delhi
Tamil Nadu
Andhra Pradesh
Madhya Pradesh
Maharashtra
Himachal Pradesh

All India Council for Technical Education

Published by the **Additional Director - General**

Publication Division

National Cyber Safety and Security Standards

(A Self Governed Body)

CYBER HOUSE – Southern Region

Prince Centre : # 102, 1st Floor, Pathari Road

Thousand Lights, Chennai - 600 006

Phone : 044 – 2829 1766

Fax : 0 84688 65111

Email : support@nationalcybersafety.com

Web : www.ncdrc.res.in

Publisher's Note : Inspite of our best efforts can creep in. Any mistake, misprints, missing pages or discrepancy etc., noticed may kindly be brought to our knowledge, so that it may be corrected in the next Edition. This book is a combined version of materials from various sources. So, the National Cyber Safety and Security Standards will not give any authenticity to the content.

The Greatness of

INDIA

India "Truth Alone Triumphs"(Satyameva Jayate)

Present Scrutiny

- 5,000 Years Old Ancient Civilization.
- 530 Languages Spoken.
- 652 Dialects.
- 18 Official Languages.
- 29 States, 7 Union Territories.
- 3.28 Million Sq. Kilometres - Area.
- 7,516 Kilometres - Coastline.
- 1.3 Billion Population.
- 5600 Dailies, 15000 Weeklies and 20000 Periodicals in 21 Languages with a Combined Circulation of 142 Million.
- GDP $1877 Billion. (GDP Rate 7.5% approximately).
- Parliamentary Form of Government
- World's Largest Democracy.
- World's 4th Largest Economy.
- World-Class Recognition in IT, Bio-Technology and Space.
- Largest English Speaking Nation in the World.
- 3rd Largest Standing Army Force, Over 1.5 Million Strong.
- 2nd Largest Pool of Scientists and Engineers in the World.

Dedicated to

Our Nation

न्यायाधीश डॉ. एस. मोहन
Justice Dr. S. Mohan
Former Judge - Supreme Court of India
Chairman - National Cyber Safety and Security Standards

Foreword

I am glad to note that National Cyber Safety and Security Standards is publishing the II Edition of National Cyber Defence Reference Handbook. Hope the book is very useful to all the people who are working in the Government sector, Private sector, Corporates and especially for Educational Institutions.

Today the cyber world has come to occupy an important place in the history of mankind. As science advances, the knowledge also expands. It is undeniable fact that cyber world has thrown a new vista but regretfully it has to be noted that it has also being misused and spreading undesirable information. It has become necessary to find out ways and means to curb this menace of spreading evil knowledge.

We live in the electronics age in which every institution of Government, Business and Industry, big and small, and even the family interact and communicate with one another electronically. Electronic devices which process data are no longer confined to what we traditionally consider as computers, but are pervasive in everyday life. They range from mobile 'smart' telephones to global positioning by satellite devices, and from health-monitoring devices to defibrillators.

Information Security is an art, not a science and the mastery of information security requires a multi-disciplinary knowledge of huge quantity of information, experience, and skill. There is a great satisfaction knowing that your employer's information, communications, systems, and people are secure. Comprehensiveness is an important part of the game you play for real stakes because the enemy will likely seek the easiest way to attacks the vulnerabilities and assets that you haven't fully protected yet.

The past decade has witnessed tremendous legal reform by countries around the world. The most influential- electronic commerce has led countries to revise and update their rules of evidence on the proof and admissibility of such evidence. And litigants have responded courts are witnessing a myriad and a rising volume of electronic evidence tendered by the parties. These ranges from emails to mobile messages, from chat records to blog entries and even "tweets" to mobile messages, resolving the many difficult issues regarding discovery and inspection of electronic documents (or electronically stores information) and the authentication and admission of electronic evidence now calls for a technologically savvy bar.

The book entitled : Basics of Computers Networks and How to Shore up Network Security, Information Security – Building Blocks, Management in Organizations and Physical Security for Information Systems, Cyber Hacking, Demystifying the Mysterious Business of Hacking, Hacking into Wireless Networks and General Anti-Hacking Measures, Cyber Crime, History of Cyber Crimes and the Challenges of Fighting Cyber Crime, Cyber Terrorism, Tools and Methods used in Cyber Crime, Cyber Offences, Computer Forensics, Significance of Cyber Security and Major Cyber Security Risks for the Common Man, Biometric Controls for Security and Web Services and Privacy.

I convey best wishes to the National Cyber Safety and Security Standards Publishing Committee.

(Dr. S. Mohan)

न्यायाधीश डॉ. टी एन वल्लीनायगम
Justice **Dr. T.N. Vallinayagam**
Judge - Lok Adalat & Former Judge - High Court of Madras & Karnataka
Chairman – National Cyber Defence Research Centre (Tamil Nadu)

Foreword

Today, given the increasing dependence on information and communication technologies, especially the Internet, for delivery of services and operations, one of the biggest challenges the world faces is that of cyber security. Cyber security is a complex issue, affecting many application domains and straddling many disciplines and fields. Securing the critical infrastructures requires protecting not only the physical systems but, just as important, the cyber portions of the systems on which they rely.

Cyber Security Research is one context where the solution to deal with cyber criminals is germinating. Investment of time and resources requires fostering strategies for research and developing transformative solution to meet critical cyber security challenges involving a certain technology, or a particular application domain, or a combination of two. One way to tackle the emerging cyber threats is to train and develop a dedicated work force that can detect and prevent attacks at different levels. Towards achieving this objective, National Cyber Safety and Security Standards (NCSSS) is planning to set up 60 National Cyber Defence Research Centres across India, with the objective of providing an atmosphere for learning cyber security.

The National Cyber Defence Research Centre multi-disciplinary team employs the best and brightest to thwart Cyber Attacks. NCDRC is focused on building science and engineering foundations for Cyber Security. Research and development is focused on making today's systems more secure while planning for tomorrow's technology.

I hope that National Cyber Defence Reference Handbook will receive great acceptance and I convey my best wishes to the team for their Cyber Security efforts towards National Security.

(Dr. T. N. Vallinayagam)

Preface

Today, the internet has turned 40, and with its maturing, the threats are increasing. Botnets and cyber-criminals are making news regularly. It has become increasingly obvious to everybody that something needs to be done to secure not only our nation's critical infrastructure but also the businesses we deal with on daily basis. The question is, "where do we begin?" what can the average information technology professional do to secure the systems that he or she is hired to maintain? One immediate answer is education and training. If we want to secure our computer systems and networks, we need to know how to do this and what security entails.

As global networks expand the interconnection of the world's information systems, the smooth operation of communication and computing solutions becomes vital. However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems.

You cannot perform your job or organize your social life effectively without using e-mail and the World Wide Web. Our reliance on these technologies and the extent to which we take them for granted are a testament of the impact of the Internet and the Web on our lives. These technologies have created a better-informed consumer and a manager who is equipped with up-to-the-second information. Communities have sprung up and supply chains have been redesigned. In general, the opportunities that have been created due to the unique properties of these technologies allow us to set higher goals for our businesses and meet them more effectively.

We have now entered the world of low impact, multiple victim crimes in which bank robbers, for example, no longer have to meticulously plan the theft of millions of dollars. New technological capabilities at their disposal now mean that one person can effectively commit millions of robberies of one dollar each. Against this background, David Wall scrutinizes the regulatory challenges that Cyber Crime poses for the criminal (and civil) justice processes, at both the national and the international levels.

The National Cyber Defence Reference Handbook will comprise the detailed perspective of the Cyber Crimes which are creating massive trouble for India's National Security and also this book provides advanced cyber protection methodologies and controlling procedures/tools.

Chapter 1: Basics of Computers Networks and How to Shore up Network Security

This chapter explains about: Basics of Computers Networks, How a Computer Works? Computer Networks, The Internet and how it Works? & How to Shore Up Network Security? How Firewalls Works and Why You Need Them? What a Firewall Can't Do? Network Security, How we can Improve Network Security Further? IP Fragments and DoS (Denial-Of-Service) Attack, IP Address Spoofing and Source Routing.

Chapter 2: Computer Viruses, Worms, Trojan Horses and Root kits: a Quick Recap

This chapter explains about: What Could Happen in a Cyber War? Computer Viruses, Computer Worms and How They Target Networks? Trojan Horses, Spyware, Root kits, The Common Symptoms of Malware Infection

Chapter 3: Information Systems and Threats to Information Systems

This chapter explains about: Information Systems, History of Information Systems, Importance of Information Systems, Basics of Information Systems, The Changing Nature of Information Systems, Globalization of Businesses and the Need for Distributed This chapter explains about the Information Systems, Global Information Systems: Role of Internet and Web Services, Information Systems Security and Threats: A Glimpse & Threats to Information Systems, Introduction of Threats to Information Systems, New Technologies Open Door to the Threats, Information-Level Threats versus Network-Level Threat, Information Systems Security: Threats and Attacks, Classifications of Threats and Assessing Damages, Protecting Information Systems Security.

Chapter 4: Information Security – Building Blocks, Management in Organizations and Physical Security for Information Systems

This chapter explains about: Building Blocks of Information Security, Information Security Management in Organizations, Information Security Awareness Scenario in Indian Organizations, Organizational Responsibility for Information Security Management, Information Security Awareness Scenario in Indian Organizations.

Chapter 5: Cyber Hacking, Demystifying the Mysterious Business of Hacking and Getting More Serious about Hacking into Networks

This chapter explains about: Cyber Hacking, Hacking and different Types of Hackers, What Hacking Entails? Demystifying the Mysterious Business of Hacking, Tricks and Techniques Employed By Not-So-Serious Hackers, Secrets of Serious Hackers No One Told You Before, Getting More Serious about Hacking into Networks, Basic Principles

of Hacking Networks, Tools in the Hacker's Arsenal, Other important Weapons of the Hackers.

Chapter 6: Hacking into Wireless Networks and General Anti-Hacking Measures

This chapter explains about: Hacking into Wireless Networks, Why Terrorists and Criminals Prefer It? What does it Take to Hack into Wireless Networks? How Do They Go About It? Fifteen Practical Countermeasures against Attacks on Encrypted Wireless Traffic, General Anti-Hacking Measures, Intrusion Detection Systems (IDS), What Firewalls can do for you and what they cannot? How to Fight Back?

Chapter 7: Cyber Crime, History of Cyber Crimes and the Challenges of Fighting Cyber Crime.

This chapter explains about: What is Cyber Crime? What is Cyber Law? What is Cyber Security? Cyber Attacks and Effects, History of Cyber Crime, The Challenges of Fighting Cyber Crime, Opportunities, General Challenges.

Chapter 8: Cyber Crime: Mobile and Wireless Devices

This chapter explains about: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations

Chapter 9: Cyber Crime and Cyber Terrorism– A detail Explanation

This chapter explains about: Data Theft, Cyber Terrorism, Phishing, Email Bombing, Cyber Bullying, Identity Theft, Email Fraud, E-mail Spoofing, Copyright Violation, Pornography, Child Pornography, Online Gambling, Forgery, Denial of Service Attack, Web Defacement, Web Jacking, Illegal Online Selling, Cyber Defamation, Software Piracy, Electronic/Digital Signature.

Chapter 10: Tools and Methods used in Cyber Crime

This chapter explains about: Introduction to Tools and Methods used in Cyber Crime, Proxy Servers and Anonymizers, Password Cracking, Key loggers, Steganography, DoS and DDoS Attacks, Attacks on Wireless Networks.

Chapter 11: Cyber Offences

This chapter explains about: Introduction, How Criminals Plan the Attacks, Social Engineering, Cyber Stalking, Cyber cafe and Cyber Crimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing

Chapter 12: Understanding Computer Forensics

This chapter explains about: Introduction, Historical Background of Cyber Forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber

Forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle

Chapter 13: Fundamentals of Cyber Security, Significance of Cyber Security and Major Cyber Security Risks for the Common Man

This chapter explains about: Fundamentals of Cyber Security, Basic Components of Computer Security, Threats of Cyber Security, Goals of Cyber Security, Significance of Cyber Security, Major Cyber Security Risks for the Common Man.

Chapter 14: Biometric Controls for Security and Issues and Challenges in Biometric-Based Security

This chapter explains about: Introduction, Access Control, User Identification and User Authentication, What is Biometrics? Nature of Biometric Identification/Authentication Techniques, Biometric Techniques, Matching and Enrolment Process in Biometrics, Key Success Factors for Biometrics Systems, Benefits of Biometrics over Traditional Authentication Methods, The Future of Biometrics.

Chapter 15: Web Services and Privacy

This chapter explains about: Privacy on the Internet – A Legal Perspective and Organizational Implications, Privacy and the Internet: Privacy Violation, The Nature of Privacy Problems on the web, Legal Issues with Use of Internet, Online Trust – The Government Scenario, Web Services and Their Privacy and Security Implications, Web Services Role in Today's Businesses, Web Services Working: An Illustration, Privacy Considerations in Web Services, Privacy in the Semantic Web, Security and Privacy Aspects of Service-Oriented Architectures.

I wish, the Initiatives of National Cyber Safety and Security Standards plays a vital role, in the mission of building a secure and resilient cyberspace for Citizens, Institutions and Government.

(Dr. S. Amar Prasad Reddy)
Additional Director-General
National Cyber Safety and Security Standards

70 +
Accolades

75 +
Case Studies

10 +
Articles by Cyber Security Experts

40 +
Diagrams

Chapters

HIGHLIGHTS

1. Basics of Computers Networks and How to Shore up Network Security
2. Computer Viruses, Worms, Trojan Horses and Root kits : a Quick Recap
3. Information Systems and Threats to Information Systems
4. Information Security – Building Blocks, Management in Organizations and Physical Security for Information Systems
5. Cyber Hacking, Demystifying the Mysterious Business of Hacking and Getting More Serious about Hacking into Networks.
6. Hacking into Wireless Networks and General Anti-Hacking Measures
7. Cyber Crime, History of Cyber Crimes and the Challenges of Fighting Cyber Crime
8. Cyber Crime: Mobile and Wireless Devices
9. Cyber Crime and Cyber Terrorism – A detail Explanation
10. Tools and Methods used in Cyber Crime
11. Cyber Offences
12. Understanding Computer Forensics
13. Fundamentals of Cyber Security, Significance of Cyber Security and Major Cyber Security Risks for the Common Man
14. Biometric Controls for Security and Issues and Challenges in Biometric-Based Security
15. Web Services and Privacy

Editorial Board

राष्ट्रीय साइबर सुरक्षा और सुरक्षा मानकों

National Cyber Safety and Security Standards

National Cyber Safety and Security Standards have been started with a great vision to safeguard the Nation from the current threats in the Cyberspace. The multi-dimensional structure of technology in the Cyberspace poses a great challenge in handling the complex problems in the Cyber domain.

National Cyber Safety and Security Standards have done an extensive research in the Cyber domain to understand the nature of cyber threats and Cyber Crimes. We have understood that the multi – faceted cyber technology cannot be handled by common standards and security policies. We came to know that, it needs different strategies for different sectors of Cyber domain.

Our Nation is treated like a hot spot for cyber attacks and information thefts by many countries. Due to this, we have taken a visionary initiative to curb and enervate the notoriously spreading cyber threats from various directions and dimensions.

A Common Platform to facilitate the experts to provide an effective solution for the complex and alarming problems in the society towards Cyber Security domain. We are developing innovative strategies and compliance procedures to curb the increasing complexity of the Global Cyber Threats.

The National Cyber Safety and Security Standards is a Self Governed Body, which is controlled and monitored by the High Level Committee Chaired by Honourable Justice Dr. S. Mohan, Former Judge, Supreme Court of India and Chairman, National Cyber Safety and Security Standards.

Accolades

सत्यमेव जयते

His Excellency

Shri. **Pranab Mukherjee**

Honourable President of India, New Delhi

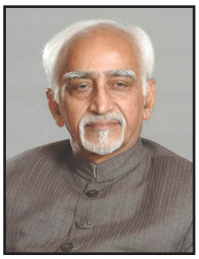
The President of India, Shri Pranab Mukherjee, is happy to know that the National Cyber Safety and Security Standards is bringing out the "National Cyber Defence Reference Handbook 2nd Edition".

The President extends his warm greetings and felicitations to all those associated with the Organisation and sends his best wishes for their future endeavours.

(Venu Rajamony)

Press Secretary to the
President of India

सत्यमेव जयते



His Excellency

Shri. **Mohammad Hamid Ansari**

Honourable Vice President of India, New Delhi

Honourable Vice President of India is happy to know that the National Cyber Safety & Security Standards, Chennai is publishing a book titled "National Cyber Defence Reference Handbook" focusing on the issues of Cyber Crime in the country.

The Vice President of India extends his greetings and good wishes to all those associated with the publication.

(Nagesh Singh)

Officer on Special Duty to the
Vice - President of India

सत्यमेव जयते

His Excellency

Shri. **Narendra Modi**

Honourable Prime Minister of India

The Prime Minister is happy to know that the National Cyber Safety and Security Standards is publishing the second Edition of the "National Cyber Defence Reference Handbook.

The Prime Minister hopes that the handbook will be a ready reckoner on matters related to cyber protection in our country.

The Prime Minister sends his best wishes to National Cyber Safety and Security Standards.

(Jagdish Thakkar)
Public Relations Officer
Prime Minister's Office

सत्यमेव जयते

His Excellency

Dr. S.C. Jamir

Honourable Governor of Odisha

I am glad to know that the National Cyber Safety & Security Standards, Chennai is bringing out the 2nd edition of National Cyber Defence Reference Handbook shortly.

Cyber crime is a fast-growing area of crime. New trends in cyber crime are emerging all the time and becoming more widespread and damaging. Highly complex, cyber criminal networks have no borders as they operate across the globe to commit a diverse range of criminal activities on an unprecedented scale.

Threats to our own National Security from cyber crime demand attention, caution and aggressive action. In this context a National Reference Handbook comprising detailed perspective of cyber crimes is handy to enhance knowledge on cyber security. It is heartening that the handbook will be issued free of cost to Central and State Government Departments/ Police Departments/National Libraries all over the country.

I wish the endeavour and publication all success

(S. C. Jamir)

सत्यमेव जयते

His Excellency

Shri. **Justice (Retd.) P. Sathasivam**

Honourable Governor of Kerala

I am very glad to know that the National Cyber Safety and Security Standards intends to publish the second edition of 'National Cyber Defence Reference Handbook' which will provide advanced cyber protection methodologies and controlling procedures.

I wish the endeavour all success.

(Justice (Retd) P. Sathasivam)

सत्यमेव जयते

His Excellency

Prof. Kaptan Singh Solanki

Honourable Governor of Haryana

I am pleased to know that National Cyber Safety & Security Standards, Chennai is going to bring out 2nd edition of 'National Cyber Crime Reference Hand Book' with a view to generate awareness against Cyber Crime.

Cyber crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child grooming etc. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. The need of the hour is to achieve perfection in every sphere in order to face this massive problem.

It is heartening that National Cyber Safety & Security Standards is devoted to promote advanced cyber protection methodologies and controlling producers. I hope that the Hand Book would prove a milestone in this context.

I extend my best wishes for the successful publication of 2nd Edition of 'National Cyber Crime Reference Hand Book'.

(Prof. Kaptan Singh Solanki))

सत्यमेव जयते

His Excellency

Shri. **Keshari Nath Tripathi**

Honourable Governor of West Bengal

It gives me immense pleasure to know that National Cyber Safety & Security Standards is going to publish a 'National Cyber Crime reference Handbook (2nd Edition)'.

I think that this publication will be very helpful and effective to address the present issues on cyber crime.

I convey my best wishes for the successful publication of the Handbook.

(Keshari Nath Tripathi)

सत्यमेव जयते

His Excellency

Shri. **Vajubhai Vala**

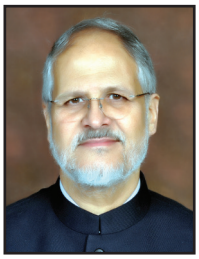
Honourable Governor of Karnataka

I am happy to learn that the 'NATIONAL CYBER SAFETY & SECURITY STANDARDS' functioning under a High Level Committee, is publishing 2nd Edition of its "NATIONAL CYBER DEFENCE REFERENCE HANDBOOK" as a national initiative to address the issues connected with Cyber Crime that are creating massive threat for the National Security which will act as a reference material for all the Legislatives, Executives ands Judiciary with a view to provide advanced Cyber Protection Methodologies and Controlling Tools and Procedures.

I send my felicitations and best wishes to the National Cyber Safety and Security Standards and all those connected with the publication which is more needed at this point of time.

(Vajubhai Vala)

सत्यमेव जयते



His Excellency

Shri. **Najeeb Jung**

Honourable Lieutenant Governor of Delhi

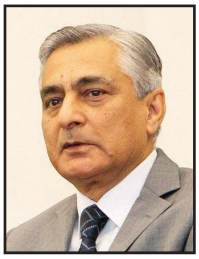
I am happy to learn that the 'National Cyber Safety & Security Standards' is bringing out the 2nd edition of the National Cyber Defence Reference Handbook. This handbook will prove to be a valuable resource for all concerned and will help counter incidences of cyber crime.

The handbook will help provide the much needed perspective on cyber crimes and the measures needed to be adopted to counter such threats to India's national security. As I understand, the handbook also contains information about advanced cyber protection methodologies and controlling procedures and tools, which will prove useful to the concerned departments and agencies.

I deeply appreciate this initiative of the 'National Cyber Safety & Security Standards' and wish their future endeavours my very best.

(Najeeb Jung)

सत्यमेव जयते



Honourable **Mr. Justice T.S. Thakur**
Chief Justice of India
Supreme Court of India, New Delhi

I am happy to note that the National Cyber Safety and Security Standards is publishing "National Cyber Reference Handbook 2nd Edition" as a national initiative which will give a detailed perspective of the cyber crimes as also methodologies for cyber protection besides controlling procedures and tools. The initiative is timely keeping in view the country's national security concerns and the need for protection of the national critical infrastructure. In a fast-changing world driven by advanced technology the compulsions arising out of national security interest and the need for dissemination of information regarding cyber methodologies and controlling procedures and tools have become inevitable. The National Cyber Defence Research Centre, headed by Justice Dr. S. Mohan, former Judge of the Supreme Court, has done commendable service to the country, the Public Authorities and constitutional bodies in updating the information regarding cyber crimes and their fallout as also ways and means of protecting oneself against such crimes.

I compliment Justice Dr. S. Mohan and his team for the work which the National Cyber Safety and Security Standards has done and the elegant Handbook being published by it.

(T.S. Thakur)

सत्यमेव जयते

Shri. **Ananth Kumar**
Honourable Minister for Chemicals & Fertilizers
Government of India

I am happy to know that the National Cyber Safety and Security Standards is bringing out the 2nd Edition of the National Cyber Defence Reference Handbook to address the present issues on Cyber Crime.

Cyber Crime has become a major menace and causing immense damage to the Society. The need of the hour is to educate the masses the adverse impact of the crime in the Society and the steps to be taken to counter the same unitedly. I congratulate you for the above initiative which is being taken at a very appropriate time.

(Ananth Kumar)

सत्यमेव जयते

Shri. **Nitin Gadkari**

Honourable Minister of Road Transport, Highways and Shipping

Government of India

It is a matter of great pleasure that the National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" to address different issues of Cyber Crime.

In today's world, cyber crime is a fast growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities.

New trends in cyber crime are threat to the global security and economy.

The Crime Reference Handbook will provide the much needed information will provide valuable inputs to give cyber crime awareness to Government sector, PSUs and industrial organisations to control cyber fraud. It will give detailed perspective to cyber crime.

I extend my hearty good wishes to the members of National Cyber Safety & Security Standards.

With best wishes.

(Nitin Gadkari)

सत्यमेव जयते

Shri. **Radha Mohan Singh**
Honourable Minister of Agriculture
Government of India

I am glad to know that National Cyber Safety & Security Standards is publishing a manual entitled "National Cyber Defence Reference Handbook 2nd Edition" with the objective to detail the perspectives of the cyber crimes which are creating massive trouble for the nation's security and also to familiarize the people with advanced cyber protection methodologies and controlling procedures. The manual being envisaged for fee of cost supply to Central and State Government Departments shall be a useful reference material to enhance the users' knowledge on cyber security.

I appreciate the initiative taken by the organization to address the burning issues prevailing in the cyber space which has already developed into an area of concern in the defamation, identity theft, hacking and allied sectors which can determine the overall safety aspects of internet users in the country.

Wish a great launch of the National Cyber Defence Reference Handbook 2nd Edition.

Radha Mohan Singh

(Radha Mohan Singh)

सत्यमेव जयते

Smt. **Najma Heptulla**
Honourable Minister of Minority Affairs
Government of India

I am glad to know that National Cyber Safety and Security Standards is bringing out a National Cyber Defence Reference Handbook for the use of the Central/State Government Departments/Police Departments/National Libraries all over the country.

The objective of the organisation to protect our critical infrastructure from cyber related issues, is indeed the need of the hour. I am sure the Handbook will comprise detailed perspective of the cyber-crimes affecting India's National Security and will also give us advanced cyber protection methodologies and controlling procedures / tools.

I extend my best wishes to the organisation of National Cyber Safety and Security Standards for success in its venture.

Najma Heptulla

(Najma Heptulla)

Shri. **Akhilesh Yadav**
Honourable Chief Minister of Uttar Pradesh

I am happy to know that National Cyber Safety & Security Standards is publishing the 2nd edition of National Cyber Defence Reference Handbook.

Cyber Crime has become a major concern for all. It ranges across a spectrum of activities. More and more criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities that know no borders. It is commendable that a Handbook is being published on such a relevant issue. I hope that the publication would be helpful in creating awareness regarding Cyber Crimes and Cyber Safety.

My best wishes for the entire endeavour.

(Akhilesh Yadav)

उत्तराखण्ड राज्य

Shri. **Harish Rawat**

Honourable Chief Minister of Uttarakhand

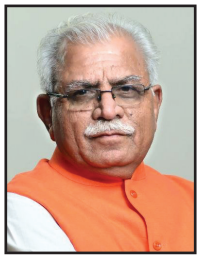
I feel extremely happy to know that National Cyber Safety & Security Standards is publishing second edition of "National Cyber Defence Reference Handbook".

I believe that this book will be very useful for the Central and State Government departments to fight against cyber crime.

I convey my best wishes for the successful publication of the book.

(Harish Rawat)

सत्यमेव जयते



Shri. **Manohar Lal**
Honourable Chief Minister of Haryana

सन्देश

मुझे यह जानकर अति प्रसन्नता हुई है कि राष्ट्रीय साइबर सुरक्षा एवं सुरक्षा मानक द्वारा देश में बढ़ते साइबर अपराध बारे जागरुकता उत्पन्न करने के लिए 'नेशनल साइबर क्राईम रेफरेंस हैंडबुक' का द्वितीय अंक प्रकाशित किया जा रहा है।

सूचना एवं संचार प्रौद्योगिकी के क्षेत्र में त्वरित बदलाव आ रहा है। इस क्षेत्र में हुई प्रगति से जहाँ हमें लाभ हो रहा है वहीं हमारे समक्ष कुछ गम्भीर चुनौतियाँ भी उत्पन्न हुई हैं। आज, भारत ही नहीं बल्कि समस्त विश्व साइबर अपराध की समस्या से जूझ रहा है। अपराध जगत देश में अशान्ति फैलाने के लिए इस प्रौद्योगिकी का दुरुपयोग तो कर ही रहा है साथ ही साइबर अपराधों के कारण राष्ट्र को करोड़ों रुपये का नुकसान भी हो रहा है। ऐसे में आवश्यक है कि हम साइबर अपराधों के प्रकोप की रोकथाम के अर्थोपाय का पता लगाएं और इस दिशा में आवश्यक ठोस कदम उठाएं।

मुझे आशा है कि 'नेशनल साइबर क्राईम रेफरेंस हैंडबुक' में साइबर अपराधों के विभिन्न रूपों एवं स्वरूपों के साथ–साथ इससे बचने और इसे नियंत्रित करने बारे विस्तृत जानकारी दी जाएगी ताकि लोग साइबर अपराधों के प्रति सचेत रहते हुए आवश्यक बचावात्मक उपाय कर सकें।

मैं 'नेशनल साइबर क्राईम रेफरेंस हैंडबुक' के द्वितीय अंक के सफल प्रकाशन के लिए अपनी शुभकामनाएँ प्रेषित करता हूँ।

(Manohar Lal)

सत्यमेव जयते

Smt. **Anandiben Patel**
Honourable Chief Minister of Gujarat

Security of self, family and the society has always been the prime in the men's priority list. Means and modes of security have also changed, transformed and evolved with the changing scenario of the threat factors. As the entire world is mostly becoming dependant on the information technology, the threats have to be defended from that angle. Our present society is heavily dependent on the internet for communication and day to day transactions.

I am happy to learn that National Cyber Safety & Security Standards is aware and concerned about the potential threat of the Cyber Crime and is publishing the Seconds Edition of the "National Cyber Defence Reference Handbook" which can be very useful for the Government Departments dealings with the subject. It is a welcome step that the copies of the hand book are to be distributed to all concerned departments free of cost. I am sure that this Hand Book will be really helpful to all its users.

Anandi Patel

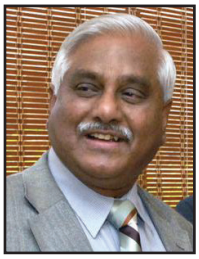
(Anandiben Patel)

Honourable **Mrs. Justice R. Banumathi**
Judge, Supreme Court of India, New Delhi.

I am happy to note that "National Cyber Safety & Security Standards" is publishing National Cyber Defence Reference Handbook 2nd Edition to address the present issues on cyber crime. In the present day context, publication of such Handbook is very relevant as the proportion of cyber-crimes is swelling at tremendous rate. The book comprehensively dwells upon the problem of cyber-crimes and provides measures and methodological tools for the advanced cyber protection. The initiative to issue 15,000 copies to State/Central government Authorities and Constitutional (Bodies at free of cost will mark a further step in combating the plague of cyber-crimes. I am sure that the Handbook will create awareness about the subject and will be useful for students of law, advocates, academicians and other stakeholders.

RBanumathi

(R. Banumathi)



Honourable **Mr. Justice V. Gopala Gowda**
Judge, Supreme Court of India, New Delhi.

It gives me immense pleasure to learn that the National Cyber Safety and Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" comprising of detailed perspective on the Cyber Crimes which pose a massive trouble for India's National Security, as a national initiative to address the present issues on Cyber Crime.

The Indian police have initiated special cyber cells across the country and have started educating the police personnel on this front. I am sure that the National Cyber Defence Reference Handbook will play its part in developing their skills in tackling the threat of Cyber Crime.

On this occasion, I congratulate the National Cyber Safety and Security Standards and every person whose effort was needed to make this handbook a possibility. I wholeheartedly extend my greetings for the success of the handbook.

(V. Gopala Gowda)

Honourable **Mr. Justice Arjan Kumar Sikri**

Judge, Supreme Court of India, New Delhi.

Cyber Crimes in India are rising at an alarming rate and pose serious economic and national security threat. The increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions, protection of personal and sensitive data have assumed paramount importance.

The economic growth of any nation and its security whether internal or external and competitiveness depends on how well is its cyberspace secured and protected.

Cyber crimes have been reported across the world and is now amongst the most important revenue sectors for global organized crime.

Cyber crimes may be committed against a person, property, government or the society at large.

As cyber criminals continue to develop and advance their techniques, they are also shifting their targets – focusing less on theft of financial information and more on business espionage and accessing government information. To fight fast-spreading cyber crime, governments must collaborate globally to develop an effective model that will control the threat. There are many challenges in front of us to counter cyber crimes. Tracking the origin of crime, shortage of skilled cyber crime fighters, widespread use of pirated software, identification of the cyber criminals and jurisdictional disputes are to name few of such challenges.

I firmly believe that there is a need for us to adopt a holistic approach towards such crimes and set up enforcement agencies to tackle the threat.

The handbook is a guidance document which comprises of detailed perspective of the cyber-crimes which are creating massive trouble for our Country's National Security and also facilitates advanced cyber protection methodologies and controlling procedures and tools.

I would like to extend my warm appreciation to the National Cyber Safety & Security Standards who worked towards the development of this document

(Arjan Kumar Sikri)

Honourable **Mr. Justice Madan Bhimarao Lokur**

Judge, Supreme Court of India, New Delhi.

The National Cyber Defence Reference Handbook is a boon for all lay persons, professionals and practitioners of law interested in issues relating to cyber crimes.

Since the first edition came out, there have been several developments that have taken place in cyber space. Primarily, there has been greater awareness and use of cyber space for useful purposes, but disturbingly for criminal activities also. The number and variety of cyber crimes has increased tremendously over the years. Heightened awareness of cyber space is not the only reason for this upsurge but the easy accessibility of internet has also contributed substantially. Anyone who is even remotely familiar with the internet can exploit its potential for good or for evil.

Many of us are unaware of the nature of cyber crimes and how to deal with them. I am sure some of us have been victims of cyber crimes such as the hacking of a password, but we tend to overlook such a crime unless it has serious consequences. Others have perhaps been unfortunate victims of far graver cyber crimes such as cyber fraud or recipients of malware. Generally speaking, very few amongst us have any idea how to deal with such crimes, serious or grave.

Sometimes even investigators are completely baffled by the nature of cyber crimes and are unable to find out not only who committed the crime but also from where the criminal activity originated. Traditional investigation techniques require the Investigating Officer to at least visit the place of occurrence but in cases of cyber crimes, it is sometimes not even possible to find out the place of occurrence. All this makes investigations into cyber crimes a difficult and time consuming affair.

Most Judicial Officers and Judges lack expertise in adjudicating issues of cyber crimes. They are required to look at cyber criminal activity in a completely different light from what was taught to them in the law college. This is often not easy. Others find it difficult to adjust and adapt to technological advancements that have been taken place over the years. This makes the adjudication process somewhat complex, particularly in the matter of accepting as authentic digital evidence and analyzing it. The problem gets more complicated if the prosecutor and the defence counsel assisting the Court are themselves not fully equipped with the latest information and informed of the latest developments and technology.

The National Cyber Defence Reference Handbook which is going into its 2nd Edition will be an asset for all of us facing these and similar problems in the cyber world. I am sure that it will be an extremely useful desktop reference for all concerned. I would like to congratulate the National Cyber Safety and Security Standards for the task undertaken by it and am sure that it will benefit one and all.

My best wishes are for the success of the Reference Handbook and hope its contents are disseminated widely.

Madan Lokur

(Madan Bhimarao Lokur)

Honourable **Mr. Justice FM. Ibrahim Kalifulla**

Judge, Supreme Court of India, New Delhi.

I am extremely delighted to know that the National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative which will comprise the detailed perspective of the cyber-crimes and advanced cyber protection methodologies and controlling procedures/tools.

In present times, internet though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. In an age where e-mail and websites have become the preferred means of communication, cyber-crimes are on the rise including email phishing, hacking user's Id including their personal information, virus imitation and cyber vandalism etc. Because of its persistent nature, it is regarded as a bigger national security threat than terrorism. Therefore, it is imperative that private and public organizations collaborate to combat cybercrime and gain knowledge about security threats and how to respond to them. I sincerely believe that this handbook will definitely prove to be an indispensable tool for the Central / State Government Authorities and Constitutional Bodies to tackle the issues of cyber-crime and to protect national critical infrastructure while simultaneously ensuring sustained development of science and technology.

I extend my sincere appreciation to National Cyber Safety & Security Standards for making it possible such a wonderful and much needed initiative in the form of this handbook and wish all the success.

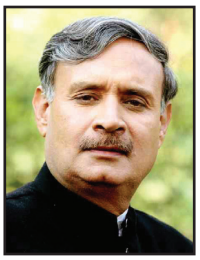
(FM. Ibrahim Kalifulla)

Honourable **Mr. Justice Vikramajit Sen**
Former Judge, Supreme Court of India, New Delhi.

This "National Cyber Defence Reference Handbook" is a salutary initiative, answering to a fundamental national security need of our time. The fluid nature of cyber crime makes it a permeating evil, persistent and dangerous beyond proportion. The advanced cyber protection methodologies and controlling procedures / tools proposed and presented herein will undoubtedly contribute to better cyber security, and the protection of India's national critical infrastructure, most of which exists today in a computer-dependent state. I further laud the complimentary issuance of 15000 copies hereof to State / Governmental Authorities and Constitutional Bodies; a pro bono measure, which will greatly supplement these vital State organs and institutions in effectively discharging their duties towards State security.

(Vikramajit Sen)

सत्यमेव जयते



Shri. **Rao Inderjit Singh**

Honourable Minister of State (IC) for Ministry of Planning and Minister of State for Defence, Government of India

I am happy to iearn that National Cyber Safety & Security Standards is publishing the 2nd edition of the "National Cyber Crime Reference Hand Book".

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural and the data exchanged in the cyberspace can be exploited for nefarious purposes by both the State and non-State actors. Large scale cyber-attacks may devastate the Government, public and private sector resources and services by disrupting the functioning of Critical Information Systems, which may threaten lives, economy and national security. With the launch of Digital India Programme, Cyber Security & safety has assumed greater importance.

I am sure that the proposed 2nd Edition of 'National Cyber Defence Reference Handbook' would cover the importance of cyber security awareness generation since Cyber Security is not just the concern of few but that of each and every netizen.

(Rao Inderjit Singh)

सत्यमेव जयते

Shri. **Dr. Mahesh Sharma**

Honourable Minister of State (IC), Ministry of Tourism Ministry of Culture Minister of State for Civil Aviation, Government of India

It gives me great pleasure in knowing that National Cyber Safety & Security Standards is bringing out the 2nd edition of "National Cyber Defence Reference Handbook".

Increased proliferation of Computers and Information Technology in practically every aspect of our lives, an exponential increase in E-Commerce has made our lives easier and given a different paradigm to the word 'comfort'. But the flipside is an explosive growth in the cybercrimes such as network intrusions, dissemination of computer viruses, identity theft, stalking, trolling, bullying, hacking, Trojan attacks, online frauds and cyber terrorism etc. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from household appliances to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications.

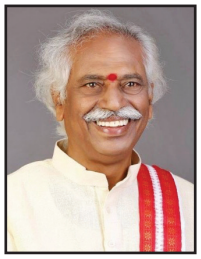
Cybercrimes can never be seen in isolation. Cyber attacks may be experienced by every single internet user and result in huge material or/ and immaterial damage. More must be done to harness the intelligence of network and information security stakeholders, not only to provide a more accurate and comprehensive assessment of cybercrime, but also to ensure that responses are effective and timely.

To tackle cybercrime efficiently, it is essential to establish active partnerships and cooperation between the Government, the nodal ministry. Security agencies, law enforcing bodies, private sector, information security organizations, financial institutions and public institutions to investigate cybercrime, to supervise financial market transactions and to enforce laws. Law enforcement agencies must work in partnership with those who will influence the future business and operating environment, so that all concerned can better anticipate changes in criminal behavior and technological misuse. Without efficient private-public cooperation, down to the level of an individual, cybercrime will never be tackled effectively. The synergisation of intent and efforts is absolutely imperative to curb this menace.

Iam sure that this handbook will be an invaluable and comprehensive source of reference material for not only the government but all the stakeholders in our collective quest of cyber security.

(Dr. Mahesh Sharma)

सत्यमेव जयते



Shri. **Bandaru Dattatreya**
Honourable Minister of State for Labour & Employment (IC)
Government of India

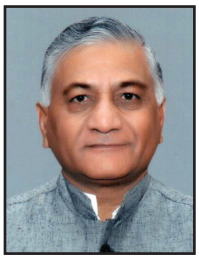
I am glad to know that the National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative to address the present issues on Cyber Crime. I am sure that the publication would be very useful to Central / State Government Departments/Police Departments and National Libraries all over the country. I believe this would also play a vital role as a reference material for various authorities and disseminate the greater knowledge on Cyber Security.

I congratulate the authorities of the High Level Committee of National Cyber Safety & Security Standards for issuance of this Handbook free of cost.

I wish the National Cyber Safety & Security Standards for all success in its activities.

(Bandaru Dattatreya)

सत्यमेव जयते



Shri. **Gen (Dr.) Vijay Kumar Singh**

Honourable Minister of State for External Affairs & Overseas Indian Affairs

Government of India

I am pleased to know that the National Cyber Safety & and Security Standards, Chennai is publishing a book titled 'National Cyber Crime Reference Hand Book 2 Edition' as a national initiative on the issues of cyber crime in the country.

I am sure the book will make the readers aware of cyber crimes and the advanced cyber protection methodologies and controlling procedures/tools.

I extend my best wishes to the National Cyber Safety and Security Standards for success in their endeavour.

(Gen (Dr) V.K. Singh)

सत्यमेव जयते

Shri. **Krishanpal Gurjar**

Honourable Minister of State for Social Justice & Empowerment

Government of India

I am happy to learn that the National Cyber Safety & Security Standards is publishing a book "National Cyber Defence Reference Handbook 2nd Edition" as a National Initiative to address the present issues on Cyber Crime.

It is good to note that the book will comprise the detailed perspective of the cyber crimes which are creating an enormous trouble for India's National Security. This book will also give us advance cyber protection methodologies and controlling procedures / tools.

I wish all success to National Cyber Safety & Security Standards in its future endeavours.

(Krishanpal Gurjar)

सत्यमेव जयते

Shri. **Sudarshan Bhagat**
Honourable Minister of State for Rural Development
Government of India

I am delighted to know that the National Cyber Safety & Security Standards is publishing a book "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative to address the present issues on Cyber Crime.

I appreciate the effort of National Cyber Safety & Security Standards in the field of cyber security and trust it will continue to serve for the cause of society in future also. It is heartening to note that the book will comprise the detailed perspective of the cyber crimes which are creating an enormous trouble for India's National Security and also that this book gives us advance cyber protection methodologies and controlling procedures/tools.

I convey my best wishes to the National Cyber Safety & Security Standards for publication of the handbook and the event all success.

(Sudarshan Bhagat)

सत्यमेव जयते

Shri. **Vishnu Deo Sai**
Honourable Minister of State for Steel and Mines
Government of India

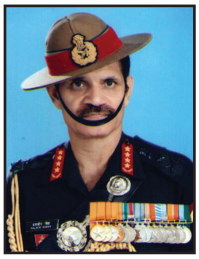
संदेश

मुझे यह जानकर अत्यन्त प्रसन्नता हो रही है कि राष्ट्रीय साइबर रक्षा अनुसंधान केन्द्र के अंतर्गत राष्ट्रीय साइबर सुरक्षा एवं सुरक्षा मानकों के दवारा **'राष्ट्रीय साइबर अपराध संदर्भ हैंडबुक-2 संस्करण'** प्रकाशित होने जा रहा है, जिसमें साइबर अपराध के संदर्भ में विस्तृत जानकारी उपलब्ध कराई जा रही है, जो आज भारत की राष्ट्रीय सुरक्षा के लिए गंभीर चुनौती बना हुआ है साथ ही यह पुस्तक साईबर सुरक्षा प्रणाली एवं इसके नियंत्रण तकनीकों के बारे में अवगत करायेगी। इस प्रकार की सामग्री का प्रकाशन वास्तव में एक सराहनीय प्रयास है।

मैं इस अवसर पर प्रकाशित की जाने वाली **'राष्ट्रीय साइबर अपराध संदर्भ हैंडबुक-2 संस्करण'** के सफल प्रकाशन की कामना करता हूँ एवं इसके सम्पादकीय सदस्यों को हार्दिक बधाई देता हूँ ।

(Vishnu Deo Sai)

General **Dalbir Singh**
PVSM, UYSM, AVSM, VSM, ADC
Chief of the Army Staff, Indian Army



The reach and vulnerability of the cyber space has necessitated its continuous appraisal in terms of security. The 'National Cyber Crime Reference Hand Book' is, therefore, a welcome endeavour in the right direction. In addition to providing a thorough insight into the issues of cyber crime, the handbook is also a medium of spreading cyber security awareness in the environment, particularly when cyberspace has also been recognized as the first man made domain of warfare.

I am sanguine that the publication of this reference book will further inspire more intense discussions on cyber security.

JAI HIND

(Dalbir Singh)
General

सत्यमेव जयते

Admiral **RK DHOWAN**
PVSM, AVSM, YSM, ADC
Chief of the Naval Staff, Indian Navy

The initiatives of National Cyber Safety and Security Standards to counter multi-dimensional threats from cyber space have their relevance in the Navy's perennial drive to protect critical IT infrastructure.

(RK Dhowan)
Admiral

सत्यमेव जयते

Honourable **Mr. Justice Mansoor Ahmad Mir**
Chief Justice, High Court of Himachal Pradesh

I am extremely delighted to learn that the 'National Cyber Safety & Security Standards is bringing out the 2nd edition of the National Cyber Defence Reference Handbook. Need for such a handbook cannot be over emphasized in an era where computers have become indispensable part of our lives. Be it the ubiquitous desktop in an office, laptop with the professionals or smart phone with the common man- Even everyday gadgets like TV, refrigerator, washing machine, car, camera etc. have computers embedded in them. While the computers have made our lives easier, they have given an easy tool to the criminals to invade our lives. According to National Cyber Records Bureau, a total of 1,791, 2,876 and 4,356 cases were registered under the Information Technology Act in 2011, 2012 and 2013, respectively. This shows an increase of more than 51%. According to latest report by Motive Security Labs, security arm of Alcatel-Lucent about 16 million smart phones are infected by malware worldwide. Report further warned that even the point of sale terminals were infected with the malware which could steal the information contained in ATM or Debit card. Another study by Assocham-Mahindra SSG pointed out that number of cyber crimes in the country may double to 3 lakh in 2015.

In such a scenario, the importance of educating the user cannot be minimized. There is need to educate people on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology, such as firewalls, anti-virus software, intrusion detection tools, and authentication services, throughout the organizations' computer systems. I am sure that National Cyber Defence Reference Handbook will provide such information in easy to understand language helping the end user to take preventive steps to stem the tide of increasing cyber crimes. Distribution of the book free of cost to the Central/State Government Departments/Police Departments/ National Libraries by National Cyber Safety and Security Standards is laudable. I expect that the users will make full use of the handbook to equip themselves against the increasing crime. I wish the handbook a resounding success.

(Mansoor Ahmad Mir)

Honourable **Mr. Justice Deepak Gupta**
Chief Justice, High Court of Tripura

I am very happy to note that the National Cyber Safety and Security Standards is bringing out the National Cyber Defence Reference Handbook. In the modern world cyber crime is increasing at a fast pace. Therefore, the members of the police and legal fraternity must be equipped with the knowledge to deal with such cases.

By incorporating the latest advancements in the fields of cyber protection methodologies and controlling procedures, this Handbook proves itself really handy as a very potent weapon in combating cyber crime. I wish this Handbook all the success it deserves and suggest that all who are engaged in this relentless fight against cyber crime should make it a part of their arsenal.

I am sure that this Reference Handbook will be a great asset to the Police, the Public Prosecutor and the Judges while dealing with such cases.

(Deepak Gupta)

Honourable **Mr. Justice Ashok Bhushan**
Chief Justice, High Court of Kerala

I am very happy to know that the National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" with a view to vindicate the present issues on Cyber Crime faced by our country. I understand that the book contains topics on advanced cyber protection methodologies and controlling procedures/tools. I am sure, the book will act as a useful reference guide on Cyber Security.

On this occasion, I appreciate the efforts of the organization in releasing the book as a National Initiative and wish the endeavour a grand success.

(Ashok Bhushan)

Honourable **Mr. Justice A.M. Khanwilkar**
Chief Justice, High Court of Madhya Pradesh

I am happy to learn that the "National Cyber Safety and Security Standards", Chennai is publishing its second edition of "National Cyber Defence Reference Handbook ".

The first edition received accolades from all quarters, for being instructive and educative. It not only helped the members of the legal profession but also other duty holders.

The need for a compendium covering multi-dimensional aspects relating to Cyber Crimes including advanced cyber protection, investigation and controlling procedures cannot be underscored - keeping in mind the challenges arising from invasion/hacking by criminals and anti national elements of Government official websites, in particular.

The handbook showcases the arduous task undertaken by the team engaged in preparing the same - which delineates holistic approach on intricate issues of Cyber Crimes.

This handbook will provide further insight to the stakeholders as also to those wanting to enlighten themselves with the new horizons in this field.

I extend my best wishes for the success of the publication and congratulate the National Cyber Safety and Security Standards, in publishing the second edition of the handbook.

(A.M. Khanwilkar)

Honourable **Mrs. Justice S.Vimala**
Judge, Madras High Court

Here is a bridge ready to connect the digital haves and digital have nots. This handbook could not have come into existence in a more appropriate time, than the present one. While there is a manifold increase in cyber crimes and the legal enforcement agencies are groping in darkness, being miserably under-equipped, nay, ill prepared to outsmart and outpace the criminal minds, it is equally amazing and awesome to see that the contours of cyber law are redrawn very frequently. The question of jurisdiction, defamation, freedom of expression, electronic taxation or intellectual property rights are becoming global issues in the face of cyber onslaught.

However, all of those who perceive the paucity of an Indian perspective will be assured of a constant companion, in their quest for demystifying the cyber crimes, with the arrival of this Handbook.

A right book at the right time, is how I want to describe this endeavour and wishes many more on this line.

(S.Vimala)

Honourable **Mr. Justice R.K. Deshpande**
Judge, High Court at Bombay

I am fortunate to get this opportunity to deliver the message in National Cyber Defence Reference Handbook 2nd Edition.

Cyber crimes have posed a serious threat to the security of the nation. The prevention and control of it, is the greatest challenge before us. To inculcate knowledge of methodologies and techniques adopted to commit such crimes, is the need of the day so as to enable us to take appropriate measures to prevent it.

I congratulate the National Cyber Safety and Security Standards, which has taken initiative to address such issues by presenting a National Cyber Defence Reference Handbook 2nd Edition. I hope, trust and believe that this Handbook shall prove to be fruitful to give us advanced cyber protection methodologies and controlling procedures/tools and infrastructures.

Once again congratulating you, I express my gratitude.

(R K Deshpande)

Honourable **Mr. Justice V.M. Kanade**
Judge, High Court at Bombay

I am happy to learn that National Cyber Safety and Security Standards is publishing 2nd Edition of "National Cyber Defence Reference Handbook" as a national initiative to address the present issues on Cyber Crime.

The number of filing of complaints has increased progressively over the past decade. It is necessary to educate the Investigating Officers, Public Prosecutors as well as the Judicial Officers on this subject.

I wish all success to the National Cyber Safety and Security Standards and its staff in this endeavour.

(V.M. Kanade)

Honourable **Mr. Justice Ram Mohan Reddy**
Judge & Chairman, Committee for Computerisation,
High Court of Karnataka.

Cyber Crime is the new war of 21st century.
The key board has replaced the gun.

It gives me great sense of pride that the National Cyber Safety and Security Standards has decided to issue National Cyber Defence Reference Handbook 2nd Edition as a National Initiative to address the present issues on cyber crime.

The essential element of change in all spheres of life is "Technology". With the advent of technology, the risk factor of misuse is imminent. The proper use of technology makes changes for betterment of life.

The Nation relies upon computers and relatively small disruption of its economic system would have wide spread serious consequences. So also is National Security. As consumers go mobile so do cyber criminals while cyber crime goes social.

Global experience in cyber hacking into computer networks steal valuable trade secretes, intellectual property and confidential strategies. For a common man, the frequently asked question is "What would you do, if you could not access your bank account or your credit/ debit card?" Everything you have worked for could be lost in a click of the mouse.

Cyber world is a jungle and a dangerous one, but with simple steps, precautions, self education and common sense, can dramatically minimize the risk. Although law has developed new rules relating to operation of computers and internet as well as punishment, nevertheless, the order of the day is cyber crime awareness.

It is gratifying to note that the Hand Book provides Cyber Protection Methodologies and Controlling Procedure/Tools, some simple, yet effective to help avoid being a victim.

(Ram Mohan Reddy)

Honourable **Mr. Justice Anand Byrareddy**

Judge, High Court of Karnataka

The proliferation and integration of Computers into every aspect of Society has inevitably led to computer-related criminal activities.

Crimes involving the use of Computers can generally be distinguished into three categories:

i. Traditional types of criminal offences that may be committed using Computers as the instrument of the crime.

ii. Content related crimes, primarily involving intellectual property and pornography.

iii. Offences that have been established specifically to address activities that attack the integrity of Computer and communication systems. Computer intrusions are accomplished by the use of malware, a term derived from combining malicious and software

In the last of the above categories, one aspect of concern relates to terrorism and the possibility that computer based attacks may be launched against a nation's critical infrastructure, such as tele-communication systems, national security information, systems operating power stations and air traffic control Systems and a host of other support systems.

National Cyber Safety and Security Standards - an autonomous body - has, after extensive research in the cyber domain to understand the nature of cyber threats and cyber crimes has found that it cannot be handled by common place security policies - and has thus endeavoured to take the Safety Security Standards to the next level by developing innovative strategies and compliance procedures to curb the increasing complexity of the global cyber threats and the result is this Second Edition of the National Cyber Defence Reference Handbook.

And to impart this information and knowledge to key personnel manning important positions in the country is a thoughtful measure that could not have come sooner.

Every recipient of this valuable document would certainly benefit immensely and would be in a position to usefully apply the tools and processes when the need arises.

With best wishes,

(Anand Byrareddy)

सत्यमेव जयते

Honourable **Mr. Justice C. K. Abdul Rehim**
Judge, High Court of Kerala

Cyber law in the country is emerging as an important field of jurisprudence in the present scenario. Magnitude and adversity of cyber crimes affecting personal liberty of individuals, order of the society and national safety is alarmingly increasing. Awareness about intricacies and perspectives of the crimes as well as about the law governing the field is an absolute essential.

It is with immense pleasure I notice that the National Cyber Safety and Security Standards is publishing a handbook on National Cyber Crime Reference. I hope this work would be of great use to equip all concerned to have adequate protective and controlling measures

I congratulate the entire team responsible in the National Cyber Safety and Security Standards for taking up such a noble venture and wish all success in the endeavour.

(C.K. Abdul Rehim)

सत्यमेव जयते

Honourable **Mr. Justice Pritinker Diwaker**
Judge, High Court of Chhattisgarh.

I am happy to learn that National Cyber Safety and Security Standards is publishing 2nd Edition of "National Cyber Defence Reference Handbook" as a national initiative to address the present issues on Cyber Crime.

I came to know that the National Cyber Safety & Security Standards is going to publish "National Cyber Defence Reference Handbook 2nd Edition. This wonderful initiative taken by your good-self gives me a lot of happiness and I am sure that the same would go a long way in curbing the issues relating to Cyber Crime.

I hope that this noble endeavour of your good-self would prove to be a treasure trove for the general public as well as the people hailing from legal fraternity.

(Pritinker Diwaker)

Honourable **Mr. Justice R. Mahadevan**
Judge, Madras High Court

It is really happy to learn that the Naitional Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition".

When our country is facing alarming threat from the perpetrators of cyber crimes, the publishing of "National Cyber Defence Reference Handbook 2nd Edition" will be an effective tool to combat cyber crimes and I have no iota of doubt that this book will be very useful and helpful to the unlettered and lettered.

(R. Mahadevan)

Honourable **Mr. Justice R. Sudhakar**
Former Judge, Madras High Court

I am happy to learn that the National Cyber Safety and Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative to address the present issues on Cyber Crime.

Our country took a big leap forward in technology and with that the misuse of technology has also increased manifold in the form of cyber stalking; cyber harassment; data diddling; hacking, etc. To deal with such crimes sternly cyber laws have been enacted and are strictly implemented. However, there is lack of awareness about the advanced protection methodologies and controlling procedures/tools and the same is obvious from the low reporting rate of cyber crimes. Therefore, in order to prevent cyber crime, it is important to educate everyone.

It is in this scenario that the publishing of National Cyber Defence Reference Handbook 2nd Edition gains added prominence, as it will contain the detailed perspective of the cyber crimes and also specifies the advanced cyber protection methodologies and controlling procedures/tools.

This book intended to be issued to the State/Central Government Authorities and Constitutional Bodies would definitely be great help in detecting cyber crimes.

I congratulate the Chairman and everyone associated with the National Cyber Safety and Security Standards for taking the initiative to make a publication on this modern day problem.

(R. Sudhakar)

Honourable **Mr. Justice Ravi R Tripathi**
Former Judge, High Court of Gujarat

It is with profound sense of satisfaction that I am writing this message when the National Cyber Safety & Security Standards is all set to launch "National Cyber Defence Reference Handbook - 2nd Edition" intended to be circulated to Governmental / Constitutional authorities / bodies free of cost. The initiative is timely and laudable.

Cyber technology is not static one. It undergoes changes from time to time, decade after decade. Dealing with its use and misuse is a multi-disciplinary and challenging task. Users of cyber technology range from a minor child to elderly person, viz. a child watching cartoon games, a student learning lessons, a family electronically communicating, a professional transacting business safely and ensuring that his employer's information, communications are secure, an official dealing with national security, and so on. At the same time, it is misused by many, viz. youth can indulge in unhindered pornography, an unscrupulous person can effectively commit robberies, anti-national elements can pose serious threat to national security/ integrity, economy, etc.

Technological innovations in cyber world would require constant and continuous moulding in dealing with cyber crimes. Curricula be updated and devised commensurate with the demands of the day from cyber technology, preferably, multi-disciplinary one. Meaning thereby, component at adjudicating system should be able to evaluate electronic evidence tendered by the parties, draw inference and reach conclusions leading to effective dispensation of justice. Similarly, defence personnel needs to conduct electronic surveillance/ interception of huge quantity of information and take remedial measures eliminating potential threat to the nation.

I am sure the Handbook will address all the issues on cyber crime. On this occasion I wish successful publication of the Handbook and its effective use.

(Ravi R Tripathi)

सत्यमेव जयते

Honourable **Mr. Justice T.P. Sharma**
Former Judge, High Court of Chhattisgarh

Congratulations on the upcoming publication of the 2nd Edition of National Cyber Defence Reference Handbook. I hope, this Handbook will prove to be a valuable resource for all concerned and will help counter incidences of cyber crime.

The Handbook will also help to provide much needed perspective on cyber crimes and measures needed to be adopted to counter such threats to India's national security. As I understand, the Handbook also contains information about advanced cyber protection methodologies and controlling procedures and tools, which will prove useful to the concerned departments and agencies.

I deeply appreciate this initiative of the 'National Cyber Safety & Security Standards' and wish all their future endeavours my very best.

12.3.15

(T.P. Sharma)

Honourable **Mr. Justice B K Patel**
Former Judge, High Court of Odisha
Chairman - National Advisory Committee,
National Cyber Safety and Security Standards

I am glad to know that National Cyber Safety and Security Standards, is going to publish "National Cyber Defence Reference Handbook 2nd Edition".

I had opportunity to participate in the National Cyber Safety and Security Standards Summit-2014 (2nd Edition) held on 19th September, 2014 at Coimbatore when I had the privilege to come across the 1st Edition of the Reference Handbook. I felt educated to have a new boarderless cyber world at my disposal more securedly.

Cyber Crime in the digital world is spreading menace round the clock across the nations. Individually, the privacy is at stake. State Nations are engaged to institutionalize investigative and adjudicatory wings in a better way to counter the threat perception. The concern of National Cyber Safety and Security Standards to advance the cyber protection methodologies and tools would definitely protect the individual privacy and National Security.

I convey my best wishes for the success of the handbook.

(B.K. Patel)

Shri. **Anthony de Sa, I.A.S.,**
Chief Secretary
Government of Madhya Pradesh

I am pleased to learn that National Cyber Safety & Security Standards is going to bring out the 2nd edition of the National Cyber Defence Reference Handbook.

This is a very welcome initiative since today many aspects of our lives rely on increased use of computers and Internet, including information and communication technologies.

I hope this initiative will not only help in spreading awareness on the volume and sophistication of cyber security threats and instances, and the need for adopting safe practices, but also enable professionals to absorb standard security procedures and prevent and contain security breaches.

I congratulate the NCSSS for this effort and wish it all success in this endeavour.

(Anthony de Sa)

Shri. **Jiji Thomson, I.A.S.,**
Former Chief Secretary
Government of Kerala

I am extremely happy to know that National Cyber Safety & Security Standards is publishing "National Cyber Crime Reference Hand Book 2nd Edition". I am sure that this Handbook will be certainly a coveted volume of reference material to enrich a greater knowledge on Cyber Security for the entire Government administraton and to provide better and effective services in the field.

I also take this opportunity to appreciate the members of the team for the efforts taken by them to prepare the publication.

(Jiji Thomson)

Shri. **Kaushik Mukherjee, I.A.S.,**
Former Chief Secretary
Government of Karnataka

I am happy to learn that the National Cyber Safety & Security Standards headed by Honourable Dr.Justice S.Mohan, Former Judge, Supreme Court of India, is publishing its 2nd Edition of "National Cyber Reference Handbook" which comprises detailed perspective of the cybercrimes, and reveals advanced cyber protection methodologies and controlling procedures / tools.

I believe that free distribution of this book to the Central/State Government Departments / Police Departments / National Libraries throughout the country will serve the purpose as a reference book for the Government departments and the Judicial authorities to enhance their sphere of knowledge on Cyber Security.

I wish all the best for this publication of a national initiative.

(Kaushik Mukherjee)

सत्यमेव जयते

Shri. **Barkos Warjri, I.A.S.,**
Former Chief Secretary
Government of Meghalaya

I am glad to learn that the office of the Additional Director General National Cyber Safety and Security Standards (An Autonomous Body), CYBER HOUSE - Southern Region is publishing the "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative to address the present issues on Cyber Crime.

Information Technology has opened up an entirely different field and new challenges. Cyber crime can be a threat to national security as well as financial stability. The Modern world is a world where computers, laptops and the internet have become a part of everyday life and this medium has also become a tool for criminals who have entered the cyber world and thrived there, in a world without geographical boundaries.

Meghalaya too, like other States, has become susceptible to cyber crime and with increasing cases of cyber crime reported in the State, a cyber crime wing has been set up.

The "National Cyber Crime reference Handbook 2nd Edition" shall hopefully serve as a reference source for various agencies of the Central and State Governments enhancing their knowledge and understanding of cyber security.

I congratulate the National Cyber Defence Research Centre for its efforts in bringing out the second edition of the Handbook.

(Barkos Warjri)

सत्यमेव जयते

Shri. **Pachau Lawmkunga, I.A.S.,**
Former Chief Secretary
Government of Manipur

I am extremely happy to note that the "National Cyber Defence Reference Handbook" is being published by the "National Cyber Safety & Security Standards". This endeavour of a standardized approach to counter the menace of cyber offences will definitely go a long way in setting a framework of response. Cyber space has emerged as a space of opportunity and the counter-point of opportunity is the misuse of it. Since technology is ever evolving, our apprehension is the concomitant expansion and evolution of the spectrum of cyber-crime. This forthcoming Reference Handbook assumes extreme importance in such a context.

I am sure that it would be a tremendously useful reference for all the stake-holders, within the Government and outside, in effectively dealing with the malicious use of cyber space. I wish the "National Cyber Safety & Security Standards" the very best and response my confidence in them in responding to any new threats with relevant updates in future.

My best wishes to National Cyber Defence Reference Handbook in this endeavour.

18/2/2014

(Pachau Lawmkunga)

सत्यमेव जयते

Shri. **G. Kameswara Rao, I.A.S.,**
Former Chief Secretary
Government of Tripura

I am happy to learn that the National Cyber Safety and Security Standards is going to publish 2nd Edition of the "National Cyber Crime Reference Hand Book" (NCCRHB).

Due to immense increase in the use of Internet and dependency of individuals in every field, a number of new crimes related to computer and other gadgets based on internet, broadly termed as cybercrimes, have evolved in the society. While information technology has proved as a blessing of science, there are many examples of curse of this science gifted technology. There are many instances of internet hackers intruding upon and leaking of most secret government documents. Money from bank accounts is being stolen by hacking secret number using this system. Extremists both overseas and inside extensively use this system to harnr people. Thus, every document has become insecure and is prone to hack. In fact, the more we depend on the information technology system, the more we are prone to great losses. Side by side, remedies also are being thought of and put in place. So, compilation of this reference handbook would certainly give a valuable resource for all concerned to counter incidence of cybercrime and threats to security.

I appreciate this noble initiative of the National Cyber Safety and Security Standards.

19/2/15

(G. Kameswara Rao)

उत्तराखण्ड राज्य

Shri. **N Ravi Shanker, I.A.S.,**
Former Chief Secretary
Government of Uttarakhand

I am delighted to know that National Cyber Safety & Security Standards is publishing 2nd Edition of "National Cyber Defence Reference Handbook" on Cyber Crime.

In present scenerio the cyber crimes are increasing day by day Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Awareness is the first step in protecting yourself, society and the nation.

I hope that the contents of this issue will be very useful to all readers. I send my blessings and best wishes.

N. Ravi Shanker

(N Ravi Shanker)

सत्यमेव जयते

Shri. **Rajeev Gupta, I.A.S.,**
Secretary, Department of Youth Affairs, Ministry of Youth Affairs & Sports
Government of India

India has the second largest number of internet users in the world after China. The total number of internet users by the end of 2014 has been pegged at 302 million. With ever increasing number of net users, there has also been marked surge in the cyber crime rate in the country. India's registered cyber crime leapt 350% in 3 years and the legal system is struggling to cope with more and more law-breakers exploiting the anonymity of the internet. The statistics also reveal that the age group of 18-30 accounts for the highest percentage of cyber crime in the country. The cyber crimes have assumed serious proportions and have started posing a threat to the society and the national security.

The present situation calls for remaining vigilant and well equipped in terms of knowledge and tools to surmount this menace. I am extremely happy that the National Cyber Safety & Security Standards (NCSSS) is bringing out"National Cyber Defence Reference Handbook 2nd Edition" at the opportune time when cybercrimes are assuming menacing proportions.

This handbook shall not only provide an insight into the ongoing cybercrimes but also enlighten about the advanced cyber protection methodologies and controlling procedures/ tools. We in the Department of Youth Affairs shall make use of this handbook to educate the youth of the country. I am sure that others will also find this handbook immensely useful in effectively dealing with cybercrimes.

NCSSS deserves all accolades for bringing out this excellent publication.

(Rajeev Gupta)

सत्यमेव जयते

Shri. **Prabhu Dayal Meena, I.A.S.,**

Secretary, Dept. of Ex-Servicemen Welfare, Ministry of Defence

Government of India

I am happy to learn that National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" to address the present issues on Cyber Crime.

The Handbook will comprise the detailed perspective of the cybercrimes which are creating trouble for India's National Security and also give us advanced cyber protection methodologies and controlling procedures/tools. This publication will definitely enhance knowledge on Cyber Security and serve as a reference material for all the stakeholders.

I convey my best wishes to the team of National Cyber Safety & Security Standards for publishing such useful Handbook on a critical and important issue. I also wish success in all their future endeavours.

14.01.2015

(Prabhu Dayal Meena)

सत्यमेव जयते

Shri. **Rakesh Garg, I.A.S.,**
Secretary, Ministry of Minority Affairs
Government of India

I am happy to hear that the National Cyber Safety & Security Standards is coming out with the 2nd Edition of their National Cyber Defence Reference Handbook. The cyber world has touched multifarious aspects of human activity and is reaching to being ubiquitous in time, space and persons. The benefits of the proliferation of cyber solutions are there for all to see and have resulted in bringing convenience and cheer to all strata of society. However there have been genuine concerns on the safe use of the cyber space including protecting our children online, the security of the transactions and for monitoring nefarious online activities. The understanding of the applicability of cyber laws, adjudication and their enforcement also requires skill sets at variance with traditional law enforcement. This area in cyber space presents an evolving and ever changing challenge to secure cyber space that requires proactive action to keep up with emerging technologies and modes of cyber operations. I hope that the National Cyber Defence Reference Handbook will act as a source for reference and in no small measure help the professionals in the field of handling Cyber Crime.

(Rakesh Garg)

सत्यमेव जयते

Shri. **Naved Masood, I.A.S.,**
Former Secretary, Ministry of Corporate Affairs
Government of India

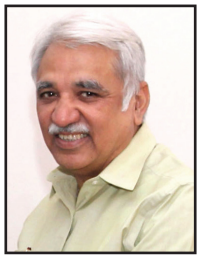
Information and Communications Technology(ICT) is contributing immensely to the advancement of society, individuals and business. Increased use of ICT, however, has made society more vulnerable to cyber-crimes, with threats to ICT systems and cyber-attacks becoming more sophisticated. Therefore, information security has become an important aspect of national security.

I am glad to learn that National Cyber Safety & Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition" as a national initiative to address the present issues on cyber crime. I convey my good wishes on this occasion.

G. Venkata Subbaiah

(G. Venkata Subbaiah)
Under Secretary to the Government of India

सत्यमेव जयते



Shri. **Sunil Arora, I.A.S.,**

Former Secretary, Ministry of Skill Development & Entrepreneurship
Government of India

It is indeed heartening to know that National Cyber Safety and Security Standards are publishing 2nd edition of 'National Cyber Defence Reference Handbook'. With every passing year, the number of internet users is increasing exponentially, as indeed should be the case in any vibrant and growing economy. With the rise in the use of internet as the daily mode of operation in Government Offices, PSUs, Universities, Banking and Online Retailing etc. cyber crime and security related issues have also started cropping up. It is, therefore, imperative that such interventions should be made that facilitate security in a more effective manner.

We do have legal framework like IPC and IT Act to cover many cyber crimes. But as the nature of crime changes very fast, more systemic efforts would have to be made to create a strong encryption or firewall which can ensure that Governments websites / accounts information of a confidential nature is available only on the need to know basis. The need of security awareness training as being critical for all end users cannot be overemphasized.

Taking the assistance of agencies such as Internet Governance Forum (an International Agency on Internet Governance), Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF) will help in creating an infrastructure, that secures and preserves data and thereby ensures cyber safety and security.

I am sure this book will go a long way in spreading cyber security awareness among the stakeholders. My best wishes for the publication of the book.

(Sunil Arora)

सत्यमेव जयते

Shri. **Dr. Shailesh Nayak, I.A.S.,**
Former Secretary, Ministry of Earth Sciences
Government of India

India at present is in the regime of rapid growth with a transitional mode of transformation to a digitally empowered society and knowledge economy. It is thus imperative that along with this transformation, the National Cyber Safety and Security Standards becomes an integral part of the entire system. In order to protect our mission critical information and information infrastructure in cyberspace, necessary security measures are required to be undertaken through well defined preventive measures and reducing vulnerabilities towards minimizing damage from cyber crimes.

Earth System Science Organisation, Ministry of Earth Sciences has been providing the nation with best possible services in forecasting the monsoons, climate information systems, ocean state, earthquakes, tsunamis and other phenomena related to earth systems through its well integrated programmes. It uses latest sophisticated technology in the field of computation, evaluation, information and communication. The core of all prediction capability is in ensuring a robust and reliable cyber infrastructure. The information generated using high-end cyber resources is used in disaster planning, aviation, shipping, climate mitigation strategy and scores of other strategic applications. Any breach of cyber infrastructure shall have a far reaching consequence on the society which can endanger the security of the country.

The history of crime has proved that the form and dimension has multiplied over time which will continue to transform itself with the advent of technology. The positive aspect of technology and its adverse effects will always sail together. The challenge here is to identify these and safeguard our valuable digital assets. Cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today's security landscape with the proliferation and ubiquitousness of computer networks.

The "National Cyber Crime Reference Hand Book" (NCCRHB) is thus very timely and appropriate which shall help the stakeholders analyze many of the motivations, tools, and tactics behind cyber attacks and the defense preparedness required to thwart such attacks.

I wish that this novel initiative shall serve as the most comprehensive guideline to ensure a safe, reliable and secure cyber infrastructure in the country. This is particularly important because cyber crime is quintessentially trans-national and can be detrimental for information dominance.

(Shailesh Nayak)

सत्यमेव जयते

Shri. **Dr. Satish B. Agnihotri, I.A.S.,**
Former Secretary (Security), Cabinet Secretariat
Government of India

Cyber space is today becoming as important in our lives as the physical space is. It is not surprising that cyber space also becomes prone to similar threats and vulnerabilities as the ones faced by the physical space. In addition cyber space lacks many of the protection and safety measures that have evolved over the ages in respect of physical spaces - commons as well as private space.

I am happy, therefore, to learn that National Cyber Safety and Security Standards is coming out with a 2nd edition of its National Cyber Crime Reference Hand book which will focus attention on various types of cyber-crimes and educate the readers regarding protection methodologies and procedures. It provides an in-depth and comprehensive coverage of diverse range of cyber risks. The Handbook spells out the approach required to protect critical infrastructure and the dynamic, layered security protocols that need to be put in place to deal with new technologies and threats.

I compliment the organization and wish all success in its endeavours.

(Satish B. Agnihotri)

सत्यमेव जयते

Shri. **Dr. Vishwa Mohan Katoch, I.A.S.,**

Former Secretary, Indian Council of Medical Research, Ministry of Health and Family Welfare, Government of India

I am happy to learn that the National Cyber Safety & Security Standards is publishing a book "National Cyber Defence Reference Handbook 2nd Edition" as a National Initiative to address the present issues on Cyber Crime.

I hope that this handbook will be of immense use to curb Cyber Crimes which may pose serious threat to Nation's Security and also to Society.

I convey my best wishes to National Cyber Safety & Security Standards for bringing out this Handbook.

(V.M. Katoch)

सत्यमेव जयते

Shri. **Dr. Lalit K. Panwar, I.A.S.,**
Former Secretary, Ministry of Tourism Transport
Government of India

I am happy to learn that the National Cyber Safety and Security Standards is publishing the second edition of the "National Cyber Defence Reference Handbook".

In the fast changing global security scenario, safeguarding the Nation's critical infrastructure from physical and cyber threats that can affect internal security, public safety and economic growth is of paramount importance for all countries.

The world is increasingly connected to internet with new technologies and devices. The time has come to understand how to manage issues regarding Cyber Security and our privacy. A concerted effort is required to create awareness about the importance of protecting privacy, safeguarding data and enabling trust.

I am sure the reference handbook would be a useful tool for enhancing knowledge on cyber crime amongst Governmental agencies.

I wish the National Cyber Safety and Security Standards all success in its endeavour.

(Lalit K. Panwar)

सत्यमेव जयते

Shri. **Bimal Julka, I.A.S.,**
Former Secretary, Ministry of Information & Broadcasting
Government of India

I am happy to learn that NCSSS is in the process of publishing the 2nd edition of "National Cyber Defence Reference Handbook". The importance of cyber-security in the present context cannot be overemphasised. ICT is now an integral part of our everyday life in all activities, and as a consequence the risks of cybercrime are increasing exponentially.

I am sure that the reference book will be a valuable resource for all concerned.

(Bimal Julka)

Shri. **A.N. Upadhyay, I.P.S.,**
Director General of Police
Chhattisgarh

It gives me great pleasure to put my views in the National Cyber Defence Reference Handbook. It is a matter of satisfaction that this Handbook would cover various aspects, concerning cyber crime including suggestion for effective implementation of strategy that will provide advanced cyber protection methodologies and procedures/tools.

I am sure that this Handbook will provide a valuable insight to police investigators, forensic experts, security administrators and judiciary to cheek and combat the growing menace of cyber crime more effectively.

(A.N. Upadhyay)

Shri. **Shahid Ahmad, I.P.S.,**
Director General of Police
Manipur

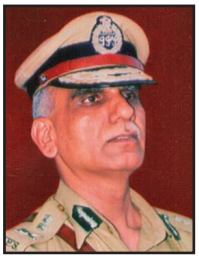
I am happy to learn that National Cyber Safety and Security Standards is publishing "National Cyber Defence Reference Handbook 2nd Edition". I hope it will help us in providing advanced cyber protection methodologies and controlling procedures/ tools for India's National Security and also enhance our knowledge on Cyber Security.

I wish the publisher a grand success.

13/1/15

(Shahid Ahmad)

Shri. **Surendra Sinh, I.P.S.,**
Director General of Police
Madhya Pradesh



I happy to learn that the National Cyber Safety and Security Standards is going to bring out the 2nd edition of National Cyber Defence Reference Handbook, so as to help the professionals engaged in providing security/ protection against computer/ internet related crimes.

I hope that this initiative will not only spread awareness on cyber security, ensure adaptation of cyber protection methodologies, but also enable the specialists to implement, standardize and control procedures and tools efficiently.

I congratulate the authorities for this noble effort and wish them all the success in this endeavour.

(Surendra Sinh)

सत्यमेव जयते

Shri. **P.K. Thakur, I.P.S.,**
Director General of Police
Bihar

I am pleased to know that the National Cyber Safety & Security Standards is going to publish 2nd edition of "National Cyber Defence Reference Handbook".

Today in the world of rapid changing technologies entire globe could be the crime scene in cyber world without any sign of physical violence or struggle at the scene of crime. Most cybercrime is an attack on information about individuals, corporations, or governments. This has encouraged the law enforcement agencies to be up-to-date in cyber protection methodologies and controlling procedures as well as cyber forensic examination.

I wish the chairman Honorable Dr. Justice S. Mohan, Former Judge, Supreme Court of India and the members of the committee best of luck for the publication of the 2nd edition of the handbook. I am sure this book will give enormous information about the National Cyber Security & Safety measures to the Administrative as well as the Judicial Authorities in the country.

19/1/15

(P. K. Thakur)

सत्यमेव जयते

Shri. **Dharmendra Kumar, I.P.S.,**
Former Director General of Police
Mizoram

It gives me immense pleasure to note that the National Cyber Defence Reference Handbook 2nd Edition has been meticulously put together by the National Cyber Safety and Security Standards as a national initiative and 1 feel that it would be of enormous help in acting as a guide for investigating officers and addressing the issues faced by police while tackling cyber crime cases.

The upward trend in cyber crime is a worrying factor for everyone as the internet and digital technologies are transforming societies by driving economic growth, connecting people and providing new ways to communicate and co-operate with one another across the world on the one hand and on the other hand this growing role of cyberspace has opened up new threats of cyber crimes that were inexistent a few years ago. Rapid increase in the use of computers, mobile phones, network, online activities and social media by individuals, commercial organizations and Government agencies for financial transactions has further increased the avenues for cyber criminals and a bigger challenge for the police officers since investigation of such crimes requires special skills, tools and procedures that most police officers are unequipped with. Further, administrative authorities, civil servants and judicial authorities lack the required knowledge of cyber security and this poses a perpetual risk in future with more transactions being rapidly shifted to the cyber space.

Therefore, it is heartening to learn that the National Cyber Defence Reference Handbook 2nd Edition, comprising of detailed perspectives on cyber crimes in India and the much needed advanced cyber protection methodologies and controlling procedures/tools is being published, which shall act as a great referral guide for police officers wanting to educate and update themselves on this issue. Moreover, I am particularly delighted to learn that 15,000 copies of this handbook are being issued free of cost for Central/State Government Departments, Police Departments and National Libraries all over the country, which shall be a boon for Police Organizations in updating themselves professionally.

I sincerely convey my genuine appreciation to National Cyber Safety and Security Standards for bringing out this handbook and I am sure that this will serve as a valuable reference material for law enforcement agencies, administrative and judicial authorities in providing them with greater knowledge on cyber security.

21/1/15

(Dharmendra Kumar)

Shri. **Omendra Bharadwaj, I.P.S.,**
Former Director General of Police
Rajasthan

I am pleased to learn that National Cyber Safety & Security Standards is publishing the 2nd edition of "National Cyber Defence Reference Handbook". I believe that this edition will carry detailed perspective of cyber crimes and shall be helpful for Law Enforcement Agencies in their fight against cyber crime and will go a long way in serving the interests of National Security.

I wish this endeavour a great success.

(Omendra Bharadwaj)

Shri. **H. Venkatesh, I.P.S.,**
Former DIG & Commissioner of Police
Thiruvananthapuram, Kerala

I am happy to hear that National Cyber Safety and Security Standards Is publishing National Cyber Defence Reference Handbook 2nd Edition

In today's world, there is immense increase in the use of Internet in every field of the society and in turn, several new crimes have evolved. Cyber crimes have expanded to including cross borders crimes and is now considered a global epidemic. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Hope this handbook will derive an attempt to provide a glimpse of various types of cyber crimes prevalent in modern technological society and steps to be taken to protect public from these cyber attacks.

I send my best wishes for the success of this creditable venture.

(H. Venkatesh)

Shri. **Rakesh Maria, I.P.S.,**
Former Commissioner of Police
Mumbai

The exponential increase in the value of information has made it lucrative for technology savvy criminals to steal and trade in it in the virtual world; a world without borders or boundaries.

Hiding behind the anonymity of the global Internet, these criminals today pose a much greater threat than simply causing financial loss. The unregulated flow of money through practically untraceable channels across international borders is helping fuel traditional crime and terrorism, which the physical world with its borders and boundaries, is finding difficult to contain.

Increasing Internet Banking frauds and the threat to personal data on the public Internet are all becoming serious challenges to the law enforcement machinery of any Sovereign State.

It is becoming evident that creating awareness about cyber crimes, information security, privacy and such related issues amongst the general public can contribute significantly to the efforts of the law enforcement machinery in containing this ever growing threat.

The advent of the 2nd Edition of the "National Cyber Defence Reference Handbook" is, therefore, timely.

Beginning with the basics of computer networking and covering different aspects related to cyber crime, information security, data privacy and computer forensics, the book promises to be an immediate reference point on all aspects relating to cyber crimes and information security.

The efforts taken by "National Cyber Safety and Security Standards" in the preparation and publication of this book is laudable.

I wish "National Cyber Safety and Security Standards" all success in their endeavours.

R. Maria 8/1/15

(Rakesh Maria)

Shri. **Surajit Kar Purkayastha, I.P.S.,**
Former Commissioner of Police
Kolkata

It is a pleasure to know that National Cyber Safety & Security Standards is going to publish their National Cyber Reference Handbook 2nd Edition. I am sure that the information provided in this book on various aspects of Cyber Security and Safety will be of immense significance to India's National Security and will be highly pertinent in the present day context. I hope the information in this Handbook will provide excellent guidance to the police organizations of the country and other law enforcers in general.

I wish success to this publication.

(Surajit Kar Purkayastha)

सत्यमेव जयते

Shri. **Brigadier JK Bansal**
Chairman, Cyber Security Group
Department of Defence Production (CSG - DDP)
Directorate of Standardisation, Ministry of Defence
Government of India, New Delhi.

I am inform you about the raising of this Cyber Security Group - Department of Defence Production (CSG - DDP) to request you for lateral exchange of any critical information or development in threat land scape which may help' bolstering our Cyber Security posture. We also look forward to attend seminars, meetings or any such platform where the National Cyber Safety and Security Standards can be benefitted by sharing collective intelligence & knowledge to continuously evolve our own cyber security procedures and frameworks.

(Brigadier JK Bansal)

CONTENTS

अध्याय 1

Chapter 1

Basics of Computers Networks and How to Shore up Network Security

Notes :

1.1. Basics of Computers Networks

1.1.1. How a Computer Works?

1.1.1.1. Essential Components of a Computer

A quick survey of how a computer works would help you understand the business of hacking better. The following are the components common to PCs (personal computers) in the order they're typically assembled:

Case : If you're using a laptop, the computer case includes keyboard and screen. For desktop PCs, the case is typically some type of box with lights, vents, and places for attaching cables. The size of the case can vary from small tabletop units to tall towers. A larger case doesn't always imply a more powerful computer; it's what's inside that counts. PC builders design or select a case based on the type of motherboard that should fit inside.

Motherboard: The primary circuit board inside your PC is its motherboard. All components, inside and out, connect through the motherboard in some way. Motherboards come in different sizes and standards, the most common by the time of the writing of this book being ATX and MicroATX.

Power Supply: Other than its CMOS (Complementary Metal-Oxide Semiconductor) which stores some information, such as the system clock, when the computer is powered down, every other component in your PC relies on its power supply. The power supply connects to some type of power source, whether that's a battery in the case of mobile computers, or a power outlet in the case of desktop PCs.

Central Processing Unit (CPU): The CPU, often just called the processor, is the component that contains the microprocessor. That microprocessor is the heart of all of the operations of the computer and the performance of both hardware and software rely on the processor's performance.

Random-Access Memory (RAM): Even the fastest processor needs a buffer to store information while it's being processed. The RAM is to the CPU as a countertop is to a cook: It serves as the place where the ingredients and tools you're working with wait until you need to pick up and use them. Both a fast CPU and an ample amount of RAM are necessary for a speedy PC.

Drives: A drive is a device intended to store data when it's not in use. A hard drive or solid state drive stores a PC's Operating System and software.

Ports: The word port is often used to describe a place on the outside of your PC where you can plug in a cable. We describe a port by its use, such as a USB port or an Ethernet port.

1.1.1.2. The Boot Process

When you first power up a PC, the machine goes through several internal processes before it's ready for you to use. This is called the boot process, or booting the PC. Boot is short for bootstrap, a reference to the old adage, "Pull yourself up by the bootstraps," which means to start something from the very beginning. The boot process is controlled by the PC's basic input-output system (BIOS). The BIOS is software stored on a flash memory chip. In a PC, the BIOS is embedded on the motherboard. The following is a summary of the boot process in a PC:

1. The power button activates the power supply in the PC, sending power to the motherboard and other components.
2. The PC performs a power-on self-test (POST). The first program that runs is usually a set of instructions kept in the computer's read-only memory (ROM). The POST is a small computer program within the BIOS that checks for hardware failures. A single beep after the POST signals that everything's okay.
3. The PC displays information on the attached monitor showing details about the boot process. These include the BIOS manufacturer and revision, processor specs, the amount of RAM installed, and the drives detected.
4. The BIOS attempts to access the first sector of the drive designated as the boot disk. The boot disk is typically the same hard disk or solid-state drive that contains your operating system. The BIOS confirms there's a bootstrap loader, or boot loader, in that first sector of the boot disk, and it loads that boot loader into memory (RAM). The boot loader is a small program designed to find and launch the PC's operating system.
5. Once the boot loader is in memory, the BIOS hands over its work to the boot loader, which in turn begins loading the operating system into memory.
6. When the boot loader finishes its task, it turns control of the PC over to the operating system. Then, the OS is ready for user interaction.

1.1.1.3. Operating Systems and what they do?

When you turn on your computer, it's nice to think that you're in control. There's the trusty computer mouse, which you can move anywhere on the screen, summoning up your music library or Internet browser at the slightest whim. Although it's easy to feel like a director in front of your desktop or laptop, there's a lot going on inside, and the real man behind the curtain handling the necessary tasks is the Operating System (OS). Most desktop or laptop PCs come pre-loaded with Microsoft Windows. Macintosh computers come pre-loaded with Mac OS X. Many corporate servers use the Linux or UNIX operating systems. There are hundreds of other operating systems available for special-purpose applications, including specializations for mainframes, robotics, manufacturing, real-time control systems and so on. The operating system (OS) is the first thing loaded onto the computer—without the operating system, a computer is useless. The purpose of an operating system is to organize and control hardware and software so that the device it lives in behaves in a flexible but predictable way. At the simplest level, an operating system does two things:

1. It manages the hardware and software resources of the system. In a desktop computer, these resources include such things as the processor, memory, disk space and more.
2. It provides a stable, consistent way for applications to deal with the hardware without having to know all the details of the hardware.

The first task, managing the hardware and software resources, is very important, as various programs and input methods compete for the attention of the central processing unit (CPU) and

demand memory, storage and input / output (I/O) bandwidth for their own purposes. In this capacity, the operating system plays the role of the good parent, making sure that each application gets the necessary resources while playing nicely with all the other applications, as well as husbanding the limited capacity of the system to the greatest good of all the users and applications.

The second task, providing a consistent application interface, is especially important if there is to be more than one of a particular type of computer using the operating system, or if the hardware making up the computer is ever open to change. A consistent application program interface (API) allows a software developer to write an application on one computer and have a high level of confidence that it will run on another computer of the same type, even if the amount of memory or the quantity of storage is different on the two machines.

The operating system's tasks, however, in the most general sense, fall into six categories:

- Processor management
- Memory management
- Device management
- Storage management
- Application interface
- User interface

You are most likely to be using a single-user, multi-tasking OS on your desktop and laptop computers today which let a single user have several programs in operation at the same time. For example, it's entirely possible for a windows user to be writing a note in a word processor while downloading a file from the Internet while printing the text of an email message.

1.1.1.4. Ports

Considered to be one of the most basic external connections to a computer, the serial port has been an integral part of most computers for more than 20 years. Essentially, serial ports provide a standard connector and protocol to let you attach devices, such as modems, to your computer. Parallel ports are a more recent invention and are much faster than serial ports. USB ports are only a few years old, and will likely replace both serial and parallel ports completely over the next several years.

The name "serial" comes from the fact that a serial port "serializes" data. That is, it takes a byte of data and transmits the 8 bits in the byte one at a time. The advantage is that a serial port needs only one wire to transmit the 8 bits (while a parallel port needs 8). The disadvantage is that it takes 8 times longer to transmit the data than it would if there were 8 wires. Serial ports lower cable costs and make cables smaller. Serial ports, also called communication (COM) ports, are bi-directional. Bi-directional communication allows each device to receive data as well as transmit it. Serial ports rely on a special controller chip, the Universal Asynchronous Receiver/ Transmitter (UART), to function properly. The external connector for a serial port can be either 9 pins or 25 pins.

If you have a printer connected to your computer, there is a good chance that it uses the parallel port. While USB is becoming increasingly popular, the parallel port is still a commonly

used interface for printers. Parallel ports can be used to connect a host of popular computer peripherals like printers, scanners, CD writers, external hard drives, etc.

Obviously, it was not a happy arrangement. The goal of USB is to end all of these headaches. The Universal Serial Bus (USB) gives you a single, standardized, easy-to-use way to connect up to 127 devices to a computer. The USB is an industry standard developed in the mid-1990s that defines the cables, connectors and communications protocols used in a bus for connection, communication and power supply between computers and electronic devices.

1.1.2. Computer Networks

A computer network is a system in which computers are connected to share information and resources. Why do you need to do that? At a simple level, it is to enable you to do things like the following:

- You can play a music CD from one computer while sitting on another computer.
- You may have a computer that doesn't have a DVD or BluRay (BD) player. In this case, you can place a movie disc (DVD or BD) on the computer that has the player, and then view the movie on a computer that lacks the player.
- You may have a computer with a CD/DVD/BD writer or a backup system but the other computer(s) doesn't (don't) have it. In this case, you can bum discs or make backups on a computer that has one of these but using data from a computer that doesn't have a disc writer or a backup system.
- You can connect a printer (or a scanner, or a fax machine) to one computer and let other computers of the network print (or scan, or fax) to that printer (or scanner, or fax machine).
- You can place a disc with pictures on one computer and let other computers access those pictures.
- You can create files and store them in one computer, then access those files from the other computer(s) connected to it

Of course, as you will see shortly, you can do much more serious things with networking.

When a computer or device A requests a resource from another computer or device B, the item A is referred to as a client. The connection can be done as peer-to-peer or client/server. A peer-to-peer network, also called a workgroup, is a network where each computer owns its own resources and can make them available. Each computer may or may not present much security. One way to secure a computer is to make sure that anybody who wants to use it must be identified. That is, everyone who wants to use the computer must have a user account on that computer. A computer network is referred to as client/server if (at least) one of the computers is used to "serve" other computers referred to as "clients". In a client/server environment, each computer still holds (or can still hold) its (or some) resources and files. Other computers can also access the resources stored in a computer, as in a peer-to-peer scenario. In a client/server network the files and resources are centralized. This means that a computer, the server, holds them and other computers can access them. Since the server is always ON, the client machines can access the files

and resources without caring whether a certain computer of the network is ON or not. In a peer-to-peer network, the other computer must necessarily be ON.

Another big advantage of a client/server network is that security is created, managed, and can be enforced rigorously. To access the network, a person, called a user must provide some credentials, such as a username and a password. If the credentials are not valid, the user is prevented from accessing the network. Fine. That's for lay men like you. Hackers go on to breach this security—that's what their business is about. That way they can access the resources of the computers on the network without being authorized to do so. One of the consequences of a client/ server network is that, if the server is turned OFF, its resources and sometimes most of the resources on the network are not available. In fact, one way to set up a client / server network is to have more than one server.

Cable is used to connect computers. Although we may use wireless networking, you should always have cables with you. A computer network can have two computers connected.

Fig. A computer network can also consist of, and is usually made for, more than two computers.

We mentioned that you could connect one computer to another. This can be done using their serial ports we discussed above. If you have to connect many computers to produce a network, this serial connection would not be practical. The solution is to use a central object that the computers and other resources can connect to, and then this object becomes responsible to "distribute" or manage network traffic.

The most regularly used types of network distributors are the hub, the router, and the switch. A hub is rectangular box that is used as the central object on which computers and other devices are connected. Like a hub, a router is another type of device that acts as the central point among computers and other devices that are part of a network. A router functions a little differently than a hub. In fact, a router can be considered a little "intelligent" than the hub. Like a hub, the computers and other devices are connected to a router using network cables. To make this possible, a router is equipped with holes, called ports. Based on advances in the previous years from IEEE (Institute Of Electrical And Electronics Engineers) and other organizations or research companies, we also have wireless routers. With this device, the computers and devices connect to the router using microwaves (no physical cable). In order to connect to a network, a computer must be equipped with a device called a network card. A network card, or a network adapter, also called a network interface card, or NIC, allows a computer to connect to the exterior. Most laptops already have a wireless card built-in so you may not have to acquire one. Many new desktop computers (from HP) now have built-in wireless capability.

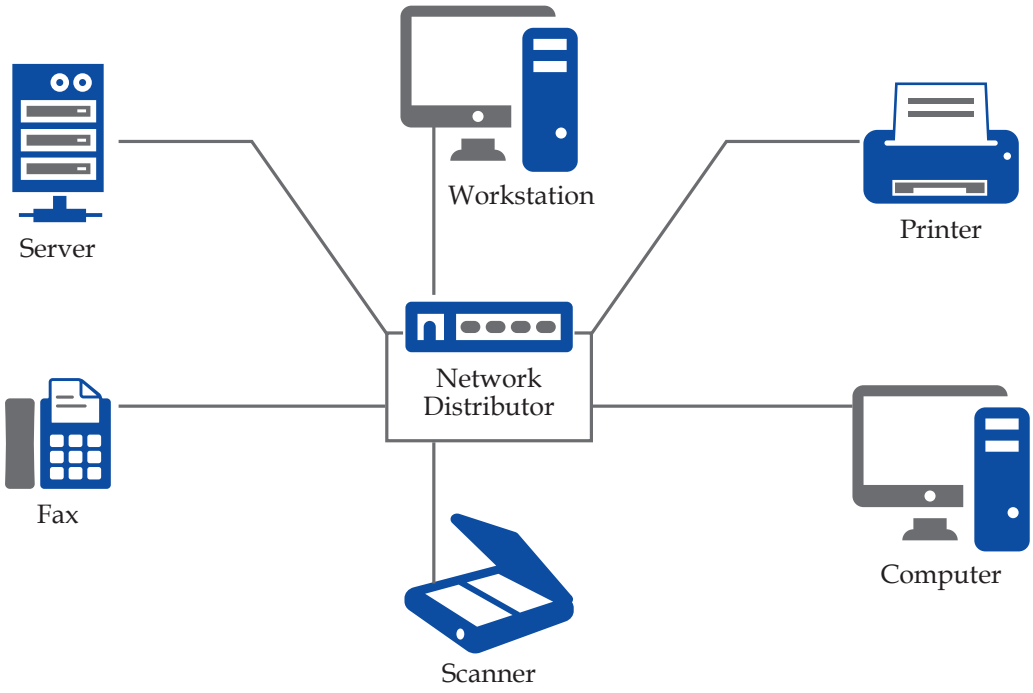


Fig. Network Distribution

1.1.3. The Internet and How it Works?

A LAN (Local Area Network) is a network that typically stays within the same building. This could be as small as one computer plugged into a router in your house to as large as an office building. Everything from small home networks to fairly large enterprise networks belong to this group. A network that stretches between several buildings, often far from each other, or between different cities is called a WAN (Wide Area Network). A WAN consists mostly of two or more LAN's connected together and forming the larger WAN. A WAN connects several LANs together via a router. Somewhere between the LAN and WAN is something that is called MAN (Metropolitan Area Networks). A MAN is larger than a LAN and connects LAN's within a limited area, such as a city, with high capacity.

The largest network is the Internet, which is composed of many different networks, both large and small—it can be thought of as a network of networks, both large WANs and small. The WANs are connected to each other via more routers. That is what an ISP (Internet Service Provider) is, a collection of routers with routes to the various networks all across the internet. All these interconnects form a web, hence the name the World Wide Web (WWW). The Internet and the World Wide Web are actually two separate entities. The World Wide Web sits on top of the Internet (Internet is physical / link layer, WWW is protocol / application layer). The Internet is a server-client network. When you sit on a computer and connect to the Internet, you are the client computer. Machines that store the information we seek on the Internet are called servers.

Besides regular networking, another way in which computers can share private information is to use their network as a private Internet. This is called an intranet. An intranet is a computer

network where connected computers use the technologies of the Internet to share resources such as folders or printers, etc. This means that a person seating on one computer can access a folder (or printer) in another computer using a browser and specifying the address of that folder (or resource).

To understand the Internet, it helps to look at it as a system with two main components. The first of those components is hardware. That includes everything from the cables that carry terabits of information every second to the computer sitting in front of you and routers, servers, cell phone towers, satellites, radios, smart phones and other devices etc. Other elements are nodes which serve as a connecting point along a route of traffic. And then there are the transmission lines which can be physical, as in the case of cables and fiber optics, or they can be wireless signals from satellites, cell phone or 4G towers, or radios.

All of this hardware wouldn't create a network without the second component of the Internet: the protocols. Protocols are sets of rules that machines follow to complete tasks. Without a common set of protocols that all machines connected to the Internet must follow, communication between devices couldn't happen. The various machines would be unable to understand one another or even send information in a meaningful way. The protocols provide both the method and a common language for machines to use to transmit data. At their most basic level, these protocols establish the rules for how information passes through the Internet Without these rules, you would need direct connections to other computers to access the information they hold. You'd also need both your computer and the target computer to understand a common language.

You've probably heard of several protocols on the Internet. For example, Hypertext Transfer Protocol (HTTP) is what we use to view websites through a browser—that's what the 'http' at the front of any web address stands for. If you've ever used an FTP server, you relied on the file transfer protocol. Protocols like these and dozens more create the framework within which all devices must operate to be part of the Internet. Two of the most important protocols are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). We often group- the two together as TCP/IP.

You've probably heard of IP addresses. These addresses follow the Internet protocol. Each device connected to the Internet has an IP address. This is how one machine can find another through the massive network. An IP address is something like a mailing address for computers on the Internet. This mailing address allows your email to arrive at the right place and your webpage customers to see the correct website. As soon as that computer is connected to the Internet it needs to be given a registered IP address (which is also generally called an Internet address). Two versions of IP technology exist today. Traditional home computer networks use IP version 4 (IPv4), but some other networks, particularly those at educational and research institutions, have adopted the next generation IP version 6 (IPv6).

An IPv4 address consists of four bytes (32 bits). These bytes are also known as octets. For readability purposes, humans typically work with IP addresses in a notation called dotted decimal. This notation places periods between each of the four numbers (octets) that comprise an IP address. For example, an IP address that "the computers see as

00001010 00000000 00000000 00000001

is written in dotted decimal as

10.0.0.1

Because each byte contains 8 bits, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255. Therefore, the full range of IP addresses is from 0.0.0.0 through 255.255.255.255. This represents a total of 4,294,967,296 possible IP addresses.

An IP address is different from a Domain Name Address or a MAC (Media Access Control) Address. For nearly every web server, the IP address is invisibly translated into a natural English "domain name" for ease of use. But technically speaking, the IP address is the true identifier of a web server—the domain name is simply a redirector pointer to help people find the web server.

- e.g. 72.246.51.15 = www.nasa.gov
- e.g. 152.91.56.138 = www.gov.au
- e.g. 208.185.127.40 = www.about.com

Another method of referring to Internet resources that you should be familiar with is the Uniform Resource Locator, or URL. Unlike DNS addresses, which are used to refer to computers, URLs are used to refer to specific resources on computers. A URL is comprised of three components. The first component is the protocol that you use to access the resource. Next, following a colon and two forward slashes, is the computer on which the requested resource is located. Finally, following another forward slash is the name of the resource on the target computer. For example, typing this http://cda.dummies.com/wiIeyCDA/Section.rdr?id= 100051 into the address box of your Web browser tells it to use the HyperText Transfer Protocol (HTTP) to connect to the computer with the DNS name cda.dummies.com and retrieve a Web page called WileyCDA/Section.rdr?id= 100051.

When you want to send a message or retrieve information from another computer, the TCP/IP protocols are what make the transmission possible. Your request goes out over the network, hitting domain name servers (DNS) along the way to find the target server. The DNS points the request in the right direction. Once the target server receives the request, it can send a response back to your computer. The data might travel a completely different path to get back to you. This flexible approach to data transfer is part of what makes the Internet such a powerful tool.

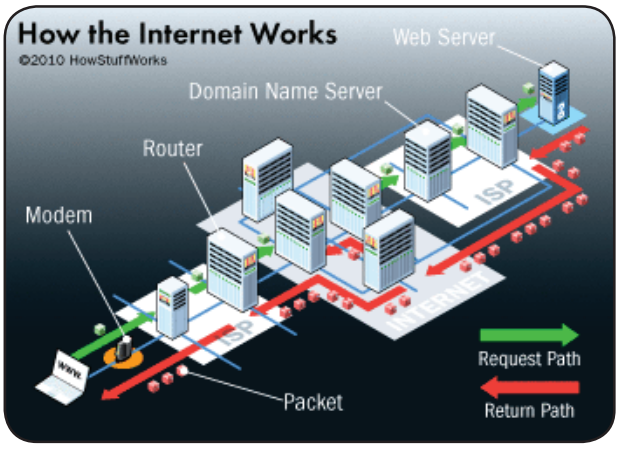


Fig. How the Internet works?

When you open your Web browser and try to connect to a website, your computer sends an electronic request over your Internet connection to your Internet Service Provider (ISP). The ISP routes the request to a server further up the chain on the Internet. Eventually, the request will hit a domain name server (DNS). This server will look for a match for the domain name you've typed in (such as www.thelastpolymath.com). If it finds a match, it will direct your request to the proper server's IP address. If it doesn't find a match, it will send the request further up the chain to a server that has more information.

The request will eventually come to the server of the website www.thelastpolymath.com. The server will respond by sending the requested file in a series of packets. Packets are parts of a file that range between 1,000 and 1,500 bytes. Packets have headers and footers that tell computers what's in the packet and how the information fits with other packets to create an entire file. Each packet travels back up the network and down to your computer.

Now an important thing. This will be of use to you when you consider an attack on the Internet itself. Packets don't necessarily all take the same path—they'll generally travel the path of least resistance. Because packets can travel multiple paths to get to their destination, it's possible for information to route around congested areas on the Internet. In fact, as long as some connections remain, entire sections of the Internet could go down and information could still travel from one section to another—though it might take longer than normal.

When the packets get to you, your device arranges them according to the rules of the protocols. It's kind of like putting together a jigsaw puzzle. The end result is that you get to see the website on your screen. This holds true for other kinds of files as well. When you send an email, it gets broken into packets before zooming across the Internet. Phone calls over the Internet also convert conversations into packets using the Voice Over Internet Protocol (VoIP).

The TCP/IP itself involves several layers of protocols. Different parts of the networking software or applications on your computer are responsible for processing the information inside each of the layers.

Network Interface Layer: This layer, which is sometimes also called the Network Access Layer, deals with all the protocols that determine how a network packet is sent across a given physical network structure. If TCP/IP were the postal service, the Network Interface Layer protocols would define how the letter carriers load their vehicles, what kinds of trucks transport the letters, and so on.

Internet Layer: This layer is concerned with giving each computer in a large network a unique address and being able to route all packets to a computer based on this address. If TCP/IP were the postal service, the Internet layer protocols would define the format for envelopes and how postal codes and street addresses are used to deliver a packet

Transport Layer: Protocols at this layer are responsible for data integrity. One of the functions of such a protocol is to ensure that all the packets for a given transmission are received. If not, the protocol may request that the originating computer send them again. If TCP/IP were the postal service, the Transport layer protocols would be responsible for keeping track of registered mail, ensuring that letters are received intact, and notifying the sender if a letter did not arrive.

Application Layer: Protocols at this layer are responsible for implementing specific applications or programs. For example, email protocols define how the message should be formatted, what commands the mail server understands that a mail program should send to a mail server to retrieve email messages. If TCP/IP were the postal service, Application layer protocols would define what you are allowed to place inside an envelope and perhaps even the language in which a postcard must be written.

1.2. How to Shore Up Network Security ?

1.2.1. How Firewalls Work and Why You Need Them?

When you connect your computer or your computer network to the Internet, you are connecting it to millions of other computers. People who may be trying to get to the private data on your computer network may be using some (or even a lot) of those computers. To keep unwanted hackers off your computer network, you should install and configure what is known as a firewall to separate the un-trusted outside world from the trusted inside computer network. A 'firewall' is a piece of software that inspects all network traffic and decide which traffic should be allowed to pass and which traffic should be blocked.

Before the term firewall was used for a component of a computer network, it described a wall that was designed to contain a fire. A brick and mortar firewall is designed to contain a fire in one part of a building and thus prevent it from spreading to another part of the building. Any fire that may erupt inside a building stops at the firewall and won't spread to other parts of the building. Now hold on for a second. You should be able to sense that the term firewall doesn't accurately describe its function as discussed above. A real firewall is a barrier to prevent fires from spreading from one room or building to another. A real firewall blocks fires completely. On the other hand, the firewalls in the context of computer networks should inspect all "fires" and let some pass through while blocking others. A term that more accurately describes the function of the Internet firewall products is doorman. The doorman is the security guard who sits behind a desk near the front entrance of a large office building and screens everybody who wants to come inside. But the use of the term firewall has come to stay. Or maybe you can think of the firewall of computer networks like the fire doors in a physical firewall. These doors are designed to provide an opening while still guaranteeing safety for all occupants.

In order for all this to work, you have to tell the firewall what is acceptable network traffic by specifying policy rules. So what exactly does a firewall do? As network traffic passes through the firewall, the firewall decides which traffic to forward and which traffic not to forward, based on rules that you have defined. All firewalls screen traffic that comes into your network, but a good firewall should also screen outgoing traffic.

A large part of administering a firewall consists of configuring rules, such as the following:

- Block incoming network traffic based on source or destination: Blocking unwanted incoming traffic is the most common feature of a firewall.
- Block outgoing network traffic based on source or destination: Many firewalls can also screen network traffic from your internal network to the Internet. For example, you may want to

The preservation of freedom is not the task of soldiers alone. The whole nation has to be strong.
- Lal Bahudur Shastri

prevent employees from watching porn on the office computer during office hours at the company's expense.

- Block network traffic based on content: More advanced firewalls can screen network traffic for unacceptable content. For example, a firewall that is integrated with a virus scanner can prevent files that contain viruses from entering your network. Other firewalls integrate with email services to screen out unacceptable email.
- Make internal resources available: Although the primary purpose of a firewall is to prevent unwanted network traffic from passing through it, you can also configure many firewalls to allow selective access to internal resources, such as a public Web server, while still preventing other access from the Internet to your internal network.
- Allow connections to internal network: A common method for employees to connect to a network is using virtual private networks (VPNs). VPNs allow secure connections from the Internet to a corporate network. For example, telecommuters and traveling salespeople can use a VPN to connect to the corporate network. VPNs are also used to connect branch offices to each other. Some firewalls include VPN functionality and make it easy to establish such connections.
- Report on network traffic and firewall activities : When screening network traffic to and from the Internet, it's also important to know what your firewall is doing, who tried to break into your network, and who tried to access inappropriate material on the Internet. Most firewalls include a reporting mechanism of some kind or another.
- Log all connection attempts that were rejected by the firewall.
- Allow outgoing email from the internal mail server.
- Allow incoming Web requests to the public Web server.
- Log all access to external Websites.

Every firewall has different methods of specifying what traffic is allowed to pass, and every firewall has different inspection possibilities. However, the basics of most firewalls are the same. Most traditional firewalls focus on the Internet and Transport layers that we have discussed earlier. These layers define where network packets come from, for whom they're intended, and whether a packet fits correctly into a sequence of related packets. More advanced firewalls, however, also operate at the Application layer. Inspecting traffic at the Application layer means that a firewall understands how packets combine to form a larger data exchange, such as an entire email message, and the structure of that email message.

A true firewall should have at least the following basic functions:

- **Packet Filtering:** The headers of all network packets going through the firewall must be inspected. The firewall makes an explicit decision to allow or block each packet.
- **Network Address Translation (NAT):** The outside world sees only one or more outside IP addresses of the firewall. The internal network can use any address in the private IP address

range. In NAT, the IP numbers and port numbers that are used in the packet are substituted with other numbers before the packet continues. Source and destination addresses in network packets must be automatically changed (or "translated") back and forth by the firewall.

- **Application Proxy:** The firewall must be capable of inspecting more than just the header of the network packets. This capability requires the firewall to understand the specific application protocol.
- **Monitoring And Logging:** Even with a solid set of rules, logging of all that happens at the firewall is important. Doing so can help you to analyze a possible security breach later and gives feedback on the performance and actual filtering done by the firewall. Because firewalls are a single point of entry for network traffic entering or leaving your internal network, the firewall is an excellent location to perform additional security tasks. Many firewalls support the following advanced functions:

❖ **Data Caching:** Because the same data or the contents of the same website may pass the firewall repeatedly in response to requests from different users, the firewall can cache that data and answer more quickly without getting the data anew from the actual website every time.

❖ **Content Filtering:** Firewall rules may be used to restrict access to certain inappropriate websites based on URLs, keywords, or content type (video streams, for example, or executable email attachments).

❖ **Intrusion Detection:** Certain patterns of network traffic may indicate an intrusion attempt in progress. Instead of just blocking the suspicious network packets, the firewall may take active steps to further limit the attempt, for example, by disallowing the sender IP address altogether or alerting an administrator.

❖ **Load Balancing:** From a security standpoint, a single point of entry is good. But from an availability standpoint, this single point of entry may lead to a single point of failure as well. Most firewalls allow the incoming and outgoing network request to be distributed among two or more cooperating firewalls.

1.2.2. What a Firewall Can't Do?

A security guard can't prevent all security problems, and neither can firewalls prevent all security problems. Security threats that a firewall can't protect you from include:

- **Inside Attack:** Users on the internal network have already passed the firewall. The firewall can do nothing to stop internal network snooping or intrusion attempts from within. Other security measures, such as configuring restricted permissions on workstations and servers, and enabling the auditing of network access, should be implemented to protect against these kinds of attacks. You can also think of deploying firewalls between your corporate servers and your internal users as well.
- **Social Engineering:** This is the term used to describe attacks in which hackers obtain information by calling employees and pretending to be a colleague at the front desk, a member

of the security staff, or just somebody from the firm doing routine checks. This person asks for privileged information, such as server names, IP addresses, or passwords. Employees should be aware of these tactics and know that certain information should never be given.

- **Viruses And Trojan Horse Programs:** Firewalls attempt to scan for viruses in all network traffic, but these wicked programs change constantly. Distinguishing between acceptable email attachments and malicious content continues to be a problem for computer users. Trojan horse programs are perhaps even harder to spot, because they don't attempt to spread to other files or computers like their virus sisters. A very small Trojan Horse program that is run once by an unsuspecting user can open up a back door to his computer. A good example of the land of damage that these programs can do is a Trojan Horse program that sends out all collected keystrokes at password prompts once a week.
- **Poorly Trained Firewall Administrators:** The firewall doesn't know what is acceptable and what is not unless an administrator tells it. Competent firewall administrators should correctly specify which network traffic should be blocked. A human doorman has the intelligence to understand that a naked man who claims that his clothes and shoes already arrived and he is supposed to join them in the third floor conference room is clearly crazy, even though his security instructions may not have a naked-man-meeting-his-clothes-upstairs clause. Most firewalls, however, can easily be confused by fragmented IP packets and should be explicitly configured to handle such fragments.

New network protocols and services are introduced constantly. New vulnerabilities and software bugs in firewalls are also discovered constantly. Administrating a firewall is not a one-time task. You should stay alert and constantly maintain the firewall rules, update and install vendor-supplied patches, and check the generated firewall log files. Unfortunately, you can't just install a firewall and forget about it.

1.2.3. Network Security

In this section we provide a brief overview of network security, focusing on cryptographic protocols used in the Internet for achieving secure services (such as online banking). The networking protocols used in the Internet can be viewed as a set of layers or protocol stack. Each layer is responsible for solving a different set of problems related to networking. The Open Systems Interconnection (OSI) model describes a seven-layered network stack: physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.

In general, we are interested in providing end-to-end security, that is, ensuring that the communication between a client and a server in the Internet has been authenticated (both parties know who they are communicating with), is confidential, and has not been tampered with. In order to achieve these goals, protocols such as IPSec, SSL, and DNSSEC have been proposed.

IP Security (IPSec): The Internet protocol (IP) is the main protocol of the network layer: it provides the information needed for routing packets among routers and computers of the network. One of the shortcomings of the original IP protocol was that it lacked any kind of general-purpose mechanism for ensuring the authenticity and privacy of IP data while in transmission. Since IP

data packets are generally routed between two devices, over unknown networks, any information included in the packets is subject to being intercepted or possibly changed. With the increased use of the Internet for critical applications, security enhancements for IP were needed. To this end, IPSec was developed to provide transparent end-to-end encryption of IP traffic and user data. IPSec is predominantly used in the commercial sector. IPSec consists of two parts: the Internet key exchange (IKE) protocol, which provides mutual entity authentication and establishes a shared symmetric key, and the encapsulating security payload and authentication header (ESP/AH), which provides end-to-end confidentiality and authentication.

One of the main uses of IPSec today is for the creation of a Virtual Private Network (VPN). VPNs are generally used by enterprises to connect remote offices across the Internet. IPSec is used in VPNs for creating a secure channel across the Internet between a remote computer and a trusted network.

Secure Socket Layer (SSL): SSL was originally developed to provide end-to-end confidentiality, integrity, and authentication between two computers over the transmission control protocol (TCP), a protocol running at the transport layer. SSL and its successor, transport layer security (TLS), have been very popular, receiving the endorsement of several credit card companies and other financial institutions for commerce over the Internet. SSL/TLS is commonly used with http to form https, a protocol used to secure Web pages. (Https is the protocol used when your browser shows a closed lock in one corner of the browser window, to indicate a secure connection.)

SSL is composed of a set of protocols: the protocol to ensure data security and integrity, called the SSL record protocol, and the protocols that are used for establishing an SSL connection. The latter consists of three sub-protocols: the SSL handshake protocol, the SSL change cipher protocol, and the SSL alert protocol. The main difference between IPSec and SSL is the layer where they are implemented. The main motivation for IPSec is to avoid the modification of any layer on top of the network layer. IPSec is implemented in the operating systems, so no modifications are required from applications. The main motivation for SSL is to create a secure channel by creating (or modifying) the applications (as long as the application runs over TCP) without changing the infrastructure of the Internet or the operating system of the user.

Domain Name Service Security Extensions (DNSSEC): The domain name server (DNS) is the protocol that translates the human-readable host names into 32-bit Internet protocol (IP) addresses: it is essentially a "yellow book" for the Internet, telling routers to which IP address to direct packets when the user gives a name such as http://www.google.com. Because DNS replies are not authenticated, an attacker may be able to send malicious DNS messages to impersonate an Internet server. Although SSL can try to prevent this impersonation (the attacker's website should not have the secret key of the real website), there are many websites and other services that run without SSL, but that still need to be reached in a trustworthy manner. In order to ensure the integrity of the DNS service, the IETF is currently working on DNSSEC. Another major concern about DNS is its availability. Because a successful attack against the DNS service would create a significant communication disruption in the Internet, DNS has been the target of several DoS attacks.

1.2.4. How we can Improve Network Security Further?

1.2.4.1. Filtering IP Data

Packet filters are rules that inspect the information in the packet header of every network packet arriving at the firewall, so that they can decide whether the packet should be allowed in or out or whether it should be dropped. If the packet is allowed to pass, it continues on its merry way. But note that an IP packet never passes any router or firewall without undergoing some modifications. Note that packet filters have limited decision capabilities because they look only at a small portion of the network packet. The firewall should use application proxy functionality to further inspect the packet

You can create packet filter rules that check the following fields in a network packet that arrives at the firewall:

- **Source IP Address:** This is the IP address that the packet lists as its sender. This field doesn't necessarily reflect the true original computer that sent the packet. The field may have been changed by hackers in what is known as IP address spoofing.
- **Destination IP Address:** This is the IP address to which the packet is being sent. Make sure you list the actual IP address in the packet filter rule and not the Domain Name System (DNS) name. Otherwise, a hacker that takes over a DNS server can immediately pass all packet filters undisturbed.
- **TCP Or UDP (User Datagram Protocol) Port Number**: In computer networking a port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. In plain English, the purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet. The protocols that primarily use ports are the Transport Layer protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite. The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. A port is identified for each address and protocol by a 16-bit number, commonly known as the port number, thus ranging from 1 to 65535 (port number 0 is reserved and can't be used). Of the thousands of enumerated ports, about 250 well-known ports are reserved by convention to identify specific service types on a host. The port number, added to a computer's IP address, completes the destination address for a communications session. The port number indicates to which service this packet is destined. That is, data packets are routed across the network to a specific destination IP address, and then, upon reaching the destination computer, are further routed to the specific process bound to the destination port number. You should allow only ports that are associated with allowed services, such as HTTP

(port 80) or FTP (port 20/21). The core network services, such as the World Wide Web, typically use small port numbers less than 1024. A process associates its input or output channels via Internet sockets, a type of file descriptor, with a transport protocol, a port number and an IP address. This process is known as binding, and enables sending and receiving data via the network. The operating system's networking software has the task of transmitting outgoing data from all application ports onto the network, and forwarding arriving network packets to a process by matching the packet's IP address and port number. Only one process may bind to a specific IP address and port combination using the same transport protocol. Note that it is the combination of IP address and port number together that must be globally unique. Thus, different IP addresses or protocols may use the same port number for communication; e.g., on a given host or interface UDP and TCP may use the same port number, or on a host with two interfaces, both addresses may be associated with a port having the same number. The port numbers are encoded in the transport protocol packet header, and they can be readily interpreted not only by the sending and receiving computers, but also by other components of the networking infrastructure. Firewalls must be configured to differentiate between packets based on their source or destination port numbers.

- **ICMP Message Type:** The Internet Control Message Protocol (ICMP) is the housekeeping protocol of the TCP/ IP protocol suite. The ICMP is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. Some of the ICMP types are very useful messages; others are very dangerous and should not be allowed to pass through the firewall.
- **Fragmentation Flags:** IP packets can be broken into smaller packets to accommodate network segments that can only handle smaller-sized packets. Unfortunately, this functionality can be misused.
- **IP Options Setting:** Optional functions of TCP/IP can be specified in this field. Hackers can exploit the Source Route option in particular. These options 'are only used for diagnostics, so the firewall should drop network packets with IP Options set.

1.2.4.2. Stateful Packet Filtering

So far we have only looked at stateless packet filtering. Modem firewalls use a more robust version, which is called stateful packet filtering. With stateful packet filtering, the firewall remembers "state" about expected return packets. Any unexpected packet arriving at the firewall claiming to be a solicited response is blocked immediately. When an IP packet is a request for information, such as an HTTP (port 80) request to a public website, the IP packet lists its return IP address and an unused return port number greater than 1023 (for example, 2065) to which to deliver the response. If the firewall knows only stateless packet filtering, it doesn't know that a packet will arrive shortly on port 2065. The only choice that a stateless packet filter firewall has is to leave all ports greater than 1023 open for all traffic. A hacker can easily use this opening to

Whatever we treasure for ourselves separates us from others; our possessions are our limitations.
- Sir Rabindranath Tagore

initiate communication with internal computers on ports greater than 1023. The firewall will pass this unsolicited traffic.

Stateful packet filtering blocks all traffic on ports greater than 1023, and allows only network traffic that matches the response port of a previously sent IP packet. The firewall internally maintains a table of information on which ports it may expect traffic. If the firewall determines that a communication exchange is finished, it removes that information from the table. In cases where the firewall is unable to detect that the communication has ended, it automatically removes that information after a short time period.

Because a temporary packet Miter allowing network traffic on the return port is automatically created, stateful packet filtering is a form of dynamic packet filtering called dynamic packet filter mirroring, or even stateful inspection.

1.2.4.3. Network Address Translation (NAT) and Hardware Firewalls

Originally, Network Address Translation, or NAT, was introduced as a short-term solution to save IP addresses in use on the Internet. An IP address is 32 bits long and with that number of bits, you can have only about four billion different IP addresses. Because many companies have claimed large blocks of IP addresses, the available IP numbers were quickly becoming depleted. As it turned out, NAT offered several unexpected advantages.

With NAT, all computers on the internal network can use a private range of IP addresses, such as 10.0.0.0/8, which is not in use on the Internet. When they make a connection to the outside world, the NAT computer replaces the private IP address, for example, 10.65.1.7—listed as Source IP address in the IP packet—with its own public IP address, 23.1.8.3, and sends the packet on its way. The destination computer on the Internet thinks the original sender is 23.1.8.3, and sends a return packet back to this IP address. The NAT computer receives a packet for 23.1.8.3 and replaces the Destination IP address with the original 10.65.1.7 to travel the last leg on the internal network NAT may as well have been called Network Address Replacing.

In other words, a NAT router creates a local area network (LAN) of private IP addresses and interconnects that LAN to the wide area network (WAN) known as the Internet. The "Network Address Translation" (NAT) performed by the router allows multiple computers (machines) connected to the LAN behind the router to communicate with the external Internet. The most common use for NAT routers is serving as an "interface" between the global public WAN Internet and a private non-public LAN.

How does it help us? Well, all NAT routers inherently function as very effective 'hardware firewalls'. As a hardware firewall they prevent "unsolicited", unexpected, unwanted, and potentially annoying or dangerous traffic from the public Internet from passing through the router and entering the user's private LAN network. How they do this is simple: With multiple "internal" computers on the LAN behind the router, .the router must know which internal computer should receive each incoming packet of data. Since all incoming packets of data have the same IP address (the single IP address of the router), the only way the router knows which computer should receive the incoming packet is if one of the internal computers on the private LAN first sent data packets out to the source of the returning packets.

Since the NAT router links the internal private network to the Internet, it sees everything sent out to the Internet by the computers on the LAN. It memorizes each outgoing packet's destination IP and port number in an internal "connections" table and assigns the packet its own IP and one of its own ports for accepting the return traffic. Finally, it records this information, along with the IP address of the internal machine on the LAN that sent the outgoing packet, in a "current connections" table. When any incoming packets arrive at the router from the Internet, the router scans its "current connections" table to see whether this data is expected by looking for the remote IP and port number in the current connections table. If a match is found, the table entry also tells the router which computer in the private LAN is expecting to receive the incoming traffic from that remote address. So the router re-addresses (translates) the packet to that internal machine and sends it into the LAN. If the arriving packet does not exactly match traffic that is currently expected by the router, the router figures that it's just unwanted "Internet noise" and discards the unsolicited packet of data. With a NAT router protecting your connection to the Internet—even if you only have one computer on the LAN behind the router—none of the Internet scanning and worms and hackers and other annoying and malicious Internet nonsense can get to your computer or computers.

Internally a NAT router is a standard network switch interconnecting the machines plugged into the router to the router's network address translation WAN interface. What's significant for our discussion is that all of the internal machines are interconnected on the same LAN. This is convenient for sharing files and data among the machines, but it creates a security problem if all of the machines are not equally secure and trustworthy. If any malware or Trojan software were to somehow get onto any one of the machines, and that machine is on the LAN with all of the others (as it normally is), the malicious software would have access to every other uninfected machine sharing the once-secure LAN. By sending "ARP broadcasts" to the LAN, an infected machine can determine the IP and "MAC" addresses of every other machine on the LAN ... and go to work on them. Malicious hackers know all about this LAN-side vulnerability. This is why many recent viruses and worms attempt to spread not only by scanning the Internet for additional vulnerable targets, but they also attempt to spread locally through Windows file sharing, RPC vulnerabilities, and many other well-known Windows insecurities. Once one machine gets hit, every machine on the LAN can fall victim.

1.2.4.4. Application Proxy

Besides stateful packet filtering and NAT, another function of a good firewall is the application proxy service, sometimes called application gateway. Consider an application proxy as an elaborate version of a packet filter. Whereas a packet filter is capable of inspecting data only in the lower levels of an IP packet, such as the IP address or port number, an application proxy is capable of inspecting the entire application data portion of an IP packet. An application proxy can inspect network traffic that uses multiple connections. Packet filters don't recognize that separate connections to the same application belong together.

1.2.5. IP Fragments and DoS (Denial-of-Service) Attack

IP network traffic travels over all kinds of network segments between the sender and the destination. Not all of these segments or links may allow the same maximum packet size. The maximum packet size is called the Maximum Transmission Unit (MTU) of the network. If a larger

IP packet has to cross a network link that allows only a smaller size, the original IP packet can be broken into smaller IP packets and continue. These smaller packets are called IP fragments. Each of these IP fragments has its own IP header that contains the source and final destination IP addresses, as well as a fragment position number, but only a small part of the original TCP information. Therefore, only the first fragment contains the TCP part that shows the TCP port number. The other fragments carry the remaining TCP information but not the TCP port number. To speed up things after crossing the network link that allows only a smaller size, the IP fragments are not reassembled again at the other side but travel independently to the final destination. There, they are reunited again in order to form the original IP packet.

What's the poor firewall to do? The arriving IP fragments, except the first one, contain no indication of a TCP port number, so the packet filters can't make a decision based on that. Blocking the second and subsequent fragments would disallow all network packets that have passed a network link with a small maximum packet size. Reassembling the packet itself and making a decision based on the complete IP packet means that the firewall would be accepting all these fragments and storing them until all fragments have arrived and then continue. This opens up a strong possibility that a hacker can make the firewall do a lot of intensive work, especially if the hacker never sends the last packet.

The firewall may be so busy with sorting out all these small packets that it can't focus on other tasks. This is called a DoS attack (Denial-Of-Service attack). This attack is like sending the doorman a card that says "See the other side for instructions" printed on both sides. Letting the second and subsequent fragments pass the firewall may be a solution, but this strategy also has a disadvantage. The first fragment can be inspected and is possibly blocked. The final-destination computer on the internal network knows that if the first fragment never arrives, it should not reassemble the fragments that did come through and use the fragment anyway. Some implementations of TCP/IP make the mistake of reassembling the fragments, and hackers capitalize on this mistake by sending a complete IP packet that is disguised as a fragment. The firewall allows the packet to pass through, thus relying on the absence of the first fragment. The final-destination computer receives this self-advertised fragment and processes it as a complete IP packet! Because the firewall doesn't block second and subsequent fragments, the hacker is able to send packets to computers on the internal network unchecked. Verify that all computers on the internal network correctly discard IP fragments when the first fragment never arrives before allowing the firewall to pass IP fragments.

1.2.6. IP Address Spoofing and Source Routing in Hacking

Just as you can use a fake return address on an envelope and a fake 'From' address on outgoing email messages, a hacker can use a fake Source IP address in the IP packets that he sends to your firewall. This is known as IP address spoofing. The firewall should not rely on the Source IP address alone to make the decision to allow the packet to pass. By the same token, it's not useful to have the packet filters block packets based on the Source IP address. Because the Source IP address can't be trusted to be true, the firewall must be able to distinguish on which network interface the IP packets arrive.

Why would a hacker do this, and how could he possibly gain any advantage by doing this? After all, if he spoofed the sender IP address, he will have a hard time receiving the possible response packets sent in return to the fake address. You'd be surprised. Here are several good reasons (that is, from a hacker's standpoint) to send a spoofed IP packet:

- The internal network may already contain a malicious Trojan Horse application installed on one of the computers. The hacker may merely want to signal the application to start doing its lowly deed, which is similar to sending a coded message to spy on the inside: "The blue sparrow will see an early spring tonight". No need to confirm.
- The hacker may want to stage a denial-of-service attack against one of the internal computers.
- The hacker may have temporarily disabled the computer that legitimately uses the spoofed sender IP address and is pretending to answer the now lost return packets at carefully timed intervals. This resembles those irritating voicemail outgoing messages that some people seem to enjoy, where you think that the person you called actually picked up the phone, but instead the voicemail message contains deliberate pauses and pretends to respond to what you said.
- The IP packet with the spoofed IP address may actually contain a routing slip that contains IP addresses that the return packet should visit on its way to the Source IP address. This is called the Source Route option. Obviously, the hacker would list an IP address that he is monitoring on the Source Route list. To prevent the Source Route option exploit, the firewall should be configured to drop all packets that have the Source Route option turned on. This is one of the options in the IP Options field of an IP packet All of the options are for diagnostics purposes only, so the firewall packet filters can drop any packet that has any option set.

Love is over brimming mystery joins death and life. It has filled my cup of pain with joy.
- Sir Rabindranath Tagore

अध्याय 2

Chapter 2

Computer Viruses, Worms, Trojan Horses and Root kits: A Quick Recap

2.1. What Could Happen in a Cyber War

The tricks of a cyber criminal would seem trifling compared to a large-scale cyber war. Yes, you read it correctly—a cyber war! This is where things start getting much more complicated and murky. The military forces of the advanced nations and their computer wizards are gradually turning the Internet into one big minefield. In this venture, they are actively helped by computer nerds and private hackers also. A couple of keystrokes could potentially unleash such chaos that nobody will be left unaffected. The mere push of a button could bring most vital things and systems like electric power grids, dams, airlines and banking to a grinding halt. In fact the chain reaction would have such serious consequences that what started as a conflict on the Internet could quickly escalate into a military one. It's not hyperbole which prompted the US to equate hacker attacks with an invasion—they clearly understand the possible consequences. The more we look at it, the scarier it gets.

There is no doubt that all this is only the tip of the iceberg for much of the preparation for cyber war is a military secret. Whenever the world has witnessed a malicious program of the type of Stuxnet it turns out that:

- The malware "blew its cover" because of a mistake or by accident.
- It had been already quietly "sitting" in various networks for a long time and doing its work.
- Many technical features of the malware are still shrouded in. guesswork.

A standard bug in standard software usually has a containable effect—at most the computer system will collapse, a power turbine will stop or, in the worst case, something somewhere comes crashing down. May be in the case of a conventional guided missile, it could explode at the wrong time or in the wrong place. But with the new wave of computer viruses, worms, Trojan Horses and rootkits created with a military objective in mind, the error caused by them will have truly catastrophic consequences. The rogue code could reach unintended targets also and could have absolutely unpredictable effects on them. Although there might be just one intended target, the number of potential victims can be much bigger—and they could be anywhere in the world because the Internet has no boundaries or limits.

2.2. Computer Viruses

2.2.1. What is Malware in General?

A quick recap of the fundamentals of computer viruses, worms, and Trojan horses etc. is essential in the beginning because they are intimately related to cyber security and its implications. You can learn more about computer viruses, worms, Trojans and other malware in our companion volume 'Cyber Crimes: Preventive Measures And Cyber Forensics'.

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau word made by "malicious" and "software." Malware is a generic term that includes a number of hostile, intrusive, or annoying software or programming code. A computer virus is a computer program that can replicate itself and spread from one computer to another. Like the flu virus, a computer virus must spread from host to host to survive.

When we get the flu, we cough and sneeze, and tiny particles carrying the virus spread the flu to other people. With computer viruses, the virus is designed to spread from your computer to other computers. Computer virus is a type of malware because many of them are indeed malicious—in other words, they can erase your files or lock up whole computer systems. Some computer viruses are rather benign—they don't do any direct damage other than by spreading themselves locally or throughout the Internet. However, computer virus has become an immensely popular word—the lay men, the media, everybody uses it and often interchangeably with malware. A software is considered malware based on what it is intended to do and what it can do. In law, malware may also be referred to as a "computer contaminant."

The actual term "virus" was first used to denote a self-reproducing program in a short story by David Gerrold in Galaxy magazine in 1969—and later in his 1972 novel, 'When HARLIE Was One'. In that novel, a sentient computer named HARLIE writes viral software to retrieve damaging personal information from other computers to blackmail the man who wants to turn him off. The first IBM PC virus in the wild was a boot sector virus dubbed Brain, created in 1986 by the Farooq Aivi and his brother in Lahore, Pakistan, reportedly to deter piracy of the software they had written. Conventional computer viruses emerged in the 1980s, driven by the spread of personal computers and the resultant increase in BBS (bulletin board system), modem use, and software sharing. Bulletin board-driven software sharing contributed directly to the spread of Trojan horse programs, and viruses were written to infect popularly traded software. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers. Macro viruses have become common since the mid-1990s. Most of these viruses are written in the scripting languages for Microsoft programs such as Word and Excel and spread throughout Microsoft Office by infecting documents and spreadsheets. Since Word and Excel were also available for Mac OS, most could also spread to Macintosh computers.

Virus technology quickly reached a stage where the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their email systems until the virus could be contained. The ILOVEYOU virus in 2000 had a similarly devastating effect In January 2007, a worm called Storm appeared— by October, experts believed up to 50 million computers were infected. That's pretty impressive, isn't it?

2.2.2. Biology of a Computer Virus

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer as a biological virus passes from person to person. Unlike a cell, a virus has no way to reproduce by itself. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses, the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

Similar to the way a biological virus must hitch a ride on a cell, a computer virus must piggyback on top of some other program or document in order to launch. Once a computer virus

is running, it can infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks.

Many older viruses had no payload: they were simply designed to spread. Some caused unintended side-effects—as a result of poor programming, in fact! A relatively small number were deleted files or corrupted data. They could be a nuisance, or they could cause loss of data, but they seldom tried to gather data for later use. Things are different now. Today, malicious programs are designed typically to steal information. This is why many Trojans about which we will learn shortly, are referred to as spyware: they're installed stealthily, without your knowledge or consent, and they monitor your actions day after day. They carefully hide their tracks using programs called rootkits. So everything runs normally and you have no reason to suspect that there's a problem.

Virus creators have added new tricks to their bag throughout the years. One such trick is the ability to load viruses into memory so they can keep running in the background as long as the computer remains on. This gives viruses a much more effective way to replicate themselves. Another trick is the ability to infect the boot sector on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. It contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can guarantee it's executed. It can load itself into memory immediately, and run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and in places like college campuses, where lots of people share machines, they can spread like wildfire.

In general, neither executable nor boot sector viruses are very threatening today. The first reason for their decline has been the huge size of today's programs. Most programs you buy today come on compact discs. Commercially distributed compact discs (CDs) cannot be modified, and that makes viral infection of a CD unlikely, unless the manufacturer permits a virus to be burned onto the CD during production. People certainly can't carry applications around on floppy disks like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have therefore now declined, because operating systems now routinely protect the boot sector. Call it "shrinking habitat," if you want to use a biological analogy. Still, we mentioned it for historical reasons.

2.2.3. How Computer Viruses Spread?

Early viruses were pieces of code embedded in a larger, legitimate program, such as a game or word processor. When the user downloads and runs the legitimate program, the virus loads itself into memory—and looks around to see if it can find any other programs on the disk. If it can find one, it modifies the program to add the virus's code into that program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time the user launches either of those programs, they infect other programs, and the cycle continues.

Before computer networks became widespread, most viruses spread on removable media, particularly floppy disks. In the early days of the personal computer and before the Internet was invented, most users regularly exchanged information and programs on floppies. We used to keep them by the dozens. If one of the infected programs is given to another person on a floppy disk, or if it is uploaded so other people can download it, then other programs get infected. This is how the virus spreads—similar to the infection phase of a biological virus. Now their place has been taken by the flash drives. It is difficult to find a flash drive which is not infected, particularly with the virus autorun.inf. Autorun.inf virus typically spreads via removable devices and it runs as soon as a device is plugged to a computer. It defeats almost all popular anti-Virus software.

Most viruses now have a destructive attack phase where they do real damage. Some sort of trigger will activate the attack phase, and the virus will then do something—anything from displaying a silly message on the screen to erasing all of your data. The trigger might be a specific date, a number of times the virus has been replicated or something similar. Now you can recall why they had created the scare called Y2K! A virus may also send a web address link as an instant message to all the contacts on an infected machine. If the recipient, thinking the link is from a friend (a trusted source) follows the link to the website, the virus hosted at the site may be able to infect this new computer and continue propagating.

Here are some of the most common ways they spread:

Once the virus has infected your system, it may automatically send out emails containing more copies of the virus using the address book in your email program. This type of virus is called an Internet "Worm," because it is a self-propagating virus.

If the virus is a macro virus (attached to a Microsoft Word document, for example), it may attach itself to any document you create or modify. If you send another document to someone by email, the virus goes along with it.

Sometimes viruses masquerade as a fun program (like an electronic greeting card) that secretly infects your system. If you pass the program along, not realizing that it contains a virus, you will be transmitting the virus manually to your friends, family, or colleagues.

2.2.4. Email Viruses

Virus authors adapted to the changing computing environment by creating email viruses. For example, the Melissa virus in March 1999 was spectacular in its attack. Melissa spread in Microsoft Word documents sent via email, and it worked like this: Someone created the virus as a Word document and uploaded it to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an email message to the first 50 people in the person's address book. The email message contained a friendly note that included the person's name, so the recipient would open the document, thinking it was harmless. The virus would then create 50 new messages from the recipient's machine and then infect a central file called NORMAL.DOT so that any file saved later would also contain the virus. At that rate, the Melissa virus quickly became the fastest-spreading

virus anyone had seen at the time. As mentioned earlier, it forced a number of large companies to shut down their email systems to control the spread. The Melissa virus took advantage of the programming language built into Microsoft Word called VBA, or Visual Basic for Applications. It is a complete programming language and it can be used to write programs that do things like modify files and send email messages. It also has a useful but dangerous auto-execute feature. A programmer can insert a program into a document that runs instantly whenever the document is opened. This is how the Melissa virus was programmed. Now Microsoft applications have a feature called Macro Virus Protection built into them to prevent this sort of virus. With Macro Virus Protection turned on (the default option is ON), the auto-execute feature is disabled. So, when a document tries to auto-execute viral code, a dialog pops up warning the user. Unfortunately, many people don't know what macros or macro viruses are, and when they see the dialog they ignore it, so the virus runs anyway. Many other people turn off the protection mechanism.

The ILOVEYOU virus, which appeared on May 4, 2000, was even simpler. It contained a piece of code as an attachment. People who double-clicked on the attachment launched the code. It then sent copies of itself to everyone in the victim's address book and started corrupting files on the victim's machine. This is as simple as a virus can get It is really more of a Trojan horse distributed by email than it is a virus. In the case of the ILOVEYOU virus, the whole thing was human-powered. If a person double-clicked on the program that came as an attachment, then the program ran and did its thing. What fueled this virus was the human willingness to double-click on the executable. The same kinds of exploits have also been passed over instant messaging networks like AIM and Windows Live Messenger. Commandeered accounts will send out links to viruses in instant messages; anyone who clicks the link and installs a Trojan application will have their own account hijacked and unwittingly spam their own friends with the compromising link.

2.3. Computer Worms and How They Target Networks?

A worm is a computer program that has the ability to copy itself from machine to machine. Worms use up computer processing time and network bandwidth in the process of replicating, and often carry payloads that do considerable damage. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself. Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand from a single copy incredibly quickly. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

A worm called Code Red made huge headlines in 2001. Experts predicted that this worm could clog the Internet so effectively that things would completely grind to a halt The Code Red worm replicated itself more than 250,000 times in approximately nine hours on July 19, 2001. The Code Red worm slowed down Internet traffic when it began to replicate itself, but not nearly as badly as predicted. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured

server, the worm copied itself to that server. The new copy then scanned for other servers to infect Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies. The Code Red worm had instructions to do three things:

- Replicate itself for the first 20 days of each month
- Replace webpages on infected servers with a page featuring the message "Hacked by Chinese"
- Launch a concerted attack on the White House website in an attempt to overwhelm it

Upon successful infection, Code Red would wait for the appointed hour and connect to the www.whitehouse.gov domain. This attack would consist of the infected systems simultaneously sending 100 connections to port 80 of www.whitehouse.gov (198.137.240.91). The U.S. government changed the IP address of www.whitehouse.gov to circumvent that particular threat from the worm and issued a general warning about the worm, advising users of Windows NT or Windows 2000 Web servers to make sure they installed -the security patch.

A worm usually exploits some sort of security hole in a piece of software or the operating system. For example, the Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server. Wired magazine took a fascinating look inside Slammer's tiny (376 byte) program.

A worm called Storm, which showed up in 2007, immediately started making a name for itself: Storm used social engineering techniques to trick users into loading the worm on their computers. And boy, it was effective—experts believe between 1 million and 50 million computers have been infected. Anti-virus makers adapted to Storm and learned to detect the virus even as it went through many forms, but it was easily one of the most successful viruses in Internet history and could someday rear its head again. At one point, the Storm worm was believed to be responsible for 20 percent of the Internet's spam mail. When this worm is launched, it opens a back door into the computer, adds the infected machine to a botnet and installs code that hides itself. Botnets are small peer-to-peer groups, rather than a larger, more easily identified network. Experts think the people controlling Storm rent out their micro-botnets to deliver spam or adware, or for denial-of-service attacks on Websites.

Many worms that have been created are designed only to spread, and don't attempt to change the systems they pass through. However, as the Morris worm and Mydoom showed, even these "payload free" worms can cause major disruption by increasing network traffic and other unintended effects. A "payload" is code in the worm designed to do more than spread the worm-it might delete files on a host system (for example, the ExploreZip worm), encrypt files in a cryptoviral extortion attack, or send documents via email. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" computer under control of the worm author. Zombie computers are discussed a little later. Networks of such machines are often referred to as botnets and are very commonly used by spammers senders for sending junk email or to cloak their website's address. A botnet is simply a collection of internet-connected computers whose security defenses have been breached and control ceded to a malicious party.

Each such compromised device, known as a "bot", is created when a computer is penetrated by software from a malware distribution. Spammers are therefore thought to be a source of funding for the creation of such worms, and the worm writers have been caught selling lists of IP addresses of infected machines. Others try to blackmail companies with threatened DoS attacks. Backdoors can be exploited by other malware, including worms.

2.4. Trojan Horses

All of us know the story of the Trojan horse in the Greek mythological story of the Trojan War. In this tale, after a fruitless 10-year siege of Troy, the desperate Greeks hid some select soldiers inside a huge wooden horse and left it outside the gates of Troy. The Greeks then pretended to sail away, and the Trojans pulled the horse into their city as a trophy of their victory. That night the Greek soldiers crept out of the horse and opened the gates for the rest of the Greek army, which had sailed back under the cover of night. The Greeks entered and destroyed the city of Troy, decisively ending the war. Similarly, a Trojan horse, or Trojan in computing, is a type of malware that masquerades as a legitimate file or helpful program with the ultimate purpose of granting a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses employ a form of "social engineering," presenting themselves as harmless, useful gifts, in order to persuade victims to install them on their computers. Trojan horses can make copies of themselves, steal information, or harm their host computer systems. Many Trojans rely on drive-by downloads or install via online games or internet driven applications in order to reach target computers. It is possible for individual hackers to scan computers on a network using a port scanner in the hope of finding one with a malicious Trojan horse installed, which the hacker can then use to control the target computer—a side effect of Trojans is that your machine is slowed down and might even crash.

Trojan Horses are closely related to computer viruses, but they differ in that they do not attempt to replicate themselves. More specifically, a Trojan Horse performs some undesired—yet intended— action while, or in addition to, pretending to do something else. A common example is a fake login program, which collects account information and passwords by asking for this info just like a normal login program does.

A Trojan gives a hacker remote access to a targeted computer system. Operations that could be performed by a hacker on a targeted computer system may include:

- Use of the machine as part of a botnet (for example to perform automated spamming or to distribute Denial-of-service attacks)
- Electronic money theft
- Data theft (for example retrieving passwords or credit card information)
- Installation of software, including third-party malware
- Downloading or uploading of files on the user's computer
- Modification or deletion of files

- Keystroke logging
- Watching the user's screen
- Crashing the computer
- Anonymizing internet viewing

A recent innovation in Trojan horse code takes advantage of a security flaw in older versions of Internet Explorer and Google Chrome to use the host computer as an anonymizer proxy to effectively hide internet usage. A is able to view internet sites while the tracking cookies, internet history, and any IP logging are maintained on the host computer. The host's computer may or may not show the internet history of the sites viewed using the computer as a proxy. The first generation of anonymizer Trojan horses tended to leave their tracks in the page view histories of the host computer. Newer generations of the Trojan horse tend to "cover" their tracks more efficiently. Several versions of Slavebot have been widely circulated in the US and Europe and are the most widely distributed examples of this type of Trojan horse.

So how do Trojan Horses infect computers? Believe it or not, you have to do some of the work yourself. The most common way Trojan horses spread is through email attachments. The developers of these applications typically use spamming techniques to send out hundreds or even thousands of emails to unsuspecting people; those who open the messages and download the attachment end up having their systems infected. In order for a Trojan to infect your machine, you have to install the server side of the application. This is normally done by social engineering—the author of the Trojan horse has to convince you to download the application. Alternately, he might send the program to you in an email message hoping you execute it. Again, this is why it is called a Trojan Horse—you have to knowingly or unknowingly run the .exe file to install the program— it doesn't propagate on its own like a virus. Once you execute the program, the Trojan server is installed and will start running automatically every time you power up your computer.

Sometimes, it's not even a person manually spreading malware— it's possible for your own computer to do so, if it's been infected already. Crackers—hackers who use their computer skills to create mischief or cause damage intentionally—can send out Trojans that turn innocent Web surfer's computers into zombie computers, so-called because the person with the infected computer rarely knows his system is under control. Crackers then use these zombie computers to send out more viruses, eventually creating networks of zombie computers known as botnets.

There are several things you can do to protect yourself from Trojan Horses. The easiest thing to do is to never open any emails or download any attachments from unknown senders. Simply deleting these messages will take care of the situation. Installing antivirus software will also scan every file you download (even if it's from someone you know) and protect you from anything malicious. If you ever find your computer has been infected with a Trojan, you should disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. You can call your computer's manufacturer, your local computer store or a knowledgeable friend if you need help.

2.5. Spyware

2.5.1. What is Spyware and What it Can Do?

Spyware is a type of malware installed on computers that collects information about users without their knowledge. Some people mistake spyware for a computer virus. A computer virus is a piece of code designed to replicate itself as many times as possible, spreading from one host computer to any other computers connected to it. It usually has a payload that may damage your personal files or even your operating system. Spyware, on the other hand, generally isn't designed to damage your computer. Spyware is defined broadly as any program that gets into your computer without your permission and hides in the background while it makes unwanted changes to your user experience. The damage it does is more a by-product of its main mission, which is to serve you targeted advertisements or make your browser display certain sites or search results. You can learn more about this in our companion volume 'Cyber Security, Cyber Attacks And Hacking'.

Spyware attach themselves to your operating system in nefarious ways. They can suck the life out of your computer's processing power. At a minimum, most spyware runs as an application in the background as soon as you start your computer up, hogging RAM and processor power. It can generate endless pop-up ads that make your browser so slow it becomes unusable. It can reset your browser's home page to display an ad every time you open it. Some spyware redirects your Web searches, controlling the results you see and making your search engine practically useless. It can also modify the dynamically linked libraries (DLLs) your computer uses to connect to the Internet, causing connectivity failures that are hard to diagnose. At its very worst, spyware can record the words you type, your Web browsing history, passwords and other private information.

Certain types of spyware can modify your Internet settings so that if you connect through dial-up service, your modem dials out to expensive, pay telephone numbers. Like a bad guest, some spyware changes your firewall settings, inviting in more unwanted pieces of software. There are even some forms that are smart enough to know when you try to remove them in the Windows registry and intercept your attempts to do so. Some are designed to track your Internet habits, nag you with unwanted sales offers or generate traffic for their host website. According to the estimates of FaceTiume Communications, more than 80 percent of all personal computers are infected with some kind of spyware. The presence of spyware is typically hidden from the user and can be difficult to detect.

Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users. While the term spyware suggests software that monitors a user's computing, the functions of spyware can extend beyond simple monitoring. Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.

The point of all this from the perspective of the makers of spyware isn't always clear. One

reason it's used is to pad advertisers' Web traffic statistics. If they can force your computer to show you tons of pop-up ads and fake search results, they can claim credit for displaying that ad to you over and over again. And each time you click the ad by accident, they can count that as someone expressing interest in the advertised product. Another use of spyware is to steal affiliate credits. Major shopping sites like Amazon and eBay offer credit to a website that successfully directs traffic to their item pages. Certain spyware applications capture your requests to view sites like Amazon and eBay and then take the credit for sending you there.

2.5.2. How Does Your Computer Get Spyware?

Spyware does not directly spread in the same way as a virus or worm because infected systems generally do not attempt to transmit or copy the software to other computers. Instead, spyware installs itself on a system through deception of the user, or through exploitation of software vulnerabilities. Most spyware is installed without users' knowledge, or by using deceptive tactics. Spyware may try deceive users by bundling itself with desirable software. Other common tactic is using a Trojan horse. Some spyware authors infect a system through security holes in the Web browser or in other software. When the user navigates to a webpage controlled by the spyware author, the page contains code which attacks the browser and forces the download and installation of spyware.

Sometimes, spyware is included along with genuine software, and may come from an official software vendor. The installation of spyware frequently involves Internet Explorer. Its popularity and history of security issues have made it a frequent target. Its deep integration with the Windows environment makes it susceptible to attack into the Windows operating system. Internet Explorer also serves as a point of attachment for spyware in the form of Browser Helper Objects, which modify the browser's behavior to add toolbars or to redirect traffic.

A spyware program is rarely alone on a computer; an affected machine usually has multiple infections. Users frequently notice unwanted behavior and degradation of system performance. A spyware infestation can create significant unwanted CPU activity, disk usage, and network traffic. Stability issues, such as applications freezing, failure to boot, and system-wide crashes, are also common. Spyware, which interferes with networking software, commonly causes difficulty connecting to the Internet. In some infections, the spyware is not even evident. Users assume in those situations that the performance issues relate to poor or faulty hardware, Windows installation problems, or another infection. Some owners of badly infected systems resort to contacting technical support experts, or even buying a new computer because the existing system "has become too slow". Badly infected systems may require a clean reinstallation of all their software in order to return to full functionality.

Spyware often ends up on your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. These applications often use clever trickery to get you to install them, from fake system alert messages to buttons that say "cancel" when they really install spyware. Here are some of the general ways in which spyware finds its way into your computer:

- **Drive-by download:** This is when a website or pop-up window automatically tries to download and install spyware on your machine. The only warning you might get would be your browser's standard message telling you the name of the software and asking if it's okay to install it. If your security settings are set low enough, you won't even get the warning.
- **Piggybacked software installation:** Some applications— particularly peer-to-peer file-sharing clients—will install spyware as a part of their standard installation procedure. If you don't read the installation list closely, you might not notice that you're getting more than the file-sharing application you want. This is especially true of the "free" versions that are advertised as alternatives to software you have to buy. As the old saying goes, there's no such thing as a free lunch.
- **Browser add-ons:** These are pieces of software that add enhancements to your Web browser, like a toolbar, animated pal or additional search box. Sometimes, these really do what they say they'll do but also include elements of spyware as part of the deal. Or sometimes they are nothing more than thinly veiled spyware themselves. Particularly nasty add-ons are considered browser hijackers—these embed themselves deeply in your machine and take quite a bit of work to get rid of.
- **Masquerading as anti-spyware:** This is one of the cruellest tricks in the book. This type of software convinces you that it's a tool to detect and remove spyware. When you run the tool, it tells you your computer is clean while it installs additional spyware of its own.

2.6. Rootkits

2.6.1. The Cleverness of it

A rootkit is malware that is installed on a computer by an intruder for the purpose of gaining control of the computer while avoiding detection. Unlike other malware, rootkits are capable of avoiding the operating system scan and other related antivirus/anti-spyware programs by hiding files and concealing running processes from the computer's operating system. Rootkits are basically Trojan Horse malware that is used in conjunction with other malicious programs in an effort to remain undetected by the computer user or the antivirus scan system. A rootkit is designed to hide the existence of certain processes or programs from normal methods of detection and enable continued 'privileged access' to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.

Rootkit installation can be automated, or an attacker can install it once they've obtained root or administrator access. Obtaining this access is either a result of direct attack on a system (that is exploiting a known vulnerability, password (either by cracking, privilege escalation, or social engineering)) or a result of. Once installed it becomes possible to hide the intrusion as well as to maintain privileged access. Like any software they can have a good purpose or a malicious purpose. The key is the root/administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

There are several different types of rootkits which are User Mode, Kernel Mode, and Firmware rootkits.

- **User Mode:** User mode rootkits are able to run on a computer through administrator privileges which means that they are capable of accessing files, network ports, and system drivers. They copy files to the PC hard drive so they are automatically activated every time you start your computer. Rootkits in user mode can be detected and removed.
- **Kernel Mode:** Kernel mode rootkits are installed at the same level as the PCs operating system so it can influence your PCs operating system which leads to unexplained events. Rootkits in kernel mode cannot be detected by the user other than the unexplained events and crashes, or the antivirus program.
- **Firmware:** Firmware rootkits are the most malicious type of malware because they are capable of creating malcode inside the firmware while you computer is shut down. Every time you start your computer this type of malware will reinstall. Firmware cannot be detected by the user and is very difficult to remove.

2.6.2. How Rootkits Work and Why it is Difficult to Deal with Them ?

The main purpose of a rootkit is to make unauthorized modifications to the software in your PC. There are different ways that this is accomplished once a rootkit has made its way into your PC.

- **Spyware:** A rootkit can modify your software programs for the purpose of infecting it with spyware. The spyware that is installed by the rootkit is sometimes difficult to detect however, you will notice strange things happening like links appearing on your desktop and changes in the habits of your web browser.
- **Back Door:** A back door is a modification that is built into a software program in your computer that is not part of the original design of the program. It creates a hidden feature in the software program that acts like a signature so the intruder can use the software for malicious purposes without being detected.
- **Byte Patching:** Bytes are constructed in a specific order which can be modified by a rootkit. If the bytes are rearranged it compromises the computer software protections so the intruder can gain control of the software for malicious purposes.
- **Source-Code Modification:** Source code modification is accomplished by modified the code in your PC's software right at the main source. The intruder inserts malicious lines of source code for the purpose of hacking software with confidential information. The code can also end up in a myriad of other programs which makes it very difficult to locate.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it PC software is designed to make very precise decision about specific types of data and a rootkit alters the software so that it makes errors in its decisions. For this reason, a rootkit is difficult to detect and difficult to remove. Detection methods include using an alternative

and trusted operating system, behavior-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.

2.7. The Common Symptoms of Malware Infection

Here are some of the common symptoms which would tell you that your computer is infected with virus, worm, Trojan or rootkit.

- Your system slows down in an unexpected manner and does not improve even after all sorts of disk cleanup etc. This can be especially noticeable if your machine is connected to a network.
- You see activity on your machine that you did not cause. For example, a disc drive light constantly flashing.
- An internal email server becomes overloaded and slows down.
- Data files become corrupted or are found missing.
- Programs such as Microsoft Word or Excel display a message advising that the file you're trying to load is not in the correct format.
- Unexpected or unexecuted changes to the content of files.
- Programs do not run, or function incorrectly.
- Unknown tasks shown displayed in Task Manager.
- Network Performance becomes extremely slow.
- You notice that certain features that are available aren't anymore.
- Changes in the sizes of programs installed—some appear much bigger than what they ought to be.
- Paucity of space in the C drive and it does not match with the total size of the programs installed—all the programs installed could be showing their correct sizes individually but the total free space available in the drive would not correspond to (size of the drive minus total size of the programs put together.)
- Unexecuted changes in the file date or time stamp.
- Longer program load times.
- Unusual or unexpected error messages.
- Unusual screen activity.
- Failed program execution or unexpected closure of programs.
- Unexpected writes to a drive.

You may think that when such symptoms are detected, may be you could use some good anti-virus software and get rid of the infestation. Not so. These symptoms may be present when you are dealing with ordinary malware the type of which abounds on the Internet. But be advised that when extremely sophisticated and highly complicated malware is used by nation states to mount a cyber attack on sensitive computer systems of another government, the malware is obviously so designed as to not present the tell-tale symptoms.

Even after malware has been removed from a computer many of the problems caused by it may still remain. Hence, one of the first things you should do in order to fix any of those problems is to make sure that all infections have actually been removed. If you know that you still have infections on your computer then, instead of trying to fix problems while the malware is still present, you should first remove all infections. Trying to fix problems on a computer that still contains infection is basically a waste of time as the problems would crop up again. Then, after you have convinced yourself that all malware has been removed you should also check to make sure the computer is clean. Once you have confirmed that your computer is absolutely free of malware you should then back up all of your important files. This is to ensure that if anything goes wrong while fixing the computer, which does happen often, your important documents will still be intact.

If any of your files have been deleted by malware you still have a chance of recovering them. Software is available for the purpose. If you are keen on free software.

For cleaning the computer, you may run Comodo Cleaning Essentials (CCE). This program has the ability to check for, and attempt to fix, many common problems caused by infections. Another way to fix most problems caused by malware is to run a specialized tool called the Windows Repair Kit. After cleaning an infection, and making sure it has been entirely removed, the first thing you should do is to reset all of your passwords. The reason is that it is quite possible that the malware was able to capture your passwords and send them to criminals. You should also take time to uninstall, and then reinstall, any security programs which were on your computer while it got infected. Also, make sure that you only have one good antivirus software installed as having several programs can actually lead to conflicts, which can cause further problems.

After securing your computer, and removing all temporary files, you can then restore any of the backed up files that could have been lost during the repair process.

अध्याय 3

Chapter 3

Information Systems and Threats to Information Systems

3.1. Information Systems

3.1.1. History of Information Systems

Information systems (IS) have always played a crucial role in civilization. In fact, IS existed in their simplistic form even in early civilization. For example, over 500 years ago, the Inca Indians of South America developed fairly comprehensive IS with databases, and processing models composed of thousands of knotted strings called quipus. To the Indians of South America, the knots on the hanging strings, for example, represented the number of people in a village, their duties, the amount of grain in a storehouse, business transactions (as of that time), poetry, cattle livestock, records of battles and other historical events. An array of knots and different colors and sizes conveyed a combination of mnemonics, digits and narrative information.

In the mid-eighteenth century, pressures to process data increased. The Industrial Revolution shifted the basic means of production from the home and small shop to the factory. With the development of large manufacturing facilities, there arose a need for the service industry to market and transport the goods produced by the manufacturing systems. The increased size and complexity of these organizations made it impossible for a single person to obtain adequate information, to manage them effectively without the aid of data processing.

In the twentieth century, the need to record more data, analyze that data to produce more information and using it for information-led decision-making have increased even further. Business investors need the details about the financial status and future prospects of the business into which they wish to invest. Bankers and vendors need information to appraise the performance and financial soundness of a business before making loans or providing business credit. Government agencies, too, need a number of reports that disclose operating parameters of business entities. The individuals most involved with and dependent on information arc those charged with the responsibility of managing and operating organizations. Thus, when businesses and other organizations try to keep track of many things, timely and accurate information is the essential resource to maintain the operations and to remain competitive. Therefore, information is considered as a corporate asset. As with most assets, the security of this corporate asset, namely information, too becomes crucial. In fact, security of information assets is considered to be one of the success factors for businesses.

3.1.2. Importance of Information Systems

Today, we live in 'Information Age' mainly because of advances in computer and communications technology, that is information and communication technology (ICT). Most of the workforce today has jobs that are information-intensive. Take, for example, the jobs of those in the field of training and teaching, accountants, lawyers, managers and executives; these jobs are predominantly based on handling large amounts of information. Added to this is the dimension of the newly emerging 'mobile workers' who work away from their 'offices'. This paradigm greatly differs from that of earlier decades, in which most jobs involved some type of physical labor applied in farms or in factories, that is progression of our society from the agricultural age to the industrial age and now to the information age. IS now have become an inseparable part of business organization. The following figure shows the interdependence of organizations and IS.

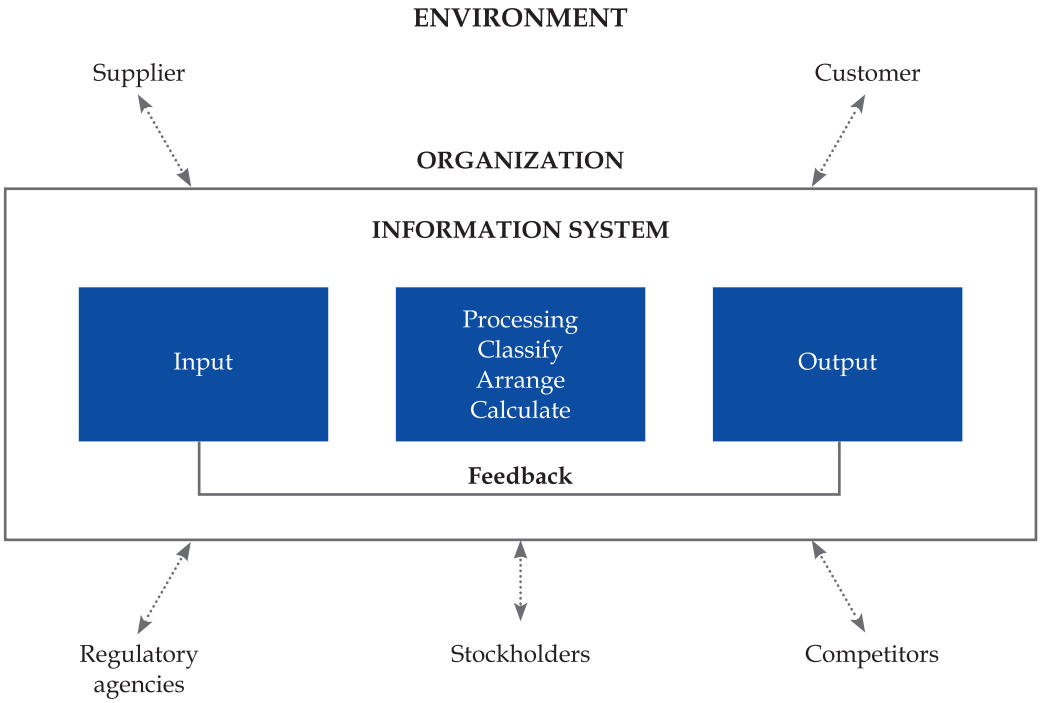


Fig. The interdependence between organizations and information systems

In today's global context, there is a consensus among strategists on a number of points regarding global businesses. Large organizations piggy-back data flows on the complex management support systems and the global communications they use to control their supply chains. Given this, business managers have reasons to believe that coordination of organizational operations is the central tenet of globalization. Thus, smooth coordination of business activities [as evidenced in supply chain management (SCM) and customer relationship management (CRM)] distinguishes the multi-domestic and multinational organizations from a truly global business. The recognition of information technology (IT) facilitating global coordination of organizations is today recognized as a key component of competitive strategy. For successful operations in the global arena, multinational organizations need to be tightly linked in their information and communication flow requirements. This amply brings out the nature and complexity of global coordination required in organizations of the future. In the global perspective of businesses today, each geographical unit plays a distinctive role. To sustain the pressures from business and to satisfy the decision-making requirement in today's dynamic environment, the nature of modern IS is such that they call for intensive and complex interaction between physically remote but interdependent units. This is why our IS today are in a networked mode - in alliance with global business partners, distributed and at multi-location giving rise to what we call the 'extended enterprise' in the digital economy.

3.1.3. Basics of Information Systems

In this section we take a brief overview of 'information systems'. We provide here only an overview, not the basics and fundamentals of information systems as there are many suitable texts available on this subject. Essentially, an information system is a set of interrelated components

that collect (or retrieve), process, store and distribute information to support decision-making and control in an organization.

Thus, IS accept data from their environment and manipulate the data to produce information that is used to solve a problem or address a business need. In the earlier days (say in the 1960s and 1970s), majority of information systems were manual systems. These days, however, information systems are mostly computerized, software-intensive systems. Today, the vast majority of computerized IS relies on data warehouses and database management system (DBMS) software to manage the storage and retrieval of the data/information in the system. Information systems consist of data, hardware, software, procedures and people. Their major functions are: input, storage, processing, control and output. IS are usually developed to support specific business functions such as the administrative functions common to most organizations. For example, in finance, we have accounting and resource management (facilities and equipment). In the finance area, organizations need financial management information systems (FMIS). For manufacturing-focused organizations, enterprise resource planning (ERP) systems are important. In the human resource (HR) area, there are HR information systems and in marketing and sales area, there are CRM systems. It is important to note at this point that not all types of information can be computerized, especially the ones with an external source. The following Table shows business area-wise organization of information.

Table : Business area-wise information

Business area	Coverage	Typical examples	Remarks
Business environment	Business conditions external to the organization that can impact its business activities	1. Rules and compliance set by regulatory agencies 2. Issues created by competitors 3. Licensing authorities' requirements	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company's products	1. Prospects 2. Customers	Organizations use these mechanisms for capturing potential customers -(prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	1. Advertisement campaigns 2. Target audience 3. Company websites	These often pertain to marketing/ prospecting activities. They can also apply to internal and other communications

External organizations	Organizations, except customers and suppliers, external to the company	1. Complementors / business partners 2. Existing competitors 3. Potential competitors	In the paradigm of networked organizations' of today, this inclusion is important
Facilities and equipments	Real estate and structures and their related components, movable machinery, devices, tools and their integrated components	1. Buildings and surroundings 2. Heavy machinery 3. Testing and other equipment 4. Factories	Software that is integral to equipments is included within this area; other software is included within information area, Integrated components (e.g., security alarm system within an office or plant) are often included as a part of the facility

In view of the discussion so far, conceptually, 'information' can be divided into three parts. First, there are data that bring together all kinds of information that can be stored (such as personal data, information concerning customers, accounting, etc.). Second, there is knowledge, that is, those aspects that are not immaterial but brought in by experienced employees. Lastly, there is the action to send information to someone or something through the information system. However, a clear distinction needs to be made between 'information systems' and 'systems and data-processing networks'. An information system refers not only to data but also to users and methods and thus is a more global notion. That is why some people define an "information system' as a system, whether automated or manual, that comprises people, machines and/or methods organized to collect, process, transmit and disseminate data that represent user information.

3.1.4. The Changing Nature of Information Systems

In the past decade, the nature of IS has undergone a dramatic change, from mainframe-based IS to client/ server computing to today's web-based information system, with the Internet having made the revolution. Alvin Toffler, in his books, talks about the rate of change affecting humanity. In one of his most popular books, Third Wave, he mentions about the impact on humanity by the three waves: first, the agricultural wave; second, the industrial wave; and third, the information wave. In line with these thoughts expressed by Toffler, it can be argued that the fourth wave has begun — the wave created by mobile technology, arid web services follow suit. The four powerful worldwide changes that have altered the business environment are:

1. globalization;
2. rise of the information economy;
3. transformation of the business enterprise;
4. emergence of the digital firm.

Modern business applications of IS show a trend toward the development of systems that are decentralized, autonomous and heterogeneous. The new generation of IS is characterized by the combination and integration of local IS (mostly databases), each with their own intended purpose and goal. Thus, today, the IS used by business enterprises and individuals are no more monolithic and no more are they housed in a single location, residing on a single piece of hardware, that is server. Information systems of today are distributed and component-based. For more details on the basics of information systems/management information systems, readers can follow standard books on the topic. In many of today's information-intensive enterprises, the local structured procedures can be effectively and flexibly integrated into the global work processes supporting the business goals.

3.1.5 Globalization of Businesses and the Need for Distributed Information Systems

Liberalization, privatization and globalization have become the three 'mantras' of success in the digital economy led by the rise of e-business. Business competition and pressures are on the rise like never before. Businesses now have no geographical boundaries. With the rise of mobile commerce (m-commerce) fuelled by mobile technologies, we are now witnessing the era of anywhere anytime computing. Naturally, 'information' that has been one of the vital corporate resources (in addition to the traditional '3Ms', i.e., man, materials and money) assumes a higher dimension when it comes to data and information security (InfoSec). In the paradigm of mobile computing, information as a vital corporate resource has the threat of falling in the hands of those for whom it is not intended. Protecting the data and information is crucial as businesses make knowledge-based decisions. We certainly do not want the confidential data and information to be leaked outside the required boundaries.

We talked about the 'waves' in the previous section. There is an important point to be noted — while the industrial age witnessed great developments in terms of engineering, a significant dimension, connectivity, was missing. Producers and consumers of goods all remained disparate and unconnected. They operated in islands of geographical pockets without knowing how the others were transacting their businesses. This isolation is not true anymore in today's paradigm of 'extended enterprise' resulting from the new way of doing the business, namely the electronic business or, popularly known as, e-business'. So, prior to e-business days, not only did the suppliers and consumers remain separated, but the knowledge producers/knowledge workers and business personnel also remained relatively unconnected.

The 'third wave' has what the 'second wave' did not have: connectivity. Connectivity is a great boon from the 'Internet' — one of the most exciting revolutions of this century and truly a paradigm changing force. Connectivity in the Information Age not only brought the consumers and producers together, but also built the bridge between the 'thinkers', business people, the governments, the common people, the academicians and so on. We need to consider at the scope of modern-day IS in this global context.

In the new paradigm, IS are handling information in all forms, not just the text-based data of the 1970s that came typically in flat files but also the rich text, images/graphics and voice. So,

we are in the realm of not only terabytes of data but also multimedia, multi-geo order of IS. The widening scope of IS can be summarized as follows:

1. 1950s: technical changes;
2 1960s-1970s: managerial controls;
3. 1980s—1990s: institutional core activities;
4. Today: digital information webs extending beyond the enterprise.

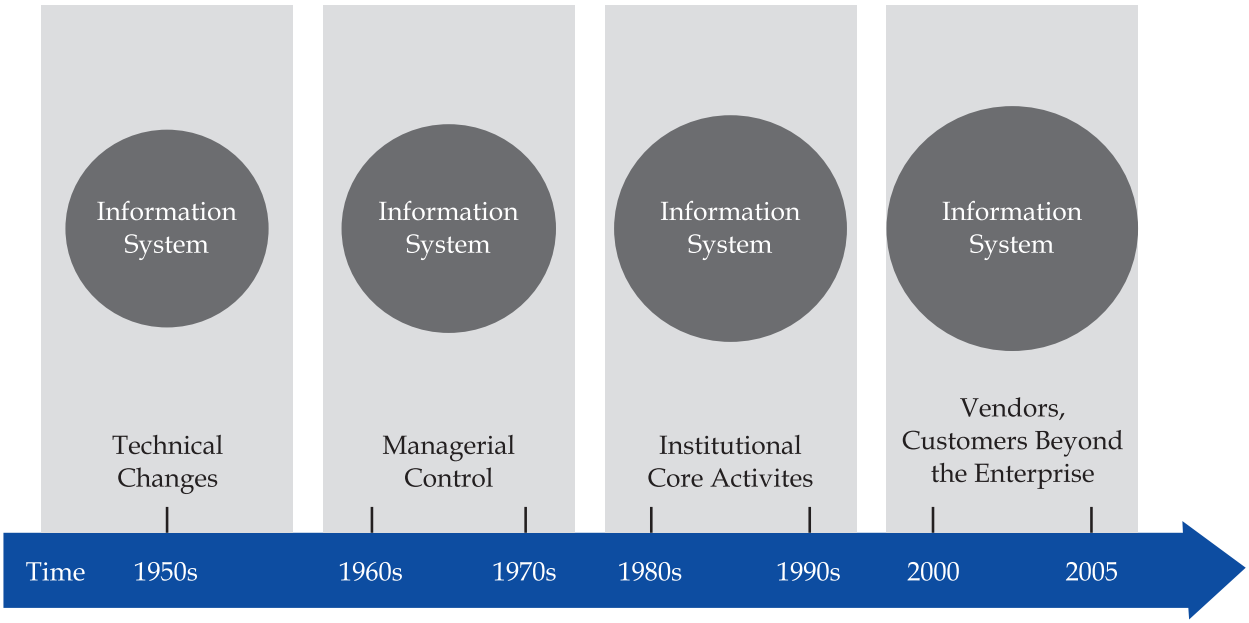


Fig. The wider scope of information systems

Today's firms are 'digital' in terms of their rapid operations mode. They are characterized by electronic commerce (e-commerce) and e-business to operate in the 'digital market' where IS link the buyers and sellers to exchange information, products, services and payments. Thus, today, the era is of the 'extended enterprise' and to serve the needs of such networked enterprises; the IS, too, are no more confined to a single location, single computer.

3.1.6. Global Information Systems: Role of Internet and Web Services

The Internet, one of the most marvelous inventions of this century, in fact, a 'killer application, is the international network of networks. The Internet is a universal technology platform that allows any computer to communicate with any other computer in the world. Furthermore, one of the advantages of the Internet is that nobody really owns' it. It is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity that we know as the Internet. In fact, the very name comes from this idea of interconnected networks as shown in following Figure.

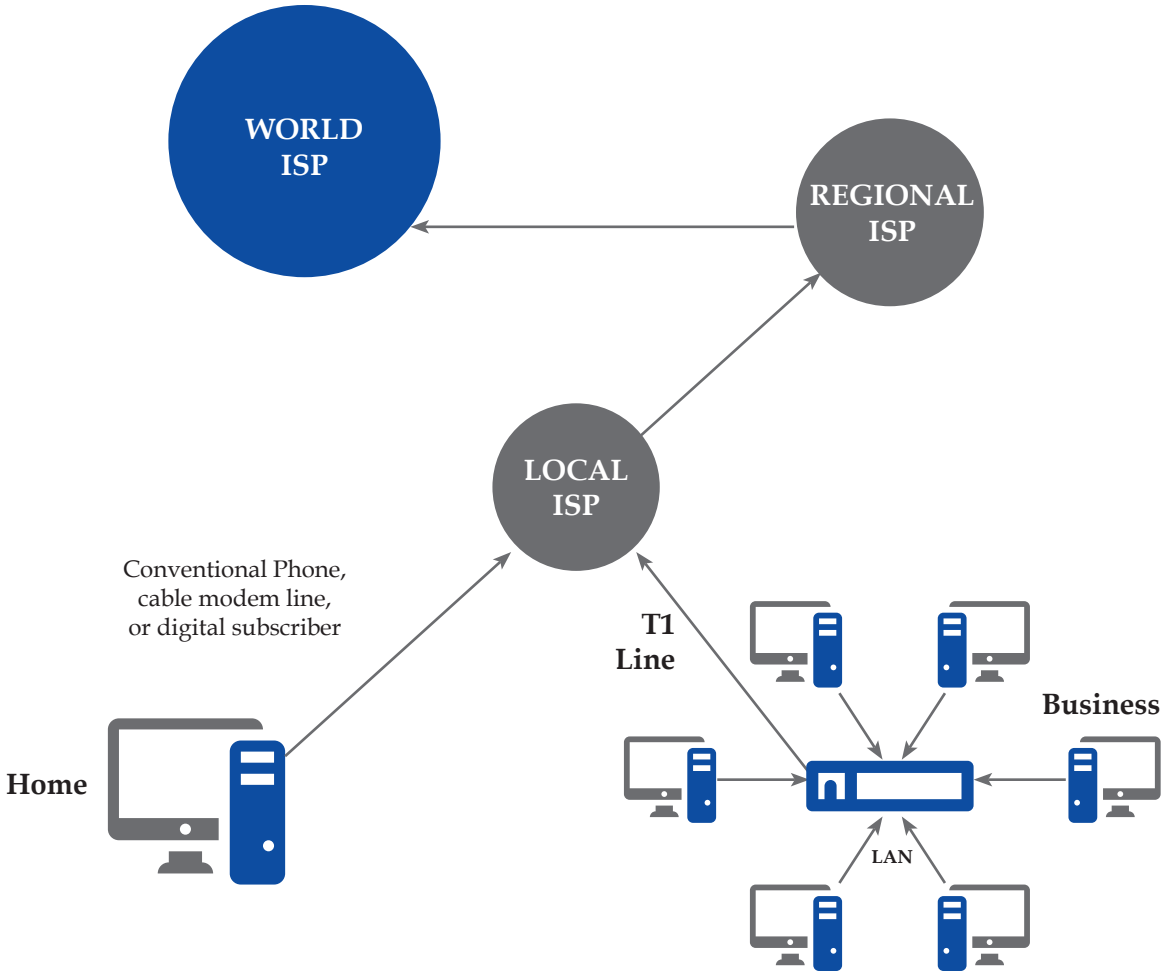


Fig. The Internet

The Internet has become so well-meshed in the day-to-day working of the knowledge workers that its contribution is acknowledged by everybody. Although the Internet, indeed, has brought the world closer in a way, this very 'free' and 'autonomous' nature of the Internet does have some implications for the security of IS as we will see later. In this section, we focus on the contribution of web services to modern IS in the global.

The Internet has revolutionized communication and thereby its contribution to information sharing. With access to a computer and an appropriate connection, anyone can interact with others worldwide. However, the web is designed to exchange unstructured information: while people can read web pages and understand their meaning, computers cannot. If corporations want to conduct business over the web, humans have to be involved unless there is a way for computers to communicate on their own. This is where web services come in. They make it possible for companies to do business through their computer systems exploiting the Internet, infrastructure.

Web services play a complementary and dominant role in building global IS for today's dynamic business world. IBM's definition of web services states that 'Web Services are self-contained, modular applications that can be described, published, located and invoked over a

network, generally, the World Wide Web (WWW).' Companies send and receive a great deal of information, by automating even a small part. However, one of the greatest benefits from web services comes from links between companies, where extended processes between companies can be automated. This is very much essential in the paradigm of today's 'extended enterprise concept.

Web services perform functions ranging from simple requests to complicated business processes. Once a web service is developed, other applications and other web services can discover and invoke the deployed service through universal description, discovery and integration (UDDI). The idea of web services is to leverage the advantages of the web as a platform to apply it to the services themselves, not just to the static information. 'Services' refer to components and the services offered that can be used to build larger application services. Web services make it easier to build service-based architectures without the applications being locked-in to a particular software vendor's products.

Web services have been proven to give a strong return on investment (ROI) and make computer-based IS more adaptable. They also help bring productivity, flexibility and low maintenance cost in the development of IS by integrating components from various third-party vendors (another avenue for implementing appropriate security measures in the IS). Web services make information available from computer systems to other applications using well-defined standards. Discussion on the details of standards adopted in web services is beyond the scope of this book.

Benefits of web services for developing IS of global nature are as follows:

1. Web services tools are available for most computer systems, including mainframes and packaged applications. This means that not only the existing applications can be retained, but also the existing knowledge of staff can be applied and extended using web services for business integration.
2. Web services are adaptable and can handle changes more readily than other integration solutions, because they use structured text as their message format. Therefore, because the cost of maintenance is reduced, the overall cost of a web services system also reduces.
3. IT managers now have the ability to exchange data between most applications, on most computers, in a consistent and standard way. Tools and further standards are therefore emerging to build composite applications that can model and manage business processes around these business-level components.
4. If necessary, an alternative application can be used to provide web services without changing the overall effect of the system. This gives significant flexibility in the choice of a supplier. This aspect is particularly important in the consideration of outsourcing security services.

3.1.7. Information Systems Security and Threats: A Glimpse

So far, we have seen that the use of IS has become mandatory for businesses to perform their day-to-day functions efficiently. In this section, we set the context for understanding the issues related to IS misuse, resulting threats and countermeasures. This section is only an overview about threats to IS.

Given the crucial role played by information systems, it is important that they remain secured and that the data contained in them do not fall into the hands of those who are not intended to have access to it. Security of IS becomes particularly important with the advent of the Internet. The access by Internet in particular allows a mass of information to remain up-to-date in real time, but it also opens the door for external encroachment. Thus, it is essential to ensure the physical protection of the information that, when stored without precautions on the hard disk of a computer connected to the Internet, can be read, copied, modified or destroyed from a working station located somewhere on the planet without the owner realizing the tampering.

In the modern business era, the use of desktop PCs, laptops, and network connectivity including the Internet and electronic mail (e-mail) is as essential as the telephone at workplace. The employees and networked IS are the most valuable assets for any organization. The misuse of information systems by employees, however, poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce their appropriate usage policies and minimize their losses as well as increase the productivity of knowledge workers. The basics of information systems security are related to:

1. Trademark, copyright, patent and trade secrets and protection strategies for each of them
2. Software licensing issues
3. Data Privacy under legal framework
4. InfoSec and control frameworks such as Control Objective for Information and related Technology
5. Evidence of digital forensic practices and ethics;
6. Computer Frauds and Abuse Acts boundaries for illegal access to computers / computer-based IS;
7. Electronic surveillance and cyber crimes.

InfoSec measures are mandated by statutes such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) (because most Indian IT/software firms have majority of their business with the United States, it is important to include this).

Summary

Information systems play a crucial role in today's complex business world. They have come a long way progressing from the precivilization era, through the agricultural era, to the present networked enterprise era in our digital economy. To fulfill the demands placed on them, today's IS are global in nature and complex in their structure. Information is an important asset and needs to be protected all the time. Threats to IS come from many avenues and these threats will continue, given our dependence on information system.

3.2. Threats to Information Systems

3.2.1. Introduction of Threats to Information Systems

Information systems security is the integrity and safety of its resources and activities. In the cyber world, it can be almost impossible to trace sophisticated attacks to their true source. The anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information-based international economy and the advancement of global collaboration and cooperation in all areas of human endeavor.

Previously, we discussed about the strategic importance of information systems (IS) and their role in the global context. In this chapter, our objective is to provide a context for management role and responsibility for ensuring the security of IS in the organization. To achieve this, our focus in this chapter is to provide an overview of 'threats to IS'.

3.2.2. New Technologies Open Door to the Threats

For companies in the modern era, in particular those engaged in electronic business (e-business), it is increasingly important to be aware of the online threats because more and more people are using the Internet to access information about their (prospective) business partners, customers and other business-related links. In today's world, almost all business organizations have IS that use integrated technologies such as the networks of computers, company intranets or Internet access to communicate and transmit information for rapid business decisions, thereby opening the organization to the external world like never before. Under these circumstances, threats from outside the organization must be addressed, because the damages from non-secured information system can result in catastropic consequences for the organization. Given this, organizations must investigate and evaluate the factors that could be a threat to the integrity of the information system.

Threatening Online Activities

Hacking of computer systems and launching of denial of service (DoS) attacks as well as spreading of malicious code, such as viruses, are well-known online threats that deserve attention in the computer security and security management domain. Far less attention is provided to the fact that the Internet has enabled a range of potentially threatening activities that are based on the active or passive dissemination of certain information. Examples of such information-based threatening activities are:

1. **Myths, rumors and hoaxes:** Hoaxes are false e-mail messages with the only purpose to spread to as many people as possible. Along with myths and urban legends, they live on the Internet. Such messages may have significant impact on companies, their reputations and thus on their businesses.

   More recently, the globally operating mobile phone company Ericsson was the victim of a hoax promising recipients free mobiles if they forward the letter to at least 20 people. Ericsson received thousands of e-mail from people asking for their free phones. The article (Park, 2000) quotes an Ericsson Australia spokesman claiming that the company was aware of the e-mail circulating for at least a couple of days and that the way it was sent makes it impossible for them to see where the e-mail originated from.

Another report (Fumento, 1999) has the story about a Canadian manufacturer who used his/her website to spread information that products of competitors may be dangerous. Moreover, the company's marketing head has been observed to actively support feminists preparing a petition to start a boycott of the company's competitors. According to Fumento (1999), however, scientific investigations suggest that the information is nothing but a myth.

2. **Threats to websites:** There are reports that the US-based car manufacturer Ford decided not to go online to combat a certain revenge website as the company was afraid that anything they would do on their own website would validate what is described on the revenge website!

3. **Limited attention to cyber crimes:** So far, threats on the information level, referred by lawyers as 'commercial terrorism through the Internet', have not received much attention in the computer security and security management literature. A look at the relevant literature suggests that these fields tend to focus on making corporate computer systems and networks secure in order to protect systems. Interested readers may like to refer to the paper by Lueg (2001).

3.2.3 Information-Level Threats versus Network-Level Threats

As a reference to the discussion in the rest of this chapter, we describe three basic terms: threat, vulnerability and countermeasures. A threat is a possible event that can harm an information system, whereas vulnerability is the degree of exposure in view of a threat. Finally, a countermeasure is a set of actions implemented to prevent threats. Next, let us consider a working definition of information-level threats. Information-level threats (or information-based threats) are threats that involve the (purposeful) dissemination of information in such a way that organizations, their operations and their reputations may be affected. Dissemination may be active as in the case of sending an e-mail or it may be passive as in the case of setting up websites.

It is important to distinguish 'information-level threats' from network-level threats'. By network-based threats we mean that in order to become effective, potential attackers require network access to corporate computer systems or to networks used by corporate computer systems. Examples for network-based threats (or threats on the network layer) are hacking of computer systems and launching of DoS attacks as well as spreading malicious code, such as viruses. Other security issues involved when data are transmitted over networks are confidentiality, authentication, integrity and non-repudiation.

Information-level threats also make heavy use of network but at the primary level is the content of a message and not its form. Sending fake inquiries to service accounts to eat up resources (e.g., flooding the mail server with many messages so that it gets choked) would qualify as an information - based attack - as it is the content of the messages that would provide a basis for the attack. Other examples of information-based threats are setting up revenge websites and disseminating false or biased information as in the case of the false accusation. Such attacks can cause considerable damage to the goodwill of the organization against which they may be launched, and customer loyalty is too good to lose.

Dissemination of information that is likely to trigger specific counter-reactions as in the case of say some falsified job advertisement also qualifies as information-based threat. Essentially, a DoS attack that is based on flooding accounts with large quantities of e-mail is a network-based attack as it is the size and the quantity of the e-mail that matters and not the content of the e-mail.

3.2.4 Information Systems Security: Threats and Attacks

Attacks can be represented by the relation among threat, vulnerability and damage. Threat and vulnerability have already been defined. Before the rise of Internet and the increase in the number of connections from and to the outside, threats were mainly physical ones (intrusion into the company premises without authorization, robberies, vandalism, etc.). Protection could be summed up in a very few access control rules using, for example, multi-locks and security guards. Nowadays the situation is quite different. Admittedly, there are still thefts of equipment or intrusion through the main console. Attacks via the network have reached a critical point and companies still do not know what the best measures to be taken are.

The above discussion brings us to classifying information systems security threats. Security threats have four principal sources that include:

1. **Human error:** for example, inadvertent disclosure of confidential information.
2. **Computer abuse or crime:** these days crime is rampant. A generic example is when a person intends to be malicious and starts to steal information from sites, or cause damage to, a computer or computer network. In particular, consider these examples; An Internet-based computer fraud can happen when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe s/he has won a large award in a non-existent foreign lottery. In the US, for example, 'wire-fraud' is a specific form of computer-related crime where the means of communications is a central feature of the offence, credit card data from hacked websites, password-sniffing programs used to obtain information required to gain access to the password owner's system.
3. **Natural and political disasters:** this can happen in the form of natural calamities and wars, riots, etc.
4. **Failure of hardware or software:** for example, server malfunctioning, software errors, etc.

Computer crime is defined as any illegal act in which a computer is used as the primary tool. Computer abuse is unethical use of a computer. Security threats related to computer crime or abuse include:

1. **Impersonation:** The impersonator enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.
2. **Trojan horse method:** Concealing within an authorized program a set of instructions that will cause unauthorized actions.
3. **Logic bomb:** Unauthorized instructions, often introduced with the Trojan horse technique, which stay dormant until a specific event occurs (or until a specific time comes, as the

instructions may keep checking the computer's internal clock), at which time they bring into effect an unauthorized act.

4. **Computer viruses:** Segments of code that are able to perform malicious acts and insert copies of themselves into other programs in the system and onto the diskettes placed in the computer. Because of this replication, a virus will progressively infect healthy programs and systems. Close relatives of viruses are worms - independent programs that make and transmit copies of themselves through telecommunications (TC) networks. Computer viruses have become a pervasive threat in personal computing.
5. **DoS:** Rendering the system unusable by legitimate users.
6. **Dial diddling:** Changing data before or during input, often to change the contents of a database.
7. **Salami technique:** Diverting small amounts of money from a large number of accounts maintained by the system. These small amounts will not be noticed.
8. **Spoofing:** Configuring a computer system to masquerade as another system over the network in order to gain unauthorized access to the resources the system being mimicked is entitled to.
9. **Super-zapping:** Using a system's program that can bypass regular system controls to perform unauthorized acts.
10. **Scavenging:** Unauthorized access to information by searching through the residue after a job has been run on a computer. Techniques range from searching wastebaskets or dumpsters for printouts to scanning the contents of a computer's memory.
11. **Data leakage:** There are a variety of methods for obtaining the data stored in a system. The data may be encoded into an innocuous report in sophisticated ways, for example, as the number of characters per line.
12. **Wiretapping:** Tapping computer TC lines to obtain information.
13. **Theft of mobile devices:** This is a new dimension that is coming up given the increase in mobile workforce.

Some of the above-mentioned crime techniques may be used for a direct gain of financial resources, others for industrial espionage, while yet others simply for destructive purposes. Probably the most important unrecognized threat today is the theft of portable computers, with access codes and information in their memories. Also to be considered are the losses owing to the theft of intellectual property, such as software, product development information, customer information or internal corporate documents.

Computer Viruses: The bête noire of Computing Era

Computer viruses deserve a special attention in the sense that they are really the 'black beasts' of modern computing era! They are the most frequently encountered threats to end-user computing and are the best-known form of computer threat. A computer virus is a piece of program

code that attaches copies of itself to other programs and thus replicates itself. Computer viruses possess certain characteristics:

The attacked program may work properly, but, at some point, will perform a malicious or destructive act intended by the attacker who has written the virus.

Although a computer virus may attack a multi-user system with shared disk facilities, viruses are best known for their rapid spread in a personal computer (PC) environment. In this environment, they proliferate through infected diskettes or programs downloaded from the Internet or other networks.

Most viruses are insidious and their presence is not obvious after the infection. In the meantime, they infect other programs.

Two principal types of viruses are boot infectors and program infectors. Boot infectors replace the contents of the first sector of the diskette or hard disk. These are the viruses that most commonly occur in personal computing. Program infectors copy themselves into the executable files stored on the hard disk.

3.2.5. Classifications of Threats and Assessing Damages

So far we have discussed the threats to IS. Discussion in this section forms the basis for understanding security management in an organization in terms of security policies, security architectures and security procedures / processes. Also we will see later, preventive measures are the best to avoid threats. However, even after all this, since we do not operate in a foolproof and ideal world, things may still go wrong and then the next action is to get into a recovery mode. Organizations expect that their security managers are in a position to evaluate the damage caused when a security incident or an actual attack takes place so. that the management can draw the budget for security-related spending. For this, it is important that the threat and resulting damages are categorized. Security managers need to know explicitly about the assets of their organizations, the vulnerability of their IS to different threats and their potential damages.

A threat is an indication of a potential undesirable event. It refers to a situation in which a person could do something undesirable (e.g., an attacker initiating a DoS attack against an organization's e-mail server) or in which a natural occurrence could cause an undesirable outcome (e.g., a fire damaging an organization's information technology (IT) hardware). Threats consist of the following properties.

1. **Asset:** something of value to the organization (information in electronic or physical form, IS, a group of people with unique expertise, etc.).
2. **Actor:** who or what may violate the security requirements - confidentiality, integrity, and availability (CIA) - of an asset. Actors can be from inside or outside the organization.
3. **Motive (optional):** indication of whether the actors intentions are deliberate or accidental.
4. **Access (optional):** how the asset will be accessed by the actor (network access or physical access).

- **Outcome :** the immediate result of violating the security requirements of an asset (disclosure, modification, destruction, loss, interruption, etc.).

The major categories of damages resulting from threats to the IS are:

- destruction of information and /or other resources;
- corruption or modification of information;
- theft, removal or loss of information and /or other resources;
- disclosure of information (confidential data);
- modification of important or sensitive information;
- interruption of access to important information, software, applications or services.

Each threat and vulnerability must be related to one or more of the organizational assets requiring protection. Thus, prior to assessing damages (caused by security incidents), we need to identify assets. Typically, there are five categories of logical and physical assets:

1. **Information :** documented (paper or electronic) data or intellectual property used to meet the mission of an organization.
2. **Software:** software applications and services that process, store or transmit information.
3. **Hardware:** IT physical devices considering their replacement costs.
4. **People:** the people in an organization who possess skills, competencies, knowledge and experience that are difficult to replace.
5. **Systems:** IS that process and store information (conceptually, a system is a combination of information, software and hardware assets. In computer networking terms, any host, client or server also can be considered a system).

Another way of grouping the threats is to put them together in groups based on some common themes suggested as follows:

1. **Human actors using-network access:** The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
2. **Human actors using physical access:** The threats in this category are physical threats to an organizations critical assets. They require direct action by a person and can be deliberate or accidental in nature.
3. **System problems:** The threats in this category are problems with an organizations IT systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code and other system-related problems.
4. **Other problems:** The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (such as floods,

earthquakes and storms) that can affect an organization's IT systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructures (TC, electricity, etc). Other types of threats outside the control of an organization can also be included here. Examples of these threats are power outages, broken water pipes, etc.

Thus, we can see that threat profiles can be represented as a tree structure. This structure depicted in the following figure that shows the assets, access, actors, motives and the other possible outcomes. An important point to notice is that organizations should have a suitable method for 'asset classification' to know which of their assets are critical.

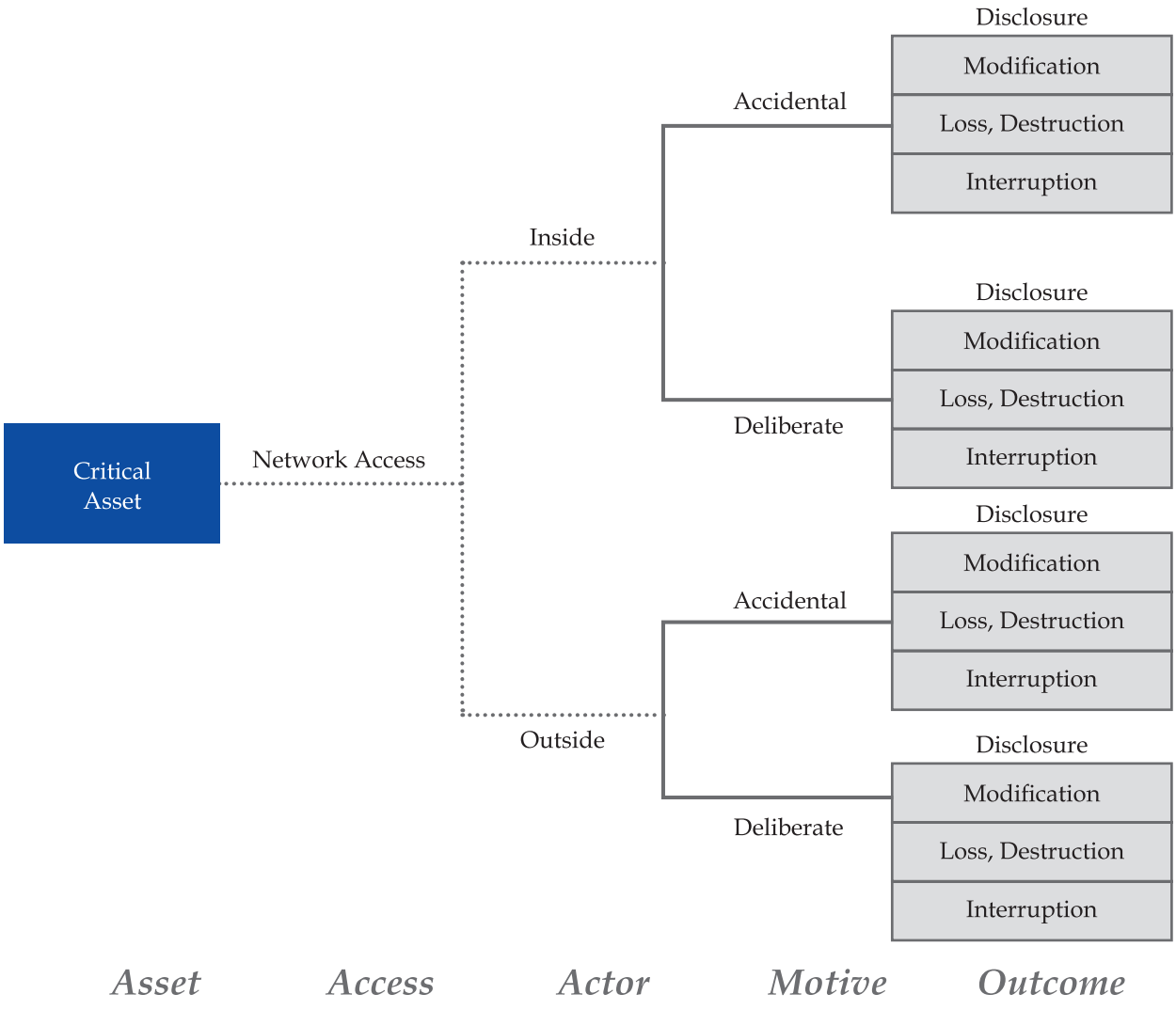


Fig. Generic Threat Profile

Organizational assets are evaluated using various suitable units of measurements. Monetary value of assets is the most commonly used unit. It is not always easy to measure assets in absolute terms. In such cases, measurement for assessment of damages can be done in relative ways, for example, information. The value of information can be measured as a fraction or percentage of total

"When a man is denied the right to live the life he believes in, he has no choice but to become an outlaw."
- Nelson Mandela

budget, assets or worth of a business in relative fashion. Assets may also be ranked by sensitivity or importance to an organization in relative ways.

The impact of information security (InfoSec) incidents may well be financial, in form of immediate costs and losses of assets. For example, the cost of downtime per hour caused by a DoS attack can be computed by measuring the loss of :

1. **Productivity:** (number of employees impacted) x (hours wasted) x (burdened hourly rate). Note that burdened hourly rate could be the notional cost of the employees - for example, billing rate of the employees to the customer or in terms of their outgoing cost to the employing organization (salary of the employees).
2. **Revenue:** direct loss and lost future revenues.
3. **Financial performance:** credit rating and stock price.
4. **Other expenses:** equipment rental, overtime costs, extra shipping costs, travel expenses, etc.

Hidden costs are difficult to handle. Consider the example of a DoS attack where the damaged reputation of the company can have a negative impact on the relationship of the company with its customers, suppliers, financial markets, banks and business partners. These hidden costs are extremely difficult to quantify and measure. The bottom line is that the cost of an information systems security incident in a company has to be measured in terms of the impact on its business; hence, identical incidents in two different companies can have different costs. To evaluate these costs and measure the impact of a security incident on a company, organizations need a systematic approach and a comprehensive risk management system.

Reason for Security Breaches

IS and networks are often inherently insecure because they are designed with functionality, not /security, as their primary goal. Most organizations view security threats as inbound, that is from outside /to inside. However, there are major threats to security that are introduced not by external sources but by employees themselves. It is important that organizations understand the inside threats and extend perimeter security controls to local desktops with security measures such as host-based intrusion detection system (IDS), personal firewall and anti-virus software.

1. **Employee Issues and social engineering:** With easy availability of hacking tools, disgruntled employees can find ingenious ways of unauthorized access to corporate confidential data. Security breaches can even happen owing to accidental risk of attaching wrong files in e-mail attachment or sending e-mail to wrong recipient. This shows why policies about e-mail usage are so important.

   Social engineering attacks can trick legitimate, though naive, users into providing them with access to corporate systems. Sharing folders on a PC, choosing weak passwords, sharing passwords, leaving important printouts on desk and not locking the screens are some of the examples of lack of sense of security, due care and diligence. Whether the origin of such

incidents is malicious intent or inadvertent employee error, the result is the same: loss of revenue, productivity and potential liability.

2. **Rise in mobile workers:** Prevalence of laptops and wireless connectivity to the Internet has only compounded the security control problems for organizations. The mobile workers using laptops at homes without appropriate controls (as per organizational guidelines) may introduce viruses, worms or offensive content into the corporate network when they connect their laptops at workplace. The use of laptops also poses significant exposure of an organization's confidential information when it gets out of the organization network. Therefore, organizations must have appropriate mobile computing policies in place to protect their information assets.

3.2.6. Protecting Information Systems Security

The discussion in the previous section shows that the security of IS needs to be maintained by measures taken to prevent threats to these systems or to detect and correct the effects of any damage. The aim of information systems security is to protect corporate assets or, at least, to limit their loss. Security measures limit the access to information to authorized individuals; there can be no privacy or confidentiality of data records without adequate security.

We need to understand that good InfoSec design starts with a threat model — what the system is designed to protect, from whom, and for how long. Threat modeling involves thinking about the system as a whole and imagining the vulnerability landscape. It must take into account the information to be protected, the people who will use the system as well as how they will use it. Whether external or internal, threats are opportunities that have the potential to cause harm or loss to organizations. As such, organizations need to adopt adequate measures to combat such threats to mitigate the resulting risks.

Information systems controls play a crucial role to ensure secure operations of IS and thus to safeguard assets and the data stored in these systems. Information systems controls need to be established to ensure that the business applications achieve their objectives in an efficient manner, and that organizations need to institute a set of policies, procedures and technological measures. Information systems controls are classified as follows:

1. **Preventive controls:** prevent an error or an attack from taking effect. These are designed to prevent or restrict an error, omission or unauthorized intrusion.
2. **Detective controls:** detect a violation. These controls exist to detect and report when errors, omissions and unauthorized use or entry occur.
3. **Corrective controls:** detect and correct an exceptional situation. These controls are designed to correct errors, omissions and unauthorized users and intrusions once they are detected.

Information systems controls are classified as:

1. **General controls:** controls applying to the entire IS activity in the organization.
2. **Application controls:** controls that are specific to a given application (payroll). Application controls are employed at application security layer. This topic will be discussed in detail in reference to the security audit best practices.

If I had the power to influence Indian journals, I would have the following headlines printed in bold letters on the first page: Milk for the infants , Food for the adults and Education for all. ***- Lala Lajpat Rai***

From the preceding discussions we learn that, for protecting the IS, threats must be stood before effective InfoSec measures are devised. This is typically done through risk assessment for safeguarding IS. During risk assessment, vulnerabilities and threats are analyzed. Threats can be classified according to the way they can occur — non-fraudulent, that is accidental, and fraudulent, that is intentional. A more elaborate way to classify threats is to say that they can be fundamental, which represents what an attacker really wants to do: information disclosure, information tampering, DoS, repudiation and illegitimate use — for example, masquerade or authorization violation and underlying threats, for example, eavesdropping or administrative error.

Given the role of IS and threats to them, the matter of their security warrants senior management attention in an organization. This is so because, in addition to assuring protection against threats and compliance with certain legal requirements, InfoSec has evolved into a powerful tool for developing business solutions. Effective InfoSec promotes business objectives and expands business opportunities; therefore, InfoSec can be viewed as a business enabler. When managed effectively, InfoSec can deliver a competitive edge by generating new markets and revenue streams and leveraging new distribution channels. The nature and degree of threats faced by organizations vary; therefore, a risk assessment of the likelihood that security will be compromised is needed. An acceptable level of InfoSec can be introduced and maintained only if the set of security controls, procedural and technical, is correctly identified, implemented and maintained. These activities must be seen as a never-ending process. Furthermore, organizations should aim to gain an understanding of the specific characteristics of the emerging environment that may generate new threats. The consequences of failure to do so may severely impair their ability to carry out their business and may even lead to legal exposures and liabilities. This is where security policy plays a crucial role.

Summary

Information system is a unit that includes technologies, people and processes. Threats, that organizations have to cope with are numerous and can have catastrophic consequences on the future of the organizations. The last few years have seen a proliferation of automated IS, reliance on the Internet to enable most of the essential services and infrastructures, and the growing threat of organized cyber attacks capable of causing debilitating disruption to our critical infrastructures. Proliferation of computers and networks in the age of the Internet has enabled not only novel services, such as e-mail, the web and electronic commerce (e-commerce), but also new ways to affect companies, their businesses and their reputations. The Internet has the potential to become an even greater threat to computer security than dial-up telephone modems. However, a look at the relevant literature suggests that information-level threats are not yet sufficiently addressed.

It is now widely acknowledged that security of computer-based IS is an important topic and the state-of-the-art security tools can provide some protection against threats ranging from hackers trying to break into corporate computer systems to DoS attacks. Companies should be able to reduce vulnerabilities as well as the potential impact of still successful attacks. However, it is unlikely mat there will ever be a 'security end state'. The situation is like accepting that software

will be buggy; similarly, when it comes to IS, some levels of threats are always residual. There is a need for an equally important step toward a realistic assessment of computer security and toward a lasting change of attitudes and expectations. One of the most overlooked threats in a corporate security program is the threat posed by employee behavior. Prevention of the misuse of IS by employees has a direct business value. User awareness and training also play a role here. Controls and policies play a crucial role in mitigating threats to information systems security; although not fool-proof in themselves, they occupy a central role in information systems security management.

अध्याय 4
Chapter 4

Information Security – Building Blocks, Management in Organizations and Physical Security for Information Systems

4.1. Building Blocks of Information Security

4.1.1. Introduction

So far, we have discussed about the role of information systems (IS) in the global context, the crucial role that IS play in the modern digital economy, how information systems are getting complex given the combined effect of globalization and liberalization, etc. We discussed about organizational responsibility for the information systems security. We also explained the role of security policies and security procedures, standards and guidelines, etc. With this background, we now present the layers of information security (InfoSec).

4.1.2. Basic Principles of Information Systems Security

With the background set through earlier chapters, our aim in the current chapter is to provide a comprehensive overview of the fundamental concepts in InfoSec. This is essential for forming the right kind of background for the discussion on risk assessment and analysis, which is the cornerstone for any security management exercise in organizations.

In the paradigm of information systems security, 'system' can denote a number of things:

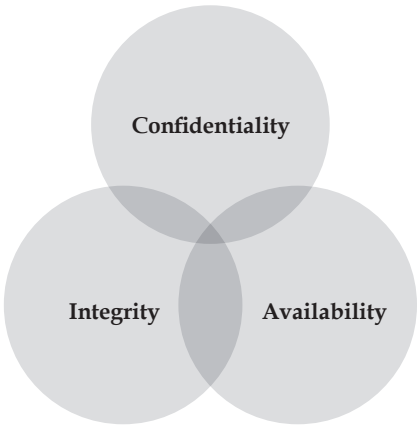


Fig. Security Goals

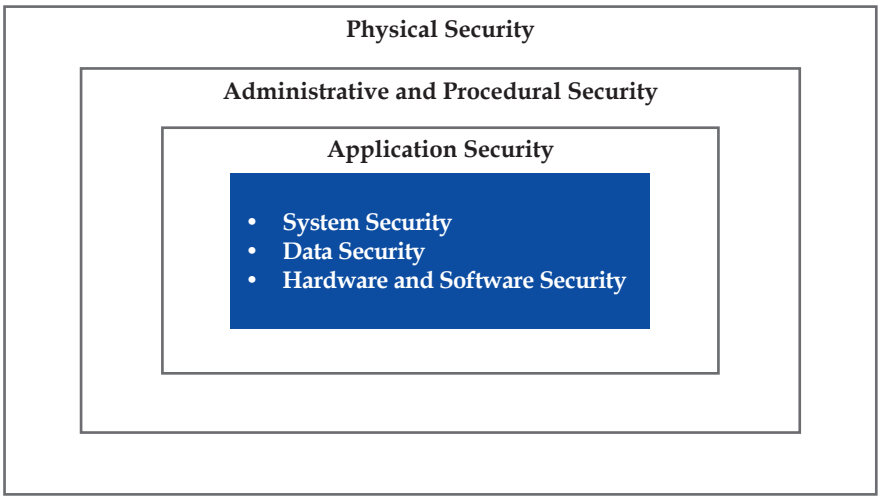


Fig. Security Layers

"Take up one idea. Make that one idea your life - think of it, dream of it, and live on that idea. Let the brain, muscles, nerves, every part of your body, be full of that idea, and just leave every other idea alone. This is the way to success that is way great spiritual giants are produced." ***- Swami Vivekananda***

1. A product or component, for example, a protocol for cryptograph, a card for wireless network access, a smart card or say a motherboard or Personal Computer Memory Card Industry Association (PCMCIA) card of a personal computer (PC), disk controller on a PC, that is a hardware unit that performs a certain function with the virtue of its design.
2. An operating system (OS) and communication system on a network.
3. Organization staff, organization structure, security policies, standards, guidelines and procedures together as a collection.
4. The Internet, which is a system consisting of a large number of computers and computer networks.
5. An application system such as a financial accounting system, a payroll system, etc.

4.1.3. Security-Related Basic Terms and Definitions

In this section, we introduce some fundamental terms important for discussions about security-related topics. These terms are important in the domain of e-security, that is matters of electronic security. Only the major terms related to InfoSec and e-security are addressed here.

1. **Electronic security:** Protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the interception techniques or any other illegitimate means of obtaining information.
2. **Non-repudiation:** Method by which the sender of data is provided with a proof of delivery and the recipient is assured of the sender's identity (ID), so that neither can later deny having processed the data. This concept is connected with the concept of electronic signature.
3. **Electronic signature:** Process that operates on a message to assure message source authenticity and integrity, and source non-repudiation.
4. **Encryption:** Modification of data for security purposes prior to their transmission so that they are not comprehensible without the decoding method.
5. **Cipher:** Cryptographic transformation that operates on characters or bits of data.
6. **Cryptanalysis:** Being able to 'break' the cipher so that the encrypted message can be read. It can be accomplished by exploiting weaknesses in the cipher or in some fashion determining the key.
7. **Cryptography:** Principles, means and methods for rendering information unintelligible and for restoring the encrypted information to an intelligible form.
8. **Denial of Service (DoS) attacks:** The DoS attack might use some of the following techniques to overwhelm a target's resources;
    - filling up a target's hard drive storage space by using huge electronic mail (e-mail) attachments or file transfers;
    - sending a message, which resets a target host's subnet mask, causing a distribution of the target's subnet routing;

- using up all of a target's resources to accept network connections, resulting in additional network connections being denied.

Subnet mask is a scheme that distinguishes network ID from host ID. It is used to specify whether the 'destination host is local or remote.

9. **Interception:** This term is typically used with defense systems and warfare. The term is introduced here because it is used in explaining other security-related terms in this section.
10. **TEMPEST:** This is a short name that refers to investigation, study and control of compromising emanations from telecommunications (TC) and automated IS equipment. This term is often used in connection with military/defense applications.
11. **TEMPEST test:** This is yet another term used in connection with military/defense applications. It refers to laboratory or on-site test to determine the nature of compromising emanations associated with TC or automated IS.
12. **TC and automated information systems security:** Protection afforded to TC and automated IS, in order to prevent exploitation through interception, unauthorized electronic access or related technical intelligence threats and to ensure authenticity.
13. **Technical penetration:** Deliberate penetration of a security area by technical means to gain unauthorized interception of information-bearing energy.
14. **Spoofing:** Interception, alteration and retransmission of a cipher signal or data, in such a way as to mislead the recipient. Spoofing refers to an attacker deliberately including a user (subject) or a device (object) into taking an incorrect action by giving its incorrect information.
15. **Steganography:** Art of hiding the existence of a message. For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image. The word 'steganography' comes from the two Greek words: steganos meaning 'covered' and graphein meaning 'to write'. Steganography can be used to make a digital watermark to detect the illegal copying of digital images. Thus, it aids confidentiality and integrity of the data.

4.1.4. The Three Pillars of Information Security

The following three concepts are considered the pillars of InfoSec confidentiality, integrity, and availability (CIA). These concepts represent the fundamental principles or InfoSec. All the InfoSec controls and safeguards, and all the threats, vulnerabilities and security processes are subject to this CIA yardstick.

4.1.4.1. Confidentiality

In the domain of InfoSec, the concept of 'confidentiality' is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights.

4.1.4.2. Integrity

This is yet another very important concept in InfoSec. The concept of integrity ensures that:

- Modifications are not made to data by unauthorized personnel or processes.
- Unauthorized modifications are not made to data by authorized personnel or processes.
- The data are internally and externally consistent, that is the internal information is consistent among all subentities and the internal information is consistent with the real world, external situation.

4.1.4.3. Availability

This is the last of the important triad in InfoSec. The concept of availability' ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, availability' guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

4.1.5. Other Important Terms in Information Security

The term automated information systems security is synonymous with computer security. There are also several other important concepts and terms that a security professional/security practitioner/students of InfoSec course must fully understand. These concepts include identification, authentication, accountability, authorization and privacy. Let us have a brief description of each of these terms:

1. **Identification:** It indicates the means by which users claim their identities to a system. It is most commonly used for access control, and is necessary for authentication and authorization.
2. **Authentication:** This is the testing or reconciliation of evidence of a user's ID. It establishes the users ID and ensures that the users are who they say they are. Authentication is a security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's eligibility to receive specific categories of information.
3. **Accountability:** A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual. Audit trails and logs support accountability.
4. **Authorization:** The rights and permissions granted to an individual (or process), which enable access to a computer resource. Once a user's ID and authentication are established, authorization levels determine the extent of system rights that an operator can hold. Thus, authorization is the access rights granted to a user, program or process.
5. **Privacy:** This means the level of confidentiality and privacy protection that a user is given in a system. It is an important component of security controls. Privacy guarantees not only the fundamental tenet of confidentiality of a company's data, but also the privacy level of data, which is being used by the operator.

4.1.6. Information Classification

Having discussed some basic security terms, we now turn to another important topic from security perspective: information classification. Generally speaking, organizations like to 'classify' their information for suitable treatment in terms of InfoSec. It is not possible to protect all the information and IS in the organizations. There are several reasons why the organizations (government, private, public and defense) like to classify information. The main reason is that not all data/information have the same level of importance or same level of relevance/criticality to an organization. Some data, such as trade secrets, formulae (used by scientific and/or research organizations) and new product information (such as the one used by the marketing staff and sales force), are so valuable that their loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility. Events like those could damage the company's goodwill.

Thus, it is obvious that information classification provides a higher, enterprise-level benefit. The primary purpose is to enhance CIA, and to minimize the risks to the information. It is well known that in most countries, information classification has had the longest history in the government sector. Its value has been established, and it is a required component when securing trusted systems. In this sector, information classification is primarily used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

The other reason for information classification may also be the compliance required with privacy laws and legislations, or other regulatory compliance. A company may wish to employ classification to maintain a competitive edge in a tough marketplace. There may also be sound legal reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information. In all, classification of information and information assets helps organizations to apply security policies and security procedures toward protection of information assets that are considered critical. We can summarize the benefits of information classification as follows:

- Information classification is a demonstration toward an organizations commitment to security protections.
- It helps identify which information is most sensitive or vital to an organization.
- It supports the tenets of CIA as it pertains to data
- It helps identify which protections apply to which information.
- It fulfils statutory requirements toward regulatory, compliance or legal mandates.

Thus, the key point is that the information produced or processed by an organization must be classified according to the organization's sensitivity to its loss or disclosure. These data owners are responsible for defining the sensitivity level of the data. This approach enables the security controls to be properly implemented according to its classification scheme. In the next section, terms used for classification of data/information are introduced.

4.1.7. Terms for Information Classification

The following definitions describe several schemes used for levels of data/ information classification, ranging from the lowest to the highest level of sensitivity:

1 **Unclassified:** Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.

2 **Sensitive but unclassified (SBU):** Information that has been designated as a minor secret, but may not create serious damage if disclosed. Answers to tests are an example of this kind of information. For example, consider health care information of a hospital.

3 **Confidential:** Information that is designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security. This level is used for documents labeled between SBU and secret in sensitivity.

4 **Secret:** Information that is designated to be of a secret nature. The unauthorized disclosure of this information could cause serious damage to the country's national security.

5 **Top secret:** This is the highest level of information classification (e.g., information in defense organizations). Any unauthorized disclosure of top secret information will cause exceptionally grave damage to the country's national security.

Given the 'information overload' in the present dynamic business environments, it is neither good to deal with too much information nor good to provide employees and other business entities with 'all' the data. Therefore, the organizations make data available to those concerned on a 'need-to-know' basis. For this reason, the following data/information classification is also prevalent in most private organizations:

1. **Public:** Information that is similar to unclassified information, that is all of an organization's information that does not fit into any of the other categories can be considered public. This information should probably not be disclosed. However, if it is disclosed, it is not expected to seriously or adversely impact the company.

2. **Sensitive:** Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality, as well as from a loss of integrity owing to an unauthorized alteration.

3. **Private:** Typically, this is the information that is considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees. Salary levels and medical information could be considered as examples of 'private information'.

4.1.8. Criteria for Classification of Data and Information

Let us now discuss what criteria could be used for classifying information that is treated as a corporate resource. Several of the following criteria are used to determine the classification of an information object:

Nationalism in India has … roused the creative faculties which for centuries had been lying dormant in our people.
- Netaji Subhash Chandra Bose

1. **Value:** It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization or its competitors, it needs to be classified.
2. **Age:** The classification of the information may be lowered if the information's value decreases over time. In the Department of Defense, some classified documents are automatically declassified after a predetermined time period has passed.
3. **Useful life:** If the information has been made obsolete owing to new information, substantial changes in the company or other reasons, the information can often be declassified (considerations like these are especially important in CRM, data warehousing and DM domain).
4. **Personal association:** If information is personally associated with specific individuals or is addressed by a privacy law, it may need to be classified. For example, investigative information that reveals informant names may need to remain classified.

4.1.9. Information Classification: Various Roles

From the security perspective, the roles and responsibilities of all participants in the information classification program must be clearly defined. A key element of the classification scheme is the role the users, owners or custodians of the data play in regard to the data. Concepts such as these are important for project leaders and project managers in software development organization even from configuration management and data management perspective, aspects that are emphasized by continuous improvement models such as the International Organization for Standardization (ISO) 9001:2000 and Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMM-I) (see www.isp.com and www.sei.cmu.edu for details). The information on roles provided in the following table is also important from the legal perspective that is very important in security domain.

4.1.10. Business Systems' Classification

We have discussed how organizations like to classify their information. Just like information and data of an enterprise or organization are classified, so are business systems in organizations. The following Table presents the generally accepted classification. This concept is especially important in the risk analysis for information systems security.

Table : Business Systems' Classifications

Business systems' classification	Meaning
Critical	Functions supported by the system cannot be performed unless they are replaced by identical capabilities. Critical applications/systems cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.
Vital	Functions can be performed manually but only for a brief period of time. Higher tolerance to interruption than with critical systems and, therefore, lower cost of interruption provided restoration is within a certain time frame (usually a week).

Business systems' classification	Meaning
Sensitive	Can be performed manually, at a tolerable cost, for an extended period of time. While it can be performed manually, it usually is a difficult process and requires additional staff to perform.
Non-critical	These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

4.1.11. Event Classification

Event that can result in damage to IS are typically classified as:

1. **disaster:** an event that causes permanent and substantial damage or destruction to the property, equipment, information, staff or services of the business;
2. **crisis:** an abnormal situation that presents some extraordinary high risks to a business and that will develop into a 'disaster' unless carefully managed;
3. **catastrophe**: major disruptions resulting from the destruction of critical equipment in processing.

The following Figure presents the relationship among various security-related terms.

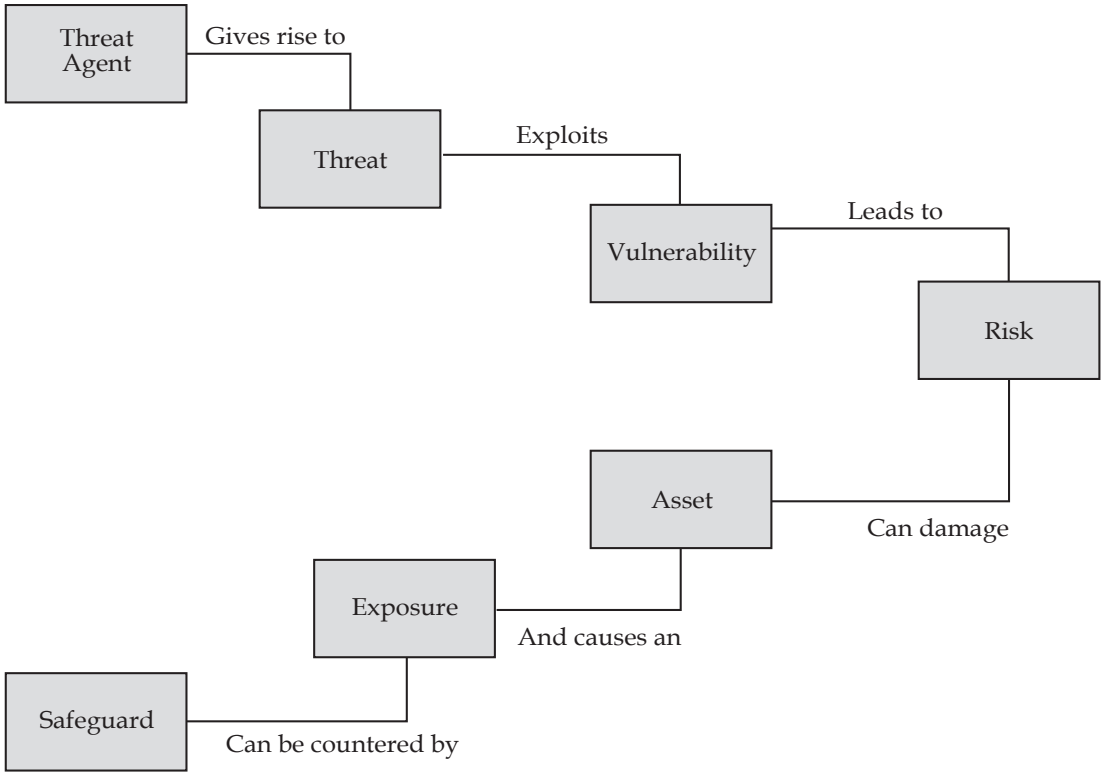


Fig. Relationships among Different Security Concepts

4.2. Information Security Management in Organizations

4.2.1. The Context for Information Security Management (ISM)

The prime driver for enterprise security is Internet connectivity. According to International Data Corporation (IDC), the worldwide information security market was worth USD 6.7 billion in 2000. With a compounded annual growth rate (CAGR) of 25.5%, this market was projected to more than triple to USD 21 billion by the end of 2005. According to an IDC analyst, remote local area network (LAN), Internet, extranet/intranet and wireless access services will drive the need for advanced InfoSec services, as technologies for circumventing network security systems continue to keep pace with the technologies designed to defend against them. This provides us the context for the chapter. We use the context to learn about organization's responsibilities for managing InfoSec.

4.2.2. Security Policy, Standards, Guidelines and Procedures

Security Policy and Policy Types

We aim to discuss two important terms in this section: 'policy' as a general term along with various types of policies and the meaning of 'security policy'; as a specific term. A policy is one of those terms that can mean several things in the information security domain. For example, consider a firewall. There are security policies on firewalls which refer to the access control and routing list information. Note that even standards, procedures and guidelines are referred to as 'policies' in the larger sense of a global InfoSec policy. A well-written policy is more than an exercise created on paper - it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a governmental or regulatory function. A policy can also provide protection from liability owing to an employee's actions or can form a basis for the control of trade secrets.

Types of Policies

When the term 'policies' is used rather than "policy, the intent is to refer to those policies that are distinct from the standards, procedures and guidelines.

The following figure shows that 'Policies' are considered as the first and the highest level of documentation. Lower level elements of standards, procedures and guidelines flow from policies. However, this does not imply that the lower level elements are not important. It is just that the higher level policies, being general in nature, should be created first for strategic reasons and then the tactical elements should follow. With this brief introduction, we now list the policy types and then describe each briefly. Essentially, there are the following types of policies:

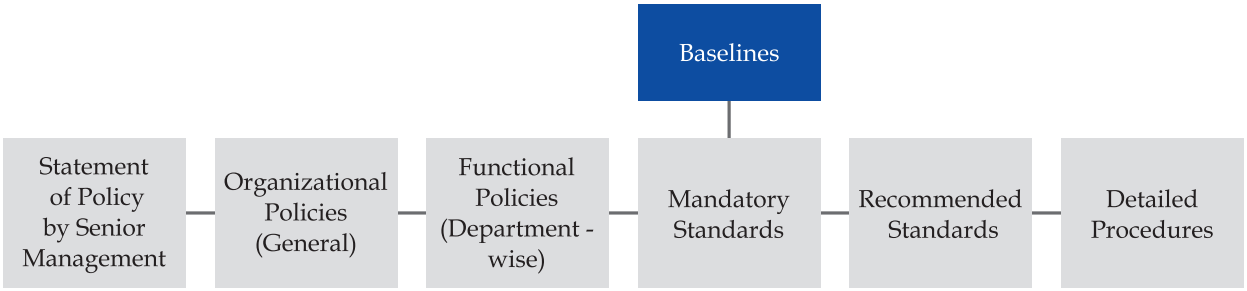


Fig. Policy Hierarchy Chart

1. **Senior management statement of policy:** This is the first step in the policy creation process. This is a general, high-level statement of policy that contains the following elements:
   - an acknowledgement of the importance of computing and networking resources, that are part of the information system, to the organization's business model;
   - a statement of support for InfoSec throughout the business enterprise;
   - a commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.
2. **Regulatory policy:** These are security policies that an organization must implement owing to compliance, regulation or other legal requirements as prevalent in the organization's operating environment, both internal and external. The various entities with which the business organization interacts can be financial institutions (such as those in the banking sector), public utilities or some other types of organizations that operate in the public interest. Regulatory policies are usually very detailed and specific to the industry in which the business organization operates. The two main purposes of the regulatory policies are:
   - ensuring that an organization follows the standard procedures or base practices of an operation in its specific industry;
   - giving an organization the confidence that it is following the standard and accepted industry policy.
3. **Advisory policy:** These are security policies that may not be mandated but are strongly recommended. Normally, the consequences of not following them are defined (e.g., Business Conduct Guidelines in an organization — not following these could result in job termination). An organization with such policies wants its employees to consider these policies mandatory. Most policies fall under this broad category.
4. **Informative policy:** These are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal entities (within the organization) or external parties.

Having discussed the term 'policy' in general, let us now turn to 'security policy'. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization. A security policy can be an organizational policy, an issue-specific policy or a system-specific policy.

Security policy can be defined as a codified set of processes and procedures applied to secure the fulfillment of its obligations and the continuation of its activities even in the presence of possible interferences. This definition may appear to be vague as compared to the others that may be found in technical computer-related publications — it is actually crafted by choosing each word precisely. Security policies are most often referred to in the context of information technology (IT), telecommunications (TC) or information and communications technologies (ICTs). Moreover they are often, erroneously though, associated exclusively with the deployment of computer hardware

or software and the configuration of the hardware or software, to the point of the 'configuration' being called security policy.

The definition given in the International Organization for Standardization (ISO) standard 17799 is a slightly different one: 'Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation'. It should be remembered that ISO standard 17799 assumes an implicit definition of what is a policy, and a separate indication is provided about the necessity of a policy document including an indication of possible contents (not reproduced here): 'A policy document should be approved by management, published and communicated, as appropriate, to all employees'.

It must be pointed out that any other standard on security should not be applied or used in a mechanical way like a-fixed formula, but rather it should be interpreted keeping in perspective the needs and working model of the 'entity' (e.g., business, non-profit organization, university, etc) in which its application is planned, as well as the needs of the organization that created it. This is because in an organizational security policy, the management establishes how a security program will be set up, establishes the program's goals, assigns responsibilities, shows the strategic and tactical value of security and outlines how enforcement should be carried out. Thus, the security policy must address prevalent laws and regulations as applicable as well as the liability issues that may arise and how they must be addressed to satisfy the statutory requirements.

Security Engineering Principles

It shows the goals of security engineering as a discipline

Goals of Security Engineering

1. Understand security risks;
2. establish security needs;
3. develop security guidance (policies, standards, and procedures);
4. determine acceptable risks;
5. establish security assurance.

Who Practices Security Engineering?

1. Product developers;
2. product vendors;
3. product integrators;
4. product buyers;
5. security evaluation organizations;
6. system administrators;
7. consulting/lT service organizations;
8. program/project management teams.

Security Related Process Areas in Systems Security Engineering Capability Maturity Model (SSE-CMM) (Version 3.0)

The SSE-CMM provides a community-wide standard metric to establish and advance security engineering as a mature measurable discipline. It contains five levels of maturity.

level 1: performed informally;

level 2: planned and tracked;

level 3: well defined;

level 4: quantitatively controlled;

level 5: continuously improving.

The Security Best Practices in the SSE-CMM are given in the following list of process areas (PAs):

PA01: administer security controls;

PA02: assess impact;

PA03: assess security risk;

PA04: assess threat;

PA05: assess vulnerability;

PA06: build assurance argument;

PA07: coordinate security;

PA08: monitor security posture;

PA09: provide security input;

PA10: specify security needs;

PA11: verify and validate security.

Standards, Guidelines and Procedures

Policy hierarchy chart represent the hierarchical nature of relationship between business goals and objectives, technology strategy, information security strategy, standards and procedures. The following Figure: Building blocks of information security presents the components/building blocks of information security. The word policy' is prominent in all these figures and therefore we must now discuss some most common terms in connection with security management, namely policies, standards, guidelines and procedures.

In reference to the Figure: Policy hierarchy chart, it can be seen that the next level down from policies consists of the three, elements of policy implementation, namely standards, guidelines and procedures. These three elements hold the actual details of the policy, such as how it should be implemented and what standards and procedures should be followed. They are published in an organization via manuals stored on the company intranet, booklets

for distribution to the employees and other entities concerned with it, for spreading security awareness in the organization. An important point to note is that standards, guidelines and procedures are separate yet linked documents from the general policies, especially the senior-level policy statement. It is not a recommended practice to create a single document to cover the needs of all these elements.

Electronic Mail (E-Mail) Policy : An Example

In an organization, the following may be stipulated with respect to the use of e-mails by employees and individuals who work in the organization (say contractor personnel)

1. **E-Mail policy coverage:**
   - Confidentiality of information disclosed through e-mail communication:
   - sender's responsibility for the contents of the e-mails;
   - disclosure of sensitive information such as passwords, personal identification number (PIN) and credit card.
2. **Appropriate use of e-mails:**
   - Employees and other personnel working for the organization and using the organization e-mail facilities shall use e-mail strictly for business use only.
   - No obscene or profane message should be sent through e-mails.
   - E-Mail should not be used for sending spam mails, chain mails, graphics, etc.
   - E-Mails should not be automatically forwarded to addresses outside the company.
   - Size of the e-mail should be restricted within approved limits set by the organization.
3. **Management's authority on e-mails:**
   - The management reserves the rights to monitor the use of e-mails.
   - The management could store the e-mails for retrieval at a later date for any legal purpose.
   - Any encryption done to e-mail attachments should be with the company's approval and the encryption key should be stored for retrieval when necessary.
4. **Disclaimer notice:**
   - Since an e-mail is not a secure medium and it is very easy to read, copy or alter an e-mail, put a disclaimer similar to the one given as follows (the company can at least protect itself from any misuse):
   - 'The information in this mail is confidential and is intended solely for the addressee. Access to this mail by anyone else is unauthorized. Any copying or further distribution beyond the original recipient is not intended and may be unlawful. The opinion expressed in this mail is that of the sender and does not necessarily reflect that of the XXX company'.

Password Policy: An Example

The policy on passwords can be used to define attributes with which the password must comply. The password policy, for example, can enforce the following conditions:

- whether the user identity (ID) and password can match;
- maximum occurrence of consecutive characters;
- maximum instances of any character;
- maximum lifetime of the passwords;
- minimum number of alphabetic characters;
- minimum number of numeric characters;
- minimum length of the password;
- whether the user's previous password can be reused.

4.2.2. Information Security Scenario in the Financial Sector

In the financial sector, the Reserve Bank of India (RBI) has created a comprehensive document that lays down a number of security-related guidelines and strategies for banks to follow in order to offer Internet banking. The guidelines broadly talk about the types of risks associated with Internet banking, the technology and security standards, legal issues involved and regulatory and supervisory concerns. Any bank that wants to offer Internet banking must follow these guidelines and adhere to them as a legal necessity.

Recent InfoSec surveys indicate that the banking and finance sector companies, most serious about security, are the major investors in security solutions, and regularly revise their security policies following periodic audits. Next in line are the software service companies, business process outsourcing (BPO) firms and IT-enabled services companies. However, verticals such as manufacturing continue to lag, except the companies that have extensive enterprise resource planning (ERP) setups or those that drive their supply chain through the web. Aside from these three verticals, companies in other verticals have a long way to go in establishing InfoSec.

4.2.3. Information Security Management System (ISMS)

In the preceding sections, we discussed the working of security-related practices through policies, standards and procedures. A mechanism that works well for this is an ISMS, whose objective is to provide a systematic approach to managing sensitive information in order to protect it. It encompasses employees, processes and information. We can see that some basic measures must be applied to secure the information system. Security threats must be managed and controlled; establishing a global policy, that is, a broad security policy, with management involvement helps to do this. "While doing mis, four levels of documentation emerge, as depicted in the below figure.

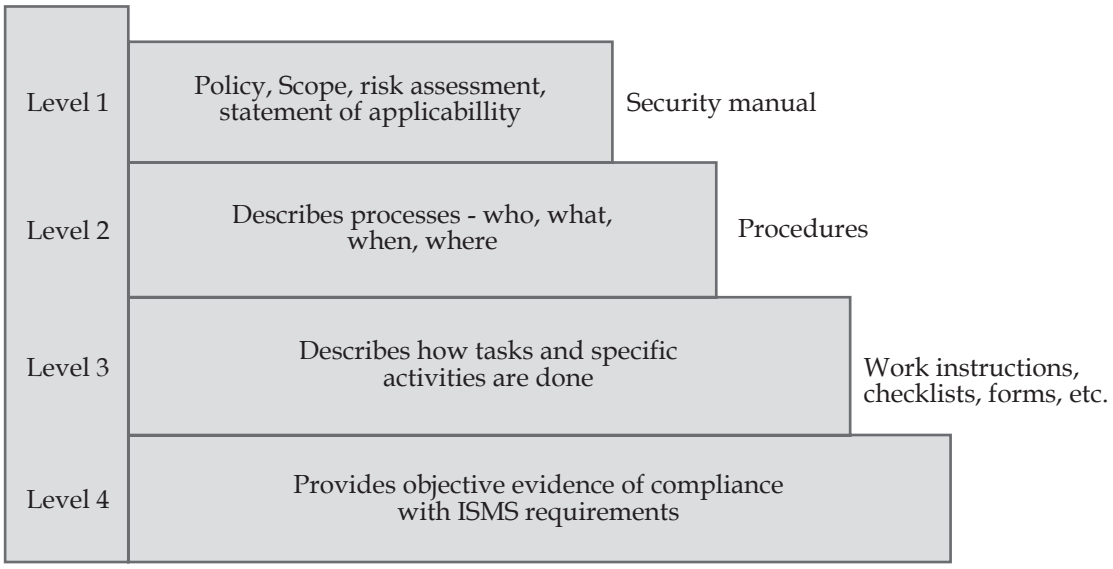


Fig. Documentation Levels in Information Security Management System

In previous chapter, we discussed threats to information systems (IS). In this chapter, in the earlier sections, the discussion was on the management's role for security formation. Given that it is necessary for the organizations to identify the nature of possible threats to its IS, one of the best practices is to establish a set of measures, called 'controls'. Controls are meant to ensure the security of IS and, beyond that, to also ensure the privacy and confidentiality of information stored in the systems. It is then necessary to continually evaluate the controls with the auditing process. We end this section by providing two mini cases.

Mini Cases

Mini Case 1

Company XYZ is a small company (20 people) with a manager and a system administrator reporting to him/her. The two prepare a security policy, according to which some operations will have to be authorized by the manager and executed by the system administrator, and the manager will know all the passwords and commands needed and how to access and modify the logs. What is wrong in this situation? What rule has been violated?

Mini Case 2

Company ABC is a part of an organization based in the United States. The company in the United States, as part of a recent decision to create a presence outside the United States, has bought the control of small companies based in India, Singapore, Taiwan and Malaysia. A part of the process for integrating the various parts is to create a common security policy by a committee that includes a member of their legal department (to verify the legal compliance). The company then plans to send managers from their headquarters (based in the United States) to each country to make sure the policy is implemented correctly. What is wrong in this planning?

4.2.4. Organizational Responsibility for Information Security Management

We discussed security policies, standards, guidelines, etc. Ideally, 'best practices' begin at the top and percolate down in the organization. The senior management team members of an organization are the 'strategists' with Vision' and long-term view. They exemplify their asset protection intent with the well-set policies directed toward this.

However, often, as it happens, too small a budget, too few personnel and too little consciousness of the management constitute approximately half of the obstacles for IT security according to a study of the META Group. It may also happen that the IT budgets invested in IT security go wrong in the long term. Given this, one of the important tasks for the top management in an organization is to make their employees aware of the IT security significance. This starts with the formation of 'security policies' as we see in this chapter. Security policies, standards and procedures stand in a certain hierarchical relationship in alliance with the organizations overall business goals. This is illustrated in the following figure.

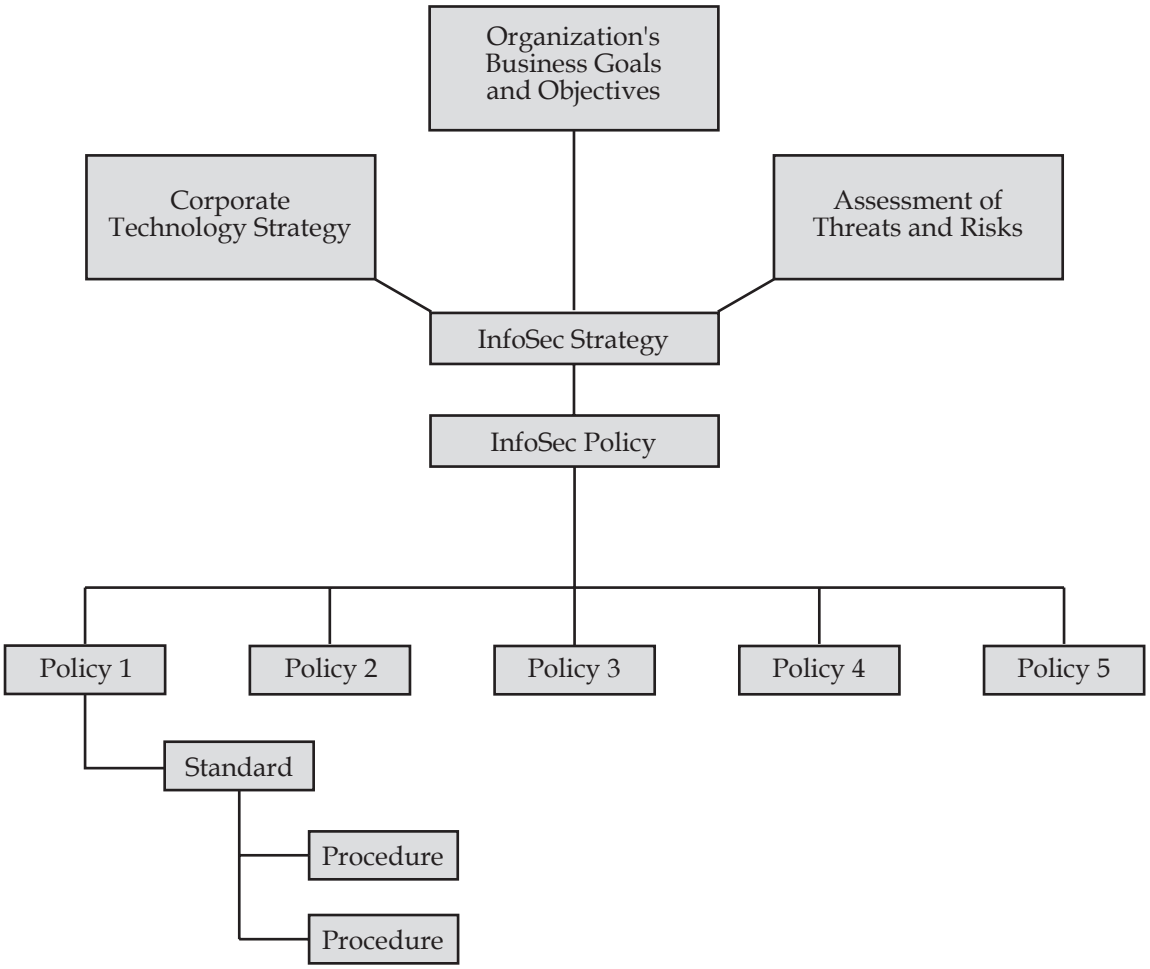


Fig: Hierarchy of Security Policies, Standards and Procedures

4.2.5. Information Security Awareness Scenario in Indian Organizations

Majority of the Indian software businesses are driven by multinationals located mainly in the United States. Today, the US InfoSec industry stands over USD 8.7 billion. In the present global

digital economy, information flows more often than not through the complex IT infrastructure present. To be efficient at managing, operating and protecting this IT infrastructure, there is a need for having a common set of guidelines for the use and access of information assets. Therefore, we discussed policies, guidelines and standards for information systems security.

In the global context for IS and the threats to IS, it is clear that many business processes do not work without reliable IT systems' confidentiality, and thus, integrity and availability of information are of high importance in today's business life. So, let us understand where do we stand on 'IT/ information security awareness' as far as the Indian scenario is concerned.

The complexity of security administration in managing large networks is, nowadays, a big issue. Although organizations know about the ever more frequent security attacks, they update their safety devices only when it is already too late. This can only be ascribed to attitude' and 'mindset' problems with respect to security. Although the scenario is progressively improving, awareness of Indian companies in the matter of information systems security still is far behind that of European countries and the United States. Although it is based on some past surveys, it is illustrated here only to drive home the point that heightening this awareness is important because India, among other countries in the South East Asian region, is now becoming one of the preferred off-shore locations (mainly owing to cost reasons and availability of English' speaking IT-trained manpower) for outsourcing businesses. The following figures show the status on 'security awareness' and 'security challenges' faced by most Indian organizations.

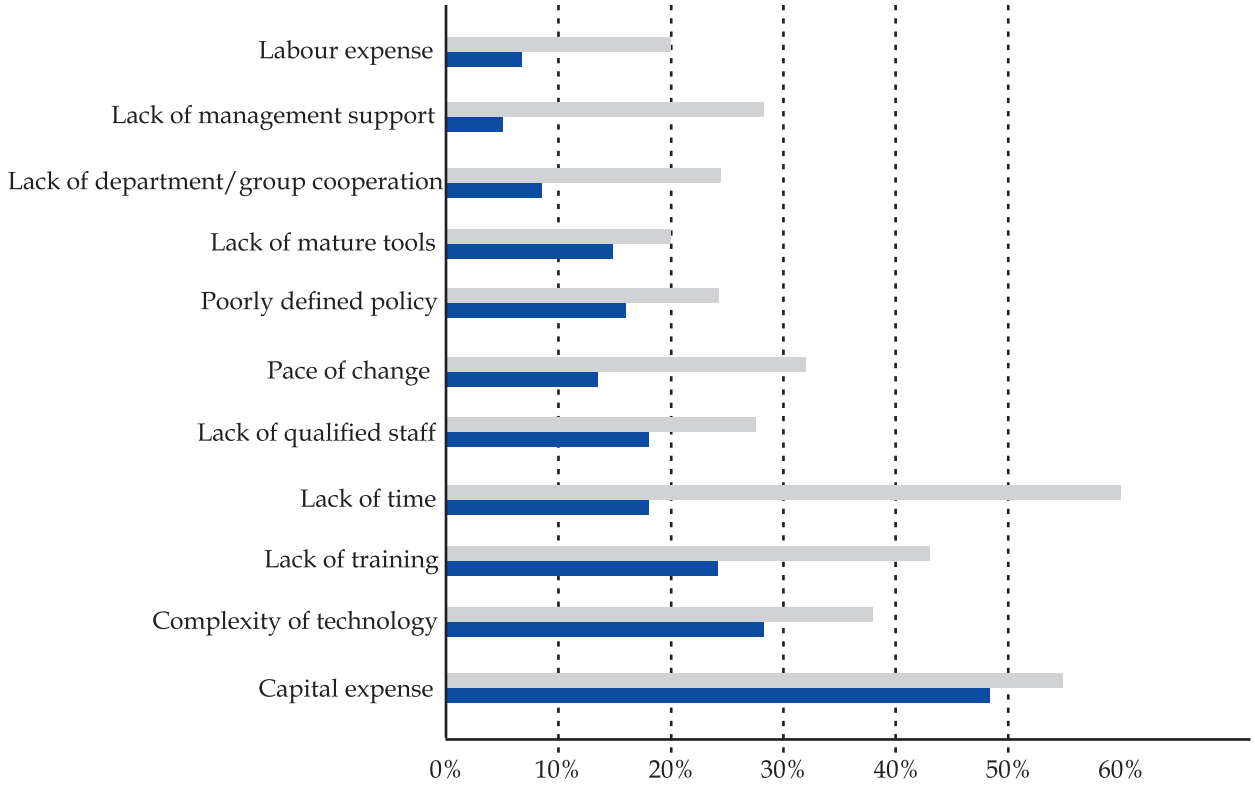


Fig. Barriers to Security

English is necessary as at present original works of science are in English. I believe that in two decades times original works of science will start coming out in our languages. Then we can move over like the Japanese. ***- Dr. A.P.J Abdul Kalam***

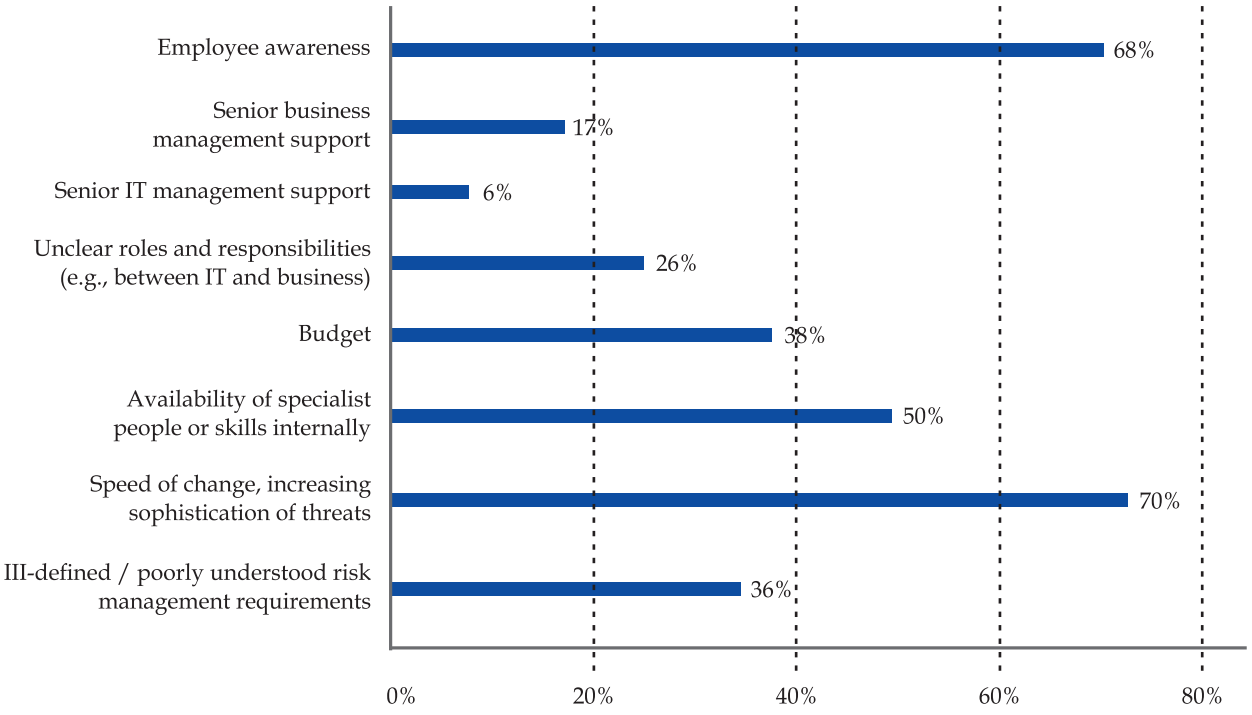


Fig. IT Security Challenges for Indian Organizations

Owing to factors such as globalization and reasons of regulatory nature, certain Indian companies are now more serious about information security. But the rest are complacent and need to do a lot more than just implementing solutions. International companies, seeking to outsource work to Indian firms, insist on security assurance/security certification and security governance. They insist on adherence to laws, standards and business practices prevalent in their respective countries. Not surprisingly, the top software services companies, IT-enabled services companies and BPO outfits are going in for security certifications such as BS 7799 or ISO 17799. Thus, regulatory requirements become one more driver for increased security awareness.

Truth does not pay homage to any society, ancient or modern. Society has to pay homage to Truth or die.
- Swami Vivekananda

अध्याय 5
Chapter 5

Cyber Hacking, Demystifying the Mysterious Business of Hacking and Getting More Serious about Hacking into Networks

5.1. Cyber Hacking

5.1.1. Hacking and Different Types of Hackers

5.1.1.1. Who are Hackers and What Drives Them?

Hacking involves finding out weaknesses in a computer or computer network and gaining unauthorized access to it from a remote station. One who does hacking is called a hacker. He may steal some data from the victim computer, alter its functioning or even take complete control of it. It needs no imagination that hackers can wreak havoc with the computers of their victims or the victims themselves, sitting thousands of miles away. The victim may be furious but there is little he can do to the hacker. We saw how the Americans and the Israelis sabotaged the Iranian uranium centrifuge plants with the Stuxnet.

According to the popular perception fostered by Hollywood, a hacker is usually a whiz kid who spends too much time with computers and suddenly finds himself submerged in the world of cyber security or criminal conspirators. On the other hand, he could also be a master criminal who wants to obtain huge amounts of money for him, or even worse, dominate the world. Computer programmers argue that someone breaking into computers must be called a cracker. But we would not go by that as most of the computer users use the words hacking and hackers in the sense we have mentioned above.

In real life, hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. In the early years, most hackers were indeed computer geeks—usually computer science students— and often fitted the profile of brilliant but crazy loners seeking to make a name for themselves. Breaking into something which is supposedly protected by some of the best brains in business, gives them a high. Adrian Lamo's specialty was breaking into the computer networks of top American companies. By 2001, when he was still only 20, Adrian told a 'Security Focus' reporter that his major problem was, "I'm running out of major US corporations." Many of them, however, have criminal proclivities and do it for ulterior motives of self or those who hire them.

One might not suspect that the art, or scourge, of computer hacking was created at one of the havens for technological excellence. True, at the famous MIT (Massachusetts Institute of Technology), a group of students had developed this technique and borrowed their name from the "hackers" of the late 1800s who found amusement in playing pranks with the then emerging telephone companies. Gaining their skills from hacking and cracking into primitive computers and exploiting the Arpanet (predecessor to the Internet), they eventually created a novelty that would become the fear of millions upon millions of Internet users in years to come.

One thing common to hackers in the early years was secrecy. No literature regarding hacking was available in the open. These computer whiz kids often learnt things by themselves. They could learn it because they were obsessed with computers. But they kept the knowledge to themselves or to like-minded people. That's how the subculture that has evolved around hackers is often referred to as the computer underground. This mold is breaking now because computer security experts do like to gain unauthorized access to computer and computer networks for good reasons, so that they may check how secure the system or the network is. Since they had to do this activity legitimately, they developed a proper science of it so that

others may also learn it and may become cyber security professionals. It has become possible for us to write a book of this type only because such legitimate professionals made the literature available in the public domain.

5.1.1.2. History of Hacking

The act of hacking had started out rather innocently, and was basically a method of trying to figure out how computer systems worked. The 1970s saw the rise in "phreaking," or phone hacking, headed by John Draper. This method allowed the user of a "blue box,", when used with a Captain Crunch whistle of 2600 Hz which accessed the AT&T long distance system, to make free long distance calls. Hackers initiated with accessing the free phone calls through a varied range of sources, thereby managing to circumvent into the nation's radio system and the phoning system resulting in a tremendous phone fraud nationwide.

Cell phone hacking has just recently surfaced and been made public ever since someone did some cellular phone hacking on Paris Hilton's cell phone. Unfortunately for her, all her celebrity friends and their phone numbers were also placed on the Internet—resulting in a barrage of calls to each of them. Mobile hacking allows a hacker to contact your cell phone, without your knowledge, and to download your addresses and other information you might have on your phone. Many hackers are not content to only get your information. Some will even change all your phone numbers! Be sure to keep a backup of your information somewhere. This particular technique is called Bluesnarfing.

After the age of "phreaking," computers became not only the target, but also the forum, for a growing hacker population to communicate. The creation of bulletin board systems (BBS) allowed this communication and the technological possibility of more serious government and credit card hacking became possible. At this time in the early 80's, hacking groups such as the Legion of Doom began to emerge in the United States, giving organization, and thus more power to hackers across the country. Once this happened, breaking into the computers became a commonplace activity, with its own groups and soon its own voice with the magazine called 2600, launched in 1984. The effects of computer hacking were serious. By 1986 the US government fully appreciated the danger that hackers represented to the national security. Accordingly, inevitably, the American Congress launched the Computer Fraud and Abuse Act that outlawed hacking. Over the years, there was a series of noticeable occurrences as the worst consequential effect of computer hacking on more high profile cases, such as the Morris Worm, responsible for infecting government and university systems, and the Mitnick case in 1995, which captured Kevin Mitnick, stealing as many as 20000 credit card numbers.

During the 1990's, when the use of the Internet widespread around the world, hackers multiplied, but it wasn't until the end of the decade that computer security became mainstream among the public. In 1999, security software became widely known by the public, and with the release of new Windows programs, which were littered with security weaknesses, they became successful because of sheer necessity. As the history of cyber warfare amply demonstrates, hacking has been growing both in scope and complexity, often beyond imagination.

5.1.1.3. Wearing Hats of Different Kinds

A "black hat hacker" is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

A "white hat hacker" breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement Some white hat hackers claim that they only should be called hackers, and that only black hats should be called crackers.

An ethical hacker is usually employed by an organization who trusts him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. The Certified Ethical Hacker is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council.) He is trained in how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a hacker.

A "grey hat hacker" is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.

The word "elite hacker" is used to describe the most skilled hacker. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

A "script kiddie (or skiddie)" is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept— hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature). - ,

A "blue hat hacker" is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed.

A "hacktivist" is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

5.1.1.4. Why You Need To Be Worried About Hacking?

"Aren't you a little paranoid about hacking?" is a question that experts are often asked. Take our word, they are not! We know that the hackers are out to get us. If only the Trojans had been as paranoid, they would have looked more carefully at the horse that they were given by the Greeks.

There are actually millions of people out on the Internet who want to break into the computers on our networks. When dealing with computer networks, a moderate amount of paranoia is a very healthy trait—the more you are concerned about possible risks, the more likely you'll be in a position to provide adequate protection for your network. As the saying goes, "Just because you're paranoid doesn't mean that they're not really out to get you."

As they say in the cyber security world, there are only two kinds of computer systems now: those that have been hacked and those that will be hacked. And just because people are computer savvy does not mean their data are safe. The website of online retailer Geeks.com featured the "hacker safe" notification from McAfee ScanAlert. Nevertheless, a hacker broke in and accessed customer credit card numbers and other personal information on its site. And in another really scary example, mortgage giant Fannie Mae in the USA narrowly avoided a software time-bomb set to destroy all data on its computers. Some disgruntled contractor who had been terminated embedded into the system a malicious code, tucked at the end of a legitimate software program scheduled to run each morning. It was set to go into effect (months after he was gone) on all 4,000 of the company's servers. It was only discovered by chance by another Fannie technician or the whole agency's database would have been wiped out

Overall, the Internet is an easy place to hide. Compromised computers around the world have helped to make hiding simple. It is easy to find the last IP address from where an attack was launched, but hackers hop from many unsecured systems to hide their location before they launch attacks. You might be thinking that hackers don't care about your computer, but they do. Hackers want access to your system for many different reasons. Over the past four years, most cyber attacks have been launched from computers within the United States. However, this doesn't mean that systems in the United States are the original source of the attack A hacker in Russia could actually use your computer to launch a denial of service (DoS) attack. To the entire world, it might even look as if you started the attack because the hacker has hidden his tracks so that only the last "hop" can be traced. If at all the police catch someone, it will be unfortunately you!

5.1.1.5. All That You Stand To Lose To The Hackers

In their white paper on cyber crime and cyber security, Bruce S. Schaeffer, Henfree Chan, Henry Chan and Susan Ogulnick have formulated what they call a "Chan Scale of Cyber In-Security", based on the potential harm that can be caused:

Chan - Low risk: Hacker has gained entry to system but minimally. Minor risk of business disruption, but access can aid attackers in information gathering and planning future attacks.

Chans - Medium Risk: Malware has been implanted in the company's network, which could cause malfunctions and mischief. There is a significant risk of a business disruption that could result in financial loss and/or damage of goodwill.

Chans - Medium-to-High Risk: Using sniffers or other equipment, hackers have obtained Personally Identifiable Information (PII) from point of sale (POS) systems. There is a significant risk of a business disruption that could create financial loss and/or damage of goodwill.

"Every action that helps us manifest our divine nature more and more is good; every action that retards it is evil."
- Swami Vivekananda

Chans - High Risk: Inside job: data stolen by disgruntled employee. There is a potential risk of business disruption, resulting in financial loss and damage of goodwill. PII may be taken, as well as company's confidential information and financial information.

Chans - Critical Risk: Hackers have gotten into the system and can access PII as well as the company's financial information and confidential information. There is a severe risk of business disruption, financial loss, damage of goodwill System, application, and database have been compromised.

The best way to establish the value of something is to evaluate the cost of a loss. Take a look at some different types of damages and consider the cost of each:

Lost Data: How important is the data on your corporate network? To answer this question, try to estimate what would happen if the data disappeared. Imagine that someone managed to break into your network and deleted all your accounting data, your customer list, and so on. Hopefully you have methods in place to restore lost data from a backup—no matter how you lose it But, for just a second, imagine that all your corporate data is gone and you have to reconstruct it Would your company still be in business if this happened to you tomorrow?

Confidential Data: If anyone were to break into your network and get access to confidential data—for example, the secret plans for the new unconventional energy source that you are developing— imagine what could happen. What would a hacker do with the data? Because you don't know, you have to assume the worst If the secret plans end up in the hands of a competitor, he or she may beat you to the market with a miracle machine, and the profits and the Nobel Prize in Physics go to that person instead of you. The damage may even be worse if the data that is stolen is your entire customer list, including complete contact and billing information.

Downtime: Have you ever called a company to order an item or to complain about something, and you were told, "I can't help you, the network is down" If so, you probably remember your reaction. The excuse sounded cheap, and you felt like taking your business somewhere else. However, network outages do happen, and often the best thing that employees can do is twiddle their thumbs and tell customers to call again later. Preventing intrusions from the Internet may cost a little bit of money, but the amount of money lost due to downtime caused by such an intrusion could cost a lot more.

Staff Time: Each time an attack on your network is successful, you must take time to fix the hole and to repair any damage. For example, if a virus infects the computers in your company, you may have to go to each computer to remove the virus and repair any damage. The time that you spend doing this adds up quickly, and— as the saying goes—time is money. Don't expect to fix a large-scale problem quickly; that is, unless you are in the information technology department of an organization that we know. After a recent virus outbreak, they solved the problem by erasing the hard drives of every single computer and reinstalling everything from scratch. When the employees came to work the next morning, they realized that all of their data was lost, and they had to start the arduous task of reconstructing it from scratch. The IT people were nowhere

to be found; for them the problem had been solved — the virus was gone. For everyone else the problem had just started.

Hijacked Computer: Imagine that someone broke into your computer and used it for his own purposes. By God, he could even be a terrorist and you could find yourself on the wrong side of the law for no fault of yours. If your computer is not used much anyway, this may not seem like a big deal. However, now imagine that the hacker uses your computer for illegitimate purposes. It will be very difficult for you to prove that you did not commit that terrorist act.

Reputation: Do you want to be the company that is mentioned in the local or national news as the latest victim of a computer attack? Imagine what this would do to your company's reputation The potential damage from such publicity has even caused some companies to sweep network intrusions under the table.

5.1.2. What Hacking Entails?

The majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws in software and operating systems. Software vulnerabilities account for the majority of successful attacks, simply because attackers are opportunistic—taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. Most software, including operating systems and applications, comes with installation scripts or installation programs. The goal of these installation programs is to; get the system's installed as quickly as possible, with the most useful functions enabled, with the least amount of work being performed by the administrator. To accomplish this goal, the scripts typically install more components than most users need. The vendor philosophy is that it is better to enable functions that are not needed, than to make the user install additional functions when they are needed. This approach, although convenient for the user, creates many of the most dangerous security vulnerabilities because users do not actively maintain and patch software components they don't use. Furthermore, many users fail to realize what is actually installed, leaving dangerous samples on a system simply because users do not know they are there. Those un-patched services provide paths for attackers to take over computers.

For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample programs or scripts. One of the most serious vulnerabilities with web servers is sample scripts; attackers use these scripts to compromise the system or gain information about it. In most cases, the system administrator whose system is compromised did not realize that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks.

The simplest means to gain access to a system is by simple file and printer sharing. This is used to allow others on say, a home local area network share files, printers, and internet connections. If

Since the cruel killing of cows and other animal have commenced, I have anxiety for the future generation.
- Lala Lajpat Rai

the computer has file and printer sharing enabled, this in fact allows these resources to be shared, and on offer, to the entire Internet! This is largely due to the fact that NetBIOS (Network Basic Input/Output System) was originally intended for use on local area networks (LAN's), where trusted sharing of resources made sense for many reasons. It was never intended to 'go global'. To penetrate, the hacker first searches using a NetBIOS scanner, for a system with sharing enabled. A program such as Netbrute, for example, by Raw Logic Software, is good enough. These programs can help the hacker, as well as the network administrator. For more comprehensive information, he could use a utility such as Languard Network Scanner. This returns a wealth of information such as domain names, login names, and more. Then the computer is his to explore.

5.2. Demystifying the Mysterious Business of Hacking

5.2.1. Tricks and Techniques Employed by Not-So-Serious Hackers

5.2.1.1. From Where do they get the Knowledge?

You can rest assured, becoming even a not-so-serious hacker is not easy. That too requires a level of knowledge of computing which most people do not have. There is considerable literature in the public domain on ethical hacking. Not much literature is available about black hat hacking though. The knowledge which black hat hackers have is either self-acquired or confined to their closed community. What we are trying to tell you that should you really want to become a hacker, lack of information would not come in your way. But almost all of it is of very high standard and lay men would not understand much from it. You have to have great knowledge of computers in the conventional manner before you could think of becoming a hacker. For basics you could read "How To Become A Hacker" from Eric S. Rymond, for example. On a higher level you could have Hack Attacks Encyclopedia by John Chirillo. Many of the authoritative texts on hacking are listed in the bibliography of this book. There are websites and magazines like 2600: The Hacker Quarterly (www.2600.com); (IN)SECURE Magazine (www.net-security.org/insecuremag.php); Hackin9 (http://hakin9.org); and PHRACK (www.phrack.org/archives) also. Even the Internet has much information. Most of them, however, will only offer you limited tutorials on how to hack (like the Hacker's Black book or the Happy Hacker book, which are outdated). Others will give you a useful insight on this world.

After some time, you will find Internet forums were people from around the world share their experiences. That comes close to the real McCoy but they are also of a very high standard. You have to reach their level of knowledge first to glean something useful from their discussions. The jargon used by a group of hackers is extremely confusing for any beginner. You could pick up some of the jargon from the Jargon File. This document is a glossary of hacker slang that has been collected since 1975, from the old days of the Arpanet (the precursor of the Internet). Many tools are available on the Internet also—the free utilities are not of much use; you will have to buy the useful ones. But once again, using them effectively requires great knowledge.

5.2.1.2. What Most of them Would Like to do and how would they do it?

Hacking into other people's email accounts is a very popular desire amongst would-be hackers. You could be a jealous lover who wants to know whether his beloved is cheating on him.

On a more responsible note, you could even be a police officer trying to read a terrorist's email. Unfortunately, there is no readymade software/ program that will hack Gmail just with a click of a button. It's quite possible that you have received spam offering a hacking guide for Hotmail or Gmail that will enable you to hack other people's Gmail or Hotmail account. Although it sounds tempting to have the power to know the private life of other persons, most of these guides and courses are nothing but scams that are looking for new victims. Had it been so easy to hack them, Hotmail and Gmail would have closed shop a long ago. Closely related to this is the business of password cracking—something which thieves and the police both need. Many programs are available for the job. John the Ripper is one such program. Rainbowcrack is a traditional password cracker that takes a long time. We shall talk about them in detail later.

Quite often they would use Google itself to hit the jackpot. Suppose a black hat hacker wants to access the email account of a certain victim. The first thing that he would do is to find out what is the secret question in the email account of their prey. Let's say that the secret question asks the name of the pet of the account owner. How can the hacker learn it? It is possible that this bit of information is buried somewhere in the Internet We will tell you how? Maybe the victim had gone into a forum on health of pets where veterinaries offer free advice and mentioned the name of his dog in one of his questions. Now you understand how you should be cautious in mentioning personal details on the Internet The hacker may use special characters that the common user doesn't use or doesn't even considered using. For example: +, /, and -. Each one of these characters is used for special purposes. For example, if you use the minus sign just before a certain word, Google will only show those searches where that word doesn't appear.

Another lovely thing a hacker would like to do is to break into your system. The most common technique used by hackers for this is called scanning. Hackers have created tools that scan computers for weak spots. It can be an operating system that hasn't been upgraded or a port in the computer that it is open without the knowledge of the user. Hackers use this "open window" to get inside your computer in order to do whatever they want to do. Some of these hacker tools are available on the Internet. IP Scanning simply pings a range of IP addresses to find which machines are alive. Another way that hackers can access your machine is through malware: programs designed to capture vital information from your computer, like login users and passwords. Malware could be hidden in a PowerPoint presentation sent by email or even in an innocent Instant Messenger message window. But the problem is getting that malware.

While hacking email accounts and getting into somebody's computer is the favorite dream of most would-be hackers, they know that those are criminal activities and could land them in trouble if they boasted about it to anyone. They would like to do something about which they could boast and get recognition for their skills in a circle much wider than their close friends. One way to achieve this is to get into and deface some well-known websites. The result is for the whole world to see. As you would read later in the book, Indian and Pakistani hackers have been defacing each other's websites since long. To accomplish this, the hackers must find out loopholes

in the designed sites and format programs to launch repeated attacks injecting the devastating programs to through these vulnerable points.

One of such tools would be the robot spider. These can be sent out and put on automatic and will look for ports of access into your computer. These spiders are running around all the time and some say that they may hit most computers that are online—up to 50 times a day. Other tools use email attachments. It has been estimated that as much as 65% of all email is spam. And as much as 1 in about 30 emails contains a dangerous virus, or some form of malware.

Some hackers want to launch DoS (Denial of Service) attacks on commercial websites or government websites. Coldlife 4.0, for example, is a tool for website hacking that falls in the category of flooder. This is a program that has been designed to overload the connection by certain mechanisms like a fast pinging that causes a sudden DoS attack.

Another popular desire is getting into networks—usually corporate networks. If someone wants to trespass into a building, he will look for the weakest points in the system. If you want to penetrate a building, you need to make some surveillance first. Learn the movements of the guards, find out what kind of equipment are they using and maybe make some small test to check how good the security is. The same thing applies to a hacker who wants to get into a network. He will need to make some surveillance first, looking for the weak spots. For doing this, there are a series of tools that a hacker can use, like network password hacking programs that have been developed by password hackers. But the most common tool is the port scanner. With a port scanner, a hacker can look for those entrances in the terminal that don't have adequate security. Once he has assured that it is vulnerable enough, he will use it for getting inside.

Many hackers, as you would learn from the companion volume 'Cyber Crimes: Preventive Measures and Cyber Forensics', are plain criminals, trying to make money. As you would have seen, one of the methods is called phishing. Phishing is a typical message that actually pretends to be sent by the business concerns and /or banks but a simple attempt to steal off the passwords and the other private information to steal money from someone's account.

5.2.2. Secrets of Serious Hackers No One Told You Before

5.2.2.1. Their Tools of the Trade

The real bad guys do all that we discussed above and much more. Hacking operating systems (OSs) is a preferred method of the bad guys. OSs comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them. Hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities.

Applications take a lot of hits by hackers. Programs such as email server software and Web applications often are beaten down. Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.

The first thing the hackers need is the right tools. They need a set of specific tools that they may call on for the task at hand. For example, to crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump. For port scanning, there is a general port scanner, like SuperScan. For an in-depth analysis of a Web application, a Web-application assessment tool such as Whisker or WebInspect would be required. For analyzing a network, you would need, for example, Ethereal. The following is a list of some of the famous commercial, freeware, and open-source tools used in the trade:

- Nmap
- EtherPeek
- SuperScan
- QualysGuard
- Weblnspect
- LC4 (formerly called L0phtcrack)
- LANguard Network Security Scanner
- Network Stumbler
- ToneLoc
- Internet Scanner
- Ethereal
- Nessus
- Nikto
- Kismet
- THC-Scan

5.2.2.2. The Methodology Of Hacking

Imagine that there is a black hat hacker and he is on a reconnaissance mission. How does he proceed? Remember that unlike what they show in the movies, hacking is a hell of a tedious Job demanding great dedication and perseverance. It does not happen in a few seconds with some clicks of the mouse. He would harness as much information as possible about the target organization and systems. He would start with a broad view and narrow his focus:

1. Footprinting is the act of gathering information about a computer system and the companies it belongs to. Footprinting is the first step hackers take in their hacking process. Footprinting is important because to hack a system the hacker must first know everything there is to know about it.
2. He would search the Internet for the organization's name, the computer and network system names, and the IP addresses: Google is a great place to start for this.

3. The hacker would start gathering information on the target's website. Things a hacker would look for are emails and names. This information could come in handy if the hacker was planning to attempt a social engineering attack (explained a little later) against the company.

4. Next the hacker would get the IP address of the website. Many services are available for this. For example, by going to httpy/www.selfseo.com/find_ip_address_of_a_website.php and inserting the web site URL, it will spit out its IP address. For example, the IP address of google.com is 64.233.187.99.

5. Then he would ping the server to see if it is up and running. Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss. There's no point in trying to hack an offline server. http://just-ping.com, for example, pings a website from 34 different locations in the world. Insert the website name or IP address and hit "Ping". If all packets went through, then the server is up.

6. Next the hacker would do a Whois lookup on the company website. He goes to, for example, http:// whois.domaintools.com and put in the target website. This gives a huge amount of information about the company. One can see the company emails, address, names, when the domain was created, when the domain expires, the domain name servers, and more!

7. For example the hacker could search "site:www.the-target-site.com email". This search could list several emails that are published on the website. Another search one could do in Google is "inurl:robots.txt this would look for a page called robots.txt. If a site has the file "robots.txt", it displays all the directories and pages on the website that they wish to keep anonymous from the search engine spiders. Internet bots, also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. The largest use of bots is in web spidering, in which an automated script fetches, analyzes and files information from web servers. A web crawler or web spider is a computer program that browses the World Wide Web in a methodical, automated manner or in an orderly fashion. Web spiders can also be used with malicious intent, although each server spidered may have a file called robots.txt which may contain rules for the bot to follow. Web site owners use the /robots.txt file to give instructions about their site to web robots; this is called The Robots Exclusion Protocol. Occasionally, we repeat, occasionally; the hacker might come across some valuable information that was meant to be kept private in that file. One has to persevere.

8. Then he would narrow his scope, targeting the specific systems he is checking out: Whether physical-security structures or Web applications, a casual assessment can turn up much information about your systems.

9. He would further narrow his focus with a more critical eye. He would perform actual scans and other detailed tests on your systems.

10. Finally, he would go in for the kill and perform the attacks.

Smart hackers want to remain as low-key as possible. Covering their tracks is a priority and many times, their success depends on them remaining unnoticed. They want to avoid raising suspicion so they can come back and access the systems anytime in the future. Hackers often remain anonymous by using one of the following resources:

- Borrowed or stolen dial-up and VPN accounts from friends or previous employers
- Public computers at libraries, schools, or kiosks at the local mall
- Open wireless networks
- Internet proxy servers or anonymizer services
- Anonymous or disposable email accounts from free email services
- Open email relays
- Unsecured computers — also called zombies or bots — at other organizations
- Workstations or servers on the victim's own network

They scan and document specific hosts that are accessible from the internet For this, they start by pinging either specific host names or IP addresses with a typical third-party utility that allows him to ping multiple addresses at the same time, such as SuperScan version 3 (www.foundstone.com/ us/resources/proddesc/superscan3.htm) and NetScanTools Pro (www. netscantools.com) for windows and fping (www.fping.com) for UNIX.

They scan for open ports by using network scanning tools like SuperScan or Nmap (http://nmap.org). They listen to network traffic with a network analyzer, such as OmniPeek (www.wildpackets.com) and Wireshark (www.wireshark.com). From this they can get information like protocols in use, such as IP, IPX, and NetBIOS; services running on the hosts, such as email, Web servers, and database applications; available remote access services, such as Windows Terminal Services/Remote Desktop, VNC, and Secure Shell (SSH); and VPN services, such as PPTP, SSL, and IPSec etc. and a lot more.

If they detect a Web server running on the system that they are targeting, they can use an enumeration utility (such as DumpSec at www.systemtools.com/somarsoft/?somarsoft.com) to extract users, groups, and file and share permissions directly from windows.

One of the good hacking tools is a vulnerability scanner called QualysGuard Suite by Qualys (www.quafys.com). It's both a port scanner and vulnerability assessment tool. Just browse to the

Qualys Web site, log in to your account, and enter the IP address of the systems you want to test. Metasploit (www.metasploit.com/ framework) is great for exploiting many of the vulnerabilities they find and allows them to obtain complete system penetration.

Then they can use identified critical security holes to do the following:

- Gain further information about the host and its data.
- Obtain a remote command prompt.
- Start or stop certain services or applications.
- Access other systems.
- Disable logging or other security controls.
- Capture screen shots.
- Access sensitive files.
- Send an email as the administrator.
- Perform SQL injection attacks.
- Launch another type of DoS attack.
- Upload a file proving your victory.

Hackers also employ social engineering to gain information they couldn't access otherwise. For example, pretending to be support personnel, they claim that they need to install a patch or new version of software on a user's computer, talk the user into downloading the software, and obtain remote control of the system. Or pretending to be vendors, they claim to need to update the organization's accounting package or phone system, ask for the administrator password, and obtain full access. Technology can make things easier—and more fun—for the social engineer. Often, a malicious request for information comes from a computer or other electronic entity the victims think they can identify. But spoofing a computer name, an email address, a fax number, or a network address is easy. Hackers can deceive through technology by sending email that asks victims for critical information. Such an email usually provides a link that directs victims to a professional- and legitimate-looking website that "updates" such account information as user IDs, passwords, and Social Security numbers. In some well-publicized incidents, hackers emailed their victims a patch purporting to come from Microsoft or another well-known vendor. Users think it looks like a duck and it quacks like a duck—but it's not Donald Duck! The message is actually from a hacker wanting the user to install the "patch," which installs a Trojan-Horse keylogger or creates a backdoor into computers and networks. Hackers use these backdoors to hack into the organization's systems or use the victims' computers (known as zombies) as launching pads to attack another system. Even viruses and worms can use social engineering. For instance, the LoveBug worm told users they had a secret admirer. When the victims opened the email, it was too late. Their computers were infected, and perhaps worse, they didn't have a secret admirer.

Password Hacking

Password hacking is one of the most common and enjoyable ways through which hackers obtain unauthorized computer or network access. It fuels their sense of exploration and desire to figure out things. Although strong passwords—ideally, longer and stronger passphrases that are difficult to crack (or guess)—are easy to create and maintain, network administrators and users often neglect this. Therefore, passwords are one of the weakest links in the information security chain. To obtain passwords from across a network, attackers can use remote cracking utilities, keyloggers, or network analyzers. There are many approaches to password cracking.

Dictionary attacks quickly compare a set of known dictionary-type words—including many common passwords—against a password database. Strong passwords usually aren't vulnerable to this kind of attack. Brutus (http://www.hoobie.net/brutus/) is a very common password cracker of this type. Dictionary attacks are very simple to prevent. Don't use a password that is in the dictionary. Some people may think that if they use a word from the dictionary but replace most of the letters with a number, then they are safe. They are not. There are 1337 speak dictionary's out there too. Basically what 1337 speak is, is changing a word like "animal" to 4nlm4l. For a secure password, we would recommend using a phrase such as "doyoulikecheese?88".Creating a phrase for your password is your best option for staying secure.

Brute-force attacks can crack practically any password, given sufficient time. Brute-force attacks try every combination of numbers, letters, and special characters until the password is discovered. Brute-force attacks can take a long or very long time. The speed is determined by the speed of the computer running the cracking program and the complexity of the password. Many password-cracking utilities let you specify such testing criteria as the character sets, password length to try, and known characters (for a "mask" attack). One such software is Proactive Password Auditor which ethical hackers use to identify and close security holes in their networks. Brute-force attacks may be prevented by creating a very long password and using many numbers and odd characters. The longer the password the longer it takes for the hacker to crack your password. If after a few days the hacker hasn't been able to crack your password through a brute-force attack, then he is very likely to just give up.

Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power. Some of the popular password-cracking software include:

- Cain & Abel (www.oxid.it/cain.html)
- chknull (www.phreak.org/archives/exploits/novell)
- Elcomsoft Distributed Password Recovery (vvww.elcomsoft.com/edpr.html)
- Elcomsoft System Recovery (www.elcomsoftconVesr.html)
- John the Ripper (www.openwall.com/)ohn)
- ophcrack (http://ophcrack.sourceforge.net)

- Pandora (www.nmrc.org/project/pandora)
- Proactive Password Auditor (www.elcomsofLcom/ppa.html)
- Proactive System Password Recovery (www.elcomsoft.com/ pspr.html)
- pwdump3 (www.openwall.com/passwords/dl/pwdump/ pwdump3v2.zip)
- RainbowCrack (http://project-rainbowcrack.com)

How do they work? To understand this you will have to understand something basic. A password hash is a password that has gone through a mathematical algorithm that transformed it into something absolutely foreign. A hash is a one way encryption so once a password is hashed there is no way to get the original string from the hashed string. A very common hashing algorithm used as security to store passwords in website databases is MD5. The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. An MD5 hash is typically expressed as a hexadecimal number, 32 digits long. MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact. For example, file servers often provide a pre-computed MD5 (known as Md5sum) checksum for the files, so that a user can compare the checksum of the downloaded file to it. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264.

Let's say you are registering for a website. You put in a username and password. Now when you submit, your password goes through the MD5 algorithm and the outcome hash is stored in a database. Now since you can't get the password from the hash, you may be wondering how they know if your password is right when you login Well when you login and submit your username and password, a script takes your password and runs it through the MD5 algorithm. The outcome hash is compared to the hash stored in the database. If they are the same, you are admitted.

If we were to run the word "cheese" through the MD5 algorithm, the outcome would be fea0flf6fede90bd0a925b4194deacll.

Password-cracking utilities take a set of known passwords and run them through a password-hashing algorithm. The resulting encrypted hashes are then compared at lightning speed to the password hashes extracted from the original password database. When a match is found between the newly generated hash and the hash in the original database, the password has been cracked.

In Rainbow attacks, a Rainbow table is a huge pre-computed list of hash values for every possible combination of characters. Having huge tables of every possible character combination hashed is a much better alternative to brute-force cracking. Once the rainbow tables are created, cracking the password is a hundred times faster than brute-forcing it Password cracking speed is

increased in a rainbow attack because the hashes are pre-calculated and thus, they don't have to be generated individually on the fly as they are with dictionary and brute-force cracking methods. A text file containing all the possible passwords would require millions of terabytes of storage space. These storage requirements require dictionary and brute-force password-cracking programs to form the password combinations on the fly, instead of reading all possible combinations from a text file. That's why rainbow attacks are more effective at cracking passwords than dictionary and brute-force attacks. If you have a good set of rainbow tables, such as those offered via the ophcrack site and Project RainbowCrack (http.V/project-rainbowcrack.com), you can crack passwords in seconds, minutes, or hours versus the days, weeks, or even years required by dictionary and brute-force methods. That is why there aren't many of these tables available. You can avoid rainbow table cracking by simply making your password extremely long. Creating tables for passwords that are long takes a very long time and a lot of resources.

Cracking Password-Protected Files: Most password-protected files can be cracked in seconds or minutes, using a password-cracking tool available from Elcomsoft called Advanced Archive Password Recovery (www.elcomsoft.com/archpr.html).

5.3. Getting More Serious about Hacking into Networks

5.3.1. Basic Principles of Hacking Networks

Network infrastructure vulnerabilities are the foundation for all technical security issues in your information systems. These lower-level vulnerabilities affect everything running on your network. That's why you need to test for them and eliminate them whenever possible. To have secure operating systems and applications, you need to have a secure network. Devices such as routers, firewalls, and even generic hosts (including servers and workstations) are potential targets. There are thousands of possible network vulnerabilities, equally as many tools, and even more testing techniques. You can eliminate many well-known, network-related vulnerabilities by simply patching your network hosts with the latest vendor software and firmware updates. The better you understand network protocols, the easier network vulnerability testing becomes because network protocols are the foundation for most information security concepts.

Ethical hackers and network security professionals know all this. They use this knowledge to protect their networks. Hackers use it to attack the networks. An attack typically goes through several steps or phases. In each phase, some attack actions will be carried out by the hacker, and these attack actions will typically involve the use of one or more hacking techniques. The hacking techniques involved in different attack phases could be different. Moreover, an attack or hacking (software) tool may cover several phases of an attack and involve multiple hacking techniques. No matter how to hack or attack a network, the attacker always takes certain procedures to accomplish his objectives. In general, these procedures fall in one of the following steps. These steps can serve as a procedural classification of hacking techniques because the hacking techniques used in each step are for the same purpose and share many common characteristics. To understand the steps better think of the target as a famous company making some sensitive defense equipments and which holds many trade secrets. Naturally, others including their competitors would desire to

steal their secrets. They may employ a hacker to do the honors so that even if the hacker is caught, no blame comes on them. Or he could be working independently also hoping to sell his loot to the highest bidder later.

- **Reconnaissance:** Reconnaissance is to gather information of the target system or network. The information of interest may include host names, host addresses, host owners, host machine types, host operating systems, network owners, network configurations, hosts in the networks, list of users, etc. We have discussed this earlier.
- **Probe:** Probe is to detect the weaknesses of the target system in order to deploy the hacking tools. After gathering enough information of the target, the hacker begins to probe the perimeter of the system for potential weaknesses. He can utilize remote exploit tools, which enable the hacker to conduct security surveys and automatically collect and report security-related vulnerabilities of remote hosts and networks. Using these hacking tools, the hacker can find out the remote services the target is providing, such as WWW, FTP, SMTP, finger, X server, etc., by scanning the hosts of the target network. In addition, the hacker can obtain such information as machine names, software names and version numbers. Then, he can refer to the known vulnerabilities of the detected services for further exploitation.
- **Toehold:** Gaining a toehold is to exploit security weaknesses and gain entry into the system. Once a vulnerability is found, the hacker will first exploit this vulnerability to build a connection (or session) between his machine and the target host, and then remotely execute hostile commands on the target. (For example, the hacker can generate an X terminal emulation on his own display.) In this way, a toehold into the target network has been established and the hacker can go further to compromise the system. Gaining entry into the system, the hacker can also search for more critical system information. If the current user identification (UID) is for a privileged user, the hacker will jump to the stealth step; otherwise, he will get into the advancement phase.
- **Advancement:** Advancement is to advance from an unprivileged account to a privileged one. In this step, the hacker uses local exploit tools to obtain additional information of the target, such as configuration errors and known vulnerabilities of the operating system. Once finding a local vulnerability, the hacker can advance from an unprivileged UID to a root UID. Then, with the highest level of privileges, the hacker can fully control the target system, steal sensitive data, maliciously modify files, and even delete the entire file system.
- **Stealth:** Stealth is to hide the penetration tracks. During the probing phase, the intrusion actions are likely to be logged by intrusion detection systems, and during the phases of toehold and advancement, the hacker may leave his activities in the system log. Hence, in order to hide, the hacker will access the local log files and modify the corresponding log entries to remove the traces and avoid detection. He may further replace the system binary code with a malicious version in order to ensure future un-logged and undetected access to the compromised system.

- **Listening Post:** Listening post is to install backdoors to establish a listening post. In this step, the hacker inserts some malicious programs into the system, such as a stealth tool, a backdoor tool, and a sniffer. These programs ensure that his future activities will not be logged. They report false information on files, processes, and the status of the network interface to the administrators. They also allow the hacker to access the compromised system through the backdoor. With the sniffer tool, the hacker can capture the traffic on the network interfaces. By logging the interesting network traffic, the hacker can better monitor and control the compromised system.
- **Takeover:** Takeover is to expand control (or infection) from a single host to other hosts of the network. From the listening post, the hacker can sniff a lot of important information about other hosts of the network, such as user names and passwords. The hacker can also obtain information through several other ways. For example, he can check some specific configuration files (e.g., /.rhosts) of the compromised host and find mutually trusted hosts. With these information, the hacker can retake the previous steps to break into other hosts. In this way, he can expand his control to the whole network.

5.3.2. Tools in the Hacker's Arsenal

We have discussed them briefly earlier. Now we will discuss them in a little more detail so that the subject is demystified further. The hackers need scanners, analyzers, and vulnerability assessment tools. The hackers do not invent tools. The tools are there. May be they were developed with some different purpose in mind; the hacker has to learn how to use them for his purposes. Just keep in mind that he would need more than one tool, and that no tool does everything he needs. And also remember that they are complex tools. It takes considerable knowledge to even use them properly. Merely purchasing a tool would not make you Into a hacker. You have got to learn to exploit them properly.

Once inside the system, he tries to advance from an unprivileged account to a privileged account In this step, he can first find some system files containing the information of privileged accounts, and then use password crackers to get the name-password pairs. He can also exploit the system bugs to advance his privileges. Now the system is under control. The hacker hurries to hide his traces before the administrators find him. So he will use stealth and backdoor tools to remove his traces while continuing his access to the system. To keep monitoring the hacked system, the hacker establishes a listening post He uses sniffers and backdoor tools to watch system activities and report crucial information, so that he can fully control the compromised system and prepare for further attacks. Finally, the hacker expands his control from a single host to other hosts in the network. The previous tools will be used again.

5.3.2.1. Scanners and Analyzers

A scanner is a tool to obtain information about a host or a network. It is developed to probe the networks and report security related information. Serving for different purposes, a scanner is used by both security administrators for securing networks and systems, and hackers for breaking into. A port scanner shows you what's what on your network. A software tool that scans the network

to see what's alive and working, port scanners provide basic views of how the network is laid out. They can help identify unauthorized hosts or applications and network host configuration errors that can cause serious security vulnerabilities.

The ports represent potential communication channels. Mapping their existence facilitates the exchange of information with the host, and thus it is quite useful for anyone wishing to explore their networked environment, including hackers. Despite what you have heard from the media, the Internet is NOT exclusively reliant on TCP port 80, used by hypertext transfer protocol (HTTP). Anyone who relies exclusively on the WWW for information gathering is likely to gain the same level of proficiency as your average casual surfer.

The big-picture view from port scanners often uncovers security issues that might otherwise go unnoticed. Port scanners are easy to use and can test systems regardless of what operating systems and applications they're running. The tests are usually performed relatively quickly without having to touch individual network hosts, which would be a real pain otherwise.

Scanners can be broken down into two categories: network auditing tools and host-based auditing tools. Network auditing tools are used to scan remote hosts. For example, NMAP is a free open source utility for network exploration and security auditing. It can rapidly scan large networks and single hosts. NMAP uses raw IP packets to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, etc. Host-based auditing tools, working in a local system, are used to scan a local host and report its security vulnerabilities. For example, the COPS package can help identify file permission problems, easy-to-guess passwords, known vulnerable services and improperly configured services. The following scanners have been found to be good for port scanning and network testing:

- **SuperScan** (www.foundstone.com/us/resources/proddesc/ superscan.htm) for ping sweeps and port scanning.
- **Essential NetTools** (www.tamos.com/products/nettools) for a wide variety of network scanning functionality.
- **NetScanTools Pro** (www.netscantools.com) for dozens of network security assessment functions, including ping sweeps, port scanning, and SMTP relay testing.
- **Getif** (www.wtcs.org/snmp4tpc/getif.htm) for SNMP enumeration.
- **Nmap** (www.insecure.org/nmap) or NMapWin (http:// sourceforge.nev/projects/nmapwin), the happy-clicky-GUI frontend to Nmap—for host-port probing and operating system fingerprinting.

A network analyzer is a tool that allows you to look into a network and analyze data going across the wire for network optimization, security, and/or troubleshooting purposes. Network analyzers are often generically referred to as sniffers, though that's actually the name and trademark of a specific product from Network Associates, Sniffer (the original commercial network analysis

tool). A network analyzer is handy for sniffing packets off the wire. A network analyzer is simply software running on a computer with a network card. It works by placing the network card in promiscuous mode, which enables the card to see all the traffic on the network, even traffic not destined for the network analyzer's host. We have discussed the promiscuous mode a little later in detail. The hacker might need to let the network analyzer run for quite a while— several hours to several days, depending on what you're looking for. The network analyzer performs, among others, the following functions:

- Captures all network traffic.
- Interprets or decodes what is found into a human-readable format.
- View anomalous network traffic and even track down an hacker.
- Track and isolate malicious network usage.

Some of the useful network analyzer programs are :

- **Cain & Abel** (www.oxid.it/cain.html) for network analysis and ARP poisoning
- **WildPackets' OmniPeek** (www.wildpackets.com/products/ distributed_network_analysis/ omnipeek_network_analyzer) for network analysis.
- **TamoSoft's CommView** (www.tamos.com/products/ commview) is a low-cost, Windows-based alternative.
- **Wireshark** (www.wireshark.org), formerly known as Ethereal, is not as user-friendly as most of the commercial products, but it is very powerful if you're willing to learn its ins and outs. Wireshark is available for both Windows and OS X.
- **ettercap** (http://ettercap.sourceforge.net) is another powerful (and free) utility for performing network analysis and much more on Windows, Linux, and other operating systems.

Incidentally, the same tools can be used to detect hacking in progress also. A network analyzer is also a good tool for detecting systems infected with malware, such as a virus or Trojan horse. Looking at your network statistics, such as bytes per second, network utilization, and inbound/ outbound packet counts, is also a good way to determine whether something fishy is going on. A few countermeasures can help prevent someone from using an unauthorized network analyzer, although there's no way to prevent it completely. You can use a network- or host-based utility to determine whether someone is running an unauthorized network analyzer on your network. Some of these are:

- **Sniffdet** (http://sniffdet.sourceforge.net) for UNIX-based systems
- **romiscDetect** (http://ntsecurity.nu/toolbox/promiscdetect) for Windows

These tools enable you to monitor the network for Ethernet cards that are running in promiscuous mode. You simply load the programs on your computer, and the programs alert you if they see promiscuous behaviors on the network (Sniffdet) or local system (PromiscDetect).

5.3.2.2. Vulnerability Assessment Tools

These vulnerability assessment tools allow one to test the network hosts for various known vulnerabilities as well as potential configuration issues that could lead to security exploits:

- **GFI LAN guard** (www.gfi.com/lannetscan) for port scanning and vulnerability testing
- **Nessus** (www.nessus.org), a free all-in-one tool for ping sweeps, port scanning, and vulnerability testing.
- **QualysGuard** (www.quafys.com), a great all-in-one tool for in-depth vulnerability testing

The trick to assessing overall network security is interpreting the results he gets from a port scan. He can get false positives on open ports, and he might have to dig deeper. For example, UDP scans— like the protocol itself— are less reliable than TCP scans and often produce false positives because many applications don't know how to respond to random incoming UDP requests. A feature-rich scanner often can identify ports and see what's running in one step. Port scans can take a good bit of time. The length of time depends on the number of hosts you have, the number of ports he scans, the tools he uses, the processing power of his test system, and the speed of his network links.

An important tenet to remember is that he needs to scan more than just the important hosts. He would leave no stone unturned. These other systems often bite you if you ignore them. Also, he would perform the same tests with different utilities to see whether he gets different results. Not all tools find the same open ports and vulnerabilities. If his results don't match after he runs the tests using different tools, he might want to explore the issue further. If something doesn't look right—such as a strange set of open ports—it probably isn't. He would test again; if he is in doubt, he would use another tool for a different perspective. He would like to scan all 65,535 TCP ports on each network host that his scanner finds. The commonly hacked ports are enumerated below.

Port Number	Service	Protocol(s)
7	Echo	TCP.UDP
19	Chargen	TCP, UDP
20	FTP data	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
37	Daytime	TCP, UDP
53	DNS	UDP
69	TFTP	UDP
79	Finger	TCP, UDP
80	HTTP	TCP

110	POP3	TCP
111	SUN RPC	TCP, UDP
135	RPC/DCE	TCP, UDP
137, 138, 139, 445	NetBIOS over TCP/IP	TCP, UDP
161	SNMP	TCP, UDP
443	HTTPS	TCP
512, 513, 514	Berkeley r-services and r-commands (such as rsh, rexec, and rlogin)	TCP
1433 (ms-sql-s)	Microsoft SQL Server TCP, UDP	
1434 (ms-sql-m)	Microsoft SQL Monitor TCP, UDP	
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal	
Server	TCP	
5631, 5632	pcAnywhere	TCP
8080	HTTP proxy	TCP

5.3.2.3. Sniffers and Snoopers

A sniffer monitors and logs network data. The network traffic that passes through a host's network interface usually contains user name-password pairs as well as other system information that would be useful to a hacker. In a network where data is transmitted without encryption, a hacker with physical access to the network can plug in a sniffer to monitor the network traffic and obtain necessary information to access other hosts in the network. A snooper, also known as spyware, monitors a user's activities by snooping on a terminal emulator session, monitoring process memory, and logging a user's keystrokes. By watching the user's actions, an hacker can obtain useful information to attack other users on the computer or even other systems in the network.

5.3.2.4. Spoofing Tools

In a network, a data packet always contains the source address field, which can expose the source of the hacker if he sends malicious packets. Hence, in order to hide and avoid detections, the hacker uses spoofing tools to forge another source address that is usually the address of another host or a nonexistent address. The spoofed address can be an IP address or a physical address, depending on the type of the network. Another usage of spoofing tools is to gain access to a network from outside. If the firewall of the target network is not configured to filter out incoming packets with source addresses belonging to the local domain, it is possible for an hacker to inject packets with spoofed inner addresses through the firewall.

Trojan Horse

A Trojan Horse in a computer system is defined as a malicious, security-breaking program, which is a piece of executable code hiding in a normal program. When the normal program is opened or executed, the hidden code will perform some malicious actions silently, such as deleting critical system files. The Trojan Horse is spread in a disguised way. It presents itself as a game, a web page, or a script that attracts people. It may come from an email with your friend as the sender or an online advertisement But if the receiver opens it, the malicious code will commit the unsolicited actions.

Password Crackers

As discussed earlier, a password cracker is to find a user's password. It is used by both computer crackers and system administrators for recovering unknown or lost passwords.

5.3.2.5. Denial of Service Tools

A DoS (Denial-of-Service) tool is used by an attacker to prevent legitimate users from using their subscribed services. DoS attacks aim at a variety of services and accomplish the objective through a variety of methods. A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are thoseof the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker.

Attackers can flood the target network, thereby throttling legitimate network traffic; can disrupt connections between two machines, thereby denying access to the service; can prevent a particular individual from accessing the service; and can disrupt the service to a specific system or person. Different from inappropriate use of resources, DoS tools explicitly and intentionally generate attack packets or disrupt the connections. For example, they can consume scarce or non-renewable resources with a large number of ICMP echo packets, break network connectivity with SYN flooding, alter network configuration by changing the routing information, or even physically destroy network components.

Denial of service (DoS) attack is among the common hacker attacks. A hacker initiates so many invalid requests to a network host that the host uses all its resources responding to the invalid requests and ignores the legitimate requests. DoS attacks against network and hosts can also cause systems to crash, and data to be lost Some common DoS attacks that target an individual computer or network device are:

- **SYN floods:** In this he attacker floods a host with TCP SYN packets. Normally when a client

attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:

1. The client requests a connection by sending a SYN (synchronize) message to the server.
2. The server acknowledges this request by sending SYN-ACK back to the client.
3. The client responds with an ACK, and the connection is established.

This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol. A SYN flood attack works by not responding to the server with the expected ACK code. The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. When a legitimate user tries to connect but the server refuses to open a connection resulting in a denial of service.

- **Ping of Death:** In this, the attacker sends IP packets that exceed the maximum length of 65,535 bytes, which can ultimately crash the TCP/IP stack on many operating systems.
- **WinNuke:** This attack can disable networking on older Windows 95 and Windows NT computers.

There are a wide variety of DDoS (distributed denial of service) attacks. There are, however, two main classes of DDoS attacks:

- Bandwidth depletion attacks
- Resource depletion attacks

A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. A resource depletion attack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service.

Bandwidth depletion attacks can be further characterized as flood attacks and amplification attacks.

A flood attack involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, preventing access by legitimate users. Flood attacks have been launched using both UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) packets. In a UDP Flood attack, a large number of UDP packets are sent to either random or specified ports on the victim system. The victim system tries to process the incoming data to determine which applications have requested data. If the victim system is not running any applications on the targeted port, it will send out an ICMP packet to the sending system indicating a "destination port unreachable'' message. Often, the attacking DDoS tool will also spoof the source IP address of the attacking packets. This helps hide the identity of the secondary victims since return packets from the victim system are not sent back to the zombies,

but to the spoofed addresses. UDP flood attacks may also fill the bandwidth of connections located around the victim system. This often impacts systems located near the victim.

An ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets ("ping") to the victim system. These packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network connection. During this attack, the source IP address of the ICMP packet may also be spoofed.

An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate the packet and send it to all the IP addresses within the broadcast address range. In this attack, the broadcast IP address is used to amplify and reflect the attack traffic, and thus reduce the victim system's bandwidth. The attacker can send the broadcast message directly, or use the agents to send the broadcast message to increase the volume of attacking traffic. If the attacker decides to send the broadcast message directly, this attack provides the attacker with the ability to use the systems within the broadcast network as zombies without needing to infiltrate them or install any agent software.

A DDoS Smurf attack is an example of an amplification attack where the attacker sends packets to a network amplifier (a system supporting broadcast addressing), with the return address spoofed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTS, which are packets (similar to a "ping") that request the receiver to generate an ICMP ECHO REPLY packet. The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IP address. This type of attack amplifies the original packet tens or hundreds of times.

Another example is the DDoS Fraggle attack, where the attacker sends packets to a network amplifier, using UDP ECHO packets.

DDoS resource depletion attacks involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users.

Protocol Exploit Attacks; We give two examples, one misusing the TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH+ACK protocol. In a DDoS TCP SYN attack, the attacker instructs the zombies to send bogus TCP SYN requests to a victim server in order to tie up the server's processor resources, and hence prevent the server from responding to legitimate requests. In a PUSH + ACK attack, the attacking agents send TCP packets with the PUSH and ACK bits set to one. These triggers in the TCP packet header instruct the victim system to unload all data in the TCP buffer (regardless of whether or not the buffer is full) and send an acknowledgement when complete. If this process is repeated with multiple agents, the receiving system cannot process the large volume of incoming packets and the victim system will crash.

Malformed Packet attacks: A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it.

Trojan Horse programs are installed on a victim's system by the attacker and allow the attacker to gain control of a user's computer without the user knowing. In the case of a DDoS attack tool setup, Trojan horse programs already installed on a victim system might be used by the attacker to gain access to a secondary victim's system allowing the attacker to install the DDoS agent code. Passive methods typically involve the attacker sharing corrupt files or building websites that take advantage of known vulnerabilities in a secondary victim's web browser. A corrupted file has malicious code embedded within it. When the victim system tries to view or execute this file, it will become infected with the malicious code.

Another passive DDoS agent installation technique uses a bugged website. A vulnerability found on web browsers allows the attacker to create websites with code or commands to trap a victim. When the victim's Web browser views the webpage or tries to access content, the webpage indirectly downloads or installs malicious code (e.g., a DDoS agent).

5.3.2.6. Countermeasures To DDoS Attacks

The countermeasures proposed for preventing a DDoS attack are currently partial solutions at best. There is currently no comprehensive method to protect against all known forms of DDoS attacks. There are three categories of DDoS countermeasures.

1. Preventing the setup of the DDoS attack network, including preventing secondary victims, detecting and neutralizing handlers.
2. Dealing with a DDoS attack while it is in progress, including detecting or preventing, mitigating or stopping, and deflecting the attack.
3. The post-attack category involving network forensics.

To detect or prevent a potential DDoS attack that is being launched, egress filtering and MIB (Management Information Base) statistics can be used. Egress filtering refers to the scanning of IP packet headers leaving a network and checking to see if they meet certain criteria. If the packets pass the criteria, they are routed outside of the sub-network from which they originated. Otherwise, the packets will not be sent. Since DDoS attacks often use spoofed IP addresses, there is a good probability that the source addresses of DDoS attack packets will not represent the source address of a valid user on a specific sub-network.

Honeypots are systems intentionally set up with limited security to be an enticement for an attacker's attack. Honeypots serve to deflect attacks from hitting the systems they are protecting as well as serving as a means for gaining information about attackers by storing a record of their activity and learning what types of attacks and software tools the attacker is using. Current honeypots can mimic all aspects of a legitimate network (such as web servers, mail servers, clients, etc.) in order to attract potential DDoS attackers. The goal of this type of honeypot is to lure an attacker to install either handler or agent code within the honeypot, thereby allowing the honeypot owner to track the handler or agent behavior and better understand how to defend against future DDoS installation attacks.

5.3.3. Other Weapons of the Hackers

5.3.3.1. Stealth And Backdoor Programs

Backdoors are programs furtively installed in the target system. They are malicious replacements of critical system programs that provide authentication and system reporting services. Backdoor programs provide continued and un-logged use of the system when being activated, hide suspicious processes and files from the users and system administrators, and report false system status to the users and system administrators. They may present themselves as an existing service, such as FTP, but implant a function to accept controls and execute commands from the hacker. They can also be a new service, which may be neglected because they hide their processes and do not generate noticeable network traffic.

5.3.3.2. Malicious Applets and Scripts

A malicious applet or script is a tiny piece of code, which is written in web compatible computer languages, such as Java, Jscript and Vbscript. The code is embedded in a web page, an email or a web-based application. When a person accesses the web page or opens the email, the code is downloaded to his personal computer and executed. The code may misuse the computer's resources, modify files on the hard disk, send fake email, or steal passwords.

5.3.3.3. Logic Bombs

A logic bomb is a piece of code surreptitiously inserted into an application to perform some destructive or security-compromising activities when a set of specific conditions are met. A logic bomb lies dormant until being triggered by some event. The trigger can be a specific date, the number of execution times (of the code), a random number, or even a specific event such as deletion of a specific file. When the logic bomb is triggered, it will usually do something unsolicited, such as deleting or changing files. Logic bombs may be the most insidious attack since they may do a lot of damage before being detected.

Buffer Overflow

A buffer overflow tool launches attacks by inserting an oversized block of data into a program's input buffer and stack to enable an hacker to execute a piece of malicious code or destroy the memory structure. When a program receives a block of input data, it puts the data into its input buffer, without the boundary checking, the hacker can write data past the end of the buffer and overwrite some unknown space in the memory. At the same time, the hacker carries the malicious code in the oversized data block. If the unknown space is a part of the system stack that records the return addresses, the overwritten part may change the normal return address to the address pointing to the malicious code. Hence, when the return address is fetched for execution, the malicious code, instead of the original code, will be executed.

5.3.3.4. Bugs in Software

A piece of software is vulnerable once it is released. First, it typically contains unknown bugs. A software bug is an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways. Most bugs arise from mistakes and errors made by people in either a program's source code or its

design, and a few are caused by compilers producing incorrect code. More complex it is, more bugs it may have. Bugs trigger errors that can in turn have a wide variety of ripple effects, with varying levels of inconvenience to the user of the program. Some bugs have only a subtle effect on the program's functionality, and may thus lie undetected for a long time. More serious bugs may cause the program to crash or freeze. The results of bugs may be extremely serious. Bugs in the code controlling the Therac-25 radiation therapy machine were directly responsible for some patient deaths in the 1980s. In 1996, the European Space Agency's US$1 billion prototype Ariane 5 rocket was destroyed less than a minute after launch, due to a bug in the onboard guidance computer program. In June 1994, a Royal Air Force Chinook crashed into the Mull of Kintyre, killing 29. This was initially dismissed as pilot error, but an investigation by Computer Weekly uncovered sufficient evidence to convince a House of Lords inquiry that it may have been caused by a software bug in the aircraft's engine control computer. In 2002, a study commissioned by the US Department of Commerce' National Institute of Standards and Technology concluded that "software bugs, or errors, are so prevalent and so detrimental that they cost the US economy an estimated $59 billion annually, or about 0.6 percent of the gross domestic product". Finding and fixing bugs, or "debugging", has always been a major part of computer programming.

If a hacker finds a bug before it is fixed or patched, he can exploit it to hack a system. For example, the unchecked buffer size is a bug for possible buffer overflow attacks. Second, for the purpose of developing software, the developers usually write some codes for debugging. These debugging codes generally give the developers a lot of authorities. In case these codes are not removed from the released version, the hacker can utilize them for attack.

5.3.3.5. Holes in Trust Management

Trust management is crucial for a large-scale security system. Due to the complexity of bust management, mistakes in managing and configuring trust relationships may happen in many cases and leave holes for a hacker to gain an authorized access as an unauthorized user. For example, logic inconsistence could be such a hole. Assume that there are three parties, a hacker, a database, and a school. The database trusts the school, but does not trust the hacker. However, if the school trusts the hacker who could perhaps an adolescent student, the hacker can access the database through the school.

5.3.3.6. Social Engineering

Social engineering is a tactic to acquire access information through talking and persuasion. The target person is a user who can access the computer system desired by the hacker. The hacker may pretend to be a salesman, a consultant, a listener, a friend of the user, or whatever roles that the user does not suspect when they are chatting and exchanging information. The hacker-thus can obtain valuable information, such as passwords, to gain access to the system.

5.3.3.7. Dumpster Diving

Trash is not trash in the eyes of a serious hacker. Trash usually contains shattered and incomplete information. The hacker can sift through garbage of a company to find and recover the original information so that he can break into the company's computers and networks. Now that's some real hard labor! Sometimes, the information is used as an auxiliary to help intrusion, such as making social engineering more credible.

अध्याय 6

Chapter 6

Hacking into Wireless Networks and General Anti-Hacking Measures

6.1. Hacking into Wireless Networks

6.1.1. Why Terrorists and Criminals Prefer it?

In July 2008,21 bomb blasts ripped through Ahmedabad, Gujarat, in which 56 people were killed and over 200 injured. In September 2008, five serial bomb blasts rocked the Indian capital, killing 21 people and wounding about 100. TV channels had received an email bearing the name Indian Mujahideen and asserting responsibility for the attacks. The police believed that the emails were sent by hacking into Wi-Fi connections of innocent people. The police maintained that three suspects were trained in an anti-hacking training class in Hyderabad and the Indian Mujhaideen had paid Rs. 70,000 per head as their fee for the three-day course. The three accused had done reconnaissance near CST railway station, Sanpada and Chembur for five times to check on the Wi-Fi connectivity. Finally, they zeroed on Sanpada from where they sent the email using US national Ken Haywood's IP address. Poor Haywood had a hard time establishing his innocence. Another mail was sent some days later using the Wi-Fi network of Khalsa college. Yet another email was sent misusing the IP address of a Chembur based-firm. Kamran Power Control Pvt Ltd.

The essential idea is simple. One way to beat this is to use a public IP address, such as a cyber cafe. But it has got its own problems. The terrorist has to remain as inconspicuous as possible so as to not arouse any suspicion and secondly, cyber cafes do not open and close at your convenience. Another way is to spoof the IP address. That requires a rather high level of skill. Yet another way is to hack into someone's Wi-Fi network and use his Internet connection to send the email. The terrorist can park his car somewhere near the Wi-Fi network and sit comfortably in the car with his laptop. After that, he can drive away. When the police eventually trace the IP address, it will be found to belong to some innocent person and by that time the terrorist could be thousands of miles away! Nowadays, there are wireless hotspots everywhere! You can get Internet access with a wireless enabled laptop almost everywhere you go. Beware, some terrorist or criminal could misuse your wireless network to commit a crime and land you in very serious trouble indeed.

Even if a person with a laptop or car with a mounted antenna was spotted near the wireless network from which the attack originated, authorities would have a very hard time finding the cracker and proving he is guilty. If before and after the attack the cracker has changed his or her wireless client card MAC address, and removed all the tools and data relevant to the attack from the laptop or PDA, then proving the attacker's guilt becomes impossible. Even if you or the company guards approach the cracker during an attack, as long as the cracker is not on the premises, he or she can simply refuse to cooperate and leave. What are you going to do? Take a laptop by force from a stranger on a street?

There are many factors contributing to this situation, both technical and administrative. Human factors such as the lack of user and even system administrators' education, is a major source of wireless insecurity in our opinion. As such, it is not going to disappear when newer, more secure standards become universally accepted. Thus, many security problems faced by modem wireless networks will persist for years ahead.

There are many other reasons also why hacking into wireless networks is a preferred option.

- It is fun for many hackers. Many geeks and computer nerds find hacking that involves tweaking both software (sniffing / penetration tools) and hardware (PCMCIA cards, USB adapters, connectors, antennas, amplifiers) more exciting than more traditional cracking over wired links. The same applies to being able to hack outdoors, while driving, while drinking beer in a pub that happened to be in some unlucky network's coverage zone, and so on.
- It gives anonymous access and an attacker is very difficult to trace. Hence its popularity with terrorists.
- Some activist type of people regard illicit wireless access as a way of preserving one's online privacy. Recent legislation in the United Kingdom (the infamous RIP or The Regulation of Investigatory Powers Bill) makes online privacy practically impossible, with ISP logs required to be kept for up to seven years. This legislation is primarily a response to September 11 and the U.S. Patriot Act, which many other countries have followed in terms of introducing somewhat similar regulations. An unintended result of this is to encourage users, keen on privacy, to view the Internet connection via someone's WLAN as a good way of remaining anonymous. Of course, at the same time they do violate the privacy of the abused wireless network's owners, but most such people are generally selfish. In their view, it's just "borrowing the bandwidth" for "self-defense" reasons.
- There are purely technical reasons (apart from the vague network perimeter) that make wireless networks very attractive for crackers. An access point is not a switch; it's a hub with a radio transceiver. The hacker feels that he is doing things the 'real' way, in a truly wireless world.
- When a frontal attack against the corporate gateway fails, a desperate Black Hat hacker would attempt to scan the company premises for insecure wireless access points or ad-hoc networks and succeed. A cracker can install a PCMCIA / PCI card / USB adapter / rogue access point as an out-of-band backdoor to the network.
- There is always the temptation of "opportunistic cracking." If one had the chance to read his neighbors' emails and check which websites they were surfing, few people would resist it. If a neighbor has an insecure wireless network, chances are an opportunistic attack will be successful.
- If the network in question is a corporate WLAN that opens future access into a large, impressive wired network, there is always a possibility of reaping sensitive data with potentially very high value from their corporate rivals and a very highspeed connection to the Internet to boot on the side for some personal fun?

6.1.2. What Does it Take to Hack into Wireless Networks?

6.1.2.2. What's in the Air, is Open to All?

If you're using wireless technology, or considering making the move to wireless, you should know about the security threats you may encounter. One of the fundamental problems with wireless is that the radio waves that connect network devices do not simply stop once they reach

We believe that mere movement is life, and that the more velocity it has, the more it expresses vitality.
- Swami Vivekananda

a wall or the boundary of a business. They keep traveling into parking lots and other businesses in an expanding circle from the broadcast point, creating a 'bubble' of transmission radiation. This introduces the risk that unintended parties can eavesdrop on network traffic from parking areas or any other place where a laptop can be set up to intercept the signals.

Wireless network refers to any type of computer network which is wireless, and is commonly associated with a network whose interconnections between nodes e.g. laptops, desktops, printers etc is implemented without the use of wires. The popularity of wireless networks is driven by two major factors: convenience and cost. A Wireless Local Area Network (WLAN) allows workers to access digital resources without being locked to their desks. Mobile users can connect to a Local Area Network (LAN) through a Wireless (Radio) connection. Demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and PDAs, and by users' desire for continuous network connections without physically having to plug into wired systems. For the same reason that WLANs are convenient, their open broadcast infrastructure, they are extremely vulnerable to intrusion and exploitation. Adding a wireless network to an organization's internal LAN may open a backdoor to the existing wired network.

6.1.2.2. Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer within range of your wireless access point can hop a free ride on the internet over your wireless connection. The typical indoor broadcast range of an access point is 150-300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could potentially open your Internet connection to a surprising number of hackers. Even if the hacker is not a terrorist, the piggybacking will use up your bandwidth and slow your connection. At the same time, they may monitor your Internet activity and steal passwords and other sensitive information.

6.1.2.3. War Driving

War driving is a specific kind of piggybacking. War Driving is all about finding out the wireless networks with WEP disabled and using only the SSID for access control. War driving is of two types:

1. Active War Driving
2. Passive War Driving

- **Active War Driving:** Active War Driving is detecting the Wireless Networks whose SSIDs are broadcasted or the Wireless Networks which are shown to all the Wireless Adapters. It can be done through any Wireless Card.
- **Passive War Driving:** Passive war Driving is detecting the wireless Networks whose SSIDs are not broadcasted or the Hidden Wireless Networks. The Wireless card should support the Monitor Mode for the Passive War Driving.

A war driver is a hacker who moves in a vehicle (and hence the word driving in it) with a laptop or a PDA (Personal Digital Assistants) like iPhone or BlackBerry which has a software

that detects Wi-Fi networks. When he finds an "open" network, that is one that is not password-protected, he could get into the network in an unauthorized manner and use it for a range of nefarious activities. Studies have shown that practically 90% of the Wi-Fi networks are not password-protected. Software for war driving is freely available on the Internet or comes even pre-installed in the device. Precisely for this reason, such attacks are increasing. When done on a moving bicycle or motorcycle, wardriving is called warbiking. Then there's warwalking (or warjogging), which is done on foot.

The broadcast range of a wireless access point can make internet connections possible outside your home, even as far away as your street. Savvy computer users know this, and some have even made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. Wardrivers often note the location of unsecured wireless networks and publish this information on websites or their forums also.

6.1.2.4. Some Key Terms Explained

Before we proceed further, understanding some key terms would be of help.

- **WAP** (Wireless Access Point): Wireless Access Point is the point from where the Wireless network are generated. Like the Wireless Routers or Switches.
- **SSID** (Service Set Identifier) :An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSID is also known as ESSID (Extended Service Set Identifier).
- **BSSID** (Basic Service Set Identifier): BSSID is the MAC Address (Media Access Control) or Physical Address of the wireless Access Point or the wireless Router. This is a unique 48 bit key provided by the manufacturer of the device. It can be in the form of Hexadecimal.
- **Beacons**: These are the wireless packets which are broadcasted to maintain the connectivity with the Wireless Access Point and Client systems. The wireless Access point broadcasts beacon frames from time to time to check connectivity with the systems.
- **Channel:** It is the frequency at with the Wireless Signal travels through air.
- **Data Packets:** These are the packets which sent and received for the transfer of data between Wireless Access Point and Client systems. All the data communicated between two Computers travels in the form of Data Packets.
- **Wired Equivalent Privacy** (WEP): It is a security algorithm for IEEE 802.12 wireless networks. Its intention was to provide data confidentiality comparable to that of a traditional wired network.
- **WPA** (Wi-Fi Protected Access): It is the successor to WEP. WPA and WPA2 are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

The IEEE 802.11 standard refers to a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). Standard802.11 specifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.

6.1.2.5. Basic Principle of Hacking a Wireless Network

Most of the wireless vulnerabilities are in the 802.11 protocol and how it works. 802.11 encryption protocols are called Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). They have their own weakness that allows attackers to crack the encryption keys and decrypt the captured traffic. WEP is vulnerable because of relatively short and weak encryption. The security of the WEP algorithm can be compromised. This vulnerability has actually helped put WLANs on the map—so to speak. WEP, in a certain sense, actually lives up to its name: It provides privacy equivalent to that of a wired network, and then some. However, it wasn't intended to be cracked so easily. WEP uses a fairly strong symmetric (shared key) encryption algorithm called RC4.

But hackers turned out to be cleverer. Hackers can observe encrypted wireless traffic and recover the WEP key because of a flaw in how the RC4 Initialization Vector (IV) is implemented in the protocol. This weakness is because the IV is only 24 bits long, which causes it to repeat every 16.7 million packets—even sooner in many cases, based on the number of wireless clients entering and leaving the network. Most WEP implementations initialize WLAN hardware with an IV of 0 and increment it by one for each packet sent. This can lead to the IVs reinitializing—starting over at 0—approximately every five hours. Given this behavior, WLANs that have a small number of clients transmitting a relatively small rate of wireless packets are normally more secure than large WLANs that transmit a lot of wireless data because there's simply not enough wireless traffic being generated. Using WEPCrack (http://wepcrack.sourceforge.net), AirSnort (http://airenort.shrnoo.com), or, my favorite, the aircrack suite (http://aircrack-ng.org), hackers need to collect only a few hours' up to a few days' (depending on how much wireless traffic is on the network) worth of packets to break the WEP key.

The wireless industry has come up with a solution to the WEP problem called Wi-Fi Protected Access(WPA). WPA uses the Temporal Key Integrity Protocol (TKIP) encryption system, which fixes all the known WEP issues. WPA2 which replaced the original WPA uses an even stronger encryption method called Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (say that fast three times)—or CCMP—based on the Advanced Encryption Standard (AES). WPA and WPA2 running in "enterprise mode" require an 802.1 x authentication server, such as a RADIUS server, to manage user accounts for the WLAN. Check with your vendor for WPA updates. Hackers can use aircrack to crack WPA and WPA2 pre-shared keys (PSKs). To crack WPA-PSK encryption, one has to wait for a wireless client to authenticate with its access point. A quick (and dirty) way to force the re-authentication process is to send a de-authenticate packet to the broadcast address.

Airodump is an 802.11 packet capture program that is designed to "capture as much encrypted traffic as possible. Airodump is primarily used to produce the capture files that then feed into

aircrack for WEP cracking. The hacker can use airodump to capture packets and then start aircrack (he can also run them simultaneously) to initiate cracking the pre-shared key. Each WEP data packet has an associated 3-byte Initialization Vector (IV). After a sufficient number of data packets have been collected, they run aircrack on the resulting capture file. Aircrack then performs a set of statistical attacks developed by a talented hacker named KoreK.

Another, relatively new, tool one can use for cracking WPA and WPA2 keys is the commercial product. Elcomsoft Wireless Security Auditor (EWSA). To use EWSA, he simply captures wireless packets in the tcpdump format (every WLAN analyzer supports this format), loads the capture file into the program, and shortly thereafter he has the PSK. EWSA is a little different because it can crack WPA and WPA2 PSKs in a fraction of the time it would normally take, but there's a caveat. The hacker has to have a computer with a supported NVIDIA or ATI video card. Using EWSA, the hacker can try to crack your WPA/WPA2 PSKs at a rate of up to 50,000 WPA/WPA2 pre-shared keys per second. Compare that to the lowly few hundred keys per second using just the CPU and you can see the value in a tool like this.

Wireless systems (clients, APs, and so on) use Carrier Sense Multiple Access/ Collision Avoidance CSMA/CA to determine whether the wireless medium is ready and the system can transmit data. Researchers at the Queensland University of Technology's Information Security Research Centre (www.kb.ceit.org/vuls/id/ 106678) discovered a new form of attack. This "Queensland" attack, also referred to as the Clear Channel Assessment attack, affects the Direct Sequence Spread Spectrum function that works as part of 802AVs Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) protocol that manages the wireless communications medium. The "Queensland" attack exploits the Clear Channel Assessment (CCA) function within CSMA/CA and makes it appear that the airwaves are busy, effectively preventing any other wireless system from transmitting. This is accomplished by placing a wireless NIC in continuous transmit mode. With the right tool, this attack is relatively simple to execute. It can wreak havoc on a wireless network, effectively bringing it to its knees. There's very little that can be done about it, especially if the attacker's signal is more powerful than that of your wireless systems.

In an evil twin attack, the attacker gathers information about a public access point, then sets up his own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the Internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.

Many laptop computers, particularly those equipped with 802.11-type Wi-Fi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of. An attacker with a network card configured for ad hoc mode and using the same settings as

your computer may gain unauthorized access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.

6.1.3. How do they Go About it?

Generally, the hackers look out for the following weaknesses:

- Unencrypted wireless traffic
- Weak WEP and WPA pre-shared keys
- Unauthorized APs
- Easily circumvented MAC address controls
- Wireless equipment that's physically accessible
- Default configuration settings

The first thing he does is to find where the signal from the audited network can be received; how clear the signal is (by looking at the signal-to-noise ratio (SNR)), and how fast the link is in different parts of the network coverage zone. He would also try to discover neighboring wireless networks and identify other possible sources of interference. If you are a security administrator, then your site survey must find out where the attackers can physically position themselves. A cracker with a highly sensitive and powerful card linked to a high-gain antenna might be able to attack from a position in which you could never expect him or her to be. Think about it when performing your WLAN site survey as the first stage of a proper wireless security audit. Do not assume that the attackers will try to get as close as they can and won't have equipment allowing them to attack from long range. After all, more sensitive and powerful cards are not obviously more expensive, cheap high-quality antennas are abundant, and prices on amplifiers are slowly falling. The cost of assembling a very decent attacker's kit is not higher than the cost of deploying a casual home WLAN. You must detect rogue access points and neighbor networks (a possible source of opportunistic or even accidental attacks). You must also baseline the interference sources to detect abnormal levels of interference in the future, such as the interference intentionally created by a jamming device.

6.1.3.1. The Software Tools

Several great WLAN security tools are available for both the Windows and UNIX platforms. Hackers use the same tools! Hence anybody who is interested in preventing hackers getting into their wireless networks must know this. Some of the good tools for assessing wireless networks in Windows are as follows:

- **NetStumbler** (www.netstumbler.com)
- **AirMagnet** (now Fluke) WiFi Analyzer (http://www.airmagnet.com/products/wifi_analyzer)
- **WildPackets' OmniPeek** (www.wildpackets.com/products/ distributed_network_analysis/ omnipeek_network_analyzer)
- **Elcomsoft Wireless Security Auditor** (www.elcomsoft.com/ewsa.html)

- **Aircrack** (http://aircrack-ng.org)

Network discovery tools are the most abundant; many of them are free also. Some of these tools are more than just network mapping software, and support advanced features such as WEP decryption on the fly or wireless IDS signature database. In general, all he needs to detect wireless networks or hosts and log wireless traffic is to put a client card into the RFMON mode and run tcpdump on the appropriate interface. The rest of the features are often a power-consuming luxury, helping users to visualize the discovered networks and decode traffic.

There are three ways of discovering wireless networks: active scanning, monitor mode sniffing, and searching for access points and ad-hoc cells with the iwlist scanning command, which is a form of active scanning anyway. Active network discovery is implemented by Netstumbler and Mini-Stumbler, Windows tools most frequently used by casual wardrivers around the world. In fact, so much so that many mistakenly equate the terms wardriving and netstumbling (which is incorrect) and recommend Netstumbler for use by IT security professionals.

The most common and useful group of wireless network discovery and traffic analysis tools (wireless sniffers) use the RFMON mode combined with hopping through all DSSS (direct sequence spread spectrum) channels. This lets one discover wireless hosts via detecting and analyzing passing traffic including all kinds of control and management frames. His client card receiving sensitivity (dBm) becomes the only limiting factor in network discovery and it can be greatly alleviated by the use of high-gain antennas and bidirectional amplifiers. Kismet (http://www.kismetwireless.com) is a workhorse for years and is a universal 802.11 sniffer that went a long way from a wardriving tool to a full-blown wireless protocol analyzer and an IDS suite. It is also advisable to implement a tool that will place the locations of wireless networks on a map. GpsDrive can be tweaked to do this without much effort. Gpsmap, a tool packaged with Kismet, is another excellent utility that we find very useful to graphically represent a Kismet wardriving session or client site survey. If you want a very easy-to-use graphical wireless sniffer, look no further. Sparing the obvious pcmcia-cs, libpcap, and tcpdump, you'll need to install Gtk-Perl (http://www.gtkperl.org/download.html) and the Net-Pcap Perl module to run Wellenreiter (http://www.wellenreiter.net/). There are many other tools like Airtraf, Gtkskan, Airfart, Mognet, and WifiScanner also. The main advantage provided by tools that use the iwlist scan command is the possibility to discover access points in the area without disconnecting from the network you are already associated with.

Encryption cracking tools are created to break 802.11-specific Layer 2 cryptographic protection. Essentially it means cracking the WEP. However, tools are now available to attack 802.1x authentication also. Currently, there are four classes of wireless encryption cracking tools:

- WEP crackers
- Tools to retrieve WEP keys stored on the client hosts
- Traffic injection tools accelerating WEP cracking and making network reckon without knowing WEP key possible

- Tools to attack 802.lx authentication systems
- There are three main ways of attacking WEP:
- Brute-forcing and improved brute-forcing
- FMS attack
- Improved FMS attack
- **WEP Brute-Forcing:** Pure WEP keyspace brute-forcing with tools such as wep_tools or dwepcrack brute-forcing options is realistic only against 40-bit WEP keys. One should never underestimate the potential of dictionary attacks, which are also applicable to 128-bit and higher WEP key size.
- **The FMS Attack:** The most common attack against WEP is Scott Fluhrer, Itsik Mantin, and Adi Shamir's (FMS) key recovery methodology discovered in 2001 (the original paper entitled "Weaknesses in the Key Scheduling Algorithm of RC4" is available from http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps). This attack was implemented first by the Wepcrack and then by AirSnort. An improved attack is available in the "Practical Exploitation of RC4 Weaknesses in WEP Environments" article available at http:// www.dachb0den.com/projects/bsd-airtools/wepexp.txt). The attacks against WEP we have reviewed so far are purely passive and rely on traffic being present on the wireless network. But can we generate the additional WLAN traffic without even being associated to the network? The answer is positive and we have the tools such as reinj or Wepwedgie. There are claims that reinj can reliably cut WEP cracking time to less than one hour and there is no reason not to believe these claims.

TKIP is supposed to take care of the vulnerabilities of WEP. When the TKIP keys are generated, distributed, and rotated using 802. lx and RADIUS, a cracker won't get far trying to crack the keys. Instead, he or she will probably choose a more lateral approach, trying to attack the 801.1 x itself. Although no ready tool to perform the offline TKIP cracking exists at the moment of writing, the bounty is too high and most likely by the time you buy this book, the cracking underground will come up with one. After all, we are talking about a hash-cracking tool similar to md5crack and a shell script to send de-associate frames and capture the handshake afterward to provide the feed for a hash cracker. Similar functionality is already implemented in a wireless attack tool, namely the Asleap-imp.

Wepcrack was the first tool but currently, the most commonly used WEP cracking tool is AirSnort from the Shmoo group (http://airsnort.shmoo.com). Dwepcrack is a WEP cracking utility created for all kinds of known attacks to determine a WEP key. It implements several techniques in a single package, which lets one run a full test of WEP key security using all cunently available methodologies for WEP cracking. Dwepdump is a prism2dump-like pcap-format file dump utility, specifically written to provide data for dwepcrack and non-FMS brute-forcing attacks against WEP. Wep_tools is particularly efficient against the original standard 40-bit WEP keys. WepAttack is an open source tool similar to Wep_tools, but with significant improvements. Just like Wep_tools, WepAttack uses brute-forcing or dictionary attacks to find the right key from the encrypted data

pcap dump file. However, the project page states that only a single captured WEP-encrypted data packet is required to start an attack. The WepAttack project page is located at Sourceforge (http://sourceforge.net/projects/wepattack/). There are also tools like LucentRegCrypto utility to retrieve WEP keys stored on the client hosts.

The more wireless traffic the hacker collects, the higher his chances are of obtaining the correct WEP key and the less time is needed to get it. To perform this task he will need a card in the RFMON mode, listening to the packets flying by and retransmitting the packets that pass a certain sanity check. A tool specifically designed to re-inject traffic for improved WEP cracking efficiency is reinj from the Wnet suite for BSD written by H1kari, an author of BSD-Airtools.

At the moment 802.1x authentication using Cisco EAP-LEAP takes the heaviest impact from the hacking community. The main target of attacks against EAP-LEAP is its reliance on MS-CHAPv2 for user authentication. Thus, the attacks against EAP-LEAP are actually attacks against MS-CHAPv2 used in the clear and any other wireless authentication method employing it would be just as vulnerable. The first tool is Asleap-imp, presented by Joshua Wright at Defcon 11. The second tool is leap by DaBubble, Bishop, and Evol. Unlike Asleap-imp, it was released to the general public via the Packetstorm Web site (http ://www.packetstormsecurity.org).

Because 802.11 management and control frames are neither authenticated nor encrypted, being able to send custom 802.11 frames gives a wireless attacker an unlimited opportunity to cause Layer 2 DoS attacks on a targeted WLAN. Even worse, a skilled attacker can spoof his or her attacking machine as an access point, wireless bridge, or client host on the unfortunate infrastructure or managed network or as a peer on the independent or ad-hoc WLAN. Then a DoS attack can be used to de-associate WLAN hosts from a legitimate access point or bridge and force them to associate with the attacker's machine. There are two main tools that allow custom 802.11 frame generation: AirJack suite (Linux) and the more recent Wnet dinject utilities collection (OpenBSD).

Knowing the basics of wireless networking and which tools to use to discover access points, dump the traffic, crack WEP, and so on is not enough. In fact, it only brings the attacker to the "script kiddie" level. A black hat hacker and a wireless security professional must know much more than this. They should understand how the protocols involved and the available attack methodologies work. Wireless attacks do not start and end with cracking WEP, as many security experts might tell you. However, if the attacker cannot break WEP (if present), all he or she can do is disrupt the network operations by DoS attacks on layers below the protocol WEP implementation.

6.1.3.2. The Hardware Tools

The hacker also needs proper hardware for hacking wireless networks. A good setup is a laptop with an Orinoco 802.11b PC Card (earlier made by Lucent, now Proxim). This card is not only compatible with NetStumbler, but it also allows you to connect an external antenna. Another bonus is that most wireless security tools are very friendly with the Orinoco card. A lot of security tool support is available for the Prism2 chipset found in wireless cards by Belkin, D-Link, Linksys, and more. They also use AirMagnet's WiFi Analyzer with a Netgear WAG511 v2 or Linksys WPC55AG card.

They can also use a handheld wireless security testing device, such as the handy Digital Hotspotter by Canary Wireless (www.canarywireless.com) or the ultra-powerful AirMagnet Handheld Analyzer (www.airmagnet.com/products/ handheld_analyzer).

An external antenna is also an important part of his arsenal. Why? Because, using an additional antenna increases the chances of finding both legitimate and (more important) unauthorized wireless systems. He can choose among three types of wireless antennas:

- **Omni-directional:** Transmits and receives wireless signals in 360 degrees over shorter distances, such as in boardrooms or reception areas. These antennas, also known as dipoles, typically come installed on APs (access points) from the factory. A high-gain omni-directional might look like a walking stick or a pool cue and will not raise any suspicions. The majority of Yagis can pass for poster holders and even the directional dishes would not surprise anyone as long as the cracker passes himself or herself off as telecom engineer troubleshooting a link or even an amateur radio enthusiast.
- **Semi-directional:** Transmits and receives directionally focused wireless signals over medium distances, such as down corridors and across one side of an office or building.
- **Directional:** Transmits and receives highly focused wireless signals over long distances, such as between buildings. This antenna, also known as a high-gain antenna, is the antenna of choice for wireless hackers driving around cities looking for vulnerable APs. As an alternative to the antennas described in the preceding list, he can use a nifty can design—called a cantenna—made from a Pringles, coffee, or pork-and-beans can. If you're interested in learning more about this, check out the article at www.turnpoint.net/wireless/has.html for details. One site in particular (www.cantenna.com) sells the Super Cantenna kit. Another good site for cantenna kits is Hugh Pepper's site: http://mywebpages.comcastnet/hughpep.

Antennas and amplifiers give an enormous edge to both the skillful attacker and defender. From the attacker's perspective, antennas give distance (resulting in physical stealth), better signal quality (resulting in more data to eavesdrop on and more bandwidth to abuse) and higher power output (essential in Layer 1 DoS and man-in-the-middle attacks). From the defender's perspective, correctly positioned antennas limit the network boundaries and lower the risk of network detection while reducing the space for attackers to maneuver. In addition, three highly directional antennas in conjunction with mobile wireless clients, running signal strength monitoring software, can be used to triangulate the attacker or a rogue wireless device. This is, of course, dependent on the attacker actually transmitting some data. When selecting your antennas for wireless security audit, a decent omnidirectional and a high-gain, narrow-beam-width antenna are the minimum.

6.1.4. Fifteen Practical Countermeasures Against Attacks on Encrypted Wireless Traffic

The simplest solution to the WEP problem is to migrate to WPA, or ideally, WPA2, for all wireless communications. You can also use a VPN in a Windows environment—free—by enabling Point-to-Point Tunneling Protocol (PPTP) for client communications. You can also use the IPSec support built into Windows, as well as Secure Shell (SSH), Secure Sockets Layer/Transport Layer

Security (SSL/TLS), and other proprietary vendor solutions, to keep your traffic secure. But keep in mind that there are cracking programs for PPTP, IPSec, and other VPN protocols as well, but overall, you're relatively safer.

If you're using WPA with a pre-shared key (which is more than enough for small WLANs), ensure that the key contains at least 20 random characters so it isn't susceptible to the online dictionary attacks available in such tools as aircrack and Elcomsoft Wireless Security Auditor.

The only potential countermeasure against wireless DoS attacks is the installation and usage of a wireless IPS on your 802.11b/g network. Otherwise, wireless technologies that use frequency hopping spread spectrum (FHSS) or orthogonal frequency division multiplexing (OFDM)—such as 802.11a, 802.11n, and technically 802.11g running over 20Mbps—are the way to go.

While the security problems associated with wireless networking are serious, there are some steps you can take to protect yourself.

1. **Position The Router Or Access Point Safely:** Wireless signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wireless signals often reach through neighboring houses and into streets. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the centre of the home rather than near windows to minimize leakage. Many routers allow you to reduce the range of your router from the administrative panel to prevent the signal leakage.

2. **Change Default Administrator Usernames And Passwords:** Most routers or access points come enabled with a default set of username/password combinations. These combinations are well documented and available online for hackers to use. If a hacker can access your device's administrative pages they can modify the configuration and control all aspects of your device. These username/password combinations can be changed from the administrative panel and should be set to something difficult to guess. Be sure to change your administrator password to one that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). The default password for most wireless kits is ADMIN or something else set by manufacturers. If you haven't changed this password then change it as soon as you can. It is surprising the amount of wireless networks that are hacked into or accessed by a third party because the ADMIN password is still ADMIN. All manufacturers' manuals can be downloaded from the Internet with their admin password easily.

3. **Change The Default SSID:** Access points and routers all use a network name called the SSID (Service Set Identification). An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank. A network

administrator often uses a public SSID, which is set on the access point and broadcast to all wireless devices in range. Manufacturers normally ship their products with the same SSID set for all routers. For example, the SSID for Netgear devices is normally 'NETGEAR'. The default SSID can be changed from the administrative panel and should be set to something unique. Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

4. **Enable MAC Address Filtering:** Each wireless device possesses a unique identifier called the physical address or MAC address. A Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. Access points and routers keep track of the MAC addresses for all devices that connect to them. Wireless routers offer the option to key in the MAC addresses of your home equipment so as to restrict the network to only allow connections from those devices.

   In Media Access Control (MAC) address controls, you configure your APs to allow only wireless clients with known MAC addresses to connect to the network. Consequently, a very common hack against wireless networks is MAC address spoofing. The bad guys can easily spoof MAC addresses in UNIX, by using the ifconfig command, and in Windows, by using the SMAC utility. However, like WEP and WPA, MAC-address-based access controls are another layer of protection and better than nothing at all. If someone spoofs one of your MAC addresses, the only way to detect malicious behavior is to spot the same MAC address being used in two or more places on the WLAN, which can be tricky. One simple way to determine whether an AP is using MAC address controls is to try to associate with it and obtain an IP address via DHCP. If you can get an IP address, then the AP doesn't have MAC address controls enabled.

   The easiest way to prevent the circumvention of MAC address controls and subsequent unauthorized attachment to your wireless network is to enable WPA, or ideallyWPA2. Another way to control MAC spoofing is by using a wireless IPS (wireless intrusion prevention system). This second option is certainly more costly, but it could be well worth the money when you consider the other proactive monitoring and blocking benefits such a system would provide.

5. **Disable SSID Broadcast:** The wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where wireless clients may roam in and out of range. For the home user, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most wireless access points allow the SSID Broadcast feature to be disabled by the network administrator. Your SSID name can be manually entered into your devices to prevent the need for SSID Broadcasts to be enabled.

6. **Disable Remote Login:** The first router worm brute forces its way into the router in this manner. Most default usernames are set to Admin. It isn't hard for a virus/worm to crack the password if the username is known. The good thing is that routers normally have this disabled by default. Be sure to confirm that it is disabled when you first set up your router

and periodically thereafter. If you need to update your router setting remotely, only set up access for the time you are going to be connected.

7. **Do Not Auto-Connect To Open Wireless Networks:** Connecting to an open wireless network like a free wireless hotspot or your neighbor's router exposes your computer to security risks and attacks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying the user. This setting should not be enabled except in temporary situations.

8. **Assign Static IP Addresses To Devices:** Most home wireless devices use dynamic IP addresses. The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices so that they can communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the Internet. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range instead and then configure each connected device to match. Using a private IP address range (like 10.0.0.x) prevents computers from being reached directly from the Internet

9. **Rename Your Wireless Network:** Many wireless access point devices come with a default name. This name is referred to as the "service set identifier" (SSIS) or "extended service set identifier" (ESSID). The default names used by various manufacturers are widely known and can be used to gain unauthorized access to your network. When you rename your network, you should choose a name that won't be easily guessed by others.

10. **Encrypt Your Network Traffic:** Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code. For more about encryption, see the US-CERT Cyber Security Tip "Understanding Encryption".

11. **Use File Sharing With Caution:** If you don't need to share directories and files over your network, you should disable file sharing on your computers. You may want to consider creating a dedicated directory for file sharing, and move or copy files to that directory for sharing. In addition, you should password protect anything you share, and use a password that is long, contains non-alphanumeric characters (such as #, $, and &), and does not contain personal information (such as your birth date). Never open an entire hard drive for file sharing.

    File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don't know. Also, many public wireless

networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to invite risk. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.

12. **Keep Your Access Point Software Patched And Up To Date:** From time to time, the manufacturer of your wireless access point will release updates to the device software or patches to repair bugs. Be sure to check the manufacturer's web site regularly for any updates or patches for your device's software.

13. **Check Your Internet Provider's Wireless Security Options:** Your internet service provider may provide information about securing your home wireless network. Check the customer support area of your provider's web site or contact your provider's customer support group.

14. **Connect Using A VPN:** Many companies and organizations have a virtual private network (VPN). A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. Whereas the deployment of wired VPNs is usually restricted to specific cases of telecommuters and remote branch offices, the wireless world is entirety different, and deploying a VPN can be applicable to any wireless link if a high level of security is needed. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites but appears to the user as a private network link—hence the name "virtual private network" VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

    A VPN is the opposite of an expensive system of owned or leased lines that can be used by only one organization. The goal of a VPN is to provide the organization with the same capabilities at a much lower cost Compare it to point-to-point bridged wireless connectivity solutions, which can also substitute expensive leased lines. VPN and wireless technologies do not compete, but complement each other.

    A VPN works by using the shared public infrastructure, while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be entered by data that is not properly

encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses. A WLAN can be compared to a shared public network infrastructure or, in some cases (hot spots, community nodes), is a shared public network infrastructure. The virtual part of the term entails mutually exclusive and peaceful coexistence of two separate networks within single network segments, be it coexistence of IP, IPX, and DDP on the same LAN, or IP, IPSec, and L2TP traffic going through the Internet cloud. The private part acknowledges that the interaction and the underlying network are only understandable to the endpoints of the channel and not to anyone else. It applies to both secrecy and authenticity of transmitted data.

But remember that attacks on VPNs are also possible. Point-to-Point Tunneling Protocol (PPTP) and various IPSec implementations are the most common VPN solutions encountered. PPTP took a heavy battering from the security community and multiple tools have built-in options to attack PPTP tunnels. Anger is one such tool.

15. Don't Overlook Bluetooth: You undoubtedly have various Bluetooth-enabled wireless devices, such as laptops and smart phones, running within your home or office. Mobile devices have become a completely new dilemma for information security. We honestly believe they're one of the greatest risks in any given business. Although vulnerabilities are not as prevalent as they are in 802.11 based Wi-Fi networks, they still exist (currently, over 60 Bluetooth-related weaknesses are listed at http://nvd.nist.gov), and quite a few hacking tools take advantage of them.

Looking for Bluetooth networks is called warnibbling. The tools for Bluetooth network discovery such as Redfang from @Stake and a graphical user interface (GUI) for it (Bluesniff, Shmoo Group) are already available to grab and use and more tools will no doubt follow suit. Class 1 Bluetooth devices (output transmission power up to 100 mW) such as Bluetooth-enabled laptops and access points can cover a 100-meter radius or greater if high-gain antennas are used. Bluetooth devices are usually set to the first (lowest) security mode out of the three Bluetooth security modes available and have the default of "0000" as the session security PIN. It is also common to use the year of birth or any other meaningful (and guessable) four-digit number as a Bluetooth PIN. This happens for convenience reasons, but the unintended consequence is that it makes the cracker's job much easier. In our observations, about 50 percent of Bluetooth-enabled devices have the default PIN unchanged. There are also devices that have default PINs prewired without any possibility of changing them: all the attacker would have to do is find the list with the default PINs online.

One can even overcome the personal area network distance limitation of Bluetooth's signal (typically just a few meters) and attack Bluetooth devices remotely by building and using a BlueSniper rifle. Bluesniping has emerged as a specific form of Bluesnarfing, or for simply identifying Bluetooth-enabled devices, at longer ranges than normally possible. According to Wired Magazine, this method surfaced at the Black Hat Briefings and DEF CON hacker conferences of 2004 where it was shown on the G4techTV show The Screen Savers. In the article 'Rifle' Sniffs

Out Vulnerability in Bluetooth Devices', the 'rifle' features a directional antenna, Linux-powered embedded PC, and module all mounted on a Ruger 10/22 folding stock. According to Flexilis, the rifle is capable of targeting Bluetooth at ranges over one mile. This type of Bluesniping has been utilized to demonstrate the increasing security vulnerability of Bluetooth devices.

According to the Bluetooth Special Interest Group (SIG), in order to break into a Bluetooth device, a hacker must "Force two paired Bluetooth devices to break their connection", known as Blueballing. One should take away from this the caveat of never pairing with unknown devices or in public places. The connection between one's cellular phone and one's Bluetooth-enabled headset, for instance, could be broken and the cellular phone may be able to be hijacked by the remote "Bluesniper" for one purpose or another.

6.2. General Anti-Hacking Measures

6.2.1. Intrusion Detection Systems (IDS)

6.2.1.1. Why You Need Intrusion Detection?

Doors can be opened to hackers in varied ways. Two of the most common ways by which they can gain access to your computer is simply through emails, or web pages that you visit that have spyware, or Trojans (a file which looks innocent, but actually will later open doors to a hacker) attached to them. Other ways are spiders robots sent out over the Internet to find unprotected computers, and open doors. Many experts maintain that every computer attached to the Internet may be attacked by such a spider as many as 50 times each day. So, if you do not have an intrusion prevention system in place, up-to-date, then you may have regular unexpected visitors— and you may not even know it.

The spider robots work automatically—looking for and identifying computers on the Internet that have doors, or ports, open to them. This information is then reported back to the hacker—letting them know which computers to target—and which port to use. For this reason, every now and then, Microsoft comes out with a new patch for Windows, in order to close some faulty door that hackers have discovered and have been using.

Network Intrusion Detection System (NIDS) is a very important thing these days. Each company's software will vary somewhat (for copyright and originality purposes), but you do need one for your own network, or home computer. It differs from a firewall in that the purpose of a firewall is to stop unauthorized external contacts with your system. Firewalls offer hacker prevention largely for contacts from outside the network. Most of these will now notify the owner or network controller of intrusion attempts. Network intrusion detection systems, on the other hand, will give you warnings about events that take place within the network itself. Some systems try to combine some of the features of a firewall and an intrusion detection system into one great package—and some of them can even remove existing malware on your system! Intrusion detection software can also stop phishing emails, spam, and those pop-up ads. They can also prevent dial up hacker from invading your system. When selecting your intrusion detection software, you need to know that there are basically two kinds. One is passive, meaning that an alarm will be sounded. A second kind is active, meaning that it will terminate the communication

with the computer trying to obtain access, and it will notify the Webmaster. In the next section, we will leam more about them.

6.2.1.2. Basic Types of IDS

Intrusion detection systems (IDSs) are divided into two major categories: signature-based and knowledge-based. Signature-based IDSs are the most common and easy to implement, but they are also the easiest to bypass, and also lack the capability to detect novel attacks. These IDSs compare events on the network to signs of known attacks called attack signatures. If a hacking tool is modified to alter some part of its attack signature, the attack is likely to go unmentioned. Besides, the attack signatures database has to be well secured and frequently updated. Most of the practical systems, such as Snort, are signature-based detectors.

Knowledge-based IDSs monitor the network, collect statistics about standard network behavior, detect possible deviations, and flag them as suspicious. For these reasons, knowledge-based IDSs are also called behavior-based or statistical. Proper network baselining is essential for efficient statistical IDS operations. Although knowledge-based IDSs are not easily fooled, their main problems are false positives and difficulties detecting some covert channel communications. The possibility of false-alarm generation is particularly worrisome on wireless networks due to the unreliable nature of the Layer 1 medium. Also, attacks launched at the early stage of the baselining period can severely interfere with the IDS learning process, making deployment of a knowledge-based IDS on a production network a somewhat risky task.

In the Anomaly Detection type of intrusion detection, the normal user behavior is defined and the system looks for any significant deviation from these established normal uses. The goal of anomaly detection is to create a white-list of the only activities that are allowed in the network. But the main problem with anomaly detection IDS is the large number of false alarms. Anomaly detection schemes are, however, a popular tool for detecting credit card fraud and other very specific scenarios. A proper wireless IDS should implement and integrate both attack signature comparison and network traffic anomaly detection.

6.2.1.3. Categorizing Suspicious Events on WLANs

Once a sufficient number of network behavior statistics are gathered, a proper wireless IDS can start looking for the suspicious events indicating the possibility of malicious attack. These events might be manifested as the presence of certain frame types, frequency of frame transmission, frame structure and sequence number abnormalities, traffic flow deviations, and unexpected frequency use. These events can indicate successful or unsuccessful cracker attacks, a host with mis-configured security settings, attempts to access and reconfigure the deployed access points, the use of traffic injecting tools, advanced DoS attacks against 802.11i-enabled hosts, or attempts to overwhelm the AP buffers with large numbers of connections from the wired or wireless side.

The best way of knowing these signatures is trying out the tools in question and sniffing out their output: “Attack through defending, defend through attacking”. A wireless network discovery or attack tool must transmit data to provide us with an IDS signature. Netstumbler and its smaller Pocket PC MiniStumbler are the most common wireless IDS signature generators in the

wild. They are free, easy to install and use, and, of course, run under the most common operating system in the world. There isn't a way to discover a passive traffic sniffer and WEP cracker, and it doesn't matter how hard you try. The only reliable way to detect "passive" attackers is spotting them physically using optical devices and the "geek with a laptop and antenna" attack signature. However, remember that crackers can easily modify or eliminate the signatures to avoid detection.

6.2.1.4. Commercial Wireless IDS Systems

Well-known wireless IDS solutions include AirDefense Guard (http://www.airdefense.net/products/airdefense_ids.shtm) and Isomair Wireless Sentry (http://www.isomair.com/products.html). These solutions are based on deploying an array of sensors around the monitored WLAN and centralizing their output to the management server or console. The server can be a specialized hardware appliance with a secure Web interface and SNMP (Simple Network Management Protocol) management or a Linux server machine linked to the Windows-based management console. Some of these solutions can analyze non-802.11 wireless traffic or even the RF interference in the monitored band, which is useful. WiSentry (http:// www.wimetrics.com/products/download_wisentry.php) is a commercial software-only solution for WLAN monitoring and intrusion detection that does not require specialized hardware sensors. Another commercial tool that combines both security auditing and IDS features is AirMagnet from Global Secure Systems (http://www.gsec.co.uk/products/_wireless_security.htm). AirMagnet is available in handheld, laptop (must use Cisco Aironet cards), and "combo" editions.

6.2.1.5. When to Suspect Hacking?

Hackers, by nature are very stealthy. Their ability to gain access to your computer through the Internet can easily be done without your knowledge—and most of them seem to prefer that approach. Before time is spent on being able to detect a hacker, you must understand that a determined hacker cannot be stopped! They will get in—even to the US Department of Defense's systems! In January 2012? a group of hackers (calling themselves by a strange name of Lords of Dharmaraja) broke into Symantec, the makers of the Norton cyber security software suite. Symantec admitted—on Facebook of all places—that "a segment of its source code used in two of our older enterprise products had been accessed." The hackers uploaded a portion of the source code to Pastebin, and though it's since been taken down, the code and the message can be accessed through Google's cache. The very thought of a famous anti-virus software itself having been hacked is frightening. The hackers threatened to release the source code of Symantec's product Norton Anti-virus.

Some common things that might (we repeat, might—that is, not necessarily) tip you off to an intrusion are:

- Lights showing hard drive activity being busier than what your own activities call for
- Suspicious files left on your computer—often in the Windows Temp directory with a tmp. suffix
- Obvious tampering—destroyed files, missing files, etc.

- Or, the worst case—someone's taking money out of your bank account or using your credit cards (Please note, though, that this could also be the result of phishing, too—not necessarily hacking)
- Your firewall keeps receives multiple packets from a single web address and notifies you.

6.2.2. What Firewalls Can Do for You and What They Cannot?

A firewall, at its most basic level, controls traffic flow between a trusted network (such as a corporate LAN) and an un-trusted or public network (such as the Internet). The most commonly deployed firewalls today are port-based (or packet filtering) firewalls, or some variation (such as stateful inspection) of this basic type of firewall. These firewalls are popular because they are relatively simple to operate and maintain, generally inexpensive, have good throughput, and have been the prevalent design for more than two decades.

Port-based firewalls (and their variants) use source/destination IP addresses and TCP/UDP port information to determine whether or not a packet should be allowed to pass between networks or network segments. The firewall inspects the first few bytes of the TCP header in an IP packet to determine the application protocol—for example, SMTP (port 25), and HTTP (port 80).

Most firewalls are configured to allow all traffic originating from the trusted network to pass through to the un-trusted network, unless it is explicitly blocked by a rule. For example, the Simple Network Management Protocol (SNMP) might be explicitly blocked to prevent certain network information from being inadvertently transmitted to the Internet. This would be accomplished by blocking UDP ports 161 and 162, regardless of the source or destination IP address. Static port control is relatively easy. Stateful inspection firewalls address dynamic applications that use more than one well-defined port (such as FTP ports 20 and 21). When a computer or server on the trusted network originates a session with a computer or server on the untrusted network, a connection is established. On stateful packet inspection firewalls, a dynamic rule is temporarily created to allow responses or replies from the computer or server on the un-trusted network. Otherwise, return traffic needs to be explicitly permitted, or access rules need to be manually created on the firewall (which usually isn't practical). All of this works well as long as everyone plays by the rules. Unfortunately, the rules are more like guidelines and not everyone using the Internet is nice!

The Internet has spawned a new generation of applications being accessed by network users for both personal and business use. Many of these applications help improve user and business productivity, while other applications consume large amounts of bandwidth, pose needless security risks, and increase business liabilities—for example, data leaks and compliance—both of which are addressed in the following sections. And many of these applications incorporate "accessibility" techniques, such as using nonstandard ports, port-hopping, and tunneling, to evade traditional port-based firewalls. IT organizations have tried to compensate for deficiencies in traditional port-based firewalls by surrounding them with proxies, intrusion prevention systems, URL filtering, and other costly and complex devices, all of which are equally ineffective in today's application and threat landscape.

Security Administrators design network diagrams placing firewalls and intrusion detection systems at the perimeters of their network and implement these designs. However, the most neglected parts are actually the most important:

- Checking the logs of the firewall (both firewall and system)
- Fully utilizing intrusion detection software

First of all, the firewall logs can collect as much or as little information as the administrator wants. If this information is never examined, then the firewall should not be logging it at all. The configuration of firewalls to log the correct data without logging too much information is an ongoing battle that changes with the topology of the network. The key to successful logging is planning. Before the implementation of the firewall is complete, the administrator should plan out what events he wants to be logged and what information associated with those events should be logged. This is where the education of an administrator really helps out. The security administrator knows what activity should and should not be going on through his firewall. Most firewalls offer user-defined alerts that can send emails or alert pagers to any suspicious activity. However, what if the attacker does not set off any alerts? What if the traffic is legitimate traffic to the firewall, but a box is exploited? The third challenge after logging the information is putting it into a form that can be understood. The faster these events can be brought to the administrator's attention, the less time an hacker has to do his damage. There are many products available that arrange firewall logs in a simple, easy to read, report.

In addition to the firewall logs, the system logs of key boxes should be examined on a routine basis. Lance Spitzner's paper titled, "Watching Your Logs", goes into detail on how to filter your system logs for the correct information and how to put this information in an easy to read form. Security administrators need to be educated to know exactly what logs need to be examined and what triggers should be set up in order to catch illegal activity.

In addition to understanding the alerts, security administrators need to understand the purpose of using both firewalls and mansion detection software. Firewalls are vulnerable to attacks that are allowed to pass through from the outside because of protocol and traffic that never has to hit the firewall. Some examples of this include the hacking of public viewable boxes (DMZ servers) and internal attacks. In computer security, a DMZ (sometimes referred to as a perimeter network) is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military action is not permitted. In the example of DMZ servers. Web servers are the number one target. Since the firewall should allow web traffic to your public web servers, the firewall cannot do anything. However, intrusion detection software can examine the packets traveling to the server for what are called signatures. Signatures are packets that can be identified as having a specific purpose, such as a specific exploit on a web server. The software can then block the packet and in some

cases send packets back to the attacker dropping the connection completely.

Through the proper implementation and use of firewalls and intrusion detection systems, many black hat hacking attempts can be neutralized before they start. However, if one happens to slip by the defenses, the logs of the systems can be used to determine who invaded the network and what kind of damage was done.

6.2.3. How To Fight Back?

6.2.3.1. Locate And Identify The Hacker

In the event that a computer is hacked or probed, the first thing that an administrator does not need to do is retaliate. This solves absolutely nothing and puts the administrator in the same category as the attacker. This also reveals to the hacker that there are actually computer systems out there and someone is monitoring them. This could prompt the attacker to try some different types of attacks. The best thing to do is to gather up enough information about the attack to where the facts can be put together to determine exactly what the attacker did or was trying to do and proceed from there. If it is just a script kiddie scanning a network for possible targets, there is not much that you can do or perhaps need to do. If an administrator tried to track down every person that scanned their network, he would not get very much done. If a computer is hacked, the main thing to determine is whether the hacker is done or he is still on the box. The one thing that needs to happen first is to try and determine where the hack is coming from. An IP address can go a long way in tracking down a hacker. Do not start deleting files off the system. If a hacker sees files magically disappearing, he may decide to get off the computer or delete valuable logs before the administrator can get the information needed to prosecute the hacker. Once an administrator has identified the hacker and has enough information to prosecute him, the box should be removed from the network.

In a perfect world every administrator would be able to catch the hacker in the act. Unfortunately, it does not work this way most of the time. Usually the box is hacked and the administrator discovers this after the hacking. Much research has been devoted to the problem of recovering from attacks. The main things to remember are to remove the box from the network and to not change or delete any files on the disk. Some files may contain certain clues about the identity of the hacker and how long he has been on your box.

6.2.3.1. Honeypots or Honeynets

A honeypot is a network decoy set as a trap to detect and deflect attempts at unauthorized use of information systems. A honeypot is composed of a network site that is isolated, protected, and monitored. The network site appears to contain information or a resource that would be of value to attackers. Honeypots are used to distract adversaries from more valuable devices on a network, to provide early warning regarding new attacks and exploitation trends, and to allow in-depth examination of attackers' behavior. Most antivirus companies use honeypots to capture and study malware. Tools such as honeypots may turn the tables on the hackers. The administrator can collect IP addresses fairly easily and report these addresses to the proper authorities. While honeypots are a good educating tool and a good way to catch some beginner Black Hats in the

act, these boxes should be monitored very closely and should only be implemented on networks by experienced security administrators.

While these boxes can be used to educate administrators as to the ways of hackers, they can also be used to catch hackers. However, a well-configured honeypot is a warning of activity to come. Since honeypots are usually the least secure, these boxes are likely to be the first ones attacked. Alerts spawned by the attacking of these boxes can keep an attacker from moving on to any of the real boxes in a network.

Before setting up a honeypot, an administrator needs to protect his network from the box being compromised. A few rules to remember are as follows:

- Confine the honeypot to its own network. If the box is compromised, ensure that the hacker does not have access to the rest of the production network.
- As an extension of the first point, do not block all outgoing access on the honeypot. If an attacker compromises the box and then cannot get anywhere else, he will get suspicious and leave. This may lead to not gaining enough information about the attacker.
- If network intrusion detection system is being utilized on the network, make sure there are special alerts sent out for any honeypot. These alerts, as mentioned above, can be early warning signs that an attacker is looking at your network.
- Store logs that could be used as evidence off of the honeypot. If a skilled attacker does compromise the box, the first thing that he will do is look to delete or change the logs.
- Keep the honeypot up to date. Do not think that if you are running Windows 2000 SP 1 and IIS 5.0 on all your boxes and your honeypot is running Windows NT 4.0 SP3 with IIS 4.0 that a hacker will not be suspicious and may not attack the box at all.

6.2.3.3. Deception Systems

An amusing way to fight back against attackers is with deception systems. One of the more famous ones is Fred Cohen's Deception Toolkit. This is a combination of the most commonly hacked protocols in one kit. This kit interacts with the attacker so the attacker thinks he is on a real system. Another notable deception systems is the "00[Sub]7", the Ultimate SubSeven Logging Tool by Jeff Capes. One of the most common port scans on a system nowadays is for port 27374, or the SubSeven port. SubSeven is a very powerful Trojan that can do any number of things to a victim's computer. This deception tool looks like a SubSeven server listening on the standard port. It logs all activity that goes on between the client and the fake server. The user can send the attacker a message with the attacker's IP saying that he is being logged as well as some other goodies. This is more of a tool geared toward the home user instead of a corporate environment.

अध्याय 7
Chapter 7

Cyber Crime, History of Cyber Crimes and the Challenges of Fighting Cyber Crime

7.1. What is a cyber crime?

Cyber crime is a generic term that refers to all criminal activities done rising the medium of communication devices computers, mobile phones, tablets etc. in the Internet, cyber space and the worldwide web.

The simplest and one among the first official definition given by group of experts constituted by OCED (Organisation for Economic Co-operation and Development) in 1983. They defined the term computer crime as any illegal, unethical or unauthorised behaviour involving automatic processing and transmission of data. According to Cambridge Dictionary defines that Cyber crime as crime as committed with the use of computers or relating to computer, especially through the internet.

There isn't really a fixed definition for cyber crime. The Indian Law The IT Act, 2000 has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008 the Indian Cyber Law, but "Cyber Security" is defined under Section (2)(nb) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

7.2. What is Cyber Law?

Cyber law (also referred to as Cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, law of torts, privacy, constitutional law and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet. In India The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008 is known as the Cyber law.

7.3. What is Cyber Security?

Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach. Cyber security strategies — for example, the

"Those who work at a thing heart and soul not only achieve success in it but through their absorption in that they also realize the supreme truth – Brahman. Those who work at a thing with their whole heart receive help from God."
- Swami Vivekananda

development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime — can help to reduce the risk of cyber crime. The development and support of cyber security strategies are a vital element in the fight against cybercrime.

The legal, technical and institutional challenges posed by the issue of cyber security are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.

The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

Jurisdiction and sovereignty

History of policing and law is always plaqued with question of jurisdiction and the fight are still on in this cyber era. Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve" the laws of at least three jurisdictions:

1. The laws of the state/nation in which the user resides,
2. The laws of the state/nation that apply where the server hosting the transaction is located, and
3. The laws of the state/nation which apply to the person or business with whom the transaction takes place. So a user in one of the states in USA conducting a transaction with another user in Australia through a server in Mumbai could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. The laws of a nation may have extra-territorial impact extending the jurisdiction beyond the sovereign and territorial limits of that nation. This is particularly problematic as the medium of the Internet does not explicitly recognize sovereignty and territorial limitations. There is no uniform, international jurisdictional law of universal application.

7.4. Cyber attacks and effects

Cyberspace is constantly under assault. Cyber spies, thieves, saboteurs, hackers and thrill seekers break into computer systems, steal Personal data and trade secrets, Vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies.

7.5. History of Cyber Crime

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around

since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.

Today, computers have come a long way with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a billion operations per second. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

The term computer used in this definition does not only mean the conventional desktop or laptop computer. It includes Personal Digital Assistants (PDA), cell phones, sophisticated watches, cars and a host of gadgets. Recent global cyber crime incidents like the targeted denial of service attacks on Estonia have heightened fears. Intelligence agencies are preparing against coordinated cyber attacks that could disrupt rail and air traffic controls, electricity distribution networks, stock markets, banking and insurance systems etc.

Unfortunately, it is not possible to calculate the true social and financial impact of cyber crime. This is because most crimes go unreported.

7.5.1 What's a cyber crime, and what's not?

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web. There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point and even after its amendment the Information Technology Act, 2000 does not define the term.

The offences covered under Chapter XI of the Indian Information Technology Act, 2000 include:

- Tampering with the computer source code or computer source documents
- Hacking
- Data Theft
- Spreading Virus & Computer Contaminants
- Damaging Computers and Computer Network

"All who have actually attained any real religious experience never wrangle over the form in which the different religions are expressed. They know that the soul of all religions is the same and so they have no quarrel with anybody just because he or she does not speak in the same tongue." ***- Swami Vivekananda***

- DoS Attacks
- Abating Crimes
- Data Destruction
- Source Code Theft
- Publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest.
- Failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign state, public order or for preventing incitement to the commission of any cognizable offence.
- Securing access or attempting to secure access to a protected system.
- Misrepresentation while obtaining, any licence to act as a Certifying Authority or a digital signature certificate.
- Breach of confidentiality and privacy publication of digital signature certificates which are false in certain particulars Publication of digital signature certificates for fraudulent purposes.

7.6. The Challenges of Fighting Cybercrime

Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation. This chapter focuses on the challenges of fighting cybercrime.

7.6.1. Opportunities

Law enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures.

It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed was not modified.

Forensic software is able to search automatically for child pornographic images by comparing the files on the hard disk of suspects with information about known images. For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification the offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face. Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.

Revolution did not necessarily involve sanguinary strife. It was not a cult of bomb and pistol.
- Shahid Bhaghat Singh

7.6.2. General Challenges

7.6.2.1. Reliance on ICTs

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e-mail communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services. The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.

Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures. Even short interruptions to services could cause huge financial damages to e-commerce businesses - not only civil communications could be interrupted by attacks; the dependence on ICTs is a major risk for military communications.

Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system, so offenders can design effective attacks by concentrating on this single target.

The dependence of society on ICTs is not limited to the western countries - developing countries also face challenges in preventing attacks against their infrastructure and users. The development of cheaper infrastructure technologies such as WiMAX has enabled developing countries to offer Internet services to more people. Developing countries can avoid the mistakes of some western countries that concentrated mainly on maximizing accessibility, without investing significantly in protection. US experts explained that successful attacks against the official website of governmental organisations in Estonia could only take place due to inadequate protection measures. Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run.

Strategies must be developed to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling the law enforcement to fight cybercrime effectively.

7.6.2.2. Number of Users

The popularity of the Internet and its services is growing fast, with over 1 billion Internet users worldwide. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware and wireless access will enable even more people to access the Internet. With the growing number of people connected to the Internet, the number of targets and offenders increases. It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million. Although Internet usage rates are lower in developing countries, promoting cybersecurity is not easier, as offenders can commit offences from around the world.

The increasing number of Internet users causes difficulties for the law enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can rather easily be carried out, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed was not modified.

7.6.2.3. Availability of Devices and Access

Only basic equipment is needed to commit computer crimes, which generally requires the following elements:

- Hardware;
- Software; and
- Internet Access.

With regards to hardware, the power of computers grows continuously. There are a number of initiatives to enable people in developing countries to use ICTs more widely. Criminals can commit serious computer crimes with only cheap or second-hand computer technology - knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes.

Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.

The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialised countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so called "wardriving". The term describes the act of driving around searching for accessible wireless networks. The most common was of access to network connections by offenders are:

- Public Internet terminals;,
- Open (wireless) networks;
- Hacked networks; and
- Prepaid services without registration requirements.

Law enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users. However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate

the investigation of law enforcement agencies, such legislation could hinder the growth of the information society and development of e-commerce. It has been suggested that this limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case Autronic v. Switzerland, the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

7.6.2.4. Availability of Information

The Internet has millions of web pages of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia, an online encyclopedia where anybody can publish.

The success of the Internet also depends on powerful search engines that enable the users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. "Googlehacking" or "Googledorks" describes the use of complex search engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password protection systems. Reports have highlighted the risk of the use of search engines for illegal purposes. An offender, who plans an attacks can find detailed information on the Internet that explain how to build a bomb by using only those chemicals that are available in regular supermarkets. Although information like this was available even before the Internet was developed, it was however, much more difficult to get access to that information. Today any Internet user can get access to those instructions.

Criminals can also use search engines to analyze targets. A training manual was found during investigations against members of a terrorist group highlighting how useful the Internet is for gathering information on possible targets. Using search engines, offenders can collect publicly available information (e.g., construction plans from public buildings) that help in their preparations. It has been reported that insurgents attacking British troops in Afghanistan used satellite images from Google Earth.

7.6.2.5. Missing Mechanisms of Control

All mass communication networks - from phone networks used for voice phone calls to the Internet -need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and even transnational communication infrastructure. The Internet also needs to be governed by laws and law-makers and law enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

The Internet was originally designed as a military network based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked. As a result, the Internet's network infrastructure

is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network.

Today, the Internet is increasingly used for civil services. With the shift from military to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed from military purposes, these central control instruments do not exist and it is difficult to implement them retrospectively, without significant redesign of the network. The absence of control instruments makes cybercrime investigations very difficult.

One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology using encrypted anonymous communication services. If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites. But the blocking of illegal content can be avoided, if customers use an anonymous communication server encrypting communications between them and the central server. In this case, providers may be unable to block requests because requests sent as encrypted messages cannot be opened by access providers.

7.6.2.6. International Dimensions

Many data transfer processes affect more than one country. The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked. Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to its final destination. Further, many Internet services are based on services from abroad e.g., host providers may offer webspace for rent in one country based on hardware in another.

If offenders and targets are located in different countries, cybercrime investigations need the cooperation of law enforcement agencies in all countries affected. National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities. Cybercrime investigations need the support and involvement of authorities in all countries involved.

It is difficult to base cooperation in cybercrime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations. Investigations often occur in very short timeframes. Data vital for tracing offences are often deleted after only a short time. This short investigation period is problematic, because. traditional mutual legal assistance regime often takes time to organise. The principle of dual criminality also poses difficulties, if the offence is not criminalised in one of the countries involved in the investigation. Offenders may be deliberately including third countries in their attacks to make investigation more difficult.

Criminals may deliberately choose targets outside their own country and acting from countries with inadequate cybercrime legislation. The harmonisation of cybercrime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cybercrime investigations are the G8 24/7 Network and the provisions related to international cooperation in the Council of Europe Convention on Cybercrime.

7.6.2.7. Independence of Location and Presence at the Crime Site

Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyber-offences are transnational. International cybercrime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cybercrime legislation. Preventing "safe havens" is one of the key challenges in the fight against cybercrime. While "safe havens" exist, offenders will use them to hamper investigation. Developing countries that have not yet implemented cybercrime legislation may become vulnerable, as criminals may choose to base themselves in these countries to avoid prosecution. Serious offences affecting victims all over the world may be difficult to stop, due to insufficient legislation in the country where offenders are located. This may lead to pressure on specific countries to pass legislation. One example of this is the "Love Bug" computer worm developed by a suspect in the Philippines in 2000, which infected millions of computers worldwide. Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalised in the Philippines. Another example is Nigeria, which has come under pressure to take action over financial scams distributed by e-mail.

7.6.2.8. Automation

One of the greatest advantages of ICTs is the ability to automate certain processes. Automation has several major consequences:

- It increases the speed of processes;
- It increases the scale and impact of processes;
- It limits the involvement of humans.

Automation reduces the need for cost-intensive manpower, allowing providers to offer services at lower prices. Offenders can use automation to scale up their activities - many millions of unsolicited bulk spam messages can be sent out by automation. Hacking attacks are often also now automated, with as many as 80 million hacking attacks every day due to the use of software tools that can attack thousands of computer systems in hours. By automating processes offenders can gain great profit by designing scams that are based on a high number of offences with a relatively low loss for each victim. The lower the single loss is the higher is the chance that the victim will not report the offence.

Automation of attacks affects developing countries in particular. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialised countries. The greater numbers of crimes that can be committed through automation pose challenges for law enforcement agencies worldwide, as they will have to be prepared for many more victims within their jurisdictions.

7.6.2.9. Resources

Modern computer systems that are now coming onto the market are powerful and can be used to extend criminal activities. But it is not just increasing power of single-user computers that poses problems for investigations. Increasing network capacities is also a major issue.

One example is the recent attacks against government websites in Estonia. Analysis of the attacks suggests that they were committed by thousands of computers within a "botnet" or group of compromised computers running programs under external control. In most cases, computers are infected with malicious software that installs tools allowing perpetrators to take control. Botnets are used to gather information about targets or for high-level attacks.

Over recent years, botnets have become a serious risk for cybersecurity. The size of a botnet can vary, from a few computers to more than a million computers. Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet. Botnets can be used for various criminal activities, including:

- Denial of Service attacks;
- Sending out spam;
- Hacking attacks; and
- File-sharing networks.

They increase both the computer and network capacity of criminals. Using thousands of computer systems, criminals can attack computer systems that would be out of reach with only a few computers to lead the attack. Botnets also make it more difficult to trace the original offender, as the initial traces only lead to the member of the botnets. As criminals control more powerful computer systems and networks, the gap between the capacities of investigating authorities and those under control of criminals is getting wider.

7.6.2.10. Speed of Data Exchange Processes

The transfer of an e-mail between countries takes only a few seconds. This short period of time is one reason for the success of the Internet, as e-mails have eliminated the time for the physical transport of a message. However, this rapid transfer leaves little time for law enforcement agencies to investigate or collect evidence. Traditional investigations take much longer.

One example is the exchange of child pornography. In the past, pornographic videos were handed over or transported to buyers. Both the handover and transport gave law enforcement agencies the opportunity to investigate. The main difference between the exchange of child pornography on and off the Internet is transportation. When offenders use the Internet, movies can be exchanged in seconds.

E-mails also demonstrate the importance of immediate response tools that can be used immediately. For tracing and identifying suspects, investigators often need access to data that may be deleted shortly after transfer. A very short response time by the investigative authorities is often vital for a successful investigation. Without adequate legislation and instruments allowing investigators to act immediately and prevent data from being deleted, an effective fight against cybercrime may not be possible.

"Quick freeze procedures" and 24/7 network points are examples for tools that can speed up investigations. Data retention legislation also aims to increase the time available for law enforcement

agencies to carry out investigations. If the data necessary to trace offenders are preserved for a length of time, law enforcement agencies have a better chance of identifying suspects successfully.

7.6.2.11 Speed of Development

The Internet is constantly undergoing development. The creation of a graphical user interface (WWW) marked the start of its dramatic expansion, as previous command-based services were less user-friendly. The creation of the WWW has enabled new applications, as well as new crimes - law enforcement agencies are struggling to keep up. Further developments continue, notably with:

- Online games; and
- Voice over IP (VoIP) communications.

Online games are ever more popular, but it is unclear whether law enforcement agencies can successfully investigate and prosecute offences committed in this virtual world.

The switch from traditional voice calls to Internet telephony also presents new challenges for law enforcement agencies. The techniques and routines developed by law enforcement agencies to intercept classic phone calls do not generally apply to VoIP communications. The interception of traditional voice calls is usually carried out through telecom providers. Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners. Therefore, new techniques are needed.

New hardware devices with network technology are also developing rapidly. The latest home entertainment systems turn TVs into Internet Access Points, while more recent mobile handsets store data and connect to the Internet via wireless networks. USB (Universal Serial Bus) memory devices with more than 1 GB capacity have been integrated into watches, pens and pocket knives. Law enforcement agencies need to take these developments into account in their work - it is essential to educate officers involved in cybercrime investigations continuously, so they are up-to-date with the latest technology and able to identify relevant hardware and any specific devices that need to be seized.

Another challenge is the use of wireless access points. The expansion of wireless Internet access in developing countries is an opportunity, as well as a challenge for law enforcement agencies. If offenders use wireless access-points that do not require registration, it is more challenging for law enforcement agencies to trace offenders, as investigations lead only to access points.

7.6.2.12. Anonymous Communications

Certain Internet services make it difficult to identify offenders. The possibility of anonymous communication is either just a by-product of a service or offered with the intention to avoid disadvantages for the user. Examples for such services — that can even be combined are:

- Public Internet terminals (e.g., at airport terminals or Internet cafes);
- Wireless networks;

- Prepaid mobile services that do not need registration;
- Storage capacities for homepages offered without registration;
- Anonymous communication servers;
- Anonymous remailers.

Offenders can hide their identities through, for example, the use of fake e-mail addresses. Many providers offer free e-mail addresses. Where personal information should be entered, it may not be verified, so users can register e-mail addresses without revealing their identity. Anonymous e-mail addresses can be useful e.g., if users wish to join political discussion groups without identification. Anonymous communications may give rise to anti-social behaviour, but they can also allow users to act more freely.

Taking into consideration the various traces the users leave clarifies the need to enable instruments to prevent the user from profiling activities. Therefore various states and organizations support the principle of anonymous use of Internet e-mail services e.g., this principle is expressed in the European Union Directive on Privacy and Electronic Communications. One example of a legal approach to protect user privacy can be found in Article 37 of the European Union Regulation on Data Protection. However, some countries are addressing the challenges of anonymous communications by implementing legal restrictions — one example is Italy, which requires public Internet access providers to identify users, before they start using the service.

These measures aim to help law enforcement agencies identify suspects, but they can be easily avoided - criminals may use unprotected private wireless networks or SIM-cards from countries not requiring registration. It is unclear whether the restriction of anonymous communications and anonymous access to the Internet should play a more important role in cyber security strategies.

7.6.2.13 Encryption Technology

Another factor that can complicate the investigation of cybercrime is encryption technology, which protects information from access by unauthorized people and is a key technical solution in the fight against cybercrime. Like anonymity, encryption is not new, but computer technology has transformed the field. It is now possible to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data. It is uncertain to what extent offenders already use encryption technology to mask their activities — for example, it has been reported that terrorists are using encryption technology. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology but experts highlight the threat for an increasing use of encryption technology in Cybercrime cases.

Tools are available to break encryption. Various software products are available enabling users to protect files against unauthorized access. It is possible, but often difficult and slow, to break encryption — if investigators have access to the software used to encrypt files, they may be able to unpick the encryption. Alternatively, they may be able to break the encryption through, for example, a brute force attack.

Depending on encryption technique and key size, it could take decades to break an encryption. For example, if an offender uses encryption software with a 20-bit encryption, the size of the keyspace is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption. Using a 56-bit encryption, a single computer would take up to 2,285 years to break the encryption. If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billion years to break it. The latest version of the popular encryption software PGP permits 1024-bit encryption.

Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft's operating Systems, for example, allows the encryption of an entire hard disk. Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them, the widespread availability of this technology for any user could result in greater use of encryption. Tools are also available to encrypt communications — for example, e-mails and phone calls can be sent using VoIP. Using encrypted VoIP technology, offenders can protect voice conversations from interception.

Techniques can also be combined. Using software tools, offenders can encrypt messages and exchange them in pictures or images — this technology is called steganography. For investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.

The availability and use of encryption technologies by criminals is a challenge for law enforcement agencies. Various legal approaches to address the problem are currently under discussion, including: potential obligations for software developers to install a back-door for law enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations. But encryption technology is not only used by offenders — there are various ways such technology is used for legal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks, self-protection is an important element of cyber security.

Summary

The investigation and prosecution of cybercrime presents a number of challenges for law enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime, but also to draft adequate and effective legislation. This section has reviewed key challenges to promoting cybersecurity and areas where existing instruments may prove insufficient and the implementation of special instruments may be necessary.

In our desire for eternal life we pray for an eternity of our habit and comfort, forgetting that immortality is in repeatedly transcending the definite forms of life in order to pursue the infinite truth of life.
- Sir Rabindranath Tagore

अध्याय 8

Chapter 8

Cyber Crime : Mobile and Wireless Devices

8.1. Introduction

In this modern era, the rising importance of electronic gadgets (i.e., mobile hand-held devices) which became an integral part of business, providing connectivity with the Internet outside the office — brings many challenges to secure these devices from being a victim of cybercrime. In the recent years, the use of laptops, personal digital assistants (PDAs), and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment. According to Quocirca Insight Report (2009), by the end of 2008 around 1.5 billion individuals around the world had the Internet access. In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the Smartphone.

Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. Although IT departments of organizations as yet are not swapping employees' company-provided PDAs (as the case may be) for the Smartphones, many users may bring these devices from home and use them in the office. Research in Motions (RIM) Blackberry Wireless Hand-held is an alternate technology. According to Research in Motion Annual Report (2009) there are over 175,000 organizations with BlackBerry Enterprise Server installed behind the corporate firewall (i.e., corporations that use the BlackBerry enterprise server and client/server software for data communication between corporate BlackBerry devices and other mail systems). Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

8.2. Proliferation of Mobile and Wireless Devices

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Let us understand the concept of mobile computing and the various types of devices.

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

- **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
- **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
- **Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
- **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
- **Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
- **Smartphone:** It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
- **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
- **Fly Fusion Pentop computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop, that is, not tethered. As more personal devices find their way into the enterprise, corporations are realizing cybersecurity threats that come along with the benefits achieved with mobile solutions.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all. Thus, while "wireless" is a subset of "mobile," in most cases, an application can be mobile without being wireless. Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have

software installed on them; this includes networked PDAs and Smartphones. In this chapter the term "hand-held" is used as an all-embracing term.

8.3. Trends in Mobility

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.

To assess major challenges in the mobility domain, let us see the statistics found during the surveys. In one such survey, reported by Quocirca, employees working in government departments have lost or mislaid over 1,000 laptops, lost more than 500 phones or mobile E-Mail gadgets and lost over 700 other mobile devices (i.e., probably memory sticks, cameras, etc.). Another such survey, reported by Quocirca, of the 2,853 respondents, 29% had a broad experience of wireless laptops, 14% had a broad experience of smart hand-helds, with around a further 60% in each case having a more limited or unofficial experience. Findings from surveys like these help us demystify many perceptions about mobile and wireless connectivities. The results of surveys like these indicate that we are grappling with a "perception problem"; most people have not as yet come to terms with the fact that the hand-held devices may look "harmless" but they can cause serious cybersecuriry issues to the organizations.

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operators networks - and the other is within the mobile networks — that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Key Findings for Mobile Computing Security Scenario

1. **With usage experience, awareness of mobile users gets enhanced:** Survey showed that those with broad wireless laptop experience place less emphasis on this aspect for the deployment of smart hand-helds. However, an experience of small hand-held deployment boosted the numbers seeing the need for increased provision of user support and training.

2. **People continue to remain the weakest link for laptop security:** Antivirus software, secured virtual private network (VPN) access and personal firewalls are deployed over two-thirds of IT professionals, but those with a broad wireless experience regard loss, damage or unauthorized use as their major concerns. These depend on the care taken by the users and well-communicated security policies.

3. **Wireless connectivity does little to increase burden of managing laptops:** The cost and complexity of device management is seen as an issue by around half of the IT professionals surveyed. However, the level of challenge perceived to affect security, device management and use support is unaffected by a broader experience of wireless laptop deployment.

4. **Laptop experience changes the view of starting a smart hand-held pilot:** The key concerns for starting a smart hand-held are security and the cost of devices, but these lessen for those with a broad wireless laptop experience. However, the concern over choosing the most appropriate devices rises with experience; users cite further concerns over interoperability and compatibility.

5. **There is naivety and/or neglect in smart hand-held security:** Although plenty of emphasis is placed on security, a large number of IT departments do not enforce security for smart hand-helds as well as for laptops or they leave it in the hands of the users. This is more prevalent in those with limited or unofficial smart hand-held activity, but even those with a broad experience (almost one-third of those surveyed) do not treat smart hand-held security as seriously as laptops.

6. **Rules rather than technology keep smart hand-helds' usage in check:** Businesses with an existing experience of smart hand-helds favored a policy of controlled deployment, with almost two-thirds of those surveyed providing a limited choice of devices, and only one-third of the surveyed population was user of technology solution based on continuous synchronization. However, broad experience increases the use of other automated solutions, such as centralized software management and remote device deactivation.

Popular types of attacks against 3G mobile networks are as follows:

1. **Malwares, viruses and worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

   - **Skull Trojan:** It targets Series 60 phones equipped with the Symbian mobile OS.
   - **Cabir Worm:** It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
   - **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
   - **Brador Trojan:** It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.
   - **Lasco Worm:** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir s source code and replicates over Bluetooth connection.

2. **Denial-of-service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber-securiry threats to wired Internet service providers (ISPs) is a distributed denial-of-service (DDoS) attack. DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped. Botnets/zombies are used to create enough traffic to impose that kind of damage.

3. **Overbilling attack:** Overbilling involves an attacker hijacking a subscribers IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. **Spoofed policy development process (PDP):** These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

5. **Signaling-level attacks:** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

8.4. Credit Card Frauds in Mobile and Wireless Computing Era

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming common place given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Mobile credit card transactions are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.

Today belongs to "mobile computing," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment. These businesses include mobile utility repair service businesses, locksmiths, mobile windshield repair and others. Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers.

Tips to Prevent Credit Card Frauds

The current topic is about credit card frauds in mobile and wireless computing era, however, we would like to include these tips to prevent credit card frauds caused due to individual ignorance about a few known facts.

Do's

1. Put your signature on the card immediately upon its receipt.

2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
3. Change the default personal identification number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Dont's

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

There is a system available from an Australian company "Alacrity" called closed-loop environment for wireless (CLEW). The Figure shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in following Figure the basic flow is as follows:

1. Merchant sends a transaction to bank;
2. the bank transmits the request to the authorized cardholder [not short message service (SMS)];
3. the cardholder approves or rejects (password protected);

4. the bank/merchant is notified;

5. the credit card transaction is completed.

8.4.1. Types and Techniques of Credit Card Frauds

Traditional Techniques

The traditional and the first type of credit card fraud is paper-based fraud — application fraud, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information(PII) to open an account in someone else's name.

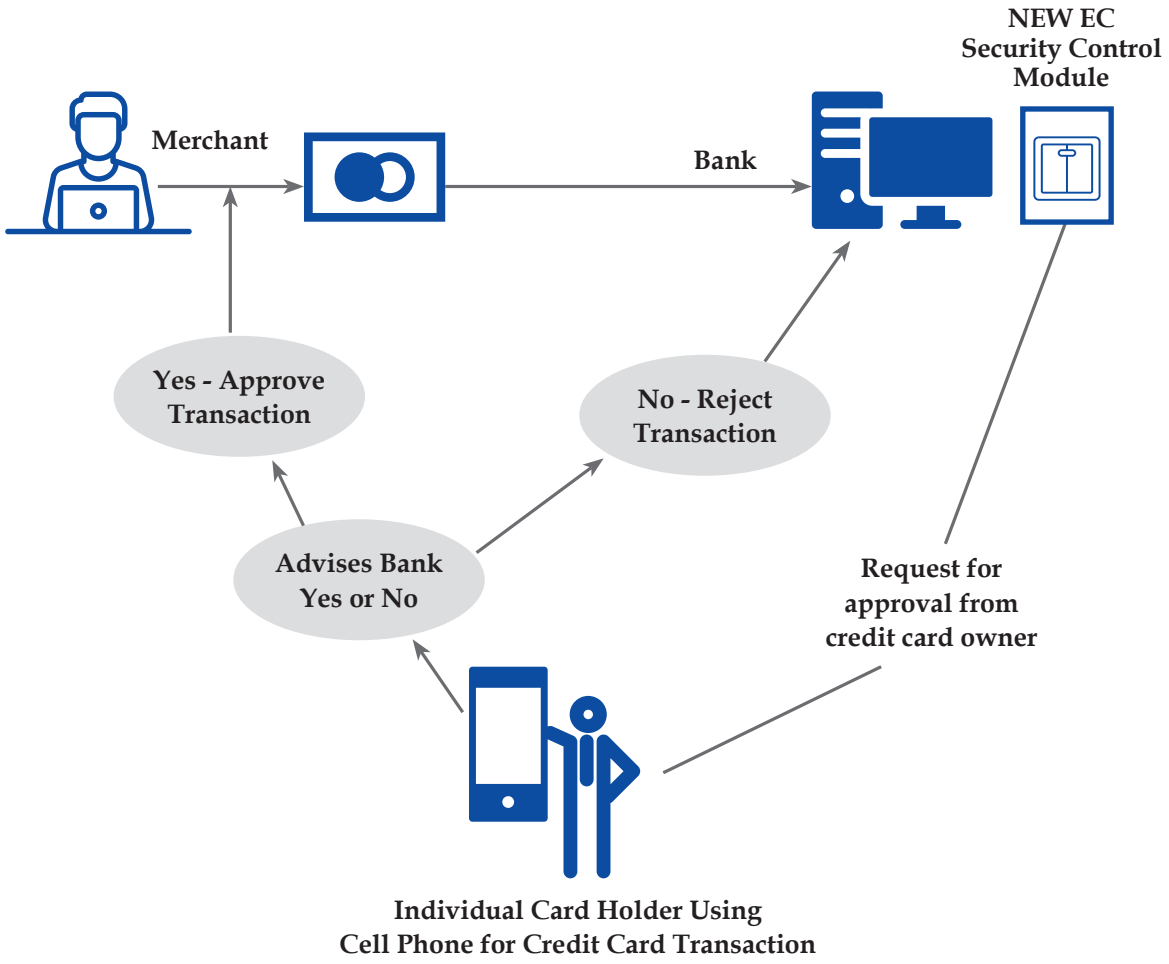


Fig. Closed-Loop Environment for Wireless (CLEW)

Potential Wireless Users - Beware!

Although wireless processing is a very good system for many companies, however, it is not for all mobile businesses. There are some drawbacks to wireless processing that many potential wireless users should be aware of before they venture into wireless processing. They are as follows:

1. **Wireless processing equipment is expensive:** There is no way to get around this. Wireless credit card machines are the most advanced processing terminals available. You get what you pay for! For a wireless terminal with a printer, expect to pay at least US$ 800 for a new

terminal and US$ 700 for a refurbished terminal. If you are purchasing a terminal that is much cheaper than any other you find, it is most likely outdated equipment that uses outdated cellular networks. In other words, it is a scam, and you are about to buy a really expensive paperweight.

2. **Wireless processing comes with extra fees:** Just like a cell phone, wireless credit card machines operate on cellular networks. You have to pay for this cellular service in addition to the high cost of equipment. Luckily, wireless fees for processing are nowhere near what they are for cell phones. Expect to pay US$ 20-25 per month for a wireless service fee.
3. **Wireless credit card machines are subject to cellular coverage blackouts:** I know what you are thinking - "My cell phone works almost everywhere, so my wireless credit card machine will too." Sadly, this is not the case. Wireless credit card processing uses a business cellular network called the Motient or Mobitex network. Your cell phone may be using a network called code division multiple access (CDMA) or time division multiple access (TDMA) [global system for mobile communications (GSM)] or some other technology-based network. The coverage that your cell phone gets is much greater than the wireless processing network. There can be some states in your country with no coverage for wireless processing at all.
4. **You cannot process checks or debit transactions over a wireless network:** Currently owing to federal regulations, it is impossible to process debit transaction or electronic checks over a wireless network. This is something that will probably end up being allowed in the future, but as of now there is not sufficient security or encryption to process these transactions wireless.

Application fraud can be divided into

- **ID theft:** Where an individual pretends to be someone else
- **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit.

Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

Modern Techniques

Sophisticated techniques enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud. Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another. Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing. Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink/website (i.e., they have been scammed).

1. **Triangulation:** It is another method of credit card fraud and works in the fashion as explained further.

- The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
- The customer registers on this website with his/her name, address, shipping address and valid credit card details.
- The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's website.
- The goods are shipped to the customer and the transaction gets completed.
- The criminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

Such websites are usually available for few weeks/months, till the authorities track the websites through which the criminal has enticed the individuals to reveal their personal details, which enabled the criminal to commit the transactions by using the credit card details of these customers. The entire investigation process for tracking and reaching these criminals is time-consuming, and the criminals may close such fake website in between the process that may cause further difficulty to trace the criminal. The criminals aim to create a great deal of confusion for the authorities so that they can operate long enough to accumulate a vast amount of goods purchased through such fraudulent transactions.

2. **Credit card generators:** It is another modern technique - computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

8.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of die ones shown in the following figure.

As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro challenges.'' Of these, some micro challenges are discussed in this section and macro-challenges in the next section.

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security etc. In this section,

"One individual may die for an idea; but that idea will, after his death, incarnate itself in a thousand lives. That is how the wheel of evolution moves on and the ideas and dreams of one nation are bequeathed to the next."
- Netaji Subhash Chandra Bose

we provide a brief discussion on these cyber security aspects. For most of the discussion here, the reference point is Windows mobile development given that the developers of the Windows OS are on the forefront of the technology in terms of their mobile computing technological initiatives. The ID theft is now becoming a major fraud in credit card business domain, wherein individual's Personally Identifiable Information (PII) is misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victims name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care.

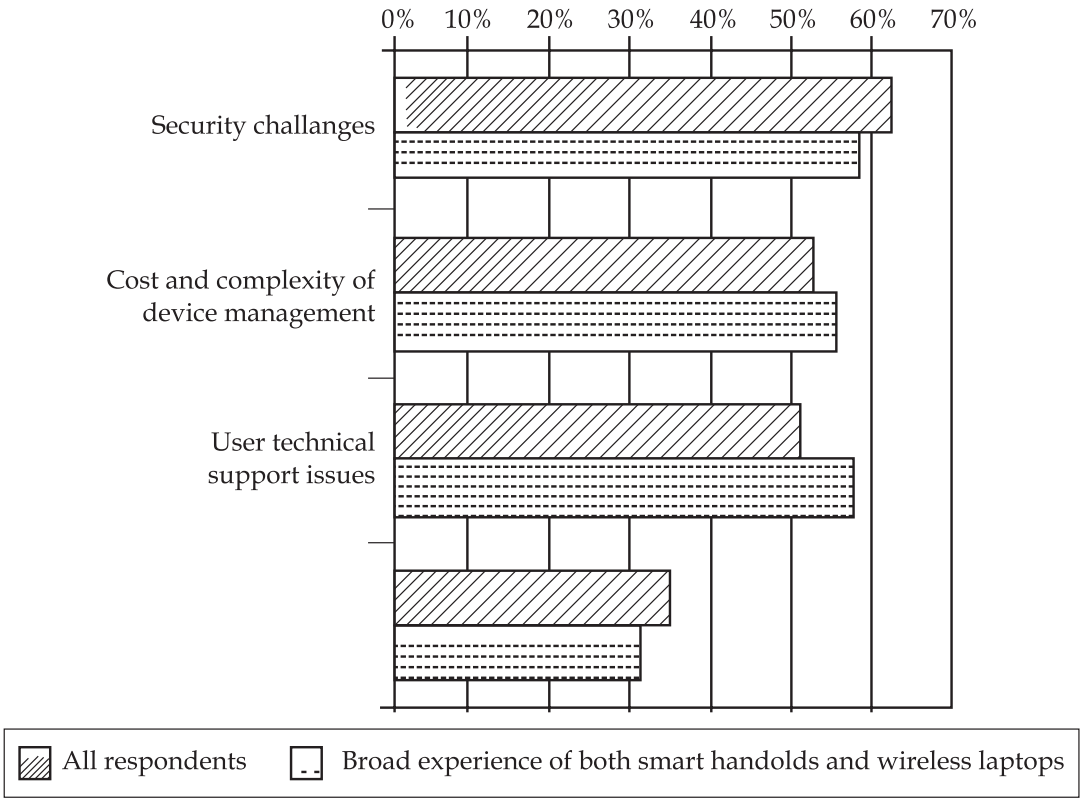


Fig. Important Issues for Managing Mobile Devices

8.6. Registry Settings for Mobile Devices

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. "ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling-the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Taking shelter in the dead is death itself, and only taking all the risk of life to the fullest extent is living.
- Sir Rabindranath Tagore

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within "group policy." Group policy is one of the core operations that are performed by Windows Active Directory. As a supporting point, consider the following: within the last 2 years, Microsoft has doubled the number of group policy settings that it ships with the OS. There are now nearly 1,700 settings in a standard group policy. The emphasis on most of the group policy settings is security.

There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against Spyware, viruses, worms, malware and other Malicious Codes that run through the networks and the Internet. Microsoft and other companies are trying to develop solutions as fast as they can, but the core problem is still not being addressed. According to the experts, the core problem to many of the mobile security issues on a Windows platform is that the baseline security is not configured properly. When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every Control Panel setting and group policy option, they may not get the computer to the desired baseline security. For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional registry changes that are nor exposed through any interface. There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.

Naive users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of "registry hacks" that are discussed in Microsoft Knowledge Base articles.

8.7. Authentication Service Security

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves mutual authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.

Authentication services security is important given the typical attacks on mobile devices through wireless networks: DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

8.7.1. Cryptographic Security for Mobile Devices

In this section we will discuss a technique known as cryptographically generated addresses (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address. The address the owner uses is the corresponding

private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices. CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery and mobility protocols. It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms are one of the most common hand-held devices used in mobile computing. Cryptographic security controls are deployed on these devices. For example, the Cryptographic Provider Manager (CPM) in Palm OSS is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of ail data and resources on the device.

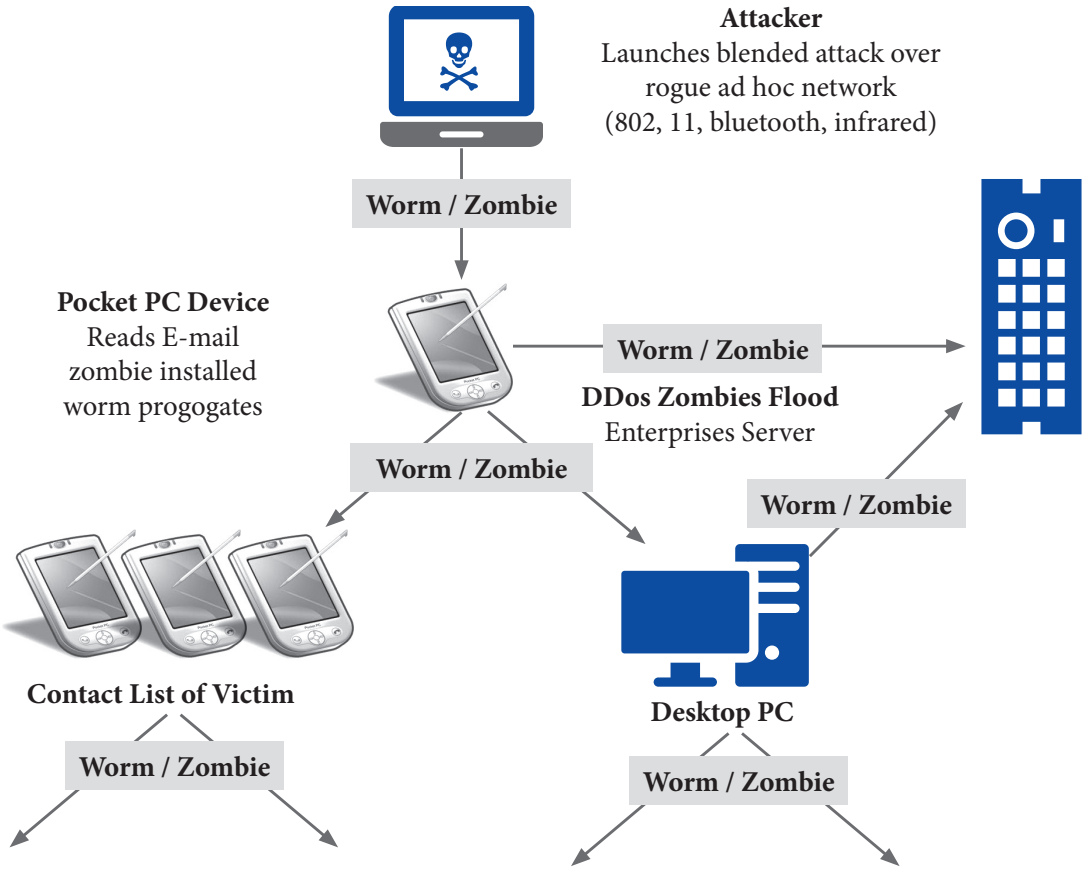


Fig. Push Attack on Mobile Devices. DDoS Implies Distributed Denial-of-Service Attack

8.7.2. LDAP Security for Hand-Held Mobile Computing Devices

LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organization's Intranet). In a network, a directory tells you where an entity is located in the network. LDAP is a light weight (smaller amount of code) version of Directory Access Protocol (DAP) because it does

not include security features in its initial version. It originated at the University of Michigan and has been endorsed by at least 40 companies. Centralized directories such as LDAP make revoking permissions quick and easy.

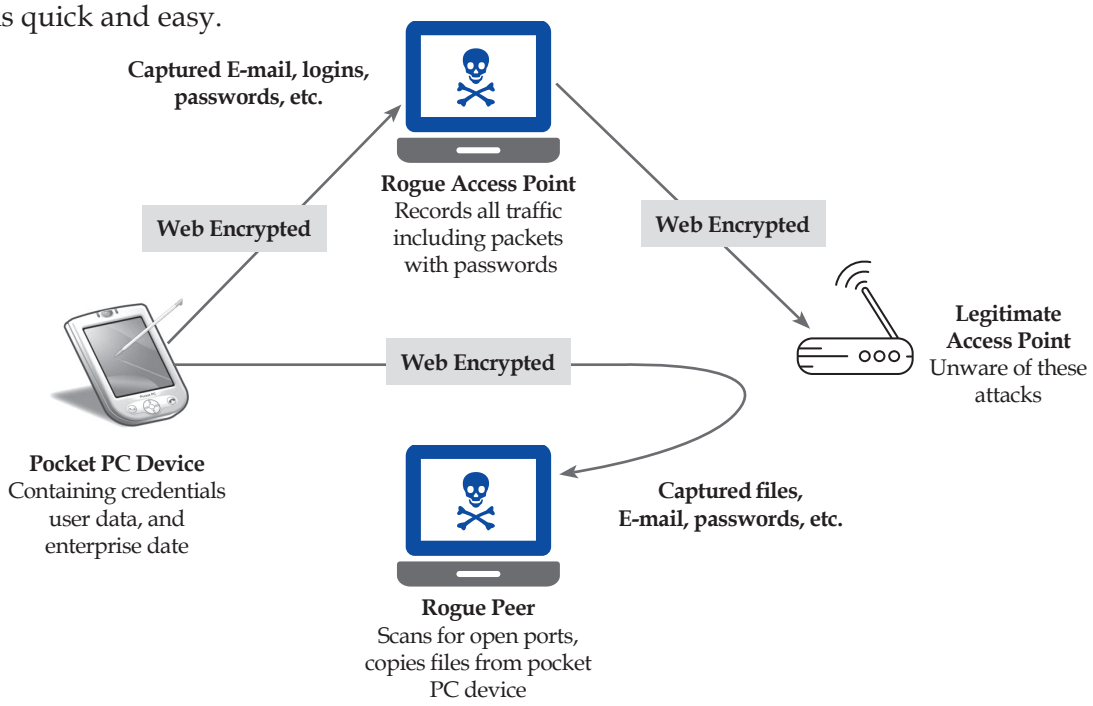


Fig. Pull Attack on Mobile Devices

8.7.3. RAS Security for Mobile Devices

RAS is an important consideration for protecting the business-sensitive data that may - reside on the employees' mobile devices. In terms of cybersecurity, mobile devices are sensitive. The following figure illustrates how access to an organization's sensitive data can happen through mobile hand-held devices carried by employees. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (impersonating or masquerading) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

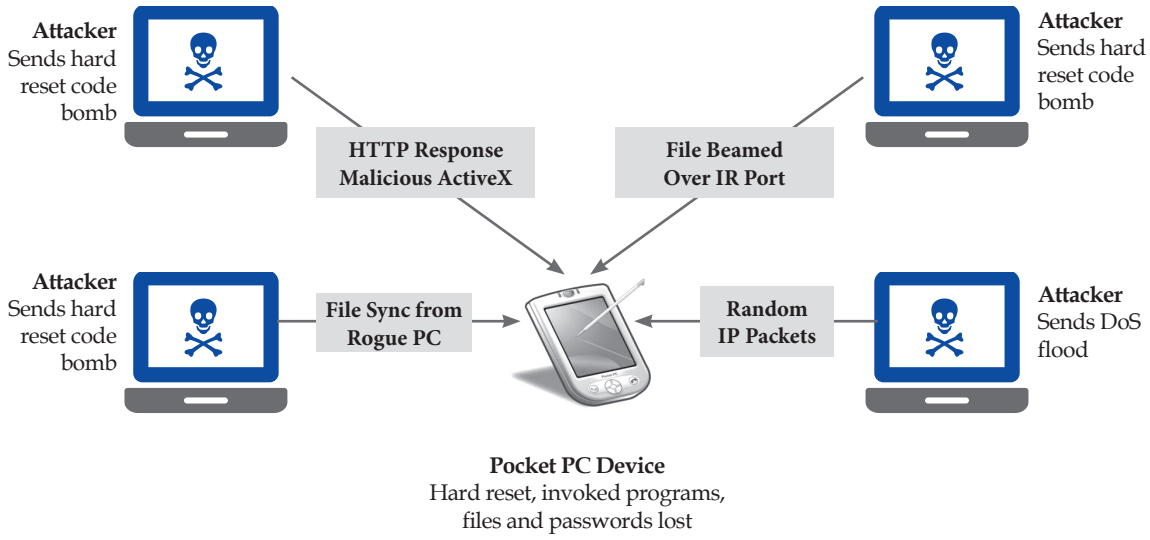


Fig. Crash Attack on Mobile Devices. DoS - Denial-of-Service Attack

Another threat comes from the practice of port scanning. First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer (either the mobile device itself or a gateway server to which it connects). A domain is a collection of sites that are related in some sense. Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls. For instance, File Transfer Protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers.

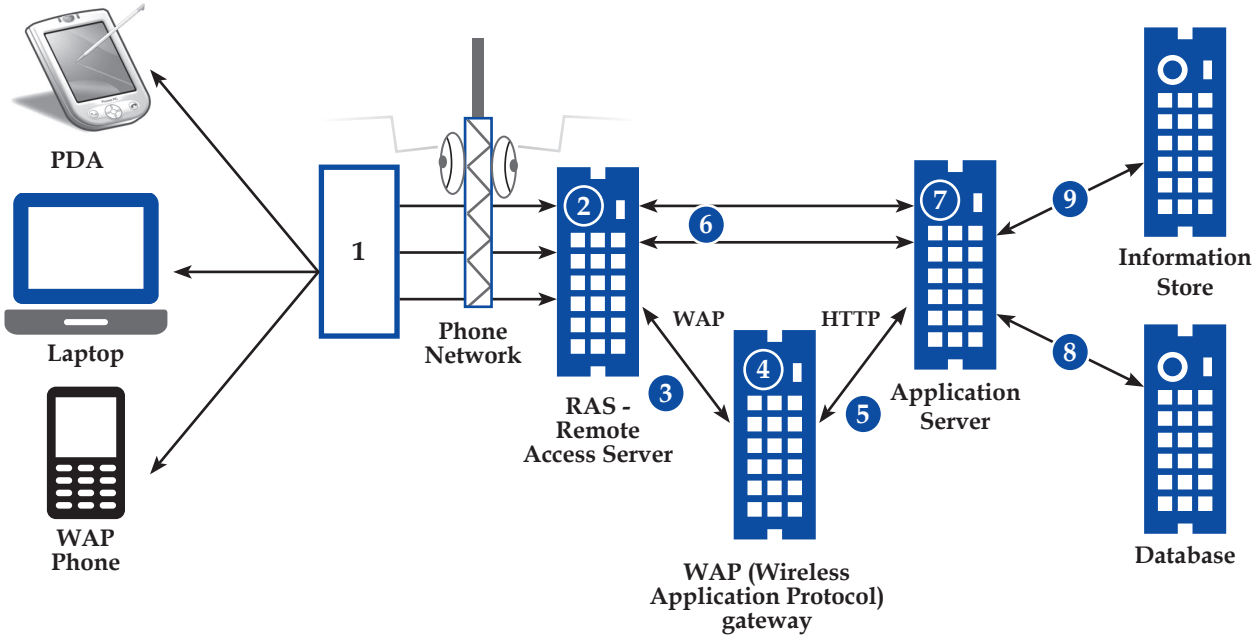


Fig. Communication from Mobile Client to Organization Information Store

Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID. A personal firewall on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement strong authentication keys will provide an additional protection.

RAS System Security for Mobile Device Clients

- The security of a RAS system can be divided into following three' areas:
- The security of the RAS server;
- the security of the RAS client;
- the security of data transmission.

Although the desired level of security of the RAS server can be controlled through implementation of local security guidelines, the RAS client (e.g., a mobile hand-held device) is typically not under the complete control of the IT personnel who is responsible for the local area network (LAN). The security of the data transmission media is generally completely out of their control. For this reason, protection of communications between the client and the server must be secured by additional means.

8.7.4. Media Player Control Security

Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment. Music and video are the two important aspects in day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for cybersecurity breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways." There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this. According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack peoples computer systems and perform a variety of actions. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computers owner is allowed to do, such as opening files or accessing certain parts of a network.

As another example, consider the following news item of the year 2004: corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer. With this happening, there are three vulnerabilities: (a) files could be created that will open a website on the user's browser (e.g., the user could be accessing from his/her hand-held device) from where remote JavaScript can be operated; (b) files could be created which allow the attacker to download and use the code on a users machine or (c) media files could be created that will create buffer overrun errors.

Registry of a computing device is an important concept; it stores information necessary to configure the system for applications and hardware devices. It also contains information that the OS continually references during an operation. In the registry, some keys control the behavior of the Windows Media Player control. Microsoft, through its developer network MSDN, describes details of registry value settings on the, mobile devices. With the increase in our mobile workforce and the resulting increase in the number of mobile computing hand-held devices used by the young employees of most IT and software organizations, it would be quite common to expect such cybersecurity attacks and hence one should be ready for security measures.

8.7.5. Networking API Security for Mobile Computing Applications

With the advent of electronic commerce (E-Commerce) and its further off-shoot into M-Commerce, online payments are becoming a common phenomenon with the payment gateways accessed remotely and possibly wirelessly. Furthermore, with the advent of Web services and their use in mobile computing applications the API becomes an important consideration.

Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.

Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices). Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of Consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.

8.8. Attacks on Mobile / Cell Phones

8.8.1. Mobile Phone Theft

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)" that really matter, are lost.

One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

- **Enough target terminals:** The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.
- **Enough functionality**: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficientiy or not at all. The expanded functionality also increases the probability of malware.
- **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Nowadays, mobiles/cell phones are becoming fancier and expensive hence increasingly liable to theft. Criminals are interested in accessing wireless service and seek potential possibility to stealing the ID.

Ensure to note the following details about your cell phone and preserve it in a safe place:

1. Your phone number;
2. the make and model;
3. color and appearance details;
4. PIN and/or security lock code;
5. IMEI number.

The International Mobile Equipment Identity (IMEI)

It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.

The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country. For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to "lock" the phone using its IMEI number. This will help to stop the usage of phone in that country, even if a SIM is changed.

Visit the weblink http://www.numberingplans.com/?page=analysis&sub=imeinr to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

1. Add a security mark on your cell phone. Use permanent marker and print your alternate contact number and short address on your cell phone instrument as well as on battery. In case someone finds your handset, it is easier to contact you if the finder of your cell phone would like to return it you.
2. Set a password and ensure the password is strong enough so that a finder of your cell phone cannot easily guess it.
3. In case of loss of your cell phone, register a complaint with cell phone service provider immediately, using your IMEI number, to enable your service provider to block your cell phone and your account details. Preserve all the details of launched complaints, that is, obtain confirmation in writing from your service provider that your phone has been disabled.
4. In case of loss of your cell phone, register a complaint at the police station and obtain FIR. Preserve all the details for launched complaints, that is, FIR report.
5. Keep an eye on your phone while traveling. During the security check at the airport security, ensure to retrieve your cell phone immediately once it enters the x-ray machine - criminals often steal phones during these vulnerable seconds.
6. Keep Wi-Fi and Bluetooth OFF when it is not required to be in use. Airports, coffee shops, hotels and all other public places wherever free Wi-Fi zone is available, criminals always have an eye to seek the vulnerability to steal information.

7. Periodic backup is important and especially if you are traveling, backup before traveling is necessary. It takes only few minutes to take backup but it is always helpful in case you lose your cell phone during traveling.
8. Do not forget to apply all the updates for cell phone software/firmware, received from manufacturers, which are routinely provided to update vulnerabilities fixes.
9. Only download applications from reputable sources - specific care should be taken while downloading plug-in applications on the cell phone. It is always advised to use the recommendations provided by cell phone manufacturers' to download directly from the Web.

8.8.2. Mobile Viruses

A mobile virus is similar to a computer virus that targets mobile phone data or applications/ software installed in it. Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified. First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.

Mobile viruses get spread through two dominant communication protocols — Bluetooth and MMS. Bluetooth virus can easily spread within a distance of 10-30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book. Readers may visit http://symbianpoint.com/types-latest-list-mobile-viruses.html to know the list of latest mobile viruses.

It is interesting to note that, like Computer Virus Hoax, variants of Mobile Phone Virus Hoax have been circulating since 1999. These hoax messages either will be sent through E-Mail or through SMS to the mobile users. The example of such hoax is given.

"All mobile users pay attention!!!!!!!!!

If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call, END THE CALL IMMEDIATELY, if you answer the call, your phone will be infected by a virus. This virus WILL ERASE all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now. You can also check this news in the CNN website.

PLEASE FORWARD THIS PIECE OF INFORMATION TO ALL YOUR FRIENDS HAVING A MOBILE PHONE."

How to Protect from Mobile Malwares Attacks

Following are some tips to protect mobile from mobile malware attacks.

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.

2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

8.8.3. Mishing

Mishing is a combination of mobile phone and Phishing. Mishing attacks are attempted using mobile phone technology. M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam. A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing. Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details. Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

8.8.4. Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V - voice and Phishing. Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

The most profitable uses of the information gained through a Vishing attack include:

1. ID theft;
2. purchasing luxury goods and services;
3. transferring money/funds;
4. monitoring the victims', bank accounts;
5. making applications for loans and credit cards.

How Vishing Works

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminals will to reach a particular audience.

1. **Internet E-Mail:** It is also called Phishing mail
2. **Voicemail:** Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
3. **Direct phone call:** Following are the steps detailing on how direct phone call works:
    - The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/ mobile phone numbers after accessing legitimate voice messaging company.
    - The criminal often uses a war dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.

- When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity. The message instructs the victim to call one phone number immediately. The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
- When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
- Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
- Such calls are often used to harvest additional details such as date of birth, credit card expiration date, etc.

Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

1. **Automated message:** Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.
   - Press 1 if you need to check your banking details and live balance.
   - Press 2 if you wish to transfer funds.
   - Press 3 to unlock your online profile.
   - Press 0 for any other query.
2. **Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself:** "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."
3. **The victim enters his/her bank account number and hears the next prompt:** "Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."
4. **The caller enters his/her date of birth and again receives a prompt from the automated system:** "Thank you. Now please type your PIN, followed by the pound key."
5. **The caller enters his PIN and hears one last prompt from the system:** "Thank you. We will now transfer you to the appropriate representative."

At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks.

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company - caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

8.8.5 Smishing

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMS PHISHING". SMS — Short Message Service — is the text messages communication component dominantly used into mobile phones.

Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to "hook" (method used to actually "capture" your information) the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI.

Smishing works in the similar pattern as Vishing. A few examples of Smishing are provided herewith to demonstrate how the victim is forced to disclose PI.

1. "We are happy to send our confirmation toward your enrolment for our 'xxxxxxx Club Membership'." You will be charged Rs. 50/- per day, unless you reconfirm your acceptance of your membership on our "Membership Office Contact no. XXXXXXXXXX."
2. "[(Name of popular online bank) is confirming that you have purchased LCD TV set, worth of Rs. 90,000/- only from (name of popular computer company)]. Visit www.abcdef.com if you did not make this online purchase''.

Pretexting, Sexting and VoIP Spam

Pretexting

It is also a form of social engineering, wherein a pretexter hides his/her purpose and/or identity to get the personal information/sensitive data about another individual. For example, the pretexter may claim his/her affiliation with a survey agency, financial institute or bank. Usually, victims are targeted over the phone and enticed to reveal their information or perform an action.

"No one is born hating another person because of the color of his skin, or his background, or his religion. People must learn to hate, and if they can learn to hate, they can be taught to love, for love comes more naturally to the human heart than its opposite." ***- Nelson Mandela***

It is more than a simple lie as it most often involves some prior research or setup and the use of pieces of known information (e.g., for impersonation: date of birth, pet names of family members and last bill amount) to establish legitimacy in the mind of the target.

This technique is often used to trick the executives to disclose the information about their customer and/or their competitor and is used by private investigators to obtain telephone records, banking records, utility records and other information directly from junior representatives of an organization. However, nowadays, this technique is also used by the criminals through vishing and Smishing attacks.

Sexting

It is the practice of sending sexually explicit text messages and photos over the cell phone. It is becoming an increasingly hot topic both in schools/colleges and in the workplace. Although most of the people think instantly of cell phones as sexting devices, digital photography, Internet (i.e., websites) and even few video game systems are also contributing sexting.

Sexting is a complex topic and no one-size-fits-all solution is available, reason being that it embraces everything from gentle naughty-blue pictures to slimy pornography. Many teens (especially, girls) who believe they are sending a private message, may have their messages widely distributed, sometimes even immediately available on porno sites. So, it is important that parents should keep an eye on the cell phones provided to the kids. Kids should be made aware that "Information shared electronically never dies" and any message such as sexting may come back to haunt them even after months and years.

VoIP Spam

VoIP Spam is the proliferation of unwanted, automatically dialed and prerecorded phone calls using VoIP. Some pundits have taken to referring to if as "Spam over Internet telephony" (SPIT). VoIP systems, such as E-Mail and other Internet applications, are susceptible to abuse by criminals to initiate unsolicited and unwanted communications. Increasingly, telemarketers, prank callers and other telephone system abusers are likely to target VoIP systems, particularly, if VoIP tends to supplant conventional telephony.

How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.
3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages

may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

8.8.6 Hacking Bluetooth

Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile devices. Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard - Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.

When Bluetooth is enabled on a device, it essentially broadcasts "I'm here, and I'm able to connect" to any other Bluetooth-based device within range. This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software on a laptop and then installs a Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

Table : Bluetooth hacking tools

Sr. No.	Name of the Tool	Description
1.	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2.	BlueSniff	This is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices.
3.	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4.	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5.	BlueDiving	Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

1. **Bluejacking:** It means Bluetooth + Jacking where Jacking is short name for hijack — act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius),

for example, sending a visiting card which will contain a message in the name field. If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact. Bluejacking is harmless, as bluejacket! users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

2. **Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

3. **Bluebugging:** It allows attackers to remotely access a users phone and use its features without user's attention. During initial days, the attacker could simply listen to any conversation his/her victim is having; however, further developments in Bluebugging tools have enabled the attacker with the ability to take control of the victim's phone and to conduct many more activities such as initiate phone calls; send and read SMS; read and write phonebook contacts; eavesdrop on phone conversations and connect to the Internet.

4. **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Further research is underway to know whether Bluetooth attackers could do anything more serious such as disabling airbags or brakes through this kind of attack. The researchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking. These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

Hacking Mobile Phones

Chris Paget, a hacker, conducted a demonstration on how to intercept mobile phone calls using ah equipment that costs not more than US$ 1,500, at a DefCon conference in Las Vegas.

The hacker used a simple antenna and some basic radio equipments to broadcast a GSM signal and pretend to be a telecom service provider. After this clever trick, it is possible for a hacker to forward his/her own calls and listen to any conversation that takes place within the network.

Although this demonstration is limited to GSM networks, the hacker is quite confident about causing disruption into 3G mobile networks with a simple noise generator and a power amplifier.

Smart readers can immediately conclude that although INTEGRITY is always challenged during the transmitting of the text messages, the threat of breaching the voice communication has also become important under cybersecurity.

8.9 Mobile Devices: Security Implications for Organizations

8.9.1 Managing Diversity and Proliferation of Hand-Held Devices

In the previous sections we have talked about the micro issues of purely technical nature in mobile device security. In this section, we focus on the macro issues at the organizational level. Given the threats to information systems through usage of mobile devices, the organizations need to establish, security practices at a level appropriate to their security objectives, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, whereas others will place more value on cost and convenience. Whatever approaches an organization chooses, it is important that the policy-making effort starts with the commitment from a Chief Executive Officer (CEO), President or Director who takes cyber security seriously and communicates that throughout an organization. The best security technology features will be found to be worthless if there is no organization policy or automated enforcement to ensure that they are actually used.

In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures. Cyber security is always a primary concern; even then, at times, there is still some short sightedness. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether or not the devices have been provided by the organization. In addition (recall the micro level technical issues discussed in the previous section), close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.

In addition, employees should be encouraged to register with the IT department any devices they use for themselves, so that access can be provisioned in a controlled manner and de-provisioned appropriately when the employee leaves.

Younger workers (also referred to as Gen-Y) are pushing many enterprises to embrace mobility solutions. These younger workers prefer instant/text messaging instead of E-Mail, and frequently use social networking services such as Facebook, MySpace and Twitter. They often prefer to use personal, consumer-oriented devices (both laptops and mobile devices) in the work environment, and adapt quickly to new technology. In contrast, older workers are found to be slow to accept mobility solutions and rely almost entirely on voice communications and E-Mail. These old workers often do not see the benefit of instant messaging and social networking. Interestingly, at the same time these older workers are often found to be on the seat that provides authority and control for staffing and budget, and they can therefore greatly influence mobility policy. These different points of view between younger and older workers have created a mobility generational gap. Older workers sometimes see younger workers as being "spoiled" whereas younger workers sometimes see older workers as a barrier to progress.

8.9.2. Unconventional / Stealth Storage Devices

We have already mentioned about mobile phones and media players used by the employees. In this section, we would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes — unconventional/ stealth storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security. It is advisable to prohibit the employees in using these devices. Their small size allows for easy concealment anywhere in a bag or on the body.

Firewalls and antivirus software are no defense against the threat of open USB ports. Not only can viruses, worms and Trojans get into the organization network, but can also destroy valuable data in the organization network. Organization has to have a policy in place to block these ports while issuing the asset to the employee. However, sometimes the standard access controls with Windows OS do not allow the assignment of permissions for USB ports and restricting these devices becomes next to impossible. Disgruntled employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses. As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.

Using "DeviceLock" software solution, one can have control over unauthorized access to plug and play device. The features of the software allows system administrator to:

1. Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
2. Control the access to devices depending on the time of the day and day of the week.
3. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
4. Set devices in read-only mode.
5. Protect disks from accidental or intentional formatting.

Another factor in cyber security complications with mobile devices is their falling cost. Until few years ago, mobile devices were considered as an office supply item instead of a powerful computing platform. Early hand-helds were expensive and specialized, so they were deployed only for specific applications, but more general-purpose models are now available at a relatively low cost, often bundled with a tariff for wireless connection. So, many organizations did not have policies concerning the usage of mobile/wireless devices at work/ connected with work. Nowadays, because modern hand-held devices for mobile computing are, at times, good productivity tools, they cannot be precluded from use by employees, contractors and other business entities. Given this, it is important for the device management teams to include user awareness education; thus, they get encouraged to take some personal responsibility for the physical security of their devices, as many IT managers have learned from their bitter experience.

8.9.3. Threats through Lost and Stolen Devices

This is a new emerging issue for cyber security. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period. Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices.

The cyber security threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators. Even if these lost devices are personal, the issue is no less serious given the resulting privacy exposures! Gartner Group had predicted that by 2003 there will be over one billion mobile devices in use globally. This is true going by the sales figures quoted in annual reports published by Research in Motion. This shows that the popularity of mobile devices is increasing at a rapid rate; however, people have not been educated about the importance of securing them. The picture is indeed scary; mobile users are in an even worse position now because they are far more reliant on their mobile devices to store large amounts of sensitive information with very few concerned about backing it up or protecting it.

8.9.4 Protecting Data on Lost Devices

Given the above discussion, readers can appreciate the importance of data protection especially when it resides on a mobile hand-held device. At an individual level, employees need to worry about this. There are two reasons why cyber security needs to address this issue: data that are persistently stored on the device and always running applications. For protecting data that are stored persistently on a device, there are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device: (a) encrypting sensitive data and (b) encrypting the entire file system (this may be useful when using data outside of a database, such as in a spreadsheet). Data that are stored on hard disks in persistent memory or on removable memory sticks (whether they are in or out of the device) should be protected. There are many third-party solutions/tools available to protect data on the lost devices, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete the data on a user's device using a suitable tool.

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

8.9.5. Educating the Laptop Users

Often it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and Spyware. This is because the software assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options.

According to year 2004 finding, through one survey, it was found that some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and downloading illegal music files and movies. As per one survey of 500 European business laptop users, Malicious Code, such as Spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.

The result from a survey quoted below figure further supports this point on cyber security threats from corporate laptop users. However, despite the growth in corporate security risks, resulting from mobile working, the tone of most of the security-awareness surveys shows that only half of the companies have tools in place to manage the Internet access on laptops, with only one-quarter of businesses physically enforcing these policies. An important point to be noted is that the policies and procedures put in place for support of laptop have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise. This shows how much role "perception" plays in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

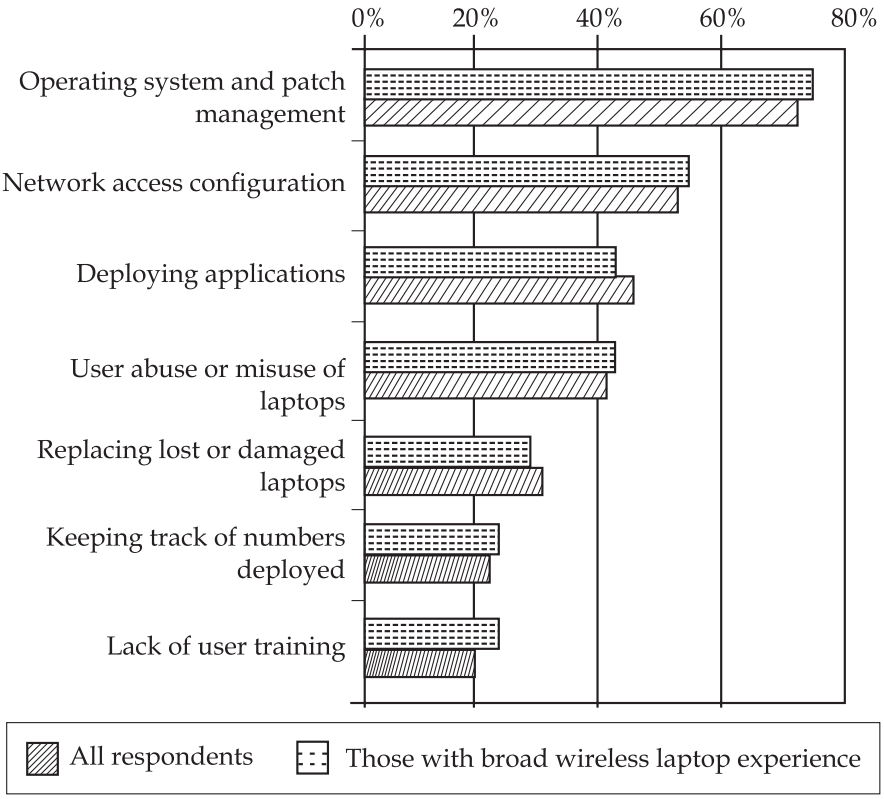


Fig. Most Important Management or Support Issues For Laptops

Look at the sky. We are not alone. The whole universe is friendly to us and conspires. The water in a vessel is sparkling; the water in the sea is dark. The small truth has words which are clear; the great truth has great silence. - ***Sir Rabindranath Tagore***

अध्याय 9

Chapter 9

Cyber Crime and Cyber Terrorism : A Detail Explanation

9.1. Data Theft

9.1.1. What is Data Theft?

According to The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Crime of data theft under Section 43(b) is stated as If any person without permission of the owner or any other person who is incharge of a computer, computer system of computer network - downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium. According to Wikipedia Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices.

Data theft is, quite simply, the unauthorized copying or removal of confidential information from a business or other large enterprise. It can take the form of ID-related theft (the theft of customer records) or the theft of a company's proprietary information or intellectual property. The act of illegally downloading data from a networked computer to a USB flash drive is called thumb sucking. The use of an iPod or other portable music player for the same purpose is called pod slurping. Because of how easy it is to copy data to these types of devices, some companies are now outlawing the use of any personal, portable data storage devices in their offices.

Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this type of information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

Illustration 1

Ms. Riya visits her cousin Ms. Ruchi's house, Riya finds the desktop computer switched on, when Riya surfs into the hard disk, she likes certain pdf files, Riya fraudulently copies certain files to her pen drive without Ruchi's permission, this act of Riya constituted crime of data theft.

Illustration 2

A famous builder's, sister applied a rule to, the email client of the builder's laptop. This rule forwarded all emails and files received by builder fraudulently to sister's email id. This builder had a corporate email id as anil.builder@company.com, a fraudulent emailed aniil.builder@gmail.com was made and all emails were forwarded automatically here. This fraudulent act of the lady is the act of data theft as the act was done without the permission of the builder and the theft was committed for commercial benefit.

Illustration 3

Mr. Sunil Verma works with an MNC, from last 4 years, he has just got a lucrative job with the competitor company, he is on a notice period for one month. On his last day with the current

employer Sunil attaches all data files with regards to clients and certain software source code to his personal gmail id. Sunil Verma thus commits the crime of data theft on his employer. This crime gets proved by the proxy server and firewall logs of the company and is substantiated by the data received from Gmail Inc.

Illustration 4

A newly launched website called www.crickymasala.com for want of content, copies without permission verbatim to verbatim content from established website www.cricknext.com. This act of www.crickymasala.com was done to gain commercial benefit to self. This act gets classified as the crime of data theft.

9.1.2. CASE LAWS

1. Just Dial v. Infomedia 18 Delhi HC

Just Dial, with a single national number 69999999 in 240 cities, has obtained injunction against Infomedia 18 Limited (one of the group company of media group TV 18), restraining it from carrying out any business or rendering any service of providing information of business, services, and products, through their newly launched website askme.in

In a suit filed by Just Dial against Infomedia 18, Just Dial alleged that Infomedia 18 had copied its extensive database and was displaying the same on its website askme.in, thereby infringing Just Dial's copyright in its valuable database. The Delhi High Court has granted an exparte injunction against Infomedia 18, restraining them from infringing Just Dial's copyright and from running the website askme.in till the next date of hearing. The High Court has also appointed commissioners to visit Infomedia 18 Ltd's office in Delhi and Mumbai and to seize and take into custody all the CPUs, compact, floppy discs and/or other storage media containing any part of the commercial or business directory database belonging to Just Dial.

2. T-Mobile data theft case (landmark case) June 2011, Chester Crown Court.

The Chester Crown Court has ordered two former employees of UK mobile operator T-Mobile to pay a total of £73,700 after stealing and selling customer data from the company in 2008. It is a landmark ruling because, it is a record fine for data protection offences, but more important than that, is that for the very first time we are seeing the criminal courts taking data protection seriously, David Turley and Darren Hames pleaded guilty to offences under Section 55 of the Data Protection Act, but the fines were, imposed under the Proceeds of Crime Act. Mr. Turley was ordered to pay £45,000 and Mr. Hames was ordered to pay £28,700. Both face an 18-month prison term if they fail to pay within six months.

9.2. CYBER TERRORISM

9.2.1. What is Cyber Terrorism?

Any act of any person on the computer or network or otherwise which threatens unity, sovereignty and security of the state can be called as cyber terrorism.

According to, The IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, crime of Cyber Terrorism under Section 66-F whoever, with intent to threaten the unity,

integrity, security or sovereignty of India or to strike terror in the people or any Section of the people by - denying or cause the denial of access to any person authorized to access computer resource; or attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or introducing or causing to introduce any computer contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or knowingly, intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data, computer database that is restricted for reasons of the security of the state or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

It means use of cyber tools to shut down critical national infrastructure such as energy, transportation and communication and coerce governments into submission. Internet bombs threats, Internet harassment and technology-driven crimes, such as focused virus strikes are the next wave of crime that the world has to encounter in the days to come.

A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism.

Illustration 1

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications". Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems. These Tamil guerillas were first public known cyber terrorists who tried to damage friendly relations with foreign states.

Illustration 2

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestor's also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders and threatened to employ the same tactics against organizations using IGC services. They demanded that IGC stop hosting the website for the Euskal Herria Journal, a New York-based publication supporting Basque independence.

Protestors said IGC supported terrorism because a Section on the Web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish

political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings".

Illustration 3

In 1998, a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA. He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people. This act was likely to cause death or injuries to persons. The attempt of this boy would be termed as an act of cyber terrorism.

Illustration 4

In 1996, a computer hacker allegedly associated with the white supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise". Such an act with racial overtones is called an act of cyber terrorism.

Illustration 5

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

Illustration 6

In 1997, 35 computer specialists used hacking tools freely available on 1,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu. This specialist thus committed the crime of cyber terrorism by causing or likely to cause injury to the interest of the sovereignty and integrity of country.

Illustration 7

Mr. Aniket Sharma on the incitement of China using his hacking skills, suppose logs in servers of power grid corporation of India Ltd. His intention is to disrupt the power supply or to the destroy the grid. Alternatively he logs into servers of the department of telecommunication in a view to disrupt internet infrastructure of India or logs in server of ISRO to gain critical information on Indian space program. Aniket commits the crime of cyber terrorism.

9.2.2. International Perspective

Radical groups use mass communication systems such as the Internet to spread propaganda. Recently, the number of websites offering racist content and hate speech has risen - a study in 2010 suggested a rise of 45 per cent in the number of web pages promoting racial hatred, violence and xenophobia between 2008 and 2010. In 2010, over 60,000 such websites existed on the Internet.

Internet distribution offers several advantages to offenders, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement to hatred websites

include websites presenting instructions on how to build bombs. Besides propaganda, the Internet is used to sell certain goods e.g. Nazi-related items such as flags with symbols,' uniforms and books, readily available on auction platforms and specialized web-shops. The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube.

Not all countries criminalize these offences. In some countries, such content may be protected by principles of freedom of speech. Opinions differ as to how far the principle of freedom of expression applies with regard to certain topics, often hindering international investigations. One example of conflict of laws is the case involving the service provider Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material. Based on the First Amendment of the United States Constitution, the sale of such material is legal under United States law. Following the First Amendment, a US court decided that the French order was unenforceable against Yahoo! in the United States.

The disparities between countries on these issues were evident during the drafting of the Council of Europe Convention on Cybercrime. The Convention seeks to harmonise cybercrime-related laws to ensure that international investigations are not hindered by conflicts of laws. Not all parties engaged in negotiations could agree on a common position on the criminalization of the dissemination of xenophobic material, so this entire topic was excluded from the Convention and instead addressed in a separate First Protocol. Otherwise, some countries (including the United States) might have been unable to sign the Convention.

Back in the 1990s the discussion about the use of the network by terrorist organizations was focusing on network-based attacks against critical infrastructure such as transportation and energy supply ("cyber terrorism") and the use of information technology in armed conflicts ("cyberwarfare"). The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorists are possible, but it is difficult to assess the significance of threats and at that time the degree of interconnection was small compared to the current status and it is very likely that this - apart from the interest of the states to keep successful attacks confidential — is one of the main reasons why very few such incidents were reported. At least in the past, falling trees therefore posted a greater risk for energy supply than successful hacking attacks.

This situation changed after the 9/11 attacks. An intensive discussion about the use of ICTs by terrorists started. This discussion was facilitated by reports that the offenders used the Internet within the preparation of the attack. Although the attacks were not cyber-attacks, as the group that carried out the 9/11 attack did not carry out an Internet-based attack, the Internet played a role within the preparation of the offence. Within this context, different ways in which terrorist organizations use the Internet were discovered. Today it is known that terrorists use ICTs and the Internet for:

- Propaganda;

- Information gathering;
- Preparation of real-world attacks;
- Publication of training material;
- Communication;
- Terrorist financing;
- Attacks against critical infrastructures.

This shift in the focus of the discussion had a positive effect on research related to cyber terrorism as it highlighted areas of terrorist activities that were rather, unknown before. But despite the importance of a comprehensive approach, the threat of Internet-related attacks against critical infrastructure should not move out of the focus of the discussion. The vulnerability of and the growing reliance on information technology makes it necessary to include Internet-related attacks against critical infrastructure in strategies to prevent and fight cyber terrorism.

But despite the more intensive research the fight against cyber terrorism remains difficult. A comparison of the different national approaches shows many similarities in the strategies. One of the reasons for this development is the fact that the international communities recognized that the threats of international terrorism require global solutions. But it is currently uncertain if this approach is successful or if the different legal systems and different cultural backgrounds require different solutions. An evaluation of this issue carries unique challenges because apart from reports about major incidents there are very few data available that could be used for scientific analysis. The same difficulties arise with regard to the determination of the level of threat related to the use of information technology by terrorist organizations. This information is very often classified and therefore only available to the intelligence sector. Not even a consensus of the term "terrorism" was yet achieved. A CRS Report for the United States Congress for example states that the fact that one terrorist booked a flight ticket to the United States via the Internet is proof that terrorists used the Internet in preparation of their attacks. This seems to be a vague argumentation as the booking of a flight ticket does not become a terrorist-related activity just because it is carried out by a terrorist.

9.2.3. Propaganda

In 1998 only 12 out of the 30 foreign terrorist organizations that are listed by the United States State Department, maintained websites to inform the public about their activities. In 2004 the United States Institute of Peace reported that nearly all terrorist organizations maintain websites — among them Hamas, Hezbollah, PKK and Al Qaida. Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda. The use of websites and other forums are signs of a more professional public relations focus of subversive groups. Websites and other media are used to disseminate propaganda, describe and publish justifications of their activities and to recruit new and contact existing members and donors. Websites have been used recently to distribute videos of executions.

9.2.4. Information gathering

Considerable information about possible targets is available over the Internet. For example, architects involved in the construction of public buildings often publish plans of buildings on their websites. Today high resolution satellite pictures are available free of charge on various Internet services that years ago were only available to very few military institutions in the world. Furthermore, instructions on how to build bombs and even virtual training camps that provide instructions on the use of weapons in an e-Learning approach were discovered. In addition, sensitive or confidential information that is not adequately protected from search-robots and can be accessed via search engines. In 2003, the United States Department of Defence was informed that a training manual linked to Al Qaeda contained information that public sources could be used to find details about potential targets. In 2006 the New York Times reported that basic information related to the construction of nuclear weapons were published on a Government website that provided- evidence about the Iraq approaches to develop nuclear weapons. A similar incident was reported in Australia where detailed information about potential targets for terrorist attacks was available on Government websites. In 2005 the press in Germany reported that investigators found that manuals on how to build explosives were downloaded from the Internet onto the computer of two suspects that tried to attack public transportation with self-built bombs.

9.2.5. Preparation of real-world attacks

There are different ways that terrorists can make use of information technology in preparing their attack. Sending out e-mails or using forums to leave messages are examples that will be discussed in the context of communication. Currently more direct ways of online preparations are discussed. Reports were published that point out that terrorists are using online games within the preparation of attacks. There are various different online games available that simulate the real world. The user of such games can make use of characters (avatar) to act in this virtual world. Theoretically those online games could be used to simulate attacks but it is not yet uncertain to what extent online games are already involved in that activity.

9.2.6. Publication of training material

The Internet can be used to spread training material such as instructions on how to use weapons and how to select targets. Such material is available on a large scale from online sources. In 2008, Western secret services discovered an Internet server that provided a basis for the exchange of training material as well as communication. Different websites were reported to be operated by terrorist organizations to coordinate activities.

9.2.7. Communication

The use of information technology by terrorist organizations is not limited to running websites and research in databases. In the context of the investigations after the 9/11 attacks it was reported that the terrorists used e-mail communication within the coordination of their attacks. The press reported about the exchange of detailed instructions about the targets and the number of attackers via e-mail. By using encryption technology and means of anonymous communication the communication partner can further increase the difficulties in identifying and monitoring terrorist communication.

9.2.8. Terrorist financing

Most terrorist organizations depend on financial resources they receive from third parties. Tracing back these financial transactions has become one of the major approaches in the fight against terrorism after the 9/11 attacks. One of the main difficulties in this respect is the fact that the financial resources required to carry out attacks are not necessary high. There are several ways in which Internet services can be used for terrorist financing. Terrorist organizations can make use of electronic payment systems to enable online donations. They can use websites to publish information how to donate, e.g., which bank account should be used for transactions. An example of such an approach is the organization "Hizb al-Tahrir" which published bank account information for potential donators. Another approach is the implementation of online credit card donations. The Irish Republican Army (IRA) was one of the first terrorist organizations that offered donations via credit card. Both approaches carry the risk that the published information will be discovered and used to trace back financial transactions. It is therefore likely that anonymous electronic payment systems will become more popular. To avoid discovery terrorist organizations are trying to hide their activities by involving non-suspicious players such as charity organizations. Another (Internet-related) approach is the operation of fake web-shops. It is relatively simple to set up an online-shop in the Internet. One of the biggest advantages of the network is the fact that businesses can be operated worldwide. Proving that financial transactions that took place on those sites are not regular purchases but donations is quite difficult. It would be necessary to investigate every transaction — which can be difficult if the online shop is operated in a different jurisdiction or anonymous payment systems were used.

9.2.9. Attacks against critical infrastructures

In addition to regular computer crimes such as fraud and identity-theft, attacks against critical information infrastructures could become a target for terrorists. The growing reliance on information technology makes critical infrastructure more vulnerable to attacks. This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks. In those cases the disruption caused by a network-based attack goes beyond the failure of a single system. Even short interruptions to services could cause huge financial damages to e-Commerce businesses — not only for civil services but also for military infrastructure and services. Investigating or even preventing those attacks presents unique challenges. Unlike physical attacks, the offenders do not need to be present at the place where the effect of the attack occurs. And while carrying out the attack the offenders can use the means of anonymous communication and encryption technology to hide their identity. As highlighted above, investigating such attacks requires special procedural instruments, investigation technology and trained personnel.

Critical infrastructure is widely recognized as a potential target of a terrorist attack as it is by definition vital for a state's sustainability and stability. An infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state. These are in particular: electrical power systems, telecommunication systems,

gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina in the United States highlights the dependence of society on the availability of those services.

The vulnerabilities of critical infrastructure with regard to network-based attacks can be demonstrated by highlighting some of incidences related to air-transportation.

The check-in systems of most airports in the world are already based on interconnected computer systems. In 2004 the Sasser computer worm infected million of computers around the world, among them computer systems of major airlines, which forced the cancellation of nights.

Today all tickets are purchased online. Airlines use information technology for various operations. All major airlines allow their customers to buy tickets online. Like other e-commerce activities, those online services can be targeted by offenders. One common technique used to attack web-based services is Denial-of-Service (DoS) attacks. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, Ebay and Amazon. As a result, some of the services were not available for several hours or even days. Airlines have been affected by DoS attacks as well. In 2001 the Lufthansa website was the target of an attack.

Another potential target for Internet-related attacks against critical air transportation infrastructure is the airport control system. The vulnerability of computer-controlled flight control systems was demonstrated by a hacking attack against Worcester Airport in the U.S. in 1997. During the hacking attack, the offender disabled phone services to the airport tower and shut down the control system managing the runway lights.

Spreading Virus or Worm's

What is spreading of Virus or Worm's?

In most cases, viruses can do any amount of damage the creator intends them to do. They can send your data to a third party and then delete your data from your computer. They can also ruin/mess up your system and render it Unusable without a re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Usually the virus will install files on your system then will change your system so the virus is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victims.

The normal effect a virus will have on your system is that over time your system will run slower. Also when you are using the Internet your connection may seem to run slower. Eventually you may have trouble running programs on your system, your system may freeze, and in the worst case you may not be able to get it to boot up when you turn your computer on.

How Viruses or Worms Spread?

Most commonly viruses today use e-mail to spread however they have used one or more of the following methods to spread in the past.

Some viruses will load themselves onto any part of a writable removable drive as possible and spread from computer to computer as people use the removable drive.

A worm is a program similar to a virus that will exploit vulnerability in an operating system or application that a computer user is running. The best defence against a worm is to have either a personal firewall on your system or be behind a corporate firewall. Another good defence is to update your system regularly. All you need to do to get a worm is to connect an unpatched computer to the Internet or infected network when your computer does not have firewall protection.

Most viruses will spread themselves using e-mail attachments. They may tell the user that they need to open the attachment to get the rest of the information that is being sent to them. Many times the virus may claim it is an administrator and the user needs to either read the data or install a program on their system. Viruses have even claimed to be Microsoft sending a system patch as an attachment to the e-mail. Microsoft would never send a system patch through e-mail. Effective antivirus management requires high degree of alertness by the computer user. Virus and worms can be implanted by a competitor or a even by enemy country.

Illustration 1

Mr. Shankaran a vendor of Nuclear corporation brings his pen drive to Nuclear corporation office premises and connects his pen drive to a computer for copying a file. He does not scan his pen drive with an Antivirus. The virus and worm present on his pen drive infects the computer. The virus causes to delete critical data and worm stops internet access. Mr. Shankaran commits the crime of spreading virus and computer contamination.

llustration 2

Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network. Robert Morris had committed a crime of spreading computer contamination.

Illustration 3

Mr. Tareek composes a religious email and attaches a worm to one of its jpg file. This email in turn gets forwarded to thousands of Muslims across the country. All the recipients of the said email are implanted by the worm thereby clogging computer networks of the recipients work place. This act of Tareek is a crime of spreading worms.

Illustration 4

In 2006, a US citizen was convicted for conspiracy to intentionally cause damage to protected computers and commit computer fraud. Between 2004 and 2005, he created and operated malicious software to constantly scan for and infect new computers.

It damaged hundreds of US Department of Defence computers in USA, Germany and Italy. The software compromised computer systems at a Seattle hospital, including patient systems, and damaged more than 1,000 computers in a California school district.

9.3. Phishing

9.3.1. What is Phishing?

According to Wikipedia phishing means, in the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Phishing is the fraudulent acquisition, through deception, of sensitive personal information such as passwords and credit card details, by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering attack.

9.3.2. Details of crime

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions. The e-mails state that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to your account. All Indian banks are exposed to phishing attacks an estimated 100 attacks per minute are recorded.

Illustration 1

An customer of ICICI Bank named Mr. Umashankar Sivasubramaniam lost Rs. 6.46 lakhs through Phishing. Mr. Umashankar Sivasubramaniam, who claimed he received an email in September 2007 from ICICI, asking him to reply with his internet banking username and password or else his account would become non-existent. After the reply to this mail he witnessed a transfer of Rs. 6.46 lakh from his account to that of a company which withdrew Rs. 4.6 lakh from an ICICI branch in Mumbai and retained the balance in its account.

On April 12th 2010, the adjudicator of Tamil Nadu, Sri PWC Davidar pronounced a landmark judgment in respect of a complaint lodged with him under ITA 2000 by The award directed the Bank to pay the customer the amount fraudulently transferred in the Phishing transaction along with expenses and interest amounting to a total of Rs 12.85 lakhs.

Illustration 2

In 2003 many people received emails supposedly from eBay claiming that the user's account was about to be suspended unless they clicked on the provided link and updated their credit card information. The scammers use mass-mailing methods and many of the recipients did not even have an eBay account. However, all it takes is 1 or 2 per cent responses for the con to result in a nice haul. These 2 per cent responses resulted in phishing out considerable data in public.

Illustration 3

Citibank is currently the target of a series of phisher scams designed to steal sensitive personal information from Citibank customers. Scam emails, supposedly from Citibank, have been randomly

mass mailed to thousands of Internet users. The scammers rely on the statistical probability that at least a few of the recipients will be Citibank customers and that a small number that are customers will fall for the scam. The scam emails generally take the form of HTML messages designed to resemble official Citibank correspondence, complete with authentic looking logos. The emails cover a range of subjects, including "Account Updates", information on "Security Updates" and "Banking alert confirmations". Links included in the emails lead to a bogus website that looks like the real Citibank site and requests victims to provide account numbers, passwords and other personal information.

Illustration 4

A URL of the UTI Bank's home page was reported to be circulating amongst email users. The web page not only was asking for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements".

In case you have received any e-mail from an address appearing to be sent by UTI BANK, advising you of any changes made in your personal information, account details or information on your user id and password of your net banking facility, please do not respond. It is UTI Bank's policy not to seek or send such information through email. If you have already disclosed your password please change it immediately," the warning says. This tricky act is of phishing.

9.3.3. Case Laws

1. Shri Umashankar Sivasubramanian v. ICICI Bank (2008). Adjudicating Officer of Judicature at Chennai, in the case was filed under Section 43 read with section 46 of the Information Technology Act, 2000 whereby the Petitioner complained of an illegal transfer of funds from his account in the respondent bank, based on the negligence of the respondent bank. The judgment is interesting and also shows the substantive wrongs alleged by the petitioner under the Information Technology Act. The adjudicating officer finally rules that the ICICI bank is liable to pay the petitioner a tidy amount of Rs. 12 lakhs.

2. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001). This was a landmark intellectual property case in which the United States Court of Appeals for the Ninth Circuit affirmed the ruling of the United States District Court for the Northern District of California, holding that defendant, peer-to-peer (P2P) file-sharing service Napster, could be held liable for contributory infringement and vicarious infringement of the plaintiffs' copyrights. This was the first major case to address the application of copyright laws to peer-to-peer file-sharing.

3. State v. Johnson Nwanonyi and Michel Obiorahmuozboa, Anambra state in Nigeria

   A local court in Malappuram district in Kerala sentenced two Nigerians to five years rigorous imprisonment on July 20, 2011 in a cyber-crime case. The two had cheated a doctor in the district of Rs. 30 lakh about two years ago. Johnson Nwanonyi(32) and Michel Obiorahmuozboa (34), both hailing from Anambra state in Nigeria, were sentenced each under sections 420 (cheating)-5 years, and 468 (forgery)-5 years of IPC and section 66(D) (phishing) of Information Technology (Amendment) Act, 2008 -2 years and a fine of Rs 1.25 lakh by a Chief Judicial

Magistrate V Dileep in Manjeri in Malappuram district. The sentence would run concurrently.

According to the charges filed by the Karipur police, the duo had cheated the doctor Dr. C C Thomas, hailing from Valluvambram in Malappuram district after they sent an e-mail inviting application to recover a huge sum of unclaimed money left behind by a Nigerian businessman. They had advertised that the money, kept aside for charitable hospital, was lying unclaimed in a bank. When the doctor responded to the e-mail, they tricked him by asking to pay 30 lakh as processing fee. But a planned move by the police and the doctor succeeded when the Nigerians were lured into Kerala in March 2010. They were then arrested by the Karipur police. The strong evidence based on which the prosecution presented the case became crucial in the first verdict against financial fraud under the IT Act. Deputy Director for Prosecution V C Ismayil appeared for the prosecution.

9.3.4. International Perspective (as per APWG Report)

The number of unique phishing reports submitted to APWG in the second half 2010 reflected a steady decrease after reaching a previous high for 2010 in June of 33,617. The H2, 2010 high of 26,353 in July was down 35 per cent from the all-time high in August 2009 of 40,621 reports. The half-yearly low for this metric, in December, with 21,020, was down 48 per cent from the all-time high.

In the latter months of 2010 APWG witnessed an increase in so-called "spear-phishing" attacks in which individuals inside companies and government agencies are targeted by cybercriminals who send individualized fake emails to their victims - often with crimeware payloads - to gain access into a corporation's network by infecting the targeted employee's computer. These emails, designed to evade spam and anti-virus filters, are very effective at infecting a user's computer. This trend is accelerating in 2011, and is responsible for some high-profile corporate data breaches.

The number of unique phishing websites detected by APWG during the second half 2010 fluctuated by more than 5,000 websites from month to month within the half year. Reaching the highest point in September with 31,705, the remaining three months saw a steady decrease down to 26,124 in December. The half-yearly high in September was down more than 44 per cent from the record high of 56,362 in August 2009. The number of unique brand-domain pairs fluctuated during the second half of 2010. The high for the half year, 16,767 brand-domain pairs in November, was down nearly 32 per cent from the record of 24,438 recorded in August, 2009.

Forensic utility of this metric

If the number of unique URLs is greater than the number of brand/domain pairs, it indicates many URLs are being hosted on the same domain to target the same brand. Knowing how many URLs occur with each domain indicates the approximate number of attacking domains a brand-holding victim needs to locate and neutralize. Since phishing-prevention technologies (like browser and email blocking) require the full URL, it is useful to understand the general number of unique URLs that occur per domain.

From July to December 2010, PandaLabs has registered 10,425,663 new malware samples. With a total malware collection of 60 million, the 2nd half of 2010 produced 17 per cent of all malware

variants recorded at the lab since it began collecting in 1990. This figure reflects the total number of different malware samples that appeared during this period.

(It is important to note cybercriminals commonly obfuscate and re-use the same samples over and over, employing polymorphism — server side or binary side — subsequently increasing numbers of variants recorded.

9.4. Email Bombing

9.4.1. What is Email Bombing?

Email bombing means, in a Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack. According to The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Crime of email bombing under Section 43(e) is stated as, If any person without permission of the owner or any other person who is incharge of a computer, computer system of computer network, disrupts or causes disruption of any computer, computer system or computer network;

9.4.2. Details of Email Bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users (or to lists that expand to that many users). Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message that is setup incorrectly. One of the most annoying things about email bombing is that the sending of nonsensical and numerous emails continue even after the server has been brought down. The email bomb can also cause serious damage such as system crashes and loss of Internet connectivity. These cases can result in more serious problems especially if you are using your Internet connection for business purposes.

Illustration 1

In one case, a foreigner who had been residing in Simla, India for almost 30 years wanted to avail of a scheme introduced by the Simla housing board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently, he sent thousands of mails to the Simla housing board and repeatedly kept sending e-mails till their servers crashed. Foreigner had committed the crime of email bombing on Simla housing board.

Illustration 2

Ms. Riya sends 600 email's per minute to her estranged boyfriend corporate emailed, in a bid to fill his email box. In this process her boyfriend is not able to receive official email's. This act of Riya is email bombing committed with complete consciousness.

9.5. Cyber Bullying

9.5.1. What is Cyber Bullying?

Cyber bullying "involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others". Cyber bullying can also be defined as, "any communication posted or sent by a minor online, by instant messenger, e-mail, Social Networking Site, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor".

9.5.2. Details of Cyber Bullying

Cyber bullying is any harassment that occurs via the Internet and Mobile phones, vicious forum posts, name-calling in chat rooms, posting fake profiles on websites, and mean or cruel email messages are all ways of cyber bullying.

While simple teasing regarding one's personal habits, figure, or any other object which generates curiosity in the young minds is not gravely harmful, but when the same verbal remarks makes a child suffer deep depression, withdrawal symptoms or even affect his studies, the seriousness of the issue does not remain bounded in only "just for fun sake". With the easy access to mobile phones and internet by the school students, the matter becomes more serious as the identity of the victim may be revealed to a bigger circle. It is however, a very much neglected fact that the habit of bullying and cyber bullying in schools open the pathway for the offender to become a habitual ragger in colleges and even turn him into a bigger cyber criminal.

With today's technology bullying has become easier then evens the children and youth of this generation do not even need to have personal confrontation. Cyber bullying can be defined as — "any communication posted or sent by a minor online, by instant messenger, e-mail, Social Networking site, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor".

Illustration 1

A student is bombarded by various threatening and taunting emails at home, even though there is no direct harassment at school. The victim has no idea who is sending the messages and starts to feel like everybody is against him. That student is being cyber bullied.

A school chat room is spammed with name-calling posts that spread vicious rumors about a specific student. The rumors aren't true but kids at school see the posts and believe them. The student is then teased by peers. This student is the victim of cyber bullying.

A defamatory fake profile is posted at a social networking site using a student's real name, photo and contact information. That student starts getting abusive email messages from strangers

who think the profile is real. Some of the messages are crude. Some of the messages are mean. This is another example of cyber bullying.

Illustration 2

Megan Meier was a 13 year old from Missouri who struck up an online friendship on the popular social networking site My Space with a person she believed was a new boy in her hometown. In actuality, the "friend" was a group of individuals, including adults, who were intent on humiliating the poor girl because of a friendship with another child that had gone away. Megan was very upset when she found out the truth, then later committed suicide once the friendship had terminated. Case stunned the community and caused state government officials to pass some of the harshest cyber bullying laws in the country.

Illustration 3

Kylie Kenney, an eighth grade student from Vermont lost two years of her life as a result of cyber bullying from classmates. From junior high through her sophomore year of high school, Kylie was forced to deal with websites created by her classmates that featured names like "Kill Kylie Incorporated" that were filled with threatening, homophobic remarks about the young girl. These hurtful kids obtained screen names with handles close to Kylie's name and used them to make suggestive remarks and sexual advances on Kylie's teammates on the field hockey team. As a result police fried charges of harassments against the individuals responsible. This act on Kylie was of cyber bullying.

Illustration 4

In South Korea, a female college student was riding the train with her dog when it defecated on the floor of the subway car. After the girl refused to clean up the mess, another passenger on the train took her picture using her cell phone and posted it online. In the months to follow, it became an Internet sensation in South Korea and "Dog Poop" girl became the target of extreme harassment. Individuals found out her name and address and soon she was forced to withdraw from school and move to another part of the country, due to constant cyber bullying.

Other Cases

In 2001 Manish Kathuria was arrested by the New Delhi Police after impersonating Ritu Kohli on the MIRC chat service. The arrest was claimed as India's first case of cyberstalking, with Kathuria being charged wider Section 509 of the Indian Penal Code for "outraging the modesty" of his victim. Having appropriated her name he "used obscene and obnoxious language", distributing her home telephone number with invitations for callers to "talk dirty".

The 2000 Hong Kong LRC report on stalking refers to a complaint that an ex-colleague posted a victim's name and mobile phone number on newsgroup, supposedly soliciting sexual services. That resulted in numerous nuisance calls and in a 'cease & desist' enforcement notice once the offender was identified. A radio personality who had been counselling her audience was reported to have been harassed by threatening email and by placement of a doctored photograph in the lonelyhearts section of a sex-related site. She alerted HK police after the offender refused to stop.

In Queensland during 2005 Anette Maree Hill pursued a Toowoomba policeman over a five year period, before being rewarded with a suspended 4.5 year prison sentence. She had bombarded the married officer with love letters, poems, cards and phone calls.

9.6 Identity Theft

9.6.1 What is Identity Theft?

According to Wikipedia Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white-collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

In India, people are very careless when it comes to privacy and personal information. We give out our address and phone numbers to shops, restaurants etc, which is unnecessary and carelessness on our part. Identity theft can occur in multiple forms. One of the main areas of concern and places via which identity theft occurs is, through service providers who have our personal information. As per the non-profit Identity Theft Resource Center, identity thefts can be sub-divided into four categories. These are financial identity theft, criminal identity theft, identity cloning, and business/commercial identity theft.

In many cases the victim is not even aware of what is being done till it is already too late. Identity theft may be used to facilitate crimes, including illegal immigration, terrorism, and espionage. It may also be used as a means of blackmail. There have also been cases of identity cloning to attack payment systems, including online credit card processing and medical insurance. Sometimes people may impersonate others for non-financial reasons too. This is often done to receive praise or attention for the victim's achievements. This is sometimes referred to as identity theft in the media and is a common trend seen by look-a-likes. One does not have to think too far back before recollecting a probable victim of identity theft in India.

9.6.2 Summary of Cyber Offence

The crime of stealing someone's personal, identifying information for the purpose of using that information fraudulently. Personal, identifying information includes: Social Security Numbers, credit card and banking account numbers, usernames, passwords, and patient records. Fraudulent uses for that information can often include: opening new credit accounts, taking out loans in the victim's name,

stealing money from financial accounts, or using available credit. The crime of identity theft is most often committed by organized crime rings or desperate individuals with opportunity.

Illustration 1

In Navi Mumbai, India an American national named Ken Haywood, whose and his most likely fault is, that his unsecured Wi-Fi Internet connection was hacked, theft of identity was committed by terrorist during Ahmedabad terrorist attacks and, terrorist committing identity theft used Haywood's Wi-Fi connection to sent terror emails to various news channels.

Illustration 2

The biggest case of identity theft ever seen, took place in August of 2009. Eleven people, including a US secret service informant, had been charged in connection with the hacking of nine major retailers and the theft and sale of more than 41 million credit and debit card numbers. This data breach is believed to be the largest hacking and identity theft case ever prosecuted by the US Department of Justice, which announced that the suspects were charged with conspiracy, computer intrusion, fraud and identity theft. Three of those charged are US citizens, while the others are from places such as Estonia, Ukraine, Belarus and China.

How else could 11 people whose nations barely get along, pull of a heist involving a whooping 41 million credit card and debit card numbers.

Illustration 3

Ms. Sweety an article clerk of a chartered accountant firm named v & v associates fraudulently obtains digital certificates of a client Mr. Sunil Oberoi from the CA's computer. Ms. Sweety then creates suniloberoi@yahoo.com a fake e-mail ID, commits financial fraud amounting to rupees four crores. This act of Ms. Sweety is an act of identity theft committed on Mr. Sunil Oberoi.

9.6.3. International Perspective

The term identity theft — that is neither consistently defined nor consistently used - describes the criminal act of fraudulently obtaining and using another person's identity. These acts can be carried out without the help of technical means as well as online by using Internet technology.

In general the offence described as identity theft contains three different phases:

In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.

The second phase is characterized by interaction with identity-related information prior to the use of those information within criminal offences. An example is the sale of identity-related information. Credit card records are for example sold for up to 60 US dollars.

The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. Examples for such offence can be the falsification of identification documents or credit card fraud.

The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods and for example steal computer storage devices with identity-related data, searching trash ("dumpster diving"407) or mail theft. In addition they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues as well as person information that can be used in identity theft scams. One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from this system. Reports highlight the risks that can go along with the legal use of search engines for illegal purposes. Similar problems are reported with regard to file-sharing systems. The United States Congress discussed recently the possibilities of file-sharing systems to obtain personal information that can be abused for identity theft. Apart from that the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information. The 2010 CSI Computer Crime and Security Survey shows that more than 45 per cent of the respondents attribute a percentage of their organization's losses greater than 30 per cent to insiders. Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating users through social engineering techniques).

The type of data the perpetrators target varies. The most relevant data are:

- **Social Security Number (SSN) or Passport Number –** The SSN that is for example used in the United States is a classical example of a single identity-related data that perpetrators are aiming for. Although the SSN was created to keep an accurate record of earnings it is currently widely used for identification purposes. The perpetrators can use the SSN as well as obtained passport information to open financial accounts, to takeover existing financial accounts, establish credit or run-up debt.
- **Date of birth, address and phone numbers -** Such data can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN). Having access to additional information like the date of birth and the address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently on a large-scale available in the Internet — either published voluntarily in one of the various identity-related fora or based on legal requirements as imprint on websites.
- **Password for non-financial accounts —** Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes. They can for example takeover an e-mail account and use it to send out mails with illegal content or takeover the account of a user of an auction platform and use the account to sell stolen goods.
- **Password for financial accounts —** Like the SSN information regarding financial accounts is a popular target for identity theft. This includes checking and saving accounts, credit cards,

debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cybercrimes.

Identity theft is a serious and growing problem. Recent figures show that, in the first half of 2010, 13 per cent of United States households fell victim to identity theft. In the United Kingdom, the cost of identity theft to the British economy was calculated at 1.8 billion British pounds every year. Estimates of losses caused by identity theft in Australia vary from less than 1 billion USD to more than 3 billion USD per year. The 2010 Identity Fraud Survey estimates the losses in the United States at 96.6 billion USD in 2010. Losses may be not only financial, but may also include damage to reputations. In reality, many victims do not report such crimes, while financial institutions often do not wish to publicise customers' bad experiences. The actual incidence of identity theft is likely to far exceed the number of reported losses.

Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet. It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (e.g., using biometric information) are costly and not widely used. There are few limits on online activities, making identity theft easy and profitable.

9.7. Email Fraud

9.7.1 What is email fraud?

Fraud whether financial, banking and social committed with the aid of an email would be called as email fraud.

Many types of fraud exist, and email is an inexpensive and popular method for distributing fraudulent messages to potential victims. According to the US Secret Service, hundreds of millions of dollars are lost annually and the losses continue to escalate. Most fraud is carried out by people obtaining access to account numbers and passwords. Never respond to any email message that asks you to send cash or personal information.

Some of the most common fraudulent messages are nonmonetary hoaxes or non-monetary chain mail. Treat these as you would spam; for more information. However, if you receive an email message that appears to involve money or asks for personal information, do not respond to that email.

Illustration 1

An industrialist's daughter studying in a reputed college in the city is a regular pub-hopper. Nothing was wrong with that. Every time she goes out pubbing with her boyfriend during weekends, someone e-mails photographs of the couple to her father. Not to take things lying down, the duo approached an Information Technology (IT) security company for help. The company after studying the emails and the IP addresses of it zeroed down on the computer used for the act. To everyone's shock, the computer belonged to the girl's ex-boyfriend. The intention was clear - to blackmail through emails to the rich father for easy money.

Illustration 2

Mr. Sunil Reddy an government employee receives an Microsoft lottery email claiming that he has won prize of $100,00,000. When Mr. Sunil Reddy responds to the email, he is asked to send

$750 for getting the cheque couriered. When the money is payed by Mr. Sunil, a photocopy of cheque with $100,00,000 as denomination with the name of Mr. Sunil Reddy is sent to him, Mr. Sunil is now asked for $2500 for banking clearance so that original cheque can be sent. This kind of email fraud is called as Nigerian 419 Scam.

Illustration 3

Lots of Indian citizens tax payers and non tax payers got a fraudulent email from fake income tax department. This email stated that a tax refund of lakhs of rupees is to be processed by the department, to process the same a link of a fake website was provided. When the link was clicked a fake income tax website opened and critical details like Pan No, turnover, tax details were siphoned off.

9.8. E-Mail Spoofing

9.8.1 What is E-mail Spoofing?

According to wikipedia e-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source, e-mail spoofing is sending an e-mail to another person so that it appears that the e-mail was sent by someone else. A spoof e-mail is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender.

Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and other parts of the email header are altered to appear as though the e-mail originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.

9.8.2. Explanation of e-mail spoofing:

This does not mean that your e-mail account was compromised. It means that the sender has fooled the mail client into believing the e-mail originated from a different address.

This is usually done for malicious reasons, either to distribute unsolicited email or to distribute e-mail viruses. Unfortunately, . there is no real way to prevent spoofing from occurring. If you receive an email that has questionable content, it is recommended to delete the email message or use an antivirus program to scan the message before opening it.

Illustration 1

Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days.

Illustration 2

Consider Mr. Siddharth whose email address is Siddharth@ hotmail.com. His friend Golu's email address is golu@yahoo.com. Using SendFakeMail, Siddharth can send emails purporting to be sent from Golu's email account. All he has to do is enter golu@yahoo.com in the space provided for sender's email address. Golu's friends would trust such emails, as they would presume that they have come from Golu (whom they trust). Siddharth can use this misplaced trust to send viruses, Trojans, worms etc. to Golu's friends, who would unwittingly download them.

Illustration 3

In another famous case, one Mr. Rao sent himself spoofed e-mails, which were supposedly from the Euro Lottery Company. These mails informed him that he had won the largest lottery. He also created a website in the name of the Euro Lottery Company, announced it that he had won the Euro Lottery and uploaded it on to the Internet. He then approached the Income Tax authorities in India and procured a clearance certificate from them for receiving the lottery amount. In order to let people know about the lottery, he approached many newspapers and magazines.

The media seeing this as a story that would interest a lot of readers hyped it up and played a vital role in spreading this misinformation. Mr. Rao then went to many banks and individuals and told them that having won such a large sum of money he was afraid for his safety. He also wanted to move into a better house. He wheedled money out of these institutions and people by telling them that since the lottery prize money would take some time to come to him, he would like to borrow money from them. He assured them that the loan amount would be returned as soon as the lottery money came into his possession. Lulled into believing him (all thanks to the Income Tax clearance) most of these people loaned large amounts of money to him. It was only when he did not pay back the loan amounts to the banks that they became suspicious. A countercheck by the authorities revealed the entire scheme. Mr. Rao was arrested. Mr. Rao could be biggest spoofer yet known.

Credit Card Fraud

What is Credit Card Fraud?

Credit card fraud is a wide ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

There are billions of rupees lost annually by consumer's who have credit card and calling card numbers stolen from online databases. Bulletin boards and other online services are frequent targets for hackers who want to access large base database of credit card information.

Illustration 1

At the kings International hotel in Mumbai four tech-savvy youngsters from Andheri, two of them software engineers, got together to earn a quick money and ended up siphoning off over Rs. 3 lakh of citizen's money. The mastermind of the gang was 19-year-old Leo Paul. A second-year engineering student at a Bandra college, teamed with Akash Kamble, a 19-year-old Lokhandwala

I have no doubt in my mind that our chief national problems relating to the eradication of poverty, illiteracy and disease and the scientific production and distribution can be tackled only along socialistic lines.
- Netaji Subhash Chandra Bose

resident and ordered the card-reader or credit card skimming device which can store data of 12 credit cards from USA, using the Internet, since it was directly not available in India.

'The boys befriended a waiter at Kings International hotel at Juhu to take their plan ahead. Every time someone ate a meal in the hotel and paid by credit card, the waiter would discreetly swipe it through the magnetic card-reader, which is no more than 6-inches long and can be stored in the pocket. Once the waiter was done, he would handover the device to Paul who would download the data from the cards on to Kamble's personal computer. The duo would then feed the data into blank cards, available in the grey market. The cards were now ready to be used in Shopping malls and theatres, or to withdraw money from an ATM. The boys forged information from more than 22 cards in this manner.

Illustration 2

One of the customers received a SMS based alert for purchasing of the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to know about the misuse. He contacted the Bank in this regards.

The tickets were booked through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India. Shaikh was working in the credit card department; due to this he had access to credit card details of some customers. He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale, Lukkad booked tickets. He used to sell these tickets to customers and got money for the same. He had given few tickets to various other institutions also, various customer's credit card details were misused through online means for booking air-tickets.

Illustration 3

It is the case sourcing engineering. US $ 3,50,000 from City bank accounts of four US customers were dishonestly transferred to bogus accounts in Pune, through Internet. Some employees of a call centre gained the confidence of the US customers and obtained their PIN numbers under the guise of helping the customers out of difficult situation. Later they used these numbers to commit fraud. Highest security prevails in the call centers in India as they know that they will lose their business. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber cafe and assessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced.

Illustration 4

Amit Tiwari had kept many names, bank accounts and clients. None of them were for real. With a plan that was both ingenious and naive, the 21-year-old engineering student from Pune. He tried to defraud a Mumbai-based credit card processing company, CC Avenue of nearly Rs. 900,000/-. He was arrested by the Mumbai Police on August 21, 2003 after nearly a year of hide and seeks with CC Avenue. He has been charged for cheating under Section 420. CC Avenue

"All power is within you. You can do anything and everything. Believe in that. Do not believe that you are weak; do not believe that you are half-crazy lunatics, as most of us do nowadays. Stand up and express the divinity within you."
- Swami Vivekananda

verifies and validates credit cards of buyers for over a thousand e-commerce Websites. It conducts checks like IP mapping, zip code mapping and reverse lookup of telephone numbers. Amit Tiwari found a way to bypass them. In May 2002, Col Vikram Tiwari signed up for CC Avenue's services. In November, he requested the company to deal with his son Amit, who offered Web designing services on www.mafiaz.com. CC Avenue's security team confirmed his credentials through bank signature verification, driving license and his HDFC Bank debit card. Everything was genuine.

Amit processed several transactions, worth Rs. 311,508/- via CC Avenue from November 2002 to February 2003. Then the transactions stopped. In April 2003, CC Avenue began receiving charge-backs from the credit card holders, who denied using mafiaz.com's Web designing service. Amit had assumed the identities of these 'customers' and purchased mafiaz.com's services with credit card details that he found on the Net. He was both the buyer and the seller. Calls to Amit's house in Lucknow went unanswered. Legal notices came back unclaimed. Amit had disappeared without a trace after committing the fraud.

Illustration 5

A complaint was filed in by Sony India Private Ltd, which runs a website called sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campaand ordered a Sony Color Television set and a cordless head phone. A lady gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction got closed at that time, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

Illustration 6

Accused Mullick was working as a courier boy for an agency called Supreet Data Tech Ltd. This company was outsourced by Barclays Bank for credit card application procedures. "Customers would be contacted over the phone for credit cards or loans offered by Barclays Bank. Supreet Data Tech Ltd. was responsible for collecting the necessary documents provided by the applicants, who would also provide details of credit cards they already had in their name. Mullick would

photocopy these documents, and hand them to the other two accused for a sum of Rs. 200/- per case. Shaikh and Umedin would then go to a cyber cafe and misuse these credit card details for online transactions. Barclays Bank and Supreet Data Tech Ltd. were not knowing about Mullick's illegal activities".

"Shaikh and Umedin used the credit card details to purchase 180 airline tickets online. These were domestic flights from Mumbai to Delhi, Jaipur, Lucknow and Rajkot. They also made about 300 transactions for mobile phone recharge ranging from Rs. 201 to Rs. 3,999. Finally, they also procured a loan of Rs. 1.69 lakh from Citibank. The total fraud was estimated to be between Rs. 25 to 30 lakh,".

Illustration 7

The Hyderabad police in India arrested an unemployed computer operator and his friend, a steward in a prominent five-star hotel, for stealing and misusing credit card numbers belonging to hotel customers. The steward noted down the various details of the credit cards, which were handed by clients of the hotel for paying their bills. Then, he passed all the details to his computer operator friend who used the details to make online purchases on various websites.

Case Laws

1. Delhi Credit Card Fraud Case

Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer working in a call centre, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony website. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating under 418, 419, 420 sections of the IPC, but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs. 20,000, and was released on a year's probation.

2. Amol Palekar Case

Well known actor and director Amol Palekar, presently based at Pune, Maharashtra was at the receiving end of a credit card fraud as an unknown person(s) used his credit card details to book a couple of air tickets online. The card was issued by Bank of India, Mumbai, and Palekar was faced with a bill of around Rs. 60K for this transaction.

3. Hotel Le Meridien, Pune Case

Almost 30 customers of Hotel Le Meridien, Pune were cheated. Four persons were creating duplicate credit cards from those belonging to customers and then using them to make purchases.

One of the person was a cashier at the Chingari Restaurant in Hotel Le Meridien, and he used credit card skimmers and readers which recorded details of the credit card being swiped. These details were then copied on blank cards with magnetic strips. Altogether they used 33 cards of 27 banks among themselves to go on a shopping spree, with the total amount of such purchases being pegged at Rs. 1 crore. The type of cards being targeted were the higher end ones, namely, Gold, Titanuim, Platinum and corporate cards, where the credit limit was higher. This came to light when a Citibank employee went to the hotel with some friends and lodged a police complaint after getting his card bill with exorbitant purchases that he had no idea about.

9.9. Copyright Violation

9.9.1. What is Copyright Violation?

Copyright infringement (or copyright violation) is the unauthorized or prohibited use of works covered by copyright law, in a way that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works.

9.9.2. Copyright Definition

For the purposes of Copyright Act 1957, copyright means the exclusive right subject to the provisions of this Act, to do or authorize the doing of any of the following acts in respect of a work or any substantial part thereof, namely: -

(a) In the case of a literary, dramatic or musical work, not being a computer programme, -

- (i) to reproduce the work in any material form including the storing of it in any medium by electronic means;
- (ii) to issue copies of the work to the public not being copies already in circulation;
- (iii) to perform the work in public, or communicate it to the public;
- (iv) to make any cinematograph film or sound recording in respect of the work;
- (v) to make any translation of the work;
- (vi) to make any adaptation of the work;
- (vii) to do, in relation to a translation or an adaptation of the work, any of the acts specified in relation to the work in sub-clauses (i) to (vi);

(b) in the case of a computer programme,-

- (i) to do any of the acts specified in clause (a);
- (ii) to sell or give on commercial rental or offer for sale or for commercial rental any copy of the computer programme: Provided that such commercial rental does not apply in respect of computer programmes where the programme itself is not the essential object of the rental".

(c) In the case of an artistic work,-

- (i) to reproduce the work in any material form including depiction in three dimensions of a two dimensional work or in two dimensions of a three dimensional work;
- (ii) to communicate the-work to the public;
- (iii) to issue copies of the work to the public not being copies already in circulation;
- (iv) to include the work in any cinematograph film;
- (v) to make any adaptation of the work;
- (vi) to do in relation to an adaptation of the work any of the acts specified in relation to the work in sub- clauses (i) to (iv);

(d) In the case of cinematograph film, -

(i) to make a copy of the film, including a photograph of any image forming part thereof;

(ii) to sell or give on hire, or offer for sale or hire, any copy of the film, regardless of whether such copy has been sold or given on hire on earlier occasions;

(iii) to communicate the film to the public;

(e) In the case of sound recording, -

(i) to make any other sound recording embodying it;

(ii) to sell or give on hire, or offer for sale or hire, any copy of the sound recording regardless of whether such copy has been sold or given on hire on earlier occasions;

(iii) to communicate the sound recording to the public.

Explanation.— For the purposes of this section, a copy which has been sold once shall be deemed to be a copy already in circulation.

Illustration 1

In 2003, a computer user in China obtained the source code of a popular game Lineagell from an unprotected website. This proprietary code was then sold to several people in 2004. One of those people set up a website, www.l2extreme.com, to offer the "Lineage" game at a discount. Despite legal warnings from the South Korean company that owned the Lineage source code, the suspect did not shutdown the site. He rented powerful servers -enough to accommodate 4,000 simultaneous gamers — and solicited donations from users to help defray the costs. The loss in potential revenues for the South Korean company was estimated at $750,000 a month. The US FBI arrested the suspect and the website was shutdown.

Illustration 2

A software professional from Bangalore (India) stolen the source code of a product being developed by his employers. He started his own company and allegedly used the stolen source code to launch a new software product. He had committed software copyright violations and source code theft.

Illustration 3

In Mumbai, an web developer from Isoftech Ltd. copied considerable amount of website content from their competitors website to their own website, they also copied brochure design and colors of the competitors. This act of Isoftech Ltd. Amounts to violation of copyright.

9.9.3. CASE LAWS

1. Luxottixa Group Ltd v. Ashok Kumar 2010 Delhi HC (John doe/ashok kumar injunction)

Delhi High Court passed an order restraining the sale and manufacture of counterfeit optical eyewear and their carry cases bearing the famous trademark RAY BAN. The local commissions issued by the Court to execute the orders of seizing and sealing the counterfeit goods was a

resounding success. Apart from over 2500 imitation products discovered from the persons named in the action, counterfeit goods were also found at various premises in the close neighbourhood of the named defendants through the "Ashok Kumar" orders. The Courts thus recognize that in certain cases of counterfeiting the Ashok Kumar type orders are the only remedy for a Plaintiff faced with large volumes of anonymous counterfeiters.

2. Taj Television v. Rajan Mandal & Ors FSR 22 2003 Delhi HC (Landmark Case).

The Delhi High Court, granted a path-breaking order authorizing a court appointed commissioner to enter the premises of any cable operator in India and record evidence of any unauthorized telecast of the FIFA World Cup football matches.

In the present case, the Plaintiff, Taj Television Ltd., based in Dubai, owned and operated an exclusive sports channel by the name of TEN SPORTS. The Plaintiff had acquired the exclusive rights to the telecast of the FIFA World Cup Football matches for India and certain other South Asian countries, from Kirch Sports, an entity that had in-turn acquired the worldwide rights from FIFA. Ten Sports was being broadcasted from Dubai in an encrypted form and could be received by only those cable operators with a decoder.

Copyright in Internet Era Cases

3. Hindustan Times v. www.legalpundits.com 2011 Delhi, HC.

In a recent decision that has ramifications on free distribution of online content, the Delhi High Court passed an ex-parte interim injunction against the website for carrying and forwarding articles published by Hindustan Times (HT) Media Group. The website: www.legalpundits.com, was allegedly found to have been picking news items from HT's online portals. Further, the website was found to be forwarding the content to the public without any consent, authorization or licence of the content owner, HT media group, and that too for financial considerations.

HT media group had moved to the court against the websites on grounds of copyright infringement, trademark violation and unfair trade practice. HT Media also claimed damages of INR 20 lakh from Legalpundits, in the complaint.

9.9.4. International Perspective

With the switch from analogue to digital, digitalization has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes.

Digitalization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalization, copying a record or a videotape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy.

The most common copyright violations include:

- Exchange of copyright-protected songs, files and software in file-sharing systems;
- The circumvention of Digital Rights Management systems;

File-sharing systems are peer-to-peer-based network services that enable users to share files, often with millions of other users. After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users.

Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks. The number of users is growing all the time — a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in file-sharing systems, with other OECD countries showing similar trends. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software. Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network. Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users. The decentralized concept of second-generation file-sharing networks makes it more difficult to prevent them from operating. However, due to direct communications, it is possible to trace users of a network by their IP-address. Law enforcement agencies have had some success investigating copyright violations in file-sharing systems.

More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult.

File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses. Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorized copies or artwork within the public domain.

Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry. It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems. Research has identified millions of file-sharing users and billions of downloaded files. Copies of movies have appeared in file-sharing systems before they were officially released in cinemas at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyright-holders more difficult, as well as law enforcement agencies.

The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as Content Scrambling Systems (CSS), an encryption technology preventing content on DVDs from being copied. This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital Rights Management (DRM) describes the implementation of technologies allowing copyright-

holders to restrict the use of digital media, where customers buy limited rights only (e.g., the right to play a song during one party). DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits.

One of the biggest difficulties with these technologies is that copyright protection technology can be circumvented. Offenders have developed software tools that enable the users to make copy-protected files available over the Internet free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation.

Efforts to protect content are not limited to songs and films. Some TV stations (especially Pay-TV channels) encrypt programmes to ensure that only paying customers can receive the programme. Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.

Without software tools, regular users are less able to commit offences. Discussions on the criminalization of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of "illegal devices" or tools that are designed to enable the users to carry out copyright violations.

9.10. Pornography

9.10.1. What is Pornography?

The graphic, sexually explicit subordination of woman through pictures and/or words that also includes Pornography is verbal or pictorial material which represents or describes sexual behavior that is degrading or abusive to one or more of the participants in such a ways as to endorse the degradation. Behavior that is degrading or abusive includes physical harm or abuse and physical or psychological coercion. In addition, behavior that ignores or devalues the real interest, desires and experiences of one or more participants in any way is degrading. Finally that a person has chosen or consented to be harmed, abused, or subjected to coercion does not alter the degrading character of such behavior.

Information Technology (Amendment) Act, 2008, crime of Pornography under Section 67-A whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct can be called as pornography.

llustration 1

An engineering student was using the auction website called www.bazee.com website to sell a video depicting two school students having sexual intercourse. Bazee.com was held liable for distributing porn and hence the CEO was arrested. The CEO was held for abating pornography by Delhi police. The case is still in Indian courts.

Illustration 2

The Delhi Police, Cyber Crime Cell registered a case under Section 67 of The IT Act, 2000. A student of the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face, used a free hosting provider to create www.amazing-gents.8m.net. He regularly

uploaded "morphed" photographs of teachers and girls from his school onto the website. He was arrested when the father of one of the victims reported the case to the police.

llustration 3

In a recent case, Ms. Poorva received an e-mail message from someone who called himself 'your friend'. The attachment with the e-mail contained morphed pornographic photographs of Ms. Poorva. The mail message said that if Ms. Poorva were not to pay Rs. 10,000/- at a specified place every month, the photographs would be uploaded to the Net and then a copy sent to her fiance. Scared, Ms. Poorva at first complied with the wishes of the blackmailer and paid the first Rs. 10,000/-. Next month, she knew she would have to approach her parents.

Then, trusting the reasonableness of her fiance she told him the truth. Together they approached the police. Investigation turned up the culprit to be Ms. Poorva's supposed friend who wanted that Ms. Poorva and her fiance should break up so that she would get her chance with him. By committing this act Ms. Poorva's friend had committed crime of pornography.

9.10.2. Case Laws

1. Miller v. California, 413 US. 15 (1973)

It was an important United States Supreme Court case involving what constitutes unprotected obscenity for First Amendment purposes. The decision reiterated that obscenity was not protected by the First Amendment and established the Miller test for determining what constituted obscene material.

The Miller test has three parts:

(1) Whether "the average person, applying contemporary community standards", would find that the work, taken as a whole, appeals to the prurient interest,

Whether the work depicts/describes, in a patently offensive way, sexual conduct specifically defined by applicable state law,

Whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.

The work is considered obscene only if above all three conditions are failed.

2. United States v. Extreme Associates is a 2005 U.S.

This case law revolving around issues of obscenity. Extreme Associates, a pornography company owned by Rob Zicari and his wife Lizzy Borden (also known as Janet Romano), was prosecuted by the federal government for alleged distribution of obscenity across statelines. After several years of legal proceedings, the matter ended on March 11, 2009 with a plea agreement by Rob Zicari and Lizzy Borden.

3. State v. Customs Officer BOMBAY HC 24 November 2010.

Bombay high court held that the act of privately viewing a pornographic film in a bungalow does not amount to public exhibition, while quashing proceedings against customs officials who had attended a party in Lonavla on August 26, 2008. The police busted a party at Taj Cottage, Prichly Hill, where 28 men and 11 women had gathered. They were

intoxicated and the men were throwing noted at the dancing women while also watching a porn film. They were booked under section 292 (obscenity) of the Indian Penal Code, among others. Justice VK Tahilramani gave her verdict on five petitions and upheld the contention that whatever activities were taking place were for private viewing of the persons in the bungalow. They were not selling, hiring, circulating, producing or exhibiting the obscene film, she observed. The petitioners contended that private viewing on a personal computer does not amount to offence under section 292. The judge rejected the prosecution's statement that a bungalow is a lodge and hence a public place and that it can be said that the accused were publicly exhibiting the film. The judge noted the statement of two prosecution witnesses that the bungalow was not a lodge. Justice Tahilramani said it was not even the prosecution's case that anyone from the public could walk into it at any point. "As such, the spot where the activities took place could not be said to be a public space. Hence, it cannot be said that there was any public exhibition of obscene films in the bungalow".

4. State v. Ts.Balan & Aneesh Balan, Additional District and Sessions Court, Kerala.

The Additional District and Sessions Court here has upheld a lower court's verdict in the first cyber case filed in the State sentencing a Pentecostal Church priest and his son to rigorous imprisonment in 2006.

Disposing of the appeal filed by the priest T.S. Balan and his son, Aneesh Balan, against the order of the Chief Judicial Magistrate, on Wednesday,

Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to check the growing trend of cyber crimes in the State.

The court upheld the magistrate's order sentencing the two to three-year rigorous imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the information technology (IT) Act; awarding six months rigorous imprisonment under Section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs. 10,000 under Section 469 of the code.

The court revoked the sentence under Section 66 of the IT Act.

The cyber case dates back to January-February 2002 and the priest and his son became the first to be convicted of committing a cyber crime.

The two were found guilty of morphing, web-hosting and e-mailing nude pictures of Pastor Abraham and his family.

Balan had worked with the pastor until he fell out with him and was shown the door by the latter.

Balan joined the Sharon Pentecostal Church later.

The prosecution said the duo had morphed photographs of Abraham, his son, Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs with captions.

The morphed pictures were put on the web and the accused, who edited a local magazine called The Defender, wrote about these photos in his publication.

Valsan received the pictures on the Internet and asked his father to file a complaint to the police. A police party raided the house of Balan and his son at Perumbavoor and collected evidences.

The magistrate's verdict came after a four-year trial, for which the court had to procure a computer with Internet connection and accessories.

The police had to secure the services of a computer analyst too to piece together the evidences. Twenty-nine witnesses, including the internet service provider and Bharat Sanchar Nigam Ltd., had to depose before the court.

9.10.3. International Perspective:

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;

Worldwide access, reaching a significantly larger number of customers than retail shops;

- The Internet is often viewed as an anonymous medium (often erroneously)— an aspect that consumers of pornography appreciate, in view of prevailing social opinions.
- Recent research has identified as many as 8.2 million pornographic websites that may be available on the Internet at any time. Besides websites, pornographic material can be distributed through:
- Exchange using file-sharing systems;
- Exchange in closed chat-rooms.

Different countries criminalise erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material, seeking to protect minors. Studies indicate that child access to pornographic material could negatively influence their development. To comply with these laws, "adult verification systems" have been developed. Other countries criminalize any exchange of pornographic material even among adults, without focusing on specific groups (such as minors).

For countries that criminalize interaction with pornographic material, preventing access to pornographic material is a challenge. Beyond the Internet, authorities can often detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often readily available on servers outside the country, enforcement is difficult. Even where authorities are able to identify websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers. The principle of

National Sovereignty does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities. Even when authorities seek the support of countries where offensive websites are hosted, successful investigation and criminal sanctions may be hindered by the principle of "dual criminality''. To prevent access to pornographic content, countries with exceptionally strict laws are often limited to prevention (such as filter-technology) to limit access to certain websites.

9.11. Child Pornography

9.11.1. What is Child Pornography?

Child pornography refers to images or films (also known as child abuse images) and in some cases writings depicting sexually explicit activities involving a child; as such, child pornography is a record of child sexual abuse.

Under The IT Act, 2000 as amended by the Information Technology (Amendment) Act, 2008, crime of Child Pornography under Section 67-B say's, Whoever publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or facilitates abusing children online or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children is known as child pornography.

Illustration 1

Mumbai Police arrested an army officer from his residence for allegedly uploading obscene photographs and video clips involving children on the Internet. The German Police while looking for Internet — related offences, had come across the obscene contents being uploaded on a child pornography site from Mumbai. They brought the issue before the Interpol, which alerted the CBI in Delhi in March 2010. The CBI passed on the information to the Mumbai Police which nabbed the Army officer and seized incriminating objects from his house.

Army officer, who was with the Army from 20 years, has "downloaded all child pornography material from the Internet. Police were awaiting forensic report of the two hard disks, containing hundreds of obscene photographs and video clips, seized from Army officer's residence. This act of uploading obscene photographs and video clips of children's on Internet is an act of child pornography.

Illustration 2

The cyber crime police arrested Will Heum (56), a Dutch national living in Chennai, for uploading child pornographic materials on the Internet. Police recovered his personal computer and pornographic materials from his house. Heum is already facing a case in a Chengalpattu court for sexually abusing children of Little Home, an orphanage he had opened near Mamallapuram. He was arrested in May 2002. Out on bail and living in a rented house in Choolaimedu, he was uploading pictures of children being sexually abused, police said.

This is the first case of child pornography to be registered in the country under the IT Act, which came into force on October 27, 2009. Heum was booked under Section 67-B of the IT Act, 2008, which deals with child pornography, and remanded in judicial custody after being produced before the XI metropolitan magistrate court in Chennai. A tip-off from the Child Exploitation Online Protection Centre in Germany through Interpol that led to the arrest of Heum.

Illustration 3

An undercover agent downloaded 11 files containing child pornography from a file sharing program in December 2008. According to a plea agreement in the case. A computer and other electronic devices seized during a February 2009 raid on his home turned up 88 images and 12 video files of minors being sexually abused. This agent admitted computer contained more than 600 images of child pornography.

Illustration 4

In Stockport, Manchester police arrested Harry P., former RAF engineer, and found 20,000 images of child pornography in his computer. Harry's computer provided the police more up to date information on the Wonderland Club and improved the chance of online tracking. Harry P. turned out to be one of the key members. As he was actively abusing children producing images for others, this enhanced Harry's status within the Club. Three members of the Club actually travelled to Stockport to Harry's home address and had pictures taken on his bed with the victims. Those pictures did not contain indecent poses but were apparently taken, as one of the members e-mailed them round the net, as some remembrance of the visit to Harry's house. Harry was sentenced to prison for abuse of three children's for the crime of the child pornography.

Illustration 5

In Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophile. The Mumbai police arrested the couple for child pornography.

9.11.2. Case Law

1. Hari Ram v. State of Rajasthan & Anr, Criminal Appeal No. 907 OF 2009 (Arising out of S.L.P. (Crl.) No.3336 of 2006)

   "The law as now crystallized on a conjoint reading of Sections 2(k), 2(l), 7A, 20 and 49 read with Rules 12 and 98, places beyond all doubt that all persons who were below the age of 18 years on the date of commission of the offence even prior to 1st April, 2001, would be treated as juveniles, even if the claim of juvenility was raised after they had attained the age of 18 years on or before the date of commencement of the Act and were undergoing sentence upon being convicted."

2. The Delhi Public School Case

   A Eleventh standard student while having the oral sex with a girl student recorded the clip of approximately 2.30 minutes by his mobile and circulated amongst his friends.The students were expelled from the school and two arrests were also made in the same conjunction. Later the student arrested was granted bail.

3. The Air Force Balbharati School Case.

In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT Act, 2000. A student of the Air Force Balbharati School, New Delhi,, was teased by all his classmates for having a pockmarked face. He decided to get back at his tormentors. He created a website at the URL www.amazing-gents.8m.net. The website was hosted by him on free web space. It was dedicated to Air Force Bal Bharti School and contained text material. On this site, lucid, explicit, sexual details were given about various "sexy" girls and teachers of the school. Girls and teachers were also classified on the basis of their physical attributes and perceived sexual preferences. The father of the girl, being an Air Force officer, registered a case under section 67 of the IT Act, 2000 with the Delhi Police Cyber Crime Cell. The police picked up the concerned student and kept him at Timarpur (Delhi) juvenile home. It was almost after one week that the juvenile board granted bail to the 16- year-old student.

4. International Perspective

In contrast to differing views on adult pornography, child pornography is broadly condemned and offences related to child pornography are widely recognized as criminal acts. International organizations are engaged in the fight against online child pornography, with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child; the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography; and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others.

Sadly, these initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography. An increase in bandwidth has supported the exchange of movies and picture archives.

Research into the behavior of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80 per cent had pictures of children between 6-12 years on their computer; 19 per cent had pictures of children younger than the age of 3; and 21 per cent had pictures depicting violence.

The sale of child pornography is highly profitable with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context. Search engines find such material quickly. Most material is exchanged in password-protected closed forums, which regular users and law enforcement agencies can rarely access. Undercover operations are thus vital in the fight against child pornography.

Two key factors in the use of ICTs for the exchange of child pornography pose difficulties for the investigation of these crimes:

1. The use of virtual currencies and anonymous payment:

Cash payment enables buyers of certain goods to hide their identity, so cash is dominant in many criminal businesses. The demand for anonymous payments has led to the development of

virtual payment systems and virtual currencies enabling anonymous payment. Virtual currencies may not require identification and validation, preventing law enforcement agencies from tracing money-flows back to offenders. Recently, a number of child pornography investigations have succeeded in using traces left by payments to identify offenders. However, where offenders make anonymous payments, it is difficult for offenders to be tracked.

2. The use of encryption technology:

Perpetrators are increasingly encrypting their messages. Law enforcement agencies note that offenders are using encryption technology to protect information stored on their hard disks, seriously hindering criminal investigations.

In addition to a broad criminalization of acts related to child pornography other approaches such as the implementation of obligations of Internet Service to register users or to block or filter the access to websites related to child pornography are currently implemented internationally.

9.12. Online Gambling

9.12.1. What is Online Gambling?

Gambling in India is prohibited under the Public Gambling Act 1867. However the word 'gambling' is not defined in the Public Gambling Act 1867. According to the Supreme Court of India, "Gaming is the act or practice of gambling on a game of chance. It is staking on chance where chance is the controlling factor. 'Gaming' in the two Acts would, therefore, mean wagering or betting on games of chance. It would not include games of skill like horse racing". The supreme court in the case of 'State of Andhra Pradesh v. K. Satyanarayan' (1967) stated that 'Rummy' cannot be called a "game of entire chance" and "is mainly and preponderantly a game of skill". Moreover in the case of 'M.J.Sivani v. State of Karnataka' (1995) the Supreme Court ruled that when the element of chance preponderates in a game, it cannot be a game of mere skill.

Thus it is now clear that an act is gambling if it depends upon chance and there is no skill involved in the act. 'Skill' and 'chance are the determining factors in this regard. When the dominant element in a game is 'chance' and not 'skill' then such a game is definitely gambling. However section 12 of the Public gambling Act provides that the foregoing provisions of this Act shall not apply to any game of mere skill wherever played.

There are thousands of Websites that offer online Gambling. The special issue with online gambling is that it is legalized in several countries. So legally the owners of these websites are safe in their home countries. Virtual casinos, Cases of money laundering etc are online cases.

The law related to gambling is also applicable to online gambling. All gambling contracts are considered to be wagering contracts and it is not possible to enforce such contracts under the ICA, detailed above.

9.12.2. Regulation of gambling

The courts have defined gambling as 'the payment of a price for a chance to win a prize'. The dominant element of skill or chance shall determine the nature of the game. A game may be

deemed to be gambling if the element of chance or luck predominates in deciding its outcome. As a result, Indian courts have held that betting on horse racing and a few card games are not gambling. The right to undertake the business of gambling and lotteries is not considered as a fundamental right protected by the Constitution of India. It may however be pointed out that the state government run lotteries make significant contributions to the state exchequer of several state governments and the Union government, and hence there is a resistance to complete prohibition. The following legislation is pertinent to gambling:

The Public Gaming Act, 1867

This Act provides punishment for public gambling and for keeping of a 'common gaming house'. This Act also authorizes the state governments to enact laws to regulate public gambling in their respective jurisdictions. The penal legislations in respective states have been amended in accordance with their policy on gambling. However, this legislation does not have any direct impact on online gambling unless a wide interpretation is given to the definition of common gaming house so as to include virtual forums as well.

The Indian Contract Act, 1872 (ICA)

The ICA is a codified umbrella legislation that governs all commercial contracts in India. Under the ICA, a wagering contract is the one which cannot be enforced. The Act lays down; 'Agreements by way of wager are void, and no suit shall be brought for recovering anything alleged to be won on any wager or entrusted to any person to abide by the result of any game or other uncertain event on which any wager is made'. Gambling, lottery and prize games have held to be wagering contracts and thus void and unenforceable. While a wagering contract is not illegal, it cannot be enforced in a court of law. Thus, the courts will not entertain any cause of action that arises out of a wagering contract.

Lotteries (Regulation) Act, 1998

This Act provides a framework for organizing lotteries in the country. Under this Act, the state governments have been authorized to promote as well as prohibit lotteries within their territorial jurisdiction. This Act also provides for the manner in which the lotteries are to be conducted and prescribes punishment in case of breach of its provision. Lotteries not authorized by the state have been made an offence under the Indian Penal Code. Several non-lottery playing states, like Gujarat and Uttar Pradesh, have prohibited the sale of other state-government lotteries under this Act.

Indian Penal Code, 1860

Section 294A deals with keeping lottery office. It says that whoever keeps any office or place for the purpose of drawing any lottery not being a State lottery or a lottery authorized by the State Government, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine, or with both and whoever publishes any proposal to pay any sum, or to deliver any goods, or to do or forbear doing anything for the benefit of any person, on any event or contingency relative or applicable to the drawing of any ticket, lot, number or figure in any such lottery, shall be punished with fine which may extend to one thousand rupees.

Illustration 1

Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net'. Whenever accessed, the site would name him as the beneficiary of the 12.5/- million. After confirmation a telugu newspaper published this as news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency.

However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs. 1.73/- million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of Rs. 12.5/- million was held in his name.

Illustration 2

The website getwin.com permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics, rugby, volleyball, motor cycling etc.

Additionally it also has links to online casino. The website has no technical measures in place to prohibit residents of India (where online gambling is illegal) from betting at their website. Indian citizens if caught gambling on this website would be booked under Indian laws.

9.12.3. International Perspective

Internet games and gambling are one of the fastest-growing areas in the Internet. Linden Labs, the developer of the online game Second life, reports that some ten million accounts have been registered. Reports show that some such games have been used to commit crimes including:

- Exchange and presentation of child pornography;
- Fraud;
- Gambling in online casinos; and
- Libel (e.g. leaving slanderous or libellous messages).

Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 34 billion in 2011 for Internet gambling (although compared with revenues from traditional gambling, these estimates are still relatively small).

The regulation of gambling over and outside the Internet varies between countries - a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 16.8 billion in 2012, it took the lead from Las Vegas (USD 16.6 billion). Macau's success derives from the fact that gambling is illegal in China and thousands of gamblers travel from Mainland China to Macau to play.

The Internet allows people to circumvent gambling restrictions. Online casinos are widely available, most of which are hosted in countries with liberal laws or no regulations on Internet gambling. Users can open accounts online, transfer money and play games of chance. Online casinos can also be used in money-laundering and activities financing terrorism. If offenders use online casinos within the laying-phase that do not keep records or are located in countries without money-laundering legislation, it is difficult for law enforcement agencies to determine the origin of funds. It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online gambling. There have been several legislative attempts to prevent participation in online gambling: notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.

9.13. Forgery

9.13.1. What is Forgery?

According to Indian Penal Code, 1860 Forgery means whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract or with intent to commit fraud or that fraud may be committed commits forgery.

Forgery is the process of making, adapting or imitating objects, statistics or documents with the intent to deceive copies, studio replicas, and reproductions are not considered forgeries, though they may later become forgeries through knowing and willful misrepresentations. Forging money or currency is more often called counterfeiting. But consumer goods may also be counterfeits if they are not manufactured or produced by the designated manufacture or producer given on the label or flagged by the trademark symbol. When the object forged is a record or document it is often called a false document, Tampering computer source documents.

Illustration 1

In October 1995, economic offences wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desk Top Publishing Systems. This constitutes forgery using computer.

Illustration 2

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totalling several billion rupees. He had committed crime of forgery which rocked the country and accounted for serious losses to the government exchequer. Government had to change certain rules relating to stamp papers later in the view of Telgi matter.

9.14. Denial of Service Attack

9.14.1. What is Denial of Service Attack?

Denial of Service attacks (DOS attacks) involves flooding a computer with more requests than it can handle. This causes the computer (e.g. a web server) to crash and results in authorized users being unable to access the service offered by the computer. It also says that, an attack against a

Those who govern must see how the people react to administration. Ultimately, the people are the final arbiters.
- Lal Bahudur Shastri

computer or network that attempts to limit or prevent access to the Internet by flooding it with requests (for a webpage or online resource) or email (causing the email system to overload).

9.14.2. Explanation of Denial of Service Attack

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems attack a single target. Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. A denial of service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced Web sites accessed by millions of people to temporarily cease operation.

Denial-of-service attacks have had an impressive history having, in the past, blocked out websites like Amazon, CNN, Yahoo, eBay and future bazzar.com. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the server's crash. Sometimes, many computers are entrenched in this process by installing a Trojan on them; taking control of them and then making them send numerous demands to the targeted computer.

Illustration 1

If a aggrieved student of university continuously sends thousands of requests to university website and because of this act university website is rendered non accessible to other legitimate students who also want to access the university website thus denying service such a act on the part of aggrieved student can be called as denial of service attract.

Illustration 2

A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com. In distributed denial of service attacks, the attacker uses zombie's i.e. computer's which are unknowingly used by the attacker to simultaneously attacker the target. These zombies's innocently became the crime abetters.

Illustration 3

A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007. The attacks were apparently connected with protests against the Estonian government's decision to remove a Soviet-era war memorial from the capital city. It is suspected that the attacks were carried out by Russian hackers. The attack lasted several days.

9.15. Web Defacement

9.15.1. What is Web Defacement?

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.

Illustration 1

Mr. Mahesh Mhatre and Mr. Anand Khare were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell. They had allegedly used password cracking software to crack the FTP password of the police website. They then replaced the homepage of the website with pornographic content. This act constituted website Defacement.

Illustration 2

As of 2010 over 1981 Indian websites were hacked into and defaced. The hackers put in words like bugz, death symbol, Paki-king. In the case of 123medicinindia.com, a message was left behind which said - "Catch me if u can my deraz lazy adminzzz" — challenging the system administrators to trace the miscreants. The offenders were allegedly a group of hackers who go by various names either they are Chinese or Pakistanis or Nigerians or disgruntled Indian Citizens, but this act Constitutes website Defacement.

9.16. Web Jacking

9.16.1. What is Web Jacking?

When someone forcefully takes control of a website (by cracking the password and later changing it) The actual owner of the website does not have any more control over what appears on that website it is known as web jacking. The word web jacking is derived from the word hijacking. Web jacking takes place when a hacker forcefully gains control of a website by cracking the password. The actual owner does not have any control on the website, but the hacker can change the contents of the websites. The Gold fish case is an example of web jacking in which the site was hacked and the information relating to gold fish was changed.

9.16.2. Explanation of Web Jacking

The administrator of any website has a password and a username that only he (or someone authorized by him) may use to upload files from his computer on the web server where his website is hosted. Ideally, this password remains secret with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator.

Computers doesn't recognize people but recognizes only usernames and passwords. The web server will grant control of the website to whoever enters the correct password and username combination. There are many ways in which a hacker may get to know a password, the most common being password cracking wherein a "cracking software" is used to guess a password. Password cracking attacks are most commonly of two types.

The first one is known as the dictionary attack. In this type of attack the software will attempt all the words contained in a predefined dictionary of words. For example, it may try Rahim, Rahul, Rakesh, Ram, Reema, Reena ... in a predefined dictionary of Indian names. These types of dictionaries are readily available on the Internet.

The other form of password cracking is by using 'brute force'. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, and letters till the correct password is found. For example, it may try out password combinations like abc123, acbd5679, sdj#%^, weuf*(-)*. Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second. When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

Illustration 1

In an incident reported in the USA, the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her.

The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'.

In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

Illustration 2

XM group, a group of diversified companies, had given there 12 different websites to be hosted, designed and maintained to one M/S ebizy solutions, XM group had paid there complete money for domain registrations and part money of designing of websites. One fine day ebizy solutions makes all websites of XM group offline and does not share the password with XM group citing reasons of non-payment etc. This act of ebizy solutions may be termed as web jacking.

9.17. Illegal Online Selling

9.17.1. What is Illegal Online Service?

It is becoming increasingly common to find cases where sale of illegal articles such as counterfeit currency, counterfeit branded products, narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles. Additionally, there are several online payment gateways that can transfer money around the world at the click of a button.

The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as "Internet pharmacies". These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs. This poses a serious potential threat to the health and safety of patients. The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

As pointed out earlier, the online lottery is the most popular form of Internet gambling in India. Most companies marketing and distributing or conducting state government-sponsored lotteries through the Internet are not allowed to sell their services in the states that banned lotteries. In most cases, these marketers and distributors limit their online services to consumers who are residents of the states where a lottery is permissible. Notwithstanding the fact there has been no reported case of breach by any company promoting online lotteries, most of these companies (as a safeguard) seek an undertaking from their consumers relating to their residence.

There have been instances where one state has banned the lottery of other states, including online lotteries. In a recent case, the Karnataka High Court upheld the decision of the Karnataka government to make itself a 'lottery free zone' by imposing a ban on lotteries of all other states, including online lotteries under the Lotteries (Regulation) Act 1998. The state government, in this case, directed the closure of the terminals and kiosks selling the online lotteries.

Illustration I

In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site, Orkut.com, was believed to be one of the modes of communication for gathering people for the illegal "drug" party. Such an act of selling tickets of an illegal party or gathering or directly selling banned drugs is an act of illegal selling on internet.

Illustration 2

An suspect creates an email ID using fictitious details. He then posts messages, about the illegal products, in various chat rooms, bulletin boards, newsgroups etc. Potential customers can contact the seller using the email IDs provided. The motive behind the act is Illegal financial gain.

Illustration 3

If a person sells Guns, RDX, Bullets, confidential papers on a website either created by him or on commercial website. This action amounts to illegal selling of goods on internet.

9.17.2. Case Law

1 Sanjay Kumar Kedia v. Narcotics Control Bureau 2007 SC.

The Supreme Court deciding a special leave petition touched on Section 79 of the Information Technology Act, 2000. The Petitioner (Sanjay Kumar Kedia) was ostensibly running an online pharmacy which was allegedly used to sell psychotropic substances to customers without prescriptions. He was subsequently issued a notice Section 67 of the Narcotic Drugs and Psychotropic Substances Act, 1985. Thereafter the petitioner filed an application for bail several times which was rejected by the courts and hence preferred the special leave petition to appeal against the orders

for refusal of bail. The counsel for the petitioner cited section 79 as a defense stating that it granted immunity from prosecution. He stated that the companies of the petitioner only provided third party data and information without any knowledge as to the commission of an offence under the Act. The respondents (Narcotics Control Bureau) rebutted this by stating that the petitioner and its associates are not an intermediary as defined under section 79 of the said Act as their acts and deeds was not simply restricted to provision of third party data or information without having knowledge as to commission of offence under the NDPS Act. The company (Xponse Technologies Ltd. And Xpose IT Services Pvt. Ltd headed by Sanjay Kedia) has designed, developed, hosted the pharmaceutical websites and was using these websites, huge quantity of psychotropic substances (Phentermine and Butalbital) have been distributed in USA with the help of his associates. The Supreme Court quite correctly applying the law as it stands held that (a) the petitioner was not an innocent intermediary as defined under section 79 of the Technology Act according to the investigating agencies, they were the owners and were responsible for the contents therein; and (b) Section 79 will grant immunity to an accused who has violated the provisions of the Information Technology Act, 2000 and not grant an immunity under the Narcotic Drugs and Psychotropic Substances Act, 1985.

9.18. Cyber Defamation

9.18.1. What is Cyber Defamation?

According to Wikipedia, Cyber Defamation is a crime conducted in cyberspace, usually through the Internet, with the intention of defaming others. Sending defamatory email, writing derogatory comments on facebook, orkut or other social networking sites also constitutes cyber defamation. The Internet can be used to spread misinformation, just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators. Minors are increasingly using web forums and social networking sites where such information can be posted as well. Criminal behavior can include (for example) the publication of intimate photographs or false information about sexual behaviors.

In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID. This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators. These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia, where strict procedures exist for the regulation of content. However, the same technology can also be used by offenders to:

- Publish false information (e.g. about competitors);
- Libel (e.g. leaving slanderous or libellous messages);
- Disclose secret information (e.g. the publication of State secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as

online statements are accessible to a worldwide audience. The moment information is published over the Internet, the author(s) often loses control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated ("mirroring") and made available by people that are unwilling to rescind or remove it. In this case, information may still be available in the Internet, even if it has been removed or corrected by the original source. Examples include cases of 'runaway e-mails', where millions of people can receive salacious, misleading or false e-mails about people or organizations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech and protection of the potential victims of libel needs to be well balanced.

Illustration 1

Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut. Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile.

The profile had been sketched in such a way that it drew lewd comments from many who visited her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

Illustration 2

India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Illustration 3

The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer. The lawyer took exception to a community called 'We hate India', owned by someone who identified himself as Miroslav Stankovic. The community featured a picture of the Indian flag being burnt. This act constitutes cyber defamation of the country.

Illustration 4

Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Suggestive names like 'sex teacher" were posted on the profile. The matter came to light after the girl's family started receiving vulgar calls referring to Orkut. The girl was badly cyber defamed.

Illustration 5

A son of Cola Company's CEO studying in 9th standard of a convent school made a fake facebook profile and hosted his juvenile ex-girlfriends photograph. He also wrote a foot note "I

am a call girl" along with her mobile number. This juvenile girl got hundreds of unsolicited & abusive calls. This act of the juvenile boy constitutes cyber defamation of the girl.

Illustration 6

A tweet from a disgruntled/frustrated employee tarnished the MNC Company's reputation in the job market so much, it affected its recruitment process. This tweet also simultaneously released potentially confidential information to competitors.

9.18.2. Case Laws

1. Tata Sons v. Greenpeace International Delhi HC IA 9089/2010 in CS (OS) 1407/2010

   Justice S. Ravindra Bhat, authoring the judgment noted that, though the internet has a wider reach and potential for injury, traditional standards for the grant of injunctions in cases of libel will be applicable. The court reasoned that these traditional standards are well developed and there is no constitutional mandate which allows the court to create a differentiation. If this reasoning is strictly applied it would mean that the conventional rules of defamation will be applied in cases of internet defamation. If applied liberally, courts may in cases of a legislative vacuum, apply other developed legal principles without differentiation. [Cyber defamation Injunction not granted].

2. Gremach Infrastructure Equipments & Projects Limited & Ors v. Google India Private Limited. 508/2008 Bombay HC, Order passed by Justice DR. D. Y. CHANDRACHUD Google Inc. is the owner of the popular blogging platform Blogpost. Blogpost hosted a blog by one toxicwriter (a pseudonym chosen by the blogger to mask his/her identity). The writer had allegedly written certain defamatory comments about an Indian Mining Company. The Bombay High Court found the postings prima facie defamatory and ordered Google to reveal toxicwriter's identity. This is only the interim order. It is unclear as to whether the company has asked for damages against google (and whether safe harbors will come into play).

   Google seeked to comply with the order as not only the blog which was available at www.toxicwriter.blogspot.com but also its cache is available on Google. A few snapshots though were made available on another website. Free Speech and Privacy issues notwithstanding Google may give the identifying information of the blogger. The reason for this is its own privacy policy. It stated that, "[w]e have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request.

3. Lalit Modi Case

   In Chris Lance Cairns v. Lalit Modi [2010] EWHC 2859 (QB) the London High Court Queen's Bench Division has allowed a former cricketer accused of match fixing over Twitter to continue with the libel action to trial in order to protect and vindicate his reputation.

4. Moore v. Allen

   Statements at issue were truthful and therefore not defamatory however the case was decided in favor of the plaintiff under a claim of "tortuous interference with employment contracts.

"The plaintiff was awarded $60,000 in damages against a blogger who posted truthful information about him that contributed to his losing his job.

9.19. Software Piracy

9.19.1. What is Software Piracy?

Software piracy is unauthorized copying and use of Software without proper license. Similarly, simultaneous use of single user license software by multiple users or loading of single user license software at multiple sites, also amounts to software piracy. By buying software, one only becomes a licensed user and not an owner. One can make copies of the program only for back-up purposes, but it is against the law to give copies to friends and colleagues or sell such copies to others. It is not possible to completely eliminate Software piracy, but the same can be controlled by enforcing the laws and generating awareness in the society.

Buying a Software Owning a Software

Buying a software = Becoming licensed to use it under certain restrictions.

Any Copyright infringement is the unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as, the right to reproduce or to make derivative works that build upon it. For electronic and audio-visual media, such unauthorized reproduction and distribution of a copyrighted work is often referred to as piracy (however there is no legal basis for the term 'piracy').

The society doesn't really treat software piracy like other kinds of theft as nothing is physically taken away. There is no immediate effect on the inventory or productive capacity of the programmer. Only copies of the disk or other storage medium are made and the legal owner is still in possession of the software. With digital technology, perfect copies of the original can be made in no time. Most often, the actual cost of creating goods is determined by the production cost of individual item. However with software, the reverse is true. The cost of producing copies is negligible compared to the cost of constructing the original. Hence it becomes very easy and all the more attractive to make copies of unauthorized software.

Illustration 1

Mr. Shanti bhai had all legal software's like OS, Office Software, tally etc. in his office. In March 2011, his son was to be wedded so his son thought of making a marriage invitation, existing legal software's were not suited for making graphical invitations. His friend suggested him to borrow his legal corel draw package and install it on his computer and when the work is accomplished remove the installation. The moment Shanti bhai's son installed the borrowed software on his computer, he committed an act of software piracy.

Illustration 2

One Mr. Bam for only once for the sake of converting one commercial design form from Microsoft word format to pdf, installed in his computer trial version of Adobe acrobat professional and accomplished his commercial work, this knowingly undertaken act of Mr. Bam constitutes Software Piracy.

Success in science and scientific work come not through the provision of unlimited or big resources, but in the wise and careful selection of problems and objectives. Above all, what is required is hard sustained work and dedication.
- Lal Bahudur Shastri

Illustration 3

Mr. Khurana buys a pirated Game DVD from roadside CD, DVD seller, this very act of Mr. Khurana of knowingly buying a pirated games DVD constitutes a crime of software piracy.

9.19.2. Case Laws

1. Microsoft Corporation v. Yogesh Papat, Delhi HC

   The court approached each piece of evidence in turn and, based on the assumption that 100 computers were sold each year and on the evidence of the software's popularity, held that Microsoft had suffered a total profit loss of Rs. 1.98 million, plus interest at 9% from the date of the decree until the date of payment.

   Justice Predeep Nandrajog, who presided in this case, stated that:

   "It stands established that the defendant has infringed the plaintiffs copyright by making illicit copies of the operating systems software by openly copying whatever operating system is currently saleable."

2. Autodesk, Inc. & Another v. Mr. Prashant Deshmukh & Others

   The court here raised concerns about increasing instances of piracy of software of reputed companies such as Microsoft and AutoCAD in the country, which might cause discouragement amongst the investors in the development of such software in the lack of dwindling license fees. Furthermore, the use of pirated software for commercial rather than personal purposes should, according to the court, be more heavily frowned upon, and therefore the court awarded the plaintiffs the permanent injunction sought for as also punitive damages amounting to Rs. 1 lakh against Defendant No. 2.

3. Apple Computer, Inc v. Franklin Computer Corp

   In this case, it was held that the copyright Act extends to operating programmes as well as application programmes, whether fixed in source code or object code or embodied in read only memory. (ROM)

4. Whelam Association Inc, v. Jaslow Dental Laboratory Inc., 797.F.2d.l22. (3rd. Cir 1986).

   In this case, the court held that it is not necessary for the computer's program's purpose or function including its structure, sequence and organization.

5. Playboy Enterprises, Inc, v. Frena

   Here the defendant operated a subscription bulletin board service. Once logged into the BBS, subscribers could view or download any of the 170 computerized photographs that were copyrighted by playboy Enterprises. The court held that because the defendant supplied the product which was copyrighted, he was liable, since public display and distribution of the photographs were in violation of the plaintiffs copyright.

9.20. Electronic / Digital Signature

9.20.1. What is Electronic/Digital Signature

Information Technology (Amendment) Act, 2008, Section 2 (p), "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or

procedure in accordance with the provisions of Section 3; and Section 2(ta) electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature.

9.20.2. Explanation of Digital / Electronic Signature

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signature of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Publishing a Electronic Signature Certificate false in certain particulars is a cyber crime and knowingly creates or publishes a Electronic Signature Certificate for any fraudulent or any unlawful purpose is a cyber crime.

Illustration 1

Mr. Deshpande publishes his Electronic Signature but the issuing certifying authority (CA), which is shown on his Electronic Certificate does not confirm issuance of the said certificate because Mr. Deshpande has faked CA's name on the electronic certificate. This act of Mr. Deshpande is a cyber crime.

Illustration 2

Mr. Tiwari enters into a transaction of E-Contract with an USA based software company. He signs this contract with the Electronic Signature which was revoked by the Certifying Authority and which is no longer valid. The act of Mr. Tiwari knowingly signing using revoked or suspended certificate is a cyber crime.

अध्याय 10
Chapter 10

Tools and Methods Used in Cyber Crime

10.1. Introduction

In this chapter, we will focus upon different forms of attacks through which attackers target the computer systems. There are various tools and techniques and complex methodologies used to launch attacks against the target. Although discussing all of them is virtually impossible in a single chapter, yet still, we have provided an insight toward these techniques to enable the reader to understand how the computer is an indispensable tool for almost all cybercrimes. As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it.

Network attack incidents reveal that attackers are often very systematic in launching their attacks. The basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. **Initial uncovering:** Two steps are involved here. In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means — searching the information about the target on the Internet by Googling social networking websites and people finder websites. The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute. In the second step, the attacker uncovers as much information as possible on the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges. From prevention perspective, at this stage, it is really not possible to detect the attackers because they have done nothing illegal as yet and so their information requests are considered legitimate.

Scareware, Malvertising, Clickjacking and Ransomware

1. **Scareware:** It comprises several classes of scam software with malicious pay loads or of limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. Some forms of Spyware and Adware also use scareware tactics. Some websites display pop-up advertisement windows or banners with text such as: "Your computer may be infected with harmful Spyware programs. Immediate removal may be required. To scan, click 'Yes' below." These websites can go as far as saying that a user's job, career or marriage would be at risk. Webpages displaying such advertisements for such products are often considered as scareware. Serious scareware applications qualify as rogue software.

2. **Malvertising:** It is a malicious advertising - malware + advertising - an online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space. Cybercriminals attempt to distribute malware through advertising. Possible vectors of attack include Malicious Code hidden within an advertisement embedded into a webpage or within software which is available for download.

3. **Clickjacking:** It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages. Clickjacking takes the form of embedded code and/or script which is executed without netizen's knowledge Cybercriminals take the advantage of vulnerability across a variety of browsers and platforms to launch this type of attack, for example clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hansen in 2008. The exploit is also known as User-Interface (Ul) redressing.

4. **Ransomware:** It is computer malware that holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration. It typically propagates as a conventional computer worm, entering a system through, for example, vulnerability in a network service or an E-Mail attachment. It may then

   - disable an essential system service or lock the display at system start-up and
   - encrypt some of the user's personal files.

   In both cases, the malware may extort by

   - prompting the user to enter a code obtainable only after wiring payment to the attacker or sending an SMS message and accruing a charge;
   - urging the user to buy a decryption or removal fool.

5. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool is used to discover exactly which services are running on the target system. At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion. Crossing the line toward electronic crime (E-crime): Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system. The attacker usually goes through several stages of exploits to gain access to the system. Certain programming errors can be used by attackers to compromise a system and are quite common in practice. Exploits usually include vulnerabilities in common gateway interface (CGI) scripts or well-known buffer-overflow holes, but the easiest way to gain an entry is by checking for default login accounts with easily guessable (or empty) passwords. Once the attackers are able to access a user account without many privileges, they will attempt further exploits to get an administrator or "root" access. Root access is a Unix term

Table : Websites and tools used to find the common vulnerabilities

Website	Brief Description
http://www.us-ccrt.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cyber security. US-CERT publishes information about a variety of vulnerabilities under "US-CERT Vulnerabilities Notes."

http://cve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackerstorm.com/	This website was created for open-source vulnerability database (OSVBD) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.
http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.zone-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced web pages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http.www.osvdb.org/	OSVDB: This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing, its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.wOOwOO.org/files/ LibExpIoit	LibExploit is a generic exploit creation library. It helps cyber security community when writing exploits to test vulnerability.
http://www.immunitysec.com/ products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitels ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugin for drag and drop GUI exploit creation (optional).
http://www.coresecurity.com/content/ core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems). "Root" is basically an administrator or super-user access and grants them the privileges to do anything on the system.

Very often I indulge in less vigorous pranks with children who can afford to give me the benefit of their company. It is only so long as a man can retain the child in him that life can be free from those dark shadows which leave inevitable furrows on a man's forehead. ***- Sardar Vallabhbhai Patel***

6. Capturing the network: At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files and services that have a backdoor password. There are a number of "hacking tools" which can clean up log files and remove any trace of an intrusion; most of the time, they are individual programs written by hackers. Such tools provide copies of system files that look and act like real thing, but in fact they provide the attacker a backdoor entry into the system and hide processes he/she might be running on that system and his/her user information. This allows the attacker to return to the system at will, which means that the attacker has "captured" the network. Once the attacker has gained access to one system, he/she will then repeat the process by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defenses against attacks from internal sources.

7. Grab the data: Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.

8. Covering tracks: This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected. The attacker can remain undetected for long periods or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action, etc.

   During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself. How is it possible is described in the next section.

10.2. Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network.

The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy. This enables an attacker to surf on the Web anonymously and/or hide the attack. A client connects to the proxy server and requests some services (such as a file, webpage, connection or other resource) available from a different server. The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client. Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).

2. Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.

3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address (visit http://www.multiproxy.org/multiproxy.htm for more information).

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact there are special servers available known as cache servers. A proxy can also do logging.

Listed are few websites where free proxy servers can be found:

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information. Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client. In 1997 the first anonymizer software tool was created by Lance Cottrell, developed byAnonymizer.com. The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user.

Phishing

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail. This message and other such messages are examples of Phishing — in addition to stealing personal and financial data — and can infect systems with viruses and also a method of online ID theft in various cases. Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. These messages look authentic and attempt to get users to reveal their personal information.

Note: It is believed that Phishing is an alternative spelling of "fishing," as in "to fish for information/ The first documented use of the word "Phishing" was in 1996.

How Phishing Works?

Phishers work in the following ways:

1. Planning: Criminals, usually called as phishers, decide the target (i.e., specific business/business house/an individual) and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
2. Setup: Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.

One individual may die for an idea; but that idea will, after his death, incarnate itself in a thousand lives. That is how the wheel of evolution moves on and the ideas and dreams of one nation are bequeathed to the next.
- Netaji Subhash Chandra Bose

3. Attack: This is the step people are most familiar with - the phisher sends a phony message that appears to be from a reputable source.
4. Collection: Phishers record the information of victims entering into webpages or pop-up windows.
5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Phishing started off as being part of popular hacking culture. Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

10.3. Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system. Usually, an attacker follows a common approach - repeatedly making guesses for the password. The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information . Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. users name or login name;
5. name of user's friend/relative/pet;
6. users birthplace or date of birth, or a relatives or a friends;

7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is still considered manual cracking, is time-consuming and not usually effective.

Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format. For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called authentication.

Even though these functions create hashed passwords, which may be cryptographically secure, an attacker attempts to get possession of the hashed password, which will help to provide a quick way to test guesses for the password by applying the one-way function to each guess and comparing the result to the verification data. The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools to get the plain text password.

Password cracking attacks can be classified under three categories as follows:

1. On line attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving)

10.3.1. Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack." It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle). This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

10.3.2 Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used. Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

10.3.3. Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak.

Here are some of the examples of "weak passwords":

1. Susan: Common personal name;
2. aaaa: repeated letters, can be guessed;
3. rover: common name for a pet, also a dictionary word;
4. abcl23: can be easily guessed;
5. admin: can be easily guessed;
6. 1234: can be easily guessed;
7. QWERTY: a sequence of adjacent letters on many keyboards;
8. 12/3/75: date, possibly of personal importance;
9. nbusr 123: probably a username, and if so, can be very easily guessed;
10. p@$$\/\/0rd: simple letter substitutions are preprogrammed into password cracking tools;
11. password: used very often — trivially guessed;
12. December 12: using the date of a forced password change is very common.

A strong password is long enough, random or otherwise difficult to guess - producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it. Here are some examples of strong passwords:

1. Convert_£100 to Euros!: Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
2. 382465304H: It is mix of numbers and a letter at the end, usually used on mass user accounts

and such passwords can be generated randomly, for example, in schools and business.

3. 4pRte!ai@3: It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.
4. MoOoOfIn245679: It is long with both alphabets and numerals.
5. t3wahSetyeT4: It is not a dictionary word; however, it has both alphabets and numerals.

10.3.4. Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters. The difficulty in remembering such a password increases the chance that the user will write down the password, which makes it more vulnerable to a different attack (in this case, the paper being lost or stolen and the password discovered). Whether this represents a net reduction in security depends on whether the primary threat to security is internal (e.g., social engineering) or external. A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed. However, the person who created the password is able to remember it because it is just the four direction keys on the square number board (found at the right of most keyboards) plus a five in the middle. If you practice it, it is just one swift motion of moving two fingers around the board (which is very easy to use). Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also include password aging; the users are required to choose new passwords regularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training. The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.

5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Similarly, netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks.
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the web links displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks.
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks.
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

10.4. Keyloggers and Spywares

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

10.4.1. Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses (will discuss more on this in subsequent sections of this chapter) without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily. A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutabie (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.

10.4.2.Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

10.4.3.Antikeylogger

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit http://www.anti-kevloggers.com for more information.

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft
5. It secures E-Mail and instant messaging/chatting.

10.5. Spywares

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as key loggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

It is clearly understood from the term Spyware that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP).

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practices perspective.

Virus and Worms

Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random. Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

The following figures explain how viruses spread (a) through the Internet, (b) through a stand-alone computer system and (c) through local networks.

Work is undoubtedly worshiped but laughter is life. Anyone who takes life too seriously must prepare himself for a miserable existence. Anyone who greets joys and sorrows with equal facility can really get the best of life.
- Sardar Vallabhbhai Patel

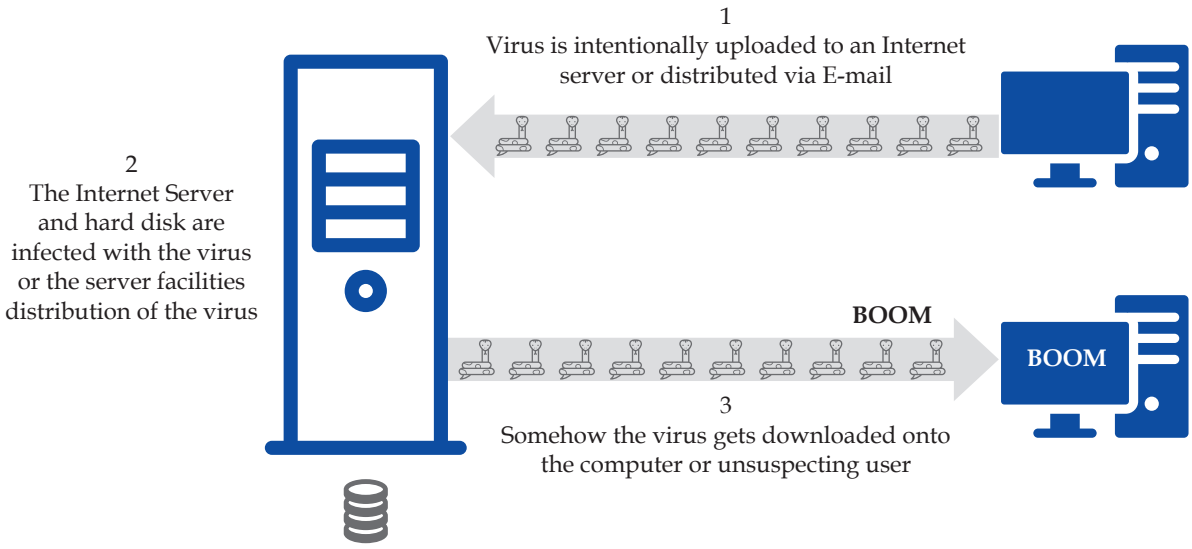


Fig. Virus Spreads Through the Internet

Computer virus has the ability to copy itself and infect the system. The term virus is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability. A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives. Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.

As explained in earlier sections, the term computer virus is sometimes used as a catch-all phrase to include all types of malware, Adware and Spyware programs that do not have reproductive ability. Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses. Viruses are sometimes confused with computer worms and Trojan Horses, which are technically. A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions. Worms and Trojans, such as viruses, may harm the systems data or performance. Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for users to take note of them. Some viruses do nothing beyond reproducing themselves.

Table : Difference between computer virus and worm

Sl. No.	Facet	Virus	Worm
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing ' networks worms

Sl. No.	Facet	Virus	Worm
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus.	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from The Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F Shock and Jon A Hupp at Xerox PARC published a paper in 1982, The Worm Programs and after that the name was adopted.
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Types of Viruses

Computer viruses can be categorized based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. Boot sector viruses: It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors. The first sector is called the BOOT and it carries the master boot record (MBR). MBR's function is to read and load OS, that is, it enables computer system to start through OS. Hence, if a virus attacks an MBR or infects the boot record of a disk, such floppy disk infects victims hard drive when he/she reboots the system while the infected disk is in the drive. Once the victims hand drive is infected all the floppy diskettes that are being used in the system will be infected. Boot sector viruses often spread to other systems when shared infected disks and pirated software(s) are used.
2. Program viruses: These viruses become active when the program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is excuted (i.e., opened - program is started). Once these program

files get infected, the virus makes copies of itself and infects the other programs on the computer system.

3. Multipartite viruses: It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active. When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.

4. Stealth viruses: It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system. It alters its file size and conceals itself in the computer memory to remain in the system undetected. The first computer virus, named as Brain, was a stealth virus. A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.

5. Polymorphic viruses: It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program. Polymorphic generators are the routines (i.e., small programs) that can be linked with the existing viruses. These generators are not viruses but the purpose of these generators is to hide actual viruses under the cloak of polymorphism. The first all-purpose polymorphic generator was the mutation engine (MtE) published in 1991. Other known polymorphic generators are Dark Angels Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'n'Roses Polymorphic Engine (GPE) and Dark Slayer Confusion Engine (DSCE).

6. Macroviruses: Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macroembedded in a document. Once a macrovirus gets onto a victims computer then every document he/she produces will become infected. This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.

7. Active X and Java Control: All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work — such as enabling or disabling pop-ups, downloading files and sound — which invites the threats for the computer system being targeted by unwanted software(s) floating in cyberspace.

As Windows OS is the most used OS across the globe, the lists of viruses displayed in following Table are the attacks on Windows OS. The terms "Virus" and "Worm" are used interchangeably and hence readers may find that the viruses listed under Table may be referred as worms on some websites and/or in some books.

Table : The world's worst virus attacks!!!

Sr. No.	Virus	Brief Description
1.	Conficker	It is also known as Downup, Downadup and Kido. It targets Microsoft Windows OS and was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. The name Conficker is blended from a English term "configure"and the German word "Ficker," which means "to have sex with" or "to mess with" in colloquial German.
2.	INF / AutoRun	AutoRun and the companion feature AutoPlay are components of the Microsoft Windows OS that dictate what actions the system takes when a drive is mounted. This is the most common threat that infects a PC by creating an "autorun.inf" file. The file contains information about programs meant to run automatically when removable devices are connected to the computer. End-users must disable the AutoRun feature enabled by default in windows. AutoRun functionality is used in attack vector attacks.
3	Win32 PSW. OnLineGames	It is a dangerous virus that replicates itself as other viruses and spreads from one computer system to another carrying a payload of destruction. It can infect several computers within few minutes. It is more concerned with gamers around the world, stealing confidential and other financial credentials as well as gaining access to the victims account. This virus is also termed as Trojan.
4	Win32/Agent	This virus is also termed as Trojan. It copies itself into temporary locations and steals information from the infected system. It adds entries into the registry, creating several files at different places in the system folder, allowing it to run on every start-up, which enables to gather complete information about the infected system and then transferred to the intruders system.
5	Win32/FlyStudio	It is known as Trojan with characteristics of backdoor. This virus does not replicate itself, but spreads only when the circumstances are beneficial. It is called as backdoors because the information stolen from a system is sent back to the intruder.
6	Win32/Pacex.Gen	This threat designates a wide range of malwares that makes use of an obfuscation layer to steal passwords and other information from the infected system.
7	Win32/Qhost	This virus copies itself to the System32 folder of the Windows directory giving control of the computer to the attacker. The attacker then modifies the Domain Name Server/System (DNS) settings redirecting the computer to other domains. This is done to compromise the infected machine from downloading any updates and redirect any attempts made to a website that downloads other malicious files on the victim's computer.

Sr. No.	Virus	Brief Description
8	WMA/Trojan Downloader. GetCodec	This threat as the suffix. GetCodec modifies the audio files present on the system to ".wma" format and adds a URL header that points to the location of the new codec. In this manner, the host computer is forced to download the new codec and along with the new codec several other Malicious Codes are also downloaded. This means that the end-user will download the new codec believing that something new might happen, whereas the Malicious Code runs in the background causing harm to the host computer. At present, there is no way to verify the authenticity of the codec being downloaded as a new enhancement or a Trojan Horse; therefore, users must avoid unnecessary downloading of new codecs unless they are downloaded from a trusted website. Unnecessary downloading of codecs should also be avoided.

A computer worm is a self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Almost every day new viruses/worms are created and they become new threat to netizens. In summary, in spite of different platforms (i.e., OS and/or applications), a typical definition of computer virus/worms might have various aspects such as:

1. A virus attacks specific file types (or files).
2. A virus manipulates a program to execute tasks unintentionally.
3. An infected program produces more viruses.
4. An infected program may run without error for a long time.
5. Viruses can modify themselves and may possibly escape detection this way.

Trojan Horses and Backdoors

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, raining the file allocation table on the hard disk. A Trojan Horse may get widely redistributed as part of a computer virus. The term Trojan Horse comes from Greek mythology about the Trojan War.

Like Spyware and Ad ware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet. It is also possible to inadvertently transfer malware through a USB flash drive or other portable media. It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines. (Users

would not know that these could infect their network while bringing some music along with them to be downloaded.)

Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive. On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Visit http://en.wikipedia.org/wiki/List_of_trojan_horses to get the list of noteworthy Trojan Horses. Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

Trojan War

The Trojan Horse is a tale from the Trojan War, as told in Virgil's Latin epic poem The Aeneid Quintus of Smyrna. The events in this story from the Bronze Age took place after Homer's /tad and before his Odyssey. It was the stratagem that allowed the Greeks finally to enter the city of Troy and end the conflict. In the best-known version, after a fruitless 10-year siege, the Greeks construct a huge wooden horse in an attempt to once and for all destroy Troy from the inside. According to Quintus, it was Odysseus who came up with the idea of building a great wooden horse in which 30 men could hide to be wheeled into the city without the Trojans knowing. The Greeks build a huge, magnificent wooden horse in 3 days under the leadership of Epeios. Odysseus' plan also calls for one man to remain outside of the horse. This man will act as though the Greeks abandoned him, leaving the horse as a gift for the Trojans. The Greeks chose their soldier Sinon

to play this role, as he is the only volunteer. Virgil describes the actual encounter between Sinon and the Trojans; Sinon successfully convinces the Trojans that he has been left behind and the Greeks are gone, and the horse is wheeled inside the city walls as a victory trophy. That night, the Greek soldiers hidden inside the horse emerged and opened the city gates for the rest of the Greek army. They raid and destroy the city of Troy, finally ending the Trojan War.

Backdoor

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.

A backdoor works in background and hides from the user. It is very similar to a virus and, therefore, is quite difficult to detect and completely disable. A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system. Most backdoors are autonomic malicious programs that must be somehow installed to a computer. Some parasites do not require installation, as their parts are already integrated into particular software running on a remote host. Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes. Attackers often discover these undocumented features and use them to intrude into the system.

What a Backdoor Does?

Following are some functions of backdoor :

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.
4. It records keystrokes that a user types on a computers keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. It distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8. It installs hidden FTP server that can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.

10. It provides no uninstall feature, and hides processes, files and other objects to complicate its removal as much as possible.

Following are a few examples of backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit http://www.cultdeadcow.com/tools/bo.html to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server, server builder and client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors:** SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. Backdoors can present into SAP User Master that supports an authentication mechanism when a user connects to access SAP and ABAP Program Modules which support SAP Business Objects.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests.

How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. Stay away from suspect websites/weblinks: Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things.
2. Surf on the Web cautiously: Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the Web. It may be experienced that, after downloading the file, it never works and here is a threat that - although the file has not worked, something must have happened to the system — the malicious software deploys its gizmos and the system is at serious health risk. Enabling Spam filter "ON" is a good practice but is not 100% foolproof, as spammers are constantly developing new ways to get through such filters.
3. Install antivirus/Trojan remover software: Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply and clients consume.

There are different levels of P2P networking:

1. Hybrid P2P: There is a central server that keeps information about the network. The peers are responsible for storing the information, if they want to contact another peer, they query the server for the address.
2. Pure P2P: There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as "serverless" P2P.
3. Mixed P2P: It is between "hybrid" and "pure" P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called "supernodes."

Advantages of P2P Networks:

1. It enables faster delivery of information from one computer to another by bypassing a central server.
2. It increases personal efficiency and personal empowerment. Users will no longer have to wait in queues to perform essential tasks, as all activities take place at the user's discretion.
3. It represents significant cost savings over client/server models. As resources and computing power are distributed across the entire network, there is no need for expensive centralized servers; this will reduce the need for centralized management, storage and other related resources.
4. It offers easy scalability and all that is necessary for a network to grow is add more peers.
5. It increases a network's fault tolerance. As no part of the system is essential to its operation, you can take down a few nodes and the network remains functional.
6. It leverages previously unused resources found on hundreds of millions of computers (and other services) that are connected to the "edges" of the Internet.
7. It frees up bandwidth on the Internet (or on a private network). In traditional client-server model, the server is the bottleneck and often cannot handle everything the client requests.
8. It requires no centralized management, oversight or control.
9. It offers increased privacy, as all data and messages are directly exchange between two computers.
10. It results in networks that are more flexible and adaptable compared with traditional client-server networks.

Besides all these advantages, there are still many reasons why P2P might not be the right model and is used only for specific set of activities.

10.6. Steganography

Steganography is a Greek word that means "sheltered writing". It is a method that attempts to hide the existence of a message or communication. The word "steganography" comes from the two Greek words: steganos meaning "covered" and graphein meaning "to write" that means "concealed writing." This idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes. The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messengers head and then tattooing a secret message on it, letting his hair grow back and then shaving it again after he arrived at the receiving party to reveal the message.

Given the sheer volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One lesser known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist! Steganography is always misunderstood with cryptography. The different names for steganography are data hiding, information hiding and digital watermarking.

For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data. Digital watermarking is the process of possibly irreversibly embedding information into a digital signal. The signal may be, for example, audio, pictures or video. If the signal is copied then the information is also carried in the copy.

The term "cover" or "cover medium" is used to describe the original, innocent message, data, audio, still, video and so on. It is the medium that hides the secret message. It must have parts that can be altered or used without damaging or noticeably changing the cover media. If the cover media are digital, these alterable parts are called "redundant bits." These bits or a subset can be replaced with the message that is intended to be hidden. Interestingly, steganography in digital media is very similar to "digital watermarking." In other words, when steganography is used to place a hidden "trademark" in images, music and software, the result is a technique referred to as "watermarking".

Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. It is said that terrorists use steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple. For example, say every fourth letter of a memo could hide a message. This simple technique has an added advantage over encryption that it does not arouse suspicion,

that is, there is not much scope for getting started an investigation! Presence of an encryption could set off an investigation, but a message hidden in plain sight would get ignored.

In October 2001, the New York Times published an article claiming that al-Qaeda had used steganographic techniques to encode messages into images, and then transported these via E-Mail and possibly via Usenet to prepare and execute the 11 September 2001 Terrorist Attack.

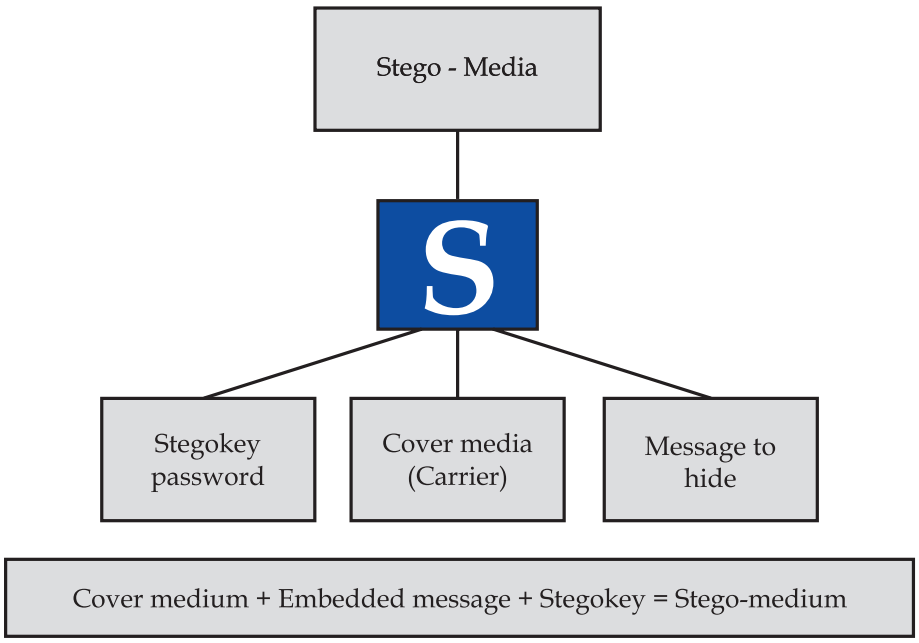


Fig. How Steganography Works

10.6.1 Steganalysis

Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography. The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it. Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

10.7. DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

10.7.1. DoS Attacks

In this type of criminal act, the attacker floods the bandwidth of the victims network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile

phone networks and even root name servers (i.e., domain name servers). Buffer overflow technique is employed to commit such kind of criminal attack known as Spoofing. The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system. A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests. As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:

1. Unusually slow network performance (opening files or accessing websites);
2. unavailability of a particular website;
3. inability to access any website;
4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

10.7.2. Classification of DoS Attacks

See the following Table for classification of DoS attacks.

Table: Classification of DoS attacks.

Sr. No.	DoS Attacks	Brief Description
1	Bandwidth attacks	Loading any website takes certain time. Loading means complete webpage (i.e., with entire content of the webpage — text along with images) appearing on the screen and system is awaiting users input. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting, say for example, 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site. The attacker does the same — he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service.
2	Logic attacks	These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.

Sr. No.	DoS Attacks	Brief Description
3	Protocol attacks	Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victims system to consume excess amounts of its resources.
4	Unintentional DoS attack	This is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary sites regular users', potentially hundreds of thousands of people, click that link within a few hours and have the same effect on the target website as a DDoS attack.

10.7.3. Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as ping flood. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle. This requires the attacker to have a faster network connection than the victim (i.e., access to greater bandwidth than the victim). It is very simple to launch, but to prevent it completely is the most difficult.

2. **Ping of death attack:** The ping of death attack sends oversized Internet Control Message Protocol (ICMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim. The maximum packet size allowed is of 65,536 octets. Some systems, upon receiving the oversized packet, will crash, freeze or reboot, resulting in DoS (e.g., the ping of death attack relied on a bug in the Berkeley TCP/IP stack, which also existed on most systems that copied the Berkeley network code).

3. **SYN attack:** It is also termed as TCP SYN Flooding. In the Transmission Control Protocol (TCP), handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address). The server replies with a SYN-ACK. The client then does not send back an ACK, causing the server (i.e., target system) to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.

4. **Teardrop attack**: The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code. Windows 3. 1x, Windows 95 and Windows NT OSs as well as versions of Linux are vulnerable to this attack.

5. **Smurf attack:** It is a way of generating significant computer network traffic on a victim network. This is a type of DoS attack that floods a target system via spoofed broadcast ping messages. This attack consists of a host sending an ICMP echo request (ping) to a network broadcast address (e.g., network addresses with the host portion of the address having all 1s). Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic. On a multi-access broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. Internet relay chat (IRC) servers are the primary victim of smurf attacks on the Internet.

6. **Nuke:** Nuke is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. It is achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD).

10.7.4. Tools Used to Launch DoS Attack

Various tools use different types of traffic to flood a victim, but the objective behind the attack and the result is the same: A service on the system or the entire system (i.e., application/website/network) is unavailable to a user because it is kept busy trying to respond to an exorbitant number of requests. A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service.

Blended Threat

Blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan Horses and Malicious Code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, transmit and thereafter spread an attack. Characteristics of blended threats are that

1. They cause harm to the infected system or network.
2. They propagate using multiple methods as attack may come from multiple points.
3. They also exploit vulnerabilities.

To be considered a blended threat, the attack would normally serve to transport multiple attacks in one payload. For example, it would not only just launch a DoS attack but it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. Therefore, while a worm may travel and spread through E-Mail, a single blended threat could use multiple routes including E-Mail, IRC and file-sharing networks.

Finally, rather than a specific attack on predetermined ".exe" files, a blended threat could do multiple malicious acts, such as modify your ".exe" files, HTML files and registry keys at the same time - basically it can cause damage to several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats require no human intervention to propagate.

Source: http://vsww.webopedia.com/didyouknow/internet/2004/virus.asp (11 January 2010).

Permanent Penial-of-Service (PDoS) Attack

A PDoS attack damages a system so badly that it requires replacement or reinstallation of hardware. Unlike DDoS attack - which is used to sabotage a service or website or as a cover for malware delivery - PDoS is a pure hardware sabotage. It exploits security flaws that allow remote administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt or defective firmware image - a process which when done legitimately is known as flashing. Owing to these features, and the potential and high probability of security exploits on network-enabled-embedded devices (NEEDs), this technique has come to the attention of numerous hacker communities. PhlashDance is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) who detected and demonstrated PDoS vulnerabilities at the 2008 EUSecWest Applied Security Conference in London.

10.7.5. DDoS Attacks

In a DDoS attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the DoS attack.

A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called "secondary victims'' and the main target is called "primary victim.''

Malware can carry DDoS attack mechanisms - one of the better-known examples of this is MyDoom. Typically, DoS mechanism triggered on a specific date and time. This type of DDoS attacks involves hard coding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack. A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent. Nowadays, Botnet is the popular medium to launch DoS/DDoS attacks. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts.

10.7.6. How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.

1. Implement router filters. This will lessen your exposure to certain DoS attacks.

2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.
5. Observe your systems performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain "hot spares" - machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Table: Tools for detecting DoS/DDoS attacks

Sr.No.	Tool	Brief Description
1.	Zombie Zapper	It is a free, open-source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Stacheldraht. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep.
2.	Remote Instrusion Detector (RID)	It is a tool developed in "C" computer language, which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies. It detects the presence of Trinoo, TFN or Stacheldraht clients.
3.	Security Auditor's Research Assistant (SARA)	It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
4.	Find DDoS	It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
5.	DDoSPing	It is a remote network scanner for the most common DDoS programs. It can detect Trinoo, Stacheldraht and Tribe Flood Network programs running with their default settings.

A few heart-whole, sincere, and energetic men and women can do more in a year than a mob in a century.
- Swami Vivekananda

10.8. Attacks on Wireless Networks

Even when people travel, they still need to work. Thus, work seems to be moving out of the traditional offices into homes, hotels, airport lounges and taxis. The employee is no longer tied to an office location and is, in effect, "boundaryless." When one talks to the young generation about their lifestyles, one realizes that gone are those days when an "office" conjured up the image of the four walls, set in the formal setting, typical office decor and with all the formality that one can imagine, which may perhaps be difficult for our new generation to appreciate. In the yesteryears, "working" meant leaving home, commuting to the workplace, spending those typical 9 am - 6 pm in the office and then shutting down the work and commuting back home or wherever that one wished to be after office hours. The "working" and "away from work" were cleanly delineated distinct states that one could be in. Gone are those days and now we are in the era of computing anywhere, anytime! There is no doubt chat workforce "mobility" is on the rise.

The following are different types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, tele-cottagers and, in some cases, branch workers.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels. This type includes the sales and field forces.

Wireless technologies have become increasingly popular in day-to-day business and personal lives. Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs. Wireless networks are generally composed of two basic elements: (a) access points (APs) and (b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other. APs are connected through physical wiring to a conventional network and they broadcast signals with which a wireless device can connect.

Wireless access to networks has become very common by now in India — for organizations and for individuals. Many laptop computers have wireless cards preinstalled for the buyer, for example, in India, such cards are provided by TATA Indicom, Reliance and Airtel. There are many hotels and equivalent establishments all over the world (including India) where the rooms are "Wi-Fi enabled." There is no denying that the ability to enter a network while on the move (working away from home or in other locations that are not routine office locations, working while in hotels, etc.) has great benefits.

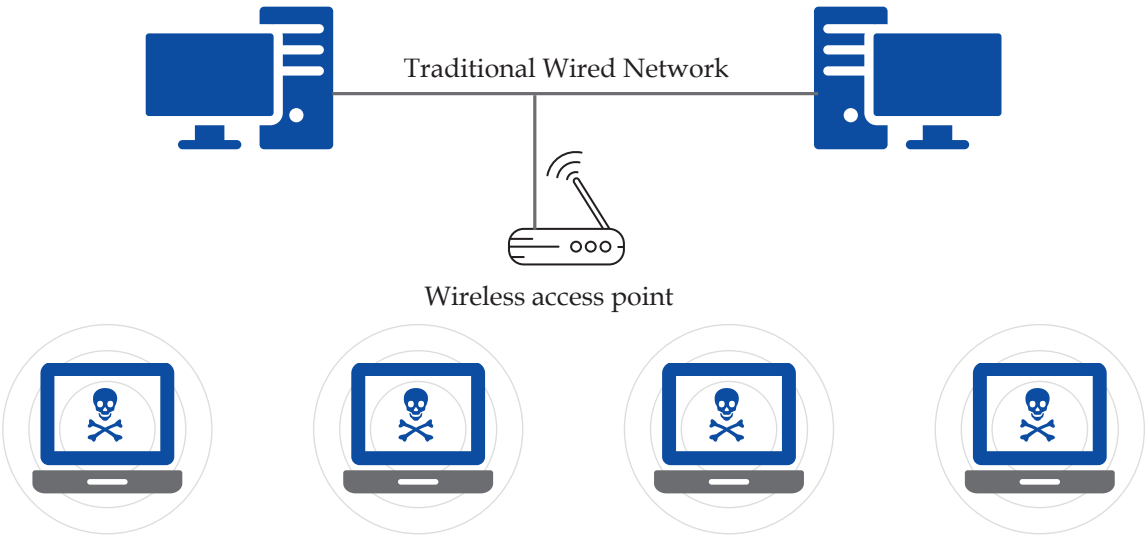


Fig. Wireless Networks

10.8.1. Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as wireless cracking. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. Stuffing: It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. Also termed as reconnaissance technique, it gathers the required information about the active/available Wi-Fi networks. The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as
   - Passive scanning of wireless network;
   - detection of SSID;
   - cohering the MAC address;
   - collecting the frames to crack WEP.
2. Spoofing: The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage. The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network. It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one. The attacker can conduct this activity easily because while setting up a wireless network, the computers no longer need to be informed to access the network; rather they access it automatically as soon as they move within the signal range. This convenient feature is always exploited by the attacker.

- MAC address Spoofing: It is a technique of changing an assigned media access control (MAC) address of a networked device to a different one. This allows the attacker to bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.

. • IP Spoofing: It is a process of creating IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. To engage in IP Spoofing, the attacker uses a variety of techniques to find an IP address of a trusted host(s) and then modifies the packet headers so that it appears that the packets are coming from that host, that is, legitimate sender.

- Frame Spoofing: The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications. Frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detected unless the address is entirely faked/bogus.

3. Denial of service (DoS): We have discussed this attack in previous chapters..

4. Man-in-the-middle attack (MITM): It refers to the scenario wherein an attacker on host A inserts A between all communications — between hosts X and Y without knowledge of X and Y. All messages sent by X do reach Y but through A and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.

5. Encryption cracking: It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

10.8.2 .Theft of Internet Hours and Wi-Fi based Frauds and Misuses

Information communication technology (ICT) is within reach of people nowadays and most of the new systems (i.e., computers) are equipped for wireless Internet access as more and more people are opting for Wi-Fi in their homes. Wireless network into homes is becoming common necessity because of lifestyle and availability of inexpensive broadband routers that can be configured easily and/or there is no need to configure these devices at all because of plug-and-play feature. This enables the Internet on the finger tip of home users and in case, unfortunately, he/she visits a malicious webpage, the router is exposed for an attack. Thus, as the networks become stronger and more prevalent, more of the signals are available outside the home of the subscriber, spilling over into neighbors apartments, hallways and the street. In today's era of high dependability on the Internet for many aspects of our life and given that predators are lurking around as potential cybercriminals, they (criminals) often wonder how they can find out who they are stealing it from so that they can get an idea if that information is safe. According to a study by Jupiter Research,

14% of wireless network owners have accessed their neighbor's connection. It appears that more and more people are logging on for free.

The New "Wars" in the Internet Era!

1. **Warkitting:** Warkitting was identified by Tsow. Jakobsson, Yang and Wetzel in 2006. This is a combination of wardriving and rootkitting - an attack in which the wireless access point's configuration or firmware is modified over the wireless connection. This allows the attacker to control all traffic for the victim and may even permit to disable Secure Socket Layer (SSL) by replacing HTML content, when it is being downloaded. The attacker first discovers vulnerable wireless routers through wardriving and/or by retrieving the necessary data from existing Wi-Fi access point databases such as WiGLE (www.wigle.net) or WiFiMaps (www.wifimaps.com) to carry out a warkitting attack.

2. **WAPKitting:** In this attack, external software clutches the control of router's firmware that can be easily accomplished by exploiting open administrative access. WAPkitting can theoretically proceed by more traditional means such as buffer overflow. The ability to install arbitrary control software on a wireless router opens unlimited possibilities to an attacker.

3. **WAPjacking:** This type of attack is very similar to DNS poisoning attacks. It changes the settings of existing firmware that helps an attacker to engage in malicious configuration of firmware settings; however, it makes no modification to the firmware itself, that is, allow connections to be hijacked and/or rerouted without the user's knowledge. WAPjacking is less powerful attack compared to WAPkitting.

   WAPkitting and WAPjacking are independent of the means of infection, and specify the relative modifications done to a WAP upon corruption. Warkitting, on the other hand, does not specify the type of WAP alteration, but it does relate to how infection occurs.

Be careful with use of WAPs; when you are using a WAP to gain access to computer on a network, be aware of the local laws/legislations where you are doing it because things can become dangerous from security and privacy as well legal perspective. Maybe if corporations were not in such a hurry to release this technology and thought about it more thoroughly, they would not have to deal with security breaches and creating superior protection for their own systems. The moral of the story is that you must secure your network.

10.8.3. How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and non-intuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.

4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade routers firmware periodically.
11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

Summary

When information systems are the target of offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system or computer-network. The perpetrators range from teenagers (script kiddies/cyberjoyriders) to organized crime operators and international terrorists.

A computer can be the target of offense; tools may be used in an offense, or may contain evidence of an offense. An understanding of different uses of a computer will provide foundation of the application of the" criminal statutes.

अध्याय 11
Chapter 11

Cyber Offences

11.1. Introduction

Technology is a "double-edged sword" as it can be used for both good and bad purposes. People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose. Computers and tools available in IT are also no exceptions; like other tool, they are used as either target of offense or means for committing an offense. In today's world of Internet and computer networks, a criminal activity can be carried out across national borders with "false sense of anonymity"; without realizing, we seem to pass on tremendous amount of information about ourselves. Are we sure this will never be misused? One should not share his/her Personally Identifiable Information such as date of birth, personal E-Mail address, bank account details and/or credit card details with others.

Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc. The criminals take advantage of the widespread lack of awareness about cybercrimes and cyber laws among the people who are constantly using the IT infrastructure for official and personal purposes. People who commit cybercrimes are known as "Crackers".

Hackers, Crackers and Phreakers

- **Hacker:** A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers.
- **Brute force hacking:** It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.
- **Cracker:** A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.
- **Cracking:** It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called "phreaking"). These sites usually display warnings such as "These files are illegal; we are not responsible for what you do with them."
- **Cracker tools:** These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Irojans, viruses, war dialers and worms.
- **Phreaking:** This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.
- **War dialer:** It is program that automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in.

Source: Nina Godbole (2009), Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. Wiley India.

An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected. The categories of vulnerabilities that hackers typically search for are the following:

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.

To help the reader understand the network attack scenario, the below figure illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

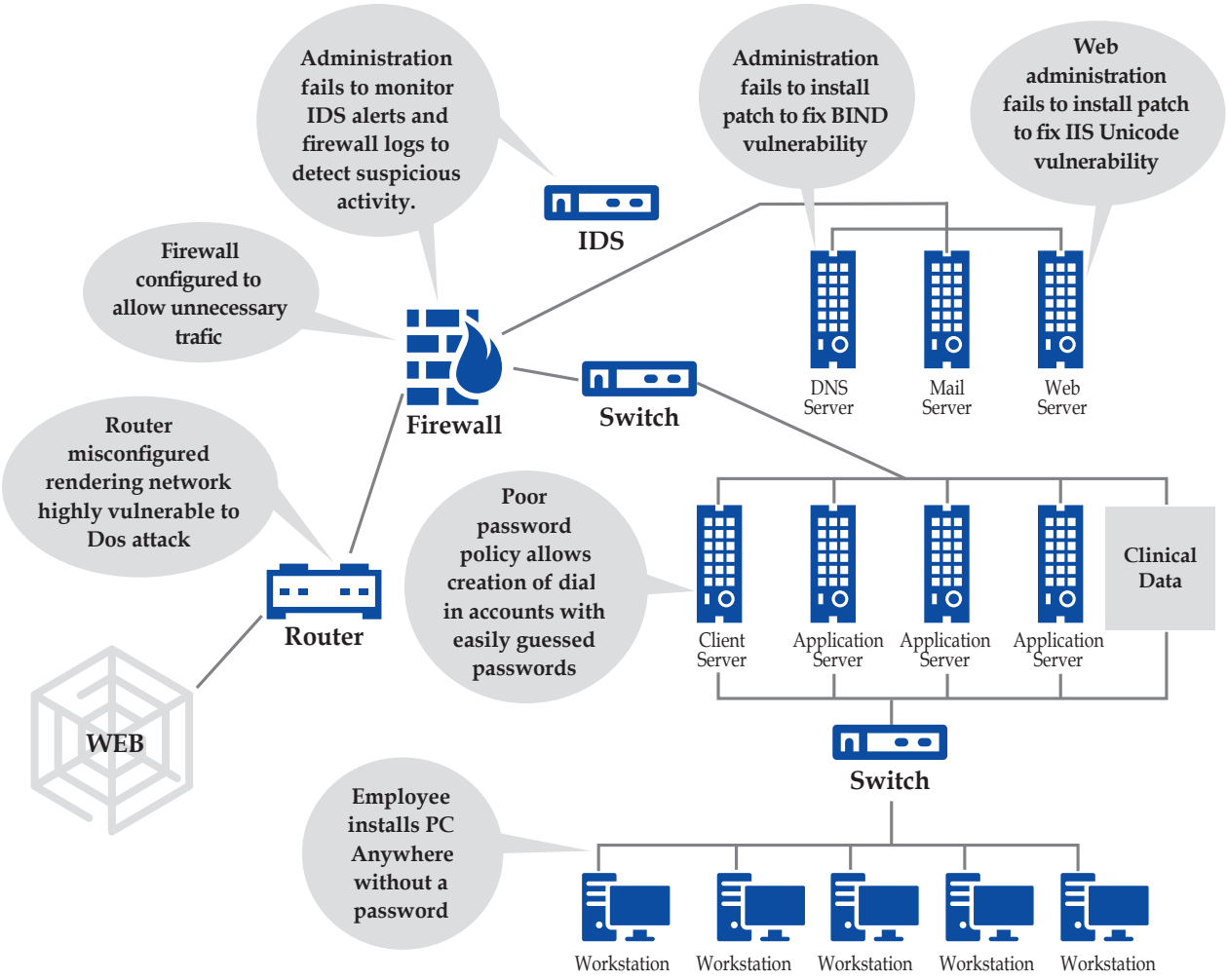


Fig. Network Vulnerabilities - Sample Network

11.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

Generally, Cybercrime can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).

1. Crimes targeted at individuals: The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography, copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.
2. Crimes targeted at property: This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.
3. Crimes targeted at organizations: Cyber terrorism is one of the distinct crimes against organizations/governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system.
4. Single event of cybercrime: It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. Series of events: This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

11.2. How Criminals Plan the Attacks

Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization. (The custodian of a property can be an individual or an organization; for discussion purpose not mentioned here). Criminals plan passive and active attacks. Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security perimeter of an organization is an inside attack; it is usually attempted by an "insider" who gains access to more resources

than expected. An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

11.2.1. Reconnaissance

The literal meaning of "Reconnaissance" is an act of reconnoitering - explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

In the world of "hacking," reconnaissance phase begins with "Footprinting" — this is the preparation toward preattack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment. Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.

Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

11.2.2. Passive Attacks

A passive attack involves gathering information about a target without his/her (individuals or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees.
2. Surfing online community groups like Facebook will prove useful to gain the information about an individual.
3. Organizations website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target.
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

Tips for Effective Search with "Google"' Search Engine

The Google search engine can be used indigenously to perform "Reconnaissance" phase ot an attack. The following commands can be used effectively in the Google search engine.. http://groups.google.com: This site can be used to search the Google newsgroups.

- **Site:** If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within www.google. com. [help site:com] will find pages about help within .com URLs (uniform resource locator). Note that, there should be no space between the "site:" and the domain. This feature is also available through advanced search page, under Advanced Web Search > Domains.
- **Filetype:** This will search within the text of a particular type of file. The file type to search must be typed after the colon.
- **Link:** The query [link:] will list the webpages that have links to the specified webpage. For instance, [link: www.google.com] will list webpages that have links pointing to the Google homepage. Note that there can be no space between the "link:" and the webpage URL. This functionality is also accessible from the advanced search page, under Page Specific Search > Links.
- **Inurl:** If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the URL For instance, [inurl:google search] will return documents that mention the word "google" in their URL. and mention the word "search" anywhere in the document (URL or no). Note that there should be no space between the "inurl:" and the following word. Putting "inurl:" in front of every word in your query is equivalent to putting "allinurl:" in front of your query; this implies [inurl:google inurl:search] is the same as [allinurl: google search].
- **Cache:** If you include other words in the query, Google will highlight those words within the cached document. For instance, [cache: www.google.com web] will show the cached content with the word "web" highlighted. This feature is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the webpage that Google has in its cache. For instance, [cache: www.google.com] will show Google's cache of the Google homepage. Note that there should be no space between the "cache:" and the webpage URL.
- **Related:** The query [related:] will list webpages that are "similar" to a specified webpage. For instance, [related: www.google.com] will list webpages that are similar to the Google homepage. Note that there should be no space between the "related:" and the webpage URL. This feature is also accessible by clicking on the "Similar Pages" link on Google's main results page, and from the advanced search page, under Page Specific Search > Similar.
- **Info**: The query [info:] will present some information that Google has about that webpage. For instance, [info: www.google.com] will show information about the Google homepage.

Note that there should be no space between the "info:" and the webpage URL. This feature is also accessible by typing the webpage URL directly into a Google search box.

- **Define:** The query [define:] will provide a definition of the word/phrase you enter after it gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).
- **Stocks:** If you begin a query with the [stocks:] operator, Google will treat the rest of the query terms as stock ticker symbols and will link to a page showing stock information for those symbols. For instance, [stocks: intc yhoo] will show information about Intel and Yahoo. (Note that you must type the ticker symbols, not the company name.) This feature is also available if you search just on the stock symbols (e.g., [intc yhoo]) and then click on the "Show stock quotes" link on the results page.
- **Allintitle:** If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For instance, [allintitle: google search] will return only documents that have both "google" and "search" in the title. This feature is also available through advanced Search page, under Advanced Web Search > Occurrences.
- **Intitle:** If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word "google" in their title and the word "search" anywhere in the document (title or no). Note that there should be no space between the "intitle:" and the following word. Putting [intitle:] in front of every word in your query is equivalent to putting [allintitle:] at the front of your query; this implies that [intitle:google intitle:search] is the same as [allintitle: google search].
- **Allinurl:** If you start a query with [allinurl:], Google will restrict the results to those with all of the query words in the URL. For instance, [allinurl: google search] will return only documents that have both "google" and "search" in the URL.

Note that [allinurl:] works on words, not on URL components. In particular, it ignores punctuation. Thus, [allinurl: foo/bar] will restrict the results to page with the words "foo" and "bar" in the URL, but won't require that they be separated by a slash within that URL, that they be adjacent, or that they be in that particular word order. There is currently no way to enforce these constraints.

Source: http://www.google.com.tw/help/operators.html

Network sniffing is another means of passive attack to yield useful information such as Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network. The network traffic is sniffed for monitoring the traffic on the network - attacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Along with Google search, various other tools are also used for gathering information about the target / victim.

11.2.3. Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called "Rattling the doorknobs" or "Active reconnaissance".

Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

11.2.4 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

Note: Usually, most of the attackers consume 90% of the time in scanning, scrutinizing and gathering information on a target and 10% of the time in launching the attack.

Port Scanning

A "port" is a place where information goes into and out of a computer and so, with port scanning, one can identify open doors to a computer. Ports are basically entry/exit points that any computer has, to be able to communicate with external machines. Each computer is enabled with three or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner, and other peripherals. The important char- acteristic about these "external ports" is that they are indeed external and visible to the naked eye. Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap offer an automated mechanism for an attacker to not only scan the system to find out what ports are "open" (meaning being used), but also help to identify what operating system (OS) is being used by the system.

Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones, are open and which ones are locked. Port scanning

is an act of systematically scanning a computer's ports. In technological terms, "port scanning" refers to the act of using various open-ended technologies, tools, and commands to be able to communicate with another remote computer system or network, in a stealth mode, without being apparent, and be able to obtain certain sensitive information about the functions of system and the properties of the hardware and the software being used by the remote systems.

In "portscan," a host scans for listening ports on a single target host. In "portsweep" a host scans multiple hosts for a specific listening port. The result of a scan on a port is usually generalized into one of the following three categories:

1. **Open or accepted:** The host sent a reply indicating that a service is listening on the port.
2. **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.
3. **Filtered or blocked:** There was no reply from the host.

TCP/IP suite of protocols is used to communicate with other computers for specific message formats. Most of these protocols are tied to specific port numbers that are used to transfer particular message formats as data. Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.

1. Ports 20 and 21 - File Transfer Protocols (FTP) - are used for uploading and downloading of information.
2. Port 25-Simple Mail Transfer Protocol (SMTP) - is used for sending/receiving E-Mails.
3. Port 23 - Telnet Protocol - is used to connect directly to a remote host and Internet control message.
4. Port 80 - It is used for Hypertext Transfer Protocol (HTTP).
5. Internet Control Message Protocol (ICMP) - It does not have a port abstraction and is used for checking network errors, for example, ping.

11.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password;
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks - delete the access logs, so that there is no trail illicit activity.

11.3 Social Engineering

Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action. Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes. It is generally agreed that people are the weak link in security and this principle makes social engineering possible. A

social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.

Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders. It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner. The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble. The sign of truly successful social engineers is that they receive information without any suspicion. A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on.

Social Engineering Example

- Mr. Joshi: Hello?

  The Caller: Hello. Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

- Mr. Joshi: Ohh ... okay. I will be at my home by then, anyway.

  Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

- Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?

  Caller No sir. But we will have to check your account to ensure the same. What is the password of that account?

- Mr. Joshi: My password is "ABCD1965," all characters in upper case.

  Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there. Mr. Joshi: Thank you. Bye. Caller: Bye and have a nice day.

11.3.1 Classification of Social Engineering

Human-Based Social Engineering

Human-based social engineering refers to person-to-person interaction to get the required/ desired information. An example is calling the help desk and trying to find out a password.

- **Impersonating an employee or valid user:** "Impersonation" (e.g., posing oneself as an employee of the same organization) is perhaps the greatest technique used by social engineers to deceive people. Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.

- **Posing as an important user:** The attacker pretends to be an important user - for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system. The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.
- **Using a third person**: An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
- **Calling technical support:** Calling the technical support for assistance is a classic social engineering example. Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.
- **Shoulder surfing:** It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
- **Dumpster diving:** It involves looking in the trash for information written on pieces of paper or computer printouts. This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded. It is also called dumpstering, binning, trashing, garbing or garbage gleaning. "Scavenging" is another term to describe these habits. In the UK, the practice is referred to as "binning" or "skipping" and the person doing it is a "binner" or a "skipper."

In practice, dumpstering is more like fishing around than diving in. Usually, people dumpster dive to search the items, to reclaim those, which have been disposed of but can still be put to further use, for example, E-Waste, furniture, clothes, etc. The term "dumpster diving" may have originated from the notional image of someone leaping into large rubbish bins, the best known of which are produced under the name "dumpster." "Scavenging" is equivalent of "dumpster diving," in the digital world. It is a form in which discarded articles and information are scavenged in an attempt to obtain/recover advantageous data, if it is possible to do so. Consider, for example, going through someone's trash to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN number in India, credit card identity (ID) numbers, etc.]. According to a definition in the glossary of terms for the convoluted terminology of information warfare, "scavenging" means "searching through object residue (e.g., discarded disks, tapes, or paper) to acquire sensitive data without authorization."

Computer-Based Social Engineering

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet. For example, sending a fake E-Mail to the user and asking him/her to re-enter a password in a webpage to confirm it.

1. **Fake E-Mails:** The attacker sends fake E-Mails to numerous users in such that the user finds it as a legitimate mail. This activity is also called "Phishing". It is an attempt to entice the Internet users (netizens) to reveal their sensitive personal information, such

as user-names, passwords and credit card details by impersonating as a trustworthy and legitimate organization and/or an individual. Banks, financial institutes and payment gateways are the common targets. Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website. Thus, Phishing is also an example of social engineering techniques used to fool netizens. The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails lures to fish for passwords and financial data from the sea of Internet users (i.e., netizens). The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users. As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

Fake E-Mails : Unfortunately, free websites are available to send fake E-Mails.

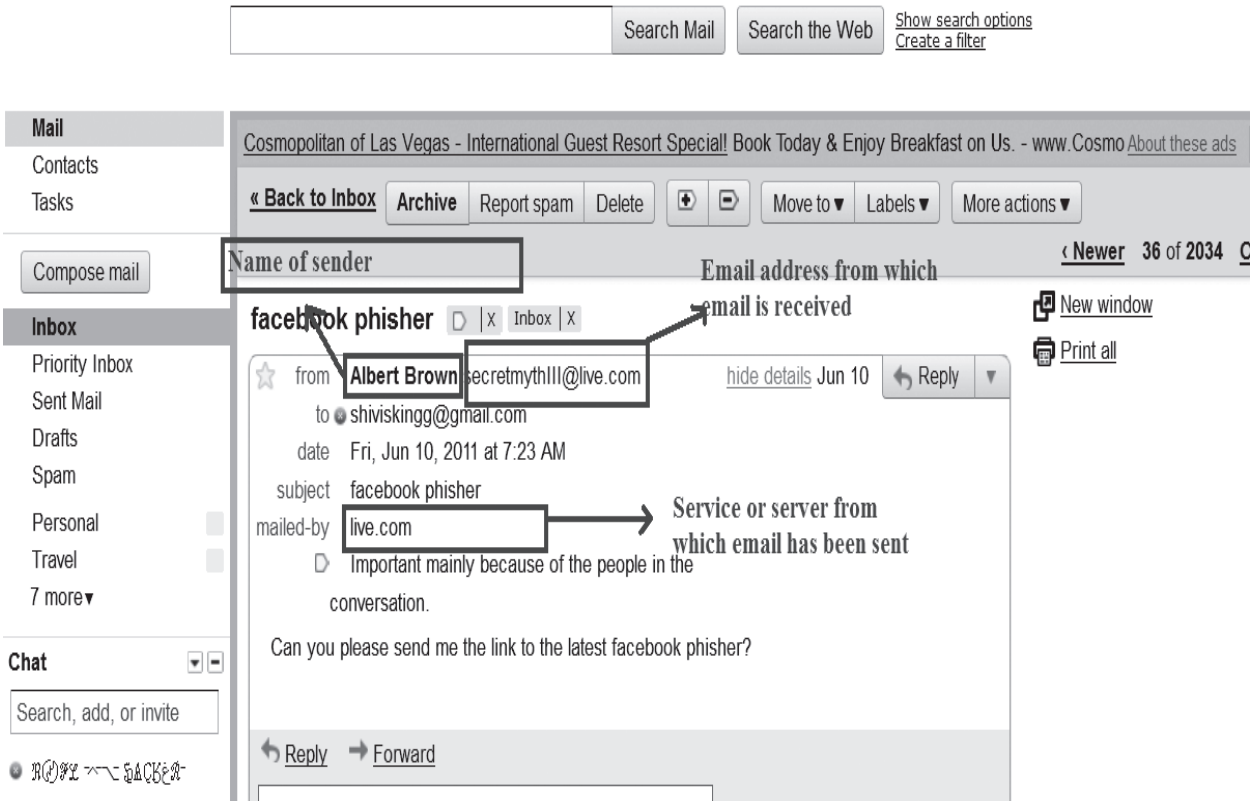


Fig. Sending Fake E-Mails

- E-Mail attachments: E-Mail attachments are used to send malicious code to a victims system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

- Pop-up windows: Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Social engineering indeed is a serious concern as revealed by the following past statistics on numbers:

1. As per Microsoft Corporation recent (October 2007) research, there is an increase in the number of security attacks designed to steal personal information (PI) or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was US$ 1.8 million.
2. The Federal Trade Commission (FTC) report of 2005 shows that "more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations".
3. According to a 2003 survey [released on 2 April 2006 by the United States Department of Justice", "An estimated 3.6 million - or 3.1% - of American households became victims of ID theft in 2004." This means that now, more than ever, individuals are at a high risk of having their PI stolen and used by criminals for their own personal gain.

Typically, many organizations have information valuable enough to justify expensive protection mechanisms/ security mechanisms. Critical information may include patient records in the medical and healthcare domain [known as protected health information (PHI)], corporate financial data, electronic funds transfers, access to financial assets in the financial services domain, and PI about clients or employees. Compromising critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and collapse of the organization. To respond to the threats, organizations implement InfoSec plans to establish control of information assets. However, "social engineers" try to device a way to work their way around this to obtain the valuable information, an illicit act on ethical grounds.

Social engineering succeeds by exploiting the trust of the victim. Hence, continuous training/ awareness sessions about such attacks are one of the effective countermeasures. Strict policies about service desk staff never asking for personally identifying information, such as username and passwords, over the phone or in person can also educate potential victims and recognize a social engineering attempt.

Social engineering and dumpster diving are also considered passive information - gathering methods.

11.4. Cyberstalking

The dictionary meaning of "stalking" is an "act or process of following prey stealthily - trying to approach somebody or something." Cyberstalking has been defined as the use of information

and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization. The behavior includes raise accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the persons property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

11.4.1. Types of Stalkers

There are primarily two types of stalkers.

- **Online stalkers:** They aim to start the interaction with the victim directly with the help of the Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
- **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/ newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet. The victim is not aware that the Internet has been used to perpetuate an attack against them.

11.4.2. Cases Reported on Cyberstalking

The majority of cyberstalkers are men and the majority of their victims are women. Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking. In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor. However, there also have been many instances of cyberstalking by strangers.

11.4.3. How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.

3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.

4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

5. The stalker may post the victims personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.

6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.

7. Some stalkers subscribe/ register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-mails.

Cyberbulllying

The National Crime Prevention Council defines Cyberbullying as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.

11.4.4. Real-Life Incident of Cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi — the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the endues involved, we have changed their names.

Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad. The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.

A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days. This person was chatting on the Internet, using her name and giving her address, talking in obscene language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

This was the first time when a case of cyberstalking was registered. Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

11.5. Cybercafe and Cybercrimes

In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15-35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.

In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or raise terrorist communication. Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people.

Public computers, usually referred to the systems, available in cybercafes, hold two types of risks. First, we do not know what programs are installed on the computer — that is, risk of malicious programs such as key loggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior. Second, over-the-shoulder peeping (i.e., shoulder surfing) can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

Indian Information Technology Act (ITA) 2000 does not define cybercafes and interprets cybercafes as "network service providers" referred to under the erstwhile Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. The concept of "due diligence" was interpreted from the various provisions in cyber-cafe regulations where available or normal responsibilities were expected from network service providers.

Cybercriminals prefer cybercafes to carry out their activities. The criminals tend to identify one particular personal computer (PC) to prepare it for their use. Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target — techniques used for this. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

A recent survey conducted in one of the metropolitan cities in India reveals the following facts (this is an eye-opener after going through the following observations):

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.

3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cybercriminals hoodwink the investigating agencies. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button. Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Internet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes — one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security.

There are thousands of cybercafes across India. In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.

Note: There is an expectation that the Indian Computer Emergency Team referred to under section 70B of ITA 2008 may itself be designated as the agency of the central governement with a national jurisdiction and (Computer Emergency Response Team) CERT, and may itself be stepping into the shoes of the Indian Computer Emergency Team.

Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or sign out" before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options / before logon.

2. **Stay with the computer:** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.

3. **Clear history and temporary files:** Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. Therefore, before you begin browsing, do the following in case of the browser Internet Explorer:

   - Go to Tools —> Internet options —> click the Content tab —> click AutoComplete. If the checkboxes for passwords are selected, deselect them. Click Ok twice.
   - After you have finished browsing, you should clear the history and temporary Internet files folders. For this, go to Tools —> Internet options again —» click the General tab —» go to Temporary Internet Files —> click Delete Files and then click Delete Cookies.
   - Then, under history, click clear history. Wait for the process to finish before leaving the computer.

4 **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.

5. **Avoid online financial transactions:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.

6. **Change passwords:** If you are accessing any website (including bank websites) from cyber café, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at home.

   It is very important to do so especially when you have entered your transaction password from such shared computer or cybercafé computer. Change these passwords from your own PC at workplace or at house.

7. **Virtual keyboard:** Nowadays almost every bank has provided the Virtual Keyboard on their website. The virtual keyboard is designed to protect your password from malicious "Spyware" and "Trojan Programs". Use of Virtual Keyboard will reduce the risk of password theft.

8. **Security warnings:** One should take utmost care while accessing the websites of any banks/ financial institution. Individual should take care while accessing computers in public places, that is, accessing the Internet in public places such as hotels, libraries and holiday resorts. Moreover, one should not forget that whatever is applicable for cybercafes (i.e., from information security perspective) is also true in the case of all other public places where the Internet is made available (refer to Appendix J in CD). Hence, one should follow all tips about safety and security while operating the systems from these facilities.

11.6. Botnets: The Fuel for Cybercrime

11.6.1. Botnet

The dictionary, meaning of Bot is "(computing) an automated program for doing some particular task, often over a network".

Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically. The term is often associated with malicious software but can also refer to the network of computers using distributed computing software."

In simple terms, a Bot is simply an automated computer program. One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access. Your computer system maybe a part of a Botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge. "Zombie networks" have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools. Another option is to steal an existing Botnet. The following figure explains how Botnets create business.

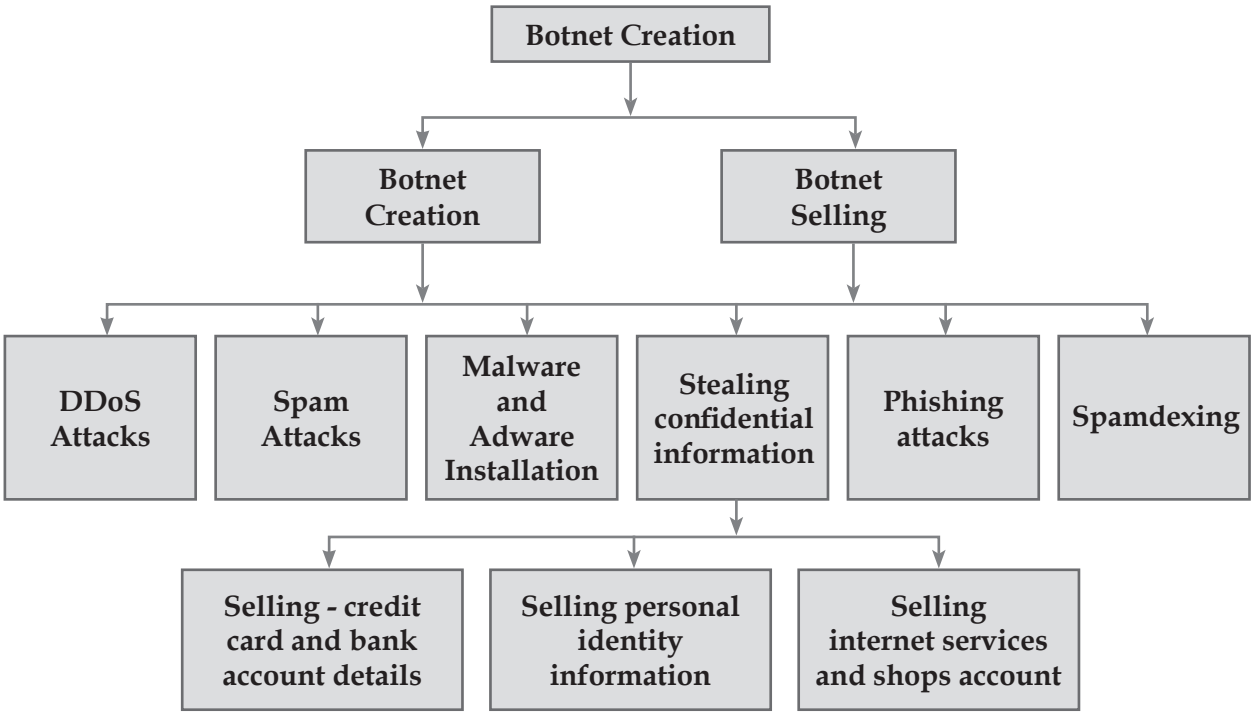


Fig. Botnets are Used for Gainful Purposes

If you salute your duty you no need to salute anybody, but if you pollute your duty, you have to salute everybody.
- Swami Vivekananda

Explanation for Technical Terms used in Fig,

- **Malware:** It is malicious software, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.
- **Adware:** It is advertising-supported software, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.
- **Spam:** It means unsolicited or undesired E-Mail messages.
- **Spamdexing:** It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
- **DDoS:** Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

One can reduce the chances of becoming part of a Bot by limiting access into the system. Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

One can ensure following to secure the system:

1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
3. **Use a firewall to protect the system from hacking attacks while it is connected, on the Internet:** A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-a-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.
5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized

toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.

6. **Check regularly the folders in the mail box — "sent items" or "outgoing" — for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.

7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

11.7. Attack Vector

An "attack vector" is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome. Attack vectors enable attackers to exploit system vulnerabilities, including the human element. Attack vectors include viruses, E-Mail attachments, web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.

To some extent, firewalls and antivirus software can block attack vectors. However, no protection method is totally attack-proof. A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.

Zero-Day Attack:

A zero-day (or zero-hour) attack is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package.

Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZGRT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems.

The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware. If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

In the technical terms, payload is the necessary data being carried within a packet or other transmission unit — in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs. From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end-user at the destination.

The attack vectors described here are how most of them are launched.

1. **Attack by E-Mail:** The hostile content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.

2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.

3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, hoaxes, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computers operator to succeed. Social engineering and hoaxes are other forms of deception that are often an attack vector too.

4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics, and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

5. **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.

6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses. Next they begin scanning the Internet from the computer they have just infected, and start looking for other computers to infect. If the worm is successful, it propagates rapidly. The worm owner soon has thousands of "zombie" computers to use for more mischief.

7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart (IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.

8. **Foistware (sneakware):** Foistware is the software that adds hidden components to the system on the sly. Spyware is the most common form of foistware. Foistware is quasi-legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.

9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

11.8. Cloud Computing

The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals. Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet ("cloud")-based development and use of computer technology ("computing"). The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks. Cloud computing is a term used for hosted services delivered over the Internet. A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand — typically by the minute or the hour;

2. it is elastic in terms of usage - a user can have as much or as little of a service as he/she wants at any given time;

3. the service is fully managed by the provider — a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

11.8.1 Why Cloud Computing?

The cloud computing has following advantages.

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one users computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

The cloud computing services can be either private or public. A public cloud sells services to anyone on the Internet. A private cloud is like a proprietary network or a data center that supplies the hosted services to a limited number of people. When a service provider uses public cloud resources to create a private cloud, the result is called a "virtual private cloud." The goal of cloud computing is to provide easy, scalable access to the computing resources and IT services.

Note: Although cloud computing is an emerging field, the idea has been evolved over few years. It is called cloud computing because the data and applications exist on a "cloud" of Web Servers.

11.8.2. Types of Services

Services provided by cloud computing are as follow

- **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
- **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the providers servers. Developers can create applications using the provider's APIs. Google Apps is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.
- **Software-as-a-service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

11.8.3. Cybercrime and Cloud Computing

Nowadays, prime area of the risk in cloud computing is protection of user data.

Table : Risks associated with cloud computing environment

Sr. No.	Area	What is the Risk?	How to Remediate the Risk?
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendors monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/ laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.
4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster - availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.

Sr. No.	Area	What is the Risk?	How to Remediate the Risk?
6.	Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
7.	Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at die stake.	Organization should ensure getting their data in case of such major events.

The risk areas identified in the above Table are considered to be key obstacles to adoption of cloud computing and making it an area of active research across the globe.

Summary

In this chapter we have discussed how technology is used in a different way for conducting illegal activities against a person, property, and/or organizations including governments. Considerable amount of time is spent in gathering information about a target. Therefore, one should have adequate knowledge about the technology to use, the different tools and techniques. Public networks and cybercafes are used to hide the ID for information gathering as well as launching attacks and hence it becomes important to take utmost care while operating/surfing through such facilities. People are the weakest link in the security domain and, hence, they get either exploited/deceived to obtain the required information; thus, this is called social engineering. Cyberstalking is another way through which criminals interact with victims directly, avoiding face-to-face conversation. Criminals do this either for harassing and/ or threatening behavior or to get the information from the victim. The Internet has become an integral part of the lifestyle nowadays and IT is found to be pervasive - the result is cloud computing; however, we should also be aware of threats inducing from such technologies like Botnets and attack vectors. Every technology has some limitations and attackers having good amount of knowledge will always try to exploit it.

अध्याय 12

Chapter 12

Understanding Computer Forensics

12.1. Introduction

The purpose of this chapter is to address the other side of crime, that is, use of forensic techniques in the investigation of cybercrimes. "Cyberforensics" is a very large domain and addressing it in a single chapter is indeed a challenge. Complex technical aspects involved in digital forensics/computer forensics are not possible to cover in a single chapter. Therefore, this chapter is aimed at only providing a broad understanding about cyberforensics.

The term "chain of custody" has a recurring mention in this chapter because it is a central concept in forensics. The terms "cyberforensics," "digital forensics" and "computer forensics" are used interchangeably. Definitions of these terms are provided.

Cyberforensics plays a key role in investigation of cybercrime. "Evidence" in the case of "cyberoffenses" is extremely important from legal perspective. There are legal aspects involved in the investigation as well as handling of the digital forensics evidence. Only the technically trained and experienced experts should be involved in the forensics activities.

Toward the end, a ready reckoner of cyberforensics tools is provided in a tabular form for readers' convenience. Considering the widespread use of hand-held devices [personal digital assistants (PDAs), mobile phones and all its varieties as well as the iPods, etc.], With this background, let us proceed to understand the historical background.

12.2 Historical Background of Cyberforensics

Computer is either the subject or the object of cybercrimes or is used as a tool to commit a cybercrime. The earliest recorded computer crimes occurred in 1969 and 1970 when student protestors burned computers at various universities. Around the same time, people were discovering methods for gaining unauthorized access to large-time shared computers. Computer intrusion and fraud committed with the help of computers were the first crimes to be widely recognized as a new type of crime.

The application of computer for investigating computer-based crime has led to development of a new field called computer forensics. Sometimes, computer forensics is also referred to as "digital forensics." Computer forensics/digital forensics has existed for as long as people have stored data inside computers.

Discussion on the legal side of cybercrime serves as a link to this chapter through the term "evidence," "digital evidence" in particular. Basically, computer forensics experts need digital evidence in cases involving data acquisition, preservation, recovery, analysis and reporting, intellectual property theft, computer misuse corporate policy violation, mobile device (PDA, cell phone) data acquisition and analysis, malicious software/application, system intrusion and compromise, encrypted, deleted and hidden files recovery, pornography, confidential information leakage, etc.

Computer forensics is still a relatively new discipline in the domain of computer security. It is a rapidly growing discipline and a fast growing profession as well as business. The focus of

computer forensics is to find out digital evidence — such evidence required to establish whether or not a fraud or a crime has been conducted. There is a difference between computer security and computer forensics. Although "computer forensics" is often associated with "computer security," the two are different.

Computer forensics is primarily concerned with the systematic "identification," "acquisition," "preservation" and "analysis" of digital evidence, typically after an unauthorized access to computer or unauthorized use of computer has taken place; while the main focus of "computer security" is the prevention of unauthorized access to computer systems as well as maintaining "confidentiality' "integrity" and "availability" of computer systems. Thus, the goal of computer forensics is to perform a structured investigation on a digital system. Computer crime is any criminal offense, activity or issue that involves computers.

There are two categories of computer crime: one is the criminal activity that involves using a computer to commit a crime, and the other is a criminal activity that has a computer as a target.

Information security experts consider "cyberlaw compliance" as one of the many aspects of "techno-legal information security." They advise organizations to formulate an appropriate plan of action to comply with cyberlaws as a part of the IS practice. This association of cyberlaw into the information security domain has gained additional importance due to some amendments that have been made to ITA 2000. Typical types of data requested for a digital forensics examination by the law enforcement agencies include: investigation into electronic mail (E-Mail) usage, website history, cell phone usage, cellular and Voice over Internet Protocol (VoIP) phone usage, file activity history, file creation or deletion, chat history, account login/logout records and more. Therefore, it becomes necessary to address the legal issues involved in cyber forensics.

Note: Forensics means a "characteristic of evidence" that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence level)

In precise terms, "forensics science" is the application of science to law and it is ultimately defined by use in court. Forensics science is the application of physical sciences to law in search for truth in civil, criminal and social behavioral matters to the end that injustice shall not be done to any member of society. An alternative definition for digital forensics science is:

the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

The goal of digital forensics is to determine the "evidential value" of crime scene and related evidence.

The roles and contributions of the digital forensics/computer forensics experts are almost parallel to those involved as forensics scientists in other crimes, namely, analysis of evidence,

provision of expert testimony, furnishing training in the proper recognition, and collection and preservation of the evidence. Now, let us understand the term "digital forensics science."

12.3. Digital Forensics Science

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence. There is a number of slightly varying definitions. The term computer forensics, however, is generally considered to be related to the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/ information which is magnetically stored or encoded. The objective of "cyberforensics" is to provide digital evidence of a specific or general activity. Following are two more definitions worth considering:

1. **Computer forensics:** It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations. In other words, it is the collection of techniques and tools used to find evidence in a computer.
2. **Digital forensics:** It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices. In general, the role of digital forensics is to:

1. Uncover and document evidence and leads.
2. Corroborate evidence discovered in other ways.
3. Assist in showing a pattern of events
4. Connect attack and victim computers
5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
6. Extract data that may be hidden, deleted or otherwise not directly available.

The typical scenarios involved are:

1. Employee Internet abuse
2. data leak/data breach — unauthorized disclosure of corporate information and data (accidental and intentional);
3. industrial espionage (corporate "spying" activities);

Why are people so afraid? The answer is that they have made themselves helpless and dependent on others. We are so lazy, we do not want to do anything ourselves. We want a Personal God, a Savior or a Prophet to do everything for us.
- Swami Vivekananda

4. damage assessment (following an incident);
5. criminal fraud and deception cases;
6. criminal cases (many criminals simply store information on computers, intentionally or unwittingly) and countless others
7. copyright violation

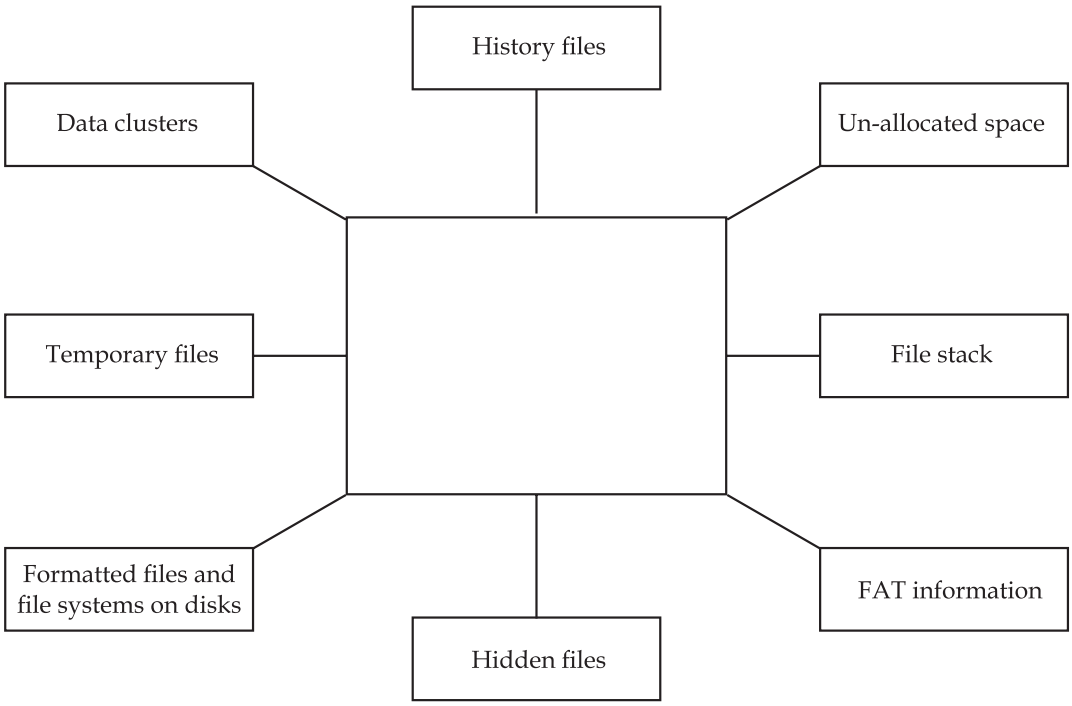


Fig. Data Seen Using Forensics Tools. FAT Means File Allocation Table

Using digital forensics techniques, one can:

1. Corroborate and clarify evidence otherwise discovered.
2. Generate investigative leads for follow-up and verification in other ways.
3. Provide help to verify an intrusion hypothesis.
4. Eliminate incorrect assumptions.

12.4. The Need for Computer Forensics

The convergence of Information and Communications Technology (ICT) advances and the pervasive use of computers worldwide together have brought about many advantages to mankind. At the same time, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime. This has lead to new risks for computer users and also increased opportunities for social harm. The users, businesses and organizations worldwide have to live with a constant threat from hackers who use a variety of techniques and tools to break into computer systems, steal information, change data and cause havoc. The widespread use of computer forensics is the result of two factors: the

increasing dependence of law enforcement on digital evidence and the ubiquity of computers that followed from the microcomputer revolution.

Digital Forensics Investigations and E-Discovery

Digital evidence plays a crucial role in the threat management life cycle, from incident response to high-stakes corporate litigation. Forensics discoveries provide the ability to search and analyze various pieces of potential evidence of electronic nature. Evidence can involve computer hard drives, portable storage, floppy diskettes, portable music players and PDAs, just to name a few.

All forms of evidence are verified and duplicated prior to investigation to ensure the integrity of the evidence for litigation purposes if needed. Managers who are responsible for litigation tend to take help from forensics professionals to solve a growing range of evidentiary and investigative challenges.

Key evidence often resides on more than a user hard drive or file server, requiring the capture and analysis of evidence from enterprise productivity servers, network logs or proprietary databases.

Many threats arise from illegal Internet activities that extend beyond the firewall and require new investigative and forensics approaches. Users are becoming more sophisticated and so are their efforts to circumvent security policies or encrypt, delete or destroy digital evidence. Forensics professionals need supporting solution for the acquisition, management and analysis of digital evidence. Such computer forensics services include the following:

1. Data culling and targeting;
2. discovery/subpoena process;
3. production of evidence;
4. expert affidavit support;
5. criminal/civil testimony;
6. cell phone forensics;
7. PDA forensics.

Specific client requests for forensics evidence extracting solution support include:

1. Index of files on hard drive;
2. index of recovered files;
3. MS Office/user generated document extraction;
4. unique E-Mail address extraction;
5. Internet activity/history;
6. storage of forensics image for 1 year
7. keywords search;
8. chain of custody

9. mail indexing;
10. deleted file/folder recovery;
11. office document recovery;
12. metadata indexing;
13. conversion to PDF;
14. log extraction;
15. instant messaging history recovery;
16. password recovery;
17. format for forensics extracts (DVD, CD, HDD, other)
18. network acquisitions.

Such types of computer evidences are important because quite often the evidence becomes the deciding factor in a criminal, civil or employee dismissal action. Investigations involving trade secrets, commercial disputes, and misdemeanor and felony crimes can be won or lost solely with the introduction of recovered E-Mail and other electronic documentation. If someone makes an attempt to delete, erase or otherwise hide critical evidence, you need the competent data recovery capabilities of forensics discoveries. Evidence that may not be known to attorneys may exist and often can be found during the forensics process. Also, timelines of computer usage is of help in crafting deposition questions and in targeting witnesses for interview.

Computer users typically "delete" incriminating and/or sensitive computer files (e.g., using tools such as "Deep Freeze," a software tool that is actually meant to protect your computer) but the information may still exist in slack space on the computer's hard drive that is hidden (do see the list of links provided at the end of this box). This computer data may linger for months or even years. However, it can be recovered and documented using computer forensics methods and techniques. Unfortunately, there are many examples of computer usage in violation of company policy. Sexual harassment, embezzlement, theft of trade secrets, abuse of the Internet and unauthorized outside employment on company time are just a few examples of violation that warrant a forensics examination of a computer. Even in investigations where hard drives are reformatted in an attempt to hide evidence, forensics discoveries can still potentially recover critical information (do see the list of links provided at the end of this box). Forensic discoveries can also aid in recovering passwords for critical files that have been maliciously set or changed.

The media, on which clues related to cybercrime reside, would vary from case to case. There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology; for example, external storage devices such as mini hard disks (pen drives) are available in amazing shapes.

Looking for digital forensics evidence (DFE) is like looking for a needle in the haystack. Here is a way to illustrate why there is always the need for forensics software on suspect media — the capacity of a typical regular hard disk is 500 GB (gigabytes). In an A4 size page, there are approximately 4,160 bytes (52 lines x 80 Characters = 4,160 bytes assuming 1 byte per character). This is equivalent to 4 KB (kilobytes). An A4 size of paper sheet has thickness of 0.004 inches. Data of 4 MB (megabyte; 1,000 times of 4 KB) when printed on A4 size of paper would be 4 inches thick. Data of 4 GB if printed on A4 sheet would be 4,000 inches, that is, 1,000 times of 4 MB. This would turn out to be 4 inches thick. The printout of 500 GB would be 500,000 inches! It would be virtually impossible to "retrieve" relevant forensics data from this heap!! There comes the help from forensics software - it helps sieve relevant data from the irrelevant mass (vital few from trivial many as the proverb goes).

The term "chain of custody" is important.

Chain of custody means "the chronological documentation trail, etc. "that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic.

Chain of Custody Example

The basic idea behind ensuring "chain of custody" is to ensure that the "evidence" is NOT tampered with. The recovery of a "crime weapon" at the murder scene would be an example of "chain of custody." This is explained below.

Case Study

Officer Amar collects the knife and places it into a container, then gives it to forensics technician Balan. Forensics technician Balan takes the knife to the laboratory and collects fingerprints and other evidence from the knife. He then gives the knife and all evidence gathered from the knife to evidence clerk Charu. Charu then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife and original copies of the lifted fingerprints).

The chain of custody requires that from the moment the evidence is collected, every transfer of evidence from one person to another person should be documented as it helps to prove that nobody else could have accessed that evidence. It is advisable to keep the number of evidence transfers as low as possible. In the courtroom, if the defendant challenges the chain of custody of the evidence, it can be proven that the knife in the evidence room is the same knife as found at the crime scene. However, if due to some discrepancies it cannot be proven who had the knife at a particular point in time, then the chain of custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

In a broader perspective "evidence" includes everything that is used to determine or demonstrate the truth of an assertion. Evidence can be used in court to convict people who are believed to have committed crimes; therefore, evidence must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct that can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The purpose behind recording the chain of custody is to establish that the alleged evidence is, indeed, related to the alleged crime, that is, the purpose is to establish the integrity of the evidence. In the context of conventional crimes, establishing "chain of custody" is especially important when the evidence consists of fungible goods.

Note: "Fungibitity" means the extent to which the components of an operation or product can be interchanged with similar components without decreasing the value of the operation or product.

For a person to be considered as "identifiable person," he/she must always have the physical custody of a piece of evidence. Practically speaking, this means that a police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place. All such transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to withstand legal challenges to the authenticity of the evidence. Documentation must include conditions under which the evidence is collected, the identity of all those who handled the evidence, duration of evidence custody, security conditions while handling or storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).

Note: Chain of custody is also used in most evidence stations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of Evidence.

Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party.

12.5. Cyberforensics and Digital Evidence

Cyberforensics can be divided into two domains:

1. Computer forensics;

2. network forensics.

Many security threats are possible through computer networks. Therefore, "network forensics" assumes importance in the context of cybercrime.

Network forensics the study of network traffic to search for truth in civil, criminial and administrative matters to protect users and resources from exploitation, invasion of privacy and any other crime fostered by the continual expansion of network connectivity;

As compared to the "physical" evidence, "digital evidence" is different in nature because it has some unique characteristics. First of all, digital evidence is much easier to change/ manipulate! Second, "perfect" digital copies can be made without harming original. At the same time the integrity of digital evidence can be proven. Another subtle aspect (of digital evidence) is that it is usually in the form of the "image" — this means that it is convenient and possible to create a defensible "clone" of storage device. Different information (clues) can be found at different levels of abstraction. Understanding the uniqueness of digital evidence

is important for appreciating the phases involved in a digital forensics investigation and maintaining the "chain of custody"

There are many forms of cybercrimes: sexual harassment cases — memos, letters, E-Mails; obscene chats or embezzlement cases — spreadsheets, memos, letters, E-Mails, online banking information; corporate espionage by way of memos, letters, E-Mails and chats; and frauds through memos, letters, spreadsheets and E-Mails. In case of computer crimes/cybercrimes, computer forensics helps. Computer forensics experts know the techniques to retrieve the data from files listed in standard directory search, hidden files, deleted files, deleted E-Mail and passwords, login IDs, encrypted files, hidden partitions, etc. Typically, the evidences reside on computer systems, user created files, user protected files, computer created files and on computer networks. Computer systems have the following:

1. Logical file system that consists of
    - File system: It includes files, volumes, directories and folders, file allocation tables (FAT) as in the older version of Windows Operating System, clusters, partitions, sectors.
    - Random access memory.
    - Physical storage media: It has magnetic force microscopy that can be used to recover data from overwritten area.
        a) Slack space: It is a space allocated to the file but is not actually used due to internal fragmentation and
        b) unallocated space.
2. User created files: It consists of address books, audio/video files, calendars, database files, spreadsheets, E-Mails, Internet bookmarks, documents and text files.
3. Computer created files: It consists of backups, cookies, configuration files, history files, log files, swap files, system files, temporary files, etc.
4. Computer networks: It consists of the Application Layer, the Transportation Layer, the Network Layer, the Datalink Layer.

The Father of Forensics Science - the Sherlock Holmes of France:

The year 1877-1966 was the era of Dr. Edmond Locard. He is considered as the pioneer in forensics science and was popularly known as the Sherlock Holmes of France. He formulated the basic principle of forensics science: "Every contact leaves a trace." This came to be known as Locard's exchange principle. Following is one of his most famous quotes:

Wherever he steps, wherever he touches, whatever he leaves, even without consciousness, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent

because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. In other words, Whenever two human beings come into contact, something from one is exchanged to the other, that is, dust, skin cells, hair, etc."

Locard studied medicine and law at Lyon, eventually becoming the assistant of Alexartare Lacassagne, a criminologist and professor. He held this post until 1910, when he began the foundation of his criminal laboratory. He produced a monumental seven-volume work, Traite de Criminalistique. and in 1918, developed 12 matching points for fingerprint identification. He continued with his research until his death in 1966.

12.5.1. The Rules of Evidence

This is a very important discussion, especially, for those who are students of legal courses. Indian IT Act amended the Indian Evidence Act. According to the "Indian Evidence Act 1872," "Evidence" means and includes:

1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
2. All documents that are produced for the inspection of the court are called documentary evidence.

Legal community believes that "electronic evidence" is a new breed of evidence. They also, at times, have an apprehension that the law of evidence as per Indian Evidence Act of 1872 may not hold good for electronic evidence. Some lawyers express doubts and apprehensions about the process of leading electronic evidence in the courts. However, this is not true; the traditional principles of leading evidence, along with certain newly added provisions in the Indian Evidence Act 1972 through the Information Technology Act (ITA) 2000, constitute the body of law applicable to electronic evidence. The challenges, however, need to be understood from the "rules of evidence" perspective.

Paper evidence, the process is cleat! and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

It is only logical that the process used in the case of digital evidence mimic the process that is used for paper evidence. As each step requires the use of tools or knowledge, the process must be documented, reliable and repeatable. The process itself must be understandable to the members of the court. Acquisition of digital evidence is both a legal and technical problem. In fact, these two aspects are irrevocably related. The law specifies what can be seized, under what conditions, from whom and from where. It requires to determine what particular piece of digital evidence is required for examination, that is, is it a particular file or a word processing document or an executable program, etc It may also require examination to determine where a particular piece of evidence is physically located. Is the file on a local hard drive or is it on a server located in another legal jurisdiction? In short, it may be necessary to show a technical

basis for obtaining the legal authority to search. Likewise, it may require technical skills to actually accomplish the search. The product of this phase is usually raw media, devoid of meaning or usefulness.

There are number of contexts involved in actually identifying a piece of digital evidence:

1. Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.
2. Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.
3. Legal context: We must place the evidence in the correct context to read its meaning. This may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

"Digital evidence originates from a number of sources such as seized computer hard drives and backup media, real-time E-Mail messages, chat room logs, Internet service provider records, webpages, digital network traffic, local and virtual databases, digital directories, wireless devices, memory cards, digital cameras, etc. Digital forensics examiners must consider the trustworthiness of this digital data. Many vendors provide technology solutions to extract this digital data from these devices and networks. Once the extraction of the digital evidence has been accomplished, protecting the digital integrity becomes paramount concern for investigators, prosecutors and those accused.

Similarly for the evidence in regular crimes, it is important to "isolate" the potential evidence. Some important tips are — do not turn ON the computer or review media, restrict physical and remote access, unplug computer power, network and phone fine, and document times, people and steps taken. A point to note is that the need to unplug the computer power depends on the crime situation and the type of analysis required. For example, for live analysis of the digital evidence, it would not be advisable to unplug the power. Therefore, it is best to involve qualified specialists early in the process. Following are some guidelines for the (digital) evidence collection phase:

1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.
2. Capture a picture of the system as accurately as possible.
3. Keep detailed notes with dates and times. If possible, generate an automatic transcript (e.g., on Unix systems the "script" program can be used; however, the output file it generates should not be given to media as that is a part of the evidence). Notes and printouts should be signed and dated.
4. Note the difference between the system clock and Coordinated Universal Time (UTC). For each timestamp provided, indicate whether UTC or local time is used (since 1972 over 40 countries throughout the world have adopted UTC as their official time source).

5. Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
6. Minimize changes to the data as you are collecting it. This is not limited to content changes; avoid updating file or directory access times.
7. Remove external avenues for change.
8. When confronted with a choice between collection and analysis you should do collection first and analysis later.
9. Needless to say, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly, in a crisis. If possible, procedures should be automated for reasons of speed and accuracy. Being methodical always helps.
10. For each device, a systematic approach should be adopted to follow the guidelines laid down in your collection procedure. Speed will often be critical; therefore, where there are a number of devices requiring examination, it may be appropriate to spread the work among your team to collect the evidence in parallel. However, on a single given system collection should be done step by step.
11. Proceed from the volatile to the less volatile; order of volatility is as follows:
    - Registers, cache (most volatile, i.e., contents lost as soon as the power is turned OFF);
    - routing table, Address Resolution Protocol (ARP) cache, process table, kernel statistics, memory;
    - temporary file systems;
    - disk;
    - remote logging and monitoring data that is relevant to the system in question;
    - physical configuration and network topology;
    - archival media (least volatile, i.e., holds data even after power is turned OFF).
12. You should make a bit-level copy of the system's media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. Try to avoid doing forensics on the evidence copy.

Address Resolution Protocol (ARP) is a very important part of IP networking. ARP is used to connect OSI Layer 3 (Network) to OSI Layer 2 (Datalink). For most of us this means that ARP is used to link our IP addressing to our Ethernet addressing (MAC Addressing). For you to communicate with any device on your network, you must have the Ethernet MAC address for that device. If the device is not on your LAN, you go through your default gateway (your router). In this case, your router will be the destination MAC address that your PC will communicate with. There are two types of ARP entries: static and dynamic. Most of the time, you will use dynamic ARP entries.

What this means is that the ARP entry (the Ethernet MAC to IP address link) is kept on a device for some period of time, as long as it is being used. The opposite of a dynamic ARP entry is static ARP entry. With a static ARP entry, you are manually entering the link between the Ethernet MAC address and the IP address. Because of management headaches and the lack of significant negatives to using dynamic ARP entries, dynamic ARP entries are used most of the time.

12.6. Forensics Analysis of E-Mail

It was mentioned how criminals can use fake mails for various cybercrime offenses. There are tools available that help create fake mails. Forensics analysis of E-Mails is an important aspect of cyberforensics analysis — it helps establish the authenticity of an E-Mail when suspected. This aspect is explained in this section - we start with understanding E-Mail components and then the E-Mail header structure is explained. E-Mails are now the most common means of communication worldwide and are often the subject of forensics analysis if this happens to constitute "digital evidence." Owing to the rising pressures from regulatory agencies and also due to possible litigations in global businesses, organizations are obligated to electronically store information to support discovery and disclosure requests. In this section, we want to discuss how E-Mail messages/IDs can help in forensic analysis of cybercrimes.

An E-Mail system is the hardware and software that controls the flow of E-Mail. The two most important components of an E-Mail system are the E-Mail server and the E-Mail gateway. E-Mail servers are computers that forward, collect, store and deliver E-Mail to their clients and E-Mail gateways are the connections between E-Mail servers. Mail server software is a network server software that controls the flow of E-Mail and the mail client software helps each user read, compose, send and delete messages. An E-Mail consists of two parts, the header and the body. Message headers are the important part for investigating E-Mail messages and hence it will be discussed in detail in this section. The "header" of an E-Mail is very important from forensics point of view — a full header view of an E-Mail provides the entire path of E-Mails journey from its origin to its destination. The header view includes the originating Internet Protocol (IP) address and other useful information. There is usually a link provided on the E-Mail from its origin to its destination.

1. Return-Path: <secret@hotmail.com>
2. Received: from mailhub-1 .net.treas.gov ([10.7.14.10]) by nccmail.usss.treas.gov for <avenit@usss.treas.gov>; Fri, 18 Feb 2000 11:46:07-0500
3. Received: from mx-relay.treas.gov ([199.196.144.6]) bytias4.net.treas.gov via smtpd (for mailhub.net.treas.gov [10.7.8.10]) with SMTP; 18 Feb 2000 16:55:44
4. Received: from hotmail.com (f7.law4.hotmail.com [216.33.149.7]) by mx-relay2.treas.gov for <avenit@usss. treas.gov>; Fri, 18 Feb 2000 11:55:44 - 0500 (EST)
5. Message-ID: <20000218165543.56965.qmail@hotmail.com>
6. Received: from 199.196.144.42 by www.hotmail.com with HTTP; Fri, 18 Feb 2000 08:55:43

7. X-Originating-IP: [199.196.144.42]
8. From: "Secret" <secret@hotmail.com>
9. To: avenit@usss.treas.gov
10. CC: smith@aol.com

Header information varies with E-Mail service provider, E-Mail applications and system configuration. As we know, the header part carries information that is needed for E-Mail routing, subject line and time stamps whereas the body contains the actual message/data of an E-Mail. The header and the body are separated by a blank line. The header contains several mandatory and optional fields, trace information and heading fields. The E-Mail header is a sequence of fields (it may not be in a particular order), each consisting of a field name and a field value. An example of a heading field would be: To: xyz@abccom.in. Headers on E-Mail can easily be "spoofed" by spammers and other irresponsible network users. E-Mails, when used in cyberforensics investigation, must get uniquely identified, if, for example, an E-Mail is suspected to be one of the evidence sources.

As mentioned earlier, the body of an E-Mail is separated from the header and it might also contain attachments in the form of MIME or SMIME (also known as S/MIME — secure/multipurpose Internet mail extensions). It is a protocol that provides digital signatures and encryption of Internet MIME messages. It is an encoding protocol.

We have mentioned previously that an E-Mail has two parts and header is one of those two parts. However, there is a header protocol: when an E-Mail message is sent, the user typically controls only the recipient line(s), that is, To, Cc and Bcc, if mentioned, and the Subject and Date. The rest of the header information is added by mall software while it is processed. Along the E-Mails route, a server can add or delete lines (anonymous remailer). The discussion that follows is with reference to those numbers. Header Protocol Analysis is important for investing evidence that may come in form of an E-Mail.

Every computer that receives this message adds a "Received : field" with its complete address and time stamp; this helps in tracking delivery problems. Element 5 of the mail header is the Message-ID, a unique identifier for this specific message. The Message-ID is logged and it can be traced through computers that are on the message route if there is a need to track the mail. Element 6 of the E-Mail header shows where the E-Mail was first received from with the IP address of the sender. It also shows the date and time when the message was sent. In this regard, it is important to understand the difference between simple mail transfer protocol (SMTP) and Hypertext Transfer Protocol (HTTP). HTTP is used to transfer display able webpages and related files whereas SMTP is used to transfer E-Mail. Thus, SMTP is a protocol for sending E-Mail messages between servers whereas HTTP is a set of rules used to browse through Internet commonly used with web browsers such as Internet Explorer, Firefox). When you request, E-Mail logs you and you should ensure that you get them from the right server.

Next, consider element 7 of the sample mail header shown in E-mail header example Table - it shows the originating IP address of the sender, but without the date and time the IP address will not allow you to identify the specific user. This may or may not be present in headers. If the IP address is a "Static" Address, you will be able to identify the specific user (most IP addresses are "dynamically" assigned). Element 8 indicates the name and E-Mail address of the message originator, that is, the "sender." Generally, this is the domain name we want to trace. Element 9 shows the name and E-Mail address of the primary recipient; the address may be for a mailing list (sales_dep@company.com) or system wide alias (avenit@usss.treas.gov) or a personal username. The next element, element 10, of the sample mail header lists the names and E-Mail addresses of the "courtesy copy" recipients of the message. Some E-Mails may have "Bcc:" recipients as well; these "blind carbon copy" recipients get copies of the message, however their names and addresses are not visible in the headers.

Once we get the IP address our task is to find the Internet service provider details. The following links are worth visiting:

1. www.all-nettools.com (among other tools; a link to E-Mail tools is available here);
2. www.ip2location.com (there is a utility here that helps you know where your Internet visitors are coming from, that is, which country, which state, which city, which Internet service provider, which domain name, which connection type, which ZIP code, etc. It helps you trace an IP address to Country, Region, City, Latitude, Longitude, ZIP Code, Time Zone, Connection Speed, Internet service provider, Domain Name, IDD Country Code, Area Code, Weather Station Code and Name).
3. www.domaintools.com (there are DNS tool and many other tools available here);
4. www.dnsstuff.com (domain/E-Mail-related tools are accessible from this site);
5. http://www.hackingspirits.com/cyb_forensics/fsic_articles/trace_emails.html is a good link to know tracing the origin of an E-Mail, that is, locating countries from an IP address.

The Internet service provider plays an important role in E-Mail forensics. The Internet service provider provides Internet access to businesses, organizations, schools, colleges and individuals. Examples of Internet service provider are VSNL (Videsh Sanchar Nigam Limited), Sify, Hathway, Rolta, MTNL/BSNL, Reliance, etc. The details available from the Internet service provider are name, address and contact number of the subscriber of the Internet facility, type of IP address, any other relevant information with regard to IP address at a particular given date and time, usage details, etc.

Points to Remember when you Use E-Mail as an Evidence

1. Ensure the use of E-Mail is subject to agreed procedures, which are supported and enforced by management at a high level. Acceptable Use Policies ought to prescribe good usage and identify bad usage.
2. Train users of E-Mail about acceptable use of E-Mail, and about their rights and the obligations expected of them.

3. Implement access control mechanisms to computer systems - so that its use can be attributed to a person, a terminal, a date and a time.
4. Ensure computer systems are kept safe and secure so that the systems and the data within are protected from unauthorized access and accidental or deliberate loss and damage.
5. Retention and deletion of E-Mail should be organization-defined and not user-defined. Individual users should not have any discretion as to the categories of E-Mails that should be retained or deleted.
6. Implement a solution that archives and stores E-Mails centrally. The archive should support all the main file formats and also retain metadata.
7. The archive should classify E-Mails entering the archive at the point of entry. The archive should prevent the entry of duplicates.
8. Make sure that the archiving platform facilitates the exporting of evidence as files as a part of the E-Discovery process.
9. Implement an archiving solution that allows full search and retrieval. Metadata should be searchable as should content.
10. Enable logging of all events acting on the archive. The logs should be retained as part of the archive, for auditing and verification purposes.
11. Provide contingency for continuity of both archiving and discovery in the event of an outage.
12. Ensure the archiving platform supports the marking-up of files so that privileged materials can be withheld and/or redacted during E-Discovery.

E-Mail headers are organized bottom-up. This means that the E-Mail was handed from the machines at the bottom of the E-Mail header to the ones at the top of it. These machines are referred to as Message Transfer Agents (MTAs) and each of them adds a "received" section to the E-Mail header, sometimes referred to as "received header". This is similar to postmarks used in conventional postal systems. The order of the "received" sections is like a stack of pancakes, with the one receiving the E-Mail last at the top of the stack. This means that three MTAs were involved in the delivery of the E-Mail message with the one at the bottom being the one receiving the original message from the sender.

Note: E-Mail tracing is done by examining the header information contained in E-Mail messages to determine their source.

While tracing E-Mails, the "header information" is included along with E-Mails either at the beginning or the end of E-Mail messages.

To determine the source of the E-Mail, investigators must first examine the received section at the bottom of the header and work their way up in a bottom to top approach.

It is also important that during E-Mail investigation cases the logs of all servers in the received chain are examined as soon as possible. The time stamp is very important in E-Mail investigation

cases because HTTP and SMTP logs get archived frequently, especially by large Internet service providers. When a log is archived, a considerable amount of time and effort is involved to retrieve and decompress the log files needed to trace E-Mails. Fake E-Mail creation tools are rampantly used by cybercriminals. Therefore, it is possible that some E-Mails have fake headers with fake "from" E-Mail addresses to fool investigators; however, extreme caution and careful scrutiny should be practiced in investigating every part of the E-Mail header.

Typically, the sender's E-Mail address can be found after the "From" section of the header. However, that is not the only place it can be found. It can also be found under other sections depending on the E-Mail client uses. These sections include the following (this is not the exhaustive list; it is just an example to give you some idea):

1. X-originating E-Mail;
2. X-sender;
3. return-path.

At times, E-Mail addresses can suggest the method used to generate the E-Mail and the server that the E-Mail originated from (i.e., hotmail, oudook, corporate server, Internet service provider, etc). However, E-Mail addresses should be viewed with caution by investigators as they can be easily faked. Note that some headers begin with an "X-," this means that they are X-headers. You can use X-headers to sort and filter E-Mails sent by SourceForge. Depending on the context of the message, custom E-Mail headers (X-headers) are added to the E-Mail. The customer headers can be used by E-Mail agents and clients to filter and sort E-Mail. For example, both Outlook and Thunderbird support filtering on custom E-Mail headers. Thus, X-headers are inserted by E-Mail client programs or applications that use E-Mail to pass information to E-Mail handling programs for processing. They may be introduced by large vendors and picked up for use by others. In this way an X-header can be considered as a de facto standard. An example of this is the "X-Mailer" header which many E-Mail clients use to define the E-Mail client application and version used.

1. **Received:** from search.org ([64.162.18.2]) by sgiserver1.search.org with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2650.21) id K9HBB4C4; Mon, 21 May 2001 09:47:01-0700

2. **Received:** from webl4506.mail.yahoo.com ([216.136.224.69]) by SEARCH.ORG with SMTP (IPAD 2.52) id 3579700; Mon, 21 May 2001 08:47:23-0800 Message-ID: <20010521164640.85785.qmail@webl4506.mail.yahoo.com>

3. **Received:** from [216.104.228.118] by web14506.mail.yahoo.com; Mon, 21 May 2001 09:46:40 PDT Date: Mon, 21 May 2001 09:46:40 -0700 (PDT) From: Can Do <can_do1@yahoo.com> Subject: check out this E-Mail header To: todd@search.org MIME-Version: 1.0 Content-Type: text/plain; charset = us-ascii

Next, let us understand how fake E-Mail addresses can be detected. The sender's E-Mail address can be easily faked and can be hard to detect. If the server mentioned in the bottom

As long as we believe ourselves to be even the least different from God, fear remains with us; but when we know ourselves to be the One, fear goes; of what can we be afraid? ***- Swami Vivekananda***

"received" section does not match the server of the E-Mail address, this suggests that the E-Mail address is a fake one.

Now let us consider Sendmail. Sendmail is a general purpose Internet work E-Mail routing facility that supports many kinds of mail-transfer and delivery methods, including SMTP used for E-Mail transport over the Internet. Sendmail is a descendant of the delivermail program that was written by Eric Allman. Sendmail is a well-known project of the free and open-source software (OSS) and Unix communities, and has spread both as free software and proprietary software. It is a very widely used MTA. MTAs send mail from one machine to another. Sendmail is not a client program, which you use to read your E-Mail but rather a behind-the-scenes program that actually moves your E-Mail over networks or the Internet to where you want it to go. If there is ever a situation to reconfigure Sendmail, you will also need to have the sendmail.cf package installed. In case you need documentation on Sendmail, you need to install the sendmail-doc package.

To uniquely identify each E-Mail, all MTAs use some sort of unique identifier. This identifier is referred to as "Message-ID." Message-ID field is inserted into a header either by mail user agent (MUA) or the first MTA. Even though the Message-ID is optional as per RF2822, it recommends using it. Sendmail, for example, is one MTA that handles E-Mail delivery and relaying process. Sendmail uses Message-ID for tracing E-Mails and for logging process IDs. It recommends including Message-ID in E-Mails and also recommends setting relevant macros in its configuration file to implement compulsory checking of Message-IDs.

Deep analysis on Message-IDs may reveal some sort of information that will open a window to trace the source of an E-Mail. Also Message-ID will help to find a particular E-Mail log entry within a log file of E-Mail server.

Received: from infvic.it (adsl-98-201.38-151.net24.it [151.38.201.98]) by mail-relay2.bpvi.it (Postfix) with ESMTP id 2887550074 for <redazione@infvic.it>; Mon, 19 Apr 2004 10:41:54 +0200 (CEST) From: sfiorillo@hotmail.com

Only technical envy spammers can spoof the Message-ID cleverly. So deep analysis on Message-IDs may reveal some sort of information that will open a window to trace the source of an E-Mail. Also the Message-ID will help to find a particular E-Mail log entry within a log file of E-Mail server. There are some commonalities between conventional mails and E-Mails; for example, like conventional mail service, when E-Mail is routed from source to destination all intermediate relay servers (SMTP) insert their stamp at the beginning of the header. This stamping procedure helps to trace the E-Mail if such a demand arises. The stamp consists of three fields, namely. "From," "SMTP-ID" and "For."

The text shows an E-Mail header that passed through several MTAs, that is, E-Mail header with several identifiers. Each MTA inserted a unique ID in the header of E-Mail. There are several identifiers in the header field of an E-Mail that may help to trace the source of the E-Mail. Analyzing intermediate SMTP-IDs is beyond the scope of this book. However, in this section, we have briefly discussed intermediate SMTP-IDs.

In the context of E-Mail, "messages" are viewed as having an "envelope" and "contents." The envelope contains information required to accomplish transmission and delivery. The contents contain the object to be delivered to the recipient. The delivery has to be at a valid E-Mail address and this is where the RFC2822 comes into picture.

12.7. Digital Forensics Life Cycle

As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination. .The cardinal rules to remember are that evidence:

1. is admissible;
2. is authentic;
3. is complete;
4. is reliable;
5. is understandable and believable.

Let us now understand what is involved in the digital forensics process.

12.7.1. The Digital Forensics Process

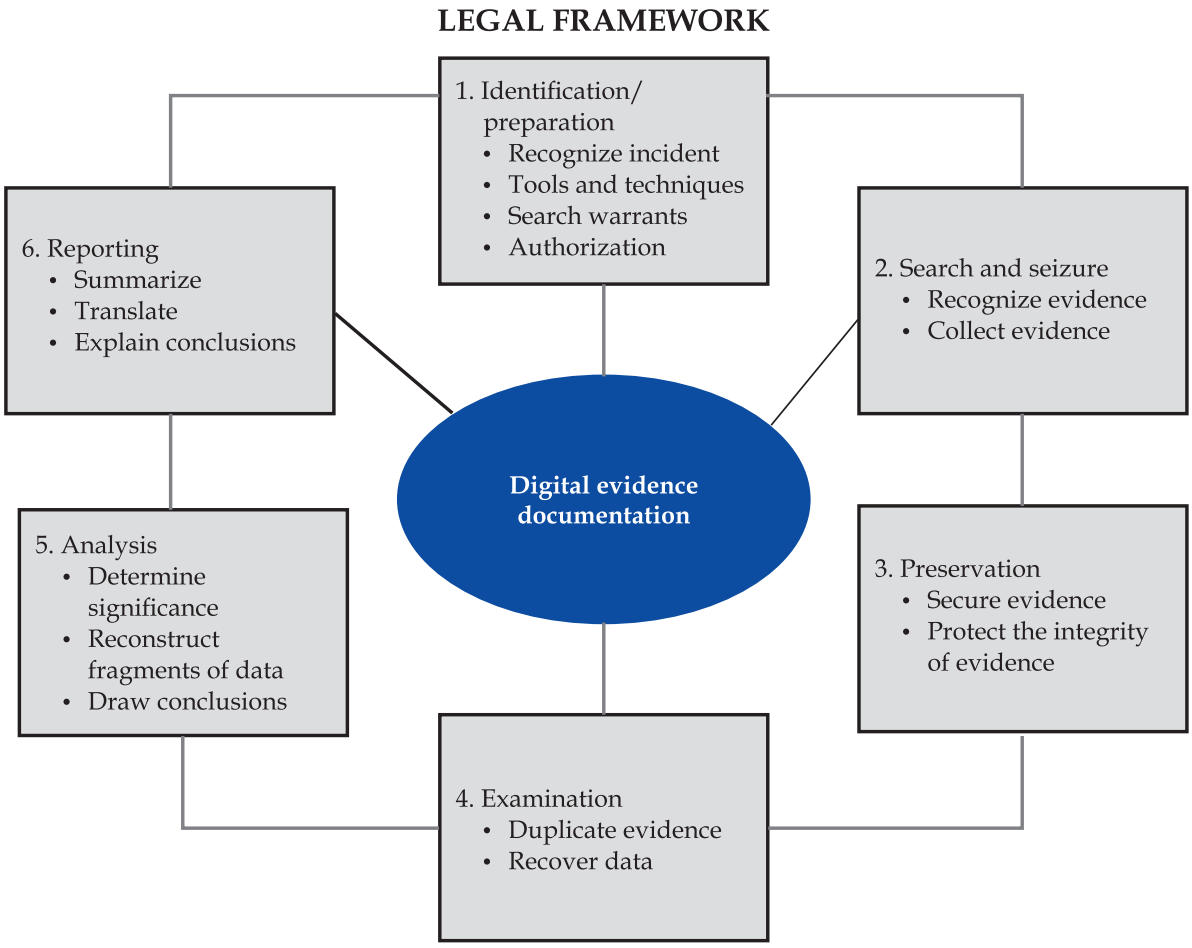


Fig. Process Model for Understanding a Seizure and Handling of Forensics Evidence Legal Framework

The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying. Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case. The exhibits should be introduced and presented and/or challenged by properly qualified people using a properly applied methodology that addresses the legal theories at issue. The tie between technical issues associated with the digital forensics evidence and the legal theories is the job of "expert witnesses."

As part of the court procedure, the exhibits are introduced as evidence by either side. Testimony is presented to establish the process to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/ or reconstruct the information contained in the exhibits and to establish, to the standard of proof required by the matter at hand, that the evidence reflects a sequence of events that is asserted to have produced it. The party must show not only the evidence to be admitted but must also establish that the evidence is relevant, authentic and that the evidence presented is not the result of hearsay, original writing or the legal equivalent thereof, and more probative than prejudicial.

अध्याय 13
Chapter 13

Fundamentals of Cyber Security, Significance of Cyber Security and Major Cyber Security Risks for the Common Man

13.1. Fundamentals of Cyber Security

13.1.1. Basic Components of Computer Security

Given that attacks against information technology systems are very attractive, and that their numbers and sophistication are expected to keep increasing, we need to have the knowledge and tools for a successful cyber defense. Cyber security is the branch of security dealing with digital or information technology. Computer security is an important aspect of cyber security. Computer security rests on confidentiality, integrity, and availability.

13.1.1.1. Confidentiality

Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information to those who need that information. The first formal work in computer security was motivated by the military's attempt to implement controls to enforce a "need to know" principle. This principle also applies to industrial firms, which keep their proprietary designs secure lest their competitors try to steal the designs.

Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. A cryptographic key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected. For example, enciphering an income tax return will prevent anyone from reading it. If the owner needs to see the return, it must be deciphered. Only the possessor of the cryptographic key can enter it into a deciphering program. However, if someone else can read the key when it is entered into the program, the confidentiality of the tax return has been compromised.

Encryption schemes are used to protect messages against eavesdroppers, and therefore achieve message confidentiality. Specifically, the information we want to protect (commonly called the plaintext) is transformed with an encryption algorithm (also called a cipher) into mangled data (commonly called the ciphertext) such that it is unintelligible to anyone not possessing the secret key. In general, the security of an encryption scheme depends on the difficulty of breaking the secrecy of the plaintext. In practice, an encryption scheme needs to be only as secure as the system requires.

Other system-dependent mechanisms can prevent processes from illicitly accessing information. Unlike enciphered data, however, data protected only by these controls can be read when the controls fail or are bypassed. They can protect the secrecy of data more completely than cryptography, but if they fail or are evaded, the data becomes visible. Access control mechanisms sometimes conceal the mere existence of data, lest the existence itself reveal information that should be protected. Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself. The precise number of people who distrust a politician may be less important than knowing that such a poll was taken by the politician's staff. How a particular government agency harassed citizens in its country may be less important than knowing that such harassment occurred.

Resource hiding is another important aspect of confidentiality. Websites often wish to conceal their configuration as well as what systems they are using; organizations may not wish others to know about specific equipment (because it could be used without authorization or in inappropriate ways), and a company renting time from a service provider may not want others to know what resources it is using. Access control mechanisms provide these capabilities as well.

13.1.1.2. Fundamentals of Cryptography

Hash Functions

An important primitive in cryptography is a hash function. The basic goal of a cryptographic hash function is to provide a seemingly random and compact representation (the hash value) of an arbitrary-length input string (which can be a document or a message). A hash function has two properties: (1) it is one way (it is hard to invert, where hard means it is computationally in feasible), and (2) it is collision resistant (it is hard to find two inputs that map to the same output).

Hash functions have a variety of applications from integrity verification to randomization functions. Network administrators can store in a database the hash of the passwords instead of the raw passwords themselves. The one-wayness property of hash functions prevents an attacker from obtaining the passwords if the database is compromised. Furthermore, hash functions are used in several cryptographic algorithms, such as message integrity codes, digital signatures, and encryption schemes.

Hash functions in practice are most susceptible to collision attacks. In this attack, the adversary tries to find two inputs to the hash function that map to the same output. If hash functions are used for signature schemes, a collision attack can allow an adversary to forge a signed message. Most recently SHA-1, the most popular hash function at the moment, has been successfully attacked. Although these attacks have not yielded a practical use for the two inputs mapping to the same hash output, the potential for finding useful attacks is increasing. In order to avoid practical attacks on hash functions, in January 2007 NIST (National Institute of Standards & Technology) announced a public competition for a new cryptographic hash function that would become the new federal information processing standard.

Secret-Key and Public-Key Cryptography

In an analogy to the way locks are opened with keys, cryptographers have used the idea of a key to refer to the information necessary to access cryptographically protected data. Modern cryptography follows Kerckhoffs' principle, which states that "the security of a system should depend on its key, not on its design remaining obscure". In short, the common practice in cryptography is not to rely on the secrecy of the algorithms, only on the secrecy of the secret keys.

There are two types of encryption algorithms, one which uses a secret key shared between the two communicating parties, and another one in which only one party knows the secret key, and everyone else (even the adversary) knows the public key (known as public-key cryptography).

Secret-key cryptography, also known as symmetric cryptography, involves the use of a single key shared between a pair of users. The fact that you need to share a secret key with every

other party that you wish to communicate with makes secret key cryptography cumbersome for several applications. There are two main problems with the key management in symmetric key systems. First, since secrets are shared between pairs of users, a large system will contain a large number of secrets, which is hard to manage. The second problem is related to the initial sharing of secrets between users. In particular, the difficulty of establishing an initial secret key between two communicating parties, when a secure channel does not already exist between them, presents a chicken-and-egg problem. This problem is most commonly solved using Key Distribution Centers (KDC), which are trusted intermediaries between communicating parties. By having trusted intermediaries, a party only needs to share a secret key with the KDC. Whenever two new parties need to communicate, they establish a secret key with the help of the KDC. Using a KDC has two important shortcomings! first, the KDC introduces a single point of failure and if it crashes the whole system fails. Second, the security of the entire system breaks if the KDC is compromised. These two problems are solved through the use of public-key cryptography.

In public-key cryptography, also known as asymmetric cryptography, parties do not share any secrets and different keys are used for encrypting and decrypting. This is a particularly powerful primitive as it enables two parties to communicate secretly without having agreed on any secret information in advance. In this setting, one party (the receiver) generates a pair of keys, called the public key and the secret key. The public key can then be made openly available so anyone can (for example) encrypt a message for the receiver. The receiver then uses its secret key to recover the message.

Public-key algorithms are less efficient than their secret-key counterparts; therefore, in practice public-key cryptography is often used in combination with secret-key cryptography. For example, in the Pretty Good Privacy (PGP) set of algorithms for encrypting emails, a public key is used to encrypt a symmetric key. The symmetric key, in turn, is used to encrypt the bulk of the message. Although public-key cryptography is computationally more intensive than secret-key cryptography, it requires simpler key management. However, a central problem in public-key cryptography is ensuring that a public-key is authentic, that is, we need to make sure that the public key we have was created by the party with whom we wish to communicate, and that it has not been modified or fabricated by a malicious party.

A Public Key Infrastructure (PKI) provides the necessary services to distribute and manage authentic public keys. A trusted server called a Certification Authority (CA) issues a public-key certificate to each user in its system, certifying the user's public-key information. The main benefits of a CA are that it can operate offline and that its compromise does not lead to the compromise of the secrets of the existing users of the system. There are two main approaches to PKI: centralized (such as the X.509 model) and decentralized (such as the "web of trust" used in PGP).

The most common examples of public-key encryption schemes are RSA (named after the initials of the inventors), and El-Gamal. RSA is based on the presumed difficulty of factoring large integers, the factoring problem. Both cryptosystems rely on exponentiation, which is a fairly expensive operation. More efficient schemes have been introduced that rely on elliptic curve cryptography.

Secret-key encryption algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. The most common examples of secret-key algorithms include the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) block ciphers, and the RC4 stream cipher. RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code". It is the most widely used software stream cipher and is used in popular protocols such as Secure Sockets Layer (SSL) (to protect Internet traffic) and WEP (to secure wireless networks).

13.1.1.3. Integrity

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and credibility and on the trust that people place in the information. This dichotomy illustrates the principle that the aspect of integrity known as credibility is central to the proper functioning of a system. For example, a newspaper may print information obtained from a leak at the White House but attribute it to the wrong source. The information is printed as received (preserving data integrity), but its source is incorrect (corrupting origin integrity).

Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. The distinction between these two types of attempts is important. The former occurs when a user tries to change data which he has no authority to change. The latter occurs when a user authorized to make certain changes in the data tries to change the data in other ways. For example, suppose an accounting system is on a computer. Someone breaks into the system and tries to modify the accounting data. That is, an unauthorized user has tried to violate the integrity of the accounting database. But if an accountant hired by the firm to maintain its books tries to embezzle money by sending it overseas to a Swiss bank account and hiding the transactions, a user (the accountant) has tried to change data (the accounting data) in unauthorized ways (by moving it to a Swiss bank account). Adequate authentication and access controls will generally stop the break-in from the outside, but preventing the second type of attempt requires very different controls.

Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events (user or system actions) to detect problems or (more commonly) may analyze the data itself to see if required or expected constraints still hold. The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt.

Working with integrity is very different from working with confidentiality. With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the

trustworthiness of the data. The origin of the data (how and from whom it was obtained), how well the data was protected before it arrived at the current machine, and how well the data is protected on the current machine all affect the integrity of the data. Thus, evaluating integrity is often very difficult, because it relies on assumptions about the source of the data and about bust in that source—two underpinnings of security that are often overlooked.

Data integrity techniques are used against unauthorized modification of messages. Specifically, the sender generates a code based on the message and transmits both the message and the code. The receiver then uses a verification algorithm that checks if the message has been altered in an unauthorized way during the transmission. The receiver can also verify that the message has indeed come from the claimed source.

Data integrity in secret-key cryptography is achieved using Message Authentication Codes (MACs). Given a key and a message, a MAC value is generated that protects the integrity of the message by allowing verifiers (who also possess the secret key) to detect any changes to the message content. MACs can also be used to provide authentication. In general, there are two types of MAC schemes. A HMAC (Hash-Based Message Authentication Code) is based on keyed hash functions and is characterized by its efficiency. HMAC-SHA-1 and HMAC-MD5 are used within the IPsec and SSL protocols, respectively. Another type of MAC is generated based on block ciphers, such as CBC-MAC and OMAC.

Unlike secret-key cryptography, a ciphertext generated by a public-key encryption, accompanied by its associated plaintext, can provide data integrity for the plaintext and authentication of its origin. The integrity code of a message can only be generated by the owner, while the verification of the integrity check can be done by anybody (both properties of a signature). Therefore, the integrity check in public-key cryptography is called a digital signature. These characteristics allow for the provision of non-repudiation. Non-repudiation means that the owner cannot deny a connection with the message and is a necessary requirement for services such as electronic commerce. Examples of signature schemes include the Digital Signature Standard (DSS) and RSA-PSS.

13.1.1.4. Availability

Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable. System designs usually assume a statistical model to analyze expected patterns of use, and mechanisms ensure availability when that statistical model holds. Someone may be able to manipulate use (or parameters that control use, such as network traffic) so that the assumptions of the statistical model are no longer valid. This means that the mechanisms for keeping the resource or data available would be working in an environment for which they were not designed. As a result, they can often fail. For example, suppose Mr. X has compromised a bank's secondary system server, which supplies bank account balances. When anyone else asks that server for information, Mr. X can supply any information he desires. Merchants validate checks by contacting the bank's primary

balance server. If a merchant gets no response, the secondary server will be asked to supply the data. Mr. X's colleague prevents merchants from contacting the primary balance server, so that all merchant queries go to the secondary server. Mr. X will never have a check turned down, regardless of his actual account balance. Notice that if the bank had only one server (the primary one), this scheme would not work. The merchant would be unable to validate the check.

Attempts to block availability, called DoS (Denial Of Service) attacks, can be the most difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment. Complicating this determination is the nature of statistical models. Even if the model accurately describes the environment, atypical events simply contribute to the nature of the statistics. A deliberate attempt to make a resource unavailable may simply look like, or be, an atypical event. In some environments, it may not even appear atypical.

13.1.1.5. Authentication

There are two classes of authentication: data origin authentication and entity authentication. Data origin authentication, also called message authentication, is the procedure whereby a message is transmitted from a purported transmitter (or origin) to a receiver who will validate the message upon reception. Specifically the receiver is concerned with establishing the identity of the message transmitter as well as the data integrity of the message subsequent to its transmission by the sender.

In entity authentication, which is concerned with validating a claimed identity of a transmitter, a "lively" correspondence is established between two parties, and a claimed identity of one of the parties is verified. Important properties of authentication include the establishment of message freshness, verifying whether data has been sent sufficiently recently, and user liveness: the lively correspondence of the communicating parties. The main techniques that handle user liveness include challenge-response mechanisms, time stamps, or freshness identifiers such as nonces. (A nonce is an arbitrary number used only once in a cryptographic communication. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.)

User authentication can be divided into three categories:

1. **Knowledge-based authenticators ("what you know")** — characterized by secrecy or obscurity, e.g., passwords, security questions such as mother's maiden name, and so forth.
2. **Object-based authenticators ("what you have")** — characterized by physical possession, e.g., security tokens, smart cards, and so forth.
3. **ID-based authenticators ("who you are")** — characterized by uniqueness to one person, e.g., a biometric such as a fingerprint or iris scan. Different types of authenticators can be combined to enhance security. This is called multi-factor authentication. For example, the combination of a bank card plus a password (two-factor authentication) provides better security than either factors alone.

13.1.2. Threats to Cyber Security

A threat is a potential violation of security. The three security services—confidentiality, integrity, and availability—counter threats to the security of a system. The violation need not actually occur for there to be a threat. The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks. Those who execute such actions, or cause them to be executed, are called attackers.

Threat is usually divided into four broad classes:

- Disclosure, or unauthorized access to information;
- Deception, or acceptance of false data;
- Disruption, or interruption or prevention of correct operation; and
- Usurpation, or unauthorized control of some part of a system.

Snooping, the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information. Wiretapping, or passive wiretapping, is a form of snooping in which a network is monitored. (It is called "wiretapping" because of the "wires" that compose the network, although the term is used even if no physical wiring is involved.) Confidentiality services counter this threat.

Modification or alteration, an unauthorized change of information, covers three classes of threats. The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released. If the modified data controls the operation of the system, the threats of disruption and usurpation arise. Unlike snooping, modification is active; it results from an entity changing information. Active wiretapping is a form of modification in which data moving across a network is altered; the term "active" distinguishes it from snooping ("passive" wiretapping). An example is the man-in-the-middle attack, in which a hacker reads messages from the sender and sends (possibly modified) versions to the recipient, in hopes that the recipient and sender will not realize the presence of the intermediary, integrity services counter this threat.

Masquerading or spoofing, an impersonation of one entity by another, is a form of both deception and usurpation. It lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. Similarly, if a user tries to read a file, but an attacker has arranged for the user to be given a different file, another spoof has taken place. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity). Although primarily deception, it is often used to usurp control of a system by an attacker impersonating an authorized manager or controller. Integrity services (called "authentication services" in this context) counter this threat.

Some forms of masquerading may be allowed. Delegation occurs when one entity authorizes a second entity to perform functions on its behalf. The distinctions between delegation and masquerading are important. If Mr. X delegates to Mr. Y the authority to act on his behalf, he is giving permission for him to perform specific actions as though he were performing them himself. All parties are aware of the delegation. Mr. Y will not pretend to be Mr. X; rather, he will say, "I am Mr. Y and I have authority to do this on Mr. X's behalf." If asked, Mr. X will verify this. On the other hand, in a masquerade, Mr. Y will pretend to be Mr. X. No other parties (including Mr. X) will be aware of the masquerade, and Mr. Y will say, "I am Mr. X." Should anyone discover that he is dealing with Mr. Y and ask Mr. X about it, he will deny that he authorized Mr. Y to act on his behalf. In terms of security, masquerading is a violation of security, whereas delegation is not.

Repudiation of origin, a false denial that an entity sent (or created) something, is a form of deception. For example, suppose a customer sends a letter to a vendor agreeing to pay a large amount of money for a product. The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unsolicited shipment without payment. The customer has repudiated the origin of the letter. If the vendor cannot prove that the letter came from the customer, the attack succeeds. A variant of this is denial by a user that he created specific information or entities such as files. Integrity mechanisms cope with this threat.

Denial of receipt, a false denial that an entity received some information or message, is a form of deception. Suppose a customer orders an expensive product, but the vendor demands payment before shipment. The customer pays, and the vendor ships the product. The customer then asks the vendor when he will receive the product. If the customer has already received the product, the question constitutes a denial of receipt attack. The vendor can defend against this attack only by proving that the customer did, despite his denials, receive the product. Integrity and availability mechanisms guard against these attacks.

Delay, a temporary inhibition of a service, is a form of usurpation, although it can play a supporting role in deception. Typically, delivery of a message or service requires some time t, if an attacker can force the delivery to take more than time t, the attacker has successfully delayed delivery. This requires manipulation of system control structures, such as network components or server components, and hence is a form of usurpation. If an entity is waiting for an authorization message that is delayed, it may query a secondary server for the authorization. Even though the attacker may be unable to masquerade as the primary server, he might be able to masquerade as that secondary server and supply incorrect information. Availability mechanisms can thwart this threat.

Denial of service, a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive. The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both).

Denial of service poses the same threat as an infinite delay. Availability mechanisms counter this threat Denial of service or delay may result from direct attacks or from non-security-related problems. From our point of view, the cause and result are important; the intention underlying them is not. If delay or denial of service compromises system security, or is part of a sequence of events leading to the compromise of a system, then we view it as an attempt to breach system security. But the attempt may not be deliberate; indeed, it may be the product of environmental characteristics rather than specific actions of an attacker.

13.1.3. Goals of Cyber Security

Given a security policy's specification of "secure" and "non-secure" actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack. The strategies may be used together or separately.

Prevention means that an attack will fail. For example, if one attempts to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented. Typically, prevention involves implementation of mechanisms that users cannot override and that are trusted to be implemented in a correct, unalterable way, so that the attacker cannot defeat the mechanism by changing it. Preventative mechanisms often are very cumbersome and interfere with system use to the point that they hinder normal use of the system. But some simple preventative mechanisms, such as passwords (which aim to prevent unauthorized users from accessing the system), have become widely accepted. Prevention mechanisms can prevent compromise of parts of the system; once in place, the resource protected by the mechanism need not be monitored for security problems, at least in theory.

Detection is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures. Detection mechanisms accept that an attack will occur; the goal is to determine that an attack is underway, or has occurred, and report it. The attack may be monitored, however, to provide data about its nature, severity, and results. Typical detection mechanisms monitor various aspects of the system, looking for actions or information indicating an attack. A good example of such a mechanism is one that gives a warning when a user enters an incorrect password three times. The login may continue, but an error message in a system log reports the unusually high number of mistyped passwords. Detection mechanisms do not prevent compromise of parts of the system, which is a serious drawback. The resource protected by the detection mechanism is continuously or periodically monitored for security problems.

Recovery has two forms. The first is to stop an attack and to assess and repair any damage caused by that attack. As an example, if the attacker deletes a file, one recovery mechanism would be to restore the file from backup tapes. In practice, recovery is far more complex, because the nature of each attack is unique. Thus, the type and extent of any damage can be difficult to characterize completely. Moreover, the attacker may return, so recovery involves identification and fixing of the vulnerabilities used by the attacker to enter the system. In some cases, retaliation (by attacking the attacker's system or taking legal steps to hold the attacker accountable) is part of recovery. In all these cases, the system's functioning is inhibited by the attack. By definition, recovery requires

resumption of correct operation. In a second form of recovery, the system continues to function correctly while an attack is underway. This type of recovery is quite difficult to implement because of the complexity of computer systems. It draws on techniques of fault tolerance as well as techniques of security and is typically used in safety-critical systems. It differs from the first form of recovery, because at no point does the system function incorrectly. However, the system may disable nonessential functionality. Of course, this type of recovery is often implemented in a weaker form whereby the system detects incorrect functioning automatically and then corrects (or attempts to correct) the error.

13.2. The Significance of Cyber Security

13.2.1. The Bearing of Cyber Security on National Security

Our society, economy, and critical infrastructures have become greatly dependent on computer networks and other information technology solutions. As our dependence on information technology increases, cyber attacks become more attractive options, and potentially more disastrous too. Cyber attacks are cheaper, more convenient, and less risky than physical attacks involving soldiers and conventional military hardware. If the perpetrator happens to be a nation state like the USA and Israel as in case of the Stuxnet attack, they have the excellent option of complete deniability. Above all, the cost of development is a fraction of what you spend in developing a major weapon system like a new missile, bomb, tank or aircraft. As a consequence, all political and military conflicts now have a cyber dimension, the size and impact of which are difficult to predict, and the battles fought in cyber space can be more important than events taking place on the ground. Remember that a cyber attack is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage, from denial of service to the destruction of critical infrastructure. The nature of a national security threat has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, scale, and power of an attack.

The use and abuse of computers, databases, and the networks that connect them to achieve military objectives was known in the early 1980s in the Soviet Union as the Military Technological Revolution (MTR). After the 1991 Gulf War, the Pentagon's Revolution in Military Affairs (RMA) became almost a household term. The Revolution in Military Affairs is intimately associated with modem information, communications, and space technology. Dozens of real world examples, from the US to Russia, from the Middle East to the Far East, prove that the ubiquity and vulnerability of the Internet have tangible political and military ramifications. As the Internet becomes more powerful and as our dependence upon it grows, cyber attacks may evolve from a corollary of real-world disputes to play a lead role in future conflicts.

Cyber security has quickly evolved from a technical discipline to a strategic concept. Globalization and the Internet have given individuals, organizations, and nations incredible new power, based on constantly developing networking technology. While information gathering, processing and communications have been digitized and revolutionized, almost everyone from students, soldiers, spies, propagandists, to hackers and terrorists is armed with the latest and best tools of computer technology. Computer technology is, in fact, a great leveler. Hitherto all

the instruments of national security were so terribly costly that only national governments could afford them. You could not imagine a situation where terrorists would have tanks or air forces. Their arsenal was limited to the AK-47 rifles they bought in illegal arms markets and the bombs they could make in their cellars. Computers have changed all that. Now a lone terrorist, operating from his single room apartment, can actually cause so much damage to a power plant which perhaps scores of them could not inflict, in spite of losing many lives and wasting several trucks laden with explosives. This is truly the intellectual's delight. Both big and small players have advantages unique to them. Nations robust in information technology exploit superior computing power and bandwidth; small countries and even lone hackers exploit the amplifying power of the Internet to attack a stronger conventional foe.

When one of the parties happens to be terrorists, we call it cyber terrorism. It has all the advantages of conventional terrorism and much more. The additional advantage comes from the fact that there is an aura of mystery surrounding those who indulge in cyber terrorism. Hackers, in any case, are known as creatures of the night. When they join terrorists, their mystery deepens. Almost everybody has a fear of the unknown. Hence there is great media hype about what hackers can do. Another great advantage of cyber terrorism is that there is little which can be done to punish the perpetrators. By the time you trace them, they could be thousands of miles away. Moreover, all you can do is damage control. The cyber terrorist presents no such target against which or against whom you could launch a retaliatory strike as the Americans did on Afghanistan following the 26/11 attacks. This is asymmetric warfare at its conceivable best.

The mindboggling achievements of cyber espionage serve to demonstrate the high return on investment to be found in computer hacking. Traditional forms of espionage, such as human intelligence, are dangerous and cost intensive. The start-up cost in case of cyber espionage is very low. Computer hacking yields free research and development data and access to sensitive communications vital for the important industries of any nation. The industries of a nation are not merely profit-making ventures for capitalists. Their trade secrets are vital for the development of that nation. If some automobile manufacturing company of a nation has developed the design of a compact, exceptionally fuel-efficient, less-polluting, powerful engine, it has great military potential as well. If the design secrets are leaked out to enemy countries, the nation will lose that edge.

13.2.2. How Modern, Complex Systems have become more Vulnerable?

It is a fact that large, complex infrastructures are easier to manage with computers and common operating systems, applications, and network protocols. But this convenience comes at a price. The situation is simple to understand. If you have an old-style plant where everything is done by mechanical or electromechanical systems, the plant may be less efficient but it is safe in the sense that it is insulated from outsiders. Outsiders could approach it only physically and to counter that you could provide perimeter security and access control, etc. But you cannot live with a less efficient plant. Hence you modernize it. Most systems of the plant become computer dependent, network dependent and Internet dependent. This means that even if the plant is physically isolated from the outside world, electronically it is connected to the whole world. Yes,

that means access to anybody with bad intentions. The new age hacker does not have to enter the plant physically. He will insert his malware electronically sitting thousands of miles away and they can do more sabotage than perhaps a team of terrorists put together. Remember, the moment you are 'connected' you become vulnerable to all who would try to intrude into your network. Hackers tend to be creative people, and they are able to exploit such complexity to Find ways to read, delete, and/or modify information without proper authorization.

Internet-dependent nations are a tempting target because they have more to lose when the network goes down. The more important a nation, the more of its vital systems and establishments would be dependent on computers and networks. Consider, banking for example. Till a few decades ago, all the details of your accounts were maintained in heavy ledgers. Now they are maintained on computers. If anything goes wrong with the central server, your account details will be in trouble. Of course, banks do maintain backup data but it will take a while before normalcy is restored and businesses would lose a great deal in that period. Moreover, with e-banking a great amount of banking transactions take place over networks like Internet. Anything wrong with the Internet and everything comes to a grinding halt. From railway and airline reservations and traffic control to management of electric power grids, everything is dependent upon sophisticated computers and networks. National security planners should consider that electricity has no substitute, and all other infrastructures, including computer networks, depend on it. You damage it anywhere and it will have a cascading effect Cyber forensic examination of captured hard drives proves that terrorists have studied computer hacking, and Western economies are a logical target. For example, tension in the Middle East is now always accompanied by cyber attacks. During the 2006 war between Israel and Gaza, pro-Palestinian hackers successfully denied service to around 700 Israeli Internet domains.

13.2.3. In Cyber War Advantage Lies with the Attacker

There is a simple handicap in effective cyber defense. You have a hell of a lot to protect. In this age, nations have millions upon millions of computers connected to the Internet. The attacker has to breach the defenses of only one of them. After that, the attack marches on by itself. Cyber attackers have a great advantage over conventional military leaders. There is practically no moral inhibition to computer hacking because there is no perceived human suffering in the target. There is no blood and gore associated with cyber attacks. Hence there is no guilt complex with anybody. Hackers, in fact, take great pride in what they do.

In cyber warfare the natural advantage lies with the attacker because he has more targets to strike and more ways to hit them— his options are limited only by his imagination and skills. Further, an attacker's most important advantage remains anonymity and the great difficulty in locating him. They can route attacks through countries with which a victim's government has poor diplomatic relations or no law enforcement cooperation so as to throw the needle of suspicion towards them while they relax over a martini somewhere far away.

Cyber defense suffers from the basic disadvantage that you have millions of targets to protect. Consequently, at the technical level, it can be difficult even knowing whether one is under cyber

attack. All things considered, the current balance of cyber power favors the attacker. This stands in contrast to our historical understanding of warfare, in which the defender has had traditionally enjoyed advantage—it takes three times as many forces to attack than to defend. Therefore, many governments may conclude that, for the foreseeable future, the best cyber defense is a good cyber offense. They are also a powerful and often deniable way to project national power. Moreover, the attacks can be launched even without the presence of a modicum of overt tension between two nations.

In cyber conflict, the terrestrial distances between adversaries become irrelevant because everyone is a next-door neighbor in the cyber space. Hardware, software, and bandwidth form the landscape in cyber warfare—not mountains, fields, valleys, jungles or waterways. The most powerful weapons in cyber warfare are not based on strength, but logic and innovation. Basically, tactical victories amount to a successful reshuffling of the bits—the 1s and 0s—inside a computer. Nothing more than that! That's why it stands to reason that cyber warfare will find favorites with nations other than superpowers also—whoever has got the brains, has got the weapons even if their citizens might be starving.

When it comes to non-state actors, there is little which can be done to combat cyber warfare through legal means. Proving the origin of a cyber attack conclusively, in the first place, is very difficult. Law enforcement and counterintelligence investigations suffer from the fact that the Internet is an international entity, and jurisdiction ends every time a telecommunications cable crosses a border.

13.2.4. Cyber Threats to a Nation's Critical Infrastructure

On April 26, 2007, the Estonian government moved a Soviet World War II memorial from the center of its capital to a military cemetery. The move inflamed public opinion both in Russia and among Estonia's Russian minority population. Beginning on April 27, Estonian government, law enforcement, banking, media, and Internet infrastructure endured three weeks of cyber attacks, whose impact still generates immense interest from governments around the world. Estonians conduct over 98% of their banking via electronic means. Therefore, the impact of multiple Distributed Denial-of-Service (DDoS) attacks, which severed all communications to the Web presence of the country's two largest banks for up to two hours and rendered international services partially unavailable for days at a time, was severe. Less widely discussed, but likely of greater consequence— both to national security planners and to computer network defense personnel—were the Internet infrastructure (router) attacks on one of the Estonian government's ISPs, which disrupted government communications for some time. We shall learn about DDoS attacks a little later in the book.

In 2008, the Russo-Georgian war demonstrated that there will be a close relationship between cyber and conventional operations in all future military campaigns.

- Consider These Relatively Recent Incidents
- In June 2003, the US government issued a warning concerning a virus that specifically targeted financial institutions. Experts said the BugBear.b virus was programmed to determine whether

a victim had used an email address for any of the roughly 1,300 financial institutions listed in the virus's code. If a match was found, the software attempted to collect and document user input by logging keystrokes and then provide this information to a hacker, who could use it in attempts to break into the banks' networks.

- In August 2006, two Los Angeles city employees hacked into computers controlling the city's traffic lights and disrupted signal lights at four intersections, causing substantial backups and delays. The attacks were launched prior to an anticipated labor protest b$ the employees.
- In October 2006, a foreign hacker penetrated security at a water filtering plant in Harrisburg, Pennsylvania. The hacker planted malicious software that was capable of affecting the plant's water treatment operations.
- In September 2007, the Israeli military launched a cyber attack against Syrian air defense prior to its destruction of its alleged nuclear reactor in the Deir ez-Zor region. The attack was called Operation Orchard. A team of elite Israeli Shaldag Special Forces commandos had arrived at the site the day before so that they could highlight the target with laser beams. As many as eight aircrafts had participated in the attack and hence protection from Syrian air defenses was necessary.
- In 2009, during a time of domestic political crisis, hackers knocked the entire nation-state of Kyrgyzstan offline;
- In 2010, as we have already discussed, how the Stuxnet worm attacked the Iranian uranium enrichment centrifuges.

Such incidents should not be dismissed as pranks of computer nerds or psychopathic hackers. Thus is serious stuff. A modem nation's critical infrastructure operates in an environment of increasing and dynamic threats, and adversaries are becoming more agile and sophisticated. Terrorists, transnational criminals, and intelligence services can use various cyber tools that can deny access, degrade the integrity of, intercept, or destroy data and jeopardize the security of the nation's critical infrastructure.

All of the critical infrastructures (energy, telecommunications, transportation, banking and finance, continuity of government services, water supply systems, gas and oil production, and emergency services) are dependent on the computer communication infrastructures. Moreover, the computer information infrastructures are themselves dependent on many of the critical infrastructures, such as electric power grid and telecommunications systems. A successful cyber attack on the supervisory control and data acquisition (SCADA) and other control systems for the critical infrastructures could have a significant impact on public health, economic losses, and potential loss of lives. Securing control systems in critical infrastructures is thus a national priority. Therefore there is increasing concern among both government officials and industry experts regarding the potential for a cyber attack on the national critical infrastructure, including the infrastructure's control systems.

In January 2003, computers infected with the Slammer worm (SQL Server worm) shut down safety display systems at the Davis-Besse power plant in Oak Harbor, Ohio. A few months later,

another computer virus-was widely suspected by security researchers of leading to a power loss at a plant providing electricity to parts of New York State. A third incident was the power outage of August 2003 in the Midwest and Northeast of the United States, and Canada. Even though the incident was not an act of terrorism, it demonstrates the vulnerability of the electric power grid. In fact, some of the documents gathered from Al Qaida in 2002, suggested that they were considering a cyber attack on the power grid.

In May 2009, President Obama made a dramatic announcement: "Cyber hackers have probed our electrical grid ... in other countries, cyber attacks have plunged entire cities into darkness." Investigative journalists subsequently concluded that these attacks took place in Brazil, affecting millions of civilians in 2005 and 2007, and that the source of the attacks is still unknown. Security studies from the US Department of Energy (DOE) and commercial security consultants have demonstrated the cyber vulnerabilities of control systems. In one of the most recent demonstrations of the vulnerability of the critical infrastructure, a security researcher was able to break into a nuclear power station and within a week take over the control plant. Back in 2000, a 48-year-old Australian man, who was fired from his job at a sewage-treatment plant, remotely accessed his workplace computers and poured toxic sludge into parks and rivers.

The Department of Defense (DOD) and the Federal Bureau of Investigation (FBI), among others, have identified multiple sources of threats to the USA's critical infrastructure, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. According to media reports, technology has been shipped to the United States from foreign countries with viruses on the storage devices. Further, US authorities are concerned about the prospect of combined physical and cyber attacks, which could have devastating consequences. For example, a cyber attack could disable a security system in order to facilitate a physical attack. All things considered, cyber attacks have profound strategic consequences; therefore, they must be taken seriously by national security leadership.

Military leaders must expect to receive Denial of Service (DoS) attacks against their network infrastructure the moment hostilities start building up. As early as the 1999 Kosovo war, unknown hackers attempted to disrupt NATO military operations via the Internet and claimed minor victories. In future conflicts, DoS attacks may encompass common network "flooding" techniques, the physical destruction of computer hardware, the use of electromagnetic interference, and more. The most frightening scenario, however, is "unrestricted cyber war". Here, an adversary would try to cause maximum damage to civilian infrastructure in order to rupture the social fabric of a nation. Air-traffic control, stock exchange, emergency services, and power generation systems could be targets. The goal would be as much physical damage and as many civilian casualties as possible.

In 2001, James Adams revealed in the pages of Foreign Affairs that the US Department of Defense had in fact put cyber war theories to a real-world test in a classified 1997 Red Team exercise codenamed "Eligible Receiver". Thirty-five US National Security Agency (NSA) personnel, simulating North Korean hackers, used a variety of cyber and information warfare (IW) tools and tactics, including the transmission of fabricated military orders and news reports, to attack the

U.S. Navy's Pacific Command from cyberspace. The Red Team was so successful that the Navy's "human command-and-control system" was paralyzed by mistrust, and "nobody... from the president on down, could believe anything."

More than one-and-a-half decade later, it stands to reason, and it has been amply indicated by sophisticated attacks like the Stuxnet, Duqu and Flame (that we have discussed later) also that many militaries have indeed crossed that threshold. A 2009 report on the cyber warfare capabilities of the People's Republic of China (PRC) described a highly-networked force that can now communicate with ease across military services and through chains of command. Furthermore, each military unit has a clear, offensive cyber mission in times of both war and peace. In peacetime, strategic intelligence is gathered via cyber espionage to help win future wars. In war, a broad array of computer network operations (CNO), electronic warfare (EW), and kinetic strikes would be used to achieve information superiority over an adversary, especially during the early or preemptive-strike phases of a conflict.

13.2.5. Multiple Routes of Mounting Cyber Attacks

Hackers used to break into networks for the thrill of the challenge or for bragging rights in the hacker community. Now state-sponsored hackers have acquired the capability of disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of a nation's citizens across the country.

An important player is cyber warfare is a disgruntled insider or a traitor. Insiders do not require a great deal of knowledge about computer intrusions themselves. However, their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization as well as employees who accidentally introduce malware into systems. He is the cyber-age equivalent of a 'mole' that spies and intelligence agencies used to plant earlier in foreign countries.

While criminal groups, International corporate spies and organized crime organizations seek to attack systems for monetary gain, foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" computer under control of the worm author. A zombie, in folklore, is an animated corpse resurrected by mystical means, such as witchcraft. The term is often figuratively applied to describe a hypnotized person bereft of consciousness and self-awareness, yet ambulant and able to respond to surrounding stimuli. A similar thing happens in this type of cyber attack also. What happens is that a cracker—a computer hacker who intends mischief or harm—secretly infiltrates an unsuspecting victim's computer and uses it to conduct illegal activities. The user's computer is called a zombie computer because he generally remains unaware that his computer has been taken over by somebody else—he can still use it, though it might slow down considerably. Networks of such machines are often referred to as botnets. Botnets are small peer-to-peer groups, rather than a larger, more easily identified network. A botnet is simply a collection of internet-connected computers whose security defenses have been breached and control ceded to a malicious party. Each such compromised device, known

as a "bot", is created when a computer is penetrated by software from a malware distribution. Botnet operators take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The Storm botnet, for example, comprising over 50 million computes, for example, is highly resilient to efforts to take it down. Its command and control architecture is based on a peer-to-peer (P2P) network, with several redundant hosts spread among 384 providers in more than 50 countries.

By the second decade of the new millennium, the notion that every user working with the Web is under attack every minute turned from an apocalyptic scare to somber reality. Let's look at the facts: The number of unique malware signatures detected yearly has soared north of 10 million; the power of botnets has exceeded the might of the planet's best supercomputers by a couple orders of magnitude; and headlines about multimillion-dollar cyber-heists committed by online criminals constantly lurk in the news.

An increasingly prominent form of targeted attack seeks to extract scientific, corporate and government secrets from unsuspecting victims. Known in industry parlance as the Advanced Persistent Threat, or APT, this highly tailored attack usually arrives via email and includes a message that references current events or a matter directly relevant to the recipient. The message usually is spoofed so that it appears to have been sent by somebody who is indeed authorized or expected to send such a mail. You can learn more about this in our companion volume 'Cyber Crimes: Preventive Measures And Cyber Forensics'. Towards the end of July 2011, about a hundred energy industry executives in the USA received an email about an upcoming golf tournament in which they were scheduled to play in Huntsville, Ala., fit October. The message encouraged each recipient to fill out an attached form and name his or her team members and captains. The attached PDF was identical to the form that is still on the golf tournament's website, but in reality it contained some hidden extras: a pair of Adobe Reader exploits that would install a tiny Trojan horse program if recipients weren't using the latest, most secure version of Reader. The Trojan opened a backdoor on the infected PC and exfiltrated documents, spreadsheets and other files to a server controlled by the attackers. When investigators traced the attack back to the compromised server, they found it had relayed its cache of stolen documents onto servers in China, the country most frequently fingered as the source of APT attacks.

In August 2011, the famous anti-virus software company McAfee released details about a five-year Advanced Persistent Threat campaign it called Operation Shady RAT (Remote Access Tool). McAfee revealed that this was a targeted operation by a specific actor which had infiltrated computer systems of national governments and global corporations, spanning 70 victims in 14 countries. The actor is widely believed to be China.

Then there are sophisticated and targeted attacks from malware families that steal financial data, such as ZeuS and TDSS. Widely considered to be the work of Russian malware gangs motivated by profit, modem versions of ZeuS (such as JabberZeuS) and its cousin, SpyEye, are especially dangerous because they are designed be used with special-purpose plug-ins that allow hackers to target customers of specific financial institutions.

We also have "hacktivist" groups like Anonymous and splinter groups such as Lulzsec and Antisec whose activities and their intended targets are unpredictable. Anonymous has existed in various forms for several years, but the group gained international notoriety in late 2010, when it coordinated a distributed denial-of-service attack against Visa, PayPal and other companies.

13.2.6. Awareness and Cyber Defense Preparations

On June 27, 2011, The Homeland Security Department in the USA unveiled a new system of guidance intended to help make the software behind websites, power grids and other services less susceptible to hacking. The system includes an updated list of the top 25 programming errors that enable today's most serious hacks to take control of the websites. The first on the list is a programming mistake that allows so-called SQL-injection (Structured Query Language fir maintaining database management systems) attacks on websites, which were successfully used by the hacker group LulzSec. That group was able to use the flaws to cause databases to spit out user names and passwords from websites, including one associated with the FBI's InfraGard program and NATO's online bookstore. InfraGard, incidentally is a FBI program is an effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. InfraGard can be thought of as a partnership between the FBI and the private sector—this alone shows how seriously the cyber threat has been taken there. And if such a program itself could be subjected to attack, you must sit up and wonder what the cyber attackers are capable of doing.

Cyber Analysis and Warning Typically Encompasses Four Key Capabilities:

- **Monitoring**—that is, detecting cyber threats, attacks, and vulnerabilities and establishing a baseline of system and communication network assets and normal traffic.
- **Analysis**—that is, using the information or intelligence gathered from monitoring to hypothesize about what the threat might be, investigate it with technical and contextual expertise and identify the threat and its impact, and determine possible mitigation steps. Analysis may be initiated in reaction to a detected anomaly. This is a tactical approach intended to triage information during a cyber incident and help make decisions. It may also be predictive, proactively reviewing data collected during monitoring to look at cyber events and the network environment to find trends, patterns, or anomaly correlations that indicate more serious attacks or future threats.
- **Warning**—that is, developing and issuing informal and formal notifications that alert recipients in advance of potential or imminent, as well as ongoing, cyber threats or attacks. Warnings are intended to alert entities to the presence of cyber attack, help delineate the relevance and immediacy of cyber attacks, provide information on how to remediate vulnerabilities and mitigate incidents, or make overall statements about the health and welfare of the Internet.
- **Response**—that is, taking actions to contain an incident, manage the protection of network operations, and recover from damages when vulnerabilities are revealed or when cyber incidents occur. In addition, response includes lessons learned and cyber threat data being

documented and integrated back into the capabilities to improve overall cyber analysis and warning.

13.3. Major Cyber Security Risks for the Common Man

13.3.1. Why You Need to Know Them?

The first step in mounting a good cyber defense is to know what's coming at you. Hackers and cyber criminals are constantly coming up with new ways to attack your PC and your privacy. Accordingly, we have compiled a list of ten serious security problems that you need to be aware of. It may so happen that even as you read this book, your computer could get hit by a new variant of a familiar foe, like a Trojan Horse, or a completely new type of attack, but something that could be too new for your anti-virus program to catch. There are ways we can minimize our risk, however. To protect yourself, you should, of course, know how to keep your PC patched and your anti-malware tools current. In addition, we will provide tips to help you avoid these new dangers, and to contain the damage if you do get hit. Here are the newest perils—and how to foil them.

13.3.2. Attack of the Zombie PC Armies

Many people have made a business out of building and selling self-contained bot development kits that let potential herders (as individuals who run a botnet are called) direct their own scam. The kits, costing anywhere from $20 to $3000, permit aspiring criminals to create full-featured botnets and other malicious software, ranging from customizable worms to keyloggers—no techie chops required.

Clever Web Controls: After building a new bot and sending it out to unsuspecting computer users, the wannabe hacker can use sophisticated command-and-control tools to direct the resulting network easily. Experts have found a new web-based botnet control they've dubbed Metaphisher. Instead of issuing text commands, herders can use the control's highly graphical user interface, complete with well designed custom icons and intuitive controls. According to iDefense Labs, Metaphisher-controlled bots have infected more than a million PCs worldwide. The command suite even encrypts communications between itself and the bot herder, and relays information about virtually every aspect of infected PCs to the botmaster—including their geographic location, the Windows security patches installed, and the browsers other than Internet Explorer loaded on each PC. All these easy-to-use kits and controls undoubtedly contribute to the huge numbers of bot-infected PCs that cyber crime investigators have uncovered during many criminal investigations. Many such bot herders have been arrested who were controlling as many as 1.5 million zombie PCs each!

How it Works: Quick Bot Deployment with Simple Tools

1. A would-be criminal buys a bot-building kit online for a small fee.
2. With no programming skills, the criminal uses his kit to build a new bot not yet known to anti-virus makers.
3. The criminal sends his new bot out as an email attachment or plants it on malicious websites.
4. The resultant botnet rakes in cash with spam, spyware, and denial-of-service attacks.

Your Defenses

1. Avoid unknown sites and don't click links in unsolicited email. Like most malware, bots tend to be distributed in these ways.
2. Remain suspicious of email attachments, even when a message seems to come from somebody you know. Crooks love to use genuine email addresses in "spoofed" virus-laden email missives.
3. Consider an alternate browser such as Mozilla Firefox or Opera. IE has been a favorite hacker target.

13.3.3. Stealing Your Data and Making it available free on the Net

It's bad enough when one crook uses a keylogger to steal your bank log-in and passwords. It's much worse to have all of your sensitive information sitting in an unprotected FTP (File Transfer Protocol) site, open to anyone who happens across it. File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host or to another host over a TCP-based (Transmission Control Protocol) network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.

Unfortunately, that is exactly what security researchers have started seeing over the past year. The anti-spyware firm Sunbelt Software found one such FTP server while investigating a keylogger that wasn't even particularly widespread. The server, based in Washington, D.C., was packed with nearly a gigabyte of stolen credentials. Not only do keyloggers capture anything you type, they can take screen shots of your PC's display, and they can glean data from the Windows Protected Storage area, which is the place where Internet Explorer stores its saved passwords, One of the log files on the FTP server held pilfered passwords for a number of US banks and for Buy.com, along with Yahoo, Hotmail, and other email account user names and passwords, plus account details for online casinos and a host of other sites. The danger is international: The log records were in myriad languages—German, Spanish, Hungarian, Turkish, and Japanese, among others—and it held IP addresses that pointed to infected computers scattered around the world.

Your Defenses

Use a firewall that can block unknown programs from communicating with the Net to keep keyloggers from phoning home. The free ZoneAlarm firewall can do this; the built-in Windows XP firewall can't.

Cycle passwords, and don't use the same name and password at multiple sites. For more password tips, please read the companion volume 'Cyber Crimes : Preventive Measures and Cyber Forensics'.

13.3.4. Taking Over of Legitimate Sites by Phishers

Phishing is one of the most lucrative computer crimes, and it continues to grow rapidly. You can learn more about phishing in our companion volume 'Cyber Crimes: Preventive Measures

And Cyber Forensics'. Phishers make their fake sites look exactly like the original sites. Modern scammers operate sophisticated server-side software that pulls all of the text, graphics, and links directly from the target bank's live site. All of the queries you input go to the real site—except your log-in data. That choice information goes straight to the bad guys. Some phishing sites have become so smooth that they can even trap cautious and experienced Web surfers. In their "Why Phishing Works" study, experts at University of California at Berkeley and Harvard presented test subjects with websites and had them look for the fakes. As it turned out, "even in the best-case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website," the report states. The best phishing site was able to fool more than 90 percent of participants.

Browser Redirects Below The Radar: The key for the phisher is to inveigle you into visiting the bogus site. You may be well conditioned not to trust an email missive purporting to be from your bank and asking you to click a link to check your account details. But phishers today are adopting more forceful means to push your browser to their sites. A malware-enabled technique called smart redirection secretly sends your browser to the scammer's website even if you manually type your bank's correct Web address (URL) into the browser, Malware on your machine monitors the availability of dozens or hundreds of duplicate fake bank sites, hosted on computers around the world, and redirects your browser to an available fake site whenever you attempt to reach your bank. And if authorities subsequently close down one site, the smart redirection software on an infected system simply sends the victim to a destination site that has eluded shutdown.

How It Works: Clever Lures Set Out to Catch the Wary:

1. A well-informed, careful user manually types a bank URL into the browser address bar.
2. Malware on the computer redirects the user to a live phishing site.
3. By pulling text and images from the live bank site in real time, the phishing site looks just like the actual thing.
4. The sophisticated phisher fools even the careful user, who types in his bank account log-in.

Your Defenses

1. Don't trust an unsolicited email message from any company, no matter how good it looks. The best phishing sites and scam email messages lack obvious flaws.
2. Type in your bank's URL yourself or use a bookmark; avoid clicking an email link.
3. Look for a padlock icon, which indicates a secure site, in the browser's toolbar, not the webpage.
4. Use one of the many available anti-phishing toolbars that can warn you when you encounter a known phishing site. Netcraft offers one popular free toolbar; Tom Spring looks at others in his Spam Slayer column "Fight Fraud and Phishing With New Tools."

13.3.5. The Human Security Hole

You can update Windows and each of your applications, and you can use security software to protect your PC, but one constantly exploited weakness can never be patched: human fallibility.

Cyber criminals use an ever-changing array of tricks and traps to lure you in, and they're getting sneakier. A recent eBay auction trap highlights the effectiveness of good social engineering. According to reports from US-CERT (US Computer Emergency Readiness Team) and Internet security companies, clever phishers were using a vulnerability in the eBay site to add auction links to eBay's pages. Those links brought unsuspecting users to a new site that would ask them for their eBay logins. You're no doubt suspicious of random email messages that prompt you to click a link and enter your account information. But if you are prompted after clicking a link on a verifiable eBay page, you just might get caught with your guard down.

Your email gets equal attention. Clever crooks steal or buy email addresses, not to pelt you with spam, but to send out virus-laden messages that appear to originate from a genuine address—without ever infecting the supposed sender. Combined with a list of known email addresses at a particular company, these spoofed email messages allow for carefully crafted and targeted attacks that are far more successful than the net-cast-wide approach used to distribute most malware today.

Spoofed email addresses are also useful in conjunction with such attacks as the recent one that took advantage of a new, zero-day exploit in Microsoft Word. To get hit, all you'd have to do is open a .doc attachment—and why wouldn't you open an email from Mr. C down the hall? Criminals know that if they can fool you with an email or top-notch phishing site, they're well on their way to owning your computer. But there's a positive flip side: A well-informed user constitutes the best defense against any Internet attack. Stay educated, and stay safe.

Your Defenses

1. Subscribe to security-focused RSS feeds to keep abreast of the latest Internet threats. RSS Rich Site Summary (originally RDF Site Summary, often dubbed Really Simple Syndication) is a family of Web feed formats used to publish frequently updated works—such as blog entries, news headlines, audio, and video—in a standardized format. An RSS document (which is called a "feed", "web feed", or "channel") includes full or summarized text, plus metadata such as publishing dates and authorship. We recommend the feeds at F-Secure, Kaspersky, and Sophos.

2. Obtain a wealth of security advice, product reviews, and tips at PCWorld.com's Spyware & Security Info Center.

13.3.6. Redirecting of your Browser to Scam Websites

Odds are, you use Domain Name System (DNS) servers every day. They translate human-friendly names like "www.pcworld.com"into the numerical IP addresses that computers use to find each other on the Internet. Your ISP (Internet Service Provider) has its own DNS server, as do most companies. The Internet can't get by without them. But more than a million DNS servers around the world—up to 75 percent of all servers, according to networking firm - The Measurement Factory—run old or mis-configured DNS software. Such systems are subject to a wide enough range of serious attacks. SANS Institute, a computer security research and education organization, lists DNS software as one of the top 20 vulnerabilities of the Internet. For example, it was widely reported that cyber criminals used mis-configured DNS servers in lethal denial-of-service attacks

that forced anti-spam firm Blue Security to shut its doors permanently. You can learn more about domain name system in our companion volume 'Cyber Crimes: Preventive Measures And Cyber Forensics'.

Such attacks work in several ways. One tactic is "cache poisoning," where an offender can simultaneously target everyone who uses the DNS server. A successful attack tricks a company's or ISP's server into sending everyone who uses it to a phishing or other malicious site. You might type 'www.americanexpress.com' or 'www.yahoo.com', but you will end up at a website that installs an arsenal of malware on your computer. Another lethal ploy: When bad guys send spoofed requests to DNS servers that are recursive, the servers respond by sending answer messages to the intended victim. The responses contain more data than the original requests, which thus magnifies the attack beyond what the crooks could send themselves. The hapless victim is completely overwhelmed by garbage data and can't respond to genuine requests from regular users.

Your Defense

It is admittedly difficult to cope with for an individual. If you are in a company, ask your company's IT group to make sure your DNS server is not recursive and its software is up-to-date.

13.3.7. When Rootkits and Viruses Team Up

Rootkits are a malware inventor's dream : they allow worms, bots, and other malevolent software to hide in plain sight. The files don't show up in Windows Explorer, the running processes don't display in the Task Manager, and many current anti-virus programs can't find rootkit-hidden malware—which is precisely why malware writers increasingly use them to hide malicious apps. Now it is possible to build rootkit functionality directly into long-standing malware like the Bagle worm also.

The security firm eEye has discovered that it is possible to hide files in the boot sector of the hard drive. John Heasman, security consultant for Next-Generation Security Software, has found that rootkits could hide malicious code within a PC's BIOS (Basic Input/ Output System) by using functions in the BIOS's Advanced Configuration and Power Interface feature. A project run by Microsoft and University of Michigan researchers really blew the lid off rootkit research, devising a method to virtually "jack up" the operating system and then use software called SubVirt to run it from below. As far as the operating system knew, it was running normally, but the "virtual machine" completely controlled everything the OS (Operating System) saw and could easily hide itself.

High-Stakes Hide-And-Seek: Merely finding today's dangerous rootkits is a serious challenge for security software. Detecting a rootkit on a Windows PC is not unlike shining a flashlight at objects in a darkened room, and then trying to identify each object by the shadow it casts on the wall. Specialized software, such as F-Secure's BlackLight and Sysinternals' RootkitRevealer, scans the Windows file system and memory for characteristic irregularities that rootkits leave behind. But those tools may not work in every case. Recently, the adware program Look2Me effectively broke BlackLight by disabling a key system call. The discovery was accidental, but rootkit makers will undoubtedly pay attention to it in their next round of malware.

How Cloaked Malware Manages to Hide on Your PC

1. A Trojan Horse with rootkit software invades a PC as a drive-by download.
2. The malware makes deep system changes to hide from antivirus apps.
3. The camouflaged Trojan Horse pulls keyloggers and spyware onto your PC.

Your Defenses

Look for anti-virus software that provides rootkit scanning and removal. Kaspersky's and F-Secure's latest applications have it now; others will likely add it soon.

Use a rootkit detector such as Sysintemals' RootkitRevealer and F-Secure's Blacklight, both free downloads. Other scanners are also becoming available; you may read Privacy Watch for more information.

Viruses in Cell Phones and What They Can Do?

As if viruses on your PC weren't bad enough, these nasty programs can now target your cell phone as well. Following the discovery of Cabir.A in June 2004, the number of viruses has continued to climb. Like their computer-based cousins, mobile viruses can wreak havoc by crashing the phone and wrecking its operating system There is a great range in what they can do. Some of them are mere nuisances that change icons and make the device more difficult to use; some are strictly money-minded. A Trojan Horse currently infecting Russian phones sends text messages to services that charge the sender a fee. While these pests are not a major problem in the United States, they are significant threats in Europe and Asia. Bluetooth is the most common—but not the only—vector of infection. The Mabir virus, for example, spreads via SMS messages. The vast majority of mobile viruses hit phones using the Symbian operating system, but a few go after Windows Mobile- and Java-based phones also.

Your Defenses

1. Disable "open" Bluetooth on your phone or PDA to close down the most common infection route.
2. Keep a close eye on the itemized part of your cell phone bill for unexpected charges.
3. Use a mobile antivirus program. F-Secure, Kaspersky, McAfee, and Trend Micro all offer them

13.3.8. Malware on Your Passport?

Could your passport, a pack of razor blades, or even your pet cat carry a computer virus? It may seem far-fetched, but recent findings from a trio of Dutch researchers serve to demonstrate the possibility. RFID (Radio-Frequency Identification) chips are small, inexpensive devices that can be embedded in stickers and in pet ID tags, and soon they'll show up in driver's licenses and US passports also. They're used for electronically transmitting information—say, inventory data for shipping pallets, or your passport number—over-short distances. Though highly useful, some implementations of the RFID technology have security weaknesses. For example, the information on some tags can be rewritten} and other tags can be read from an unusually great distance.

In an attempt to exploit some of these weaknesses, the Dutch university researchers conducted a controversial proof-of-concept study using modified RFID tags and a virus-like command to "infect" the back-end database that stored the tag's records. Theoretically, an RFID system could thus be made to crash or run malicious code— a scary prospect for a critical business or government technology. Numerous computer security experts have pointed out that a reasonably well-built system with effective "middleware" between the RFID reader and the database probably wouldn't be vulnerable to such an assault. And sensitive RFID chips can use encryption and shielding covers to protect against acquiring an unasked-for malicious payload. The planned U.S. passports will use both measures. Still, the study illustrates a basic point: nearly every system has exploitable flaws.

Your Defense

RFID signals can't pass through metal or foil-lined cases. If you carry an RFID security pass, keep it in a metal business-card holder or similar enclosure.

13.3.9. Ransom Ware

It sounds like a plot concocted by Austin Powers' nemesis, Dr. Evil: Get onto your victims' computers, kidnap their files, and hold the data hostage until they pay up. But such attacks, though rare, have occurred all over the world. Cryzip, one early example of ransomware, searches for 44 different file types (such as Microsoft Word or Excel files) on a hard drive, and compresses them into a password-protected zip file. It then tells the victim to deposit $300 in one of 99 randomly selected e-gold accounts. Once paid off, the criminals provide the victim with the necessary password.

Sometime later, another ransomware application, named Arhiveus came to light. Rather than of directing payment to a potentially traceable e-gold account, it instructed victims to buy prescription drugs from a specific online pharmacy and then send the order ID to the malware author as proof of payment. "It looks like a Russian-based pharmacy that they're hosting in China," says Lurhq's Joe Stewart. "Appended to the URL is what looks like an affiliate ID— they probably get a cut". In his examination of both Cryzip and Arhiveus, Stewart found the necessary passwords to "free" the data embedded within the malware code itself, unencrypted.

How Ransomware Works?

1. An unsuspecting user accidentally visits a rigged website, and the ransomware Trojan Horse slithers into the PC.
2. The ransomware zips up the entire contents of the My Documents folder into a password-protected file.
3. The user gets a ransom note demanding money, or a purchase at a particular online store, in return for the password.

Your Defenses

If you're a victim, go to the police. Don't pay the ransom, and don't visit any links in the ransom note.

Write down the details from any ransom notes or messages, and turn off the infected PC. From an uninfected PC, run a Web search using details from the ransom note. You may be able to find the password online.

Try using an undelete program to recover your files. However, remember that some files may not be recoverable at all.

13.3.10. They Can Attack all Operating Systems

Window's popularity meant that it had to be the prime target of attacks. Mac and Linux users have been understandably complacent as Windows users suffer a seemingly endless series of attacks that exploit hole after hole in Microsoft's operating system. Windows' ubiquitous nature means that malware targeting its many security holes has the greatest chance to infect the most PCs. But as alternative operating systems grow in popularity, they become more attractive targets, too. But these alternative OSes—once considered safe computing havens—won't remain so for long. The Mac is under attack as hackers aim at the 70-odd reported security holes in OS X. One of these vulnerabilities was exploited by the first piece of malware to hit OS X Tiger: the so-called Oompa-loompa instant-messaging worm. And while Internet Explorer users are probably well accustomed to hearing reports of new browser bugs that could allow "remote code execution" (read: giving an attacker control of your PC), Mac users now need to beware as well—the most recent of Apple's three major security patches this year closed one such hole in the Safari browser.

Linux has a case of worms, too; the number of malicious programs targeting that OS has increased greatly. Rootkits, the looming threat for Windows PCs, actually trace back to attacks meant to take surreptitious control of the administrative "root" user on Unix OSes. Also, while being able to run your own personal Web server is part of the open-source draw, doing so can allow crooks to hijack your site or take control of your PC.

The latest twist is cross-platform malware: single programs that can assault two or more types of systems. A proof-of-concept virus that attacks both Windows and Linux appeared some time back. The virus, created by antivirus firm Kaspersky, contains no payload and does no damage. Known variously as Virus.Linux.Bi.a and also Virus.Win32.Bi.a, it infects just a single type of Linux file format (ELF) and a single type of Windows file format (PE). And it's based on old Linux elements that aren't part of newer systems. Still, it was enough of a wake-up call to prompt Linux creator Linus Torvalds to write a fix.

Your Defense

1. Consider using a Mac or Linux antivirus program, such as Panda Antivirus for Linux and Mac products from vendors such as McAfee and Symantec. If nothing else, you'll be a good neighbor and help stem the flow of Windows viruses.
2. Whatever your OS, keep it fully up-to-date and patched.

अध्याय 14
Chapter 14

Biometric Controls for Security and Issues and Challenges in Biometric-Based Security

14.1. Introduction

Biometrics is the science for determining a person's identity (ID) by measuring his/her physiological characteristics. Authentication is a fundamental concept in security, especially with respect to human-computer interaction. In this chapter, biometrics methods are discussed. We start with the basics of biometrics to understand what it is, its place in user authentication for physical access control and various technologies and techniques used in biometrics. Issues and challenges in implementing a biometrics system will be discussed in this chapter.

Biometrics has got interesting origin in the Chinese civilization. The earliest known use of biometrics dates back to the seventh century during Chinas Tang Dynasty. During this period fingerprints were used to sign and validate contracts. Over the last century, biometrics has grown enormously. Technologies are being developed to verify or identify individuals on the basis of measurements of the face, hand geometry, iris, retina, finger, ear, voice, speech, signature, lip motion, skin reflectance, deoxyribonucleic acid (DNA).

Biometrics techniques of today have been made possible by the advances in computing technology and the need that arises owing to universal presence and connectivity of computers all over the world. Biometrics identification is a much more sophisticated method of controlling access to computing facilities than badge readers. However, the two methods operate in the same way. Biometrics techniques used for user identification typically include fingerprint recognition, palm recognition, handprint recognition, voice pattern recognition, signature samples, retinal scans and iris scans.

Biometrics provides a higher level of security than badges because it cannot be lost, stolen or shared. Thus, biometrics can provide a greater degree of security than traditional authentication methods; however, these methods are expensive as well as complex to deploy. Given this, as of now, biometrics identification techniques are suitable only for high-security, low-traffic entrance control for physical access. In this chapter, we explore the latest advances in biometrics.

14.2. Access Control, User Identification and User Authentication

These terms are important in the discussion of biometrics and therefore we first deal with them before proceeding with the rest of this chapter. Access control refers to the procedures and mechanisms used either to restrict entry into the premises where something confidential is stored — for example, the premises wherein information systems (IS)/computing facilities are hosed — or to restrict entry to the computing device, or to software and/or data within the computer and to those persons authorized to use such resources. In this context, identification and authentication of users are important for information systems security.

User identification refers to the action of the user claiming his/her ID when communicating with a device. Authentication is the process of proving that the claimed ID is genuine. Thus, the proof of ID is a critical process in access control. It may take one of the following three types either individually or in combination:

1. something that the user 'knows' [password, personal identification number (PIN), etc.];

2. something the user 'possesses' (badge, smart card, etc.);

3. something the user 'is' (user's biological characteristics).

Biometrics concerns itself with the third type. It is something so unique to a person and embedded with the person that it cannot be lost, stolen or copied. Given the unique nature of human biometrics ID, biometrics methods occupy an important place in user identification/ authentication.

14.3. What is Biometrics

The term biometrics comes from the Greek words bios meaning life and metrikos meaning measure. It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, today, a wide variety of applications require reliable verification schemes to confirm the ID of an individual, recognizing humans on the basis of their body characteristics has become more and more interesting in emerging technology applications. Biometrics is used as one of the methods for physical access control. It is, basically, a collection of methods for identification based on measuring the physiological characteristics that are unique to each and every individual. Some examples of such characteristics are:

1. voice;

2. fingerprints;

3. body contours;

4. retina and iris;

5. handwriting style/handwritten signature;

6. gait (not as commonly used as the characteristics mentioned above).

Readers would like to note that gait is the peculiar way one walks and is a complex spatiotemporal biometrics. Biometrics experts say that gait is not supposed to be very 'distinctive', but is sufficiently 'discriminatory' to allow verification in some low-security applications. It is important to be aware that 'gait' is, a behavioral biometrics and may not remain invariant, especially over a long period of time, owing to the fluctuations in body weight, major injuries involving joints or brain or inebriety. However, because acquisition of gait (i.e., capturing the movement/walking style of an individual) is similar to acquiring a facial picture, it may be an acceptable biometrics. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input-intensive and computationally expensive.

Biometrics methods, in general, involve performing some human action for configuring a system used to recognize the physiological parameters of the ID (human entity) to be authenticated, for example, most often, this could be:

14.4. Nature of Biometrics Identification/Authentication Techniques

It is very important to understand the inherent nature of biometrics before proceeding further in this chapter. In the world of security, identification and authentication techniques have

'accuracy' implications that are based on 'probabilistic' phenomena. This means that another issue surrounding the topic of biometrics is that of 'certainty as probability' and there is a good reason for this. When an individual's claims of ID and privilege are verified in a truly reliable way, the identification is authoritative'. The practical value of any identification/authentication scheme, however, generally exists in one of the following three states:

1. certain and unambiguous (deterministic);
2. certain, based on a low probability of error (probabilistic);
3. uncertain and ambiguous and therefore (for all practical purposes) false.

Unfortunately, a biometrics attribute is not necessarily unambiguously permanent; therefore, all biometrics schemes are probabilistic. Design and implementation steps that can reduce the likelihood of an error are essential to orderly deployment of the technology. Biometrics techniques are most reliable and effective when used as an authenticating technique as part of a multi-factor scenario. For example, if an individual makes a claim of ID at the bank with his/her name, and that claim is supported (authenticated) by a biometrics identifier, then the probability of error is very low. Errors are much more likely to occur where the system must figure out the ID of an individual on its own (identify). This point is a crucial one to remember. Now let us understand the nature of biometrics identification and biometrics authentication.

Biometrics Identifications and Biometrics Authentication

Biometrics Identification

Biometrics identification is a sophisticated variation on a token-based, single-factor security scheme. In this case, the token is some physical attribute of the person - fingerprint, iris, retina, face, vein pattern, etc. Biometrics identification systems typically follow three high-level processing steps. First, the system must 'acquire' an image of the attribute through an appropriate scanning technique.

Once the scanned content is acquired, it must be 'localized' for processing purposes. During this step, extraneous informational content is discarded and 'minutiae' are isolated and turned into a 'template', a sort of internal canonical form for matching attributes stored in a database.

Minutiae are the uniquely differentiating characteristics of the biometrics attribute. Whorls and loops and their relationship to one another on a fingerprint are examples of the minutiae that might be extracted. Finally, templates stored in the database are searched for a match with the one just presented. If a match is found, the identification is a success and the succeeding steps of the security process can begin.

Biometrics Authentication

Biometrics authentication virtually eliminates the risk of anonymity in a 'two-factor security scenario' by using a 'physical attribute' of the person to authenticate a token. Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other is typically something that can be memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. Two-way authentication process

is similar to biometrics identification. First, the requestor presents a token to assert the ID. For example, an automated teller machine (ATM) or credit card is inserted into a reader. A number encoded on the card is actually the token; the card is more like a container for the token, but treating the card as a token is appropriate. As with identification, the system must 'acquire' an image of the personal attribute. Second, the attribute must be 'localized', the minutiae extracted and a matching template created.

Finally, the value of the token is used to look up the template previously stored for this individual. If it matches the template presented on this occasion, the requestor is authenticated.

14.5. Biometrics Techniques

In this section, major biometrics techniques are described in brief. A detailed treatment of each of the techniques is beyond the scope of this chapter. Some of the emerging technologies in biometrics are described here. They fall in major categories such as hand-based techniques, eye-based techniques, face-based techniques, voice-based techniques and signature-based techniques:

1. Fingerprint: Fingerprint identification techniques fall into two major categories — Automated Fingerprint Identification Systems(AFISs) and Fingerprint Recognition Systems (FRSs). AFIS is typically restricted to law-enforcement use. Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction. Fingerprint recognition for identification acquires the initial image through a live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and therefore reduce the sensitivity and reliability of optical scanners. Solid-state sensors overcome this and other technical hurdles because the coated silicon chip itself is the sensor. Solid-state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image, so they are less sensitive to dirt and oils. Fingerprint recognition is generally considered reliable enough for commercial use, and some vendors are already actively marketing readers as a part of local area network (LAN) login schemes. The following Figure illustrates contours on a fingerprint of humans that is unique for each individual.

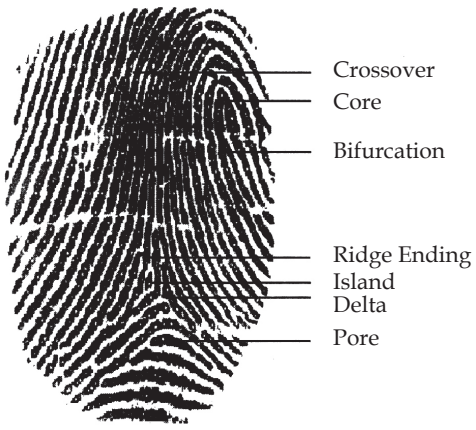


Fig. Finger Contour

Fig. Finger Recognition System

2. Hand geometry: The essence of hand geometry is the comparative dimensions of fingers and the locations of joints. Basically, the shape of a person's hand (the length and the width of the hand and fingers) measures hand geometry. This is a unique trait that differs significantly among people and hence is used in some biometrics systems to verify the ID of people. A person places his/her hand on a device that has grooves for each finger. Reference marks on the plate allow calibration of the image to improve the precision of matching. The system compares the geometry of each finger, and the hand as a whole, to the information in a reference file (called the template) to verify that person's ID. Some systems perform simple, 2D measurements of the palm of the hand. Others attempt to construct a simple 3D image from which to extract template characteristics. Readers may find it interesting to note that one of the earliest automated biometrics systems, Idenrimat, was installed at the jfhearson-Hamill investment bank on Wall Street (Manhattan, NY, USA) during the late 1960s. It used hand geometry and stayed in production for almost 20 years. In one of the most popular descendants of the Identimat, a small digital camera captures top and side images of the hand.

Fig. Hand Geometry Recognition System

3. Hand vein and palm vein biometrics: Hand vein recognition attempts to distinguish individuals by measuring the differences in subcutaneous features of the hand using infrared (IR) imaging.

   Like face recognition system, vein recognition system, too, must deal with the extra issues of 3D space and the orientation of the hand. Like retinal scanning, it relies on the pattern of the veins in the hand to build a template with which to attempt matches against templates stored in a database. The use of IR imaging offers some of the same advantages as hand geometry over fingerprint recognition in manufacturing or shop-floor applications where hands may not be clean enough to scan properly using a conventional video or capacitance technique.

   The pattern of blood veins is unique to every individual, even among identical twins. Palms have a broad and complicated vascular pattern and thus contain a wealth of differentiating features for personal identification. Furthermore, it will not vary during the person's lifetime. It is a very secure method of authentication because this blood vein pattern lies under the skin. This makes it almost impossible for others to read or copy.

Fig. Human Palm Vein Geometry

Palm biometrics works by getting the vein pattern image captured. An individual's vein pattern image is captured by radiating his/her hand with near-IR rays. The reflection method illuminates the palm using an IR ray and captures the light given off by the region after diffusion through the palm. The deoxidized hemoglobin in the vein vessels absorbs the IR ray, thereby reducing the reflection rate and causing the veins to appear as a black pattern. This vein pattern is then verified against a preregistered pattern to authenticate the individual. As mentioned before, given that

veins are internal in the body and have a wealth of differentiating features, attempts to forge an ID are extremely difficult, thereby enabling a high level of security. In addition, the sensor of the palm vein device can only recognize the pattern if the deoxidized hemoglobin is actively flowing within the individual's veins. Palm vein recognition-based system is not dangerous; a near-IR ray is a component of sunlight and so there is no more exposure when scanning the hand than by walking outside in the sun.

4. Signature: Signature is the way a person signs his/her name and is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal and commercial transactions as a method of verification. Signatures are a behavioral biometrics that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

   While a signature is not strictly biometrics (because it is not a part of human body), it is a simple, concrete expression of the unique variations in human hand geometry. Forensic experts have developed criteria over the years for verifying the authenticity of a signature. Automating this process allows computer automation to take the place of an expert in looking for unique identifying attributes. In addition to the general shape of the signed name, a signature recognition system can also measure both the pressure and the velocity of the point of the stylus across the sensor pad. Signatures, however, are difficult to model for variation, and are reliable, especially when compared with other simpler alternatives.

   Keystroke dynamics is a variation on signature recognition that measures the typing rates and intervals. Regarding keystroke dynamics, it is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometrics is not expected to be unique to each individual but it offers sufficient discriminatory information to permit ID verification. Owing to the fact that keystroke dynamics are a behavioral biometric, for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

5. Retinal scan: For a retinal scan, there is a system used for reading a person's retina to scan the blood-vessel pattern of a retina on the backside of the eyeball. This pattern is known to be extremely unique among people. A camera is used to project a beam inside the eye and capture the pattern and compare it to the reference file recorded previously (called the template). Thus, retinal recognition creates an 'eye signature' from the vascular configuration of the retina, an extremely consistent and reliable attribute with the advantage of being protected inside the eye itself. An image of the retina is captured by having the individual look through a lens at an alignment target. Diseases or injuries that would interfere with the

retina are comparatively rare in the general population, so the attribute normally remains both consistent and consistently available.

6. Iris scan: The 'iris' is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas and furrows. It is the uniqueness of each of these characteristics that makes it amenable as a biometrics method for identification. These unique characteristics are captured by a camera and compared with the information gathered during the enrolment phase.

   The issue of 'intrusiveness' of biometrics techniques is an important one. At this point, it should be noted that iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification that the iris presented as a biometrics factor is genuine. Though empirical tests with the technology will improve its reliability, it appears quite promising and even practical for many applications, especially in two-factor scenarios. While some of the technical issues of iris scanning seem pedestrian, they present implementation challenges. A careful balance of light, focus, resolution and contrast is necessary to extract the attributes or minutiae from the localized image. While the iris seems to be consistent throughout adulthood, it does vary somewhat up to adolescence.

7. Face/facial thermogram: Facial images are the most common biometrics characteristics used by humans to make a personal recognition, hence the idea to use this biometrics in technology. Face recognition technology is still in its early stages, and most tests and applications have been run against relatively small databases. The similarity score produced by each comparison determines the match — the highest score wins. Acquisition for biometrics identification purposes requires the individuals race to be presented to a video camera. An evident deficiency in some current schemes is the ability to fool or confuse some systems with makeup.

8. Voice: Voice recognition techniques are generally categorized according to two approaches - automatic speaker verification (ASV) and automatic speaker identification (ASI). ASV uses voice as the authenticating attribute in a two-factor scenario. ASI attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrolment time, and more than one enrolment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern - matching algorithms used in voice recognition are similar to those used in face recognition.

Biometrics Signature versus Digital Signature:

The practice of signatures is probably as old as the human civilization starting from the time at which people learnt how to hand-sign. Thus, the act of signing a document has long been accepted by nearly every culture as one's recognition and agreement on the contents and implications of written words. However, now in the digital era, the increasing recognition of electronic signatures

by lawmakers is bringing to the forefront concerns over electronic security (e-security) for privacy and protection of individuals.

For those conducting business transactions over private networks or the Internet, some form of official acknowledgement is now essential and legally binding. The security implications of producing or recognizing 'original' electronic documents (e-documents) will be more important than ever before. It is in this respect that an understanding to distinguish between the terms 'biometric' and 'digital' signatures becomes important.

What Is a Digital Signature?

Digital signature is a term used to describe a long numeric code that is uniquely assigned to one person, hence the reference to 'signature'. Note that it has nothing to do with a real signature. The purpose of a digital signature is to be used in encryption systems. A digital signature is issued to an individual by a Certificate Authority (CA). This is a group or an organization responsible for maintenance and safekeeping of digital signatures. Because of their length, no one actually remembers or even knows their digital signatures.

An individual's digital signature will normally reside on his/her computer, or can be stored on a card (similar to banking cards). When someone wishes to encrypt an e-document, they will use a password or PIN that in turn allows the digital signature to be used.

Although secure once encrypted, digital signatures are only as safe as is the medium where they reside. Anyone obtaining access to your password, PIN or computer can potentially make unauthorized use of your digital signature. The use of a digital signature, however, does not guarantee the ID of the originator.

What Is a Biometrics Signature?

Biometrics signature is a term used for referring to a signature that has been recorded/captured using a variety of input devices such as digitizing tablets, personal digital assistants (PDAs), computer displays or other contact-sensitive technologies. Typically, biometrics signatures can also be used to provide and control access security to buildings, networks, computers, documents and databases.

This method allows real handwritten signatures to be incorporated into e-documents during electronic transactions. Not every technology captures signature information in the same way. Some systems have a static approach and will only record an image of a signature and as such do not record the unique behavioral elements associated with the execution of a signature. In a biometrics system, the geometric and dynamic characteristics of the signing process will be recorded and incorporated in an e-document. Most of the elements that make a signature unique and identifiable can be derived from the digital signature data. Furthermore, the data that are incorporated in an e-document can be used to lock and protect the contents from alteration.

Handwriting results from a highly complex series of dynamic neuromuscular tasks from the brain to the fingertips. A naturally developed signature represents the most often reproduced

and habitual act of writing. Although we never sign exactly the same way twice, the signature adheres within certain boundaries unique to each individual. This natural variation is an essential component of handwriting. It also means that each signature is unique in that no two will be identical in all discrete features. Unlike fingerprints, retinal scans or DNA patterns that remain constant over time, the execution of a person's signature will be unique to each individual at that particular moment. Handwriting remains one of the most powerful human identifiers that exist today. Identical twins will have the same DNA pattern while their handwriting and signatures remain distinctively different.

Why Biometrics Signatures are Useful In the Security World ?

For a layman, the pictorial appearance of a conventional signature can be convincingly imitated. Forensically, when there is a question of whether or not the signature on a document is genuine, visual and microscopic examination by expert is required. This involves evaluating and comparing the general and discrete features of the contested signature with known signatures. With biometrics signatures, the authentication can be done in real time or after the fact. In the event that a biometrics signature is contested, the signature data can be extracted from the document and submitted to similar forensic investigation and analysis to verify the authenticity of the signature.

In fact, some of the biometrics data that are captured such as speed, acceleration, deceleration, and the amount of time the pen is on and off the paper are accurately measured. These data are either unavailable or qualitatively assessed at best in conventional forensic examinations of signatures. The additional behavioral features recorded from biometrics signatures make them even more difficult, if not impossible, to imitate.

Biometrics signatures represent an ideal bridge between the long-recognized convention of signing a document and the need for e-documents to be uniquely recognized by individuals. This application provides individuals with security and control on documents originated, transacted and stored in the digital domain.

14.6. Matching and Enrolment Process in Biometrics

In the discussion so far, several times, there was a mention of the terms 'enrolment' and 'template'. In this section, we explain these extremely important terms associated with biometrics. As humans, we are more comfortable recognizing our friends and family members through their faces, voices, mannerisms and gaits (the way they walk). Also, most of us are more comfortable using PINs and passwords for proving who we are. However, teaching computers how we do this so easily is a challenge. For this purpose, enrolment and template creation are the necessary steps in biometrics. Almost all biometrics systems share the same matching flow.

There are a number of key terms that appear in the following Figure that are explained as follows:

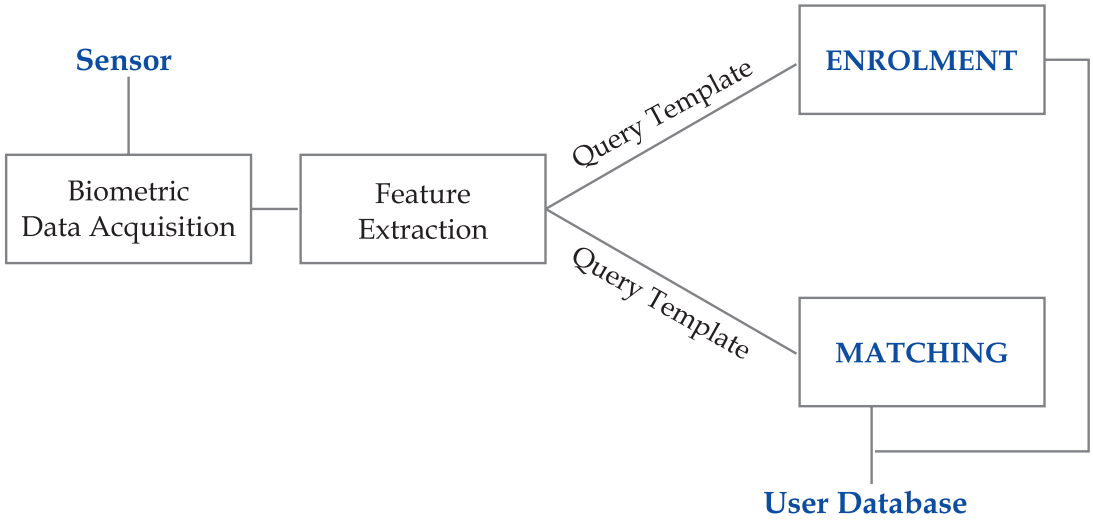


Fig. Process Flow in Biometrics Matching

1. Biometrics: A measurable physical characteristic or personal behavioral trait used to recognize the ID, or verify the claimed ID, of an enrollee.
2. Behavioral biometrics: This is a biometrics that is characterized by a behavioral trait that is learnt and acquired over time rather than a physiological characteristic. However, physiological elements may influence the monitored behavior.
3. Biometrics data: These are also known as biometrics sample. These data consist of biometrics characteristics of the entity under authentication and are physiological data in nature. They are the information extracted from the biometrics sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data). Thus, biometrics sample/biometrics data are the raw data representing a biometrics characteristic of an end-user as captured by a biometrics system (e.g., the image of a fingerprint, retinal scan data, etc.).
4. Enrolment: It is the process by which a subjects (entity under authentication) biometrics data are initially acquired, accessed, processed and stored in the form of a template. Thus, it is the process of collecting biometrics samples from a person and the subsequent preparation and storage of biometrics reference templates representing that persons ID.
5. Enrolment time: It is the time period a person must spend to have his/her biometrics reference template successfully created.
6. Template: It is a crucial element in the working of biometrics systems as it is the deciding and defining element of biometrics technology. A template is nothing but a small file derived from the distinctive features of a users' biometrics data used for performing biometrics matches. It is important to note that the biometrics systems store and compare biometrics templates, and not biometrics data.

7. Match/matching: It is the process of comparing a biometrics sample against a previously stored template and scoring the level of similarity. Accept or reject decisions are based on whether this score exceeds the given threshold.

8. Feature extraction: This is the automated process of locating and encoding distinctive characteristics from biometrics data in order to generate a template. Feature extraction takes place during enrolment and verification process.

9. Biometrics engine: It is the software element of the biometrics system that processes biometrics data during the stages of enrolment and capture, extraction, comparison and matching.

10. Biometrics device: It is the part of a biometrics system containing the sensor that captures a biometrics sample from an individual.

11. Comparison: It is the process of comparing a biometrics sample with a previously stored reference template or templates.

12. Minutiae: It is the unique, measurable physical characteristic scanned as an input and stored for matching by biometrics systems. For fingerprints, minutiae include the starting and ending points of ridges, and ridge junctions among other features.

14.7. Key Success Factors for Biometrics Systems

For any effective biometrics system, there are a few important factors associated with it: accuracy, speed and throughput rate, acceptance by users, uniqueness of biometrics organ and action (on which the techniques are based), reliability (i.e., resistance to counterfeiting), data storage requirements, enrolment time (this term was explained in the previous section), intrusiveness of data collection, etc. Effective functioning of biometrics systems would depend on these factors. In this section, these factors are explained in brief.

14.7.1. Accuracy

Accuracy is the most critical characteristic of a biometrics identification verification system. If the system cannot accurately separate an authentic person from an impostor, it should not even be termed a biometrics identification system. There are two issues that arise - false rejection rate (FRR) and false acceptance rate.

1. FRR: This rate is generally expressed as a percentage. It is the rate at which authentic, enrolled persons are rejected as unidentified or unverified persons by a biometrics system. The FRR is also known as Type I error. In access control, if the requirement is to keep the unauthorized persons out, false rejection is considered the least important error. However, in other biometrics applications it may be the most important error. In the banking or retail business domain, when a biometrics system is used to authenticate the customer ID and account balance, false rejection means that the transaction or sale is lost, upsetting the customer. Most banks and retailers tend to be OK with a few false accepts as long as there are no false rejects. They do this keeping their business interests in mind.

   There is a reason why the matter of false rejection creates so much anxiety - it has a negative effect on throughput, frustrations and operations impediments by causing unnecessary

delays in personnel movements. Another problem with FRR is that sometimes it is incorrectly attributed to the 'failure to acquire'. Failure to acquire occurs when the biometrics sensor is not presented with sufficient usable data to make an authentic or impostor decision. Examples of unusable data include smudged prints on a fingerprint system, improper hand positioning on a hand geometry system, improper alignment on a retina or iris system or mumbling on a voice recognition system. The issue is that subjects under identification (humans) cause failure-to-acquire problems, either accidentally (unintentionally) or on purpose to fudge the security system for their illicit purpose. When FRRs rise, it may be OK if it is a tight security area such as defense or medical institution but not OK if it is a retail business/ commercial centre (where biometrics-based access controls are anyways not suitable). 'FAR' is a reverse situation. This is the rate (stated as percentage) at which unenrolled persons or impostors are accepted as authentic, enrolled persons by a biometrics system. FAR is also known as Type II error.

2. Crossover error rate (CER): It is the rate at which the FRR and FAR match. It is also known as 'equal error rate' (ERR) and is stated as a percentage. This is the most important measure of biometrics system accuracy. It is important to understand the meaning of false non-match rate (FNMR). A biometrics solution's FNMR is the probability that a user's template will be incorrectly judged to not match his/her enrolment template. Given this, we can say that ERR is the rate at which the FNMR is equal to the false match rate (FMR). Thus, ERR or CER presents the accuracy level at which the probability of a false match is the same as the probability of a false non-match. ERR is commonly used as a representation of overall system accuracy, because it is a general indicator of a system's resistance to break-ins and ability to match templates from authorized users.

14.7.2. Speed and Throughput Rate

For biometrics system characterization, speed and throughput are important. Data-processing capability of the biometrics system decides the speed; it is stated as how fast the accept or reject decision is enunciated. It relates to the authentication procedure; the system setup, card input or PIN (if a verification system); inputting the physical data by inserting the hand or finger, aligning the eye speaking access words or signing a name processing and matching of data files; enunciation of the accept or reject decision; in case of a portal system, movement through the door and closing of the door, etc. A system speed of 5 s from start-up through decision enunciation is good as per generally accepted standards. Another standard is a portal throughput rate of 6—10 per min, which equates to 6-10 s per person through the door. In spite of great strides in the biometrics research, it is not easy for most biometrics systems to meet these standards.

14.7.3. Acceptability by Users

User acceptability to-date is a big challenge for pervasive deployment of biometrics systems. This is mainly owing to the social stigma attached to the biometrics systems given their nature and lack of adequate awareness on biometrics identification systems. Biometrics system acceptance occurs when those who must use the system, that is, management and unions involved in the organizations, need

to come to an agreement that biometrics should be deployed for the protection of organizational assets. Also consider the social stigma factor mentioned as well as the lack of awareness; fingerprinting is a particularly sensitive topic, given that it is associated with criminals. Eye retina scanning requires users to trust that the system will not damage their eyes, a feeling they carry possibly owing to rumors and inadequate information about how the retinal scanning technology works. It is clear that uncooperative users can overtly or covertly compromise, damage or sabotage the biometrics scanning equipment. Given this the management has to decide about the implementation based on the cost/benefit associated with a biometrics system. Biometrics has got privacy implications too.

14.7.4. Uniqueness of Biometrics Organ and Action

The purpose of a biometrics system is positive identification of the personnel - given this, it is important that the systems are based on unique characteristics of the employees. So, when the base is a unique characteristic a file match is a positive identification rather than a statement of high probability that it is the right person. Out of the many physical characteristics that can be used, only three can really be considered unique enough for identification: the fingerprint, the retina of the eye (the blood-vessel pattern inside the black of the eyeball) and the iris of the eye (random pattern of features in the colored portion of the eye surrounding the pupil).

14.7.5. Reliability of Biometrics

When using biometrics verification systems, it is vital that they operate in an accurate fashion. The concept of a biometrics system's reliability is related to its 'selectivity'. Reliability is the probability that a matcher system will correctly identify the mate when the mate (i.e., entity whose biometrics unique character is being matched) is present in the system repository, whereas selectivity is the number of incorrect mates determined for a given search.

Only authorized persons must be allowed to access and it must preclude the others without breakdown or deterioration in performance accuracy or speed. In addition, these performance standards must be sustainable without high levels of maintenance or frequent diagnostics and system adjustments. The tradeoff between reliability and selectivity offers the greatest system design challenge since these parameters are interdependent.

14.7.6. Data Storage Requirements in Biometrics Systems

Earlier computer systems had primary and secondary memory size constraints, that is, limited random access memory (RAM) and disk size. This is less of an issue today as computer technology has advanced in both hardware and software. Even then, the size of biometrics data files remains a factor of interest. Given the large size of biometrics match templates, even with the current ultra-high-speed processors, large data files take longer than small files to process. This is especially so in biometrics systems that perform 'full identification', that is, matching the input file against every file in the database. Typically, biometrics file size varies between 9 and 10,000 bytes, mostly falling in the 256-1,000 byte range.

14.7.7. Enrolment Time in Biometrics

We discussed 'matching and enrolment'; enrolment time is also not so much of an issue these days. In the early days, biometrics systems sometimes had enrolment procedures requiring many repetitions

and several minutes to complete. Consider the following: a system requiring a 5-min enrolment instead of 2 min causes 50 h of expensive non-productive time if 1,000 users must be enrolled. In addition, line waiting time must also be considered. All this adds to the total cost. The accepted standard for enrolment time is 2 min per person. Most of the systems available in the market today meet this standard.

14.7.8. Data Collection Intrusiveness

Origins of this factor come from the users' concerns about the collection of biometrics data from inside the human body — especially the retina inside the eyeball. Early biometrics systems illuminated the retina with a red light beam that happened to coincide with increasing public awareness of lasers, sometimes demonstrated as red light beams cutting steel! Although there has never been any injury reported owing to retinal scans using the light beams, public fear and user sensitivity still remain. An advance form of such public concern is about intrusions into human body, a space that is considered private.

14.7.9. Requirements About Subject and System Contacts

Under biometrics methods for identification, the users are required to make a firm physical contact with the instrument for biometrics data collection. This factor is an extension of the concerns mentioned in the previous section, given that the users need to make mouth contacts (voice-based identification), eye contacts (retinal scans) and hand contact (hand geometry-based identification). This factor involves a lot of human psychology too — 'If I wish to make contact with the instrument as my own accord, then it is OK but if an organization and agency makes me do it then I am not OK with it', probably because the users imagine a possible misuse of what they think is 'private information' about their body. In a way, it is the attitude about the biometrics techniques that is having an impact on adoption rates of these techniques.

14.8. Benefits of Biometrics over Traditional Authentication Methods

Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometrics cannot be borrowed, stolen or forgotten and forging one is practically impossible. From the preceding discussions, one can see that biometrics is an alternative to using passwords for authentication in logical or technical access control. Biometrics is based on the third type of authentication mechanism — something you are Biometrics is defined as an automated means of identifying or authenticating the ID of a living person based on physiological or behavioral characteristics. In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images. Authentication in biometrics is a one-to-one' search to verify a claim to an ID made by a person. Biometrics is used for identification in physical controls and for authentication in logical controls.

In the domain of physical security passwords and PINs are the most frequently used authentication techniques for controlling access. In higher security applications, handheld tokens are used instead of passwords. However, passwords, PINs and tokens have a number of problems that raise questions about their suitability for modern security access control applications, particularly high-security applications such as access to defense systems or medical data systems. Biometrics provides a number of benefits compared to the traditional methods:

1. increased level of security;
2. greater convenience;
3. higher level of accountability;
4. fraud detection and fraud deterrence.

14.9. The Future of Biometrics

According to one European report, interesting developments are happening in the field of biometrics; strong R&D presence, large number of leading developers and, thus, market conditions look bullish. In an increasingly insecure world, biometrics indeed has a promise to fulfill. There are several other factors that will push the growth of biometrics technologies. A major inhibitor of the growth of biometrics has been the cost to implement them. That is beginning to change as computer hardware and software as well as manufacturing prices fall.

Forensic scientists developed most biometrical applications for governmental purposes. Relatively few biometrics applications are used in the private sector. For the future of biometrics, experts propose four scenarios: biometrics at the borders, in the health sector, in business and in everyday life. They can be placed on a continuum ranging from public-sector applications to private applications with little or no government involvement. Privacy, security, usability and user acceptance concerns differ according to the environment. The first scenario, that is, biometrics in day-to-day life, draws attention to one basic fact that biometrics technologies can never be 100% secure. It is a matter of trade-off between allowing impostors through the system (false accept) and denying access or services to legitimate users (false reject). As far as the use of biometrics in business is concerned, it can be for various purposes: internal (e.g., for employees) and external (e.g., with clients and other companies). In the business world, backup/alternative procedures are important and biometrics access systems are only as secure as their weakest link, which is, in this case as in most cases, human. Users, concerned about their privacy, may reject biometrics when there is a little perceived added value for them.

Let us consider the health sector as a potential area of real-life application of biometrics. It is clear that strong identification is essential in the health sector — retrieving medical histories, administering medicine, handing out prescriptions and carrying out medical procedures, all rely on the correct identification of the individual. In addition, there is a strong need for privacy given the sensitive nature of medical data. These two requirements make the health sector a very likely field for the application of biometrics. For countries like India with common sharing of borders with the neighboring countries and constantly facing terrorist threats from anti-social elements passing across the border, this last scenario is of great relevance. Biometrics at the borders is likely to occur within the shortest time frame as concrete plans for this application already exist. The use of biometrics will need to ride through different legal and regulatory regimes in the areas of applications. The importance of secure enrolment is while handling the cross-border travelers for their quest for necessary visas.

According to some experts in the industry, the future of biometrics remains uncertain. How well do biometrics keep the 'bad guys' out and let the 'good guys' in will always be a question

that is asked when customers look to implement a biometrics technology. Both FMR and FNMR continue to improve and it is the balance between the two that will be critical when implementing a biometrics technology. In terms of R&D, there are a number of new technologies that are under development that are looking at other physiological features for identification:

1. DNA matching;
2. body salinity (salt) identification;
3. body odor identification;
4. vein pattern identification;
5. ear shape identification;
6. palm print identification;
7. 'electronic nose' identification.

In conclusion, we see that the field of biometrics is evolving. Biometrics is now not just used to control physical access, but is also used in a variety of industries and circumstances. Biometrics technology is improving and falling in price as vendors increase revenue. As a result, funding is becoming more widespread and the development of biometrics is on the rise.

Summary

The widespread implementation of biometrics applications raises a series of challenges. In this chapter, we discussed some special aspects of biometrics that matter. Important among them are the issues around design of biometrics systems, as well as implementation and interoperability issues. The work in the area of biometrics standards shows a good promise to harmonize some design-related issues. The past few years have seen an explosion of activity in the biometrics standards area resulting in an acceleration of the standardization process. Given the very nature of biometrics, biometrics as yet does not seem to enjoy a wide acceptance and also it does seem to have many social and legal implications. Biometrics technologies are still largely undergoing development and are not yet mature enough for a widespread use in the society. Overall, biometrics systems are still being considered risky and they invite a lot of public debate although year by year the technical side of biometrics is improving. Finally, the decision whether or not to use biometrics technologies in a security solution as well as which one to select from the available technologies should consider state-of-the-art risk assessment practices, cost/benefit analyses and the potential.

अध्याय 15

Chapter 15

Web Services and Privacy

Introduction

The focus of this chapter is web services, applications and technologies based on web services and privacy issues surrounding them. We are going to discuss how web services can impact data privacy. Explaining web services architecture, however, is not the aim of this chapter; it is assumed that readers have conceptual familiarity with web services. An idea about service-oriented architecture (SOA) will be provided to the extent that is needed to understand other aspects of web services. Use of digital credentials to support privacy when interacting with web services-based business applications is also discussed. This chapter covers the privacy aspects given that web services and web agents and context-sensitive applications interact to carry out sophisticated tasks on users' behalf. Privacy comes into picture because, in the course of this interaction, they (web services, agents and context sensitivity) might automatically exchange sensitive, private information about these users.

When web services and web agents interact to carry out sophisticated tasks on behalf of users, a natural result of this increasing trend toward lesser human involvement and more automation (using agents) is that the users will have less control over how web agents and web services manipulate their personal information (PI).

The issues of privacy preservation must therefore be appropriately tackled. Before we take up the discussion about web services privacy and the associated security issues, we need to touch base with privacy exposures from the Internet use because Internet is the vehicle for deploying web services published on it. The terms 'Internet' and 'web' will be used interchangeably throughout this chapter. We shall also discuss privacy issues associated with the semantic web. Platform for privacy preferences (P3P) privacy concept too will be introduced in this chapter. We commence the discussion in this chapter with a discussion about the privacy on the Internet from legal and organizational standpoints and then we go to the core topic of this chapter — web services and privacy.

15.1. Privacy on the Internet - A Legal Perspective and Organizational Implications

There should be no disagreement that the Internet has truly 'revolutionalized' our life as far as information gathering is concerned. However, with this 'ease of information availability', many other challenges are now on hand, a major one being the challenge of preserving our data privacy.

15.1.1. Privacy and the Internet; Privacy Violation

Let us understand what is different about our concerns with privacy when we deal with the Internet. Informed consent and collection of information are two important aspects while interacting on the Internet. 'Loss of privacy' versus violation of privacy' is another good pair of concepts to consider. An ethical collection of PI causes a loss of privacy. Obtaining informed consent is sufficient but not necessary for an ethical collection of PI. An unethical collection of PI causes a violation of privacy. Collection of PI is unethical when it does not comport with the reasonable expectation of privacy for this situation.

The web has indeed spurred an information revolution, even reaching sectors left untouched by the personal computing boom of the 1980s. It made information ubiquity a reality for sizeable segments of the world population, transcending all socio-economic levels. The ease of information access, coupled with the ready availability of personal data, also made it easier and more tempting for interested parties (individuals, businesses and governments) to intrude on people privacy in unprecedented ways. Today, despite all the regulatory and technical efforts aimed at tackling

these aspects of the problem, privacy violation incidents on the web continue to hit the headlines. Regulatory and self-regulatory measures addressing one or more aspects of this problem have achieved a limited success. Differences and incompatibilities in privacy regulations and standards have a significant impact on electronic business (e-business). For example, US web-based businesses might be unable to trade with millions of European consumers because their practices do not conform to the European Unions (EU's) Data Protection Directive [interested readers can visit the EU Directive uniform resource locator (URL) provided in the Further Reading section for greater details on this initiative]. In the next section, we focus first on web privacy from users' perspectives and then we consider the organizational dimensions by addressing web privacy practices.

15.1.2. The Nature of Privacy Problems on the Web

Two major factors-contribute to the privacy problem on the web:

- the inherently open, non-deterministic nature of the web;
- the complex, leakage-prone information flow of many web-based transactions that involve the transfer of sensitive PI.

To comprehend the first factor, we can contrast the web with traditional, closed, deterministic multi-user systems, such as enterprise networks. In these systems, only known users with a set of predefined privileges can access data sources. On the contrary, the web is an open environment in which numerous and a priori unknown users can access information. Examples of the second factor include applications involving citizen-government, customer—business, business—business and business—government interactions. In some of these applications, PI that a web user submits to a given party might, as a result of the application's intrinsic work flow, be disclosed to one or more other parties. Assembling PI from multiple sources, originally collected for different purposes, is known as 'digital dossier'.

15.1.3. Legal Issues with Use of Internet

Preserving privacy on the web, therefore, has an important impact on many web activities and web applications. Of these, digital government(DG) and e-business are two of the best examples. DG is a major application domain for web services. It aims at improving government-citizen interactions using information and communication technologies. Government agencies collect, store, process and share information about millions of citizens who have different preferences regarding their privacy. This naturally raises a number of legal and technical issues that must be addressed to preserve citizens' privacy through the control of the information flow among different entities [users, web services and database management systems (DBMSs)].

In the context of e-business, privacy violations tend to be associated mostly with marketing practices. Typical cases occur when businesses capture, store, process and exchange their customers' preferences to provide customized products and services. In many cases, these customers do not explicitly authorize businesses to use their PI. In addition, a legitimate fear exists that companies will be forced to disclose their customer's personal data in court. For example, in a scenario with music-recording companies, users may illegally download music. Mishaps such as these have negatively affected businesses and, consequently, the web-based economy. Consumers' mistrust naturally translates into a significant reluctance to engage in online business transactions. According to Gartner Group, information privacy will be the greatest inhibitor for consumer-based e-business.

15.1.4. Online Trust - The Government Scenario

As said before, DG is another class of web applications in which web privacy is a critical issue. Government agencies collect, store, process and share personal data about millions of individuals (remember the term 'digital dossier'). DG potentially transforms citizen—government interactions in two ways: by improving service delivery, including costs and by improving communication between citizens and government. A citizen's privacy is expected to be protected through regulations that government agencies and any business that interacts with them must implement. Users tend to trust government agencies more than businesses. Additionally, governments' foray in developing techniques for gathering and mining citizens' personal data has stirred controversy — for a worldwide experience on e-government. Overall picture seems to indicate that in general, people are not inclined toward using the Internet for voting purpose. Younger citizens tend to support e-government/DG more than the older ones. This has implications for countries such as India where the percentage of young population is high.

15.1.5. Web Services and Their Privacy and Security Implications

Wherever a person or system interacts with, or has the opportunity to interact with an application, there is a threat/risk opportunity for applications and information to be compromised. The benefits of web applications including global accessibility, open source and rapid development opportunities increase these threats exponentially. Often, a web application is the only thing standing in the way of an attacker and sensitive business information. Web application attacks account for two-thirds of all attacks. Firewalls only stop network service attacks. Depending on the application, an attacker may be able to view or manipulate sensitive information, obtain unauthorized access to an application or be able to take control of the whole application. Today, people are spending a lot more time online and spending a lot more money online.

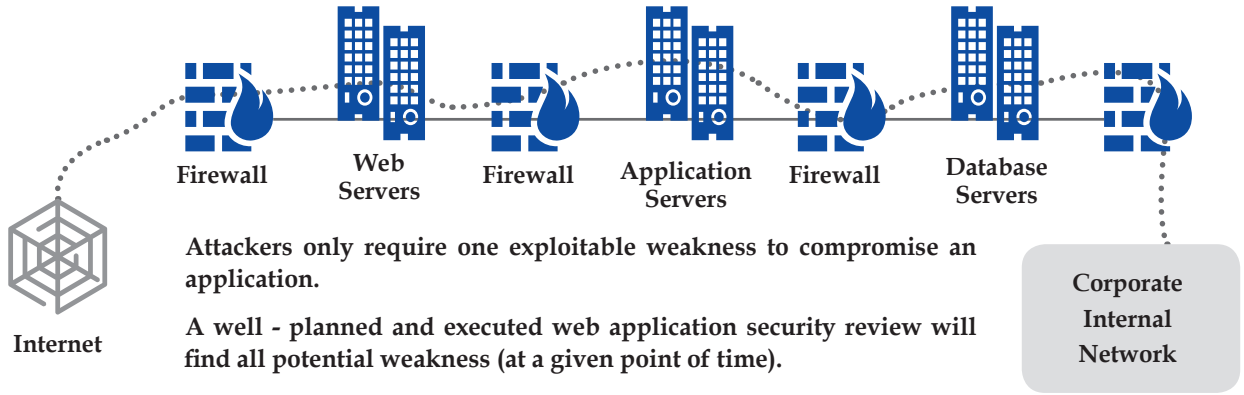


Fig. Web Applications: The Path of Easiest Exploit

As the monetary value of online activity grows, so too does the correlation between application attacks and organized and financial crime. For example, consider this: in February 2006 at Sydney, 400 customer credit card details were compromised. Investigations identified 478 attempts over three days using six different Internet protocols (IPs) to access administrator passwords. Intrusions originated from Germany, United States and Indonesia. In October 2006, at Sydney, hackers compromised Nortel PABX to make AUD 9,000 worth of calls in a week to Arab Emirates, South America and Africa — ZD Net Australia, 17 October 2006. Advanced attacks focus on compromising

applications and not the network because any information entered via the web page almost always reaches the back-end database server.

15.1.6. Web Services Role in Today's Businesses

In spite of these known cyber crime threats, today, in our net-centric digital world, web services play a crucial role in enterprise applications, DG, that is, e-government and information systems (IS). Web services are applications that expose interfaces through which web clients can automatically invoke them. IBM's definition of web services states that 'Web Services are self-contained, modular applications that can be described, published, located and invoked over a network, generally, the World Wide Web'. Generally web agents are intelligent software modules that are responsible for some specific tasks - for example, searching for an appropriate doctor for a user, searching an address on a map, etc. As another example, consider a government web service providing social and welfare benefits

C2C: Person (consumer) to Person - E-mail (SMTP, RFC-822)

B2C: Person to Application - Web (HTTP, HTML)

A2A: Application to Application - Web Services (XML, SOAR, UDDI, WSDL)

(e.g., health insurance and child support). A citizen accessing this service would typically provide sensitive private information. To preserve the citizens' privacy, the web service must support mechanisms that translate the citizen's right to conceal any PI and decide what, when and to whom any of that information may be revealed. In the next section, we provide an illustrative example to demonstrate web service authentication function offered on the web by Microsoft passport technology.

15.1.7. Web Services Working: An Illustration

Web services are middleware; using web services, you can connect applications together, no matter how each application is implemented or where it is located. Simple object access protocol (SOAP), to put it simply, allows Java objects and Component Object Model (COM) objects to talk to each other in a distributed, decentralized, web-based environment.

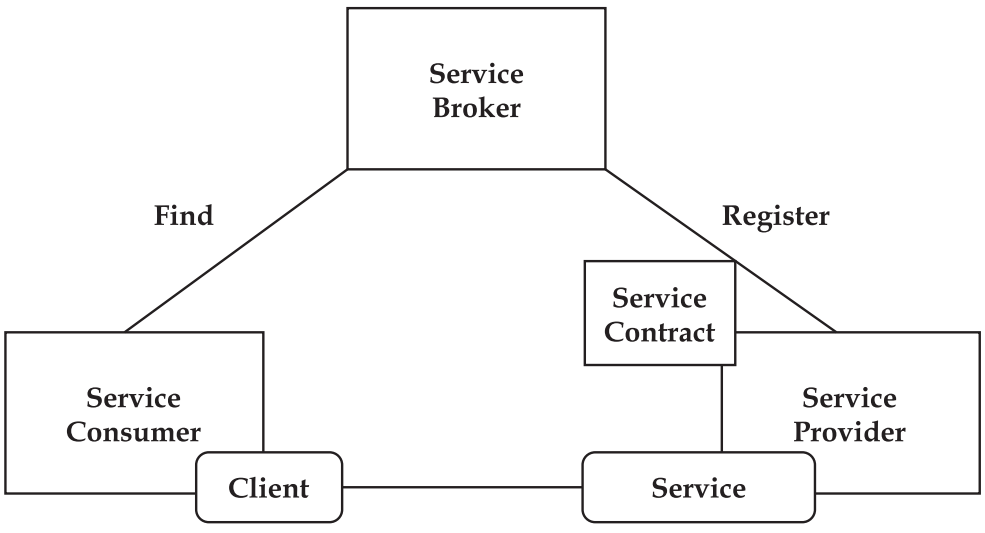


Fig. How Web Services Work - Broker, Consumer and Provider

"As I have said, the first thing is to be honest with yourself. You can never have an impact on society if you have not changed yourself... Great peacemakers are all people of integrity, of honesty, but humility." ***- Nelson Mandela***

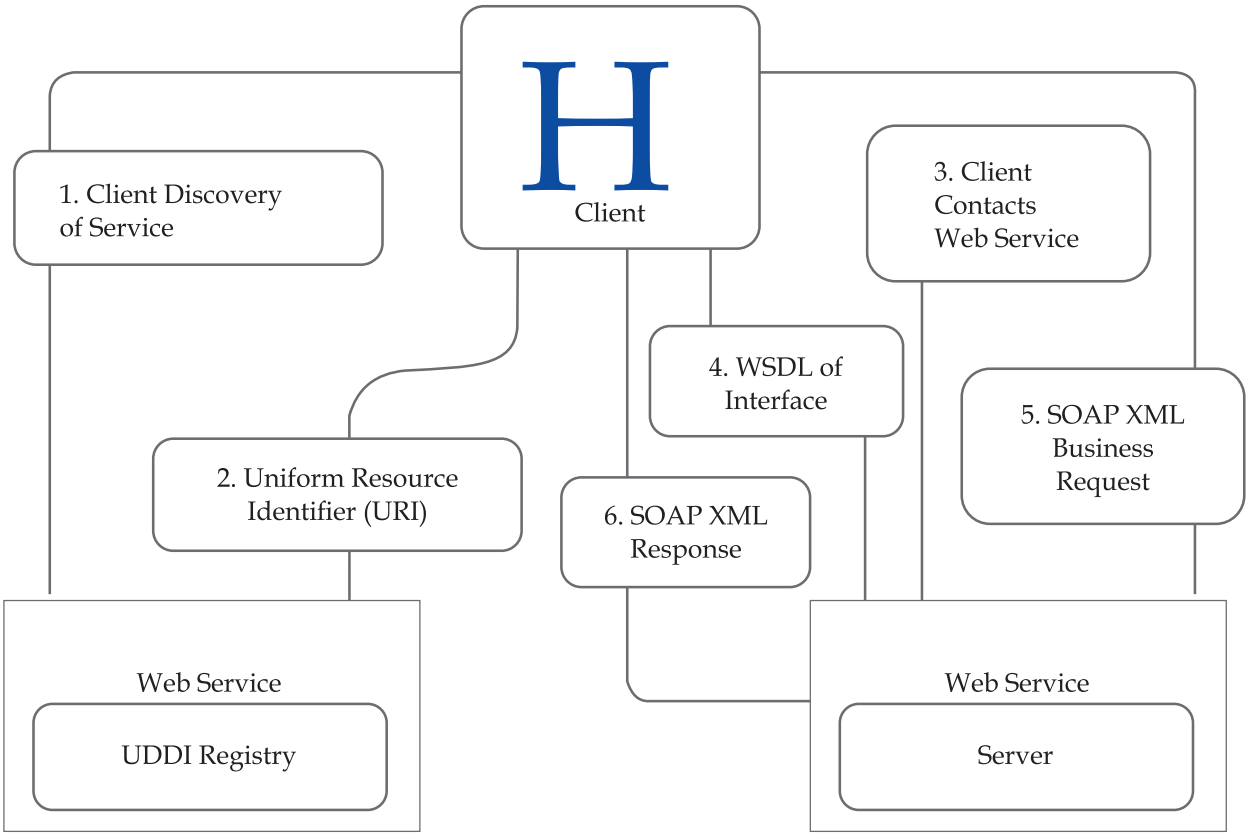


Fig. How Web Services Work - UDDI, SOAP and WSDL

More generally, SOAP allows objects (or code) of any kind, on any platform, in any language to cross-communicate. SOAP is a protocol that is paired with universal description, discovery and integration (UDDI) to provide registry and messaging services among businesses. Take any online electronic marketplace as an example. There are a lot of businesses, each offering its own services (web services). In the present-day electronic commerce (e-commerce), there is no mechanism that allows one business to discover automatically the services that its prospective partners offer. The so-called next generation dotcom will offer a mechanism for exactly this kind of automated discovery. This new breed of dotcom needs a solution that can describe the services — the web services. Specifically, this means that you need a format or some type of grammar with which you can describe the answers to the following questions:

1. What are the services offered in your online business?
2. How can you invoke your business services?
3. What information do your business services need from the user when s/he invokes your service?
4. How will the user provide the required information?
5. In which format will the services send information back to the user?

Web Services Description Language (WSDL) Provides the Mechanism for Doing all of These Jobs.

However, there is one important point to note: the two standards WSDL and UDDI provide little or no support for privacy enforcement and hence the need for P3P (this is discussed in a section 'How Website Privacy works with P3P').

Having explained SOAP, WSDL and UDDI, here is one detailed example to illustrate web services in action for solving business problems. This example describes how an online retailer could use a variety of Web services technologies. Consider a retailer who uses web services support in WebSphere Application Server to improve communications with suppliers. For example, web services can connect this retailer to its wholesale suppliers. The concept of middleware' is not new. What is new in web services is that this connectivity is based on open standards and web technologies. Web services operate at a level of abstraction that is similar to the Internet, and they can work with any operating system (OS), hardware platform or programming language that can be web enabled.

In this illustration (refer below Figure: WebSphere storefront for garden implements retail business), the retailer sells plants and gardening supplies. As customers order merchandise, the site checks the merchandise availability in its inventory database. The scenarios described show how the inventory system can grow in stages, using various web services technologies to improve its capabilities. Suppose that the 'Plants by WebSphere storefront' (an application) does not use web services. The retailer has established impressive Internet storefront (a portal), enabling customers to shop and order merchandise. To determine whether a customer order can be filled, web applications rely on enterprise beans to query the Plants by WebSphere inventory database. If the item is in stock, the site confirms the order to the customer. If a customer orders an item that is out of stock, the site notifies the customer that the item is out of stock, and encourages the customer to place the item on backorder. Later, long after the customer has left the Plants by WebSphere site, the site administrator or inventory manager might call or fax the supplier to obtain more inventories (WebSphere is IBM's flagship product in web services development). The following Figure shows how things work out.

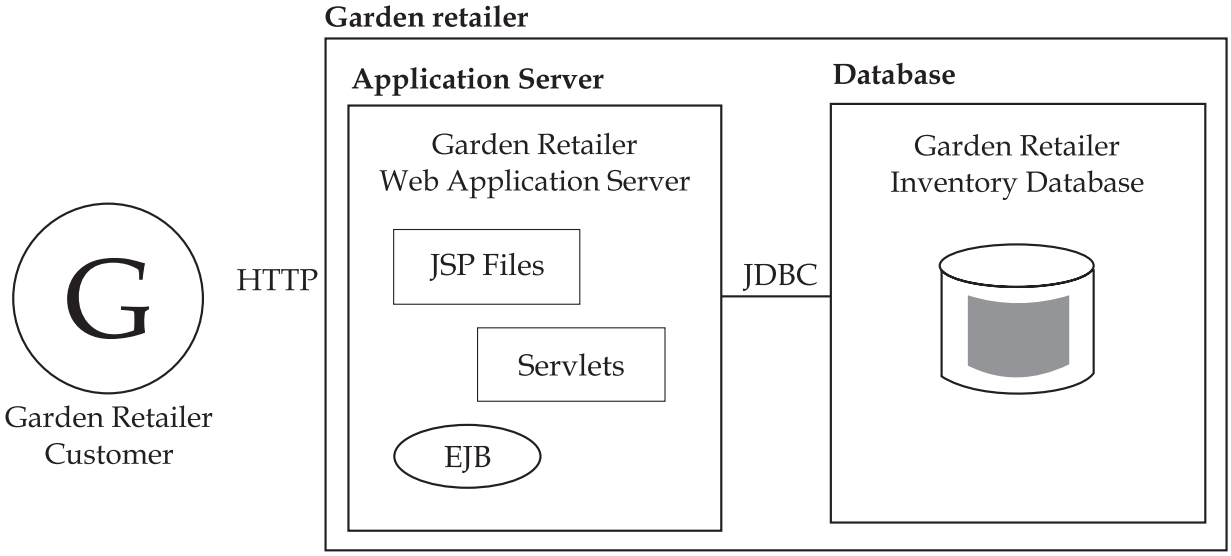


Fig. WebSphere Storefront for Garden Implements Retail Business

Life's errors cry for the merciful beauty that can modulate their isolation into a harmony with the whole.
- Sir Rabindranath Tagore

Now let us understand how web services could make a difference to this retail business. Web services could result into an automated way to have out-of-stock items shipped to its warehouse or directly to customers. If suppliers can be contacted quickly enough, business does not have to inform its customers that the item was out of stock. It would be possible for the retailer to reduce its own inventory if doing so is a desirable business move. The technical functionality in web services includes open messaging and registry protocols. They enable developers to build software components that can automatically seek out and interact with other components built into the same standards. An important requirement for applications built into web services is that they should be able to 'talk to each other, that is, cross-application communication. These applications can be written as software components that can be housed in an application on a local network or on the Internet, and they are accessible by other network applications. There is also a 'dependency' aspect in web services — as websites come to depend on other web services, they will require support for server-to-server and application-to-application communication.

15.2. Privacy Considerations in Web Services

Simply, a web service is a functionality that can be programmatically accessible via the web. Note that BPEL is business process execution language used in web services application development. It is an extended markup language (XML)-based workflow definition language that allows businesses to describe inter- or intra-enterprise business processes that are connected via web services. DAML is Defense Advanced Research Projects Agency (DARPA) agent markup language, a language designed to express information so that it can be easily used by computer programs. WSCI is web service choreography interface.

Now let us discuss how to preserve privacy in web services. Web services are increasingly being adopted as a viable means to access web-based applications. Web technologies are driving a paradigm shift in several economic activities including business-to-customer (B2C), business-to-business (B2B) and government-to-citizen relationships. Web services are the way of application architecture and so this discussion is important.

A large amount of information gets collected, stored, processed and shared about millions of citizens who have different preferences regarding their privacy. This naturally raises a number of legal and technical issues that must be addressed to preserve citizens' privacy through the control of the information flow among different entities (users, web services and DBMSs). Solutions addressing this issue are still in their infancy. They consist, essentially, of enforcing privacy by law or by self-regulation.

A point to note is that the current trend in web technologies is to provide access to business and government applications through web-based services (or, simply, web services). Another key point in the context of privacy discussion is the following: a citizen accessing this service would typically provide sensitive private information. To preserve citizens' privacy, the web service must support mechanisms that translate the citizens right to conceal any PI and decide what, when and to whom any of that information may be revealed.

15.2.1. Data Privacy Considerations in Web Services

In this section, we take up various illustrations to explain data privacy considerations in web services. Users of a web service include persons (e.g., citizens and case officers), applications and other web services. In many cases, users interacting with a web service are required to provide a significant amount of sensitive personal information (SPI) [e.g., their social security number (SSN), credit card number, health information and address]. Users of web services, however, may expect or require different levels of privacy according to their perception of the information sensitivity. For example, a user may have tighter privacy requirements regarding medical records than employment history. The user's perception of privacy also depends on the information receiver (i.e., who receives the information) and the information usage (i.e., the purposes for which the information is used).

The set of privacy preferences applicable to a user's information is called user privacy profile. A user privacy profile is typically defined by the user but can also be uniformly set for a group of individuals. Privacy profiles are dynamic, users can create, view, update or delete their privacy profiles. To provide support for resolving legal disputes over privacy violation, the underlying web service architecture must trace all of these operations. We also define a user's privacy credentials as a signature that is typically appended to any request that the user submits to the web service. They determine the privacy scope for the corresponding user. A privacy scope for a given user defines the information that a web service can disclose to that user. For example, a case officer accessing a government web service may have privacy credentials granting a privacy scope that includes information about citizens' employment, housing, etc. Privacy credentials may be assigned to users on an individual or group basis.

A web service generally has its own privacy policy that specifies a set of rules applicable to all users. Service privacy generally specifies three types of policy: usage policy, storage policy and disclosure policy. The usage policy states the purposes for which the information collected can be used. For example, consider a government web service for medical care that provides healthcare coverage for low-income citizens. The Medical Care service may state that the information collected from citizens will not be used for purposes other than those directly related to providing health services to citizens. The storage policy specifies whether and until when the information collected can be stored by the service. For example, the Medical Care service may state that the information it collects from citizens will remain stored in the underlying databases one year after they leave the welfare program. The disclosure policy states if and to whom the information collected from a given user can be revealed. This information may relate to individual persons or to groups of individuals. For example, the privacy policy of the web service-based Medical Care application may state that external users cannot access statistical information that reveals general characteristics of the beneficiaries (e.g., average income, racial background distribution, etc.).

A data object may be accessed by several web services. For example, consider the US National Database for New Hires (NDNH) that contains information about over 200 million hired employees.

A record in this database can be accessed (using a government web service) by an Internal Revenue Service (IRS) officer to check the accuracy of an employee's tax form. It may also be accessed (using another government web service) by an officer at a child support agency to check whether a parent is compliant with his/her child support obligations. This shows that different web services may need different information from the same data object. Thus, data objects must be able to expose different views to different web services. For each data object, there is a need to define a data privacy profile that specifies the access views that it exposes to the different web services. This is the requirement that gives rise to e-privacy considerations.

15.2.2. E-Privacy Considerations

E-Privacy has a three-dimensional feature of web service infrastructures: user privacy (as perceived by the user of a web service), data privacy (as supported at the data level) and service privacy (as exposed to users by a web service). Enforcing the requirements of these three levels of privacy poses a number of challenges. For example, enforcing privacy at the service level may require a complex and dynamic handling of users' privacy requirements. Moreover, service privacy is further complicated by service composition. For example, if there were a composite web service, it might have to transparently interact with a number of other web services to answer a citizen's request. As those services may not necessarily have a privacy policy that is compatible with the privacy policy of the composite web services, the citizens information might get revealed to parties that normally have no access rights to this information. The lack of technology-based solutions to the e-privacy problem in (simple) web services and the implicit sharing of information that results from the use of composite web services have brought to the fore legitimate concerns about privacy in web services.

15.2.3. Digital Credentials - For Privacy Protection While Interacting with Web Services

Applications that involve the electronic transfer of credentials, value tokens, profiles and other sensitive information are quickly gaining momentum owing to the boom in cross-border data flows. Traditional attempts to introduce electronic authentication, such as public-key infrastructure (PKI) and biometrics verification, expose organizations to potentially unlimited liability, lead to consumer fear and stifle the adoption of new system. To overcome these barriers, innovative solutions are needed that address the ensure spectrum of security and privacy interests for all parties involved. Digital credentials are the digital equivalent of paper documents, plastic tokens and other tangible objects issued by trusted parties. At the same time, they are much more powerful than their physical counterparts. For example, individuals can selectively disclose properties of the data fields in their digital credentials while hiding any other information. Digital credentials also provide much greater security. As a result, they can be used to securely implement objects that traditionally are made identifiable in order to deal with certain kinds of fraud. Examples are diplomas, work permits, access cards and drivers' licenses.

Digital credentials were proposed in 1993 to provide a secure way to implement all these and other objects in a fully digital manner, without eroding the privacy of their holders. As said before, 'digital credentials' are meant to be the digital equivalent of paper-based credentials. An example

of a paper-based credential could be a passport, a driver's license, a membership certificate or some kind of ticket to obtain some service, such as a cinema ticket or a public transport ticket. A credential is a proof of qualification, competence or clearance that is attached to a person. Similarly, digital credentials prove something about their owner. They may contain PI such as the person's name, birthplace and birth date or biometrics information such as a picture or a fingerprint. However, because of the still evolving and sometimes conflicting terminologies used in the fields of computer science, computer security and cryptography, the term credential is used quite confusingly in these fields. Sometimes, passwords or other means of authentication are referred as credentials.

Security benefits of digital credentials are many; they are summarized as:

1. Digital credentials offer much greater security than physical non-identity (ID) objects. For example, a digital credential can contain a built-in identifier that can be uncovered by a central party only if the digital credential is shown more than a predetermined number of times.
2. Furthermore, by encoding confidential data of the applicant into a digital credential, the issuer can discourage lending of that digital credential, even though the applicant can always hide the confidential data when using the digital credential.
3. Additional security features become available when digital credentials are embedded in smart cards or other tamper-resistant devices.
4. Digital credentials also offer security benefits over digital ID certificates.

As a result of their much greater security, digital credentials can safely be used in all kinds of applications where the use of physical non-ID objects is considered insecure. That is, they can be used to implement not only gift certificates, railway tickets and so on, but also diplomas, work permits, birth certificates and other objects that traditionally identify their holder in order to deter certain kinds of fraud.

15.2.4. Data Filters to Preserve Privacy in Web Services

In the previous section, we discussed digital credentials; there also is another new approach for preserving privacy in government web services; it is based on digital privacy credentials, data filters and mobile privacy enforcement agents. Privacy credentials define the scope of access of an entity to another entity's sensitive data. Data filters use digital privacy credentials to control the access of remote entities to local data. When an entity is authorized to deliver information to another entity, mobile privacy enforcement agents guarantee that the remote entity does not violate the local entity's privacy requirements. Let us understand how data filters use digital privacy credentials—when the query is received by that DBMS, it is first processed by a privacy-preserving data filter and then submitted to the local query processor. The data filter is a module that sits between a database query engine and the communication middleware. It is composed of two modules: the Credential Checking Module (CCM) and the Query Rewriting Module (QRM). The CCM uses the credential received with the query to determine whether the sending entity is authorized to access the requested information. If the credential authorizes access to only part of the requested information, the QRM redacts the query so that the local privacy policy of the

agency and the overall privacy policy are not violated. When the query processor receives a query, it cooperates with the Privacy Profiles Manager (PPM) to generate the final result of the query. The PPM is responsible for enforcing privacy at a finer granularity than that enforced by the CCM. For example, the local CCM may decide that a given organization can have access to local information regarding a group of citizens' health records. However, a subset of that group of citizens may explicitly request that parts of their records should not be made available to third-party entities. In this case, the local PPM will systematically instruct the query processor to discard those parts from the generated result. Thus, we can see that the PPM is a translation of the consent-based privacy model in that it implements the privacy preferences of individual citizens. It maintains a repository of privacy profiles that stores individual privacy preferences. Requests made by citizens to update their privacy profiles are also handled by the PPM.

15.2.5. Understanding Web Privacy

As we can see from the discussion so far, the web is a huge repository of information. This perception of a 'passive web' ignores its inherently active nature, which is the result of the intense volume of web transactions. A web transaction is any process that induces a transfer of information among two or more web hosts. Examples include online purchases, websites browsers and web search engine use. We refer to the information exchanged as a result of a web transaction as web information. The web information type determines the extent and consequences of a privacy violation related to that information. Access to PI or sensitive information through web transactions is generally subject to privacy policies associated with that information. These policies refer to the set of implicit and explicit rules that determine whether and how any web transaction can manipulate that information.

A web transaction is said to be privacy preserving if it does not violate any privacy rule before, while and after it occurs. Privacy policies applicable to web information could specify requirements relevant to one or multiple dimensions for web privacy.

Table : Web privacy dimensions

Web Privacy Dimension	Requirements / Assurance / Guarantee
Information collection	The privacy requirement on information collection consists of ensuring that users' private information is not collected via the web without their knowledge and explicit consent. For example, a health insurance company can guarantee its web customers that it will never attempt to scan their computers to determine whether they have visited websites of companies that sell specific medicines
Information usage	Information usage defines the collected information's usage purposes. For example, consider a citizen using a web-based government medical service, which provides healthcare coverage for low-income citizens. The service's privacy policy might have an information usage component that limits the use of personal information to purposes directly related to providing health services

Web Privacy Dimension	Requirements / Assurance / Guarantee
Information storage	The storage requirement determines whether and for how long a party (such as a business) that collects private information can store the collected information. For example, an organization might state that collected customer information will remain in the underlying databases for one year after they leave the service
Information disclosure	The web privacy's information-disclosure component determines if and to whom the company can reveal collected user information. For example, a company's website's privacy policy might state that no information collected from customers can be transferred to a third party without their explicit approval
Information security	This describes the security policies and mechanisms used to guarantee the security (and thus, privacy) of information (e.g., firewalls, encryption and authentication)
Information access control	A privacy policy must state who may access what. For example, an online business's privacy policy might state that only customer service employees are allowed to access personal information of customers. The access policy must also specify the access granularity — that is, how specific entities can get when disclosing a user's information to a third party. For example, a website's privacy policy might state that while it will not disclose information about specific individuals, it will disclose only aggregated information about large populations (statistics)
Information monitoring	Systems that collect and give access to personal information must encompass a monitoring component that builds and maintains traces of all operations that input or output sensitive information. Often, these traces are the only means to settle conflicting claims regarding privacy violation
Policy changes	Privacy policies might evolve as a result of regulatory or internal business practice changes. However, these policies must not be retroactive. For example, if a website that typically collects users' personal information changes its privacy policy, the new changes must not be systematically applicable to information collected before the changes occur

Web users' PI can be classified as belonging to any of the following three types:

1. Personal data include information such as a person's name, marital status, mailing and electronic mail (e-mail) addresses, phone numbers, financial information and health information.
2. Digital behavior refers to web users' activities while using the web, including the sites they visit, frequency and duration of these visits and online shopping patterns.
3. Communication includes web users' electronic messages, postings to electronic boards and votes submitted to online polls and surveys.

Understanding web privacy requires understanding how privacy can be violated and the possible means for preventing privacy violation. There are many factors that cause web privacy violations as explained in the next section.

15.2.6. Factors that Cause Web Privacy Violations

1. **Unauthorized information transfer:** PI is increasingly viewed as an important financial asset. Businesses frequently sell individuals' private information to other businesses and organizations. Often, information is transferred without an individual's explicit consent.
2. **Weak security:** The web's inherently open nature has led to situations in which individuals and organizations exploit the vulnerability of web-based services and applications to access classified or private information. In general, unauthorized access is the result of weak security. A common form of these accesses occurs when foreign entities penetrate, for example, through hacking the web users' computers. Consequences generally include exposure of sensitive and private information to unauthorized viewers. The consequences are even more important when the attack's target is a system containing sensitive information about groups of people.
3. **Data magnets**: Data magnets are techniques and tools that any party can use to collect personal data. Users might or might not be aware that their information is being collected or do not know how that information is collected.

15.2.7. How Website Privacy Works with P3P?

P3P is an emerging standard developed by the World Wide Web Consortium (W3C) to allow a website to show their privacy policies in a standardized machine-readable format. It is intended to be used alongside human-readable privacy policies. It can be implemented on current web servers without the need to install new software. A P3P policy is generated based on your company's data collection, data usage and data retention practices. This is then written in XML and added to company's site pages. Each P3P policy contains the following details:

1. who is collecting the data;
2. what data are being collected (name, address, age, etc.);
3. what the data are going to be used for;
4. is there the option to opt in/out for certain uses (e.g., opting out of newsletters);
5. who are the data recipients (third parties with whom your data will be shared);
6. which information the data collector allows third party access to; time period for data retention;
7. how any data disputes will be resolved (e.g., by payment or by law);
8. the location of the full human-readable privacy policy (for the website).

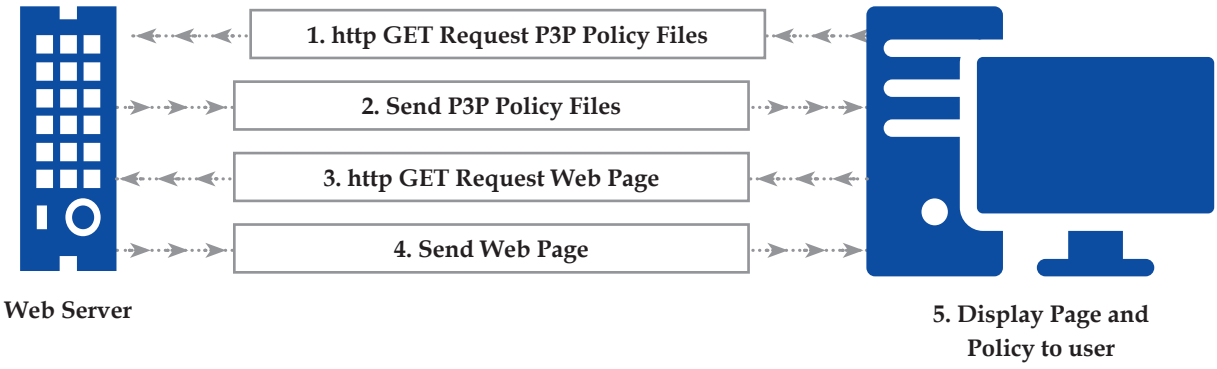


Fig. P3P - Enabled HTTP Transaction

Different statements can be given different directories, pages and cookies within a site. Note, however, that being P3P compliant does not mean that the company is complying with all the relevant data protection laws; it is merely a way to give the site visitor information regarding the company's use of data for each part of the site. There is a point to be noted on the performance aspect of a P3P-compliant website; in most cases, the first time a user visits a website, their browser will have to make one or two additional requests in order to locate and fetch the P3P policy. These requests may impose some minimal latency; however, the delay caused by this should usually be less than the delay from fetching a single image in a web page. Subsequent requests to the same site will usually not incur any additional latency owing to P3P, as long as the site's policy has not expired, how website privacy practices are followed by mature organizations based on the P3P principles.

The motivation behind P3P is to develop an industry standard that enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P assists users in understanding the privacy practices of the websites they visit before they release PI. However, it provides no' technical mechanisms that guarantee that those websites actually implement their stated privacy policy. It only provides preventive measures to preserve e-privacy. Moreover, P3P is proposed as a standard to specify the privacy of websites and not web services; it only automates the process of checking that users' privacy will not be violated when they access applications through a P3P-enabled web browser.

P3P - A Direction in Website Privacy Preservation

'P3P' is a specification that will allow users' web browsers to automatically understand websites' privacy practices. It is a technical standard developed by a diverse group of computer scientists, privacy advocates, data protection regulators and leaders in the e-commerce marketplace. At its most basic level, P3P is a machine-readable vocabulary and syntax for expressing a website's data management practices. Taken together, a site's P3P policies present a snapshot summary of how the site collects, handles and uses PI about its visitors. P3P-enabled web browsers and other P3P applications will read and understand this snapshot information automatically, compare it to the web user's own set of privacy preferences and inform the user when these preferences do not match the practices of the website s/he is visiting.

Privacy policies will be embedded in the code of a website. Browsers will read the policy, and then automatically provide certain information to specific sites based on the preferences set by the users. For instance, if the site is an e-commerce site, the browser will automatically provide shipping information. If the site is requesting demographic information, then the browser will know to provide it anonymously.

The P3P specification was developed by the World Wide Web Consortium (W3C) P3P syntax, harmonization and protocol working groups, including W3C member organizations and experts in the field of web privacy. P3P is based on W3C specifications that have already been established, including hypertext transfer protocol (HTTP), extended mark-up language (XML) and resource description framework (RDF).

P3P enhances user control by putting a website's privacy policies where web users can find them automatically, in a form users can easily understand, and, by using a common vocabulary, allows users to compare the privacy policies of the different websites they visit. Most importantly, this enables web users to act on the privacy policy information they receive. In short, the P3P-enabled web communication can bring ease, transparency and consistency to web users wishing to decide whether and under what circumstances to disclose PI. User confidence in online transactions can increase as they are presented with meaningful information and choices about website privacy practices.

15.3. Privacy in the Semantic Web

First, let us understand what semantic web is all about. The semantic web is a mesh of information linked up in such a way as to be easily processable by machines, on a global scale. You can think of it as being an efficient way of representing data on the World Wide Web (WWW), or as a globally linked database. The semantic web was thought up by Tim Berners-Lee, inventor of the WWW, uniform resource identifiers (URIs; URL is one kind of URI), hypertext transfer protocol (HTTP) and hypertext markup language (HTML). The semantic web allows two things:

1. It allows data to be surfaced in the form of real data, so that a program does not have to strip the formatting and pictures and advertisements off a web page and guess where the data on it are.
2. It allows people to write (or generate) files that explain to a machine the relationship between different sets of data.

Semantic web technologies can be used in a variety of application areas, for example: in data integration, whereby data in various locations and various formats can be integrated in one, seamless application; in resource discovery and classification to provide better, domain-specific search engine capabilities; in cataloging for describing the content and content relationships available at a particular website, page or digital library; by intelligent software agents to facilitate knowledge sharing and exchange; in content rating, in describing collections of pages that represent a single logical 'document'; and for describing intellectual property rights (IPRs) of web pages.

Now let us understand how privacy exposures arise in the semantic web. In the vision of the semantic web, the web evolves into an environment in which machines become much better able to process and 'understand' the data that they merely display at present'. In this environment, web services and web agents interact. We explained that web services are applications that expose interfaces through which web clients can automatically invoke them.

15.3.1. Digital Certificates and Privacy

We already discussed cryptography and encryption; it is a widespread misconception that the encryption of stored and transmitted data suffices to address privacy concerns. We also know addressed digital certificate and certificate authority (CA). Digital certificate is an attachment to be an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who s/he claims to be, and to provide the receiver

with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a CA. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. Under the current approach to digital certificates, individuals are given an ID certificate that will form the basis of all their-communications and transactions. The scenario is described as follows [consider this especially in light of the Health Insurance Portability and Accountability Act (HIPAA) regulation.

1. A user named John Smith receives from a CA a certificate that binds his name to his public key.
2. The certificate also specifies an expiry date and possibly other.
3. To engage in an authenticated transaction with a medical office, John Smith sends his certificate together with his own digital signature on a message that contains a unique data field. The signature prevents replay attacks and also gives the medical office cryptographically non-repudiable evidence of the transaction.
4. The medical office uses the certificate to retrieve John Smith's personal data (here, his marital status and citizenship) from various databases.
5. These databases may or may not be proprietary, and they may be online or offline.
6. The medical office also consults a revocation database to make sure that John Smith's certificate has not been revoked.
7. The business uses John Smith's certificate to look up whatever personal data it is interested in (John Smith's age, income and marital status; note that it is all sensitive information).
8. Note that the business does not need John Smith's involvement or awareness to do so, since his digital signature is not needed.

ID certificate is like an electronic version of a passport, but much more secure. However, there can be a corrosive effect on privacy. Each ID certificate can be instantaneously and automatically followed around and traced to its holder's ID as it moves through the system. This enables organizations and individuals to compile extremely precise personal dossiers, containing detailed information about a person's financial situation, medical history, lifestyle, habits, preferences, whereabouts and so on. The dossiers can be compiled, linked and updated in real time without human intervention. Moreover, individuals will be unable to repudiate their actions, because these are digitally signed by them; this results in all sorts of risks, including legislative risks. These exceptional surveillance powers are enjoyed not only by the organizations that a person directly communicates or transacts with, but also by their unscrupulous employees, hackers, intelligence agencies, private and public organizations who acquire dossiers and any organization that issues digital certificates. Typical representatives of the latter group are financial institutions, governments (local, state and federal), insurance companies, healthcare providers, post offices,

public transport organizations and consumer reporting bureaus. We summarize the disadvantages of ID certificates as follows:

1. The transaction process requires a sufficient delay to identify and correct frauds or other undesirable conditions. This may result in organizations not being able to serve as many customers as they could otherwise, or in customers leaving and going elsewhere (especially when browsing the web).
2. Because certificate holders are not guaranteed that their transactions will be authorized, there is a significant uncertainty in the transaction process. Business may be lost on the basis of erroneous or irrelevant data, or simply because the online connection fails (e.g., owing to peak load or a natural disaster).
3. In case the representatives of an organization are spread out geographically, central database verification may be expensive (owing to communication costs or the difficulty of dealing with peak load) or may simply not be an option because of the absence of network connections.
4. Requests for central database look-up may be dishonored for many reasons and may be expensive (many large databases are operated by commercial organizations such as consumer reporting bureaus). This point is related to direct marketing.
5. It is difficult for organizations to protect their online databases against misuse by hackers and intrusion by insiders. This exposes the organizations to incidents that might incur legal liability or damage their reputation.
6. The trend is for governments to require organizations that maintain databases with personal data to adhere to (legal or self-enforced) privacy standards. This adds significant compliance costs.
7. The possession of data about the personal preferences and lifestyle of individuals enables organizations to discriminate against their customers in a variety of ways. This increases the likelihood of complaints and encourages legislative action.

15.3.2. Use of Private Credentials

Although standards bodies and ID certificate providers recommend issuing ID certificates that specify a pseudonym instead of a real name, it is an ineffective recommendation. Pseudonymous certificates that can only be obtained by certificate applicants who identify themselves do not prevent tracing and linking; they are similar to SSNs, credit card numbers and health registration numbers, but with a better authentication. The alternative of not requiring certificate applicants to identify themselves offers better privacy, but is highly undesirable in most applications. The notion of private credential' is being proposed to guard online privacy of consumers who are very often subject to inroads into their private information by direct marketing agencies. Private credentials axe not only more secure and efficient than their paper counterparts, but more functional too. For instance, a private credential holder can disclose a specific portion of the data that has been encoded into a private credential, without revealing any other information; this is much like using a marker to cross out data on a paper-based certificate, but much more powerful. Also, a private credential can be presented in such a manner that the verifier is left with no evidence at all of the

disclosed property (much like waving a passport when passing customs, a practice customary in several countries) or only with partial evidence (much like presenting a paper-based certificate with crossed-out data fields so that a photocopy can be made).

Private credentials are advantageous not only to individuals, but also to organizations that rely on the verification of digital evidence. Among others, they prevent issuers and other central parties from competing unfairly, minimize the scope for law enforcement intrusions on databases, reduce the scope for discrimination and ID fraud, foster fair competition with respect to the collection and use of personal data, are the cheapest and most effective way to comply with as many of the privacy principles of codes of conduct and privacy legislation as possible, improve transaction finality and cultivate goodwill among customers. This point is to be noted with reference to privacy issues in direct marketing.

15.3.3. Web Services - Context Specifications and Context Propagations

Before taking on the discussion about privacy concerns associated with context-sensitive' web applications, let us first focus on 'context specification by understanding how context is propagated. Context propagation allows programmers to associate information with an application that is then carried along with every request. Common use-cases for context propagation are any type of application in which information needs to be carried outside the application, rather than the information being an integral part of the application. Examples of these use-cases include diagnostics monitoring, application transactions and application load balancing. Context propagation is possible using different protocols than those used by the application.

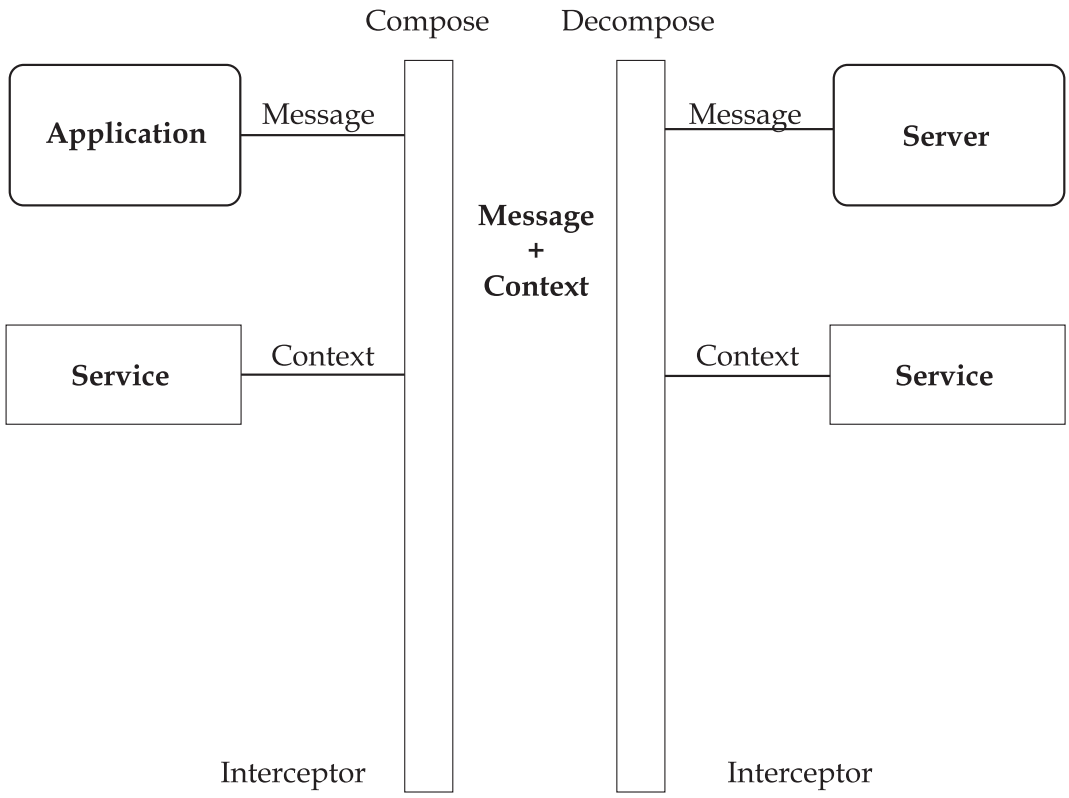


Fig. Context Propagation Protocols in Web Services

Context contains information about the execution environment of an activity that supplements information in application payloads. The first element of the Web Services Context Specification (WS-context) specification is the context structure. The context structure defines a normal model for organizing context information. Context contains information about the execution environment of an activity that supplements information in application payloads.

To appreciate much of the discussion in this section, readers need to understand what is 'service-oriented message architecture'.

Privacy Considerations in the Use of Context - Sensitive Technologies

First, we understand what 'context' and 'context sensitiveness' is about. The word 'context' has two meanings: one is the English language meaning for regular communication; in that sense, 'context' is the part of a text or statement that surrounds a particular word or passage and determines its meaning. In reference to web services, 'context' means the circumstances in which an event occurs, a setting. In computer science literature, 'context' is defined as 'the collection of nearby people and objects, as well as changes to those objects over time'. The meaning of context sensitiveness' is explained a little later in this section.

Both 'context' and 'context sensitiveness' arise in 'tracking applications'. A considerable amount of effort is expended to locate and track inanimate objects, including vehicles, equipment, cargo containers, pallets, cartons and packages. The motivations include efficiency in production and logistics, and the security of assets. Throughout Human history, measurement of human movement has been done by tracking peoples locations; although not to their (i.e., humans') liking.; and there are current attempts by a variety of commercial, law and order and other interests to increase the prevalence and intrusiveness of these activities. There is also a great deal of tracking of inanimate objects, whose underlying purpose is in part or in whole the tracking of a person whose location is reasonably inferred to be in close proximity to the object. Examples include the carriers of magnetic-stripe cards, the users of mobile phones and the drivers of commercial vehicles such as taxis and trucks.

Context Sensitiveness and Concerns Around It

'Context sensitive' refers to a program feature that changes depending on what you are doing in the program. For example, context-sensitive help provides documentation for the particular feature that you are in the process of using.

The increasing availability of information about people's context makes it possible to deploy context-sensitive services, where access to resources provided or managed by a service is limited depending on a person's context. For example, a location-based service can require an individual to be at a particular location in order to let the individual use a printer or learn his/her friends' location(s). However, constraining access to a resource based on confidential information about a person's context could result in privacy violations. For instance, if access is constrained based on a person's location, granting or rejecting access will provide information about this person's location and could violate the person's privacy.

Context Sensitiveness: Some Illustrations

Through the following examples, it is demonstrated how a naive implementation of context-sensitive access decisions to resources can lead to privacy violations. In the first example, confidential

information leaks to a service that provides information. In the second example, confidential information leaks to a person who is granted access to some other information. In the third example, confidential information leaks to a person who grants other people access to your information.

Example 1: Confidential information leaks to a service.

Assume that you let people see your current calendar entry only if they stand in front of your office, that is, you impose a context-sensitive constraint. A cell phone service provides people's location information, and a calendar service offers your calendar information. Given this setup, when someone unknown to you asks the calendar service for your calendar entry, the calendar service could learn the requestor's location while making an access decision, either by querying the location service directly or by being told by a third entity that the constraint imposed by you is fulfilled. Therefore, the requestor's location information could leak to the calendar service (i.e., to the organization running this service), and his/her privacy could be violated.

Example 2: Confidential information leaks to a person.

Assume that you allow people to access your calendar entry if you are in your office. Therefore, if somebody can retrieve this entry, s/he will also learn that you are in your office. A person planning on breaking into your house would happily take advantage of this information leak.

Example 3: Confidential information leaks to a person who grants to other people the access to your information.

Assume that you grant yourself access to your calendar entry constrained to your boss being at a particular location. When the calendar system grants you access to you entry, you will learn boss's location, which could be an information leak from your boss's privacy perspective.

Use of Context-Sensitive Technologies for Tracking People

Person tracking involves the plotting of the trail, or sequence of locations, that is or was followed by a person over a period of time. This may get used either for retrospective analysis, or it may be a 'real-time' trace, such that the surveillance knows where the person is at any particular point in time, with a degree of precision that may be as vague as a country or as precise as a suburb, a shop or a set of coordinates accurate to within a few meters. Location technologies provide, to parties that have access to the data, the power to make decisions about the person subject to the surveillance and to take action for or against their interests. These actions may be based nor only on the place where the person is, or a place where the person has been, but also on a place where the person is not, or has not been. Tracking technologies extend that power to the succession of places the person has been, and also the place that they appear to be going.

Design Issues for Context-Sensitive Applications Based on Web Services

When composing web services, the functionalities provided by the component services must be considered. We also need to ensure that data and message types, sequence logic, etc., are compatible. Consideration must also be given to non-functional requirements such as privacy, security, predictability and interoperability. For example, when composing a personalized purchasing service, we must also consider utility services such as ID management and user profiling. However, sharing and maintaining sensitive user information at the service provider's end raises privacy concerns. With some ID management services such as Microsoft's proposed passport, the user has little control over how information is shared with a service provider.

'Personalization' (of web services) is tailoring a consumer product, electronic or written medium, to a user based on personal details or characteristics they provide. Therefore, when it comes to web services architecture, especially 'personalization of web services', designers face a challenge from both security and privacy perspectives, because the distinction between functional and non-functional features is not always clear cut. Also, what is a non-functional feature to one party (e.g., security) may be a functional feature for another party (if that party happens to be a security service provider). Personalization involves a process of gathering user information during interaction with the user, which is then used to deliver appropriate content and services, tailor-made to the user's needs. Features such as privacy, performance or usability are clearly non-functional from an end-user perspective. Features such as order processing or catalog aggregation are clearly functional. When creating a personalized service, there are many non-functional features involved in addition to the functional features considered:

1. Privacy: Users need to disclose private information to the service provider, but they also want to be in control over who has access to which information.
2. Security: Users expect their PI to be protected from interception and corruption on its way to and from the service provider.
3. Predictability (online trust): Users will trust a personalized service if they perceive the query results as relevant and free of bias, and that their profile is not misused.
4. Usability: While personalization can enhance the relevance of information, it can also put a burden on users in terms of how the user profiles are collected.

15.4. Security and Privacy Aspects of Service-Oriented Architectures

We mentioned about the security and privacy challenges faced when web services are 'personalized'. Let us consider a Travel Agency service to illustrate security issues. This service provides its travel packages through collaboration with other partner services such as Airline, Hotel and Credit Card services. After finding its candidate partners (e.g., through a Discovery service), it will contact them to determine the compatibility with regards to its requirements and capabilities, and binds with the desired services. Afterwards, it will interact with its partners according to the agreements and contracts made at the binding time. In this scenario, each service (e.g., the Credit Card) should be able to communicate securely with other partner services, that is, security properties such as confidentiality and integrity should be provided considering the requirements of message exchange between services. In addition, each service should be able to protect its resources including the data that it receives from other services in its perimeter by employing some access control mechanism. Moreover, services may expose policies (e.g., security and privacy policies) that are useful for other services to understand if they can/want to fulfill the requirements of each other for binding. Then, agreements, for example, on security policies, that detail obligations and privileges of services will act as contracts that govern the interactions. Also, since the Travel Agency, Airline, Hotel and Credit Card services work closely together in this scenario, they may want to form a trusted security federation to be able to efficiently share identifications, credentials and other security-related information regarding the service execution and customer information. Based on this scenario, we identify the following security dimensions: (1) secure messaging, (2) resources

protection, (3) security properties binding, (4) contractual interactions and (5) federated trust management. Each of this is discussed as follows:

1. **Secure messaging:** Security issues in messaging for web services have much in common with those of distributed systems in general, but there are some unique problems. As with other systems, messages must be kept confidential, and their integrity must be protected while they are in transit. Other requirements include non-repudiation and authentication. Traditional security protocols such as secure sockets layer (SSL) and transport layer security (TLS, a protocol for establishing a secure connection between a client and a server) are insufficient when intermediaries are used to process messages. For instance, in the travel agency example presented in this scenario is common in web services, where intermediaries other than end recipients are expected to be present and have a role in processing SOAP messages, for example, to add properties such as reliability or verification that interaction is occurring in compliance with the specified business protocol. Indeed, a significant part of the SOAP specifications revolves around intermediaries. SSL and TLS are insufficient in this scenario, because (1) they do not permit only parts of a message to be encrypted and/or signed and (2) messages are completely decrypted and re-encrypted at each recipient. This means that it is not possible, using SSL, to send a message where different recipients can read different parts of the message and sign only portions of a message.

2. **Resources protection:** Access control can be used to protect resources from unauthorized clients. the Credit Card service provides a means for banks to inform the service about invalidated (e.g., blocked) credit cards. It is important that this functionality is only available to authorized banks; otherwise, the Credit Card service could easily be fooled into rejecting valid credit cards. For a general web service, the first resource to consider is the service itself. For example, a service can become overloaded by nonsensical and malicious requests. To protect against this form of denial of service (DoS) attacks, requests from malicious users must be filtered out. Initial solutions to this problem are available in the form of application-level. Filtering of requests is done at the application level, based on the format of the message (e.g., whether it conforms to the XML schema of genuine requests), and based on access control policies. Another resource that must be protected is the set of operations offered by the web service. Different clients will have access to different operations. For instance, in the travel agency scenario, the Travel Agency service has access to the operation offered by the Credit Card service to validate a credit card, but it does not have access to the operation that invalidates a credit card. Along with protecting access to the operations, one must consider the data objects that can be manipulated via the operations. Sometimes, requesters are allowed access to only some of the data objects that an operation can be applied.

3. **Security properties binding:** From a security point of view, partners need to verify compatibility between security/privacy requirements and assurances. Various security properties, including confidentiality, integrity, authentication and privacy, which are commonly expressed in service policies, should be captured in a format that allows automated reasoning about security properties of services. For instance, policy assertions of a Credit Card service may specify that the service require encryption of interaction messages, which digital signature standards are supported to ensure integrity and what types of credentials are recognized by the

service as proof of ID. In this context, WS-Security Policy builds on and extends WS-Policy by defining a set of policy assertions for security properties. However, these assertions are limited to the security properties, supported by WS-Security. Not focused on web services, the W3C's P3P is a language that provides an XML-based vocabulary for specifying privacy practices of a website for collecting and using data. Complementary to P3P is A P3P preference exchange language (APPEL), which allows users of websites to specify their privacy preferences. However, the lack of clear semantics of these languages makes them difficult to use effectively to allow automated reasoning about privacy properties.

4. **Contractual interactions:** Agreements that follow binding of services are implicitly or explicitly conceived as contracts that govern interactions among services. In its simplest form, port types in WSDL interfaces could be considered as a kind of implicit contract between the service provider and the client. Explicit contracts are business-level contracts that specify the relationships and roles of parties in collaboration. In fact, interaction roles, identifiable from the business protocol, could be associated with a set of obligations and privileges. Each service partner, according to its interaction roles and agreed-upon service policies, has a set of obligations and acquires a set of privileges that should be enforced according to the terms of contracts. The main challenges of contracting in SOAs are related to enforcement of obligations and auditing. For instance, in a negotiation between the Travel Agency and the Hotel services, the Hotel service may request a set of credentials, for example, the details of the customer and his/her credit card number, but does not supply or grant the expected privileges for vicious reasons, for example, cancel the transaction unexpectedly before committing it and so learn the details of the customer. It should be noted that proposals for contract enforcements such as third-party certification, reputation and credit models exist, but do not scale well in autonomous, heterogeneous, distributed and possibly dynamic environments. Automated enforcement of contracts in such environments is a far-reaching (if not impossible) objective. Besides, the possible automated support that security protocols can provide, contracts' enforcement, still requires approaches that integrate regulatory frameworks. Currently, e-business XML (ebXML) is the only effort that to some extent considers contractual agreements related to security properties in collaborations. Auditing of service transactions also helps in resolving disputes between services according to the contracts between them. However, secure and robust mechanism for auditing is required for SOA.

5. **Federated trust management:** Sophisticated security mechanisms rely on the use of credentials (also called certificates, tokens or assertions). In order to properly utilize credentials, mechanisms must be in place to issue, validate and revoke them. In a service-oriented setting, these mechanisms are provided by specialized services. For instance, such a service can be used by the Travel Agency service to determine if a traveler's passport credential is valid. The purpose of security federations is to consolidate customer IDs or accounts at various services. By sharing information about customers, composite services can operate more efficiently, and customers avoid the need to register and establish IDs at each of the participating services. Two industry standards address this issue, namely WS-Federation and the Liberty Alliance. WS-Federation builds on the WS-Trust specification and in particular on the security token service defined for managing credentials. On the other hand, the Liberty Alliance builds on

the security assertion markup language (SAML) specification and in particular on the different types of credentials (called assertions) that it defines.

We end the discussion of this section with some concluding remarks. When composing web services, the functionalities provided by the component services must be considered. We also need to ensure that data and message types, sequence logic, etc., are compatible. However, service composition amounts to much more than functional composition. Consideration must also be given to non-functional requirements such as privacy and interoperability. For example, when composing a personalized web service, we must also consider utility services such as ID management and user profiling. But maintaining and sharing sensitive user information in a utility service raises privacy concerns. So the question is where to draw the line while designing privacy-preserving web services because the distinction between functional and non-functional features is not always clear cut. Also, what is a non-functional feature to one party (e.g., security) may be a functional feature for another party (if that party happens to be a security service provider). Features such as privacy, performance or usability are clearly non-functional from an end-user perspective. Features such as order processing or catalog aggregation are clearly functional. When various features of web services interact, care must be taken during the design phase that the web services-based application does not end up violating user privacy. This is important because, often, the user trusts the intermediary, but is unaware of the privacy violation caused by information hiding.

Summary

Web services are increasingly being adopted as a viable means to access web-based applications. Government agencies collect, store, process and share information about millions of citizens who have different preferences regarding their privacy. Web technologies are driving a paradigm shift in several economic activities including B2C, B2B and government-to-citizen relationships. Web services are increasingly being adopted as a viable means to access web-based applications. The current trend in web technologies is to provide access to business and government applications through web-based services (or, simply, web services). This naturally raises a number of legal and technical issues that must be addressed to preserve citizens' privacy through the control of the information flow among different entities. Web services, and more generally SOAs, are gaining momentum as an effective framework for enabling application integration not only within but also outside organization boundaries. Many longstanding technologies embody the ability to locate and track people. During the last couple of decades of the twentieth century, new technologies have been developed with the express purpose of increasing those capabilities. These technologies are considered as serious detriment of civil freedoms. Implications are drawn for technology-using organizations, technology providers, policy makers and Privacy and Data Protection Commissioners.

According to some privacy professionals, prevailing 'data protection' or 'Fair Information Practices (FIPs)' movement has been an utterly inadequate response to the incursions of technology into personal and social freedoms. Solutions addressing this issue consist, essentially, of enforcing privacy by law or by self-regulation. In this milieu, the discussion in this chapter covered privacy issues associated with web services, owing to increasingly used business applications that utilize the underlying web services infrastructure. We also discussed the use of digital credentials and data filters to support privacy.

Stand up, be bold, be strong. Take the whole responsibility on your own shoulders, and know that you are the creator of your own destiny. All the strength and succor you want is within you. Therefore, make your own future.
- Swami Vivekananda

Case Studies

Case Study 1: Official Website of Maharashtra Government Hacked

This case study related to Website hacking. This is an incidence reported in September 2007. The impacted website was http://www.maharashtragovernment.in. A few days after the Chief Minister of the state inaugurated the new, citizen-friendly service-based web portal of the Brihanmumbai Municipal Corporation, the Maharashtra government's official website was hacked which lead to the shutting down of www.maharashtra.gov. The state officials, however, said that there was no data lost and that there was no serious damage to the website. State Officials further stated that the website gets updated daily with information on various government regulations and decisions, and supports links to all government departments. However, IT experts had to restore the official website of the Government of Maharashtra, having succumbed to the attack by the hacker.

As per reports, the site was attacked early in the morning by a person or a group proclaimed as "cool-hacker." The hacker left an imprint of a hand on the hacked website. The state's information and technology department came to know about the incident next day morning. They immediately blocked all access to the website. The IT department has lodged an FIR (First Information Report) with the police in an attempt to trace the culprit.

Joint commissioner of police, in his official remark, stated that the state's IT officials lodged a formal complaint with the cybercrime branch police following this incidence. He expressed confidence that the hackers would be tracked down. The Commissioner also mentioned that the hacker had posted some Arabic content on the site. According to sources, hackers were suspected to be from Washington. IT experts gave to understand that the hackers had identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia. Officials further added that this might be a red herring to throw investigators of their trail. For those who are not familiar with the term "red herring," it refers to the tactic of diverting attention away from an item of significance.

The State Government website contained detailed information about government departments, circulars, reports and several other topics. IT experts, who were assigned to work on restoration of the website, told Arab News that they feared that the hackers may have destroyed all of the website's contents. The worrisome part was that according to a senior official from the State Government's IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall. However, state officials denied there being any data loss or any serious damage to the website. The officials said that the hacker could only manage to damage the homepage.

Point to note here is that the website was hacked for the second time in the past two weeks, the fourth time since July 2007. The previous attack took place on 5 September 2007. This incidence of repeated attack on the website underscores the need for security measures being in place (intrusion detection system – IDS, intrusion prevention system – IPS and firewalls).

Case Study 2: E-Mail Spoofing Instances

This is an example E-Mail bombing. An American teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misleading information was spread by sending spoofed E-Mails purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth emerged, the values of the shares could not be restored to the earlier levels. This resulted in thousands of investors losing a lot of money. This can be considered as a cybercrime against an organization because the impacted organization was the one about whom false information was spread.

There is another example of E-Mail Spoofing incident in India. A branch of the Global Trust Bank experienced a customer run-down on the bank owing to a certain rumour spread about the bank not doing well financially. Under panic, many customers decided to withdraw all their money and close their accounts. It was revealed later that someone had sent out spoofed E-Mails to many of the bank's customers announcing that the bank was in a very bad shape financially and could close operations any time. In the next few days, unfortunately, this information turned out to be true. So, can we say that this instance of E-Mail Spoofing saved many customers?

Another shocking example of the E-Mail Spoofing involves a former executive from a well-known company in the state of Gujarat. The executive faked himself to be a lady by adopting a false name. He then created a fake E-Mail ID. Using that ID, the executive contacted a businessman based in the Middle East. The executive posing as a woman then went into a long cyber courting relationship with the Middle East businessman. During this "cyber dating," the executive used to send many "emotional blackmailing" messages to the businessman. One such message threatened the businessman that if he ended this relationship, "she" (i.e., the executive posing as a woman) would end her life! What is worse, the executive gave another woman's E-Mail ID to the businessman. This too was a non-existent address. When the Middle East businessman sent a mail at that ID, he was shocked to learn that the executive (who presented himself as a woman) had died and that now the police was searching him as the suspect in that death case! Using this trap and trick the executive exhorted from the businessman several hundred thousands of Indian Rupees threatening that the businessman would get exposed if he did not part with that money. The executive also sent E-Mails to him from different E-Mail IDs making the poor businessman believe that they were mails from high court and police officials. All this was done to extract more money from the gullible businessman. Finally, businessman flew to India to lodge a case with the Police. Internet users indeed enjoy "anonymity" and can get away with many things.

Case Study 3: E-Mail Bombing Involving a Foreigner

This example brings out an instance based on E-Mail bombing. A foreigner had been residing in Shimla, India for almost 30 years. He wanted to avail a scheme that was introduced by the Shimla Housing Board to buy land at lower rates. His application, however, was rejected on the grounds that the scheme was available only to Indian citizens. Feeling furious, the foreigner decided to take revenge. He transmitted thousands of mails to the Shimla Housing Board. He did not stop there. He kept on sending E-Mails till their servers crashed. An interesting question is which law of the land would have been used for filing a case against this non-Indian person.

Case Study 4: I Love You Melissa – Come Meet Me on the Internet

This example involved the VBS_LOVELETTER virus - also known as the Love Bug or the ILOVEYOU virus. It is said to be written by a Filipino undergraduate. In May 2000, it was proven that this virus is deadlier than the Melissa virus and it became the world's most prevalent virus. It impacted one in every five personal computers in the world. When the virus was brought under control, the true magnitude of the losses was unbelievable. The attack from this virus caused losses to the tune of almost US$ 10 billion. It is interesting to see how the virus works. The original VBS_LOVELETTER thrived on the addresses in Microsoft Outlook. It utilized that address book and E-Mailed itself to those addresses. The E-Mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER- FORYOU. TXT.vbs." Even with such dubious sounding subject line, even those who had some knowledge of viruses did not notice the tiny .vbs extension. People believed the file to be a text file and this mail also fooled people who are wary of opening E-Mail attachments. The message in the E-Mail read as follows: "Kindly check the attached LOVELETTER coming from me."

Since the initial outbreak, over 30 variants of the virus have been developed, many of them following the original by just a few weeks. The Love Bug propagates itself using the Internet Relay Chat (IRC). It E-Mails itself to users in the same channel as the infected user. However, unlike the Melissa virus this virus does have a destructive effect. The Melissa virus, once installed, merely inserts some text into the affected documents at a particular instant during the day. On the other hand, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. Thus, it succeeds in creating ever- increasing versions of itself, that is, self-propagation mode. The world's most famous worm probably was the Internet worm let loose on the Internet sometime in 1988 by Robert Morris. At that time, the Internet was in its early formative and developing years. The Internet worm affected thousands of computers and almost brought Internet development to a complete halt. It took a team of experts several days to get rid of the Internet worm and in the meantime many of the computers had to be disconnected from the network.

Case Study 5: The "Piranhas" Tragedy with Children

It is related to Web Jacking. This incident was reported in the US. There was a hobby website for children. The owner of the site received an E-Mail informing her that a group of hackers had gained control over her website. They demanded a ransom of one million dollars from her. The owner was a school teacher. She did not pay due attention to that (threatening) mail because she did not think it was serious. She thought it was just a scare tactic and so she simply ignored the E-Mail. After about three days, she started getting several telephone calls from almost all over the country and then she came to know that the hackers had really web jacked her website. The hackers had altered a portion of the website which was entitled "How to have fun with goldfish." They had replaced the word "goldfish" with the word "piranhas." Piranhas are tiny but extremely dangerous flesh-eating fish! It was sad because, the fatal result of this apparently minor sounding "find-and-replace" cyberprank was terrible. Many children who visited the popular website believed what the contents of the website suggested. These unfortunate children did not realize what would be in their fate. They followed the instructions to try playing with piranhas, which they bought from pet shops and were very seriously injured!

Case Study 6: Doodle me Diddle!

This is a real-life example of "Data Diddling" technique. Indian Electricity Boards suffered as victims of data diddling. Such programs got inserted when private parties were computerizing their systems. The NDMC Electricity Billing Fraud Case in 1996 is a typical example. The computer network was used for preparing receipts and for keeping the accounts of electricity bills by the NDMC, Delhi. Money collection, computerized accounting, record maintenance and remittance in the bank were outsourced to a private contractor who was a computer professional. He misappropriated vast amount of money by manipulating data files to show less receipt and bank remittance. As we know, this kind of attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Case Study 7: Ring-Ring Telephone Ring – Chatting Sessions Turn Dangerous

Here is a real-life example of Cyberstalking crime which was registered with Delhi police. "Stalking" is defined as "pursuing stealthily." As we learned, "cyberstalking" means following a person's activities, that is, a person's navigation across the Internet by posting messages (sometimes even threatening messages) on the bulletin boards that are visited by the victims, entering the chat rooms frequented by the victim, constantly bombarding the victim with E-Mails, etc. Richa Sharma was the first lady to register a cyberstalking case. Her husband's friend provided her a telephone number in the general chat room. Some websites do provide general chatting facility (e.g., websites like MIRC

and ICQ) where a person can easily chat without revealing his/her true identity. The friend of Ms. Sharma's husband also encouraged chatters to speak in profane language to Ms. Sharma. As a result, Ms. Sharma received more than 30 calls in 3 days and many chatters contacted her. Almost all of the calls were made to her at odd hours from all over India and a few of the calls came in from outside India too. This created havoc in the personal life of Ms. Sharma and caused her much mental stress. She got fed-up with these calls and chat drama and complained to the police against a person who she felt was using her identity to chat over the Internet at the website www.mirc.com. In her complaint, Ms. Sharma mentioned that the person was chatting on the Net using her ID and also complained about the obscene language used by that person while chatting with her. Ms. Sharma, further complained that the same person was deliberately giving her telephone number to other chatters, asking them to call her at odd hours.

Case Study 8: Young Lady's Privacy Impacted

This comes under the Trojan, viruses and other malware Section. We should be careful, else untoward things can happen as illustrated by this example. A young magazine journalist in Mumbai was working on an article about online relationships. The article was about how people can easily find friendship and even love companions on the Internet. During the tenure of her research work, she happened to make a lot of online friends. One of these "friends" (ill-minded, unfortunately for the young lady) managed to infect her computer with a Trojan. The young journalist lady lived in a small, one-bedroom apartment and her computer was located in a corner of her bedroom. She had the habit of never powering off her computer. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. A year later she realized that hundreds of her "private" pictures were posted on pornographic sites around the world! Her fiancé broke the engagement and the young lady was thrown into suicidal depression.

Case Study 9: Job Racket Exposed by Mumbai City Cybercrime Cell

This example illustrates how cybercriminals use Smishing to cheat people. This case happened in the year 2009. Himesh Kapadia, aged 26 years, received an SMS offering him a job in Marriot Hotel. Himesh, in response, eagerly mailed his resume. He also deposited over ₹1.7 lakhs (₹1,70,000) as per the instruction of a person who claimed to be a London diplomat. Himesh grew suspicious when he was asked for additional money and finally approached the cybercrime cells of the Mumbai Police. The investigations resulted in the arrest of a couple and five Nigerians allegedly involved in cheating people by promising them housekeeping jobs in Marriot Hotel, London. While the Nigerians, posing as London diplomats, would send SMSs and E-Mails offering jobs in the hotel, the couple operated the bank accounts.

As Himesh recalls, in September 2009, he began exchanging mails with James Richard who claimed to be a London diplomat. He had asked Himesh to pay differing sums of money. Even after paying over ₹1.7 lakhs (₹1,70,000) he continued to exhort more money from Himesh. The police directed the bank authorities to block the account holder's ATM facilities. In last week of November 2009, the bank informed the police that a couple approached the bank to withdraw money from the account. Mumbai Police arrested the couple and later the Nigerians who came looking for them to collect the money.

Case Study 10: Indian Banks Lose Millions of Rupees

This is a real-life example showing the techniques used by cybercriminals. Banks across the country lost ₹6.57 crore (₹6,57,00,000) to Internet frauds in 233 incidents of cybercrime, with Tamil Nadu topping the list in last fiscal year. ₹2.09 crore (₹2,09,00,000) has been lost by various banks in the Indian state of Tamil Nadu in seven cases reported between April and December 2008. The lending

institutions in Maharashtra had reported the highest number of incidents, 23 in all. They lost ₹55.54 lakhs (₹55,54,000) to online fraudulent practices. This was revealed by the erstwhile Minister of State for Home told the Lok Sabha in February 2009.

The banks in other Indian states – Andhra Pradesh, Rajasthan and West Bengal – lost ₹89.93 lakhs (₹89,93,000), ₹64.29 lakhs (₹64,29,000) and ₹35.72 lakhs (₹35,72,000), respectively, while Kerala and Delhi lost ₹17.60 (₹17,60,000) and ₹10.90 lakhs (₹10,90,000), respectively, owing to cyber frauds. A total of 11 cases of Internet frauds were reported from Andhra Pradesh, 8 from Delhi, 7 from Tamil Nadu, 6 from Karnataka and 5 from West Bengal during the said period. Surprisingly, banks in Bihar, Goa and Jharkhand did not lose a single penny to such activities and no case was reported from any of these states. The Minister presented a state-wise list of number of incidents of Internet frauds that includes cases of fraudulent withdrawal of money from banks through Internet/online banking, as reported by the banks to the Reserve Bank of India. According to a data updated till 2007, out of the total 355 people arrested across the country, a maximum 156 people were arrested in Madhya Pradesh in connection with cheating- related cases under IT Act – Fraud digital signature (Section 64) and Breach of Confidentiality/Privacy (Section 72) – and IPC Crime (Forgery and Criminal Breach of Trust/Fraud). The highest numbers of cases, 153, were also registered in Madhya Pradesh for forgery and Criminal Breach of Trust/Fraud out of the total of 302 cases in the said period. Similarly, a total of 41 incidents – 38 under IPC crime and 3 under IT Act – were reported in Chhattisgarh for cyber frauds. A total of 59 people were also arrested in Andhra Pradesh, 36 in Punjab, 16 in Andaman and Nicobar Island and 4 in Delhi in connection with cheating-related incidents in 2007. The amount lost to cyber frauds during April 2007 and March 2008 were ₹5.58 crore (₹5,58,00,000) and 374 people were arrested in this connection.

Case Study 11: Infinity E-Search BPO Case

This case brings to the fore the emerging threat arising from "sale of personal information". We learn here that the definition of "sensitive personal information" is very important for organizations to be clear on what they wish to protect from theft. This is especially important for the BPO (business process outsourcing) organizations to whom the clients entrust their confidential data.

A fraud discovered at a Gurgaon-based BPO created an embarrassing situation for Infinity E-Search, the company in which Mr. Kapoor was employed. A British newspaper reported that one of its reporters had covertly purchased personal information of 1,000 British customers from an Indian call-center employee. However, Mr. Kapoor, the employee of Infinity E-Search (a New Delhi-based web designing company) was reportedly involved in the case, denied any wrong-doing. The company also said that it had nothing to do with the incident.

It so happened in this case that the journalist used an agent, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data was itself not substantiated by the journalist. In this kind of a situation we can only say that the journalist used "bribery" to induce an "out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention. This example breaks the misconception that BPOs in India are not covered under the Information Technology Act and Amendments thereof.

Case Study 12: Charged for Computer Intrusion

This example is related to Computer Network Intrusion. The story of this incident was released in 4 November 2009. Scott R. Burgess, aged 45, Jasper, Indiana, and Walter D. Puckett, aged 39,

Williamstown, Kentucky, were indicted for computer intrusion. This was announced by Timothy M. Morrison, US Attorney, Southern District of Indiana, after an inquiry by the Federal Bureau of Investigation (FBI) and the Indiana State Police.

It is alleged that Burgess and Puckett accessed the Stens Corporation computer systems, based in Jasper, Indiana, from various places on approximately 12 different occasions without authorization. It was further alleged that the computer intrusions were performed for the purpose of gaining commercial and personal financial benefits. Furthermore, it was alleged that Burgess and Puckett were working for a business competitor of Stens at the time of the intrusions.

A maximum of 5 years imprisonment with $250,000 fine is what Burgess and Puckett had to face. An initial hearing was scheduled before a US Magistrate Judge. However, an indictment was only a charge and is not an evidence of guilt. A defendant was presumed innocent and was entitled to a fair trial at which the government must prove guilt beyond a reasonable doubt.

Case Study 13: Small "Shavings" for Big Gains!

This incident, involving a Salami attack-like technique, was published on 17 September 2009. Michael Largent, aged 22, resident of Plumas Lake area, was sentenced to 15 months in prison and compensation of over $200,000. This was the punishment given by the US District Judge Morrison C. England Jr. for fraud and related activity in connection with computers. After release from prison, Largent also had to face 3 years of strict restrictions due to illegal use of computers and the Internet. This case was jointly investigated by US Secret Service and the FBI. The US Attorney's Office for the Northern District of California, San Jose Division, also assisted with this case.

The case was prosecuted during the period November 2007 through May 2008. The prosecution was done by the Assistant US Attorney Matthew D. Segal, who worked as prosecutor in the office's Computer Hacking and Intellectual Property (CHIP) unit. According to Attorney Mathew, the accused Michael Largent developed a computer program allowing him to defraud a few companies such as "E-Trade," "Charles Schwab & Co." and Google by opening or attempting to open more than 58,000 brokerage accounts. He did this to steal the "micro-deposits." Michael knew that a financial institution make a micro-deposit when an account is opened to test the functionality of an account. The amounts deposited in this case were in the range $0.01 to $2.00.

To cover his identity, Michael Largent used false names, addresses, driver's license numbers and social security numbers, including the names of known cartoon and comic book characters to open the accounts. When the deposits took place, he would divert the funds into his own bank accounts or onto prepaid debit cards, without the authorization or knowledge of his victims. As a result, Michael Largent fraudulently obtained or attempted to obtain tens of thousands of dollars which he used for personal expenses.

Two organizations, namely, E*TRADE (E-Trade Financial Corporation) and Charles Schwab & Co. Inc., in parallel notified the law enforcement agency when they detected the fraud. Assistant US Attorney Robin R. Taylor, also of the CHIP unit, brought the criminal complaint and the indictment in this case in May 2008 and Segal took over in January 2009. In sentencing, Judge England observed that Michael Largent's scheme took some sophistication, and wondered why he had not used his skills and talents in a lawful way.

Case Study 14: Man Goes Behind Bars for Computer Fraud Offense

Here is another example similar to the previous one. This example shows the hazards of not monitoring remote access permissions and the consequences of perhaps too much faith placed in the

"insiders" with a naive belief that the "insiders" would never bring harm to their organizations. The ill use of administrator account and password also comes to the fore. There are tremendous learning implications for organizational information security practices. Noteworthy is the nature of punishment given to the guilty thereby creating an opportunity for remorse and also to morally guide others to avoid his wrong-doing. Read on for further details on this case. Jeffrey H. Sloman, US Acting Attorney for the Southern District of Florida, and Jonathan I. Solomon, Special Agent in Charge (from FBI, Miami Field Office) announced that defendant, Lesmany Nunez, on 14 July 2009, was sentenced by Chief US District Judge Federico A. Moreno to 12 months and 1 day imprisonment after pleading guilty to computer fraud, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii). Upon his release from prison, Nunez was ordered to serve 3 years of supervised release, with a special condition that he performs 100 hours of community service by lecturing young people on the implications of hacking into other people's computers and networks. Nunez was also ordered to pay $31,560 in restitution.

As per the facts revealed during in-court statements, Nunez, aged 30, was a former computer support technician at Quantum Technology Partners (QTP), located in Miami-Dade County. QTP provides services such as data storage, E-Mail communication and scheduling for their client companies. Late Saturday night, Nunez remotely accessed QTP's network without authorization, using an administrator account and password. He first changed the passwords of all of the IT system administrators and then he shut down almost all of the QTP servers. What is more, Nunez also deleted files. Had he not done that, it would have been possible to re-install the data from backup tapes much easily and in less time. As a result of Nunez's malformed acts, QTP and their clients could not perform their normal business functions for a number of days, suffering a tremendous business loss.

As a result of the unauthorized access to the system and the deletion of data, QTP suffered over $30,000 in damages. This included the cost of responding to the offense; conducting a damage assessment; restoring the data, system and information to their previous condition; and other costs incurred due to the interruption of network services. Through forensics investigations, Nunez was identified as the perpetrator. Investigators found that the activity on QTP's computer could be traced to his home network. Additional evidence was also found subsequently when they performed a search of his computer.

Case Study 15: Software Developer Arrested for Launching Website Attacks

This real-life example shows the crime by a young software engineer who launched a series of "denial-of-service attacks" on various websites. It shows what misled/confused youth can do and in turn, how they become cybercriminals by embracing false motives. It is a reflection of rapidly changing values in our society. Forensics comes the fore in the example.

Bruce Raisley, aged 47, was a software developer from Monaca, Pennsylvania, when he was charged with the offense of computer fraud and abuse. He quietly surrendered to the FBI on 1 July 2009. More specifically, Bruce was charged with the unauthorized access of protected computers with the intention of causing denial-of-service and/or losses to the websites. A number of websites were impacted – among them were, RollingStone.com and the website of Rick A. Ross Institute of New Jersey (Rick Ross Institute), based in Hudson County, NJ, who run the Internet archive service "for the study of destructive cults, controversial groups and movement" and "Perverted Justice," a Portland, Oregon-based organization (operated by X. E.). Perverted Justice is an organization that seeks to identify and expose pedophiles and sexual predators targeting minors.

Around 2004, Bruce had volunteered for "Perverted Justice." Perverted-Justice.com. mentioned before, is a loosely organized group of computer gamers, students and the occasional well-meaning

but misguided "reactionary" who claimed that their primary purpose was to bring about the complete destruction of the lives of anyone they believe is guilty of chatting with one of their "baiters." Their baiters troll Internet chat rooms pretending to be young teen-aged girls in the hopes of entrapping men into sexually suggestive conversations. Once targeted, members of "Perverted Justice" organization search the Internet for all available information to publicly identify the "target," along with complete information about the target – the family, target's employer, friends, associates, neighbors, etc. Next, they launch a brutal harassment campaign against anyone listed on their site via phone calls, Internet messages, E-Mails, neighborhood flyers, etc. Another impacted organization was Corrupted-Justice.com – a civil rights advocacy organization. It is a group of like-minded people who are dedicated to bringing about an end, using legal means, to the harassment and terrorism being perpetrated by the vigilante group. In this case, host of attacks were mounted on Corrupted Justice, an organization whose stated purpose is claimed to educate the public on the actions of various purported cybervigilante groups, including perverted Justice. In year 2006 or around that time, Bruce had become a member of "Corrupted Justice," after becoming disenchanted with Perverted Justice!

According to the criminal complaints received, in September 2006 and July 2007, Radar Magazine and the Rolling Stone published two separate articles ("Strange Bedfellows" and "To Catch a Predator": The New American Witch Hunt for Dangerous Pedophiles). Both articles presented positive and negative views on the activities conducted by "Perverted Justice" and its volunteers. The articles described what was termed as "questionable tactics" by Perverted Justice to silence critics. One of these tactics was an episode between X.E. and Bruce. In or about 2007, Strange Bedfellows was reprinted on numerous websites.

Case Study 16: CAN-SPAM Act Violation through E-Mail Stock Fraud

This comes under Spamming. Here is a real life happening on that. This example involves the CAN-SPAM Act. The full form of CAN-SPAM Act is "Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003." Five individuals pleaded guilty on 23 June 2009 in the federal court in Detroit for their involvement in a wide-ranging international stock fraud scheme that had the illegal use of bulk commercial E-Mails or "spamming." Considering the advanced age of one of the fraudsters in this example, we can say that just like cybercrime knows no national boundaries, criminals seem to have no heed to their age!

Alan M. Ralsky, aged 64, and Scott K. Bradley, aged 38; both pleaded guilty to conspiring to commit wire fraud, mail fraud and of violating the CAN-SPAM Act. This act defines a "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." It exempts "transactional or relationship messages." Ralsky and Bradley also pleaded guilty to "wire fraud" and "money laundering" apart from the violation of CAN-SPAM Act. Under the terms of his plea agreement, Ralsky acknowledged facing up to 87 months in prison and a $1 million fine under the federal sentencing guidelines while Bradley acknowledged facing up to 78 months in prison and a $1 million fine under the federal sentencing guidelines.

Case Study 17: Business Liability through Misuse of Organization's Information Processing Assets

This example is a real-life scenario of how criminals can create false E-Mail IDs. In one bank, a management trainee of the bank was engaged with a girl working in the same bank. They were to get married in due course of time. During the post-engagement period, the couple exchanged many E-Mails; however, the boy and the girl used to write the mails during work hours using the company

computers. Unfortunately, after some time the relationship went sore and the two broke up. The girl created fraudulent E-Mail IDs such as "indian bar associations." She used that ID to send E-Mails to the boy's foreign clients. The girl used the bank's computer for sending these mails. The mails had negative publicity about the bank. The boy lost a large number of clients assigned in his portfolio. Moreover, those clients sued the bank. The bank was held accountable for the E-Mails sent using the bank's system. This small example is a lesson – organizations must have well-established computing guidelines and strict vigilance on how organizations computing and communication facilities are being used.

Case Study 18: Parliament Attack

This example illustrates the Forensics fundamentals scenario in which it was used. Bureau of Police Research and Development (BPRD) at Hyderabad handled some of the top cyber cases. One such case involved analyzing and retrieving information from the laptop recovered from terrorists, who attacked the Parliament. The laptop was seized from the two terrorists, who were gunned down when Parliament was under siege on 13 December 2001. Police sent the seized laptop to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. Inside the laptop there were a number of evidences that established the motives of the two terrorists, namely (a) the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and (b) the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. It was also found that the emblems (of the three lions) were carefully scanned and the seal was also deviously made along with residential address of Jammu and Kashmir. But careful forensics detection proved that it was all forged and was created using the laptop.

Case Study 19: Game Source Code Stolen!

Source code theft is considered as an IPR theft (IPR is Intellectual Property Rights) and this example is about source code theft in real life. Given the life style and preferences of the young generation today, one can understand the popularity of game software packages. Game software can be loaded on the mobile handsets as well. It is an episode of IPR theft that took place in 2003.

It so happened that a computer user in China obtained the source code of a popular game "Lineage I" from an unprotected website. This proprietary code was then sold to several people in 2004. One of those people set up a website, www.l2extreme.com, to offer the "Lineage" game at a discount. After noticing this, the South Korean company that owned the Lineage source code sent legal warnings. However, in spite of those warnings, the suspect did not shut down the site. He rented powerful servers – enough to accommodate 4,000 simultaneous gamers and solicited donations from users to help defray the costs. The loss in potential revenues for the South Korean company was estimated at $750,000 a month. The US FBI arrested the suspect and the website was shut down.

Case Study 20: The Petrol Pump Fraud

Thank God that in India, we do not as yet have the system of automated petrol pumps! This feeling of relief comes after reading this example of fraud. The fraud took place in a petrol pump in the US. In India, it is a common practice to keep an "eye" on the delivery of petrol (of course, assuming that the pump has been calibrated and periodically inspected to ensure that it is dispensing as it should). The example here can be considered as "Salami Technique" example, because things got discovered based on "little-by-little" happening! Here is how that happened.

Four men in Los Angeles, US, were charged with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem was noted

when a rising number of consumers complaints were received which claimed that they had been sold more gasoline than the capacity of their gas tanks! However, the fraud was dificult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for 5 and 10 gallon amounts (precisely the amounts typically used by inspectors).

Case Study 21: Xiao Chung's Story – Life of a Hacker

We mentioned about "motives" for hacking. Here is story of young hacker Xiao Chung (he has got another pet name in the dark world of the ace hacker community but it is kept confidential) who seemed eager to tell his story. Like many hackers, he wants recognition for his hacking skills even as he values anonymity to remain un-detected. The New York Times found him through another well-known hacker who belongs to a hacker group and who vouched that Xiao Chung is too skilled. On condition that he should not be identified by his real name, Xiao agreed to allow a reporter to visit his modest home in a poor town outside Changsha, and watch him work. It is quite eerie – just a few quick keystrokes and Xiao Chung proudly brings up a screen displaying his latest victims. He says with a quite a wicked smile, "Here's a list of the people who've been infected with my Trojan Horse, and they don't even know what's gone wrong with them!" You may think that Xiao may be earning a lot from his craft; but that is not true. For all the seemingly terrific power in his hand to "affect" so many people, the hacker has a modest living - he works from a dingy apartment on the outskirts of this city in central China.

Case Study 22: Killers Take Tips from 26/11 Attack to Use VOIP

Here is a real-life incidence involving cyber terrorism in the country that has just about settled from the shock of 26/11 attacks on Mumbai. Those attacks revealed the wireless communication technology used by the terrorists. This real-life example comes from that background. E-Mail forensics is already explained – fully aware that electronic mails can be traced, cybercriminals as well as terrorists adopt a technique whereby they do not send attack-related mail and yet they communicate with their counterparts. This real-life example shows how that technique was used.

Investigations in the murder of criminal lawyer Shahid Azmi revealed that the killers had used communication techniques similar to the ones used by terrorists during the 26/11 terror attacks and the 11/7 train blasts. According to crime branch sources, gangster Bharat Nepali, who had hired men to eliminate Azmi, had used Voice over Internet Protocol (VoIP) system to communicate with the killers. During the investigations it was revealed that at least six calls were made, before and after Azmi's murder, using VoIP service from Hong Kong, Los Angeles, London and Israel. The usage of VoIP for criminal activity came to light during the 26/11 terror attacks in Mumbai. Handlers of the terrorists, who attacked the city on the night of 26 November 2008, were found to be using VoIP service to communicate with the 10 men who laid siege at various locations in the city.

Case Study 23: "Robberson" Brothers Caught for Selling Pirated Software

Investigation of Maurice A. Robberson and his brother Thomas Robberson was commenced by BSA (Business Software Alliance). In early 2002, BSA had received complaints from software publishers and that was the basis for the investigation. After reviewing the reported websites, BSA made undercover purchases and determined that the software sold was pirated. After this, BSA referred the case to the Federal Bureau Washington Field Office. The FBI Field Office conducted independent investigation and subsequently shut the operation down in October 2005. The investigation determined that starting in late 2002 the Robberson brothers sold more than $5 million of counterfeit software products. In addition to running four for-profit websites, the Robberson brothers were also co-conspirators with Danny Ferrer in the operation of www.BbuysUSusA.com.

It turned out from the investigations that, during the operation of the websites, Thomas Robberson grossed more than $150,000 by selling software with a retail value of nearly $1 million. Maurice Robberson amassed more than $ 855,000 through sales of software with a retail value of nearly $5.6 million. In March 2008, Maurice Robberson was sentenced to 36 months in prison, whereas his brother Thomas was sentenced to 30 months. Both were also ordered to undergo an additional 3 years of supervised release and pay restitution.

Case Study 24: BSA Uncovers Software IPR Breaches

This is a glaring example of software piracy as Intellectual Property Offense. This is one more example of the breach uncovered by BSA happened in Georgia State, US, in July 2008. It involved interaction with eBay. Launched in 1995, eBay started as a place to trade collectables and hard-to-find items. Today, eBay is a global marketplace where institutional buyers as well as individuals can buy and sell practically anything. You do not have to register to take a look at what's available, but you will need to register if you want to buy or sell. Today, eBay is the world's online marketplace – it is a place for both buyers as well as sellers to come together and trade almost anything. People use such facilities for the convenience, at times overseeing the risks involved as we learn in this example.

A woman was stopped from selling counterfeit copies of Corel software on eBay. An investigation revealed that she had sold more than $212,000 worth of unlicensed software to hundreds of consumers, in the period January–May 2008. A $250,000 civil judgment was entered against her. In another episode of similar kind, uncovered by BSA, a person from yet another state was found to be involved. Jon Crain of Coraopolis, Pennsylvania, operated nearly 20 websites distributing unlicensed copies of Adobe, McAfee, Microsoft and Symantec software online. He was first targeted in March 2007 as part of an international legal action against five software pirates. The other offenders were located in the UK, Austria, and Germany. In many of these cases, BSA was alerted to the illegal activity by reports or complaints from disappointed consumers who were initially attracted by low price deals. BSA sued Crain, and a civil judgment was entered that included a hefty settlement payment and a requirement to remove the unlicensed software from his website.

Another example is this incidence that took place in July 2008. Jeremiah Mondello, a 23-year Oregon man, was sentenced to 4 years in federal prison for selling more than $1 million worth of pirated software and distributing malware via instant message networks to steal financial data from dozens of consumers. He then used the stolen bank account credentials to set up more than 40 online auction accounts in the victims' names and withdraw money from their debit accounts. In addition to the prison sentence, federal investigators also seized computers and $220,000 in cash from Mondello. The government also was entitled to seize his home and surrounding land.

Case Study 25: Pune City Police Bust Nigerian Racket

This story had appeared in Pune Mirror dated 25 October 2010. Name of the victim has been masked to respect the privacy of the person. However, all the events mentioned here are real and are presented exactly as they happened, as mentioned in the chain of events mentioned here is as at the time of writing this. What is described here is a real-life example of that. This example re emphasizes the need for cybercrime awareness. As you can see in this example, even an educated person working in technology field got fooled by the perpetrators and suffered a big financial loss. It also shows the greed of criminals.

The police succeeded in nabbing two suspects in this fraud case. This fraud happened when the police started probing into a complaint received from a young software engineer working in Pune city.

Arjun Changaokar, a resident in Warje area, was duped into parting with ₹10.27 lakhs (₹10,27,000) by making him believe that he was going to be offered a high profile job in a London hotel called New Climax. In an E-Mail chat with an alleged UK-based Councillor, Arjun, the techie from Rajiv Gandhi Infotech Park at Hinjewadi, was convinced to pack up and leave India for UK! The fraud got exposed when Arjun found that there was no flight to UK from Indira Gandhi International Airport at the time he was told by the conmen! The efforts expended by Warje police were successful and two perpetrators, including a bank account holder, were arrested. However, the real mastermind Chong-Ching, who is a foreign national, was still absconding. A special squad of cyber experts has been investigating the Nigerian fraud racket run from Meera Road. The three accused in the FIR (First Information Report) filed by the victim include Shailendra Ramesh Soni, aged 24, a resident of Shivajinagar in Govandi in Mumbai, Naresh Shubrakaran Sharma, aged 27, a resident of Queens Park in Mira-Bhayandar in Thane and Chong-Ching, the foreign national whose complete name and address could not be traced (as at the time of writing this). The fraud took place during the period 26 July–24 September 2010. The accused have been charged under various sections of the IPC (Indian Penal Code – see Appendix P in CD) and the Indian IT Act (see Appendix O in CD) for cheating and conspiracy using Information Technology.

As per complaint filed by the victim Arjun Changaokar, the fraud started with the mail he received on 26 July 2010. In that mail he was offered a job in UK-based hotel "New Climax." A person calling himself Chong-Ching claimed to be authority at the hotel and offered to victim the post of Sales Supervisor with a handsome UK salary. The victim responded to the E-Mail and accepted the offer. There onward, the correspondence continued. In another E-Mail, a person called John Smith Levis introduced himself as UK councillor. John claimed to have been given the responsibility by the hotel to provide Visa. To get the Visa and to pay for journey expenses and accommodation in the UK, John asked the victim for various amounts of money in a number of E-Mails. John gave to the victim several account numbers in different branches of Axis Bank and ICICI Bank. Victim Arjun deposited those amounts ranging from ₹2 to 5 lakhs (₹2,00,000 to 5,00,000) on different occasions. Over a 2-month period, Arjun (the victim) deposited a total amount of ₹10.27 lakhs (₹10,27,000)!

The victim arranged the money from various sources. He shared with his parents and friends the news of his overseas job. According to the E-Mail, the victim received on 10 October 2010, he was supposed to catch a fight from Indira Gandhi International Airport and a person was going to meet Arjun at the airport with a Visa and an air ticket. During the correspondence, receipts with fake stamps (as it turned out later) and signatures of the British High Commissioner were sent to victim. When victim (Arjun) reached the airport, he found that there was no such person waiting for him. That is when the victim realized that he had been cheated. Arjun returned to Pune and tried to contact the concerned person but the concerned person never replied to his mails. Arjun then decided to approach the police.

Inspector (Crime Branch) Solankar said "After receiving the complaint, we started investigating the accounts in which Arjun had deposited the requested amounts of money. We identified an account in the name Shailendra Soni in the Shivajinagar branch of Axis Bank. We sent a team to Govandi and laid a trap for him." After the inquiry, the Police discovered that Soni was asked by someone called "Sharma" for permission to use his account. Police nabbed Sharma in Mira-Bhayandar. The investigation revealed that someone hailing from Nigeria asked them to commit the crime. He offered 7% of the total amount to Sharma. Sharma, in turn, got Soni's help by offering him a 5% commission. Sharma had met the suspected foreign national several times and they had been running this racket for many years. Sharma has various cheating crimes registered to his name. The Police took up the investigation aimed at finding out other crimes committed by this gang.

"When an idea exclusively occupies the mind, it is transformed into an actual physical or mental state."
- Swami Vivekananda

Mini Cases

- Case Study 26: Cyber pornography Involving a Juvenile Criminal
- Case Study 27: Indian Cyber defamation Case of a Young Couple
- Case Study 28: The Zyg-Zigler Case
- Case Study 29: Internet Time Stealing
- Case Study 30: New York Times Company vs. Sullivan Case of Cyber defamation
- Case Study 31: The Indian Case of Online Gambling
- Case Study 32: An Indian Case of Intellectual Property Crime
- Case Study 33: The Slumdog Millionaire Movie Piracy Case
- Case Study 34: Malicious Hacking Case – Organ Donation Database Deleted
- Case Study 35: The Case of Counterfeit Computer Hardware
- Case Study 36: The Chinese Case of Trade Secret Stealing Involving an E-Waste Company
- Case Study 37: Social Networking Victim - MySpace Suicide Case
- Case Study 38: State of Tamil Nadu vs. Suhas Katti Case
- Case Study 39: Pune Citibank MphasiS Call Center Fraud
- Case Study 40: NASSCOM vs. Ajay Sood and Others
- Case Study 41: Indian Case of Cyber defamation
- Case Study 42: Indian Cases of Cybersquatting
- Case Study 42.1: Yahoo Inc. vs. Akash Arora Case of Cyber squatting
- Case Study 42.2: Tata Sons Ltd vs. Ramadasoft Case of Cybersquatting
- Case Study 42.3: SBI Cards and Payment Services Private Limited vs. Domain Active Pty. Limited
- Case Study 42.4: Mahindra & Mahindra Limited (M&M) Case
- Case Study 42.5: Titan Industries Ltd. vs. Prashanth Koorapati and Others
- Case Study 42.6: Bennett Coleman & Co Ltd. vs. Steven S Lalwani Case
- Case Study 42.7: Rediff Communication Limited vs. Cyberbooth Case
- Case Study 43: Swedish Case of Hacking and Theft of Trade Secrets
- Case Study 44: IPR Violation
- Case Study 45: Indian E-Mail Spoofing Case

Case Study 26: Cyber pornography Involving a Juvenile Criminal

There was a recent Indian incident involving cyber pornography related to an 8th grade student of a certain Delhi school. The classmates used to tease the boy for having a pockmarked face. This went on for quite some time and the teasing did not stop in spite of student's appeals to his friends and complaints to the school teachers. Tired of the cruel jokes about his face, the boy decided to get back at his tormentors. As revenge, he scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. Action against this student was taken after the father of one of the girls (featured on the website) objected and lodged a complaint with the police.

In another incident that occurred in Mumbai it was found that a Swiss couple would gather slum children and would force them to appear for obscene photographs. The couple would then launch these photographs on to websites expressly designed for pedophiles. The Mumbai police arrested the

couple under the charge of cyber pornography. Section 67 B of the ITA 2008 (Indian IT Act amendment of 2008) addresses child pornography and makes searching and browsing also as offenses.

Case Study 27: Indian Cyber defamation Case of a Young Couple

Sujata, a young girl, was about to get married to Sudesh whom she met during a social event. She was mighty pleased because she never believed in finding a perfect match through an arranged marriage. Sudesh seemed to be open-minded and pleasant. They used to meet quite often during the pre-marriage period. One day when Sujata met Sudesh, he looked worried and even a little upset. He did not seem interested in talking to her. When she asked, he told her that members of his family had been receiving E-Mails that contained malicious stories about Sujata's character. Some of them were of her past affairs. He told her that his parents were very upset and he felt they were justified in getting upset; after all, Sujata was going to be their daughter-in-law soon. Sudesh told Sujata that his parents were considering breaking off the engagement. Sujata was shocked obviously, but fortunately, Sudesh was able to convince his parents and other elders of his house to approach police instead of blindly believing the mails. During investigation, it was revealed that the person sending those E-Mails was none other than Sujata's stepfather. Sujata was the main source of income in the family after her mother expired; the father was a drunkard and had no means of livelihood. Sujata's father (when he gave in during the police enquiries) admitted that he had sent those E-Mails to break the engagement. He wanted Sujata to remain with him to continue providing him financial support. He admitted that Sujata's marriage would have caused him to lose control of her property of which he was the guardian till she got married. Sujata's mother had bequeathed her all the property through a registered will because she was not sure if the property would be safe in the hand of her chronic alcoholic husband.

Section 49 of the Indian Penal Code is mentioned in reference to cyber defamation. Readers may like to note that copy of the IPC (Indian Penal Code) is available. The investigation traced the perpetrators through E-Mail forensics. Another famous case of cyber defamation occurred in America. Friends and relatives of a lady were inundated with obscene E-Mail messages appearing to originate from her account. These mails gave the lady a bad name and made her an object of ridicule. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing them, had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene E-Mails, they also launched websites about her basically meant to malign her character.

Case Study 28: The Zyg-Zigler Case

It is said that in the US, it is common to fire people from jobs. One employee of a bank in the US was dismissed from his job. The disgruntled man felt offended at have been mistreated by his employers. He decided to take revenge. He first introduced a logic bomb into one of the core banking systems of the bank. The logic bomb was programmed in such a way that the system would take 10 cents off from all the accounts in the bank and would deposit them into the account of the person whose name was alphabetically the last in the bank's rosters. This disgruntled man then opened an account in the name of Ziegler. The amount debited from each of the accounts in the bank was so trivial that neither the account holders nor the bank officials noticed any fault. Finally, this phenomenon came to the notice of the bank officials when another person by the name of Zygler opened his account in that bank. He was astonished to find a substantial amount of money being transferred into his account every Saturday!

Case Study 29: Internet Time Stealing

This is a case that took place before the ITA 2000, was enacted. In this case a services person was impacted. As you read on, you will realize how determination led to revelation about the fraud which

otherwise would not be detected. The fraud described in this case could be detected due to victim's alertness. Recall the discussion in Section 4.12.2 about "Theft of Internet Hours."

Colonel Bajwa, a resident of New Delhi, asked a nearby net cafe owner to visit for re-installing his Internet connection. For this purpose, the net cafe owner needed to know his username and password. After setting up the connection, the cybercafe owner walked away with the username and password noted down. He then sold this information to another net cafe. After about a week, Colonel Bajwa discovered that his Internet hours were almost over! Out of the 100 hours that he had purchased, more than 90 hours had been used up within the span of that week. He noted that this had happened although he was inactive in that week in terms of his use of the Internet from that connection that was set up with the help of the net cafe owner. Colonel Bajwa was surprised and became suspicious of his suddenly depleting Internet account. So, he reported the incident to the Delhi Police. The Police could not believe that time could be "stolen" because they were not aware of the concept of "time-theft" at all. They could not understand how something "immovable" such as the Internet "hours" could be stolen and so they rejected Colonel Bajwa's report. Colonel Bajwa was not willing to give up and he decided to approach The Times of India, New Delhi. They, in turn, prepared a report about the shortfall of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi took charge of the case and the police under his directions raided the cyber cafe and arrested the owner under the charge of theft as defined by the Indian Penal Code. The net cafe owner spent several weeks locked up in Tihar jail till the bail was granted. There are two points to note: (a) the modified IT Act, that is, the ITA 2008 addresses the cyber cafe issue and (b) not having encountered such a situation before, the police were perplexed by the theft about something they considered "immovable."

Case Study 30: New York Times Company vs. Sullivan Case of Cyber defamation

Here is the brief for the New York Times Co. v. Sullivan Case – facts of the case decided together with Abernathy v. Sullivan; this case concerns a full-page advertisement in the New York Times which alleged that the arrest of the Rev. Martin Luther King, Jr. in Alabama was part of a campaign to destroy King's efforts to integrate public facilities and encourage blacks to vote. L. B. Sullivan, the Montgomery city commissioner, filed a libel action against the newspaper and four black ministers who were listed as endorsers of the advertisement, claiming that the allegations against the Montgomery police defamed him personally. Under Alabama law, Sullivan did not have to prove that he had been harmed. He also did not have to prove the defense claim that the advertisement was untruthful because the advertisement contained factual errors. Sullivan won a $500,000 judgment. Question presented was "Did Alabama's libel law, by not requiring Sullivan to prove that an advertisement personally harmed him and dismissing the same as untruthful due to factual errors, unconstitutionally infringe on the First Amendment's freedom of speech and freedom of press protections?" Conclusion: The court held that the First Amendment protects the publication of all statements, even false ones, about the conduct of public officials except when statements are made with actual malice (with knowledge that they are false or in reckless disregard of their truth or falsity). Under this new standard, Sullivan's case collapsed.

This was a US Supreme Court case which recognized the actual malice standard before press reports could be considered to be defamation and libel, and hence allowed free reporting of the civil rights campaigns in the southern US. It is one of the key decisions supporting the freedom of the press. The actual standard for malice requires that the publisher is aware whether the statement is false or acts in an irresponsible manner without regard of the truth. The decision established that for a plaintiff to win a libel ruling against a newspaper, "actual malice" or "reckless negligence" must be proved on the part of the paper if the statement in question is about a public official or a public figure. In the case of a private figure, the petitioner must merely prove carelessness.

Case Study 31: The Indian Case of Online Gambling

There are millions of websites, hosted on many servers, to offer online gambling services. It is believed that many of these websites are actually fronts for "money laundering." Fraud cases of "Hawala" dealings and money misdeals over the Internet have been reported in the past. It is not yet fully known if these sites have any relationship with drug trafficking. Recent Indian case about cyber lotto is very interesting. Kola Mohan was the man who invented the story of winning the Euro Lottery. He created a website and an E-Mail address on the Internet with the address "eurolottery@usa.net." Whenever accessed, the site would declare him as the recipient of the 12.5 million pound. A Telugu newspaper published this as news after confirmation. Meanwhile, Kola Mohan collected large sums of money from the public as well as from some banks for mobilization of the deposits in foreign currency. He could have gone on merrily. The fraud, however, got exposed when a discounted cheque from Kola Mohan with the Andhra Bank for ₹1.73 million bounced. Kola Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

Case Study 32: An Indian Case of Intellectual Property Crime

This case study is related to "Cyber squatting". Satyam vs. Siffy is the most widely known case for that. Bharti Cellular Ltd. made a case in the Delhi High Court with a complaint that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with network solutions under different fictitious names. The court ordered Network Solutions not to transfer the domain names in question to any third party. Similar issues were brought to various High Courts earlier. Yahoo had sued a man called Akash Arora for use of the domain name "Yahooindia.Com" deceptively similar to its "Yahoo.com." As this case was governed by the Trade Marks Act 1958, the additional defense taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods. We know that intellectual property crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc. In other words, this is also referred to as cybersquatting.

Case Study 33: The Slumdog Millionaire Movie Piracy Case

This incident was posted on 23 July 2009. A San Marcos man pleaded guilty to a felony charge of using the Internet to distribute a pirated copy of "Slumdog Millionaire" in violation of federal copyright law. Owen Moody, aged 25, pleaded guilty to uploading a copyrighted work being prepared for commercial distribution, admitting that he uploaded a copy of "Slumdog Millionaire" late 2008 to a website called thepiratebay.org, with the illicit desire that others could download the movie over the Internet. Moody also posted a link to the upload at the Internet websites called demonoid.com and mininova.org. At the time Moody uploaded the movie, it was in limited release in domestic theaters and was not yet available on DVD. Moody used the Internet screen names "Tranceyo" and "Gizmothekitty." He found the copy of "Slumdog Millionaire" on an Internet website called funfile.org, where someone had uploaded a digital copy of the movie that had been sent as an Academy Award "screener" to a member of the Academy of Motion Picture Arts and Sciences for voting consideration. When Moody searched the Internet, he realized the movie was not readily available to the general public. Moody then downloaded the movie from funfile.org and uploaded it to piratebay.org. He also created links to the movie on the two other websites, to make the movie available to the general public. Moody uploaded the movie from his home in San Marcos, the US. rights to "Slumdog Millionaire" under copyright ownership of Fox Searchlight Pictures, Inc., which is located in Los Angeles County. At that time, the movie was in limited release in domestic theaters and was not yet available on DVD. Moody

pleaded guilty to the charge in front of the US District Judge Gary A. Fees in Los Angeles. Judge fees scheduled to sentence Moody on 5 October 2009. In the US, if you upload a copyrighted work, such an act carries a statutory maximum penalty of 3 years in central prison and a $250,000 fine or twice the gross gain or gross loss attributable to the offense, whichever is greater.

Another case: In first week of July 2009, a Ventura County man who obtained Academy Award screeners of "The Curious Case of Benjamin Button" and "Australia" pleaded guilty to uploading the films to the Internet. Derek Hawthorne, aged 21, of Moorpark, pleaded guilty to uploading a copyrighted work being prepared for commercial distribution. He was sentenced by the US District Judge R. Gary Klausner on 28 September 2009. The US Secret Service was involved in the investigation of cases running against Moody and Hawthorne.

Case Study 34: Malicious Hacking Case – Organ Donation Database Deleted

The typical "motives" behind cybercrime seem to be greed, desire to gain "power" and/or "publicity," desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset, the desire to sell network security services. This is a real life example showing the consequences of computer hacking. We know that disgruntled employees tend to get into criminal acts, seen from the "motive" perspective of cybercrimes. The example shows the "data loss" considering the critical data and systems of an organization that were deleted in a criminal act; an act that was performed with malice and ill intentions.

This is a classic case of an "Insider attack". It involved hacking a former employer's computer network. In this case, the former IT Director of at a non-profit organ and tissue donation center was sentenced to 2 years in prison for hacking into her former employer's computer network, announced Assistant Attorney General Lanny A. Breuer of the Criminal Division and US Attorney for the Southern District of Texas Tim Johnson.

The woman called Danielle Duann, aged 51, of Houston, pleaded guilty on 30 April 2009, to criminal indictment charging her with unauthorized computer access. Duann was sentenced to jail by US District Judge David Hittner in the Southern District of Texas. In addition to the 2-year prison term, Judge Hittner sentenced Duann to a 3-year period of supervised release following completion of her prison sentence and ordered her to pay $94,222 in restitution to compensate her former employer for the damage that resulted from her actions.

While pleading guilty, Duann admitted that she had illegally accessed the computer network of LifeGift Organ Donation Center and then intentionally deleted organ donation database records, accounting invoice files, database and accounting software applications and various backup files, without authorization. LifeGift is the exclusive supplier of organ procurement services for more than 200 hospitals throughout 109 counties in North, Southeast and West Texas.

As per the court documents, LifeGift removed Duann from her position as their director of Information Technology on 7 November 2005, and revoked all of her previous administrative rights and access to the LifeGift computer network. In pleading guilty, Duann admitted that beginning of the evening of 7 November 2005, and continuing until 8 November 2005, she repetitively gained unlawful access to the LifeGift computer network via a remote connection from her home and intentionally caused damage by deleting numerous database files and software applications, as well as their backups, related to LifeGift's organ and tissue recovery operations. Duann further admitted that in an attempt to conceal her activities, she disabled the computer logging functions on several LifeGift computer servers and erased the computer logs that recorded her remote access to the LifeGift network. This case was

investigated by the FBI and was jointly prosecuted by Trial Attorney Thomas Dukes of the Criminal Division's Computer Crime and Intellectual Property Section and Special Assistant US Attorney Bret W. Davis of the US Attorney's Office for the Southern District of Texas. This example emphasizes the point that the possibility of "insider attacks" should never be ignored and that disgruntled employees do have the potential to cause damage to their organizations. Systems Administrators as professionals possess tremendous amount of technical knowledge about how computer systems perform and, as this example shows, it can get put to malignant use with their motive to settle their personal scores!

Case Study 35: The Case of Counterfeit Computer Hardware

This is a slightly different kind of case reported on 3 December 2009. Christopher Myers, aged 40, and Timothy Weatherly, aged 27 were charged with conspiracy, trafficking in counterfeit goods and smuggling in counterfeit labels. In 2003, Myers founded a company called Deals Express. He conspired with Weatherly, who in 2005 established a company called Deals Direct, Inc to import counterfeit Cisco brand computer hardware from China. For making the hardware look genuine they attached fake Cisco labels to the components and packaged them in counterfeit Cisco boxes along with counterfeit Cisco manuals.

Myers and Weatherly arranged to have the counterfeit components despatched from China to various shipping addresses in Kansas State, including self-storage facilities in Lenexa, Merriam, Mission, Overland Park, and Kansas City, KS, as well as UPS stores in Seattle, WA, and Portland, OR. In November 2005, shipments of counterfeit goods were confiscated in Louisville, KY, Los Angeles, CA and Wilmington, OH. These seized goods included counterfeit hardware items such as network cards, connectors, manuals, labels and boxes. In August 2005, Weatherly established a website for Deals Direct and began using eBay to sell counterfeit Cisco products under the name "direct2technology." Myers and Weatherly made suggestions to their suppliers in Shenzhen, China, and Hong Kong for adjustments to the products to make them appear more authentic. After these counterfeit goods were seized, the defendants made various changes in their shipping arrangements in an attempt to avoid detection, including change of shipment address and having counterfeit goods shipped through other countries including Sweden.

Myers and Weatherly, upon conviction, would face a maximum penalty of 5 years in federal prison and a fine up to $250,000 on the conspiracy charge and a maximum penalty of 10 years and a fine up to $2 million on each of the trafficking counts. Immigration and Customs Enforcement and the National Bureau of Investigation worked on the case. Assistant US Attorney Scott Rask prosecuted the case. Legal professionals would know that defendants are considered not guilty until and unless they are proven guilty. The charges filed merely contain accusations of unlawful conduct.

Case Study 36: The Chinese Case of Trade Secret Stealing Involving an E-Waste Company

This case was published in September 2009 by the US Department of Justice. A citizen of the People's Republic of China was charged in connection with the scheme devised to steal trade secrets and proprietary information relating to computer systems and software with environmental applications from his New Jersey employer, Acting US Attorney Ralph J. Marra, Jr., announced. The indictment charges Yan Zhu, aged 31, a.k.a. "Wesley ZHU," a.k.a. "Westerly Zhu," who resides in Lodi, with conspiracy to steal trade secrets and wire fraud. On the morning of 9 April 2009, FBI Special Agents arrested Zhu at his residence while he was in the US on a work visa. Later that day, the defendant Zhu made an initial appearance in federal court in front of US Magistrate Tonianne J. Bongiovanni. The Magistrate released the defendant Zhu on a $200,000 secured bond. Zhu was later arrested on the accusation in Federal Court after the case was assigned to a US District Judge.

The indictment describes a scheme in which Zhu, along with other unindicted co-conspirators, used his employment with a business, which is identified in the indictment only as "Company A," to obtain access to the company's trade secrets and proprietary and confidential information relating to computer software developed for the Chinese market. According to the charges made against Zhu, he (i.e., Zhu) worked with Company A as a senior environmental engineer from May 2006 until his termination in July 2008. Company A is a software development and consulting company with its principal office in Mercer County. The company is in the business of developing supporting, and implementing software and computer systems for ecological applications. While in the services of Company A, Zhu worked on a comprehensive hazardous waste information management system that Company A developed for the Chinese market. The purpose of this product was to allow a Company A customer, such as an environmental regulatory agency, as well as entities that interact with the environmental regulatory agency, such as hazardous waste producers and shippers, to enter, organize and view certain data regarding pollution and hazardous waste within that agency's jurisdiction. In addition, it was alleged that Zhu worked on Company A database application that was related to this software system.

The allegation further stated that Zhu operated his scheme with at least two co-conspirators, identified only as Co conspirators 1 (CC-1) and 2 (CC-2), both Chinese nationals residing in China. According to the indictment, CC-1 had been introduced to Company A through Zhu and hired as Company A's sales representative in the Science and Technology High-Tech Zone in Xian City, Shanxi Province, China. Company A rented office space in Xian City. From this office CC 1 represented Company A and hosted the subject software on his/her own computer system. The charges filed allege that Zhu, CC-2 and CC-1, were all associated with a company known only as "Company X," an environment-related software company in China. It is further alleged that Zhu and his co-conspirators exploited the trust placed in Zhu by Company A by stealing Company A's trade secrets and proprietary and confidential business information, and exploiting an opportunity for Company A to market its product to the Chinese government. The indictment also alleges that, as early as January 2008, Zhu began sending Company A's computer software source code to CC-2 in China. Eventually, the Indictment alleges, the co-conspirators used this computer source code to develop a modified version of the Mercer County company's software in China, which was marketed under the Company X banner. It is further alleged that the co-conspirators took control of the Mercer County company's office in China, and used that space to conduct business for Company X. According to the indictment, Zhu was terminated on 17 July 2008, in part because Company A became aware that Zhu had sent Company A trade secret and confidential and proprietary information to his personal E-Mail account.

The charge of conspiracy to steal trade secrets carries a maximum penalty of 10 years in prison and a fine of $250,000 or twice the aggregate loss to the victims or gain to the defendants. Each count of wire fraud carries a maximum penalty of 20 years in prison and a fine of $250,000 or twice the aggregate loss to the victims or gain to the defendants. Despite the accusation, the defendant is presumed innocent unless proven guilty beyond a reasonable doubt. Marra credited Special Agents of the FBI's Trenton Resident Agency, under the direction of Special Agent in Charge Weysan Dun in Newark, with the investigation leading to the indictment. The government was represented by Assistant US Attorney Eric M. Schweiker of the Criminal Division in Trenton.

Case Study 37: Social Networking Victim - MySpace Suicide Case

This is about "MySpace" suicide case reported in the New York Times. "Myspace" is a social networking Site. In that section, there was the mention about a mother convicted of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed

suicide. This case shows that social networking sites, though popular, can result in someone losing his/her precious life, as this real-life case reveals. This case, (a real-life story) was reported in New York Times and posted on 26 November 2008. It is a sad story of the family members and friends of the teenaged girl who lost her life. She was a victim of social networking. Megan Meier, aged 13, committed suicide in October 2008. Apparently, the suicide was caused by cruel messages she received on the social networking site "Myspace." This incidence, in a way, is also sad reality in a "boyfriend oriented culture."

According to the legal experts in the US, this was country's first cyberbullying verdict, in which a Missouri woman was convicted of three misdemeanor charges of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide. The accused, Ms. Lori Drew went through a 5-day trial. During the trial, prosecutors portrayed Ms. Lori Drew had worked in collusion with her daughter, Sarah, aged 13 at that time, along with Ms. Ashley Grills, a young family friend and also an employee of Ms. Lori Drew's magazine coupon business in Dardenne Prairie. The testimony showed that they "created" a teenage boy, "Josh Evans," as an identity on MySpace. The conspiracy was to make this pseudo character (created on MySpace) to communicate with Sarah's rival, Megan Meier, who was also 13 years old then. Megan was known to have a history of depression and suicidal impulses. According to testimony at the trial there were weeks of online courtship with "Josh." Megan was distressed one afternoon in October 2006, when she received an E-Mail message from "Josh" saying that "The world would be a better place without you."

Ms. Ashley Grills, who is now 20, testified (under an immunity agreement) that shortly after that message was sent, Megan wrote back, "You're the kind of boy a girl would kill herself over." Totally depressed having such a message from her boyfriend (in reality only a pseudo character on MySpace) Megan hanged herself that same afternoon in her bedroom. The jury appeared to reject the government's contention that Ms. Lori Drew had intended to harm Megan. However, the convictions signaled the 12-member Jury's belief that she had, nonetheless, violated federal laws that prohibit gaining access to a computer without authorization. Specifically, the jury found Ms. Lori Drew culpable of illegally accessing a computer system on three occasions, in reference to the fraudulent postings on MySpace in the name of "Josh Evans." The federal Computer Fraud and Abuse Act was passed in 1986 in the US and has been amended several times since then. According to legal and computer fraud experts, the application of the law appeared to be expanding with technology and the growth of social networking on the Internet. In general, prosecutions under the act have been associated with people who are computer systems hackers. Until recently, social networking sites such as MySpace did not exist. Therefore, this case would be simply another important step in the expanded use of this statute to protect the public from computer crime. Although it was unclear how severely Ms. Lori Drew would be punished, the jury reduced the charges to misdemeanors from felonies, and no sentencing date was set. According to computer fraud experts, the conviction was highly significant as it was the first time that a federal statute designed to combat computer crimes was used to prosecute what were essentially abuses of a user agreement on a social networking site.

Under federal sentencing guidelines, Ms. Lori Drew could face up to 3 years in prison and $300,000 in fines, even though she had no previous criminal record. Her lawyer asked for a new trial. While this is a case from another country, it is a lesson for all of us. This case sends an overwhelming message to users of the Internet and social networking sites.

Case Study 38: State of Tamil Nadu vs. Suhas Katti Case

This case study related to Cyber defamation and it is a truly landmark case. It is considered to be India's First cybercrime conviction. People's perception is that conviction takes a very long time

in the jurisdiction. However there are exceptions as seen in this case. This well-known case of Suhas Katti (year 2004) is available in the public domain. It is noteworthy for the fact that the conviction was achieved successfully within a relatively short time of 7 months from the date of filing of the FIR (First Information Report). The case illustrates how the Indian IT was used to file the case. Similar cases have been awaiting judgment in other states for a much longer time. This case had a relatively more efficient handling in the sense that this was the first case of the Chennai Cybercrime Cell going to trial. Therefore, it deserves a special mention.

This case involves posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also sent to the victim for information by the accused. However, this was done through a false E-Mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was said to be interested in marrying her. She, however, married another person. Later, the wedding ended in a divorce, and the accused once again started making contacts with the lady. On her reluctance to marry him, the accused took up the harassment through the Internet. On 24 March 2004, a charge sheet was filed under Section 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. Prosecution examined 12 witnesses and complete documents were marked as "Exhibits."

The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further, the Defense Counsel argued that some of the documentary evidence was not sustainable under Section 65B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the cybercafe owners and came to the conclusion that the crime was conclusively proved. The judgment was submitted in May 2004 as stated below:

"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs. 500/- and for the offence under Section 509 IPC sentenced to undergo 1 year simple imprisonment and to pay fine of Rs. 500/- and for the offence under Section 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs. 4000/-."

The accused paid the fine amount and was lodged at Central Prison, Chennai. This is considered as the first case convicted under Section 67 of ITA 2000 in India.

IMPORTANT NOTE – The information contained in this case is meant for informational purpose only and is based on material available in public domain. Authors do not make any claim about its accuracy or authenticity. The name of the victim is masked to protect identity. The information provide here is based on the extracts from the Judgment pronounced in the First Cybercrime Conviction in India.

Case Study 39: Pune Citibank MphasiS Call Center Fraud

BPO and call center business is growing in India has become a popular destination for outsourcing back office work. This case involves a BPO scenario and is an eye opener. US$ 3,50,000 belonging to four US customers were fraudulently transferred to fake accounts. This was enough to give ammunition

to those lobbying against outsourcing of work from the US to other countries; especially to India. Such cases are not uncommon but media likes to focus on them when it happens in India. It is a case of sourcing engineering, also known as "social engineering." Some employees gained customer confidence and obtained their PIN numbers to commit fraud. They got these under the disguise of helping the customers out of dificult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering/social engineering.

As an industry practice in security, the call center employees are checked when they go in and out of the work place. This is done to ensure that they do not copy down numbers or any other business confidential information. However, in this case, the employees of the call center must have remembered these numbers, gone out immediately to a cyber cafe and accessed the Citibank accounts of the customers. All accounts were opened at Pune. The customers lodged a complaint that the funds from their accounts were transferred to Pune accounts. This is how the criminals were traced. Police were able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

The ISO 27001 standard for information security recommends many controls and one such control is about HR checks. As a best practice, there should be strict background check of the call center executives. However, even the best of background checks cannot fully eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national database where a name can be referred to. In this case first round of investigations did not disclose that the criminals had any criminal history. Customer education is crucial so that customers are not taken for a ride. Most consumers may feel that banks are guilty of not doing this.

Case Study 40: NASSCOM vs. Ajay Sood and Others

This case comes under Phishing. The petitioner in this case was the National Association of Software and Service Companies (NASSCOM), India's premier software association. The defendant was Ajay Sood & Others and the case was delivered in March 2005. In this case, the Delhi High Court declared "Phishing" on the Internet to be an illegal act, entailing an injunction and recovery of damages.

The court elaborated on the concept of "Phishing," in order to lay down a precedent in India. The court stated that it is a form of Internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company, in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. The court also stated, by way of an example, that typical Phishing scams involve persons who pretend to represent online banks and siphon cash from E-Banking accounts after conning consumers into handing over confidential banking details.

According to the Delhi High Court, even though there is no specific legislation in India to penalize Phishing, it held that Phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the E-Mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of Phishing as passing off and tarnishing the plaintiff's image.

The defendants were running a placement agency engaged in providing head-hunting and recruitment services. In order to obtain "personal data," which they could use for purposes of head-hunting, the defendants composed and sent E-Mails to third parties in the name of NASSCOM. The

high court recognized the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to NASSCOM. The court further ordered the defendants not to hold themselves out as being associates or a part of NASSCOM. For readers not savvy with legal terms – "Ex–parte" means on behalf of only one party, without notice to any other party. For example, a request for a search warrant is an ex parte proceeding, since the person subject to the search is not notified of the proceeding and is not present at the hearing.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers, from which the fraudulent E-Mails were sent by the defendants to various parties, were taken into custody by the local commissioner appointed by the court. The offending E-Mails were then downloaded from the hard disks and presented as evidence in court. During the progress of the case, it became clear that the defendants, in whose names the offending E-Mails were sent, were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action.

On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Later, the defendants admitted their criminal acts and the parties settled the matter through the recording of conciliation in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of ₹1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones (a) It brings the act of "Phishing" into the ambit of Indian laws even in the absence of specific legislation. (b) It demonstrates a point – the perception that there is no "damages culture" in India for violation of IP rights is not true. This case re-affirms Intellectual Property owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

Case Study 41: Indian Case of Cyber defamation

This is another well-known case available in the public domain. Though an old case, it is considered to be India's first case of cyber defamation, in which a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through E-Mails and passed an important ex-parte injunction. For readers who do not come from legal background, ex-parte is a Latin legal term meaning "from (by or for) one party." An ex-parte decision is one decided by a judge without requiring all parties to the controversy to be present. According to legal doctrines in Australia, Canada, the UK, India and the US, "ex–parte" means a legal proceeding brought by one person in the absence of and without representation or notice of other parties. It is also used as a slack reference to unacceptable one-sided contacts with a court, arbitrator or represented party without notice to the other party or counsel for that party.

The Delhi High Court conceded an ex-parte ad interim order in the case entitled "SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra" being Suit No. 1279/2001. This matter was handled by one of India's leading cyber lawyers. The defendant Jogesh Kwatra was an employee of the plaintiff company. He started sending defamatory, derogatory, vulgar, filthy, obscene and abusive E-Mails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R.K. Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory E-Mails to the plaintiff.

Arguing on behalf of the plaintiffs, the cyber lawyer handling the case contended that the E-Mails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. The lawyer further argued that the aim of sending the said E-Mails was to malign the impeccable reputation of the plaintiffs all over India and the world. The lawyer further contended that the acts of the defendant in sending the E-Mails had resulted in invasion of legal rights of the plaintiffs. Further, it was argued that the defendant is under a duty not to send the aforesaid E-Mails. After the claimant company made a discovery that the said worker of their organization was possibly involved in the act of sending offensive E-Mails, the claimant terminated the services of the defendant.

After hearing detailed arguments of the lawyer, Honorable Justice J.D. Kapoor of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. As a result, the Delhi High Court stopped the defendant from sending defamatory obscene derogatory, humiliating, vulgar and abusive E-Mails either to the plaintiffs or to its associate companies and/or sister concerns all over the world including their Managing Directors and their Sales and Marketing departments. In addition, Honorable Justice J.D. Kapoor also stopped the defendant from transmitting, publishing, or causing to be published any information in the physical world as well as in cyberspace which is deprecating or slanderous or offensive to the plaintiffs.

The matter was posted for 4 October 2001. This decree by Delhi High Court has remarkable meaning because this is for the first time that an Indian Court assumes authority in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene E-Mails either to the plaintiffs or their subsidiaries.

Case Study 42: Indian Cases of Cybersquatting

These case studies are related to "cyber squatting". "Cyber squatting" means registering a popular Internet address – usually a company name – with the aim of selling it to its lawful owner. After presenting the short examples, we have summarized the learning points.

Case Study 42.1: Yahoo Inc. vs. Akash Arora Case of Cyber squatting

This is probably the first reported Indian case wherein the plaintiff (the person who lodges the complaint) is the registered owner of the domain name yahoo.com and the plaintiff succeeded in obtaining an interim order restraining the defendants and agents from dealing in service or goods on the Internet or otherwise under the domain name yahooindia.com or any other trademark/domain name which is misleadingly analogous to the plaintiffs trademark Yahoo. As on the date of writing this, there are only a small number of reported judgments in our country; however, newspaper reports and information from dependable sources indicate that there are at least 25 disputes pertaining to domain names pending before the Delhi High Court itself.

Case Study 42.2: Tata Sons Ltd vs. Ramadasoft Case of Cybersquatting

This cybersquatting case involved Tata Sons Ltd vs. Ramadasoft. Tata Sons is the holding company of India's largest industrial corporation, the Tata Group. Tata Sons won a case to evict a cybersquatter from 10 contested Internet domain names. Tata Sons had filed a complaint at the World Intellectual Property Organization (WIPO). The respondent was proceeded ex-parte. As explained earlier, an ex-parte decision is one decided by a judge without requiring all of the parties to the controversy to be present. The board reached a conclusion that the respondent owns the domain names. These domain names are confusingly similar to the complainant's trademark TATA, and the respondent has no rights or legitimate interests in respect of the domain names, and he has registered and used the domain names in bad faith. These facts permit the plaintiff to an order transferring the domain names from the respondent.

Case Study 42.3: SBI Cards and Payment Services Private Limited vs. Domain Active Pty. Limited

This is the case that involved SBI Cards and Payment Services Private Limited vs. Domain Active Pty. Limited. Sbicards.com was ordered by the World Intellectual Property Organization (WIPO) to be transferred to the Indian Company from an Australian entity, which hijacked the domain name hoping to later sell it for a hefty sum to the State Bank of India subsidiary. The panel accepted SBI Card counsels argument that the Australian company was in the business of buying and selling domain name through its website.

Case Study 42.4: Mahindra & Mahindra Limited (M&M) Case

Yet another Indian instance of cyber squatting involved Mahindra & Mahindra Limited (M&M). In this case, a young student residing in Andhra Pradesh registered the domain names mahindra.com, mahindra.net and mahindra.org, in his name. M&M made an appeal to the World Intellectual Property Organization (WIPO) saying that they had registered the name "Mahindra" as the registered trademark in India and the US. As per the order passed by the panelists, the domain names were to be immediately transferred in favor of the Indian company.

Case Study 42.5: Titan Industries Ltd. vs. Prashanth Koorapati and Others

In this case of Titan Industries Ltd. vs. Prashanth Koorapati & Ors., the Delhi High Court sanctioned an ex-parte ad interim restriction (i.e., in the meantime) to restrain the defendants from using the name TANISHQ on the Internet or otherwise and from committing any other act as is likely to lead to passing off of the business and goods of the defendants as the business and goods of the plaintiff.

Case Study 42.6: Bennett Coleman & Co Ltd. vs. Steven S Lalwani Case

This is another interesting case of cybersquatting. Since 1996, the complainant has been holding the domain name www.economictimes.com, for electronically publishing it in newspapers. The plaintiff had registered in India this mark for literary purposes. However, in 1998, Steven S. Lalwani, US, registered the same domain name. The WIPO judgment made it clear that the complainant have a very substantial reputation in their newspaper titles arising from their daily use in hard copy and electronic publication. It was also firmly held that the registration and use of the domain names by the respondents is not in good faith in that their use meant an intentional attempt to attract (with commercial gain as the purpose), Internet users to their websites by creating a possibility of misunderstanding with the complainants marks as to the source, sponsorships, affiliation or endorsement of those websites and the services on them.

Case Study 42.7: Rediff Communication Limited vs. Cyberbooth Case

In Rediff Communications Ltd. vs. Cyberbooth, petitioner, the proprietor of the well-known portal and domain name rediff.com filed for embargo against the defendant, registrant of the domain name rediff.com. The Judge was convinced that there was a clear intention to deceive and granted interim relief to the plaintiff. The judge affirmed that a "domain name" is more than an Internet address and is entitled to as much protection as that provided for a trademark.

The discussion here assumes that readers are familiar with IPR, Copyright, Trademark, Trade secret, etc. The various statues dealing with Intellectual Property Laws in India are as follows:

- Trademarks Act 1999
- Copyright Act 1957
- Patents Act 1970 as amended by Patents (Amendments) Act 2005
- Designs Act 2005.

- Code of Civil Procedures 1908.
- Indian Penal Code 1860.
- Geographical Indication of Goods (Registration & Protection) Act 1999.
- Semiconductor, Integrated Circuit Layout Design Act 2000.
- Plants Varieties Protection and Farmers' Rights Act 2001.
- Information Technology Act 2000.

From the above cyber squatting examples described so far, note the following points:

The trademark law has been drastically broadened to accommodate domain name disputes. However, in author's opinion, the trademark law should not be too widely broadened to confer upon trademark owners the rights that they otherwise are not entitled to. The tricky question is whether the law will eventually give large trademark owners property rights in domain names, that is, the ability to exclude others from using them. In deciding how far the trademark laws should reach, it may become essential to revisit the rationale behind trademark protections. Trademark protection is meant to provide consumers with exact information about the merchandise and services presented by the mark, and to provide incentives to companies so that they become interested in investing in their marks and also to enhance quality control. Trademarks, therefore, lower consumer search costs and promote the economic functioning of the market. "Marks" themselves are not protected, but the law protects the goodwill the marks embody.

Allowing exclusive rights in domain names will put off companies from using names that are already used. Conventional financial explanation for trademark law rests on the premise that there is an countless number of marks available. However, there are only a limited number of domain names available.

One more area of concern with such a right is that it would allow trademark owners to preclude others from using not only one but several marks. It is now a general practice for companies to register all possible domain names they can think of, that contain their company name. For example, Exxon currently holds the rights of over more than 120 domain names incorporating the word "EXXON."

The current law seems to endorse protection of large companies more, that is, those who want rights in every possible variations of their name.

From a realistic point of view, the current expansion in law gives trademark owners a significant amount of leverage. For example, often people with genuine interests in their domain names cannot pay for fighting with trademark owners. Naturally, this will force many to simply turn over their rights in order to avoid corporate bullying.

Case Study 43: Swedish Case of Hacking and Theft of Trade Secrets

Stealing of IPR/trade secrets is one of the major threats to industries and individuals in the modern era. Here is a real-life scenario on that. Two well-known organizations co-operated with Government for the investigation of this case.

Philip Gabriel Petterson, a.k.a. Stakkato, aged 21, a Swedish national, was indicted on 17 May 2009, on the grounds of intrusion and trade secret theft charges. This was announced by the US Attorney for the Northern District of California and the Justice Department's Criminal Division.

The charges included one intrusion attempt and two attempts of trade secret misappropriation involving Cisco Systems Inc. (Cisco), San Jose, CA, a provider of computer network equipment and producer of Internet routers. As per allegations in the condemnation, Pettersson purposely committed an intrusion between 12 May 2004 and 13 May 2004 into the computer system and network of Cisco.

It was alleged that during the suspected intrusion, some Cisco Inter-network operating system code was misappropriated. The accusation also included two intrusion attempts involving the National Aeronautics and Space Administration (NASA), including computers at the Ames Research Center and the NASA Advanced Supercomputing Division, located at Moffett Field, CA. The accusation alleges Pettersson committed these intrusions on 19 May 2004, 20 May 2004 and 22 October 2004.

Cisco and NASA cooperated in the government's investigation. Following the incident, Cisco reported that they could not believe that any customer information, partner information or financial systems were affected. The Department of Justice worked in cooperation with the Swedish authorities on this case. From legal perspective, it is to be noted that an indictment is merely an accusation. All defendants are presumed innocent until proven guilty at trial beyond a reasonable doubt. The maximum penalty for each charge of intrusion and theft of trade secrets is 10 years in prison, a 3-year term of supervised release, and a fine of $250,000.

The prosecution was the result of an investigation by the FBI; US Secret Service; NASA Office of Inspector General, Office of Investigations, Computer Crimes Division; and numerous additional federal agencies. A senior officer at the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) prosecuted the case with assistance from other officers. CCIPS Senior Counsel also assisted in the prosecution. The Criminal Division's Office of International Affairs assisted on international coordination issues in the case. Source: www.cybercrime.gov

Case Study 44: IPR Violation

This case study is related to Intellectual property stealing. This example involves a counterfeit software program. Below is explained how this crime happened in real life.

On 12 June 2009, Rodolfo Rodriguez Cabrera, aged 43, a Cuban national, and Henry Mantilla, aged 35, of Cape Coral, FL, were accused about a plot to manufacture and sell fake International Game Technology (IGT)-brand video gaming machines, commonly known as "slot machines," and counterfeit IGT computer programs. Cabrera was arrested on 8 June 2009, based on the indictment. Mantilla was scheduled to appear based on a summon in the US District Court for the District of Nevada on 2 July 2009.

As per the indictment, Cabrera was the owner as well as operator of a company called FE Electronic in Riga, Latvia, and Mantilla owned and operated a company named Southeast Gaming Inc., in Cape Coral, FL. The indictment makes an allegation that during the period that spanned between August 2007 and 15 April 2009, Cabrera and Mantilla were part of the conspiracy that involved making illegal copies of IGT video gaming machine computer programs, placing counterfeit labels bearing IGT's registered trademark on the computer programs, installing the counterfeit computer programs in IGT gaming machine cabinets and then sell the counterfeit computer programs and gaming machines through their respective companies. They did all this without the permission of the trademark and copyright owner, IGT.

The charge against Cabrera and Mantilla indicated that they were involved with a conspiracy of trafficking in counterfeit goods, trafficking in counterfeit labels and criminal copyright infringement. If convicted of all charges, each defendant faces a maximum of up to 45 years in prison and $5.25 million in fines. The accusation also contains 13 penalty allegations that require the defendants, if convicted, to forfeit any and all counterfeit items and to forfeit up to $5 million in proceeds from their alleged criminal activity.

The case was investigated by the FBI and prosecuted by Assistant US Attorney of the US Attorney's Office for the District of Nevada and Trial Attorney of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). Significant assistance came in this case from the Central Criminal

Police Department of the Latvian Ministry of Interior; Latvia's Office of the Prosecutor General, International Cooperation Division; and Senior Trial Attorney Deborah Gaynus of the Criminal Division's Office of International Affairs. CCIPS Trial Attorney also assisted with the prosecution. IGT also provided assistance in this matter. An indictment is merely a formal charge by the grand jury. As legal professionals know, a defendant is assumed to be innocent unless and until proven guilty in a court of law. Source: www.usdoj.gov

Case Study 45: Indian E-Mail Spoofing Case

This is a case registered by the Indian police as the first case of cyberstalking in Delhi. To maintain confidentiality and privacy of the entities involved, we have masked their names. Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay and Ahmedabad. These calls created havoc in the personal life destroying mental peace of Mrs. Joshi. She decided to register a complaint with Delhi Police. A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for 4 consecutive days. The person was chatting on the Internet, using her name and giving her address, talking in profane language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

While "cyberstalking" does not have a standard definition, it means threatening, unwarranted behavior or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

This ends all the mini-cases of this section and now we move on to illustrations of financial crimes in the banking domain including the credit card frauds.

Online Scams

In this section, we present revealing information about world's most infamous scams. Many of them are related – for example, Nigerian scams (also known as "419 scams" involve one or other form of advance fee to lure the victim for the promise of a long-term gain).

In a way, "SPAM" and "SCAM" are related because Spam, is often the vehicle used to convey scams and other attempted fraudulent attacks to individuals. A "HOAX" also involves deception; however, it is done without the intention of gain or damage or for depriving the victim; sometimes the intention can be humorous. In this section, a number of Scam examples are provided. We hear about scams that are reported occasionally in the news papers. The majority of recipients may not respond to these E-Mails; however, there are a few people who do respond to such mails. From fraudsters' point of view, that is enough to make the fraud worthwhile as many millions of messages can be sent. Invariably sums of money which look large, but are very much smaller than the promised profits, are required in advance for bribes, fees, etc. – this is the money stolen from the victim, who thinks he/she is making an investment for a huge profit.

The objective is to create awareness for people so that they take due care and do not fall prey to such scams. A "fraud" is a deliberate action conducted with the motive of personal gain or an act done to damage another individual. The specific legal definition varies by legal jurisdiction. Fraud is a crime and also a civil law violation. Doing fraud with people or entities (such as organizations, institutions, etc.) for money or ill-gotten gains is a common purpose of fraud, but there have also been fraudulent "discoveries." Fraudsters cleverly exploit human characteristics such as greed and dishonesty, and victimize individuals from all walks of life. "Advance free fraud" is a classic example of this. Advance Fee Scam usually begins with a letter or E-Mail that is sent only to a selected recipient

but is actually sent to many persons. In the E-Mail an offer is made with a claim of a large payoff for the victim. Often, the subject line of the E-Mail's have some catchy text like "From the desk of Mr. XYZ," "Your assistance is needed," and so on. The details vary, but the usual story is that a person, often a government or bank employee, knows of a large amount of unclaimed money or gold which he cannot access directly, usually because he has no right to it.

The Spam E-Mails used to perpetrate scams are often transmitted from Internet cafes having satellite connection. Addresses and E-Mail content of recipient are duplicated into a webmail interface on a stand-alone storage medium, such as a memory card. During the course of many schemes, scammers look for victims to supply bank account information. Typically this is a "test" devised by the scammer to gauge how gullible the victim could be.

Case Study 46: Scam No. 1 – Foreign Country Visit Bait

This is a common trick used by fraudsters. Fraudsters take advantage of the fact that generally people are eager to go overseas with the hope of earning more money. Fraudsters devising a plot under such scenario would charm the victim through an "invitation to visit the country." The naive victims are invited to a country to meet real or fake government officials. Some victims who do travel are instead held for ransom. There are a few rumored cases, where they are illegally brought into the country without a visa and threatened into giving additional money as the penalties for being in a foreign country without a visa may be severe. At times victims are taken for ransom or they are killed – as it happened in the case of the 29-year-old Greek man called George Makronalli who was lured to South Africa and was killed.

Case Study 47: Scam No. 2 – Follow-up Scamming

This trick is used when scammers know that their victim who has just been scammed, is more likely to fall for scamming attempts rather than a randomly selected target. Often the scammer contacts the victim after a fraud – the scammer is smart enough to make a representation as a law enforcement officer. The victim is given to understand that a group of criminals has been arrested and that they (i.e., fraudsters who are pretending to be the law enforcement folks) have recovered victim's lost money. Further, fraudster/scammer tells the victim that in order to get the money back, the victim must pay a fee for processing or insurance purposes. Even when the victim realizes the scam, this follow-up scam can be successful because the scammer represents himself/herself as a totally different party and yet knows details about the transactions. For the victim, realization that he/she has lost a large sum of money and the prospect of getting it back often leads to the victim ending up paying even more money to the same scammer.

There are many variations on the most common scam stories, and also many variations on the way the scam works. What follows in the section below are some of the most notable deviations from the standard Nigerian Letter scam, but still retain the core elements; the victim is deceived by some disproportionately large gain into sending an advance payment, which once made is irrecoverable.

Case Study 48: Scam No. 3 – Purchasing Goods and Services Scam

Advertising automobiles on websites has become quite common. For that matter, there is a big boom in "Online Marketing" activities even if, at times, it may be at the cost of your personal information being stolen! In this mode of scam, the fraudsters list a non-existent high value car with a low price as bait to attract buyers eager to buy quickly; specially the young and rich targets. The scammer posts a message to the tune "I am not in the country, but if you pay me first, a friend will drive the car to you." The required payment may be the full price, or a deposit, but it would not be an insignificant fee. The picture of the car is never posted on the website because the car just does not exist. In this type of scam, the scammers use E-Mail only because they are smart enough to know that the sound of their voice and their attitude will give them away as being high risk.

Another scheme under this type of scam involves advertising fake academic conferences and enticing academics to apply to present papers. As a common practice, the conference would typically subsidize the accommodation but would not reimburse the cost of air journey undertaken by the academicians to be at the conference venue for presenting papers. One method using which the scammer baits the hopeful attendee is that they o□er free air travel to the victim, if they agree to pre-pay for hotel accommodation. The scammer can put forth a number of arguments to support why the accommodation must be pre-paid – primarily that they do not trust the victim will attend the conference unless he/she pays upfront. In this scam, fraudsters may use any goods or services – the idea is that they bait the victim with a good deal, and the victim must pay upfront and electronically.

Case Study 49: Scam No. 4 – Cheque Cashing Scam

Given the workforce mobility scenario, worsening traffic conditions and soaring property prices, working from home is becoming a common pattern now. Some scam schemes are designed to exploit the workforce mobility scenario. Such schemes are based solely on conning the victim into cashing a counterfeit cheque. The scammer gets in touch with the victims and gets them interested in a "work-at-home" opportunity. Alternatively, the scammer may ask the victims to cash a cheque or a money order under the pretext that the instrument (i.e., the cheque or the money order) cannot be redeemed locally. According to a recently used cover story, the perpetrator of the scam wished the victim to work as a "mystery shopper," evaluating the service provided by MoneyGram or Western Union locations within major retailers such as Wal-Mart.

Typically, the scammer sends the victim a cheque or money order, the victim cashes it, sends the cash to the scammer via wire transfer and the scammer disappears. Later the forgery is uncovered and the bank transaction is reversed. This makes the victim liable for the balance. Defrauding plots based solely on cheque cashing typically offer only a small part of the cheque's total amount, with the assurance that many more cheques will follow. If the victim buys into the scam and cashes all the cheques, the scammer can win big in a very short period of time. There are other scams where overpayment is involved; these usually result in smaller revenues for the scammer, but have a higher success rate as the scammer's request seems easier to believe. Some cheque-cashing scammers use several victims at various stages of the scam. A victim in the US or other "safe" country such as the UK or Canada (where typically the cashing victim resides) is sometimes approached with an offer to fill out cheques sent to them by the scammer and mail them to other victims who cash the cheque and wire the money to the scammer. Usually the scammer promises a cut of the money to the mailer of the cheque. However, that promise is usually not met, and the cheque mailer is often conned into paying for the production and shipping costs of the cheques. The information about the cheque is either been stolen or is fictionalized and the cheque is forged. Usually, it is far easier to track the victim mailing the cheques than tracking and prosecuting the scammer. Therefore, when the cheques turn up as fraudulent the person mailing them usually ends up not only facing charges for bank fraud and conspiracy, but also faces the liability for the full amount of the fraudulent cheques. As the mailer of the cheque is taking the call, there is now a lesser likelihood that the scammer will be caught. This makes it a popular variation of the scam; especially in countries where antifraud laws are not very tough.

Another variety of the cheque-cashing scheme involves owners of vacation rentals. The scammer shows interest in renting the unit for a much higher than normal rate, usually for an upcoming honeymoon, business trip, etc. The scammer also offers to pay all fees "up front," as soon as the unsuspecting unit owner agrees to the windfall rental. In the long run, a very genuine looking money order/bearer cheque arrives. Around this time the scammer makes a request that a part of the rental fee be returned and provides a convincing reason for it – for example, wedding called o□, death in the family, business failure, etc. Given the reason of the supposed crises, scammer requests the victim to return most of the rental fee via wire transfer. The owner of the unit is encouraged to keep "a fair amount" as a compensation for his time. The wire transfer is sent, only to find out later that the official looking cheque was indeed bogus and the full amount is charged back to the unit owner by his bank.

Case Study 50: Scam No. 5 – Romance Scam

Fraudsters exploit human psychology to gain victim's confidence. Romance scam is based on a "confidence trick." A confidence trick or confidence game (also known as a bunko, con, flim flam, gaffe, grift, hustle, scam, scheme, swindle or bamboozle) is an attempt to defraud a person or group by gaining their confidence. The victim is known as the mark; the trickster is called a confidence man, con man, confidence trickster or con artist. Any accomplices are known as shills (see the explanation for these terms provided in Scam No. 17 – "advance fee scam"). Confident but criminally oriented people exploit human characteristics such as greed and dishonesty. Such people have victimized individuals from all walks of life. The "confidence trick" used in romance scam involves feigned romantic intentions toward victims, gaining their affection, and then using that goodwill to commit fraud. Acts of fraud may involve access to the victims' money, bank accounts, credit cards, passports, E-Mail accounts and/or national identification numbers or by getting the victims to commit financial fraud on their behalf.

Fraudsters are tech-savvy; they modify their scamming techniques with the changing communication technologies that emerge. Money-for-romance angle is a recent variant of the Romance Scam. The con

artist approaches the victim on an online dating service, an instant messenger (like Yahoo IM) or a social networking site. The scammer claims an interest in the victim and posts pictures of an attractive person (not themselves). The scammer uses this communication for his/her confidence and then asks for money. The con artist may claim to be interested in meeting the victim, but needs cash to book a plane, hotel room or other expenses. In other cases, they claim they are trapped in a foreign country and need assistance to return, to escape imprisonment by corrupt local officials, to pay for medical expenses due to an illness while abroad and so on. The scammer may also use the confidence gained by the romance angle to introduce some variant of the original Nigerian Letter scheme – for example, saying they need to get money or valuables out of the country and offer to share the wealth, making the request for help in leaving the country even more attractive to the victim. In a newer version of the scam, the con artist claims to have "information" about the fidelity of a person's significant other, which they will share for a fee. This information is obtained through social networking sites by using search parameters such as "in a relationship" or "Married." Anonymous E-Mails are first sent to attempt to verify receipt, and then a new Web-based E-Mail account is sent along with directions on how to retrieve the information.

Case Study 51: Scam No. 6 – Lottery Scam

Probably, this is most often heard term. A lottery scam is a type of advance-fee fraud. It begins with an E-Mail notification that is most unexpected. For example, you may get a mail declaring "You have won!" a large sum of money in a lottery. Next, you, the recipient of the message, would usually be told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, you, as the target of the scam will be asked to pay "processing fees" or "transfer charges" for the winnings to be distributed. In reality, however, you will never receive any lottery payment. Quite a few E-Mail lottery scams use the names of legitimate lottery companies; however, that does not mean those legitimate companies are in any way involved with the scams.

Fake notices of lottery wins are involved in most lottery scams. The winner is usually lured to send sensitive information to a free E-Mail account. The scammer then informs the victim a small fee is required to release the funds (insurance, registration or shipping). Once the victim sends the fee, the scammer invents another fee.

Similar to the various types of overpayment fraud mentioned above, a new variation of the lottery scam involves fake or stolen cheques being sent to the "winner" of the lottery (these cheques represent a part payment of the winnings). The winner is more likely to assume the win is legitimate, and thus more likely to send the fee (which he does not realize is an advance fee). The cheque and the funds involved are pointed out by the bank when the fraud is discovered, and debited from the victim's account. In 2004, another form of the lottery scam appeared in the US. Fraud artists, using the scheme, call victims on telephones; a scammer tells a victim that a government has given them a grant and that they must pay an advance fee, usually around $250, to receive the grant.

Case Study 52: Scam No. 7 – The Hitman Scam

A "hitman" or "hitwoman" usually is a murderer who people hire to eliminate a target via contract killing. Those of you, who may have watched the Brad Pit–Angelina Jolie movie "Mr. and Mrs. Smith," would remember the "contract killing scenario." In this type of scam, an E-Mail is sent to the victim's inbox, supposedly from a hitman who has been hired by a "close friend" of the recipient to kill him or her. The scammer tells the victim that hit can be called o□ in exchange of a large sum of money. This is generally backed up with a warning not to contact the local police or a local investigation agency, or the "hitman" will be forced to go through with the plan. This is less of an advance-fee fraud and more

of an outright extortion; however, a reward can at times come in the form of the "hitman" offering to kill the man who ordered the original hit on the victim.

Case Study 53: Scam No. 8 – Bomb Scams

This type of scam comes closer to "cyber terrorism". This scam is similar to "hitman scam" wherein scammers gets in touch with a business, mall, office building or other commercial location and inform them about an impending bomb threat. The scammer threatens that he/she will detonate the bomb unless the management of the business complies with scammers' demands. Often, scammers say they have the store under surveillance; however, analysis of many such calls by police has established that most of threat calls are made from other states or even from outside the country. Some evidence may exist pointing to the scammers who hacked into the store's surveillance network, but this has not been confirmed in any case and has been refuted in others. The scammers usually demand that the store management staff or people working in the main office of the store (if the store is a chain) send money via wire transfer to the scammer. Other demands of these scammers have been more personal or humiliating, such as demanding that everyone in the store take off their clothes.

The underlying threat in the scam is a bomb threat – so, local law enforcement is obliged to quickly respond to the site under threat. However, because the scammer is usually nowhere near this location, the scammer is in little, if any, danger of being apprehended while the scam is playing out. In the meantime, law enforcement assumes that the threat is genuine, and therefore can do little to intervene without risking the detonation of the bomb. The fact that the threat was in reality a scam is usually not discovered until long after the situation is over and the extortionist has collected the money demanded.

Case Study 54: Scam No. 9 – Charity Scams

This is a trick to invoke sympathetic feeling in people's mind and use it to achieve the ulterior motive. The scammer presents himself/herself as a charitable entity looking for donations to help the impacted victims (e.g., those affected by a natural disaster, terrorist attack – for example the 9/11 World Trade Center attack, regional conflict, epidemic, etc.). Scammers very well know how to exploit people's penchant for philan-thropic work – they used 2004 Tsunami and Hurricane Katrina as the popular targets for perpetrating charity scams. There are other more timeless scam charities exploited as well, in the name of raising money for cancer, AIDS or Ebola virus research, children's orphanages (the scammer pretends to work for the orphanage or a non-profit organization), or impersonates charities such as the Red Cross or United Way. The scammer asks for donations, often linking to online news articles to strengthen their story of a funds drive.

The scammer's victims are philanthropists who believe in helping a worthy cause and therefore they expect nothing in return. Once sent, the money is gone and the scammer often disappears. Some scammers manage to keep the scam going by asking for a series of payments. At times, the victim may land in legal trouble after excluding their supposed donations from their income tax submission forms. Tax rules vary from country to country – for example, as per directives of the US Tax Law, charitable donations are tax-exempt only if donations are made to eligible non-profit organizations. The scammer may inform the victims that their contribution is deductible and that the donors should provide all necessary proof of donation. However, the information provided by the scammer is fictional. When audited, the victim faces stiff penalties. These scams have some of the highest success rates especially following a major disaster, but the average loss per victim is less than other fraud schemes. This is because, the victim is far less likely to donate more than what he/she can afford.

In a slight variant of "Charity Scam," the scammer pretends to have a terminally ill mother, or pretends to be a poor university student, and simply begs the victim for money to pay for medical treatment, to pay for college tuition, to sponsor their children, etc. The scammer assures that the money will be repaid along with the interest by some third party at a later date (often these third parties are some fictitious agency of the Nigerian government, or the scammer themselves once a payment from someone else is made available to them). Once the victim starts "donating" funds for the cause put forth by the scammer, the scammer tells the victim that additional money is needed for unforeseen expenses, similar to most other variants; giving excuses similar to those mentioned earlier. Many scammers would even go to the extent of emotionally blackmailing the victim. For example, a scammer would say that as sponsor of the children, the victim is legally liable for such costs. In some cases, a scammer may pretend to be a student and would claim that a dormitory fire destroyed everything he owned and therefore he needs the money to re-establish himself/herself !

Case Study 55: Scam No. 10 – Fraud Recovery Scams

This variant targets former victims of scams. The scammer gets in touch with the victim telling him/her that their organization can trail and catch the scammer and recover the cash lost by the victim, provided the victim is willing to pay for this service. Alternatively, the scammer may tell the victim that a fund has been set up by the Nigerian government toward reimbursement for victims of 419 frauds. Scammer may further tell the victim that all that is required is proof of loss (scammer uses this as a bait to collect personal information of the victim) and a processing and handling fee to send to the victim the amount of the claim. In this ploy, the scammer is trying to exploit victim's utmost need to recover their lost money, as well as the fact that the victim fell prey to such tricks and are, therefore, prone to get trapped into such scams. Often, these scams are conducted by the same scammer who cheated the victim in the first place, as an attempt to ensure getting every penny possible from the victim. Alternately, the original scammer "sells" information about the people he has scammed. To be on the safe side, the scammer would terminate contact, with another scammer who is also involved in the recovery scam. Sometimes the scammer impersonates the leading "fraud-related crime-fighters" in Nigeria, the Economic and Financial Crimes Commission (EFCC), which not only adds credibility to the scam, but tarnishes the reputation of the EFCC once this second scam is discovered.

Case Study 56: Scam No. 11 – Pet Scams

This is a scam derived from the adoption of a puppy or interesting pets such as African parrots, Peacock, Siamese cats, etc. A scammer first places a commercial announcement or sets up a webpage to present puppies for adoption or for sale at an incredibly low price. For this, the scammer typically uses stolen images from other websites and reputable breeders. When a victim calls back the scammer after seeing the advertisement and asks why the price is so low or asks why such expensive pet is being given up for sale/adoption, the scammer tells the victim that they (i.e., scammer and his/her so-called family) is migrating to some other country for work (usually volunteer work as missionaries – this is to generate sympathy and empathy in targeted victims mind!) or for studies. Further, the scammers claim that he/she will have no time to look after the pet given the movement plan.

Additionally, the victim will be told that the weather in the region/country that they are moving to, is like to affect the pet, or the scammer may give the excuse that that they already have too many pets to care for. In most cases it so happens that the potential victim is well targeted by studying victim's fondness for pets. In a typical "pet scam," the scammer exchanges a few E-Mails with victim to build trust. Once it is known that the victim is able to arrange a right home for the pet, the scammer offers to ship the pet, and requests the victim to only pay for shipping, or the scammer changes the original

price substantially to make it sound legitimate. The victim, who by now has an emotional bond with the pet, feels obligated and even happy to do so, as shipping is a small price to pay compared to the pet's full price at a shop or breeder. The scammer assures to complete the transaction in a timely manner so that the pet gets ready to enter a new home and the victim is now thrilled. However, after wiring the money, the victim does not get the pet (because it never existed). If the victim ever hears from the scammer again it is only for extracting additional money [(to get puppy out of airport custody, or to pay unexpected vet bills that have come up due to pet's (pretended) illness due to journey)]. This goes on until the victim stops responding.

Case Study 57: Scam No. 12 – Bona Vacantia Scam

The English term "bona vacantia" refers to property that does not any more have an owner, and is taken over by sovereigns. Depending on the country, there are different names for this procedure. For example, in the US, there is no official name for this; it just consists of land that is free, that is, not claimed by anybody, and, as a result, the property goes to the government. However, if everyone is not aware of it, you can recover it. In the UK, "bona vacantia" is a property without owner, that is, a property which has been passed to the Crown. The administration of the property rests with the Bona Vacantia Division of the Treasury Solicitor's Department. Some cases of this type of scam show that fake E-Mails and letters, claiming to be from this department, have been reported to inform the beneficiaries that they are going to benefit from an inheritance and that they need to pay a fee before getting more information or releasing the money.

Bank accounts, company assets, property or anything else that is worth the money counts as "unclaimed property" in these situations. There are cases in which people die, but they did not designate their property or items to people. Whichever department is in charge for supervising the money or property, administers them until a heir or other beneficiary can collect them as predetermined in some kind of will. These free properties or money are not kept undisclosed but advertised in the local paper, or through a website and they may request some vital personal information such as a full name or perhaps relations names and that information is validated against the list to see if there is property for the inquirer. At times, names of relatives will be required.

Given this scenario, scammers have used the possibility of this situation to their advantage for a long time. There are people who would be very receptive to the idea of receiving property or funds from a relative they did not know about. Such people can be preyed upon by scammers who just want their money. In "Bona Vacantia Scam," the scammer randomly shortlists some names from the telephone directory, E-Mail Spyware, etc. from where the person's name is available; this could even be from social networking websites. The victim is then contacted by E-Mail or letter and told he/she is heir to money that has been unclaimed. This communication is made to look very official and genuine.

Availability of bona vacantia, or unclaimed funds, is usually advertised on the Internet or by other means declaring that there are unclaimed funds and one should apply, giving their name and other personal information so that a check can be made to see if they are on the list. You might even have to enter names of family members. If there are unclaimed goods or funds matching the name of the person inquiring then they are contacted asking for more details to be submitted. The entire process takes place via letter or E-Mail and there is no agent involved. Knowledge about how recovery of unclaimed goods really works helps a person stay away from such scams.

The next step is that when the victims respond to the communication, they will be asked to give their contact details. Usually a phone call will be made saying the goods are available but there are expenses or fees that must be paid before they can be released. In almost all cases the victim will not

ever hear anything about the money they sent but the requests for additional payments will continue until the victim stops responding, having realized that he/she should not pay more to the con men. In cases like these knowing whom you are speaking to and being able to verify the same with a service such as info-trace.com/area-code-906.jsp, can save much time and money because it would be realized that the agent is not who he claims to be. Personal cheques are even better for scammers, as it allows them to get more out of you. With the information on your cheque, such as your address and account number, they can empty your accounts. Sending a personal cheque to a con artist can result in identity theft. Absolutely avoid these correspondences if you can. If you do want to investigate these claims, consult the appropriate government agency to check up on them.

Case Study 58: Scam No. 13 – Fake Job Offer Scams

These scams are also known as "employment scams" – they are a form of criminal activity perpetrated by unscrupulous individuals or organizations posing as recruiters with personnel needs and/or hiring agencies that offer, and promise, attractive jobs and big money to people seeking for employment opportunities or interested in working in certain business sector. This scam is aimed at persons who have published their resumes on job sites. The scammer sends a letter with a falsified company logo. Typically, the job offer seems to provide extraordinary remuneration and perquisites. The offer also mentions that the victim needs a "work permit" to be able to work in the country. To make the strategy believable, scammers do not forget to mention the address of a "government official" to contact – obviously it is all bogus. The fake "government official" then starts fleecing the victim by extracting "fees from" the unwary victim for the work permit and other matters. These days everybody is looking for a highly paying job and scammers take advantage of that psychology to create this kind of scam. The result (as seen from the target's perspective) is that the "targeted" applicants seem to receive bogus job offers via E-Mail with scanned appointment letters, work confirmation, and employment contracts from well-known employer. Later on, the victims are instructed to contact specified tour agencies, immigration agents and solicitors (apparently all abroad). These agencies and agents are supposed to assist them in getting them the required work permits and visas.

You should watch out for certain doubtful points and ambiguous information that might make you distrustful about false claims and likely employment scams:

1. Be cautious with job search or training services that promise or imply "guaranteed" results or any other statement assuring job opportunities that look "too good."
2. Be wary about any payment and be careful before even making a slightest amount of payment. Get in touch with official job consultants to seek information on the realistic value of the offered courses and diplomas.
3. Never pay any upfront fee for placement services that offer a "dream job."
4. Be careful with agencies stating limited time reduced rates or special deadlines to apply for a position. They will warn you to apply (and pay) before a date. In other case, the wonderful job opportunity will vanish, and your name will be removed from the list of "lucky" applicants. After the famous deadline, the offer is the same – with another deadline, of course.
5. Be wary of companies or agencies offering salaries too high for the promised job. Many of them offer fantastic starting incomes, which cannot be farther from the reality. In case, you are interested in such services, the best option is phoning or getting in contact with some company to inquire about this specific subject.

6. Of course, never depend on oral promises.
7. Be careful with listing or bank services that provide third parties with access to your resume. In this case, privacy and confidentiality must be sealed and protected, and the activity of such agencies must strictly comply with privacy policy and data protection regulations, and internal security rules that guarantee the highest possible protection of stored data.
8. Job seekers should not be duped by any promise of a refund if no job or lead materializes, which is an excellent incentive to bait those people not willing to pay money for a failed job search.
9. Be aware that fraudulent employment services will use an endless string of excuses for why you are not entitled to a refund. For instance, a request for copies of the rejection letters from the companies. The problem is that, in the most of the cases, you will not receive any of such letter from those companies, which are not obliged to reply.
10. In such cases it is advisable to seek for information on the prospective employers or recruiter through another source and contact them directly or visit their o□ces in regular business hours.
11. Forget about companies with no legitimate street address and companies or agencies that refuse to provide verifiable references.
12. Be cautious of fake references. Several websites dedicated to scam job seekers draw on remarkable lists of people who supposedly found a job through their services. An assortment of express testimonials from people already working on the ship (e.g., with cruise ships or oil rigs), including photos/images of smiling persons sporting their new safety helmets and dressed in neat company uniforms seen at their workplaces.
13. Keep in mind that there are many cases where such scammers are fully aware that many of their potential victims will go all over the Internet to seek information and references about the "agency" and its services. Therefore, scammers often post bogus messages in forums and interactive websites devoted to job hunting and career planning. There have even been cases of websites and forums edited and managed by these same tricksters just to fill them with multiple fake threads started and continued by supposed forum members engaged in long discussions, showing generally favorable opinions and perceptions toward the subject.
14. Watch out for companies or agencies who ask for your financial information. Legitimate employers do not usually need credit card or bank account numbers, which is just an option of direct deposit of paycheck.
15. Wait until the personal interview at the company's offices before agreeing to a direct deposit option, refusing to accept the job if this is the only option offered by the supposed employer.

Case Study 59: Scam No. 14 – Rent Scams

News of such scams is rampant in newspapers. People are on constant move – the workforce today is really global and people do travel all over the world in connection of their work, be it students, professionals and many others. Sometimes, people moving from one place to another want to sell or rent their real-estate property (house, apartment, etc.). Scammers take advantage of the fact that people

need accommodation or the fact that accommodations are on sale. Scammers are on the look-out for foreign students, doctors, etc. who try to contact a landlord who could offer an accommodation. After the conditions are negotiated, a fake cheque is sent for a larger sum than agreed to. After this, some "emergency" situation is "created" which requires part of that sum to be urgently wired back. It may also happen the other way round, wherein a fraudster advertises on the Net about a lodging facility and indicates that money needs to be wired as an advance payment. The victim ends up realizing that there is no accommodation! One of the tricks used by rental scammers is to pitch the rent of the "fake" lodging arrangement below the regular rental rate in a certain market. This becomes an attraction for the person looking for inexpensive lodging. This also allows the fraudster to accept as many E-Mails or inquiries as likely. You should not allow yourself to become a prey of such tricks.

You can actually scrutinize a "rent scam" mail by looking out for the following:

- Does the E-Mail begin by addressing you with Sir/Madam?
- Are there too many wrongly spelt words in the E-Mail?
- Are there character mistakes in the E-Mail? For example, Hello, my name is Susie.
- Is there excessive capitalization?
- Does the E-Mail allude to words such as "UK," "Cashiers' Cheque," "Nigeria," "Doctor," "Reverend," etc.
- Is the E-Mail from a free E-Mail provider, such as gmail, yahoo, AOL (America Online), hotmail?
- Does the E-Mail refer to another person or agent?
- Does the E-Mail mention "wanting to move in site unseen"?

If the E-Mail has most of the elements described above, then there a good chance that it is a scam. If you are unsure, it is best to not reply to the E-Mail.

Case Study 60: Scam No. 15 – Attorney Debt Collection Scams

This type of scam involves law firms collecting money owed typically to Asian companies. The scammers aim at law firms by using certifiable company names. This is a very professional scam, and you could be the target – so watch out if you are lawyer. If the scammers approach you, they will say they represent a manufacturing company somewhere in Asia. When you check on the company, you will be able to verify that it exists and is a legitimate company. Remember that creating fake websites is not at all di□cult. The story is that they want you to represent them for collecting a debt owed by a company in your county or state. They will ask you to submit a fee contract, and they will sign this and return it.

Scammers will then inform you that they have informed the debtor about having employed you and that shortly you will be notified that the debtor is paying the debt. You will then receive a certified cashier's cheque delivered by FedEx or DHL. You are required to place this cheque in your trusted account, and when the cheque is cashed you take away your fee and costs, and wire them the balance of the collected firms. The cheque may be drawn on a genuine bank that you would be aware of. Victims are then asked to take a percentage and wire the remainder to a bank in certain country – typically, Korea, China or somewhere else generally in Asia. The bank, which this cheque is drawn on, has nothing to do with the scam. The cheque is bogus!

Bankers advise that instead of depositing a suspicious cheque in your trust account, you can request that your bank send this cheque directly to the "issuing" bank and request collection. This avoids the

embarrassment of a bounced cheque in your account and should put everyone on notice that you are concerned about this cheque. One of these scams seen was very well done until the instructions for wiring the funds were given to the attorney. A tip-off was that the address in the wiring instructions had nothing to do with the legitimate front company they claimed to represent.

If the bank did not show due diligence and did not notice that it was a fake cheque, and if they deposited the funds in your account, then you would never ever have any reason to believe that this was a fraud of any kind. However, there was an attorney in Texas who actually had a cheque honoured by the bank, and wired the money to the scam address. Later the bank came back and emptied his account when the forged cheque was discovered. The bank will go against you even if they have some liability. You do not want to get into a major court case trying to protect a forged cheque. You will have a tough time trying to give reason for money that is taken away from the naive bank. If you believe a collection matter or similar scam is occurring, you should find an autonomous source for the "client" address and get in touch with them to confirm that the person who contacted you actually comes from the genuine company. Also you can call the local "debtor" and ask them if they have done business with the so-called creditor company.

What really bother is that both the "creditor" company and the "debtor" companies are real companies and have nothing to do with the scam. The best tip-off is the bizarre "wiring instructions" which will be sent to someone not related to the "creditor" who "hired" you. Some attorneys experienced that when investigation agencies were contacted about these scams, those agencies showed little interest. So be aware that you could pretty much be on your own. According to some people, the scammers prefer to be located in certain countries where it is easy for them to operate; probably due to weaker laws and possibly for many other reasons. Therefore, it is always good to check on the country mentioned on the envelop that brings the cheque to you. If the envelops originates from certain countries that are known to be infamous for frauds you can pretty well be sure that this is a scam.

Case Study 61: Scam No. 16 – Malware Scams

Malware and Trojans are explained in this case study. We have got so used to Internet convenience and the search engines running on them. Have you ever thought why it is possible for you to use the Internet for FREE? It is because there are sponsored links on the Internet and there are banner ads (advertisements) on the sites that you visit.

Be aware, however, that the third-party cookies store information about you, addresses of the sites that you browse, the IP address of your computer, in fact the entire site-to-site traffic flow. The information stored in these cookies is served to organizations that have presence on the Internet for the online marketing of their products. These practices can harm you in that your "personal information" is changing hands. Using malware to infect computers is now a very popular scam. At times the objective is to just turn the infected machine into part of a very big Botnet where computers are remotely manipulated to send Spam or attack networks. At other times the objective is to steal the identity.

There are a couple of scenarios under which these scams run. For example, anyone who has a blog has probably seen blog Spam; comments to the blog simply try to entice people to go to some other site. Most of the time, the site being advertised is merely trying to enhance its search engine rankings to create more revenue advertisements. The more links there are to a site, the more popular the search engines becomes. It is often thought that "blog Spam" is a good way to enhance the search engine rankings. In some cases this turns malicious. Some sites participate in extensive intellectual property theft to improve their rankings.

In yet another scenario, a "business" contacts you saying that your computer is running slow or is infected with malware. They will then direct you to a website and ask you to download some software;

this software can be in many forms – it may allow the scammer to gain access to your computer in order to find personal information and bank details. Here is how it works. The person or group launching the attack transmits an E-Mail message. The more authentic it looks the better. The idea is to have the receiver open the attachment that is sent through the E-Mail. Once the receiver (the victim) opens the attachment, a malware gets installed on his/her computer. Although the next happening depends on what has been installed, the results can be catastrophic. Scammers can purchase malware viruses online at a small price. Alternatively, scammers can purchase an entire virus pack with updates and 1-year technical support with an affordable fee. This activity of scammers is rampant, and at the same time more complicated and hard to spot as time goes on. The job search site victims would have no clue about a problem until it was too late.

There are ways to avoid becoming victim to malware scams:

1. Remember never to open an E-Mail attachment from an unknown person. Everybody is a suspect when it comes to online security and online privacy matters! Even those from friends should be suspect unless it's something you expected (their computers could have been taken over without them knowing).
2. Treat every attachment as suspicious. Never open anything with a suffix of .exe, .scr or .rar. Remember always that Trojans can be concealed in many ways, including pictures, which usually have a .jpg or .gif suffix – most of them may not cause harm.
3. Make sure you have a good firewall and antivirus software. Both are crucial and vital assets in your computer. They are definitely less expensive than having a bug removed.
4. It is a good idea to use a mail filter or a Spam guard. It offers you a chance to inspect your mail before you download it onto your computer, and delete any items you do not want on your hard drive, as well as blacklist certain E-Mail addresses. It is gratis, and a very helpful tool to get rid of Spam and well as potential viruses. This is one area where being suspicious works well. Until you know otherwise, assume everything is malware. If you do banking transactions online, do verify your account transactions regularly for doubtful activity. Depending on your usage, you should review the monthly statements from your credit cards and debit cards. You should also validate your credit file twice a year to see if anyone has attempted opening accounts in your name.

Case Study 62: Scam No. 17 – The Advance Fee Fraud

Fraudsters often succeed because they are good at exploiting people's confidence or naivety. An "advance-fee fraud" is a self-confidence ploy in which the targeted victim is influenced to move forward financial funds with the expectation of achieving a considerably bigger gain. Thus, as the name suggests, a "confidence trick" or "confidence game" (also known under other terms such as bunko, con, flim flam, gaffe, grift, hustle, scam, scheme, swindle or bamboozle) is an attempt to defraud a person or group by gaining their confidence. In this game, the victim is called the mark. The trickster, that is, the scammer who pulls the trick is called variously as confidence man or con man or confidence trickster or con artist. The accomplices, involved in the game, are referred to as "shills." A "shill" is the professional help – the shill is paid to help another person or association to sell goods or services. The shill pretends as if he/she has no association with the seller/group and gives onlookers the feeling that he or she is an eager customer. "Shilling" is an unlawful activity in many situations and in many jurisdictions because of the repeatedly fraudulent and detrimental nature of their actions.

People involved in the scam may be real; however, there could be impersonated people or fictitious characters played by the con artist. In this scam, the fraudster looks for many kinds of victims. For

example, the victim could be the wife or son of an expelled person who has amassed considerable wealth from illicit means; or it could be a bank employee who is aware about a wealthy person on death bed with no family or any other close relatives; or a rich foreigner who has made a bank deposit just before being killed in a plane crash (leaving no will or known next of kin); or it could be a soldier who by sheer luck has hit upon a hidden cache of gold; or a business being audited by the government; or a disgruntled worker or corrupt government official who has embezzled funds; or a refugee and so on. The money could be in the form of gold ingots, gold dust, money in a bank account, blood diamonds, a series of cheques or bank drafts, and so forth. An interesting thing to note is that typically the sums involved are usually in millions of dollars, and the investor is promised a large share, typically 10% to 40% if they assist the scam character in retrieving the money. In relation to the business of diamond trading, an interesting term "blood diamond" comes into picture. It is also called a "converted diamond," or "conflict diamond," or "hot diamond," or a "war diamond." Blood diamond refers to a diamond obtained through mining in a battlefield and sold to finance a rebellion, invading army's war efforts, or a warlord's activity, usually in the African subcontinent. Several operations are well organized in Nigeria, with offices, temporary fax numbers, and often contacts at government offices. When the victim tries researching on the backdrop of the offer, he/she will end up finding that all pieces fit together. Scammers operating with "advance-fee fraud" often attract wealthy investors, investment groups, or other business entities into scams and the result is large losses of multi-million dollars. However, there are also scammers who operate as part of smaller gangs who do not operate so "professionally" or gangs that operate independently. Scammers, operating in such scenarios, have lesser access to the connections mentioned above and therefore such small-time scammers may not have big success with wealthier investors or business entities attempting to research them. However, even the small-time scammers are able to convince middle-class individuals and small businesses, and can extract hundreds of thousands of dollars from such victims.

If the victim agrees to the deal, the other side often sends one or more false documents bearing official government stamps and seals. Often a photograph used by a scammer is not of any person involved in the scheme. Multiple "people" involved in schemes are fictitious; the author of the "WEST AFRICAN ADVANCE FEE SCAMS" article posted on the website of the Embassy of the US in Abidjan, Côte d'Ivoire, believes that in many cases one person controls many fictitious personas used in scams.

Case Study 63: Scam No. 18 – Babysitting Scams

These scams seem to be more common in the western countries. They are also known as "Nanny Scams." These scams are said to be another variation of the "advance scam". Babysitting scam\Nanny scam involves recruiting unsuspecting individuals for non-existent babysitting, nanny, or au-pair employment, that is, couple to be employed.

In one variant of this scam, a potential employee may be lured by the offer of an "advance." In another form of this scam, the victim may be asked to verify pricing and ultimately purchase items for the scammer's non-existent child. At times, victims are asked to provide résumés, references, etc. to get the victim believe that the "employer" is genuine and that the high remuneration offered are valid. Scammers are smart enough to make the victim stay focussed on his/her worthiness for employment – this way, scammers succeed in making the victim diverted from thinking whether the offer itself is worthy of replying to.

Nanny scams seem to have become a common feature in the online babysitting community. If you receive any E-Mails analogous to the examples mentioned below, be careful! Keep in mind that the names (and ages) used in these scams are constantly changing, so pay close attention to the structure of these

E-Mails rather than the details. Also note that most such mails will typically have many misspellings and grammatical errors. As you read on, you will see the examples provided of some typical mails received by the victim. These examples show that under the pretext of the babysitting job, victim's personal details are being sought! Interestingly, in almost all the babysitting scam mails, the scammer is saying that he/she is currently not in town but will be returning soon. As mentioned before, most of the times the scam mails happen to have lots of misspellings and in most such mails you will find that the grammar is also not up to mark. You will also notice the extremely informal and "slang" language used.

Note that in most of the babysitting scam mails, tempting offers are made, that is, accommodation, transportation for the candidate, etc. Also, in almost all such scam mails, the language sounds very informal, extra sweet and extra friendly; naturally because the scammer wants to lure the victim!

Typical Babysitting Scam E-Mail Example

My name is Mrs. Ashleen Joseph. My husband Philip is a Captain of a cruise ship and I have a daughter whose name is Anabella. Currently, we are on my husband's ship on a holiday and will not be back until about two or three weeks time. We live in a large apartment and I require a babbysitter who would also help me out taking care of grocery purchases. We are OK to pay $18 per hour. Can you tell us for how many hours you would be available. We can provide a Toyata Camry for you to take care of transportation problems.

I would like to know the following about you to consider you for this job:

1. What academic qualifications do you possess?
2. Do you have any good certificate to support your prior babysitting/Nanny experience?
3. How old are you?
4. Are you married?
5. Do you have any special aptitude?
6. Do you have any crime records?
7. Do you have a valid driver's license?
8. Tell us more about your temperament.
9. Can we have one or two reference(s) from you?
10. Can you handle finances if you are given a task to carry out?
11. Will your husband/boyfriend/parent support you taking up this job?

Let me know if you will available for the work offer.

Thanks and have a nice day

Mrs. Joseph

Case Study 64: Scam No. 19 – Nigerian 419 Scam

This scam has got this name because of the Nigerian Criminal Law has a section number that applies to it. You have read about the "advance fee fraud" scheme described earlier (Scam No. 17). You will realize that the mentioned scams are similar in nature. A typical example of the infamous "Nigerian Scam," (also known as) "419 Scam" is as follows:

Dear Sir,

At the outset I must first ask for your assurance in this matter; this is due to its nature. This matter is extremely sensitive and top secret though we know that a transaction of this size will make someone

nervous and at the same time elated but we are telling you that all will be all ok by end of the day. We are determined to contact you because there is some exigency in this transaction as we have been convinced about your discreetness and capability to work with such type of transactions.

Let me first introduce myself fully. I am Mr. Mohamed Abbas working as credit officer with the Union Bank of Nigeria plc (uba) – I am at their benin branch, I got information about you while I was looking for a dependable and highly regarded individual to take care of this highly top priority and crucial transaction. The work is concerned with transferring large sum of money to an overseas bank account and that is why this transaction is to be undertaken with due care.

Here is the offer:

A foreigner and an American, late beninggr John duke (snr) a diamond merchant with the federal government of Nigeria, until his unfortunate death few months ago in Kenya Airways plane (airbus a3k-300) flight kq430 banked with us at Union Bank of Nigeria plc benin and had a closing balance as at the end of March 2001 worth $36,662,000 USD, the bank now expecting a next of relatives as the heir. This bank has put in lot of effort to contact any of the dukes relation or family but the bank has not got any response so far. We believe that this is happening due to the alleged probability of fewer chances to locate any of beninggr John duke (snr) next of kin (as per our records he was not married nor had any children from his affairs with Women).

The management is being pressurized by our chairman and board members as well the directors of our bank. The bank has made arrangements for the funds to be declared "unclaimed" and if no claim comes in soon, the bank will donate the funds to the arms and it is feared that this may trigger a war in Africa and the world in general.

In other to avoid this negative consequence some of my trustworthy colleagues and I now request your permission to have you stand as the next of family connection to the late beninggr John duke (snr) so that the money will be made free to be paid into your bank account as the receiver as the kin, all document and proofs to enable you get this funds will be carefully handled. Our bank makes it mandatory for us to officially declare the recipient of this large fund at the earliest possible. That is the reason you are seeing this mail. We assure you that you that there is no risk involved in this.

As soon as you send acknowledgement to confirm the receipt of this note and in acceptance of this joint business proposal we shall inform you about the modalities involved and payment ratio to suit both parties with full clarity.

If you accept this proposal do not take due advantage of the trust placed in you. Kindly send your reply immediately with the e-mail address providing us with your most confidential telephone; fax number and your exclusive bank account particulars so that we can use this information to apply for releasing the funds into your account in your favour.

Thanks in advance in anticipation of your kind co-operation

Best regards

Mr. Mohamed Abbas

This method of deceit has been in existence through regular postal mail for more than 20 years. Now it is even more rampant due to the advent of the Internet and (free) E-Mail. Recall that it is possible to create E-Mails from fake E-Mail accounts. Over the last few years, literally thousands of people have received countless E-Mails like the one above. With respect to the sample scam text mentioned above, read what follows.

The nature and exact text of the "preposition" varies from letter to letter, as well as the purported author. Even then, there are a number of features common to most (but not all) that instantly identify them as "419" scams/Nigerian scams:

1. Often, but not always, the scam mails are written with ALL CAPS, as shown in the example. The joke in circulation is that there must be an epidemic of keyboards with broken Caps Lock keys in Nigeria!
2. As in this example, the mail/message or letter is characterized with bad syntax, malapropisms and misspellings – not expected of a writer who claims to be in high ranks, for example, a bank manager or oil industry executive, etc. One should indeed find this suspicious given that Nigeria and several other West African nations have English as their official language.
3. Interestingly, in most instances of this scam, E-Mails seem to originate from an African country and/or individual, usually Nigeria although there have been examples of such scams allegedly from Senegal, Ivory Coast, Togo, Ghana, Liberia, Angola, Chad and South Africa as well. Asian and Eastern European countries too are not lagging!
4. Almost always the scam communication mentions about "large amounts of funds" – millions of Dollars and it also mentions about those funds being "trapped" or "frozen" for a variety of ostensible reasons: "double-invoiced oil," and unclaimed accounts belonging to victims of African air disasters or other (alleged) deceased persons are among the most frequently seen versions.
5. They will typically make an offer to you, as the beneficiary, a hefty portion of these funds as a "commission" or "reward" – saying that all you have to do is to send them your bank account numbers. They will also cleverly indicate that the more such account information you send, the quicker your share of the "proceeds" will start coming into your account. The message will also indicate that your fast response will help them transfer and "release" the funds from the clutches of the inexperienced administrators, greedy bureaucrats, etc.
6. In most cases, they please you to act "immediately" giving some convincing reason or the other to make you swing into action. They often refer to some sort of "statute of limitations" or other legal constraint that is about to run out of time and they also say that they will send back the funds to the government or other entity that would undoubtedly use them for undesirable purposes.

Case Study 65: Scam No. 20 – Craigslist Scams

"Craigslist" is the idea that was conceived by Craig Newmark and has become one of the most popular sites on the Internet. Craigslist started in 1995 at San Francisco – it is possibly the definitive site for confidential program. Posted here are advertisements for employment opportunities, personal ads, and advertisements for cars, sale of pets, home supplies and a large number of other options. The website is created for various communities. Today there are 450 cities and countries throughout the world where Craigslist offers sites. A worth over 10 million US dollars (US $) is attached to Craigslist according to business experts. Unfortunately, this online classifieds website has been plagued with scammers using advance-fee fraud and similar techniques, usually involving fake cheques, to con people of their money. If you are selling anything under $1,000 on Craigslist or eBay that cannot be shipped, or if you are renting a room (remember the rental scam described earlier) you are at high risk of a fake cashier's cheque scam on Craigslist. These scammers are in search of low priced auctions, low sales prices and rental services because they have printed out bogus cheques. Their objective is to send you the bogus cheque for more than your original price or original rent, and have you give them back the extra real cash.

Occasionally, there are fraudsters who contact an individual interested in buying or selling things on Craigslist – the fraudsters then try to pull off the exact same scam. Many of the Nigerian 419 scam features (see the previous illustrations) are used regularly on Craigslist. This includes persons conducting transactions from another country, sending bank cheques that look believable, sending money that is excess over what is owed, and requesting that money be sent back to the scammer through wire transfer.

Lately, there is another advance-fee technique that has been used on Craigslist. In this method, fraudster will contact for the sale of an item and will ask the seller to dispatch the item to a location to another country. The seller then dispatches the item and furnishes the tracking number. However, the scammer never pays! At times the scammer will use someone who is offering an accommodation for rent and will pose as someone migrating from another country. The fraudster will create a situation in which it looks like there is a dire need to have the accommodation in advance. The fraudster also asks if it is possible to get the occupancy with some deposit money paid. The deposit cheque sent by the fraudster will be a bogus cheque; however, the amount written on that cheque will be far more than the deposit amount asked for by the seller. When the cheque is received by the seller (the target victim), the fraudster will ask for the excess amount to be refunded. The fake cheque will bounce and the victim will lose the amount he/she "refunded" to the scammer!

There is a related con that takes place on the rental model, particularly in the UK – the scammer places an advertisement on a "classifieds" website such as Craigslist or Gumtree pretending to seek an accommodation on rent. The scammer mentions an incredible depiction using photographs borrowed from other advertisements or other websites. The victim gets in touch with the scammer to get a viewing. However, the scammer tells the victim that to do so, the victim must go to a Western Union outlet, must transfer money to a relative to cover the amount of the deposit and must also furnish a scanned copy of the receipt in support of the money transfer made. Supposedly, this is to confirm that the victim has enough money to cover the deposit before they view the accommodation. The fraudster also tells the victim that he/she will get the money back after the viewing. In reality, however, the place offered for accommodation may or may not exist, and the receipt allows the scammer to have the funds with no viewing ever taking place.

Again, the scammer sends a rental application, or asks for some details that are typically mentioned on a rental application form, such as driver's license number, bank account information, Social Security Number or its equivalent, etc.

Below are some tips to note about a Craigslist scam mail:

1. When you do a posting on Craigslist you will get lots of E-Mails. You can spot a Craigslist scam because it has the poor wording in the E-Mail. Most of the Craigslist scams come from another country where English is not the native language. Many mails may just be the result cutting and pasting E-Mails together!
2. Craigslist scams typically have the long-wound, that is "verbose" text in the E-Mail. Typically scammers mention lots of unrelated details, that is, they mention things that have nothing to do with what they are dealing with (remember the style of writing seen in the examples for "Babysitting/ Nanny Scam" E-Mails). Scammers typically write long rambling sentences about their so-called "family problem" to gain sympathy from their victims, or it could be verbose text about the urgency of getting the transaction done, or they may tell you in a long-wound way that they know you are a good person deep down. Most of the time, there is no need to go that far – the wordy text in the mail is the tale-tale sign of a Craiglist scam!

3. The next step to spot a Craigslist scam is characterized by the mention of "religion" and a huge amount of compliments or apologies for bothering you. Somehow they believe that if they say sorry with words sounding sincere or if they keep on mentioning about religion, they will either baffle you or will make you comfortable. Typical Craigslist scammers will use flowery language in their communication with lots of religious notations thrown in.

4. Another trademark and a good way to spot a Craigslist scam is the payment by cheque or money order. There is always some reason because of which they cannot meet you and send you a cheque. Another one is that they have already sent you the cheque and entered a wrong amount. Regardless of how this Craigslist scam appears, the outcome is the same, the cheque is not good!

5. If there is a mention in the mail about some offer to pay you for your problem, it is a way to guess that it is a Craigslist scam. The trick used by scammers is to make you feel that because they are bothering you so much, they offering you something to compensate for your trouble. Only problem is the cheque, money order or any other method they come up with is always bad and you will wind up losing your money.

Case Study 66: Scam No. 21 – Pyramid Scheme Scams and Ponzi Scheme Scams

They can also be called as "pyramid scheme frauds." The way fraudsters in this team operate is in the structure of a pyramid. A pyramid scheme is considered to be a non-sustainable business model – it involves making payment promises to participants mainly for getting other people into the scheme. Any real investment or sale of products/services to customers/consumers is not intended. Basically, pyramid schemes are a form of fraud. Many countries have banned pyramid structures. Although these kinds of schemes have been around for a very long time, some people have a view that multi-level marketing which has been legalized is nothing but a pyramid scheme.

A successful pyramid scheme uses a fake but seemingly believable business with a easy-to-understand yet advanced-sounding money-making method which is used for profit. The basic concept is that "Person A" makes only one payment. To start earning, Person A has to get in the chain like others who will also make one payment each. Person A gets paid out of receipts from those new recruits. This way, they go on to recruit others. As each new recruit makes a payment, Person A gets his share. As the "business" expands, he is promised increasingly greater benefits.

The concern is that "businesses" based on pyramid structure hardly involve actual sales of real products or services with an attached monetary value. To make themselves credible, fraudsters, operating pyramid chains, equip themselves well with fake referrals, testimonials and information. The problem is that there is no end benefit. The monetary benefits only travel "up the chain." Only the originator (referred to as the "pharaoh") and a very few at the top levels of the pyramid make huge amounts of money. The amounts become less and less down the pyramid structure. There is nothing for the individuals at the bottom of the pyramid – these are the people who joined into the pyramid structure, but were not able to get in more members.

A "Ponzi scheme" is a similar fraud. Charles Ponzi was not the actual mastermind in its inception. However, his operation amassed so much money that throughout the US it came to be known as the "Ponzi scheme." A Ponzi scheme is also a fraudulent investment operation. It pays returns to separate investors either paid from their own money or from the money paid by subsequent investigators. The payments are not made from actual profit made.

Basically, a Ponzi scheme is an operation with fraudulent investment. It is a procedure that pays profits to stakeholders from their own funds or money paid by later investors, rather than from any

actual revenue made. The Ponzi scheme usually attracts new investors by offering higher returns as compared with other investments. The benefits are promised in the form of short-term returns that are either exceptionally high or unbelievably consistent. The continuity of the returns promised by a Ponzi scheme and its loud/aggressive promotion is what attracts people (who later turn out to be unfortunate victims!). Fraudsters involved with this scheme cleverly create a perception of ever-increasing flow of money to those who are targeted to be hooked in or already hooked in.

Let us take this imaginary example. Suppose, an advertisement promises amazing returns on an investment – for example, 30% on a 45-day contract. Usually, the motive is usually to cheat ordinary people who do not have deep knowledge of finance or financial jargon. Verbal constructions that sound impressive but are actually meaningless will be used to impress potential investors: watch for words such as "high return investment," "make money in short time without investing," "opportunity for offshore investment," etc.

Initially, without any monetary benefit or objective, or prior information about the investment, only a few investors are attracted to be roped in - usually this is done only for small amounts. About a month later, the investor receives the original capital along with the 30% return. At this point, the investor will have more incentive to invest additional money. As "word-of-mouth" publicity starts growing, other investors would also like to cash the "opportunity" and they communicate their intentions to participate. This results in a snowballing effect based on the promise of returns that are too high to imagine. However, the "return" to the early investors is being paid out of the fund contributed by new entrants and not from the profits made.

One reason that makes Ponzi scheme work so well initially lies in the re-investment that happens initially. The first few investors, who actually get paid the huge returns, tend to reinvest their money in the scheme, in the hope of earning more. This way, the fraudsters who are running the scheme do not actually need to pay far too much net amount. All they need to do is send financial statements to investors to show them the amount earned by keeping the money. In this manner, fraudsters are able to maintain the perception that the scheme is successfully operating with high returns and they continue the deception.

Illustrations of Financial Frauds in Cyber Domain

In this section, we have provided illustrations of banking frauds (including credit card-related crimes), online gambling, IPR crimes, digital media piracy, hacking, computer frauds, website attacks, counterfeit hardware, malicious use of the Internet, social networking victims, etc. The following Table lists the illustrations provided in this section.

Banking-Related Frauds	
List of illustrations in Section	
Title	**Topic**
Stolen Credit Card Information	Phishing and credit card frauds (banking frauds)
Phishing Incidence	Phishing (credit card frauds)
Online Credit Card Theft Ring	Credit card frauds
Understanding Credit Card Fraud Scenarios	Credit card frauds
ShadowCrew – the Internet Mafia Gang	Credit card frauds
Dirty Relations – Goods Delivery Fraud	Frauds from online purchasing

Fake Mails Promising Tax Refunds: Beware	Internet banking
Phone Scam Targets Your Bank Account	DoS (denial-of-service) attack
Cookies and Beacons – The Facebook Controversy	Cookies and Beacons
Privacy Loss through Leakage of Users' Facebook Profiles	Personal privacy loss leading to cybercrimes
Debit Card Frauds – Global Wave in Real Life	Financial frauds with debit card

Case Study 67: Illustration 1: Stolen Credit Card Information

In the previous section, it was mentioned that cybercriminals operate beyond geographic boundaries. With the background of credit card frauds (under "Phishing"), this case is interesting to read.

Stolen credit card information is savored by cybercriminals. "DarkMarket" is an English-speaking Internet cybercrime forum created by Renukanth Subramaniam in London. It was shut down in 2008 after an FBI agent infiltrated it, leading to more than 60 arrests worldwide. Renukanth Subramaniam admitted conspiracy to defraud and was sentenced to nearly 5 years in prison in February 2010. The website permitted buyers and sellers of stolen identities and credit card data to meet on the Net and establish a criminal enterprise in an entrepreneurial, peer-reviewed environment. It had 2,500 users at its peak, according to the FBI.

To the casual observer, there was not much to differentiate the Java Bean Internet cafe in Wembley from the hundreds of others in the capital. But to the surveillance officers staking it out month after month, this ordinary looking venue was the key to busting an astonishing and complicated network of cybercriminals. There were many computers inside the café and a former pizza bar employee ran an international cyber "super market" for selling stolen credit card and account details, costing the banking industry tens of millions. Renukanth Subramaniam, aged 33, was revealed as the founder and a major "orchestrator" of the secret – "DarkMarket website," where elite fraudsters bought and sold personal data, before it was infiltrated by the FBI and the US Secret Service. Membership to Dark Market was strictly by invitation. But once vetted, its 2,000 sellers and buyers traded the whole lot – from card details (obtained through hacking, Phishing attacks), to viruses using which buyers could extract money by threatening company websites. This top cybercrime site in the world offered online tutorials in illicit topics such as account takeovers, credit card deception and money laundering. There were equipments such as false ATM, pin machines as well as everything needed to set up a credit card factory.

Subramaniam, a Sri Lankan-born British citizen, was a past member of ShadowCrew's predecessor. Subramaniam worked at Pizza Hut and as a dispatch courier. In 2004, the US Secret Service uncovered ShadowCrew. "JiLsi" was one of the uppermost cybercriminal in the country. With this criminal, Subramaniam managed to set up a forum globally. Without JiLsi, DarkMarket was just not possible – that was the close association and deep involvement that JiLsi had with DarkMarket. In spite of this being so, DarkMarket's 2,000 members could never meet JiLsi in real life – he truly was a "shadow operator"! Somehow, DarkMarket was finicky about banning "rippers" who would deceive other criminals. Honor among thieves was paramount. Subramaniam was one of the top administrators. He stored his operating system on memory sticks. But when one of his memory sticks was stolen, it cost him £100,000 in losses. It also resulted in compromising the site's security. With this mishap, Subramaniam was downgraded to merely a reviewer. Surveillance officers trapped him logging on to the website when JiLsi was unaware that the fellow criminal MasterSplyntr whom he trusted was, in fact, an FBI agent called Keith Mularski.

Case Study 68: Illustration 2: Phishing Incidence

Here is an illustration of Phishing attack in real life. According to the news posted on 14 April 2010, it could well be termed India's first legal adjudication of a dispute raised by a victim of a cybercrime. The judgment for the first case was filed under the IT Act. In this judgment, Tamil Nadu's IT Secretary ordered ICICI Bank to pay ₹12.85 lakhs (₹12,85,000) to an Abu Dhabi-based NRI within 60 days – in compensation for the loss suffered by him as a result of a Phishing fraud. Phishing is an Internet fraud through which cybercriminals illegally obtain sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity.

In this case, the reimbursement, that is the compensation, included the loss suffered by the supplicant, the travel expenses and the financial loss incurred due to "complete lack of involvement of the respondent bank – as per order from Tamil Nadu's IT Secretary. The order came based on an appeal (i.e., petition) that was filed by Umashankar Sivasubramaniam. As per Umashankar's claim, he received an E-Mail in September 2007 from ICICI, asking him to reply with his Internet banking username and password or else his account would become non-existent. He replied and later he found ₹6.46 lakhs (₹6,46,000) moved from his account to the account of another company. That company did a withdrawal of ₹4.6 lakhs (₹4,60,000) from an ICICI branch in Mumbai and retained the balance in its account.

An application was prepared as arbitration for proceedings under the IT Act. The application was presented to the state IT Secretary on 26 June 2008. In that application, Umashankar held the bank responsible for the loss that he suffered. ICICI Bank, however, claimed that the applicant (Umashankar) had failed to protect his confidential information. According to ICICI Bank, Umashankar carelessly disclosed his confidential information such as password. According to the bank, he became the victim of a Phishing attack because of this carelessness. Bank spokesperson said that customers are fully apprised on security aspects of Internet banking through various means. ICICI Bank officials empathetically said that bank's security systems are continuously audited and neither the security nor bank's processes have been breached.

The bank decided to appeal the order. The bank spokesperson said that ICICI Bank endeavors to offer world-class service to its customers. They further said that they have hundreds types of transactions, which can be completed online without having to walk into a branch. Further, they added that the bank strives for convenience and safety of their customers and uninterrupted availability of services through self-service channels. The bank claims that they also continuously upgrade their systems and technology to ensure that customers get the best experience and a safe environment while transacting online.

Vijayashankarm a techno-legal consultant appeared for the petitioner. According to him, while the order may lead to tightening of cyberlaws in the country, the judgment reflects the lack of accountability of using Internet banking. He further opined that, although Phishing fraud is very common, banks are not accepting the liabilities. In his view, such a ruling will set a good precedent. In India, although there are 300-odd cases of Phishing attacks recorded or contended, most cases do not get pursued under proper legal framework. Some such cases were filed at consumer courts.

Case Study 69: Illustration 3: Online Credit Card Theft Ring

Here is a real-life example of Phishing and Credit card fraud. This case took place in June 2009 and involved 36-year-old Max Ray Butler (also known as Max Ray Vision) resident of San Francisco, California. Max pleaded guilty in Federal Court in Pittsburgh to wire fraud charges to two counts before Senior US District Judge. In connection with the guilty plea, the attorney mentioned in the court that Butler, known widely on the Internet as "Iceman," among other aliases, conducted computer hacking

and identity theft on the Internet on a massive scale. As part of the conspiracy, Butler cracked into financial institutions, credit card processing centers as well as other secure computers with the illicit purpose of acquiring credit card account information and other personal identification information. Several of these cards were made available to Christopher Aragon – he was a partner in crime and was based in the Los Angeles area. Christopher used these cards with the help of a team of associates to buy up commodities for sale. Max sold the remaining card numbers out-and-out over the Internet.

Max and Christopher formed a website known as "Carders Market." They devoted this crafty site for the acquisition, utilization and sale of credit card account information. This illicit process is known as "carding." A main intention of the site was to employ brilliant individuals to assist in carding activity. During the best of times (from criminals' view point), Carders Market had approximately 4,500 worldwide members!

Max was arrested on a criminal complaint on 5 September 2007 in San Francisco. A search of the computer systems in Max's apartment revealed more than 1.8 million stolen credit card account numbers. When these card account numbers were provided to Visa, MasterCard, American Express and Discover, it was revealed that the amount of fraudulent charges on the cards in Max's possession totaled approximately $ 86.4 million. These losses had to be borne by the thousands of banks that issued the cards. On 20 October 2009, punishment was handed: 30 years in prison, a fine of $1,000,000 or both – and that is what the law could provide as a maximum sentence. As per Federal Sentencing Guidelines, the actual sentence imposed was based on the gravity of the offense and the previous criminal history, if any, of the accused. Many agencies were involved in inquiry of Max's illegal activities – Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice; the Federal Bureau of Investigation; the Vancouver Police Department, Vancouver, Canada; the Newport Beach Police Department, Newport Beach, California; and the Orange County Sheriff's Department, Orange County, California; and the US Attorney's Office for the Northern District of California.

If we wonder what happens to the "stolen" credit card data, the following "dark market" price information below is shocking as well as an eye opener. One can well imagine how this information must be rapidly exchanging hands in the global black market (this information is as current at the time of writing this; authors by no means have any validation responsibility here):

1. Data Dumps from magnetic stripes on batches of 10 cards are sold.
2. Standard cards: $50. Gold/platinum: $80. Corporate: $180.
3. Card verification values information needed for online transactions: $3–$10 depending on quality.
4. Complete information/change of billing information needed for opening or taking over account details – $150 for account with $10,000 balance; $300 for one with $20,000 balance.
5. Skimmer device to read card data – up to $7,000.
6. Bank log-ins 2% of available balance.
7. Hire of Botnet Software robots used in Spam attacks – $50 a day.
8. Credit card images: Both sides of card – $30 each. As known to law professionals, an indictment is only a charge and is not an evidence of guilt. A defendant is presumed innocent and is entitled to a fair trial at which the government must prove guilt beyond a reasonable doubt. Source: www.cybercrime.gov

Case Study 70: Illustration 4: Understanding Credit Card Fraud Scenarios

Note that a "fraud" can be defined as willful deceit or trickery or a deceptive or spurious act. In an era of advanced technology, it should be easy to catch criminals and fraudsters. However, the reality is far from this. "Credit cards" are not "anonymous like the paper money" and so, their theft can be traced. Criminals and fraudsters do not give up; in fact, they make themselves technology savvy to keep ahead in the game! They are led by the single aim of reaping the monetary benefits and satisfying that ego!

There are more than 50 different types of cards available in the market – we have considered only the major ones. Visa and MasterCard are made up of member organizations who can be either acquirers or issuers (or both). "Acquirers" are the members of the Visa or MasterCard organizations that handle "Merchants." "Issuers" are the members of the Visa or MasterCard organizations that issue the cards to cardholders. "Merchants" are those entities who "accept" card transactions. "Service Providers" are the entities that provide services related to the processing, storing or transportation of card information on behalf of any of the entities mentioned (Issuers, Acquirers, Merchants). With that preamble, a few scenarios relating to credit card frauds are now explained. Some of them are described in the following pages.

Illustration 4.1. Credit Card Application Fraud

In an "Application Fraud," the fraudster obtains information about a person who is eligible for getting a credit card and has applied for it. The fraudster then makes his/her application to the "Issuer" with that person's details except for the residential address. The residential address of the actual applicant is substituted by fraudster's (mostly temporary) address. The issuer, not being aware of this, would end up sending the card at that address! In another variety of this fraud scenario, the fraudster obtains the card details of an already existing card member (this is done through Phishing attacks). He then calls up the call center of the issuing organization, pretending to be the actual card owner. He reports the card as "lost" and asks them to issue a "replacement card" at his address, informing them also about the change of address. Now, if the issuing organization (typically a bank) is not security-savvy enough to call the actual card holder to validate if he/she indeed had make such a request, the fraudster will get a genuine card at the cost of the scape goat (the actual card owner) to run up whopping bills for his/her own use (which they normally are smart enough to avoid) or to "sell" the card in the "dark market" – the dark market "rates" for "stolen information". With the growing number of Internet-based applications for credit card, obtaining such information would be possible with a man-in-the-middle attack launched. In a typical "man-in-the-middle attack," electronic messages, transmitted through the Internet, are intercepted. The "man-in-the-middle" attack intercepts communication taking place between two systems. For example, in an http transaction the target is the TCP connection between client and server. With the use of di□erent techniques, the attacker divides the original TCP connection into two separate and new connections – one between the client (i.e., the victim's machine) and the attacker and the other between the attacker and the server. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.

Illustration 4.2. Frauds Involving Lost and Stolen Credit Cards

In this scenario, it can so happen that a card holder genuinely loses his/her credit card when he forgets to collect it from the ATM (Automatic Teller Machine – most credit cards can be used to also withdraw cash from ATMs). Card holder may also forget to collect his/her credit card after signing for the goods purchased. There are also many other ways to lose the credit card (leaving the wallet/

purse behind in which the card is or the card getting dropped out of pocket or wallet, etc.) When the fraudster finds a lost card, either he himself uses that for shopping (which is not what the fraudster would typically do) or he sells the lost card to a gang with whom he works. There are many agencies that specialize in credit card-related crimes. For example, the Russian Business Network (RBN) is a multifaceted cybercrime organization, specializing in some cases monopolizing personal identity theft for resale! RBN was registered as an Internet site in 2006. Initially, much of its activity was legitimate. It appeared that the founders soon found that it was more lucrative to host illegal activities and started hiring criminals for their services. RBN provides web hosting services and Internet access to all types of criminal and offensive activities, with individual activities earning up to $150 million in 1 year! Recall "DarkMarket" described in Illustration 1.

Such gangs have multiple layers of operations with many counterparts. Some of them are called "runners." Their job is to show their face in the shops by physically visiting the shops for small amount purchases with the objective of ascertaining whether the "lost" card is put on hold or if it is on "hot list." In other words, "runners" are hired to find out the validity of lost/stolen cards. If the card is found to be "clean," the fraudster would either use the card immediately for a high value purchase (by forging the signature of course) or will sell it in the dark market. Dark market rates for stolen/lost credit cards were mentioned in Illustration 3: Online Credit Card Theft Ring.

Illustration 4.3. The Fraud through Merchant Collusion

This fraud occurs when the "Merchant" joins hands with the fraudster by providing details of the genuine cards in return for a share of the returns from this manipulation. The merchant can allow members of a gang to use his terminal as a host in order to transfer information on credit cards, which are swiped at the merchant's terminal. One way of doing this is that another "swipe" slot is kept hidden or discreetly near the actual swipe machine at the Point of Sale (PoS) terminal at the merchant's establishment. Always be wary and be on the look-out if the merchant is scanning your card more than once for one pretext or the other. For example, by asking you to let him scan it again because the first scan was not successful. Also, never lose sight of your credit card. Always insist that you want your credit card to be swiped in your presence: be it a restaurant or a brand hotel (five stars hotels, etc.). This is important because, as a part of collusion, once the merchant allows his terminal to the members of the fraudster gang in order to transfer the confidential information on the magnetic card on the credit card, that information is gone in the wrong hands! The fraudster's terminal, known as the "receptor" (because it receives the information), downloads the confidential details of the genuine card from the host terminal. This stolen information can be used in a number of ways to cheat the "Issuers," at a later date. The information can be used to manufacture counterfeit cards or to obtain genuine cards by reporting the card as "lost" or to defraud by mail order.

There are instances where the customer also colludes with the Merchant to cheat the Issuer. Customer uses the card at the Merchant establishment, that is, a shop/mall, for a single transaction but allows the Merchant to take multiple prints of the charge slip. The Merchant submits these charge slips with forged signatures and obtains the payment due to him (the Merchant) from the Acquirer. At the end of the card holder's billing cycle, when the credit card statement is presented for payment, the card holder disputes the charge by claiming that the transactions are fraudulent and refuses to pay. Meanwhile, the merchant has already recovered his sale due amount. Because the card holder refuses to pay the Issuer (typically the bank), it is the Issuer who has to bear the loss. The problem is that it is di□cult to "prove" such collusion. Until and unless the same card holder keeps appearing in many such cases of frauds, tracing becomes di□cult. It is said that the card issuers assume a certain

small percent of their overall transactions volume, as "bad debt" and levy it across their base of card holders (which runs in thousands and thousands). They present it in the charge statement as a line item.

Illustration 4.4. Frauds at the ATMs

Card frauds and operation frauds are the two main types of ATM frauds. Research by Retail Banking estimates that worldwide, there are more than 1.5 million ATM (Automated Tailor Machines – sometimes jocularly referred as "Any-Time-Money"!). It is said that a new ATM gets installed every five minutes somewhere in the world! All around the world, people carry out successful ATM transactions (withdrawing money from their bank accounts, viewing their bank balance, etc.). For more than three decades, ATM operations have been going on successfully. However, that does not mean that ATMs are completely risk-free. ATMs, like most other devices that are designed to store and dispense valuable items, have been targets of frauds. ATM thefts, burglaries and electronic frauds committed at the ATM make news lines almost daily, all over the world. Most of the "ATM frauds" reported by media as "debit card frauds" are to do with the compromise of "Personal Identification Number" (PIN). As per reports of Global ATM Security Alliance, only 0.0016% of all ATM transactions are impacted by crime or fraud worldwide. Notwithstanding this claim of "secure" ATM transactions, ATM fraud and security or rather the lack of it is one of the most popular topics in the media!

In Europe, "Card Skimming" fraud is one of the biggest crimes affecting ATMs. Card skimming at ATMs caused losses of 44 million Euros across Europe and is known to be a source of funding for criminal operations in the East European countries. Cash trapping and transactional reversal crimes are on the rise; especially in Eastern Europe. Thieves fix a device to the cash dispensing slot of the ATM – this action causes currency notes to get stuck inside the slot. Criminals return later to remove the cash from inside the dispenser. Trapping attacks like these resulted in losses amounting to 2 million Euros in 2005. ATM market is growing fast in Latin America and highly advanced ATM machines are deployed in this region. ATM card fraud in the Latin American region increased by nearly 15% in the last 5 years. In the Asian region, China and India are the fastest growing ATM markets. China now has more than 86,000 ATMs and the Indian ATM market is growing at the rate of 100% annually as per reports of Frost and Sullivan. The top ATM fraud in Asia is ATM dispenser trapping. Asia has one of the world's highest Phishing attacks.

Illustration 4.5. Carding Frauds

It was mentioned that "carding" involves acquisition, utilization and sale of credit card account information. When a credit card is stolen, the thief does not know whether the card is valid. So the thief wants to find out about the status of the card (active, cancelled, etc.). From the thief's perspective, there are many possibilities – the card holder may have immediately reported the loss of the card or the card limit may have been completely used up. In such cases, the card is of no use to the thief. The smart thief uses the Internet to ascertain if the stolen card is still "good" for use. The thief could use the stolen card to make a small amount purchase using the online purchase facility on the Internet. However, that would involve the "shipping address" and that would expose the thief. So the smart thief uses the stolen card for making a charity donation! That way, the thief does not have to waste time in searching items on the product catalogues on the sale portal of any online seller. The thief makes the donation amount relatively small so that the card limit is not used up. He does this for one more reason – a large amount would make the transaction immediately noticeable. Carding fraud is also used when the credit card is obtained fraudulently through card "skimming" (explained next) or when a Phishing attack is done on the card.

Illustration 4.6. Credit Card Skimming

The credit card skimming fraud is explained here. Card skimming is done with "skimmer" devices. The relative proportions in those images help us understand how tiny the device is and that makes it

simple for fraudster to conceal it out of view of the victim. Skimming is in a way, fraudster's revenge on the Customer Verification Value (CVV).

The card security code has various terminologies attached with it: Card Security Code (CSC), Card Verification Data (CVD), Card Verification Value (CVV or CV2), Card Verification Value Code (CVVC), Card Verification Code (CVC), Verification Code (V-Code or V Code), or Card Code Verification (CCV). The CVV is an algorithm (software program logic) that is very di□cult to break. The fraudster, therefore, does not take the trouble to break the code. He simply colludes with a single merchant or with a group of merchants. He provides the merchant with the terminal number similar to the one provided to the merchant by Acquirer or the bank (because in some cases the bank, that is, the Issuer and the Acquirer, can be the same institution). The only difference is that the fraudster's terminal is capable

of also reading the card data that is recorded on the credit card's magnetic strip. The swiping equipment provided by the Issuer bank/Acquirer can only process the data by connecting to the bank's server but it does not have the capability to record the data on the magnetic strip of the card. Now comes the criminal act – the fraudulent merchant or the fraudster working at the Merchant's PoS (Point of Sale) terminal, swipes your credit card twice – of course without you realizing it; even if you notice it and bring it to his notice, he will give you one explanation or the other why he swiped your credit card more than once. Now, the card is swiped once across bank-provided swiping equipment and second time on the fraudster's terminal. The security code (CVV, CCV, etc.) which is encoded on the magnetic strip on the back side of the credit card, and is decoded on the terminal, gets recorded on the fraudster's terminal. He now gets the genuine card information (card holder name, card number, date of validity) along with the security code! His job is done and he is ready to use that information for creating fake credit card.

It may so happen that in some restaurants, a waiter could have a collusion with a fraudster gang – he could hide the skimmer device in his socks. As you stand near the payment counter for your credit card to be swiped, after taking the card from you, the waiter may pretend to drop it. Then waiter will bend down to pick up the card – on its way up, the card would get swiped across the skimmer device in his socks and you may never even realize it as this may happen in less than minute! In another variant of this scenario, the skimmer device (with a slit type) could be located next to the actual card swiping device authorized to the merchant by the Acquirer. If you are not carefully watching, the fraudster colluding with the merchant (he could very well be the PoS staff of the merchant) after swiping the card with the actual credit card swiping machine, will swipe your credit card also through the skimmer device to read the confidential card details (card number, date of validity and most important the credit card security code – CCV, CVV, etc.) to his benefit!

Case Study 71: Illustration 5: ShadowCrew – The Internet Mafia Gang

This is a case reported in the public domain. It shows how ruthlessly the criminals can operate in the world of credit cards. This illustration has a lesson for all of us that we should take adequate care not to succumb to credit card frauds. Criminals used SQL Injection technique in this case. This illustration also brings to fore an important point – today's cyber fraudsters are tech-savvy people. That is how this hacker gang operated.

"ShadowCrew" was an international crime message board. The board offered a haven for "carders" and hackers to trade, buy and sell anything from stolen personal information (through identity theft) to hacked credit card numbers and false identification. As we know, a bank card number is the primary account number found on credit cards and bank cards. It has a peculiar type of internal structure and it also shares a common numbering scheme. Credit card numbers are a special case of ISO/IEC 7812 bank card

numbers. As mentioned in Illustration 3 (Online Credit Card Theft Ring), "Carders Market" is devoted to the acquisition, use and sale of credit card account information, a process known as "carding."

The genesis of this fraud group is interesting – in early 2002, ShadowCrew emerged from an underground site, counterfeitlibrary.com, and was followed up by carderplanet.com, a primarily Russian site. It was created by only a few of people, most notably Kidd (Seth Sanders), MacGyver (Kim Taylor) and CumbaJohnny (Albert Gonzalez, who would later become an informant for the Secret Service beginning April 2003). Other main people who would become Administrators and Moderators were Deck (Andrew Mantovani), BlackOps (David Appleyard) and a handful of others. Over a period of short time, ShadowCrew grew to over 3,000 members (many were "clones" and inactive accounts) worldwide with a small group of members leading the forums. During its inception, the site was hosted overseas, in Hong Kong. However, shortly before CumbaJohnny's arrest, the server was in his possession. The server was hosted somewhere in New Jersey. The downfall of the site started although it had flourished initially.

The site was doing well from the time it was launched in 2002 until its shut down in late October 2004. Although there were many criminal activities taking place on the site and all seemed well, the members were not aware of what was going on behind the scenes. Federal agents received a major breakthrough when they found CumbaJohnny. During the period April 2003 to October 2004, Cumba helped in gathering information and monitoring the site and those who used it. He started by exposing many of the Russians who were hacking databases and selling counterfeit credit cards. Some of the first to be arrested were Bigbuyer, BOA and Wolfrum. Although they were being arrested, no reports of it being linked to ShadowCrew ever came about at the time.

Case Study 72: Illustration 6: Dirty Relations – Goods Delivery Fraud

Internet seems to be breeding ground for many cybercriminals who take advantage of mail Spoofing, ID theft and many other techniques to achieve their fraud objectives. Online purchasing is possible by sending electronic mails using the Internet and there are ample opportunities for fraudulent people to play mischief by hiding their real identity through fake E-Mails. This illustration shows how this happened in a real-life scenario. Interestingly, it also shows the humantarian approach of the legal system in passing the judgment and giving due consideration in a given context of the crime.

It all started after Sony India Private Ltd filed a complaint. Sony India runs a website called www.sony-sambandh.com, targeting non-resident Indians (NRIs). The website enables NRIs to send Sony products to their friends and relatives in India by purchasing those products online. The company makes delivery of the products to the concerned recipients. In May 2002, a lady visited the website but did not log onto the site with her real name. She assumed the identity of "Barbara Campa" and sent an E-Mail to order a Sony Colour Television set and a cordless phone. In the mail, she provided her credit card number for payment and made a request for getting the products delivered to a person named "Arnavaz Ahmed in Noida area. The payment was duly cleared by the credit card agency and the transaction was processed. After carrying out the relevant procedures of due diligence and checking, the company delivered the items to Arnavaz Ahmed.

The company was very clever – at the time of delivery, the company took digital photographs showing the delivered goods being accepted by Arnavaz Ahmed. At this time, the transaction closed; however, after one and a half months, the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. Based on this, the company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case with the Indian Penal Code under Section 418 (Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect), Section 419 (Punishment for cheating by

personation) and Section 420 (Cheating and dishonestly inducing delivery of property). Copy of the Indian Penal Code is provided for readers' reference in Appendix P.

The matter was investigated into and Arnavaz Ahmed was arrested. Investigations revealed that Arnavaz Ahmed, while working at a call centre in Noida, gained access to the credit card number of an American national which he misused on the company's site. The CBI confiscated the color television and the cordless head phone. The CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arnavaz Ahmed under Sections 418, 419 and 420 of the Indian Penal Code – this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. On these grounds, the court released the convict on probation for 1 year.

The judgment is of utmost importance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code (the IPC) can be effectively applied to certain categories of cybercrimes which are not covered under the ITA 2000. Second, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride. According to Police, these E-Mail originated from an E-Mail Id which was similar to that of the Income Tax department. By investigating into this cyberfraud, at an initial stage, it was learnt that several such E-Mails have been sent to tax payers. The fraudulent E-Mail asks for the receiver's bank account number, customer identification number and Net banking password. There are nearly 3.5 million tax payers in the country and their E-Mail identity can be obtained easily from social networking sites, said a senior police officer.

Case Study 73: Illustration 7: Fake Mails Promising Tax Refunds – Beware

Internet banking has both advantages as well as perils. This illustration about fake E-Mails in the context of "Phishing" and how that was used by criminals. If you are a tax payer waiting for refunds at the end of the financial year, beware of fraudulent E-Mails circulating on the Internet. Delhi Police's Economic Offence Wing (EOW) investigated several cases where the complainants claimed to have received E-Mails in which they are asked to provide their bank account details so that the tax refund could be transferred to the accounts.

Such an E-Mail-based fraud came to light after the Police received a complaint from a south Delhi businessman. The plaintiff name was withheld due to the sensitive nature of the case. The E-Mail claimed that the receiver would receive ₹2,500 compensation from the Income Tax department if he provided with his bank details, including Net banking password. The person who sent the E-Mail also asked for his credit card details; this raised doubt in the mind of the plaintiff.

Additional commissioner of police (EOW) said that this cyber fraud, under investigation, is similar to attempted Phishing. Once the sender receives the details of the bank account, he can easily transfer the money from that account through Internet banking. As a safeguard, one should not respond to such E-Mails. One should report the matter to Police immediately. In this case, officials at the EOW got into tracing of the server from where these E-Mails originated. They asked the service provider to furnish details about the E-Mail account through which these mails were sent.

This was for the first time that such a cyber scam report went to Police. It is suspected that the gang has been operating since the past several months. It is common for fraudster gang to become active when the dates for tax returns approach. In this case, the police approached the income tax department to take steps to create awareness about such fraud E-Mails. However, this is not the first time that tax returns have come under the scanner. In 2005, the EOW had taken under arrest 12 individuals for

encashment of refund challans worth over ₹50 lakhs (₹50,00,000) through bogus bank accounts that were opened in collusion with bank staff.

Case Study 74: Illustration 8: Phone Scam Targets Your Bank Account

This illustration is about DoS attack. DoS attacks are not a new happening – these attacks are used by computer hackers to bring down websites by flooding them with huge amount of network traffic. The "masquerading" technique used by cybercriminals and this illustration shows how the technique was used.

What will happen if you get hundreds or thousands of calls on your home, business or cell phone? It will simply tie up the lines. How would you feel if you heard anything coming, as if from thin air, recorded messages, advertisements, or even phone sex menus when you answer? It is not annoying? Be careful, however, because, it could be more than that – it could be a sign that you are being victimized by the latest scam making the rounds. This "telephone denial-of-service attack" could possibly be the predecessor of a crime aimed at your bank accounts. In a current twist, fraudsters have converted this activity into telephones, using automated dialing programs and multiple accounts to overwhelm the phone lines of unsuspecting citizens. Why do you think, the criminals do it? It turns out that the calls are simply a diversionary tactic: while the lines are tied up, the criminals, masquerading as the victims themselves, are raiding the victims' bank accounts and online trading or other money management accounts.

Here is how "reconnaissance" and "passive" phase of attacks work – about the. Weeks or months before the phone calls start, a criminal uses social engineering tactics or malware to elicit personal information from a victim that victim's bank or financial institution would have – like account numbers and passwords. Perhaps you as a victim responded to a bogus E-Mail Phishing for information, inadvertently gave out sensitive information during a phone call, or put too much personal information on social networking sites that are trolled by criminals. Using the technology, criminals tie up your phone lines. Next, the criminal either reaches the financial institution pretending to be you or pilfers your online bank accounts using fake transactions. More often than not, the institution calls to verify the transactions, but of course, in this scenario (due to phone lines being made busy) they are unable to get through to the victim over the phone.

Even if you have not made any bank transactions, the criminals sometimes re-contact the financial institution in your name and ask the bank to do those transactions (say transfer of money or something similar). Or they substitute their own phone number to victims' accounts and just wait for the bank to call. For example, by stealing your password (keylogger ill utility). Using that malware, they will be able to get into the account and update your profile by putting their phone number. Now, the bank will end up calling them thinking it is you! They may have even learned about your other authentication information and would be able to masquerade to the bank. Thus, they will make your bank believe it is YOU who is talking to them! By the time you or the financial institution realizes what happened, it's too late.

The Federal Bureau of Investigation (FBI, US) first learned about this emerging scheme through one of its private industry partners, who revealed how a Florida dentist lost $400,000 from his retirement account after a DoS attack on his phones. There has certainly been a obvious rise in the number telephone DoS attacks, with numerous incidents reported in several of the Eastern States in America. To help fight these schemes, the FBI teamed up with the Communication Fraud Control Association – comprising of security professionals from communication providers – to analyze the patterns and trends of telephone DoS attacks, educate the public and identify the perpetrators and bring them to justice.

Remember always that ultimately, it is individual consumers and small- and medium-sized businesses (SMB) on the front line of this battle. So take safety measures: never disclose your personal information to an voluntary phone caller or via E-Mail; change online banking and automated telephone system passwords frequently; check your account balances often; and protect your computers with the latest virus protection and security software. Even if you have the slightest doubt that you are possibly under an attack through cell phone or under a DoS attack, contact your financial institution and your telephone provider, and file a complaint with the appropriate authorities in your location.

Case Study 75: Illustration 9: Cookies and Beacons – The Facebook Controversy

This illustration refers to "Facebook" a popular tool for "social networking." As a general privacy principle, whenever a website captures people's personal information details (such as name, birth date, home address, home telephone number, personal mobile number, etc.), the site is supposed to take an "Explicit Consent" known as "Opt-In" wherein the person visiting the website will check the box appearing on the consent form displayed on the website. "Opt-Out" is considered an "Implicit consent" wherein the person is assumed to be giving the permission as long as he/she does not uncheck the box. Thus, "Opt-Out" is a method in which personal information will be processed unless the data subject indicates it should be otherwise and "Opt-In" is a method in which personal information will be processed only if the data subject indicates it should be so.

Facebook, the social networking site, is supposed to track visitors to that site and is also supposed to have a customizable privacy setting option. People like both "cookies" (a bakery product) and "Beacon" (a typical breakfast item in the European countries). As much as these items are considered bad for our physical health, so are they also for the health and well being of our confidential data stored on the computers! Let us understand what "cookies" and "Beacons" mean in computer parlance.

Cookies are tiny text files that are stored on a client's device and may be later retrieved by a web server from a client's machine. Cookie files allow the web server to keep track of the end-user's web browser activities, and connect individual web requests into something like a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session, by recording that they have successfully supplied their username and password already. Since cookies are usually stored on a PC's hard disk, they are not portable. Cryptic or encrypted cookies with an unclear purpose, and which are set without the user's knowledge, alarm Internet privacy advocates. They may also violate data protection laws.

"Web Beacon" is a graphic on a webpage or in an E-Mail message that is designed to monitor who is reading the webpage or E-Mail message. Web Beacons are often invisible because they are typically only 1-by-1 pixel in size, with no color. Some information collected is the IP address of the computer that the web Beacon is sent to, the URL of the page the web Beacon comes from and the time it was viewed. Web Beacons are also known as web bugs, 1-by-1 GIFs, invisible GIFs and tracker GIFs (Graphics Interchange Format). Facebook uses Beacons heavily. Beacon was a component of Facebook's advertisement system that sent data from extraneous websites to Facebook. Apparently for the purpose of allowing targeted advertisements and allowing users to share their activities with their friends. On 6 November 2007, Beacon was launched with 40+ associate websites. The notorious service, which became the target of a class action lawsuit, and the service was shut down in September 2009.

Facebook Beacons raised some privacy concerns. On 20 November 2007, a civic action group called "MoveOn.org" created a Facebook group and online petition demanding that Facebook not publish their activity from other websites without explicit permission from the user. In fewer than 10 days, this group gained 50,000 members. Eventually, Beacon was changed to meet the requirement

that any actions transmitted to the website would have to be approved by the Facebook user before being published. In 29 November 2007, a note was published by Stefan Berteau, a security researcher for Computer Associates, was about his tests of the Beacon system. The note said that it was found that data was still being collected and sent to Facebook despite users' Opt-Outs whereby users had the choice not to log into Facebook at the time. This finding was in direct disagreement to the statements made by Chamath Palihapitiya, Facebook's vice president of marketing and operations, in an interview with The New York Times published the same day:

Question to Facebook VP Marketing & Operations:

In case I purchase tickets on Fandango, and refuse to issue the information to my friends on Facebook, does Facebook still get the information about my purchase?

Answer by the VP:

Not at all! We are still trying to dismiss a lot of wrong information being publicized without cause.

As per the blog posted by Louise Story of The New York Times on 30 November 2007, not only had she received the impression that Beacon would be an explicit Opt-In program, but that Coca Cola had also had a similar impression, and as a result, had chosen to withdraw their participation in Beacon. Facebook announced on 5 December 2007 that it would allow people to opt out of Beacon. In August 2008, a class action court case was submitted against Facebook and other corporations that activated Facebook Beacon when they released their common member's personal information to their Facebook user friends without members' consent through the Facebook Beacon program. In September 2009, Facebook proclaimed that it would terminate the service. In October 2009, a class action notice was issued to Facebook users who may have used Beacon. The proposed settlement would require Facebook to pay $9.5 million into a settlement fund. The named plaintiffs (approximately 20) would be compensated a total of $ 41,000, and the plaintiffs' lawyers would receive millions from the settlement fund. Moral of this illustration is: (a) limit your social networking activity; (b) choose the social networking sites that have got privacy guarding features; (c) it is your responsibility to protect your online privacy.

Case Study 76: Illustration 10: Privacy Loss through Leakage of Users' Facebook Profiles

This is one of the issues going on as per the story posted end of July 2010 at the link http://in.news.yahoo.com/43/20100729/860/ttc-profiles-of-100-mn-facebook-usersle.html. Nowadays, it is mentioned that "Phishing" and "ID Theft" are emerging as the biggest security and privacy threats online. It is a challenge for people in the digital era to protect their online privacy. Privacy has three dimensions: (a) informational privacy; (b) personal privacy and (c) territorial privacy. The first as well as second aspects are getting impacted in current times as this illustration shows. Read on to understand the issue that arose recently.

Hundred million users lost their personal details! They were all the heavy users of social networking website. These personal details were leaked online and are now available for download! Imagine the impact, people proudly (and at times carelessly too) post all sorts of their personal information on such social websites; be it their honeymoon photos, personal chats with no holds barred opinions expressed and what not. Will people ever take the heed and refrain from rampant use of social networking sites? It is a moot question.

An online security consultant scanned Facebook profiles using a certain software tool. When that was done, all the data of people, who had not hidden it through appropriate privacy settings, was collected. The list of such "personal" data was compiled – the list was uploaded for a free download!

Now it is just a matter of accessing the URL of every "searchable" Facebook user's profile, their name and unique ID – this is according to the latest BBC report. Imagine the implications considering the kind of personal information people carelessly leave on their Facebook accounts. According to the enterprising security consultant, he published the data only to highlight privacy issues, but Facebook retort said that the information was already public; apparently the news of personal information availability spread like a wild fire!

As per the basic tenet of "privacy," people who use Facebook are supposed to own their information and they are supposed to have the right to share only what they want, with those with whom they wish to share and when they want to share. However, it turns out that in this case, information that people have agreed to be made publicly available, was collected by a single researcher and that information (of personal nature) already existed in Google and many other search engines, as well as on Facebook. However, Facebook denied this and said that no private data was available for public consumption or had been compromised. Meanwhile, the list of personal data of so many users was already downloaded by over 1,000 people on Pirate Bay, the world's biggest file-sharing website.

According to one user (with name "lusifer69") the list is "terrific" and "scary" at the same time! As per Internet watchdog Privacy International, warnings were issued to Facebook to sensitize them that something like this was likely to happen. The expectation, therefore, was that Facebook should have anticipated the data attack and should have put in place measures to prevent it. People find it hard to believe that a firm employing hundreds of engineers could not possibly imagine a privacy leakage incident of this size. According to people, this is an instance of gross negligence on part of Facebook who have got 500 million user accounts as of June 2010.

Case Study 77: Illustration 11: Debit Card Frauds

This story appeared in March 2006 in Computerworld. Most of the major credit card associations and financial institutions refused to identify the origins of data compromises. Those data compromises have resulted in a rise of debit card fraud globally – this raised serious concerns about the scope and extent of the problem. These frauds attracted media and public attention as to what led to attempts by criminal gangs to compromise PIN-based card transactions. As we know "PIN" is considered extremely secure. According to the Director of Fraud Technology operations at Fair Isaac, a Minneapolis-based company, the series of recent breach disclosures points toward a possibly shifted focus by criminals from credit card fraud to PIN-based debit card fraud.

Banks all over the world do reissue thousands of cards as part of their operations when a card lost case is reported. The case in point is Citibank – they acknowledged that a transaction was put on hold for an unspecified number of Citi-branded MasterCard debit cards when they detected fraudulent cash withdrawals in several countries – Canada, Russia and the UK. In a brief statement released by Citibank, it was said that the fraud was the result of a "third-party business information breach" that took place in 2005. To protect its customers, they "blocked PIN-based transactions in those countries (mentioned above), for the customers affected by the breach." However, a spokesperson for the company refused to disclose the name of the third-party retailer involved in the breach.

With this disclosure, Citibank became the latest in a fast-growing list of financial institutions – they reissued thousands of debit cards or blocked access to certain transactions in countries where ATM cards were used fraudulently to withdraw cash and make purchases on US accounts.

The list comprises big banks such as Bank of America, Washington Mutual Bank and Wells Fargo Bank, along with many credit unions in the US. One of them was $13 billion North Carolina State

Employees Credit Union in Raleigh, North Carolina, which, over the past two weeks, reissued more than 27,500 debit cards after being told by Visa, USA of a security breach involving a US retailer.

According to senior vice president at the credit union (name not disclosed due to confidentiality reason) most of the compromised debit cards were fraudulently put to use in many countries – Romania, Russia, Spain and the UK. This at that time (year 2006) was the largest card reissue – ever done. This is considered to be the largest PIN theft ever. According to Gartner (the analyst firm) combined bank actions reflect the largest PIN theft to date and point to a new wave of PIN block card fraud.

We think "encryption" is hard to break; apparently this is not true as this fraud illustration shows. A PIN- based fraud scheme happened when hackers somehow managed the following to gain access to the encrypted PIN data that was sent along with card numbers to processors that execute PIN debit transactions. The thieves also had stolen terminal keys used to encrypt PINs, which are normally stored on a retailer's terminal controllers as conveyed by Gartner. The encrypted PIN information, along with the key for decrypting it and the card numbers, allow criminals to make counterfeit cards. The increase in such frauds has drawn legal attention in the US.

In February 2006, Representative Barney Frank (D-Mass.), the leading Democrat on the House Financial Services Committee, sent a letter to both MasterCard and Visa urging the companies to disclose the source or sources of the compromise or take responsibility themselves. Visa responded in an E-Mailed statement that it understood the need for quickly giving financial institutions the information needed to protect themselves and cardholders from losses in the event of a security breach. In the statement released it was stated that accusing a single source of the compromise before completion of investigation could be inaccurate and unfair. In the same way, revealing the name of the compromised entity would become a dominant disincentive for the compromised entity to share time-sensitive information with Visa going forward.

MasterCard, on the other hand, did not respond to requests for comment. Let us understand how the fraud started. According to a source, working for a company now, helping law enforcement officials investigate the fraud, most evidence suggests that point-of-sale systems at a California store of retailer OfficeMax were somehow involved in the compromise. As per the source, "All roads are pointing in that direction." However, it is still not clear precisely how the debit card and PIN information was accessed and who accessed it. According to the officials at least 200,000 cards may have been compromised.

OfficeMax did not respond to calls for comment, but a company spokesperson was quoted in various other media reports as denying any breach at the retailer. According to Gartner', OfficeMax officials' outright denial suggests that the source of the compromise may well be a third-party processor used by the company to process card transactions. Another company, whose name got mentioned in connection with the debit card fraud wave, is wholesaler Sam's Club, a division of Bentonville, Arkansas-based Wal-Mart Stores. It was acknowledged by Sam's Club, in December 2005, that it was cooperating with credit card associations in investigating reports of fraud involving approximately 600 cards used to purchase gas at its gas stations between 21 September 2005 and 05 December 2005. The company issued another statement soon in response to persistent rumors and false media reports tying it to the existing wave of PIN debit fraud.

The company denied that any of its internal systems had been compromised and said that a review of its gas payment systems by its own staff and an outside party revealed no breach. As the statement released, if any compromise did take place, it appears to have been limited to the Sam's Club fuel station point-of-sale system and did not involve PIN-based transactions.

References

- Cyber Security, Cyber Attacks and Hacking by Dr. N. C. Asthana, IPS & Priyamvada Asthana
- Information Systems Security - Security Management, Metrics, Frameworks and Best Practices by Nina Godbole
- Cyber Law and Cyber Crimes by Advocate Prashant Mali
- Fighting Computer Crime by D. B. Parker
- "Emerging Challenge : Security and Safety in Cyberspace" by Hundley R & Anderson R
- Cyber Security - Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole, Sunit Belapure
- Computer Forensics by John R Vacca
- www.deity.gov.in
- www.net-security.org
- Google & Wikipedia

Articles by Cyber Security Experts

WHY HACKERS CAN TARGET YOUR WEBSITE?

Mr. Arulselvar Thomas
Director - Technical Operations, Brisk Infosec Solutions
Research Head – National Cyber Defence Research Centre

Today website hacking does not limited to any one aspect or motive, there are different purpose for which websites are hacked now on a daily basis.

Defacement of website is generally what is considered as website hacking but it is not all, there is a lot more to it and is more than other things. Talking about website hacking we have classified the most sought reasons, which are as follows:

- Lack of Awareness
- Economic Gains
- System resources
- Revenge Hacking or Competition
- Showing off skills
- Script Kiddies

Lack of Awareness

This is one of the major cause of low security of the websites. People work on the outdated technologies and software, and also do not apply the vendor patches. They do not have any security measures installed to protect their websites against the attacks. This happens due to overconfidence or no knowledge about the security.

There are new ways and new vulnerabilities revealed every day which may or may not concern you but it may harm the website in some aspects, thus proper security and care of the website is very important. Once the user lose confidence due to website failure they will move to alternatives which will be a loss to the company. So to avoid this proper security measures are very important.

Economic Gains

As the name suggests this type of hacking is for Monitory Benefits. The attack of this kind are known as Drive by downloads and Blackhat SEO campaigns. Drive by Download means injecting some malicious code into the website and then affecting all the users of that website, by downloading the malicious files to their systems while Blackhat SEO refers to redirecting users to different websites which may have not been intent of the users. In this way, there will be a sense of dismal among the users giving a bad impression of the website and ultimately affecting the number of visits.

Example: Downloading a malware on user system and getting all credentials such as usernames and passwords of all the websites visited, including financial details.

System Resources

This is also a major cause for hacking of websites, the hackers use the resources such as bandwidth and physical server resources for their illegal purposes. The hackers compromise the website using the Bots and the Malicious Scripts which give them access to the server and they can use the resources as an administrator.

The bots can be used in different kind of distributed web attacks like Dos attacks, Brute force attacks or other automated attacks against other websites. Due to these illegal activities from your website your host may shut you down causing a lot of trouble for you and your users.

Example: Hacking to store illegal pirated software copies and pornographic contents. Also indulging in DOS attacks and DDOS

Revenge Hacking or Competition

Due to High competition in today's world for providing services, there is a greater probability of your website getting hacked for the benefit of other websites.

Also the losses suffered by others due to your good services may come as a revenge threat. There may be some group of people who would like to bring down your website to bring a bad name and a situation of distrust among the users.

Example: Company A & B are into same business, A gets Hacked so the customers of A will be going to B for services thus eliminating A as a competition.

Show Off

Several Hackers just hack the websites for fun and showing off their skills to the hacker community to get name and fame. This kind of hacking is done without any purpose it just exploits the security vulnerabilities present in your website. There are a lot of hackers of this kind who continuously look out for vulnerable websites and hack them thus affecting the website and its services for quite some time.

Example: Posting the defaced website links and screen shots on public domain with the coded name and claiming to have hacked it.

Script Kiddies

Script Kiddies are the people who do not have the working knowledge of the computer and networks, they are people who are trying to hack a website using the scripts written by other hackers without understanding the process of hacking.

Script Kiddies do these things to make themselves famous among their peers to get recognition as a hacker or to attract attention of someone. There is no other motive than this, and any website having vulnerability can be exploited by the script kiddies, which will hinder the services of the website and will upset the users.

Conclusion

As your website holds your presence online therefore it is important to secure it. Also it gives you some revenue from the advertisements if it holds any. People are less aware of the website security threats in compare to web applications which leads them to be an easy bait for the hackers to bring down their website.

People will lose their trust on

Your services if your website is hacked, therefore proper security methods are required to secure your website from the threats, which can be implemented after a security audit by a professional or security company.

Is Your WEB SITE is Safe? No, I'm not Asking about Your Web Application!

You got the question right? Well-nigh everyone chooses Web Applications over web sites, which clarifies that Web sites are unfortunately prone to security risk. Websites contains only information's whereas Web Application is a service over website i.e. performing certain tasks / interacting with the users etc. Web application security is expensive, yields more profit to security companies, and this is why Security companies concern about web applications but not websites. Websites have static content where the data displayed is the same for every visitor and content changes are infrequent. Web applications are dynamic and ever-changing, it relies on user interaction and the contents contributed to it. Everyone cared about Web application hence it contains interacted information, but they forgot websites – The Origin. Can't believe? Now, Google it yourself and check out the priority! "Web apps are the new future! Website is your past and present, which can make your future pleasant / unpleasant!! Better treat it right way". Comparing the both, websites are more in number so as its security issues. Most of the Web Application source codes are kept confidential for security purpose on contrary web site source codes are often openly available. This is one main reason, why websites are easily compromised.

Website compromising-Intentions behind!

- Heist of personal or sensitive data.
- Devastating the reputation.
- Altering website content.

- Intercepting confidential data.
- Making Services unavailable by performing DoS attacks.

Website -Security Glitch!

- Websites contain both general and confidential information's such as employee details, contact information and goes on.
- Reputation of the organization/Institution is devastated.
- Website compromising often leads to major attack.(Preparation Phase)
- Initial phase of any attack is information gathering, which is started from the corresponding websites.
- Phishing attacks are done often by using contact details.

Security Measures

- Using cross-platform compatible encryption: Choose Encryption method which supports all platform and doesn't unnecessarily limit user base.
- Managing Website via encrypted connections: Using unencrypted connections such as unencrypted FTP or HTTP, prevents man-in-the-middle and login/password sniffing attack.
- Data validation: Any input given by user must be validated; by this attacks like SQL injections are avoided.
- Encrypted Login pages: If Authentication is to check the validity whereas Encryption is to maintain the validity.

Conclusion:

Remember the proverb? "Elephants are not afraid of mice, but terrified by Ants", Got it now? How reputed your organizations is, a small attack on your website destroy everything! Almost Everything. Top companies concerned only about web applications (Mice) not the websites (Ants), because mice are what the profit yielders while websites is their assets. Websites are a huge part of the web and plays vital role in offering many information's. More the information, more it gets compromised soon. Discovering the vulnerabilities / threats is one difficult task .People who are preferred them as Hackers, without much knowledge are often try their skills here only, thus unknown threat like these are more vulnerable compared to identified threats. Thus Security for websites is more significant.

MOBILE PRIVACY

Mr. Sathish Ashwin
Information Security Analyst - Deep Identity
Research Head – National Cyber Defence Research Centre.

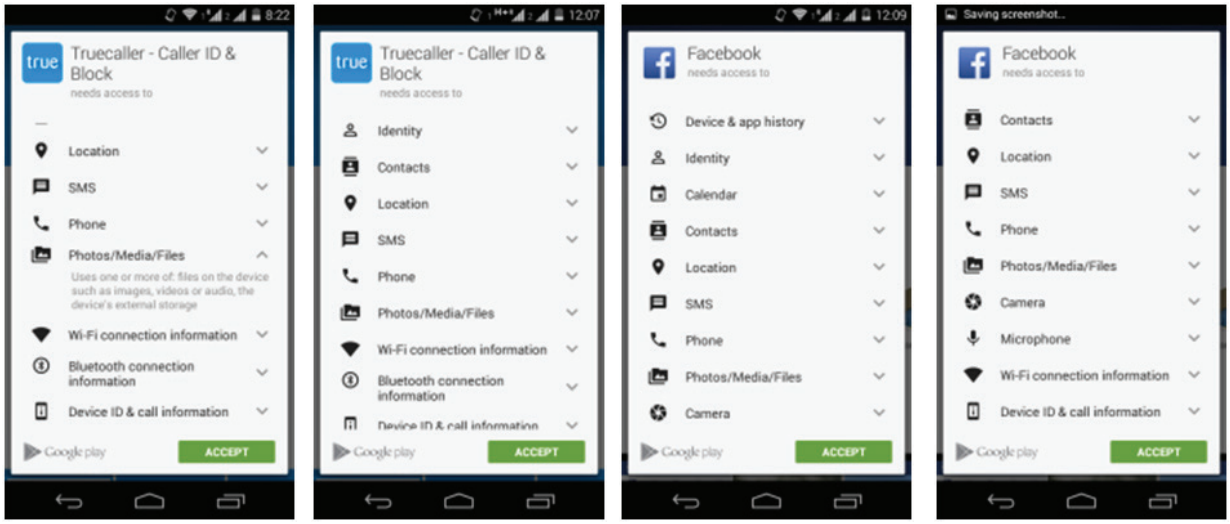
Do you really care about your mobile privacy?

The Internet has made life a lot easier by making information more accessible to all and creating connections with different people around the world. However, it has also led a lot of people to spend too much time in front of the computer, so much so that it becomes the center of their lives. Today we are into the smart world where we are spending too much of time in the smart cyber world.

Ever since whistle-blowing NSA contractor Edward Snowden revealed the elephantine extent of the NSA Surveillance State's domestic and foreign spying, everyone is much concerned about their individual privacy.

Do you know that the mobile applications you have installed are already steeling your information's without your knowledge? Recently, we even had a news that Google Map was tracking our every move.

Here are the few examples of what the mobile applications are really upto. Take a look at the images below,



In the above images you all can see that the applications requesting permissions for Phone, Contacts, SMS, Media Camera etc., Did you really know what the actually permissions that you are giving to this applications ?

In the above Truecaller App screenshot you can see its requesting permission for accessing Photos/ Media/Files "Use one or more of. files on the device such as images, videos or audio, the devices external storage".

The Original Permission behind the App.

Here you can see the original permissions behind the app. I wonder why this app need a Video & Audio recording permission?

They were able to do this because of the extensive list of permissions they requested (you know that little box that pops up when you first install an app that nobody reads). Truecaller apps are fairly that lets you to search for contact information (based on name or number), identify incoming calls, block calls you don't want to receive, and make personal contact suggestions based on time and place – so you never have to leave the service to find the right contact, so there's no legitimate reason for this app to request permission to record audio or video etc., which doesn't require a heap of permissions and is proven to be trustworthy. I'm not just blaming true caller there are lot of applications dose this.

If You Really Care About Your Privacy, Here is the Best Way to Handle this Applications:-

XPrivacy is an app that can prevent applications from leaking privacy sensitive data. XPrivacy can restrict the categories of data an application can access. This is done by feeding an application with no or fake data. There are several data categories which can be restricted, for example contacts or location. For example, if you restrict access to contacts for an application, this will result in sending an empty contact list to the application. Similarly, restricting an application's access to your location will result in a fake location being sent to the application.

To install this application you would need a rooted android mobile or tab click here for installation help.

Even if your privacy isn't important to you, there are others for whom privacy is paramount. "Even if you're comfortable giving up your personal information," Rainey said, "there are plenty of people who aren't, and they shouldn't have to fight to keep their addresses out of publicly accessible databases or off of a website where it's easily obtained. To that point, it's worth remembering that on many social networks, we give up information about those we're connected to when we let another app or service in—even if we've consciously decided we're okay trading the information requested about ourselves.

So what do you do now? We've shown you how to protect yourself and even how to watch companies track you in real time. In the end, the important thing to remember before you click through another privacy policy is to be actively aware of the decision you're making.

"Just because something claims it's free doesn't mean it is."

CRYPTOLOCKER

Mr. Sathish K (Satz)
Security Researcher, Malware, Analyst / Founder ISAHACKERS
Chair Member - National Cyber Defence Research Centre.

Introduction

CryptoLocker is a ransomware trojan which targeted computers running Microsoft Windows and was first observed & posted to the internet by Dell SecureWorks on 5th September 2013.Some ransomware just freezes your computer and asks you to pay a fee. (These threats can usually be unlocked without paying up, using a decent antivirus program as a recovery tool.) CryptoLocker is different: your computer and software keep on working, but your personal files, such as documents, spreadsheets and images, are encrypted.

The malware then displays a message which offers to decrypt the data if a payment is made by a stated deadline (e.g. 72 hours, or three days), and threatened to delete the private key if the deadline passes. If the deadline is not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in bitcoin.

The criminals retain the only copy of the decryption key on their server – it is not saved on your computer, so you cannot unlock your files without their assistance.

The decryption key is unique to your computer, so you can't just take someone else's key to unscramble your files.

The fee is $300 or EUR300, paid by MoneyPak; or BTC2 (two Bitcoins, currently about $280).

Although CryptoLocker itself is readily removed, files remained encrypted in a way which researchers considered infeasible to break. Many said that the ransom should not be paid, but did not offer any way to recover files; others said that paying the ransom was the only way to recover files that had not been backed up. Some victims claimed that paying the ransom did not always lead to the files being decrypted.

CryptoLocker was isolated in late-May 2014 via Operation Tovar—which took down the Gameover ZeuS botnet that had been used to distribute the malware. During the operation, a security firm involved in the process obtained the database of private keys used by CryptoLocker, which was in turn used to build an online tool for recovering the keys and files without paying the ransom. It is believed that the operators of CryptoLocker successfully extorted a total of around $3 million from victims of the trojan. Other instances of encryption-based ransomware that have followed have used the "CryptoLocker" name (or variations), but are otherwise unrelated.

Operation

CryptoLocker attack goes through five stages from the time it installs on your computer to the appearance of the ransom warning on your screen.

Malware Installation

CryptoLocker uses social engineering techniques to trick the user into running it. More specifically, the victim receives an email with a password-protected ZIP file purporting to be from a logistics company.

The Trojan gets run when the user opens the attached ZIP file, by entering the password included in the message, and attempts to open the PDF it contains. CryptoLocker takes advantage of Windows' default behaviour of hiding the extension from file names to disguise the real .EXE extension of the malicious file.

As soon as the victim runs it, the Trojan goes memory resident on the computer and takes the following actions:

- Saves itself to a folder in the user's profile (AppData, LocalAppData).
- Adds a key to the registry to make sure it runs every time the computer starts up.
- Spawns two processes of itself: One is the main process, whereas the other aims to protect the main process against termination.

File Encryption

The Trojan generates a random symmetric key for each file it encrypts, and encrypts the file's content with the AES algorithm, using that key. Then, it encrypts the random key using an asymmetric publicprivate key encryption algorithm (RSA) and keys of over 1024 bits, and adds it to the encrypted file. This way, the Trojan makes sure that only the owner of the private RSA key can obtain the random key used to encrypt the file. Also, as the computer files are overwritten, it is impossible to retrieve them using forensic methods.

CryptoLocker installs itself into your Documents and Settings folder, using a randomly-generated name, and adds itself to the list of programs in your registry that Windows loads automatically every time you logon.

It tries to make a web connection to each of these server names in turn, trying one each second until it finds one that responds. Once it has found a server that it can reach, it uploads a small file that you can think of as your "CryptoLocker ID."

Then a public-private key pair is generated from its C&C Server unique to your ID, and sends the public key part back to your computer.To find an active C&C server, The Trojan incorporates a domain generation algorithm (DGA) known as 'Mersenne twister' to generate random domain names. This algorithm uses the current date as seed and can generate up to 1,000 different fixed-size domains every day.

The malware on your computer uses this public key to encrypt all the files it can find that match a largish list of extensions, covering file types such as images, documents and spreadsheets.

When the Trojan finishes encrypting every file that meets the aforementioned conditions, it displays the following message asking the user to make a ransom payment, with a time limit to

send the payment before the private key kept by the malware writer is destroyed.

Curiously enough, the malware doesn't ask users for the same amount of money, but incorporates its own currency conversion table.

What Should I do if I get Infected?

If you are infected with CryptoLocker, the first thing you should do is disconnect the infected PC from the internet. If CryptoLocker can't access its C&C, it can't encrypt files. Disconnecting the machine may prevent further files from being encrypted.

There are many tools that will totally clean a CryptoLocker infection, but most victims are more concerned with recovering encrypted files. Unfortunately, you will not be able to crack CryptoLocker's encryption. It uses a very strong and reliable public/private key implementation that is similar to what commercial encryption products use. It would take decades to centuries to crack today. There is a chance that the we may eventually track down the attacker's C&C servers, and recover some private keys. However, I would not hold out much hope for this.

Rather, if CryptoLocker encrypts some of your files, you should check if you have a backup, as that is your best chance of recovering the lost data. That said, some victims have reported some success with using Windows' built-on System restore features to recover some lost files, too.

Many have asked whether or not CryptoLocker's decryption process works if you pay the ransom. Personally, I highly discourage you from ever paying extortion to cyber criminals. Not only are you paying off criminals, but you are encouraging them to continue to use these methods in the future. That said, reports claim that CryptoLocker's decryption does work. However, in order for the process to work, an infected computer must retain access to the C&C server. If the server is taken down by authorities, sink-holed, or temporarily goes offline, paying the ransom may only result in the loss of your money.

Ransomware Rescue Kit

There are Free CryptoLocker Ransomware Decryption Tool Released online. You only need a master decryption key in order to decrypt the locked files. Go to https://www.decryptcryptolocker.com Upload an email address and one of the encrypted files (one that should have no sensitive information). The online tool will scan the file to figure out the encryption specifics, and then send you a recovery program and master decryption key via an email. You can take that key and the free decryptolocker.exe command line tool and decrypt your files.

Tool may warn you that some data might not be recoverable, particularly if you've been infected by a CryptoLocker variant rather than CryptoLocker itself. You need to keep this in mind that there are many CryptoLocker variants with the names like PrisonLocker, CryptoDefense, TorLocker and CryptorBit, so the tool may not work against them.

Mitigation & Prevention

Here are some tips on how to keep your computer from getting infected with ransomware. You don't have to do all of these, but the more you do, the better off you are.

Keep regular backups of your important files. If you can, store your backups offline, for example in a safe-deposit box, where they can't be affected in the event of an attack on your active files. Your backups will be rendered useless if they are scrambled by CryptoLocker along with the primary copies of the files.

Use an anti-virus, and keep it up to date. As far as we can see, many of the current victims of CryptoLocker were already infected with malware that they could have removed some time ago, thus preventing not only the CryptoLocker attack, but also any of the damage done by that earlier malware.

Keep your operating system and software up to date with patches. This lessens the chance of malware sneaking onto your computer unnoticed through security holes. The CryptoLocker authors didn't need to use fancy intrusion techniques in their malware because they used other malware, that had already broken in, to open the door for them.

Review the access control settings on any network shares you have, whether at home or at work. Don't grant yourself or anyone else write access to files that you only need to read. Don't grant yourself any access at all to files that you don't need to see – that stops malware seeing and stealing them, too.

Don't give administrative privileges to your user accounts. Privileged accounts can "reach out" much further and more destructively both on your own hard disk and across the network. Malware that runs as administrator can do much more damage, and be much harder to get rid of, than malware running as a regular user.

Know how your applications are updated. Some applications will pop up notifications on your screen, others will notify you via email and still others will only tell you about updates when you use them. If you get a notice you don't expect, contact the company and ask.

If you receive a suspicious email (phishing?), but are not sure, contact the company by going to their website or contact them via phone. Don't click on any links or use the phone numbers in the email.

Try not to click on ads for products or companies you don't know. Even better, if you see an appealing ad, go directly to the company's website and see if the offer is there.

Download from reputable sources. Only download and install browser add-ons, plugins, and extensions that come from known source.

Take a snapshot of your entire system from time to time, perhaps once a month. This will include data and applications. Store these snapshots on an external drive that is only connected to your computer to do the backup and then is disconnected.

Have a backup of all the files on your computer to a server that is NOT on your network. Online Cloud backup systems are good for this purpose as they utilize their own application to manage the transfer and storage of your data files.

Disabling hidden file extensions in Windows will also help recognize this type of attack.

If you become infected and don't have a backup copy of your files, our recommendation is not to pay the ransom. That's NEVER a good solution, as it turns the malware into a highly profitable business model and will contribute to the flourishing of this type of attack.

Make sure you have reformatted your hard drive to completely remove the CryptoLocker trojan before you attempt to re-install Windows and/or restore your files from a backup.

Finally, awareness is the best defence. As a computer user, your job is to stay aware of what's happening on your computer. You don't have to be a computer security expert, but you should practice safe clicking. Even the safest computer users can get infected with malware, but by staying alert and aware you can dramatically reduce your chances.

There are many free tools now available in the community, that can help users to protect their systems from this malware.

1. CryptoPrevent tool, created by American security expert Nick Shaw. This tool applies a number of settings to your installation of Windows that prevents CryptoLocker from ever executing and has been proven to work in Windows XP and Windows 7 environments.
2. HitmanPro.Alert 2.5, a free utility that will help you to protect your computer against the CryptoLocker ransomware malware. HitmanPro.Alert 2.5 contains a new feature, called CryptoGuard that monitors your file system for suspicious operations. When suspicious behaviour is detected, the malicious code is neutralized and your files remain safe from harm.
3. BitDefender Anti-CryptoBlocker, an encryption-blocking tool that can detect and block malware from installation.

Intrusion prevention systems can block the communications protocol send from the CryptoLocker infected system to the remote command-and-control server where the malware retrieves the key to encrypt the files. Blocking the communications can prevent the encryption from taking place.

Money Paid

In December 2013 ZDNet traced four bitcoin addresses posted by users who had been infected by CryptoLocker, in an attempt to gauge the operators' takings. The four addresses showed movement of 41,928 BTC between 15 October and 18 December, about US$27 million at that time.

In a survey by researchers at the University of Kent, 41% of those who claimed to be victims said that they had decided to pay the ransom, a proportion much larger than expected; Symantec had estimated that 3% of victims had paid and Dell SecureWorks had estimated that 0.4% of victims had paid.[21] Following the shutdown of the botnet that had been used to distribute CryptoLocker, it was calculated that about 1.3% of those infected had paid the ransom; many had been able to recover files which had been backed up, and others are believed to have lost huge amounts of data. Nonetheless, the operators were believed to have extorted a total of around $3 million.

The Future of Ransomware

The success of CryptoLocker spawned a number of unrelated and similarly named ransomware trojans working in essentially the same way, including some that refer to themselves as

"CryptoLocker"—but are, according to security researchers, unrelated to the original CryptoLocker.

In September 2014 further clones such as CryptoWall and TorrentLocker (whose payload identifies itself as "CryptoLocker", but is named for its use of a registry key named "Bit Torrent Application"), began spreading in Australia; the ransomware uses infected e-mails, purportedly sent by government departments (e.g. Australia Post to indicate a failed parcel delivery) as a payload. To evade detection by automatic e-mail scanners that can follow links, this variant was designed to require users to visit a web page and enter a CAPTCHA code before the payload is actually downloaded. Symantec determined that these new variants, which it identified as "CryptoLocker.F", were not tied to the original.

During the first half of the year 2015, the number of incidents of ransomware has steadily increased. In early June, the security researchers at McAfee discovered "Tox" which provides neophyte cybercriminals (aka script kiddies) with everything they need to run a ransomware campaign. We've seen this "malware-as-a-service" model before as spam, phishing, spyware, and virus packages are available for sale on the black market. The malware developers do this not only to monetize their work, but also to reduce their risk of being caught. With script kiddies getting involved, you can expect a continued increase in the number of ransomware attacks for the next several months as the hacker community tries to wring as much cash out of ransomware as possible.

As long as ransomware continues to generate cash for its purveyors, you can expect even more virulent strains of CryptoLocker and its variants to rear their ugly heads. Your goal is to make ransomware unprofitable by never having to pay the ransom. You can accomplish this by having a good off-site backup of your files, keeping your applications and operating system up-to-date, and remaining vigilant as you use your computer.

CYBER THREATS: A CHALLENGE OF TODAY & OF THE FUTURE & WHAT CAN BE DONE TO LEAP FROG AHEAD OF THE HACKERS COMMUNITY

Mr. Rakesh Kumar Raju

Sr. Technical Trainer (India, SAARC, APAC, ANZ)

National Technical Committee Member - National Cyber Defence Research Centre.

Cyber Threats - Cyberspace lies at the heart of modern society; it impacts our personal lives, our businesses and our essential services. Cyber security embraces both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or industrial espionage. E-crime, or Cyber-Crime, whether relating to theft, hacking or denial of service to vital systems, has become a fact of life. The risk of industrial cyber espionage, in which one person/s Or company makes active attacks on another, through cyberspace, to acquire high value information is also very real.

Where & How it started

How old are viruses? In 1949, John Von Neumann gave lectures at the University of Illinois about what he called "self-replicating automata." On ARPANET, the precursor to the Internet, the first virus, named Creeper, was detected in 1971.

Since then, malicious software has evolved into many types. Technically, although we often refer to all malware as viruses, not every piece of unwanted software behaves like a virus – malware is not always self-replicating, and sometimes users willingly install it. To include viruses, worms, Trojans, spyware and all others, we now use the term "malware."

Malware can be divided into 2 major types:

Viruses, which infect the computer and spread on their own (generally via an exploit), such as Flash ad banners whose binaries contain buffer overflow code. Gray ware which requires some kind of user interaction but convinces them that the benefit outweighs the cost, such as browser toolbars that also track the user's activity and insert its own ads into web pages.

Within the category of viruses, there are 2 important subtypes:

Trojans such as Zeus, like the literary Trojan horse, trick users into letting down their defenses and installing them, and then often use the network to spread via email or instant message.

Worms, such as Conficker and Code Red, spread by connecting to open ports on the network and exploiting misconfigurations or other vulnerabilities in those daemons.

A Trojan can infect the same host multiple times, but that happens when another copy arrives from an external source. The local copy of the software does not try to re-infect the computer.

Are all viruses malicious? By definition, Yes. But some white hat hackers and academics have written beneficial worm-like software. It spreads via the same exploits, but then cleans infections

and/or patches the host. For example, Creeper was followed by Reaper, which removed Creeper from infected systems.

Regardless of how the virus spreads, once installed, a virus is somehow malicious.

What makes it malicious? It's behavior. (This is one of the reasons, by the way, that security analysts use Sandboxing technologies to discover new viruses. They work based on Looking at which C functions a virus contains, for example, cannot find all viruses. Forensics lab must see which functions actually execute, and what the effects are.

Most people are familiar with spyware, adware, and rootkits. But Malware could also be:

Ransomware such as the Crypto Locker worm which is fairly new. The software holds the computer hostage, often encrypting critical user data with a password or secret key, until the victim pays the extortionist. Some of the cases which has come to the fore recently is that, even after paying up the Ransomware extortionist, there can be some traces which still remain as infections on the machines.

Key loggers record key strokes and return them to a remote location – including sending administrator logins and personal email addresses for executives. Mass Mailers can transform computers into open relay mail servers for the botnet, often managed via a remote command and control server (C&C Servers), sending spam for hire. These are often operated by organized crime syndicates.

Just as viruses have evolved many vectors for spreading, they also have evolved and use multitude of different techniques for evading antivirus engines and manual analysis. This is what is a cause of concern today and may be in the future as well ….

Match flexibly, or ignore the changeable parts of the code, and match only based on the polymorphic or metamorphic engine.

Virus Code writers have found and identified different methods to write the Virus codes and hence the complexity has increased manifold. Let's take a quick look at different techniques to detect these kind of New gen Viruses / malware which go undetected by most of the AV Software's (Gateway AV Systems as well as Host based AV Systems)

Metamorphic / Polymorphic Malware Fundamental Principles

Malware must be defined semantically as the very same Virus, Worm, Bot, Key Logger etc. is likely to exist in different physical forms The techniques of polymorphism and metamorphism change the form of each instance of software in order to evade "pattern matching" detection during the detection and investigative process

Metamorphic Viruses / Malware:

Metamorphic Malware: "automatically recodes itself each time it propagates or is distributed"

Simple techniques include:

- Adding varying lengths of NOP instructions
- Permuting use registers
- Adding useless instructions and loops within the code segments

Metamorphic Malware Advanced techniques include:

- Function reordering
- Program flow modification
- Static data structure modification
- Reordering structures
- Inserting unused data types

Morphing Engine Components

- Disassembler
- Permutor
- Randomizing Inserter (code & data)
- Code Compressor
- Assemble

Threat

- Polymorphic and Metamorphic malware are evolving
- Discovery in real-time or post-mortem / Forensics is difficult
- Limited resources being applied

Polymorphic Viruses / Malware :

Polymorphism loosely means: "change the appearance of"

- If a virus is programmed to look different each time it is replicated, there would be no fixed string for anti-virus to latch onto detect it. Such a virus is known as polymorphic virus.
- Polymorphic viruses have specially designed Mutation Engines.
- They (M.E.) generate a new decryption routine each time, by switching the order of instructions.
- Mutation Engines are bundled with the virus, worm or other self-propagating code Common methods include Encryption Data appending / Data pre-pending
- The decrypted code is essentially the same in each case, thus memory based signature detection is possible Block hashing can be effective in identifying memory based remnants.

Impact on Law Enforcement:

- Incident response is slow
- Determining the source of attacks is difficult
- Prosecuting those involved is elusive

Preventing Zero Day Threats, Attacks / Vulnerabilities involve techniques like ATP (Advanced Threat Protection) or Technologies involving Sandboxing, today many Security vendors such as

Fire eye, Fortinet, Cisco, Checkpoint, MacAfee etc provide these as part of their Product offerings.

Cyber Threat Source Descriptions

Cyber threats to a control system refer to persons who attempts unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned below.

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- GAO Threat Table

National Governments (Depends on Countries & Their capabilities)

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm a Country's interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to Critical Infrastructures (Power Stations & Nuclear Stations, Airports , Railways, Digital Cities / Cyber Cities, Water Resources / Dams etc) which will be controlled via the cyber space / electronically operated over the next few years.

The tradecraft needed -is to effectively employ technology, tools & Resources which remain an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the Country's Cyberspace. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the Country's economy, full scale attack of the infrastructure to damage the ability of the Country during Times or War Or Peace.

Terrorists

Traditional terrorist adversaries of INDIA Or any other country , despite their intentions to

damage the interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We can anticipate more substantial cyber threats that are possible in the future as a more technically competent generation enters the ranks.

Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the country through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent.

Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.

Hacktivists (Groups)

Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-INDIA motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.

Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, such hackers pose a threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical networks and even fewer would have a motive to do so. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack. In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

For the purposes of this discussion, hackers can be subdivided as follows:

- Sub-communities of hackers
- Script kiddies are unskilled attackers who do NOT have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.

- Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit.
- Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.

Nature of the Computer Security Community

Hackers and researchers interact with each other to discuss common interests, regardless of color of the hat. Hackers and researchers specialize in one or two areas of expertise and depend on the exchange of ideas and tools to boost their capabilities in other areas. Information regardingcomputer security research flows slowly from the inner circle of the best researchers and hackers tothe general IT security world, in a ripple-like pattern.

GAO Threat Table (Sourced from the Internet)

The following table is an excerpt from NIST 800-82, "Guide to Supervisory Control and DataAcquisition (SCADA) and Industrial Control System Security (SME draft), provides a description of various threats to CS networks:

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power -impacts that could affect the daily lives of citizens across the country.

Threat	Description
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware / malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Having discussed Cyber Threat Scape till now, Lets now go ahead and discuss what needs to be done to STOP the cyber threats / at least prevent them to an extent.

Some Mantras to Save Your Digital Life from Getting Hacked…..

- Create strong passwords and change them frequently

There are a number of security experts that state that you should never use the same password for all of your accounts. Doing this is just asking for all your personal information to be stolen.

Make sure you've got a super strong, unique password. In other words, ensure that your password is difficult to guess. One way to come up with a creative password is to brainstorm a random sentence. Take the first letter of each word in that sentence and use that acronym as the base for your password. Try to create diverse passwords that combine numbers, symbols and other factors to ensure it is safe and secure. You should also ensure that passwords are changed every few months. This is true for you, as well as your employees.

Don't use the same password for multiple services. Using the same term for all of your passwords leaves your entire digital life vulnerable to attack. This means that if a hacker has one password, he or she has all of your passwords.

Some of the researchers are experimenting using Sanskrit language mantras as Passwords to make it more secure and less easier to crack, it is learnt to be one of the most secure ways to prevent a Password Guessing Or password crack / Dictionary attacks.

- Enable two-factor authentication. Many services, including Google, offer two-factor authentication for logging into your account. Instead of simply entering a username and password to log in, the website will prompt you to enter a code sent to your smartphone to verify your identity.
- Apply software updates when necessary. Apple, Google, and Microsoft and other Software developers typically include security bug fixes and patches in their most recent software updates. So don't ignore those annoying prompts and keep your software up-to-date.
- Do not give out personal information over the phone or in an email -unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate!
- Carefully read the permissions before installing apps -This is one of the most prominent ways in which malicious apps can gain access to your personal information. These types of issues have been especially present in the Google Play store. A lot of apps ask for a lengthy list of permissions, and that doesn't mean they're all ill-intentioned. But it's important to be aware of the types of information your apps are accessing, which can include your contacts, location, and even your phone's camera.
- Check the app publisher before installing -There have been numerous instances in which scammers have published apps in the Google Play store posing as another popular app. For example, in late 2012 an illegitimate developer posted an imposter app in Google Play pretending to be "Temple Run." A quick look at the publisher shows that the app comes from a developer named "apkdeveloper," not the game's true publisher Imangi Studios.
- Avoid inserting hard drives and thumb drives you don't trust into your computer -If you find a random USB stick, don't let your curiosity tempt you to plug it in. Someone could

have loaded malware onto it hoping that an interested person was careless enough to insert it into their device. If you don't trust the source, you're better off not putting your computer at risk.

- Make sure a website is secure before you enter personal information -Look for the little padlock symbol in front of the web address in the URL bar. Also, make sure the web address starts with the prefix https://. If these things aren't there, then the network isn't secure and you shouldn't enter any data you wouldn't want made public.
- Stop Or Prevent sending Sensitive / Confidential / Personal data via email. -Sending critical information such as credit card numbers or bank account numbers puts it at risk of being intercepted by hackers or cyber attacks. Using Technologies like DLP (Data leak prevention) can prevent the most sensitive Data to be sent out / screened by the Gateway
- Firewall's / Host computers to stop someone trying to leak confidential information from the system or even the network.
- Keep an eye out for phishing scams. -A phishing scam is an email or website that's designed to steal from you. Often times, a hacker will use this email or website to install malicious software onto your computer. These web entities are designed to look like a normal email or website, which is how hackers convince their victims to hand over personal information. Phishing scams are typically easy to spot, but you should know what to look out for. Many of these emails contain spell errors and are written in poor grammar or illegitimate info.
- Avoid logging into your important accounts on public computers. -Sometimes you've got no choice but to use a computer at the coffee shop, Public library, or Airport Or some Free Wifi hotspots. But try not to do it frequently, and make sure you completely wipe the browser's history when you're finished. And also make sure you do not save / store passwords / Cookies while browsing from public spaces.
- Back up your personal files to avoid losing them -You should keep a copy of all important files in the cloud and on some sort of hard drive. If one of them gets hacked or damaged, you'll still have a backup copy.

Create an internal policy

Do you know what the biggest cyber security risk is for your business? There are a number of business owners who are surprised to learn that it is their employees. In many cases, criminals will get inside a network thanks to one of your employees clicking on a line in an email or using a poor password Or downloading some unknown Application, Clicking on some interesting Online Advertisement etc. It is important to stay updated on the latest scams that are going around and to keep your employees aware of the scams, as well.

While staying educated is the first element, you also need to check with the person who set up the business server to ensure the right protections are in place.

Keep your computers updated

One of the simplest strategies, you can use immediately, is ensuring that your entire network is up to date. This means paying attention all notifications regarding updates to your operating systems, antivirus software, web browsers and firewalls. Ignoring any of these essentially leaves cracks in your defence system.

Know what not to do

Adding firewalls and filters to a platform that is already insecure is basically the same as attaching a padlock to a screen door. Eventually, cyber criminals will locate the vulnerability. You need to discover where the major problems are, and then have a professional fix the issues. This is the only way that you can ensure that your system is going to remain safe.

Increase employee awareness

This is one of the most cost-effective methods of preventing a cyber attack. Today, less than 40 % percent of companies train employees on cybersecurity. It is critical to understand that cyber attacks can occur just by a cyber criminal having access to an employee laptop. This is why it's imperative for your company to implement privacy training.

Network based mitigation

- Install IDS/IPS with the ability to track floods (such as SYN, ICMP, UDP Floods etc.)
- Install a firewall that has the ability to drop packets rather than have them reach the internal server. The nature of a web server is such that you will allow HTTP to the server from the Internet. You will need to monitor your server to know where to block traffic.
- Install UTM Firewalls with ATP & Sandboxing capabilities to prevent different threats & Zero day attacks.
- Have contact numbers for your ISP's emergency management team (or response team, or the team that is able to respond to DOS / DDOS attacks). You will need to contact them in order to prevent the attack from reaching your network's perimeter in the first place.

Host based mitigation

- Ensure that HTTP open sessions time out at a reasonable time. When under attack, you will
- want to reduce this number.
- Ensure that TCP & UDP Sessions also time out at a reasonable time.
- Install a host-based firewall to prevent HTTP threads from spawning for attack packets.

SOLID STATE DEVICE (SSD) FORENSICS: A NIGHTMARE FOR CYBER FORENSICS INVESTIGATORS

Mr. Santosh Khadsare

Infosec Professional, Cyber Forensics Expert, Information Warfare and Cyber Law Enthusiast & Chair Member - National Cyber Defence Research Centre

Background

If there is anyone has challenged the Locard's principle of exchange from digital forensics point of view, it is the Solid State Devices (SSDs).Gone are the days when a cyber forensic investigator could claim that if something was ever present in the digital evidence he will reproduce it. Erasing of one's tracks in the digital world has become much easier as the perpetrator needs no technical acumen but just some common sense to replace the existing storage media of this weapon (laptop/mobile phone /computing device) with SSDs. When the D-day arrives the perpetrator has to press the trigger of this weapon by issuing 'delete' command. That's all

One of the best definition of digital forensics was given at Digital Forensics research Conference (DFRWS) in 2001.It stated "Digital Forensics is use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".

To begin with solid-state refers to electronic components, devices, and systems based on the semiconductor in which the electrons or other carriers of charge are confined entirely within the solid material. In a solid-state component, the current is confined to solid elements and compounds meant specifically to switch and amplify it. Shifting the focus to the storage drives in the various state of art gadgets in which the SSDs are gaining foothold at a very fast pace. The Hard Disk Drives (HDD) are being replaced by the new entrant in all the computing devices to mention a few are laptops, desktops, mobile phones, etc. The other storage medium such as flash drives and secondary storage media have also shifted to this new technology. Some advantages of having a SSD in place of a HDD is no moving parts, less access time, reliability and energy savings.

SSDs have introduced dramatic changes to the principles of digital forensics. Identification of SSD as digital evidence is also turning out to be a challenge to begin with.

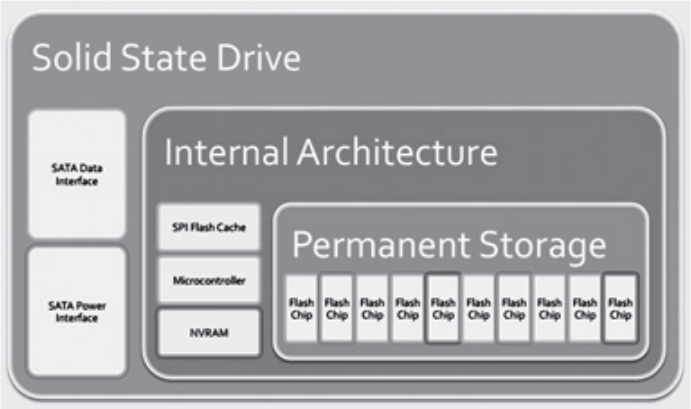
- **M.2 Evolution of Sleek and Lighter SATA SSDs.** First Generation SSD drives were available as 2.5" disks which was a limitation when making ultra-portable devices. The solution to

this problem was M.2 form factor. Devices conforming to the M.2 form factor can use Serial Advanced Technology Attachment (SATA), Peripheral Component Interconnect - Express (PCI-E) or USB3.0 connectivity. M.2 devices require a standard PCI-E connector. While most M.2 SSD drives conform to the AHCI specification, supporting all the features of their full-size counterparts and being recognized by the OS as a standard SATA SSD, some models conform to the newer Non Volatile Memory Express (NVMe) specification that requires a different driver stack.M.2 SSD drive can be Legacy SATA, PCI-E using Advance Host Controller Interface (AHCI) or PCI-E using NVMe.

- **PCI Express (PCI-E) SSDs.** PCI-E, or PCI Express, is a physical connectivity standard. PCI-E SSD drives are available in a wide range of form factors including full-size desktop expansion boards, M.2, proprietary and soldered portable storage solutions. PCI-E SSDs can use AHCI or NVMe for interfacing. On a logical level, PCI-E SSD drives can work via the AHCI or NVMe interface. In general, the following compatibility matrix applies to PCI-E SSDs (SSD and eMMC Forensics 2016 - Part 1 by Yuri Gubanov, Oleg Afonin (Belkasoft Research)):
    - **Mac OS X:** Trim command is supported on all Apple devices with factory installed PCI-E SSD drives.
    - **Macbook with Windows:** Proprietary PCI-E SSD drives are used Apple Macbooks. Windows is installed as double-boot or independent Operating System. In these configurations, trim pass-through is supported where applicable.
    - **Windows:** Trim support for PCI-E drives depends on Windows version and the presence of the correct driver. In Win 7 trim not supported on PCI-E drives regardless of the drivers, even if the PCI-E SSD would accept the command. Win 8, 8.1 and Win 10: trim is supported with native Microsoft drivers. Trimming in NVMe-based PCI-E SSDs is also supported.
- **NVM Express (NVMe) SSDs.** NVMe is a modern logical interface specification that replaces the old AHCI. NVMe is employed in certain high-end PCI-E SSD models in various form factors. Apple MacBook 2015 uses NVMe interface on a proprietary SSD drive soldered to the motherboard. NVMe is still fairly new, with some motherboards failing to recognize NVMe storage as bootable devices. Similar to SATA SSD drives that exist as 2.5" drives and as slim M.2 boards, NVM Express devices are also available as full-size PCI Express expansion cards, laptop-size boards and 2.5" drives that look similar to SATA SSD drives, only utilizing a PCI Express interface through the U.2 connector instead of a SATA port.

Exploring SSDs

Picture speaks better than words. NOR flash and NAND flash are the components of SSD. SSDs have limited erase-write cycles and the read accuracy decreases after a certain number of reads.



NAND Cells
SLC Cell – 1 bit storage
MLC Cell – 2 bits storage
TLC Cell – 3 bits storage

Fig. SSD Architecture

- **'TRIM' Scare.** There is a lot of talk that deleted artifacts cannot be reconstructed from TRIM-enabled SSD drives, due to garbage collection (GC) operation in the background even after the device is switched off. Exceptions are always there. TRIM does not affect most environments in RAID configuration, NAS configuration, older Windows (also does not work on file systems other than NTFS) or on external SSD drives attached as a USB enclosure or connected via a FireWire port.
- **Self Corrosion.** Even switching off the affected device immediately after TRIM has been issued, does not stop the destruction. Once the power is back, wiping will continue, even if installed into a write-blocking imaging device. If a self-destruction process has already started, there is no practical way of stopping it. The TRIM command is issued to the SSD controller by the operating system as the user deletes a file or goes for formatting the storage medium. This background garbage collection procedure occurs at the hardware level within the SSD itself and is called as "Self Corrosion."
- **Over Provisioning.** Allocating a specific, permanent amount of free space on an SSD, is a widely-used method for improving both SSD Performance and Endurance and is termed as Over-Provisioning (OP). Providing free space to accomplish the NAND management tasks such as Garbage Collection, Wear-Leveling, Bad Block Management means the SSD does not have to waste time preparing space on demand, a process that requires more time as data is copied, erased, and recopied. NAND flash memory's fundamental unit of is of 4 kilobyte (4KB) page, and there are 128 pages in a block. Write operation can happen one blank (or erased) page at a time. Pages have to be first erased and then written. Erasing take place block wise i.e entire blocks of pages must be erased at one time. The SSD actually writes to a different, blank page and then updates the logical block address (LBA) table (much like the MFT of an HDD). Solid State Devices have of space for extra write operations, as well as for the controller firmware, failed block replacements,

and other unique features that vary by SSD controller manufacturer. The minimum reserve is simply the difference between binary and decimal naming conventions. Performance of the SSD begins to decline after it reaches about 50% of its capacity. 28 GB space out of 128GB resulting configuration as a 100GB SSD with 28% over-provisioning.

- **Wear Leveling.** To extend the life of SSDs a process termed as Wear Leveling is used. Data is stored in blocks in SSDs and each block can tolerate a limited number of erase cycles before becoming unreliable. For example, SLC NAND flash is typically rated at about 100,000 program/erase cycles. In Wear leveling data is arranged so that the write/erase cycles are evenly distributed among all the blocks in the storage device. Wear leveling is controlled by the flash controller on the device, and uses a wear leveling algorithm to determine which physical block to use each time data is programmed.

Dynamic wear leveling and Static wear leveling are the two types of solid-state drive (SSD) wear leveling. Dynamic wear leveling pools erased blocks and selects the block with the lowest erase count for the next write. Static wear leveling, on the other hand, selects the target block with the lowest overall erase count, erases the block if necessary, writes new data to the block, and ensures that blocks of static data are moved when their block erase count is below a certain threshold. Static wear leveling is a robust method with most efficient use of memory array maximizes device life but requires high power consumption and can slow write operations. While Dynamic wear leveling is easier to implement and does not have impact on the device performance.

SSD Forensics Challenges

- **TRIM Impact on Forensics.** Theses commands are executed by the microcontroller, once triggered cannot be stopped. TRIM commands will finish even if the SSD is powered cycled. A cyber investigator will not be able to read deleted data from a TRIM-enabled SSD, and users can effectively erase whole partitions just seconds before acquisition.

- **Wear Leveling Impact on Forensics.** It concerns forensic examiners for two more reasons. First, examiners may get a different hash value each time they image a solid state drive. Hash values are a mathematical algorithm represented by a string of numbers and letters that are unique to a set of data, much like a digital fingerprint. Forensic examiners use hash values to verify they have an exact, bit for bit, copy of the original data prior to analysis. The original hash value of the data, and the copy, should be the same. Secondly, an examiner will find it difficult to forensically recover data such as deleted files. The valuable data can appear at any location in the memory array instead of where it should be due to wear leveling and over.

- **Compressing Controller Effect on Forensics.** Compression algorithms are proprietary to the chipset manufacturer hence there is no way to decompress data through off-chip analysis. These SSDs have to be sent back to the manufacturer which is an expensive and time-consuming process and is subscribed to only in most critical investigations.

- **Secure Erase Effect on Forensics.** By wiping data, a perpetuator can destroy digital evidence much faster than with a HDD. Secure erase takes just minutes rather than hours as in HDDs,

so it's feasible that a suspect can issue a secure erase command immediately before the acquisition of the device.

Other Challenges.

- Many other issues play a spoilsport during forensic investigation of SSDs.
- IDE interface allows logical data reads, but hides the internal data structures.
- Internals of SSDs are not well understood. There may be many places where forensic value data may be hidden.
- Since there are no accepted standards, every manufacturer does as per his will. They also protect their implementation details from being read.
- Due to NAND flash technology the same techniques which are used on HDD cannot be used.
- Carving and Free space analysis if possible is a formidable task.

SSD Forensics

- **Hardware.** SSD drives are either attached directly to the computer's SATA interface or connected via a write blocking device of the same type that is also used to investigate magnetic hard drives. Write blockers prevent user-induced modifications to the data stored on the SSD drive, not that of the TRIM command and the disk's internal garbage collector. It is essential to realize that an SSD drive connected via a write blocking device will continue performing background garbage collection, possibly destroying the last remnants of deleted information from the disk. Preventing the operation of internal garbage collection is only possible by physically disconnecting the built-in controller from actual flash chips, and accessing information stored in the chips directly. This method is not popular as it requires special skills and custom hardware.
- **PC-3000 Flash SSD Edition.** Professional hardware-software solution for recovering data from all types of Flash memory based storage devices (USB Flash, SD, MS, xD, MMC, CF, VoiceRecorder, iPhone, and SSD when standard interface of such drives can't access data.
- **SSD Adaptors.** Adapters are used to image SSD's SATA forensic bridges or duplicators.
- **Imaging M.2 and PCI-E SSDs.** Imaging an M.2 or PCI-E SSD drive requires the use of a dedicated adapter. Considering that there are at least three different types of M.2 SSDs (here we will not talk about the differences between B-key and M-key connectors), you are looking for a solution to support M.2 SATA (AHCI), M.2 PCI-E (AHCI) and M.2 PCI-E (NVMe) devices. Atola DiskSense is one of the hardware imaging device that creates forensically sound disk images that can be analyzed with software forensic tools.
- **Software.** Software analysis tools can take over once an image of the SSD is created. Tools such as Nuix, Encase, FTK, CyberCheck and Belkasoft Evidence Center can be used for analysis. Belkasoft Evidence Center is an integrated solution for forensic analysis of computer and mobile devices with support for 700 types of digital evidence: pictures and videos, documents,

mobile apps, encrypted files and volumes, data from browsers, instant messengers, clouds and social media, system files, registries, SQLite databases, and more.

- **Future of SSD Forensics.** By physically detaching the controller and using custom hardware to read information directly from the flash ships, investigators could extract traces of destroyed information that could be stored in various areas of the flash chips.

A group of scientists from University of California designed an FPGA-based device providing direct access to flash chips of the SSD drive while bypassing the controller. The researchers estimated the cost of their prototype as $1000, while their estimate for building production units using microcontrollers instead of FPGA's was as little as $200.

Conclusion

Technology is evolving at a rapid pace around the globe and the Solid State Devices (SSDs) have spearheading the storage wars in the digital world. Faster speed, low power consumptions and absence of moving parts are the need of the hour and the SSDs have placed all these on the table for you. But are giving sleepless nights to the forensic investigators who are running against time when the SSDs are placed on the table for investigation. Maintaining integrity do to garbage collection, recovery of deleted data due to secure delete, smart carving, data remapping, free space analysis, hardware and software for analysis tools and many other questions are left for the forensic investigator to answer. How will these questions be answered only future can tell.

References

- SSD and eMMC Forensics 2016 - Part 1 :What Has Changed in 2016 in the Way SSD Drives Self-Destruct Evidence.Demystifying eMMC, M.2, NVMe, and PCI-E. by Yuri Gubanov, Oleg Afonin (Belkasoft Research)
- SSD Forensics 2014 :Recovering Evidence from SSD Drives: Understanding TRIM, Garbage Collection and Exclusions Yuri Gubanov, Oleg Afonin (Belkasoft Research)
- http://chang-gu.blogspot.in/2015/06/unique-challenges-in-ssd-forensics.html
- http://www.seagate.com/in/en/tech-insights/ssd-over-provisioning-benefits-master-ti/
- http://www.samsung.com/global/business/semiconductor/minisite/SSD/global/html/whitepaper/whitepaper05.html
- http://searchsolidstatestorage.techtarget.com/definition/wear-leveling
- http://www.iacpcybercenter.org/solid-state-drives-ssd-issues-and-challenges/
- http://www.slideshare.net/digitalassembly/challenges-of-ssd-forensic-analysis
- Google & Wikipedia

EFFECTIVE SOCIAL ENGINEERING AGAINST TERROR THREATS

Mr. Nipun Jaswal,
Director of Cyber Security- Lucrypt Limited &
Chair Member, National Cyber Defence Research Centre

Introduction

Social engineering is an art to manipulate people in order to figure out sensitive details about the target or to take benefit from the target. However, in this article we will discuss a new aspect of social engineering that involves a much higher level of target threats, malicious characters that may or may not cause havocs throughout the world. Generally, Social engineering and OSINT(Open Source Intelligence Gathering Techniques) are two different things. However, when it comes to the matter of national security, both of the different techniques need to go hand in hand. Gathering enough information about the target and using it against the target itself is considered as a must use approach against terror threats.

Non Verbal Communication

Generally, when the communication is to be carried out with a terror threat, most of the times its non-verbal which means via email or some social media. Therefore, non-verbal communication aspect becomes very important. The Phases in the complete social engineering attack with a terror threat can be broken/simplified into the following categories-

Information Gathering/OSINT

1. Relationship
2. Development
3. Exploitation
4. Execution

Information Gathering

Carrying out the non-verbal communication with the target, the first and the most important aspect is to apply OSINT on the target. Better the profiling in OSINT, better the results.

This phase includes the following steps to be performed for the target profiling-

1. UsernameExistence Search
2. Using reset password fields to re-establish original email identity
3. Searching for a particular user on other social media
4. Linking an email to the username at various social media sites.
5. Fetching personal details like phone numbers and close contacts
6. Basically everything you can do to figure out as many as details about the target without making any direct contact

A small example of this can be seen in the following screenshot-

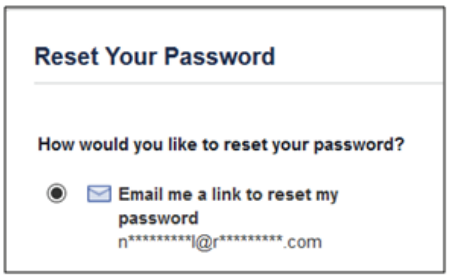


Figure : Email Address Construction

We can see from the above screenshot that if I have only the username from any other social media, I can use it on facebook or twitter to figure out the real email address or its parts. We can see masked email address in the picture above. Let us try finding the actual email address behind it-

We have,

N*********l@r*********.com

Looking at the username, we had "nipunjaswal". Therefore, we figured out-

nipunjaswal@rocketmail.com, but how? Counting the number of asterisks in the email and matching it with the username/name.

Nevertheless, real world scenarios are quite different and difficult. Let us say we have a username called "momohsab" and using the same trick, we apply reset skills to something like-

M*******b@g****.com

Counting the number of asterisks and matching the username with the email address pattern is a little bit trickier in this one because the email address has seven characters hidden, but the username has only six.

Therefore, insuch cases,

We can always try to give a shot at the "." Between first and the last name. Which means the username can be-

Momoh.sab@gmail.com

There might be cases where trailing last digits are numbers. In those cases, the most generalized approach is to try the last two digits of the birth year or to usemanual brute force from multiple source addresses. This is just one of the approach that we carried out. There are many more as stated earlier in the listed points above.

Relationship Development

Highly important and one of the most critical phase of the social engineering attack carried out on the terror threats. This phase is most critical because if the investigator accidentally blows off his cover, he can be in live threatening danger. Therefore, this phase is to be executed only by trained social engineers.

This phase is the actual phase where we make direct contact with the target through nonverbal communication.

An important thing I must remind the readers before you proceed reading is that these all techniques are what I use from the past few years in my investigations. This may not be a standardized approach but is highly effective.

Relationship development is dependent upon the type of target. Let us say I know that the target is a 23 M years old college going student. My approach would be the following-

1. Use an old Fake profile with a girl's picture to start liking the target's updates, especially when the likes on his posts are very low. Or on those posts where there are no likes or very few likes(This will actually cause the attention of the target)
2. As soon as the target is connected on the social profile, I generally wait for few hours (sometimes days) to send him the first message or begin a personal conversation.
3. On the targets who are less than 30 years of age, single or students, I generally use the similar approach with little modifications. Most of them include the following-
    - No constant chatting- this means i would not talk to the target constantly but will create the liking in the target that would force him to send messages to my fake profile at odd times when I am not online
    - Asking for mobile number is the second general step I take when the trust factor builds in
    - I would establish more trust by faking my web cam and playing a matching video to my profile picture

Once the trust factor builds in, I would ask the target to view some random links based on my relationship development profiling with the target.

However, within those links I would also include the malicious link that will eventually help me to break into the target system.

My approach to the targets above the age of 30 would be quite different and this would be same for the people who are confirmed malicious characters in the world. My approach would be the following-

1. I would rather go for a novice terror profile on the social media
2. Following almost everyone from the target's profile
3. Seeking people the target is tweeting to or is mentioning in public posts
4. Would go with another profile and will try impersonating the contact he is trying to contact.

An example here would be say our target is tweeting to the username, "ertogi8". We can actually create a similar account with the handle "ert0gi8". The only difference is the character 'o' is replaced by zero in numeric.

In the past few CCI, I have used the above technique by replying to the target by impersonating on the public posts and have been highly successful.

Important things to consider while relationship development includes-

1. Patience- A lot of patience, one bad move and the target is gone
2. Never send any malicious link unless and until the relationship factor is built
3. Try communicating in the ascent the target uses- this may include all capitals, all smalls, repeated words, use of trailing periods, broken English etc.
4. Never ask the target directly where does he live, work etc.
5. Questions should be tricky, like-

   Q: The background of your profile picture is beautiful, where is this place?

   Expected answer would be-

   A: This place is XXXXXX (Whatever, we do not have to go right)

   Next question-

   Q: Oh Wow, so u live there?

   In addition, the expected answer would be-

   No (80%) and yes (20%) most of the people choose profile pics to the places they visit. However, this is generally followed by the name of the place they live like-

   A: No, I live in XXXXXXX(Like I said we don't have to go)

   This question is quite trickier as if the person under suspicion has built trust on you or not.

   The answer would be the one that is above. However, if the person is still having suspicion and is not willing to rely on you, his answer would be "NO".That is it; we do not have to try asking him again any sooner and may be in few days.

Exploitation

Once we have the trust of the target,the next phase is to exploit the system via malicious links and phishing techniques. However, I would personally suggest not to run any public exploits as it may trigger anti-virus alarms and may cause loss of trust.

The only thing advisable here is to run for IP details that can be fetched easily by creating a page where the target visits and is logged.

Exploitation is only necessary when the target is behind a proxy server or a virtual private server that is anonymous. In those cases, we can try hooking the target browser to the browser exploitation tools or fake pages that can actually harvest target details.

Choosing the right website is also a critical step and care should be taken while choosing the one. Let us say a news website is hacked or the investigation team has their own site where they can modify any page on their will. They can use that website to create a trap for the target to fall in. An exploit framework running at an IP 172.168.10.15 will create more suspicion than a domain name which is http://www.news-at9.com Visiting the website will trigger the same exploit running at 172.168.10.15 but will catch less eyes.

Execution

The final phase of the attack on the terror threat. This phase involves gathering information from the exploited system and extracting it to a meaningful form. I found an inadequate music album on an exploited system while carrying out an investigation in earlier 2012. Later I found out that the album only contained one music file, which was NewSongExe.mp3. Examining the file headers I found out that the file was an executable and its extension was mp3 because of left shift operators in the name. This file was found out to be a program to encrypt email text, which was decrypted later by reversing the executable itself.

Other important things to do on the terror threat's system are-

- Finding the text files
- Finding documents and PDFs
- Examine cloud storage providers like SkyDrive and DropBox
- Examining the backdoors on the target's system which may lead to the entire group of terror enabled characters
- Examining window shell bags for important data related to file access
- Examining odd size files on the system

Throughout the article, we discussed information gathering, relationship development, exploitation and execution of social engineering skills on the terror enabled threats. This information will help you leveraging social engineering skills on the target. However, further reading on sharpening social engineering skills is very important.

BUILDING "SAFE & SECURED CYBERSPACE FOR WOMEN"

Smt. Shubhamangala Sunil

Cyber Security Expert & Director, "Global Cyber Security Response Team"

National Technical Committee Member - National Cyber Defence Research Centre.

Do we have "Safe and Secured Cyberspace for women" in this virtual world?

Will this Cyberspace ever be safe for Women?

For the millions and millions of women and girls who use the internet(smartphones) every day to navigate their jobs and personal lives, online abuse is not only emotionally devastating, but it also curtails their professional choices and their full participation in business and personal life. In an era when 70-80 life is connected with online and most percent of companies conduct internet searches on job candidates, and many positions require a high Clout score or thousands of Twitter followers, women simply cannot afford to not be online and miss chances to getting on the track where the world is going with this advanced technology.

Cyberspace/Virtual world is as densely populated by women as men, but it need not always be a friendly space for women in this virtual world. Young girls and women need to be alert as they make their way through cyberspace and be aware of the many pitfalls in the virtual world.

Women experience sexually explicit or threatening messages 27 times more than men. Considering the real world implications and the lengths to which women must go to protect themselves, we have to demand more from those charged with enforcing our laws and utilize the technologies more on the security side for women in today's virtual world

Technology, is an 'arbitrary benevolence' where safe, secure and effective utilisation is of the essence. Social networking sites are essentially beneficial intermediaries between people in today's world. However, there exists a nemesis to each godsend. There are many snares galore in cyberspace such as identity theft, morphing, phishing, hacking, fake images, unsafe chat zones, misuse of personal information sharing, online harassment, Women trafficking and more

Who could we blame women for deciding it's not worth the effort?

Just less than one-third of Working doctors are women, as are just more than one-third of Working women are lawyers. Yet women make up just 10 percent of those working in information security. At a moment when computer security is receiving more attention than ever before, and is it only the women in IT world should be caring about Cyber Security and as people become increasingly concerned about whether we are training enough security professionals to meet the growing demand, the lack of women in the field is especially striking—and concerning and giving space for women being the major victims.

More than in real world, women are being harassed and threatened online. Most of the cases are not reported or victims are not being able to decide the incident as cybercrime. Because we do

not take online threats and harassment seriously, women are denied their right to freely express themselves and to live without fear. Due to our inaction, thousands of women have simply opted out.

The women who are being attacked for nothing more than making a video game, abusive photos, expressing a feminist point of view, or simply reporting the news deserve better. We must not allow the Internet to be closed to female voices, and intensifying the enforcement of existing law is a critical first step to ensure the Internet is open to everyone as gender and age neutral.

At the same time, we notice that the awareness programs conducted in our nations about the information technology and security with the cybercrime and measures to stay safe in cyber space for women seems very less, which is marking the increasing note of cybercrime in cyberspace with young girls and women are more.

"The way we train our girls/Women, we don't necessarily raise them to be competitive against other people in virtual world,"

Being a victim of cybercrime is the most traumatic experience for a women posing major threat to her security. Moreover, with the advent of information technology and internet, cybercrimes with the all the benefits of anonymity, reliability and convenience have become a global phenomenon. As per United States report on Internet and Computing Trends, Indians are the second largest sharers of personal information over the internet after Saudi-Arabians. With increasing popularity of chat rooms and vulnerability of personnel data to criminal access, women in India have become soft targets of variety of cybercrimes such as pornography, sexual defamation, morphing, spoofing etc. With the objective of protection and promotion of e-commerce, Government of India enacted the Information Technology Act 2000, but in terms of computer socializing communication and cybercrimes, this act is a mere gap filler.

The most embarrassing aspect of pornography industry is the child pornography. Which can be mitigated only by spreading the awareness to young ones.

Types of Cybercrime against women:

- Online Harassment/ Cyber Stalking
  - ❖ Via
  - ❖ Email
  - ❖ SMS/WhatsApp
  - ❖ Social Network etc.
- Personal Video Upload
- Data theft/Identity Theft
- Sales and Investment frauds
- Pornography and other offensive material
- Job offers (online)
- Cyber Sexual Defamation
- Cyber flirting

- Virtual Rape
- Women Trafficking and more

(Not all crimes are listed and discussed in details only very imp Crimes are discussed here)

Cyberstalking/Online Harassment: (is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyberstalked relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected).

Personal video Upload: (Uploading the videos captured without knowledge of victims or selling the same on online)

Sales & Investment fraud: (The Internet is a quick and easy way for scam artists to find potential victims for their investment scams. With the Internet, fraudsters can operate anonymously from anywhere in the world, making them hard to catch)

Cyber sexual defamation :(happens between real or virtually known people who out of frustration start publishing defaming stories in obscene languages on various social websites subsequently it turns into cyber pornography)

Cyber flirting: (Generally cyber flirting may be considered very minimal petty offence that starts when perpetrator force the victim to hear obscene songs, messages and it may consequently result in cyber sexual defamation and breach of thrust.)

Virtual Rape: (This is a violent type of cyber victimization where the targeted woman is taken up by a harasser. He either posts constant messages like "I will rape you", "I will tear you up" or "your internet identity will be f...ed off" etc, or particular community members may "mob attack" the targeted female with such words which successfully generates more enthusiasm among other unrelated members to comment on the victim's sexuality. The profile owner then becomes a hot topic for erotic discussions, vulgar name calling etc.)

Women Trafficking: (Where online media is used to convince Women or young girls to get yielded for job offer or any other aspect and turned to trafficking).

	Harraser	Victim
Men	49.5	22
Women	28.5	72.5
Multiple Gangs	1.5	
Unknown	21.5	5.5

Source : WHOA (www.haltabuse.org)

As gender neutral we all should understand that not only the crimes in cyberspace "It is common knowledge that if any online service/app/software (not from legitimate source) is available for free, then you are a product, not a customer. What a person searches for is perennially catalogued and vaulted in the clandestine chambers of the worldwide web. Deleted evidence or data can be traced and recovered. The Internet is not a gateway to anonymity. That is one lesson that everyone entering the cyberspace should remember,"

The new term Gamergate in Virtual World:

Gamergate: The threats made against women under the guise of the online or virtual world is known as Gamergate are terrifying. Targeted women have had their personal information publicly disclosed - including their home addresses - and they have been threatened with murder, rape, and all manner of violence using the cyberspace as tool.

While Gamergate has garnered headlines, the truth is that every day is a dangerous day for working women online. Journalists, academics, and other professionals who dare to express an opinion – especially a feminist one –are routinely attacked. Young women are deciding not to pursue jobs in technology to avoid the crosshairs of men who don't think they belong. Women who are being asked to run for public office are choosing to stay on the sideliners once they see the online abuse suffered by their peers. Others are being driven offline, sacrificing their freedom of expression for safety and self-preservation. By seeing the cybercrime cases against women, she staying offline makes no sense, as directly or indirectly some where the people are 100% living in this virtual world and staying away from this space is impossible.

For these kind of cybercrime reporting any sites require that each threat must be individually reported and the time and effort it takes to report each one when you are receiving hundreds or thousands of them is emotionally taxing, time consuming, and expensive. So most efforts to make the Internet a more hospitable place for women are reactive approaches that seek to address problems after they take place, rather than proactive approaches that seek to prevent harassment at its technological roots. If it seems like all we can do is hack at the branches of this problem rather than its roots, maybe it's because we're too focused on the people who use technologies rather than the technologies themselves.

Cyber Socializing

While cyberspace have provided secure tools and spaces where all young girls and women can enjoy their freedom of expression, information and privacy of communication, the same benefits of anonymity and privacy also extend for criminal activities and commit violence against women in the virtual world

World wide web has redefined the virtual world life of ordinary individuals and has given wide opportunities for internet users including women to exchange ideas, interact with likeminded people and participate in the development of virtual societies as per one's own choices. Social networking websites (SNWs), a segment of WWW is very popular among the internet users. However, we do have the darker side of this. They have become havens for offenders to victimize women by using this, the most vulnerable targets in the internet, after children.

Socialization through social networking websites (SNWs) has become a favourite hobby for "gizmo freaks", self-supporting, educated, independent, modern women, wife at home of the 21stCentury. The social networking websites help users make new "virtual friends" and offer "promise" to reunite with old friends and relatives. Most young girls and women users avail this new way of socialization as a stress–reliever and time pass Cyber/virtual socializing through

cyberspace help women users to share with likeminded friends, their emotional needs, personal problems, job opportunities, culinary skills, tips for child care and health care including pregnancy and post pregnancy issues. But most women users discuss these "needs", tips and even their "mood swings "with their virtual friends who become "emotional comfort zones" for them either by writing on walls of some group/community forums or on the walls of their friend's profiles, or send personal messages using the advanced technologies help. Cyber socialization is the "computerized interaction with known or unknown individuals for the purpose of communication, research, entertainment, establishment of friendships or relationships due to feelings of loneliness, and sexual gratification"

Internet socializing is "electronic interaction" with virtual friends through chat rooms, emails, forums (created by domain hosts like Google, Yahoo, twitter, IRC) and social networking websites. Even though social networking websites have opened a wide window for socializing, they have also opened flood gate for various crimes against women in the cyber space. Which most of women miss to read between the lines of security in the cyberspace.

The main aim of cyber socializing is to give the users opportunity to meet with old and new friends, increase networks and socialize without actually going in person to the social gatherings sitting at home or office. But this is not a hazard free zone. The main drawback of cyber socializing is the uncertain reliability of the "virtual friend" we meet up every day in the virtual world, may be the known criminals are in touch with the victims too. At the same time, many users treat cyber socializing as a space for overriding their freedom of speech and expression This attracts many offences like cyber flame, cyber hate speech, cyber bullying and cyber eve teasing etc. Online socializing never remains risk free for women mainly due to their sexuality and also the less awareness of crimes on online. Majority of the cybercrimes targeting women happen in internet but as no society can be crime free, online/virtual societies are no exception. Cybercrime exists and it is growing in number through SNWs, mails, online chat rooms etc.

Social networking websites provide a wide range of social activities to be carried out in the cyber space. It is therefore very obvious that online socializing is also as vulnerable as real life socializing. But the patterns may differ due to the hi-tech nature of the offences and the technology used to commit the crime. The attackers may or may not be known to the victims and reasons and motives behind victimization are mostly emotional issues. The harasser also uses the broader platform of the cyber space to victimize the target under camouflaged identities. Moreover, the unequipped, not-so-fitting, or developing laws, where such offences are not recognized or are yet to be recognized, help to expand the pattern of victimization day by day with the help of available tools and platforms in this virtual space.

The two main reasons which attribute towards the growth of online victimization of women in the Cyberspace are: absence of proper gender sensitive universal cyber laws and lack of awareness of the safety modes among users of the social network and specially for internet usage too. The social networking sites are considered as a large global platform to express one's ideologies, thoughts and feelings about others. Every individual is supposed to use this platform at his or

her own. But unfortunately, there are less laws and policy guidelines to regulate cyber space and this insufficiency gives full freedom to the perpetrators.

The Sociological reasons for cybercrimes:

Most of the cybercrimes, especially in our nation remain unreported due to the hesitancy and shyness of the victim and her fear of defamation of family's name. Many times women consider that she herself is accountable for the crime done to her. The women are more vulnerable to the danger of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Women fear that reporting the crime might make their family life difficult for them, they also question whether or not they will get the support of their family and friends and what the impression of society will be on knowing about them. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.

The main problem of cybercrime lies in the modus operandi and the persistence of the cybercriminal. The police, judiciary and the investigative agencies need to stay abreast with the latest developments in web-based applications so that they can quickly identify the actual perpetrator. It is the job of the legal system and regulatory agencies to keep pace with the Technological developments and ensure that newer technologies do not become tools of exploitation and harassment. Governments can take legislative measures that ensure human rights; especially women's rights are protected online just as they are physical spaces. should not just protect users; however, it should also educate and inform all groups on how to exercise their cyber ethics in cyber world. At the same time, Individuals must become savvy both online and offline; know how to take precautionary measures in cyberspace and how to seek recourse if their rights are violated.

Cybercrimes against women are still taken lightly in India, mostly because in general the respect towards women in our modern society is on a decrease, also a lot of people are unable to come to terms with the fact that even posting images of someone online in a crime. Cybercrimes such as morphing, e-mail spoofing do not have a moral backing in society and hence are taken lightly. This brings us to the most important part where social advancement is needed, people need to recognise the rights of others and realise what constitutes a crime. They must learn not to interfere with the private lives of others, respect towards women in society needs to increase. All this can only be done if young kids are taught from a young age to respect women, the increasing number of crimes against women are a huge concern for any state however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this government should make stricter laws to apply on the Internet Service

As we all know "Just as a soldier or a terrorist put their weapons to divergent use, women should learn to use this powerful weapon of technology, especially in the cyberspace for their advancement and remain vigilant against getting trapped in disastrous situations,".

There is no single answer to cyber-risk, but rather a combination of security best practice and policy, technical measures to discover and prevent breaches, and mitigation including backup plans and insurance in the event of a disaster.

The Cybercrime problem exists between the "keyboard and the chair"

"The secret ingredient of getting the cyber security on track is cross-industry collaboration, taking identity out of the competitive space, moving it into the collaborative space. Providing awareness and training programs with respect to all sectors of Govt and Private divisions"

Providing the safe and secured Cyberspace for women is every individual responsibility

Let us take ought to be a part in

Building "Safe & Secured Cyberspace for Women"

- Respecting sensitive data of each individual on online
- Say no to visit abusive/porn websites
- Be the first to lodge complaint against any in of cybercrime
- Say no to share Personal videos online
- Be responsible individual in online activities
- Set and spread knowledge of minimum age to join cyber communities like Facebook, twitter, Myspace and so on
- Use safety tips like filtering emails, locking personal albums and information, Personal walls of social networking sites and etc.
- Stop think and Connect, while sharing Personal information/Emotions with virtual friend's/ Chat room partners or any sensitive data online.
- Know what exactly is meant by free speech while communicating in cyberspace
- Make habit of reading Policy guidelines while downloading Free/paid apps or software
- Never miss any chance in training or providing awareness to women about cybercrime and security.
- Never forget that internet has no borders of countries
- Spread word to Avoid furnishing personal details such as family background, picture related to the people with whom you are socializing, your private moments etc on social websites like Facebook, Google+, Twitter, LinkedIn as it can be easily misused.,
- Suggest all known women to check while in hotels, restraints or changing rooms in mall, to always check for two-way mirror and for any camera installed.
- Say yes to make two kinds of online presence one for social networking and other official.
- Say "NO" for trading personal information for "freebies."
- Say no for clicking links embedded in emails - type the URL into the browser and go from there.
- Be selective about who you interact with online and what information you make public.
- Discuss online safety with your family and friends.

Dreaming about Safe and Secured Cyberspace for Women in nation is right of every individual woman in our nation, let us make this dream come true.

3D : DANE - DNSSEC - DNS

Mr. Aravindh Subramanian

Associate Manager – Information Security | Gavs Technologies Pvt. Limited

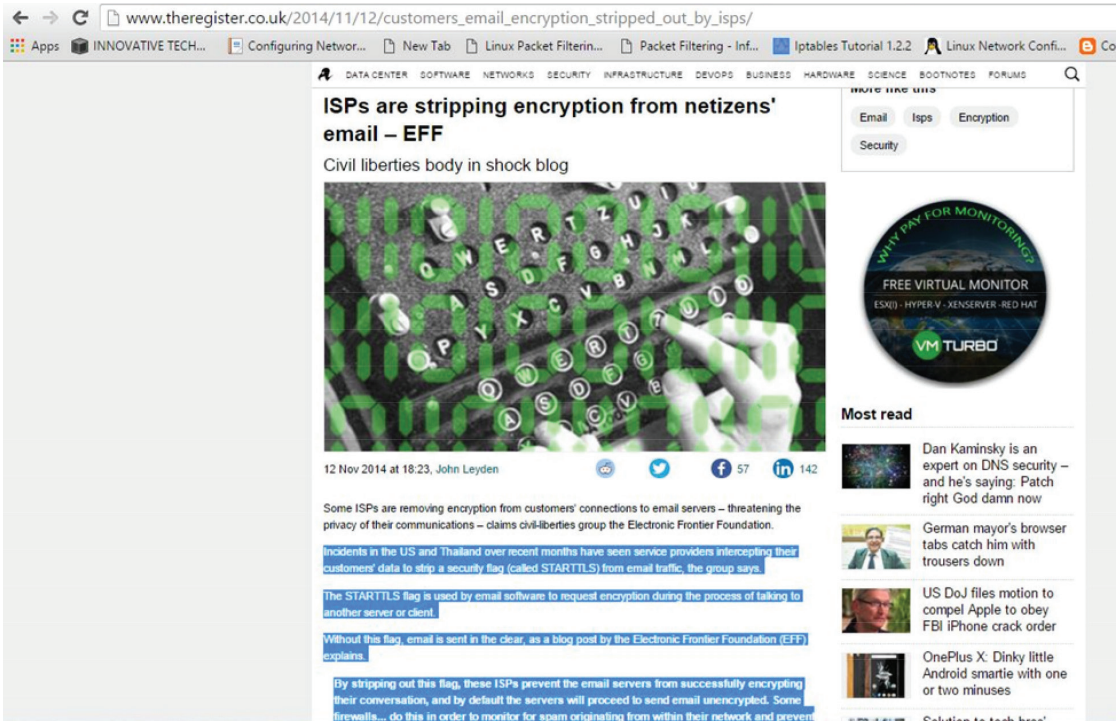
Chair Member, National Cyber Defence Research Centre

DNS is vulnerable - Cannot be trusted, No improvements since 1983 and usage of functionalityand quantity has widened.

Risks | No DNS - no webpage

| Wrong DNS - wrong webpage

Beside, Security fails with Opportunistic Encryption which leads to unauthorized and compromised certificates, Man-in-the-Middle attacker may downgrade session to non-TLS at the time of email communications.



Hacker can intercept TLS communication by mapping certificate from the way of MITM and improper configurations accepts self-signed certificates.

DANE is vow technology that might change our present and future. It's a DNSSEC trust scheme for X.509 certificates provides encrypted email communications.

DANE – DNS based Authentication of Named Entities provides, layered security by fastening the X.509 certificate of a website to the DNS. This another channel provides details about X.509 certificate to the user who can use to validate certificate.

DANE uses DNSSEC → DNS turn into policy channel → DNSSEC affix trust layer

DNSSEC - DNSSEC abbreviates "DNS Security Extensions" DNSSEC adds security to the DNS by embodying public key cryptography into the DNS hierarchy. When carried out via an attack on a networks or an ISP's infrastructure, all of the entity's users are affected. This is often referred to as DNS cache poisoning, DNS malware borne attacks, Man in the Middle attacks and DNS redirection / DNS spoofing.

NCDRC's take on DNSSEC and DANE

We have tested DNSSEC validation on our resolvers by using Bind9, Mozilla, Chrome and gateway which means our resolvers always validate queries for domains that have been singed using DNSSEC. Users automatically benefit as fast as a domain is signed using DNSSEC.

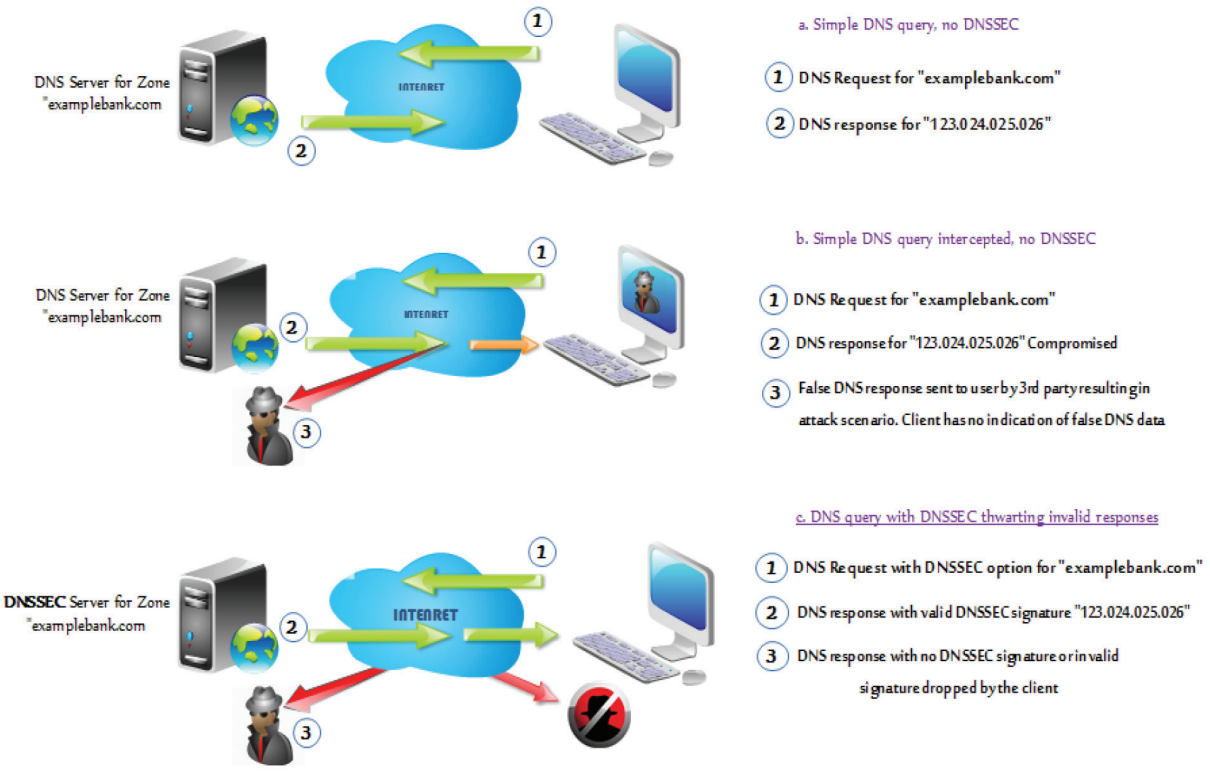
Nevertheless NCDRC moving to DANE.

So far techies deploying DNSSEC on their domain names – "sign" domain names or ask Registrar for DNSSEC (Enable DNSSEC validation on originations/ISP DNS resolvers). World really needs lots of DNS resolvers. Beside, ask ISP about DNSSEC and support on their ISP DNS resolvers.

Recent days naive techies debates on DNSSEC vs. Secure Sockets Layer (SSL)

Both DNSSEC and SSL depend on public key cryptography. DNSSEC deals with "where", and SSL deals with "how" and "who".

Testing results: Below image explains the process of with DNSSEC and without.



Below image is the proof of concept tested on Mozilla Firefox browser with DNSSEC validator

DANE is targeted by Security providers, Government or Private Email users with known security needs, Online-Payment sites, insurance providers, banks, Enterprises and Internet of Things. DANE is de facto standard technology.

CYBER SECURITY AS A CAREER

Mr. Vijay Kumar Velu

Director - Cloud Security Alliance (CSA) Bangalore Chapter

Chair Member, National Cyber Defence Research Centre,

Many top market research firms have estimated the cyber security market as around $170 Billion by 2020.The purpose of this article is to provide insights into Cyber Security World and how an individual could potentially start a career in this hyper market.

Cyber Security in General

It is the bundle of technologies, process and practices designed to protect almost everything that holdsInformation. This includes networks, computers, Mobile devices and any form of electronic gadget that transmits and stores information.

Cyber Security Professionals

Cyber Security professionals often bloom in a casual atmosphere, unusual timings, and ever-changing work tasks aimed at keeping information new and work exhilarating. The attitude of a Cyber Professional is "how a Hacker may think or act" - using difficult cracking skills often compared to those of an investigator. This level of work difficulty requires the Professionals at workforce to possess both a wide range of Technological IT skills and also advanced problem explorationabilities.

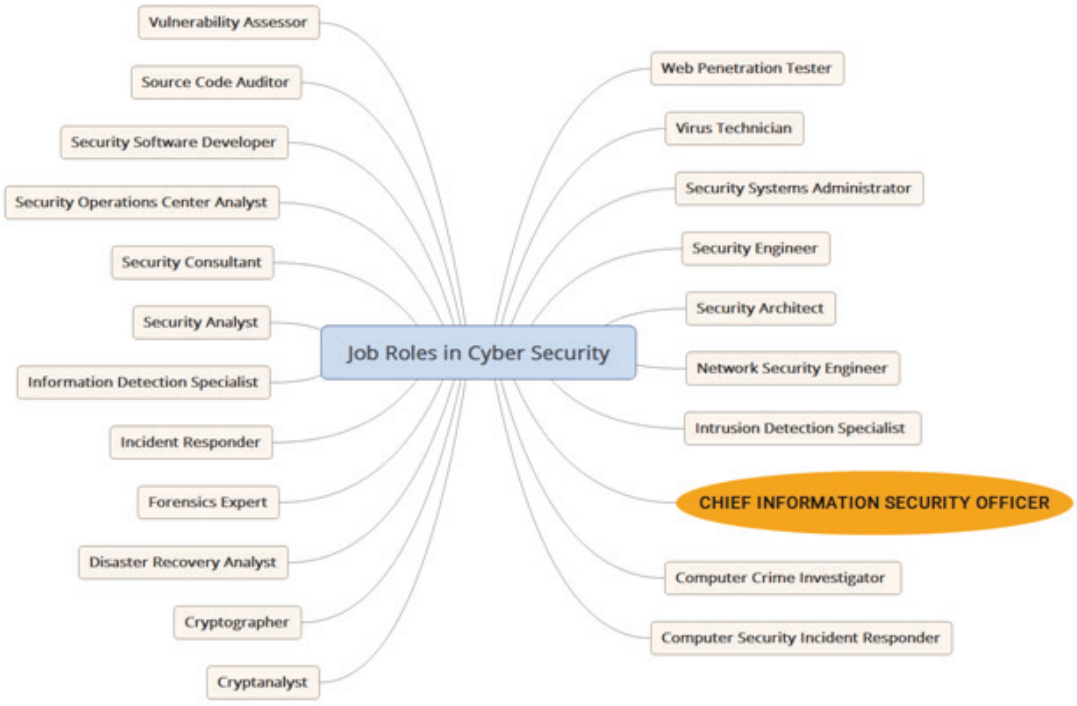


Fig. Job Roles in Cyber Security

Cyber Security Job Roles

The below diagram provides a list of the job roles that are currently available in the market. There is always a cross-over in Cyber Security jobs for an example, a Systems programmer could take over a role as Source Code Auditor or a Systems administrator and can transition himself into Security System Administrator focusing only on security.

Building the fundamentals

In order to even step into cyber security world, there is no shortage of information security oriented books that will help you understand and setup a goal for yourself. Reading them, one must build the capabilities around the below suggested areas,

Find your specialty

Cyber Security is a broad field to be working in, so people need to make sure they are specializing in a marketable skill. For a fresher, it would be difficult to make a choice, hence it is recommended to participate in information community events, seminars, workshops and look for mentors who can guide them through. It would be not logical to know everything in cyber security world and not be a master at even one skill specialization be it Audit, Forensics, analysis, architecting and so on.However if you learn everything you still have a good chance to transition yourself into Cyber Security Generalist category.

Getting a lay of the land

Just looking at the advanced technologies that are booming or what skills are in demand will stop the individual to focus on upcoming development.

Complexity

In order to make sure you generate your own demand for skill enhancement, below are some matter of attitude that an individual in cyber security can develop irrespective of their experiences.

- Skill enhancement as a problem-solver than looking at the technology as the entry point and also develop strong analytical math skills.
- Excellent verbal and written communications.
- Understanding of business management skills.
- Ethical, Honest and Trust worthy.

Mentoring

Locate a mentor who can be your trusted advisor and becoming a protégé gives you access to someone who owns the skill set that you desire, may be has the same cultural background and understands the details that can't be explained through a presentation or a manual.

Certifications

As and when the demand for Cyber Security technology has increased, hardware and software providers have developed certifications specific to their product lines. Certifications can target a specialty. There are professional and business organizations have developed respected vendor-neutral certifications that focus on validating a professional's mastery of the practice of IT Security.

Entry Level

These are usually identify professionals with zero to three years of experience who are able to implement and maintain cyber security, but are not necessarily able to plan or design security policies, conduct security audits or evaluate tools and technologies and so forth. Some of the certifications are A+, N+, S+, Linux Administration, Comptia +, MCP etc

Intermediate Level

These are usually identify professionals with three to six years of experience who can not only implement and maintain cyber security, but also may be able to assist with planning and design of policies, conduct audits and evaluate tools and technologies. Some of them includes CCNA, CEH, CCNP, RHCE, etc

Advanced Level

These usually identify the professionals with seven or more years of experience who understand cyber security thoroughly and completely and can handle multiple stuffs including planning, design, implementation, maintenance and other tasks as needed. Some of the certifications include CCIE, CISSP, PSP, LPT etc.

How does Certifications add value to you?

Always remember certification in most cases prove that you only have acquired the knowledge and passed a test. It is recommended to seek for different ways to validate your knowledge and put into action. There are no ideal ways to address the certification knowledge that you acquire.

Inserting into profession

Let's take a small step into the educational background and how it would benefit an individual and position themselves into the way the current market requirements. Be it Engineering or Technology - Electronics and Communications | Telecommunications | computer science | Industrial and others.

Let's all accept it, Entire Cyber world is built upon the layer of electronics be it Internet of Things, Smart Grids, Cellular networks and pretty much everything that we use in our day to day life.

Typically someone with any background can become a Cyber Security Professional for example an Electronics and Communication personnel comes with fair amount of basic knowledge around hardware such as Microprocessors, micro-controllers and technologies around Wireless, Digital & Analog, Antenna and Wave propagation, Assembly Language programming and so on. This knowledge that you acquire from the academic curriculum will provide you with wide breadth of information to start your career.

Security Environment

Building and practicing on your own will help you understand what you are doing, how you are doing and your knowledge level. For example an aspiring penetration tester would try and build their own Lab with the available resources and practice the concepts such as information gathering, scanning, tooling and other. This knowledge will enhance the employment opportunities.

Conclusion

In summary, the following action items will help to build a career in Cyber Security but not limited;

- Do the right rule – Demonstrate high personal integrity
- Be known as a contributor
- Always look for opportunity to build your skills in everything that you do
- Be open to shift your focus on much bigger perspectives
- Continue education
- Your goals are defined according to your commitment.

Other Contributors to the Article

Rachel Martis, Anil Dikshit, KarthikBelur Sridhar, AvinashKuduroli and Praveen Malhan.

SECURE YOUR SELF BY TOO MUCH INFORMATION (TMI)

Mr. Mayur Agnihotri

Director at ARNE Solutions & Information Security Consultant at Virtual Support Business & National Technical Committee Member - National Cyber Defence Research Centre

Social networks and new on-line services make it easy to share the details of our lives, perhaps too easily. With just a few clicks, posts and messages, you can give away enough personal information to compromise your privacy and even open yourself up to identity theft.

Hackers use information you post on-line to try and trick you into giving up access to your email, social networking and financial accounts. And sometimes they can use the information you post online to reset your account passwords so you no longer have access to them as your pet's name, mother's maiden name are often the security challenge questions for on-line sites. Children are being exposed to technology increasingly each day and at even younger ages than before. Often these children also have a better understanding of how technology works than adults and parents.

Note: Eight in ten young people are victims of cyberbullying and 45 percent experience cyberbullying on a frequent basis.

Cyber ethics help Internet users understand what type of online behavior is right and wrong. Cyber predators are people who search online for other people in order to harm them in some way.

Some Tips for Protecting Kids

- Create an open and honest environment with kids.
- Start conversations regularly about practicing online safety.
- Watch for changes in behavior
- Make sure mobile devices are secure. Use PINs and passwords, only install apps from trusted sources.

Identity theft is the illegal use of someone else's personal information in order to obtain money or credit sometime for revenge.

Information Security Education

What is Information Security?

The protection of information and information systems from unauthorized access, disruption, modification, disclosure or destruction in order to provide confidentiality, integrity, and availability.

There are three elements to protecting information:

- **Confidentiality –** Protecting information from unauthorized disclosure
- **Availability –** Defending information from unauthorized users to ensure accessibility by authorized users.

- **Integrity –** Assuring the reliability and accuracy of information resources.

Your bank ATM is a good example of an information system that must be confidential, available, and have integrity.

Threats and vulnerabilities put information assets at risk.

- **Threats –** the potential to cause unauthorized changes, or destruction to an asset.– Impact: potential breach in confidentiality, integrity failure and unavailability of information.
- **Vulnerabilities –** any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- **Risk** – the likelihood that a threat will exploit a vulnerability.

The Internet can be a major way to connect with friends and family and to alimentation an interest or a hobby

Parents should be aware of which social networking sites their child uses, and should view their child's profile to ensure that they are behaving appropriately and are not disclose private information.

Talk with your kids about cyber bullying and other online issues regularly.

- Know the sites your kids visit and their online activities. Ask where they're going, what they're doing, and who they're doing it with.
- Installing parental control filtering software or monitoring programs are one option for monitoring your child's online behavior.
- Encourage your kids to tell you immediately if they, or someone they know, is being cyberbullied.

Initiate rules about appropriate use of computers, cell phones, and other technology.

Here Are Some Tips To Remember:

- **Don't Reveal Personal Information —** Seriously consider why it's needed before you post your address, phone number, Social Security number, or other personal information on-line.
- **Manage Your Privacy Settings —** At most, only friends you know in real life should be able to see details of your profile.
- **Change Your Passwords Frequently —** In addition to choosing passwords that are difficult to guess (try to make them at least eight characters long and a combination of letters, numbers, and symbols), remember to regularly change your passwords.
- **Only Send Personal Data Over A Secure Connection —** Never shop, bank, or enter passwords or credit card numbers over public Wi-Fi or free hotspots, like in cafes or airports.
- **Turn Off The GPS (Global Positioning Service) Function On Your Smartphone Camera —** If you are going to be sharing your images on-line, you don't want people to know the exact location of where you are.

- **Consider Sharing Vacation Photos When You're Back Home—**Sharing photos of your trip and announcing you're on vacation is fun, but it's also announcing to would-be thieves that it's a good time to rob your home.

Posting personal information and photos on networking sites can be fun and convenient, but it can also lead to identity theft, cyber-bullying, or hurtful gossip. What's more, mistakes and triumphs that used to fade over time in the real world are now archived on on-line for all to see. In an age when smart phones double as shopping carts, photo albums, and even personal assistants, knowing what personal information you share matters more than ever.

Where you went to elementary school, your favorite food, where you honeymooned, your first grade teacher, father's middle name, mother's maiden name, kids names, birth dates, where you vacation, your high school sweetheart, your home phone number, mobile number and even your email address: All this information, believe it or not, unfortunately, is way, way, Too Much Information (TMI).

THE FIFTH DIMENSION OF INDIAN SECURITY: CYBER SECURITY

Mr. Nitin Pandey

Chairman: DEFCON *Lucknow & OWASP Lucknow International InfoSec Meet*

Founder of Hackers Day

National Technical Committee Member - National Cyber Defence Research Centre

In today's cyber world internet/cyber security is no more "a good to have" but "a must have". We now live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. Recognizing the importance of cyber security to our nation, I believe that it 5th dimension of Indian Security in upcoming years.

We have probably seen the news about companies around the world being hacked. These are companies that have millions of dollars invested in technology and have top-notch security professionals at the helm. While organizations invest in IT security infrastructure, many of them lack in the biggest security gap: The User.

People are trained to perform their jobs in technology, accounting, sales, etc. but lack the basic knowledge of how to protect company data from the outside. You can't assume that everyone knows the rules, cautions and dangers. Hackers are getting better and better at disguising their methods, it's not always obvious.

To have an effective security program, individuals need to know what to do when hackers call them, how to identify a hacker's emails, how to know which software apps are "safe" to download, among other things. Probably most important is what to do when those hacker attempts are identified.

The best solution to secure IT domain is Security Awareness Training. It is a critical component in protecting an organization's most important asset - its data. Training users to identify and avoid risks and make good judgments online are critical elements of network security.

The key to leveraging security awareness training to protect your data isn't just a one-time blast; it's a continual learning process. That's why a well-organized cyber security training program includes reinforcements throughout the year like posters, newsletters, videos training, evaluations and videos. India is growing fast in security awareness trainings worldwide by conducting various security conferences, meets, summits and trainings. New researchers are coming out with their precious knowledge and potential.

In an order to create participative, transparent and responsive government, Prime Minister Narendra Modi launched the much ambitious 'Digital India' programme recently which is a great initiative and an appreciative step towards making India a powerful Cyber Secured nation.

THE CYBER EXCHANGE PRINCIPLE

Mr. Vikram Karthik

Digital and Cyber Forensic Professional &

Chair Member - National Cyber Defence Research Centre

The "Cyber exchange principle" is often applied in the context of cyber crime. Forensic examination of a computer or server can uncover traces of digital invasion. The investigator is then faced with a situation where the crime scene may involve merely two computers but may span across half the globe.

The criminal in cyber crime does not leave latent fingerprints, footprints, or traces of physiological fluids in the wake of his intrusion; but bits and bytes of electronic activity may prove to be far more valuable in tracing the mischief maker.

In this article we analyse a challenging question for today's digital forensic experts, cyber scientists, and cyber analysts.

Does Locard's Exchange Principle apply in Digital Forensics?

The dramatic increase in cyber crime and the repeated cyber intrusions into critical infrastructure demonstrates the need for improved security. We believe that addressing the question of whether or not 'Locard's Exchange Principle' applies to digital forensics has the potential to guide or limit the scientific search for digital evidence.

"Every contact leaves a trace…" is the common citation of Locard's Exchange Principle in several publications. Essentially Locard's Exchange Principle may be applied to crime scenes in which the perpetrator(s) of a crime comes into contact with the scene of crime. The perpetrator(s) will both bring something into the scene, and leave with something from the scene. In the cyber world, the perpetrator may or may not come in physical contact with the crime scene, thus, this brings a new dimension to survey of crime scene.

The field of digital forensics can be strictly defined as "The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation." Furthermore, digital evidence is understood to be information stored or transmitted in binary form that may be relied on in court. However, digital forensics tools and techniques have also been used by cyber analysts and researchers to conduct media analysis, compile damage assessments, build timelines, and determine attribution.

According to the Department of Defense Cyber Crime Center's training program, cyber analysts require in-depth knowledge on how network intrusions occur, how various logs are created, what is electronic evidence, how electronic artifacts may be forensically gathered, how the data may be analyzed to produce comprehensive reports and link analysis charts.

Thus we hypothesize that Locard's Exchange Principle does apply to cyber crimes involving computer networks, such as: Identity theft, electronic bank fraud, or denial of service attacks, even if the perpetrator does not physically come in contact with the crime scene. Although the perpetrator may make virtual contact with the crime scene through the use of a proxy machine, we believe he will still "leave a trace" and digital evidence will exist.

When a crime is committed, fragmentary (or trace) evidence needs to be collected from the scene. The crime scene is visited and then sealed off by a team of investigating specialised police technicians. They both record video and take photographs of the crime scene, victim (if there is one), and any physical evidence. If necessary, they undertake a 'firearms and ballistics' examination. They also scout for shoe and tyre mark impressions, examine any vehicles, and check for fingerprints.

For the digital crimes of today, specialists need to examine a much more complex environment. Investigators need to image digital media of a multitude of types: magnetic, solid-state, or optical, for instance. Evidence might be persistent, such as that stored in non-volatile memories; or fleeting, such as over a transmission medium that has no storage. Evidence might also exist in media that is volatile but may be temporarily accessible, such as DRAM on a live system or "weakly" erased disk data. Furthermore, the investigation may involve more than the subject and host machine. It could also involve routers, servers, backup storage devices, and even printers, just to name a few.

More research is required in the cyber domain, especially in cloud computing, to identify and categorize where and how digital evidence can be found. End points such as mobile devices add complexity to this domain. Trace evidence can be found on servers, switches, routers, cell phones, etc. At least in the two examples described above, digital evidence can be found at the expansive scenes of the crime which includes numerous computers as well as peripheral devices.

A crime scene is a location where an illegal act took place and comprises of the area from which most of the physical evidence is retrieved by trained law enforcement personnel, crime scene investigators, or forensic scientists. Therefore, the Cyber Exchange Principle may find application. Looking beyond the primary crime scene for digital evidence, investigators must expand their search of the entire network. Frequently, it may happen that the computer crime investigator has to explore several scenes to find evidence. To aid this quest, standards and frameworks for digital forensics technologies are required now more than ever in our networked environment.

Some criminals have grown more cautious by hiding incriminating data through encryption techniques. However most criminals lack the knowledge or patience to implement encryption software on a continued-use basis. The minority of criminals who do encrypt their files may only use partial encryption. If only a few files on a hard drive are encrypted, investigators can analyze unencrypted copies found elsewhere on the device to find the information they are seeking. Furthermore, since most computer users tend to reuse passwords, investigators can locate passwords in more easily decipherable formats to gain access to protected files.

Conclusion

For computer forensics to progress, the law must keep pace with technological advancements. Clear and consistent legal procedures regarding computer system searches must be developed so that police and investigators can be properly trained. An International Code of Ethics for Cyber Crime and Cyber Terrorism should also be established to develop protocols for "obtaining and preserving evidence, maintaining the chain of custody of that evidence across borders," and "clearing up any difference in language issues." Following these measures may be the first steps to resolving the technological and legal limitations afflicting computer forensics. Interpol, the International Criminal Police Organization, has developed a Computer Crime Manual with "training courses" and a "rapid information exchange system" that serves as a foundation for international cooperation . Lastly, the criminal abuse of technology can be limited by equipping the police department with state-of-the-art training and equipment for forensic analysis. Only then will the world be safely prepared to face the future of technology. As one author predicts, "The next world war will be fought with bits and bytes, not bullets and bombs" .

NERVE CRACK SERVER

Mr. Sachin V

DFI - Digital forensic investigator

National Technical Committee Member - National Cyber Defence Research Centre.

What is CyberSecurity?

CyberSecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity.

What is a Web Server?

A Web Server is an information technology that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web. The term can refer either to the entire computer system, an appliance, or specifically to the software that accepts and supervises the HTTP requests.

What is Web Security?

Web application Security is a branch of Information Security that deals specifically with security of websites, web applications and webservices. At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems.

The Nerve Cracker (Streakersa.k.a Hackers)

Website security is more important than ever. Web Servers, which host the data and other content available to people on the Internet, are often the most targeted and attacked components of a company's network. Cyber criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online. As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are great: loss of revenues, damage to credibility, legal liability and loss of customer trust.

Call of Modern Era

Although securing a web server can be a daunting operation and requires specialist expertise, it is not an impossible task. Long hours of research and an overdose of coffee and take away food, can save you from long nights at the office, headaches and data breaches in the future. Irrelevant of what web server software and operating system you are running, an out of the box configuration is usually insecure. Therefore one must take some necessary steps in order to increase web server security.

Be a Rebel

Carefully plan and address the security aspects of the deployment of a public web server. Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Businesses are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support web

server administrators in making the inevitable tradeoff decisions between usability, performance and risk. Businesses also need to consider the human resource requirements for the deployment and continued operation of the web server and supporting infrastructure. The following points in a deployment plan:

- Types of personnel required -- for example, system and web server administrators, webmasters, network administrators and information systems security personnel.
- Skills and training required by assigned personnel.
- Individual (i.e., the level of effort required of specific personnel types) and collective staffing (i.e., overall level of effort) requirements.

Implement appropriate security management practices and controls when maintaining and operating a secure web server.

Appropriate management practices are essential to operating and maintaining a secure web server. Security practices include the identification of your company's information system assets and the development, documentation and implementation of policies, and guidelines to help ensure the confidentiality, integrity and availability of information system resources. The following practices and controls are recommended:

- A business-wide information system security policy.
- Server configuration and change control and management.
- Risk assessment and management.
- Standardized software configurations that satisfy the information system security policy.
- Security awareness and training.
- Contingency planning, continuity of operations and disaster recovery planning.
- Certification and accreditation.

Remove Unnecessary Services

Default operating system installations and configurations, are not secure. In a typical default installation, many network services which won't be used in a web server configuration are installed, such as remote registry services, print server service, RAS etc. The more services running on an operating system, the more ports will be left open, thus leaving more open doors for malicious users to abuse. Switch off all unnecessary services and disable them, so next time the server is rebooted, they are not started automatically. Switching off unnecessary services will also give an extra boost to your server performances, by freeing some hardware resources.

Remote access

Although nowadays it is not practical, when possible, server administrators should login to web servers locally. If remote access is needed, one must make sure that the remote connection is secured properly, by using tunneling and encryption protocols. Using security tokens and other single sign on equipment and software, is a very good security practice. Remote access should also be restricted to a specific number of IP's and to specific accounts only. It is also very important not to use public computers or public networks to access corporate servers remotely, such as in internet café's or public wireless networks.

Separate Development / Testing / Production Environment

Since it is easier and faster for a developer to develop a newer version of a web application on a production server, it is quite common that development and testing of web applications are done directly on the production servers itself. It is a common occurrence on the internet to find newer versions of a specific website, or some content which should not be available to the public in directories such as /test/, /new/ or other similar sub directories. Because such web applications are in their early development stages, they tend to have a number of vulnerabilities, lack input validation and do not handle exceptions appropriately. Such applications could easily be discovered and exploited by a malicious user, by using free available tools on the internet. To ease more the development and testing of web applications, developers tend to develop specific internal applications that give them privileged access to the web application, databases and other web server resources, which a normal anonymous user would not have. Such applications usually do not have any kind of restriction, since they are just test applications accessed that should be accessed from the developers only. Unfortunately, if development and testing is done on a production server, such applications can easily be discovered from a malicious user, which could help him compromise and gain access on the production server. Ideally, development and testing of web applications should always be done on servers isolated from the internet, and should never use or connect to real life data and databases.

Web Application Content and Server-Side Scripting

The web application or website files and scripts should always be on a separate partition or drive other than that of the operating system, logs and any other system files. Through experience we've learnt that hackers who gained access to the web root directory, were able to exploit other vulnerabilities, and were able to go a step further and escalate their privileges to gain access to the data on the whole disc, including the operating system and other system files. From there onwards, the malicious users have access to execute any operating system command, resulting in complete control of the web server.

Permissions and Privileges

File and network services permissions play a vital role in web server security. If a web server engine is compromised via network service software, the malicious user can use the account on which the network service is running to carry out tasks, such as execute specific files. Therefore it is very important to always assign the least privileges needed for a specific network service to run, such as web server software. It is also very important to assign minimum privileges to the anonymous user which is needed to access the website, web application files and also backend data and databases.

Install All Security Patches On Time

Although having fully patched software does not necessarily mean your server is fully secure, it is still very important to update your operating system and any other software running on it with the latest security patches. Up until this day, hacking incidents still occur because hackers took advantage and exploited un-patched servers and software.

Monitor and audit the server

All the logs present in a web server, should ideally be stored in a segregated area. All network services logs, website access logs, database server logs (e.g. Microsoft SQL Server, MySQL, Oracle)

and operating system logs should be monitored and checked frequently. One should always be on the lookout for strange log entries. Log files tend to give all the information about an attempt of an attack, and even of a successful attack, but most of the times these are ignored. If one notices strange activity from the logs, this should immediately be escalated so the issue can be investigated to see what is happening.

User accounts

Unused default user accounts created during an operating system install should be disabled. There is also a long list of software that when installed, user accounts are created on the operating system. Such accounts should also be checked properly and permissions need to be changed required. The built in administrator account should be renamed and is not to be used, same for the root user on a linux /unix installation. Every administrator accessing the web server should have his own user account, with the correct privileges needed. It is also a good security practice not to share each other's user accounts.

Remove all unused modules and application extensions

A default Apache installation has a number of pre-defined modules enabled, which in a typical web server scenario are not used, unless they are specifically needed. Turn off such modules to prevent targeted attacks against such modules.

The same applies for Microsoft's web server; Internet Information Services. By default, IIS is configured to serve a large number of application types, e.g. ASP, ASP.NET and more. The list of application extensions should only contain a list of extensions the website or web application will be using. Every application extension should also be restricted to use specific HTTP verbs only, where possible.

Use security tools provided with web server software

Microsoft released a number of tools to help administrator's secure IIS web server installations, such as URL scan. There is also a module called mod_security for Apache. Although configuring such tools is a tedious process and can be time consuming, especially with custom web applications, they do add an extra bit of security and peace of mind.

Stay informed

Nowadays, information and tips on the software and operating system being used can be found freely on the internet. It is very important to stay informed and learn about new attacks and tools, by reading security related magazines and subscribing to newsletters, forums or any other type of community.

Use Scanners

Scanners are handy tools that help you automate and ease the process of securing a web server and web applications.

Be a Vigilante

Maintaining a secure web server requires constant effort, resources and vigilance. Securely administering a web server on a daily basis is essential.

SECURITY ESSENTIALS IN INDIA'S MOBILE PAYMENTS ECOSYSTEM

Mr. Praveen J Vackayil

Information Security Consultant, Auditor, Trainer and Writer

Research Scholar, National Cyber Defence Research Centre

The Indian payments ecosystem has been subject to a sea change over the past few years. While debit and credit cards have found immense adoption particularly in Tier 1 and 2 cities in India, wehave been witnessing the rise of mobile as a key component inconducting financial transactions across India.

Smartphone adoption has grown phenomenally over the last 5 years in India. Low cost phones, popular social and messaging apps and the ever increasing proliferation of mobile network coverage have fostered a massive transformation in India's digital landscape. Riding this wave have been some game-changing developments in the payments sector.

As India embraces a mobile payments revolution, financial data such as card numbers, ATM PINs, CVV numbers and internet banking passwords continue to be one of the top targets of hackers across the world. This article aims to examine the foundational role that information security must play within these evolving technologies. We will review three mobile payment solutions that have demonstratedstrong potential to transform India's payments ecosystem. We will, thereafter, identify the basic information security parameters that must be addressed by these technologies to support our endeavor towards "Digital India" being a "Secure India".

Mobile Wallets

The concept of a mobile wallet is simple. The user's smartphone acts as a wallet – a single platform over which to perform phone recharges, bill payments, ticket bookings, etc. The user creates a new account with a mobile wallet and then credits money into it via card, net banking or IMPS. The topped-up amount can be spent, thereafter, on various online transactions. Since these transactions canbe conducted on their respective websites instead, the value propositionof themobile wallet is its capability to centralize and offer a singular user experience for different kinds of payments.

Mobile POS

Anyone with a credit/debit card has likely used a POS terminal – those ubiquitous blue devices, neatly cabled at check-out counters. The user swipes/inserts their card into the device and proceeds to punch in a PIN. Two-factor authentication at work. Today, Mobile POS is taking transaction portability to a whole new level. The concept involves two main devices – a smartphone with an active internet connection and a card reader with a PIN pad. The phone and the card reader are paired with each other via Bluetooth or USB. A supporting app is installed on the phone. With mPOS, businesses can take transactions to their customers' locations. For instance, a fixed

line internet service provider will need to visit his customers at their homes/offices to set up the connection and collect fees. An insurance agent will visit his customers at their homes and accept card payments towards policies. mPOS has the potential to take cashless transactions to India's remote areas as long as there is a 2G or 3G coverage in the region. As India marches towards a digital ecosystem, mobile POS terminals can empower even our neighbourhood vendors who peddle goods on mobile/hand-drawn carts.

Card-less NFC Payments

Near Frequency Communication allows data exchange between two devices placed next to each other. The technology has been around for quite a while, and we are bound to have seen it marketed as one of the features of popularsmartphones.

NFC is similar to Bluetooth, but a lot less power intensive. It is also easier to work with since, unlike Bluetooth, NFC does not require devices to pair with each other before data exchange. Banks like SBI and ICICI are already issuing NFC enabled debit and credit cards in India. Called contactless payment cards, users need only wave these cards against NFC enabled touch pointsfor making payments.

Card-less NFC payment, however, takes this convenience to the next level. In this technology, the user's smartphone replaces their card. An NFC enabled phone with a supporting app installed on it is used to make payments. The user has the ability to link multiple credit and debit cards with the app. Card-less BFC payments are yet to take off in a big way in India, but there, certainly is huge potential for growth. Roadblocks include the lack of a strong network of NFC enabled touch points, users' adoption of the technology, etc. currently exist.

Data Security in Mobile Payment Technologies

When it comes to new technologies, the prerogative for manufacturers is to get a saleable product up on the market in the shortest time possible. Product functionality is the focal point, and multiple version upgrades and product releases may be required before functionality is perfected. This being the case, security - usually regarded as anantagonist to functionality, may take a backseat. Let us identify the security essentials that must be applied on the aforementioned mobile backed payment technologies. The three fundamental components identified in each of the above technologies are:

- The smartphone itself
- The payment application installed on the phone
- The mobile POS/card reader device

The following section discusses the fundamental security requirements for each of the above components.

The Smartphone

The most important component of any mobile payment technology is of course, the phone itself. So complex and chaotic is India's smartphone market that defining a baseline set of security

controls for mobile phones can be a daunting task. Hardware variations regardless, India's prevailing software platforms have continued to remain more or less consistent – i.e., Android, IOS and Windows. Some basic security essentials must be implemented on the phone. Implementation methodology will vary depending on the phone model and its OS.

1. The phone must be a registered device with a valid IMEI number. Mobile POS organizations must ensure they have consistent access to the location and custody of each phone.
2. Measures must be in place to prevent and detect unauthorized access (both physical and logical) to the device.
3. Ideally, payment data must never be stored on the phone's internal storage or SD card. If, however, this is inevitable,
4. the phone's internal storage must be encrypted with suitable key strength
5. other apps installed on the phone must not have access to payment data
6. The phone must support a remote wipe in case it is lost or stolen
7. The phone's OS must be updated, in order to ensure protection against newly identified vulnerabilities.
8. An active and updated anti-virus must be installed on the phone.
9. The phone must be secured against man in the middle attacks.
10. The device must not be rooted, since this will empower its custodian to misuse it.
11. A defined mechanism to dispose of the phone at end of life must be in place.It must be ensured that sensitive data stored on the phone is irretrievable post device disposal.

The Payment Application

Each payment application has a unique functional and business logic. Coding standards followed while developing the application are also bound to variations depending on the application vendor. Nevertheless, security essentials that apply to mobile payment apps are fundamentally consistent.

1. Information security must be inherent in the payment application code. Adherence to application security fundamentals, such as OWASP Top 10, SANS Top 25 must be ensured and verified.
2. All instances of payment data storage and transmission must adhere to strong encryption techniques.
3. Code review continues to retain its relevance. It is absolutely vital that every line of code be reviewed by a peer/lead for correct business logic and adherence to coding best practices. Adherence to relevant secure coding guidelines must also be verified as part of the code review phase.
4. The application must be subject to periodic penetration tests.

5. Application logs must be generated, reviewed and retained for a suitably long duration. These must be available both at the client and at the server level.
6. Users' authentication and authorization levels must be clearly defined and implemented. Due consideration to two-factor authentication must be given where relevant. Users' passwords must be securely managed.
7. The underlying server and network infrastructure must be configured with strict compliance to baseline security standards.

The Card Reader

The Card Reader, an integral component of the mobile POS setup, is our next point of focus. If compromised, it would be possible to retrieve customers' card numbers and PINs from the POS device. It has been demonstrated that significant functionality changes can be imposed on hacked card readers. The security fundamentals for a traditional POS terminal will also apply to the mobile POS card reader device.

Point to Point Encryption:

Point to point encryption, or P2PE in common parlance, encrypts card data right at the point the card is swiped – namely at the mobile POS card reader. The encrypted card number is transmitted to an approved P2PE solution provider. P2PE enables a merchant to reduce their management overhead in terms of exposure to clear-text payment information.

Use of a Hardware Security Module (HSM):

An HSM is a physical device that isolates sensitive data handled by the mobile POS from the keys that actually encrypt it. Not all mobile POS vendors actually use an HSM, which means data encrypting keys (DEK) reside on the internal memory ofthe POS device itself. If compromised, retrieving the DEK and decrypting data pertaining to users' PINs, card numbers, CVV, etc. would not be very difficult. Use of an HSM helps to resolve this issue to a great extent.

A good HSM will be issued by a reputed vendor with a well-organized support network. The HSM must be configured for the secure and isolated management of all cryptographic keys pertaining to the mPOS.

Conclusion

Mobile is proving to be a crucial catalyst in Digital India's march towards a cashless economy. Mobile based payment technologies present exciting opportunities, and organizations are already tapping into them. However, an information security focus needs to be rooted right in the conception stages of these technologies. Developing a technology and then pursuing security compliance as an add-on is not the right approach. Security essentials must be builtright on the product drawing board. Security consciousness must be etched into the people interacting with these technologies, i.e. from the concept conceivers to the product developers, all the way through to the product consumers. The article explored the foundational role of information security in these technologies.