NATIONAL CYBER CRIME REFERENCE HANDBOOK

III Edition

NATIONAL CYBER SAFETY & SECURITY STANDARDS

(A Self Governed Body)

V.3.0

NATIONAL CYBER CRIME REFERENCE HANDBOOK

III Edition

▶▶ A Mandatory Disclosure

An Initiative by

राष्ट्रीय साइबर सुरक्षा और सुरक्षा मानकों
National Cyber Safety and
Security Standards

Institutional Members

Ministry of Defence
Ministry of Electronics and Information Technology
Ministry of Home Affairs
(Government of India)

New Delhi
Tamil Nadu
Andhra Pradesh
Madhya Pradesh
Maharashtra
Himachal Pradesh

All India Council for
Technical Education

Published by the **Director - General**
Publication Division
National Cyber Safety and Security Standards
(A Self Governed Body)

No. 69, Regal Building, Connaught Place,
New Delhi - 110001 **Tel:** 011- 30010144

Southern Regional Office:
Unit No. 37, 3rd Floor, Block 1, SIDCO Electronics Complex,
Thiru-Vi-Ka Industrial Estate, Guindy, Chennai 600032
Phone : 044 – 22502488

Fax : +91- 84688 65111
Email : c-defence@ncdrc.res.in
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

राष्ट्रीय साइबर सुरक्षा और सुरक्षा मानकों
National Cyber Safety and
Security Standards

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 III Edition of National Cyber Crime Reference Handbook.

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 healthmonitoring 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.

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. In this context, I convey best wishes to the National Cyber Safety and Security Standards Publishing Committee.

(Dr. S. Mohan)

न्याधीश ड़ॉ. टी एन वल्लीनायगम
Justice Dr. T. N. Vallinayagam
Judge - Lok Adalat & Former Judge - High Court of Madras & Karnataka
Chairman – National Cyber Defence Research Centre (NCDRC), 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 National Cyber Defence Resource 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 Crime 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)

राष्ट्रीय साइबर सुरक्षा और सुरक्षा मानकों
National Cyber Safety and
Security Standards

डॉ.एस.अमर प्रसाद रेड्डी
Dr. S. Amar Prasad Reddy
Director - General
National Cyber Safety and Security Standards

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.

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 Crime 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.

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)

राष्ट्रीय साइबर सुरक्षा और सुरक्षा मानकों
National Cyber Safety and
Security Standards

ई.खलिएराज
Shri. E. Khalieraaj
Addl. Director – General,
National Cyber Safety and Security Standards.

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 personal information, virus imitation and cyber vandalism etc. Because of its persistent nature, it is regarded as a bigger national security threat than terrorism.

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.

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.

In this context, I extend my best wishes for the successful publication of 'National Cyber Crime Reference Hand Book III Edition'.

E. Khal

(E. Khalieraaj)

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. **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 "National Cyber Crime 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
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 III 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. **Justice (Retd.) P. Sathasivam**
Honourable Governor of Kerala

I am very glad to know that the National Cyber Safety and Security Standards intends topublish the second edition of 'National Cyber Crime 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
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 "NATIONAL CYBER CRIME 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

Shri. **Ananth Kumar**
Honourable Minister for Chemicals and Fertilizers, Parliamentary Affairs,
Government of India

I am happy to know that the National Cyber Safety and Security Standards is bringing out the National Cyber Crime 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.

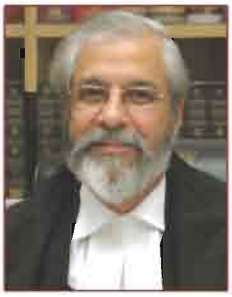
(Ananth Kumar)

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 Crime Reference Handbook 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 these books 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.

(R. Banumathi)

Honourable **Mr. Justice Madan Bhimarao Lokur**
Judge, Supreme Court of India, New Delhi.



The National Cyber Crime Reference Handbook is a boon for all lay persons, profes sionals 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 evenremotely 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.

The National Cyber Crime Reference Handbook which is going into its 3rd 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 Bhimarao Lokur)

Honourable **Mr. Justice A.M. Khanwilkar**
Judge, Supreme Court of India, New Delhi.

I am happy to learn that the "National Cyber Safety and Security Standards" is publish ing "National Cyber Crime 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 this handbook.

(A.M. Khanwilkar)

सत्यमेव जयते

General Bipin Rawat, UYSM, AVSM, YSM, SM, VSM
Chief of the Indian Army.

National Cyber Crime Reference Handbook is a great work undertaken by National Cyber Safety and Security Standards (NCSSS) to empower all the stakeholders of National Security and protect the interests of our great nation in the cyber domain.

(General Bipin Rawat)

सत्यमेव जयते

Admiral Sunil Lanba PVSM, AVSM, ADC
Chief of the Indian Navy.

Our increasing reliance on cyberspace and its rampant use for criminal activity can only be countered by adopting a holistic approach and concerted effort from all agencies that use the cyberspace. The Third Edition of the National Cyber Crime Reference Handbook is an effort towards advanced cyber protection methodologies and controlling procedures/tools to ensure that the cyberspace remains safe and conducive for overall growth and development.

My compliments to the National Cyber Safety and Security Standards team, those has drafted this book addressing important issues related to cyber security.

(Admiral Sunil Lanba)

सत्यमेव जयते

Padma Shri Dr. A. S. Kiran Kumar

Chairman, Indian Space Research Organisation (ISRO),
Department of Space, Government of India.

There is a need for developing basic infrastructure for controlling cyber security, which is a daunting problem. The need for basic infrastructure development for controlling the cyber security aspect is important. We have to bring in basic infrastructure for communication and cyber security networks and make available to the people who are governing it.

Technology and communication have brought the world closer and made interaction between people much easier but it also brings along huge amount of problems. The rate at which electronics is growing, cybercrime is also growing. In the context of cyber security, we really need to understand whether things have already gone beyond redemption or are there are ways and means by which we can protect ourselves.

I wish you all the best to National Cyber Safety and Security Standards.

(Dr. A. S. Kiran Kumar)

INDEX

CONTENTS

अध्याय
Chapter 1

Cyber Crime, History of Cyber Crimes and the Challenges of Fighting Cyber Crime

1.1. 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.

1.2. 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.

1.3. 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 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.

1.4. 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.

1.5. 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.

1.5.1 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
- 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.

1.6. 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.

1.6.1. 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.

1.6.2. General Challenges

1.6.2.1. 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.

1.6.2.2. 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.

1.6.2.3. 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.

1.6.2.4. 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.

1.6.2.5. 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.

1.6.2.6. 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.

1.6.2.7. 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 legis lation 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.

1.6.2.8. 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.

1.6.2.9. 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.

1.6.2.10. 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.

1.6.2.11 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 upto- 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.

1.6.2.12. 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.

1.6.2.13 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

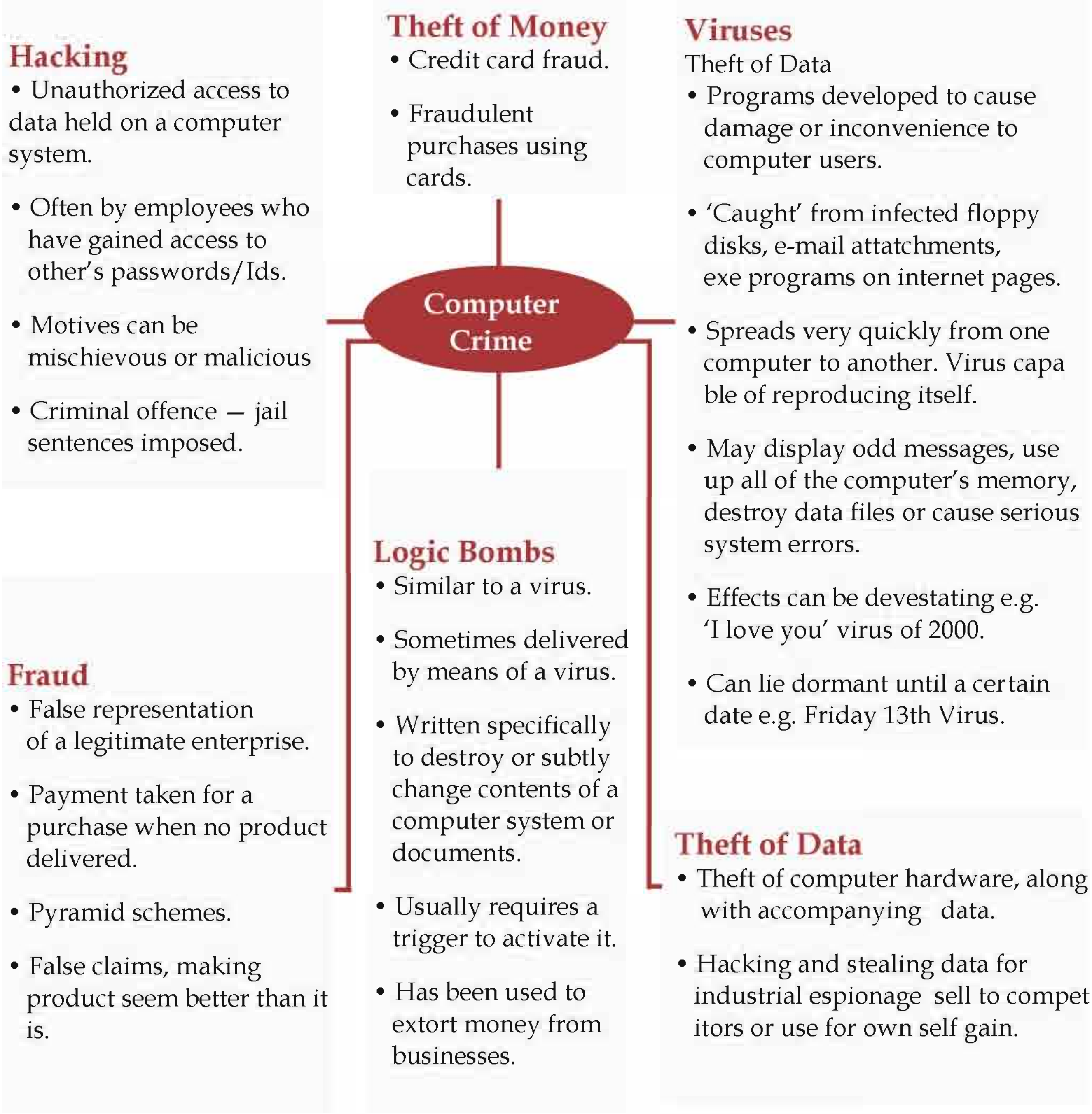
The investigation and prosecution of cybercrime presents a number of challenges for law enforcement agencies. It is vital not only to educate the people involved in the fight against cybercrime, but also to draft adequate and effective legislation. This section has reviewed key challenges to promoting cybersecurity and areas where existing instruments may prove insufficient and the implementation of special instruments may be necessary.

अध्याय 2
Chapter 2
Cyber Crime

2.1 General:

Crime Overview Computer Crime:

Computer crime: which is also variously referred to as cyber-crime, e-crime, high-tech crime, and electronic crime — can include many different types of offenses. If a computer or a network is the source, target, tool or place of the crime, it is considered as a type of computer crime. Other crimes that can be facilitated by a computer crime are fraud, theft, blackmail, forgery and embezzlement.



Computer Crime

Hacking
- Unauthorized access to data held on a computer system.
- Often by employees who have gained access to other's passwords/Ids.
- Motives can be mischievous or malicious
- Criminal offence — jail sentences imposed.

Theft of Money
- Credit card fraud.
- Fraudulent purchases using cards.

Viruses
Theft of Data
- Programs developed to cause damage or inconvenience to computer users.
- 'Caught' from infected floppy disks, e-mail attatchments, exe programs on internet pages.
- Spreads very quickly from one computer to another. Virus capa ble of reproducing itself.
- May display odd messages, use up all of the computer's memory, destroy data files or cause serious system errors.
- Effects can be devestating e.g. 'I love you' virus of 2000.
- Can lie dormant until a certain date e.g. Friday 13th Virus.

Fraud
- False representation of a legitimate enterprise.
- Payment taken for a purchase when no product delivered.
- Pyramid schemes.
- False claims, making product seem better than it is.

Logic Bombs
- Similar to a virus.
- Sometimes delivered by means of a virus.
- Written specifically to destroy or subtly change contents of a computer system or documents.
- Usually requires a trigger to activate it.
- Has been used to extort money from businesses.

Theft of Data
- Theft of computer hardware, along with accompanying data.
- Hacking and stealing data for industrial espionage sell to compet itors or use for own self gain.

Fig. Types of Computer Crime

Computer crimes are covered by both federal and state laws. Because of the nature of technology, including the use of the Internet, computer crimes often cross state lines and therefore involve federal laws and federal prosecution. They can be classified as two separate categories of crimes; one in which the target is the network or computer, and one in which crimes are executed or expedited by a computer. Due to the usage of the Internet for e-commerce, and the total dependence on technology of many businesses, computer crime is predicted to advance. As new technologies take hold, criminal elements will infiltrate the systems for their benefit.

2.2 Events — Chronology:

Ever since the Act came into being there were series of demands for bringing about changes that will make sure that the Act provided for curbing the menace of Cyber Crime, issues of data leakage and personal privacy also started making news. These demands for change were further strengthened by the BPO industry in India which had to produce credentials of data safety and privacy in India to bid for international projects which were being outsourced out of western countries. A major amendment was made to the Act with effect from 6 February 2003 consequent to the passage of a related legislation called Negotiable Instruments Amendment Act, 2002. The amendment to Negotiable Instruments Act, 2002 for the first time recognized a cheque in electronic form. These changes notwithstanding, Indian Government realizing the changing terrain of online interactions, formed an expert committee under Ministry of Information Technology to suggest amendments to Act to keep it relevant. Main reasons for looking into changes in the Act were,

a. Subject-matter being Information Technology which has an accelerated, pace of development;

b. Intensive approach employed in it as opposed to a general framework to regulate information technology.

The committee pointing out several lacunas in the enactment proposed amendments to it in the report it tendered to the ministry of information technology. The result was the Information Technology Amendment Bill, 2006 based on the report submitted by the expert committee.

During the same time, in order to provide for protection of data leakage and personal privacy a Personal Data Protection Bill was introduced in Rajya Sabha in 2006. This bill, however, remains to be passed. The Information Technology Act 2000 amendment Bill 2006 has since been passed by the Indian Parliament on December 23, 2008.

2.3 Meaning of Cyber Crimes:

Cyber Crimes are crimes committed in electronic mediums where mens rea is not a requirement. The Cambridge Dictionary defines Cyber Crimes as crimes committed with the use of computers or relate to computers especially through the internet.

The Cyber Crime is an unlawful act wherein computer is either a tool or a target or both.

Cyber Crime is a generic term, which refers to all criminal activities done using the medium of computers, internet cyberspace and the world wide. Cyber Crimes are crimes that occur in the digital place, which is the aggregation of the transaction space within each of the connected computers and the virtual spaces arising out of the connection. In short the Cyber Crimes can be defined as offences or contradictions under any law committed with the use of electronic documents.

2.4 What is Cyber Crime?

Cyber Crime is an amalgamation of two words: ‘cyber’ — related to internet or other electronic networks and ‘crime’ — a criminal activity. Literally, the word cyber according to Oxford Learners Dictionary means:

"Connected with electronic communication networks, especially the Internet."

The word cyber is generally misunderstood as the word only and wholly concerned with the web and internet however; it also includes other communication networks electronic networking devices e.g. cellular networks and devices, telephones and many other e-devices.

The word crime as defined by Merriam-Webster dictionary:

"An act or the commission of an act that is forbidden or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by that law Oxford dictionary also defines crime as: 'an act punishable by law´.

Cyber Crime contains all criminal offences, which are committed with the aid of communication devices in a network. This can be for example the Internet, the telephone line or the mobile network. It is also known as computer crime and is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy, Cyber Crime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. In his book named 'What is Cyber Crime?, the author Nagpal R. defined: "Unlawful acts wherein the computer is either a tool or target or both".

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, Cyber Crime was broken into two categories and defined thus:

a. Cyber Crime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber Crime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network; including such crimes as illegal pos session (and) offering or distributing information by means of a computer system or network.

Cyberspace is the most eminent place for E-commerce, entertainment, social networking, information and many more. But, due to the evil minded 'netizens' (a combo derived from net and citizens for the persons using internet) this technology is nowadays being manipulated to commit offences which we call Cyber Crime. Some of the examples of Cyber Crimes are hacking, spamming, stealing identities and privacy, fraud, viral and worm attacks, e-mail bombing, cyber torts, cyber terrorism, trafficking, pornography, etc These crimes in the cyberspace have been a pain in the head and hole in the pocket of other users since the early days. In the early centuries, only the only the developing countries and mostly the US had accepted computers and internet and were the early victims of the cyber villains. However, in the contemporary world, hardly a hamlet remains that had not been touched by Cyber Crime of one sort or another.

Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of Cyber Crime would be "unlawful acts wherein the computer is either a tool or a target or both". Defining Cyber Crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many Cyber Crimes, such as e-mail spoofing, cyber defamation etc

FIRST RECORDED Cyber Crime

- The first Cyber Crime ever recorded was In France during 1820.
- The person involved was Joseph-Marie Jacquard.
- He was a textile manufacturer, he made looms.
- He invented looms that can store designs.

2.5 Against Economy—Cyberspace, in Current World, has become the Place where Commerce and Money is Moving which is Very Luring for the Criminals:

The criminals armed with technological sophistication have found it much easier to carry their activities in cyber word. Some of these crimes are as follows :

2.5.1 Hacking:

The term 'computer hacking' traditionally describes the penetration of computer systems, which is not carried out with the aims of manipulation, sabotage, but for pleasure of overcoming the technical security measures. Hacking has now become a "basic offence" which is then used to commit acts of espionage, software piracy, sabotage, as well as computer fraud. Hacking is punishable under Sections 66 and 70 of Information Technology Act 2000 with punishment up to 10 years of imprisonment or `2 lakhs fine or both.

2.5.2 Malicious Programs:

Malicious programs such as Virus-Worms, Trojan Horses, Logic Bombs, Hoaxes etc intend to cause harm to its victims.

a) Virus: It is a program that searches out other program and infects them by embedding a copy of it in them "Section 13(c) of the Information Technology Act covers the area of introduction of viruses, etc and shall be liable to pay damages by way of compensation not exceeding `1 crore to the person so affected.

b) Worms: These are the programs that propagate itself over a network reproducing itself as it goes. Worm unlike virus does not require a medium to propagate itself and infect others.

c) Trojan: A Trojan horse program pretends to do one thing while actually doing something completely different. Trojans let a hacker access the victim's hard disk; and also perform many functions on his computer. In the past there have been many incidents, in India and abroad, where Trojans have been used to alter the information contained in hospital computers.

d) Logic bombs: Logic bombs, once detonated in a computer, makes the program to go into an infinite loop, crash the computer, delete data files, or some other damage to the computer or its data.

e) Hoax: It is false warning about existence of malicious program.

Spreading rate of Malware Samples in different domains is shown in fig.

2.5.3 Digital Forgery:

Digital technology facilitates perfect reproduction of documents. By using a computer, it is very easy to forge a document through printers and scanner by developing counterfeit currency, postal cards, revenue stamp, mark sheet, birth certificates etc Section 91 of Information Technology Act (read with second schedule) and amended provisions of IPC in relation to 'forgery' for the penal provisions of digital forgery.

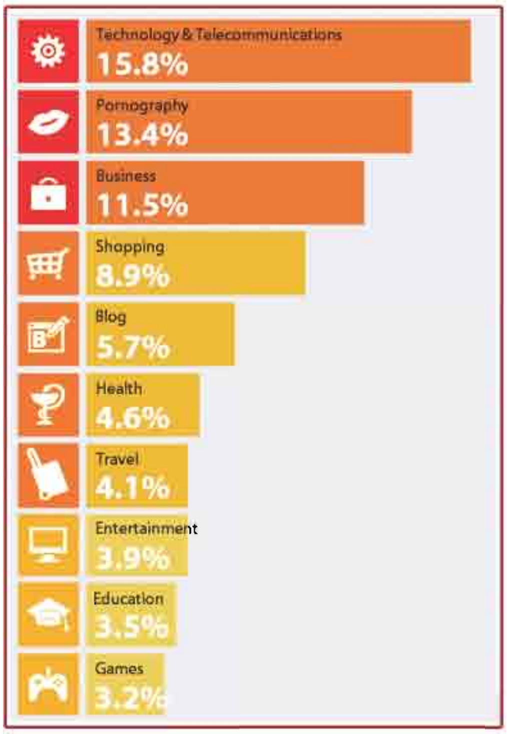


Fig. Spreading rate of malware samples in different domains

2.5.4 Piracy and Infringement of Intellectual Property Rights:

Accessible, sufficient and adequately funded arrangements for the protection of rights are crucial in any worthwhile intellectual property system. There is no point in establishing a detailed and comprehensive system for protecting intellectual property rights and disseminating information concerning them. If it is not possible for the right-owners to enforce their rights effectively in a world where expanding technologies have facilitated infringement of protected rights to a hither to unprecedented extent. They must be able to take action against infringers in order to prevent further infringement and recover the losses incurred from any actual infringement. They must also be able to call on the state authorities to deal with counterfeits.

All intellectual property systems need to be underpinned by a strong judicial system for dealing with both civil and criminal offences, staffed by an adequate number of judges with suitable background and experience. Intellectual property disputes are in the main matters to be decided under civil law and the judicial system should make every effort to deal with them not only fairly but also expeditiously. Without a proper system for both enforcing rights and also enabling the grant of rights to others to be resisted, an intellectual property system will have no value. Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. Piracy and Infringement of Intellectual Property Rights are one of the most critical crimes committed in cyberspace. Section 2(o) of the Copyright Act, 1957 affords copyright protection in India wherein the term literary work' includes computer programs, tables and compilations including computer databaseand criminal proceedings that could be started under Sections 63–70 of the Act.

2.6 Cyber Warfare:

Cyber warfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems — among many other possibilities. The cyber warfare has gained so much favour among the military strategists that most of the Armies world over have dedicated cyber warfare teams for defensive as well as offensive operations. Defence planners around the world are investing substantially in information warfare — means of disrupting the information technology infrastructure of defence systems.

2.7 Computer Related Crimes:

Over the past 20 years the technology of electronic data processing — the computer — has come to play a dominant role in business and government. It would be difficult to conceive of a person whose life is not in some way affected by the computer, for virtually everyone who has a bank account, engages in any kind of credit transaction, or has dealings with the government or any large organization is touched by it in some way. The computer is now an indispensable tool for banking, corporate records and various activities of government.

The following diagram demonstrates many different ways Cyber Criminals can make money by hacking.

But the very features of the technology that make it such a boon to society also increase its susceptibility to abuse. The absence of tangible printed records of credit transactions is testimony to the efficiency of the computer, yet it leaves the auditor without the accustomed "paper trail" for verifying accounts. A computer need not be manipulated at any particular place, but can be operated from a distance using telecommunications facilities. This too can increase the potential for abuse, for now a thief need not be near the site of the crime but can, from the relative safety of a computer terminal, acquire assets reduced to electronic impulses.

Computer Related Crimes Covered under IPC and Special Laws:

Offence	Sections
Sending threatening messages by email	Sec. 503, IPC
Sending defamatory messages by email	Sec. 499, IPC
Forgery of electronic records	Sec. 463, IPC
Bogus websites, cyber frauds	Sec. 420, IPC
Email spoofing	Sec. 463, IPC
Web-Jacking	Sec. 383, IPC
E-Mail Abuse	Sec. 500, IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

2.8 The Basic Problems Associated with Cyber Crimes:

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law anywhere in the world. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of Information Technology Act and amendments made to Indian Penal Code, problems associated with Cyber Crimes continue to persist.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyberspace the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under Section 16 of Cr PC and Section 2 of the IPC will have to give way to alternative method of dispute resolution.

2. Loss of evidence is a very common and expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

3. Cyber Army: There is also an imperative need to build a high technology crime and investigation infrastructure, with highly technical staff at the other end.

4. A law regulating the cyber-space, which India has done.

5. Though Section 75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

6. Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the PIL (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and bye-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalization. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation.

2.9 Legal Protection against Cyber Crime in India:

Cyber Crime cases have increased significantly in India. However, there is a general lack of awareness among public at large as well as police and judicial system regarding cyber law and Cyber Crimes.

As a result most of the Cyber Crimes are not reported at all. Even if some Cyber Crimes are reported, they are not investigated properly and this results in very few Cyber Crime convictions.

In most of the cases, lack of Cyber Crime conviction is the primary result of absence of proper legal assistance to prosecute Cyber Crimes. We have very few cyber law firms in India that are truly cyber law firms. Perry4Law is the best cyber law firm of India that is providing cyber law and other techno legal services.

In fact, the techno legal segment of Perry4Law known as Perry4Law's Techno Legal Base (PTLB) is managing the exclusive techno legal Cyber Crime investigation centre of India. The Cyber Crime investigation centre is playing a conclusive role in conducting Cyber Crime investigations in India and providing techno legal services to the victims of Cyber Crimes and cyber frauds.

With rapid digitalization of businesses and increasing cyber attacks. Organizations and Governments rightfully worry about the security of computer networks and infrastructures. A deeper and richer understanding of the principles and purposes; necessary and sufficient conditions for web attacks; and the patterns of origin and targets would help managers as well as national and international policy makers devise strategies to combat such crimes. The cyber laws of India are contained in the Information Technology Act 2000. The Act came into effect following the clearance of the Information Technology Bill, 2000 in May, 2000 by both the Houses of the Parliament. The Bill received the assent of the President of India in August, 2000 (Information Technology Act 2000). The Information Technology Act 2000 aims to provide the legal infrastructure for e-commerce in India. At this juncture, it is relevant to understand what the Information Technology Act 2000 offers and its various perspectives.

2.10 Various Online Frauds and Financial Crises:

During the recent financial crisis, no issue has aroused more passion than financial institution bailouts. The standard rationale for the bailouts has been one of the necessity and fear: federal regulatory agencies must have more authority in order to respond to the crisis, or else the public will face terrible consequences. But does this rationale hold up to close inspection?

The nation's federal financial regulators and the politicians claim to have saved the American economy. In truth they have done everything within their power to expand their own influence often far out of view from the public and media. Instead of openly explaining their actions, the bailout agencies have attempted to prevent the public from reviewing their decision-making, often at tremendous cost to taxpayers.

Identity theft and frauds are crimes where someone wrongfully obtains and uses another's personal data in a way that involves fraud or deception for financial gain. To avoid these typesof offences giving of personal details to others should be avoided.

Another category of money related crime is credit card fraud. Here again somebody's credit card may be wrongfully used for one's personal gain. This risk has grown multifold as people do purchase online through their credit cards. The websites offering product take all the details of the credit card and store information on the server. So anybody who can access the server can use the credit card details for financial gains.

Apart from this, financial frauds includes market manipulation scheme, issuance of false stock, online gambling, sale of illegal articles.

The word fraud has not been defined in the Indian Penal Code. However, Section 25 of IPC defines the word 'fraudulently' as, there can be no-fraud unless there is an intention to defraud. Wherever the words fraud, intent to defraud or fraudulently occur in the definition of a crime under the IPC, two elements at least are essential to the commission of that crime.

1. Deceit or an intention to deceive, and
2. Either actual injury or possible injury or an intent to expose some person to actual or possible injury.

Both are essential requisites of fraud i.e. deceit or intention to deceive and actual or possible injury to an individual are present in all such seams, intended to gain advantage at the risk of loss to others.

2.11 Cyber Crime Preventive Methods:

Computer is now emerging as a new crime tool. The growing menace from crimes committed against computers, or against information on computers, is commanding the attention of various nations. The phenomenal growth of computers and Internet services has engendered the problem of Cyber Crime proliferation on the account of investigation difficulties and lack of strong evidences. Further, existing laws and preventive measures are not effective to curb such crimes. This lack of legal protection calls for businesses and governments to adopt solid technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. This paper discusses ramifications of Cyber Crime including discussion on current and emerging forms of computer related illegalities and tools and techniques used in such crimes. In addition, some preventive measures are suggested that can be taken by corporate houses and law enforcement agencies including framing of new laws and subsequent issues that arise.

Computer crime is an expanding division of criminal activity. Also known as Cyber Crime, cases include intrusion/infiltration, financial and identity theft, espionage, and cyber warfare. Computer crime may also include child pornography and copyright infringements, as well as any other illegal activity that was performed with assistance of a computer.

Not only the law is for people but people are also for the law. Prevention is better than cure and so the common people must take some preventive measures to be out of the evil sight of Cyber Crimes. First comes the 'VIGILANCE.' Without knowing the enemy, one cannot combat it. Thus, people require to know and being vigilant about the cyberspace and the dark fissure of crimes committed there within. The netizens must be updated with the information regarding cyber worlds and the techniques to use them. Moreover, the authorities too should be dwelled with the knowledge regarding these spheres of internet so that they can manipulate the law to outcome the problems of cyberspace. Cyber insurance should also be done for the companies so that their loss may be compensated.

Thousands of Cyber Crimes plague the country every year. Yet, not a single Indian Insurance company offers a comprehensive anti-Cyber Crime policy for the corporate sector. "In India there are few takers for Cyber Crime insurance primarily because of the high cost vis-a-vis their exposure. These policies are of a high value and, on request from a few brokers, are customised for banks. We sell one or two policies a year," an HDFC Ergo official explained. The anti-virus software must be updated regularly and firewalls arid spywares must be installed in each and every computer systems. Information should not be provided to each and every sites blindly. One should only rely on the sites he/she trusts. An eye on the children by the parents could serve as an anti-pornography campaign.

This will be good both for the children as well as for parents to eradicate Cyber Crime. Backup must be kept for the important data so that viral contamination cannot chew up any important information. Another milestone in ensuring the safety and security of the people through advanced means of Information Technology was added with the launching of the Cyber Crime investigation cell by the Punjab Governor and Administrator, Union Territory, Chandigarh, Gen. (Retd.) S.F. Rodrigues, at an impressive function in police station. Set up by the Chandigarh Police with the participation of NASSCOM and Punjab Engineering College, Chandigarh this Cell will help in checking computer related crimes, such as unauthorized access to a computer, online banking fraud, "phishing", sale of illegal articles like wildlife products, drugs etc, pornography, online gambling, e-mail spoofing and cyber stalking.

New law should be organized which wholly deals with the evils of cyber-crime covering all the spheres of cyberspace and the officers must be appointed having valid qualification efficient fully in cyberspace and crimes in it. Following some of these ways, one can be in safe hands in the world of cyberspace and the Cyber Crimes can be prevented more efficiently.

2.12 Preventive Steps for Individuals:

2.12.1 Children:

Children should not give identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not share photographs with anyone on the net without first checking or informing parents, guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a faceto- face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

2.12.2 Parents:

Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol.

There is also a software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site their children have visited. Parents can use this software to keep track of the type of activities of children.

2.12.3 General Information:

Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these:

- Try not to panic.
- If you feel any immediate physical danger contact your local police.

  Avoid getting into huge arguments online during chat and discussions with other users.
- Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.
- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as others.
- Do not share personal information in public space online; do not give it to strangers.

- Be extremely cautious about meeting online introduced person. If you choose to meet do so in a public place along with a friend.

- If an online situation becomes hostile, log off and if a situation places you in fear, contact the local police.

- Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

2.13 Preventive Steps for Organizations and Government:

Computer is now emerging as a new crime tool. The growing menace from crimes committed-against computers, or against information on computers, is commanding the attention of various nations. The phenomenal growth of computers and Internet services has engendered the problem of Cyber Crime proliferation on the account of investigation difficulties and lack of strong videnc-es. Further, existing laws and preventive measures are not effective to curb such crimes. This lack of legal protection calls for businesses and governments to adopt solid technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. This paper discusses ramifications of Cyber Crime including discussion on current and emerging forms of computer related illegalities and tools and techniques used in such crimes. In addition, some preventive measures are suggested that can be taken by corporate houses and law enforcement agencies including framing of new laws and subsequent issues that arise.

Computer crime is an expanding division of criminal activity. Also known as Cyber Crime, cases include intrusion/infiltration, financial and identity theft, espionage, and cyber warfare. Computer crime may also include child pornography and copyright infringements, as well as any other illegal activity that was performed with the assistance of a computer.

2.13.1 Physical Security:

Overview:

If an intruder gets physical access to a computer, they can easily gain access to the information stored on the computer. Methods range from simply tucking the computer under their arm and walking off with it to collect the data at leisure, using a ´rescue disk´ or some other method of starting the computer with no passwords, removing the hard drive and starting it on their own computer, with full access to the information stored on the drive.

Most operating systems have some method of starting the computer with no passwords this is intentional, because most organizations will lose or forget a critical password at some time. This can only be done when a person is physically present at the computer, however — the operating system designers rely on the user being aware of this fact, and securing the computer room. There are methods, in most operating systems, of disabling the 'no password' start — if you choose to implement them, be extremely careful and document the passwords well. But secure the copy of the passwords. Physical security is the most sensitive component, as prevention from Cyber Crime Computer network should be protected from the access of unauthorized persons.

2.13.2 Access Control:

Simply defined, the term ˝access control˝ describes any technique used to control passage into or out of any area. The standard lock that uses a brass key may be thought of as a simple form of an ˝access control system˝.

Over the years, access control systems have become more and more sophisticated. Today, the term ˝access control system˝ most often refers to a computer-based, electronic card access control system. The electronic card access control system uses a special "access card", rather than a brass key, to permit access into the secured area.

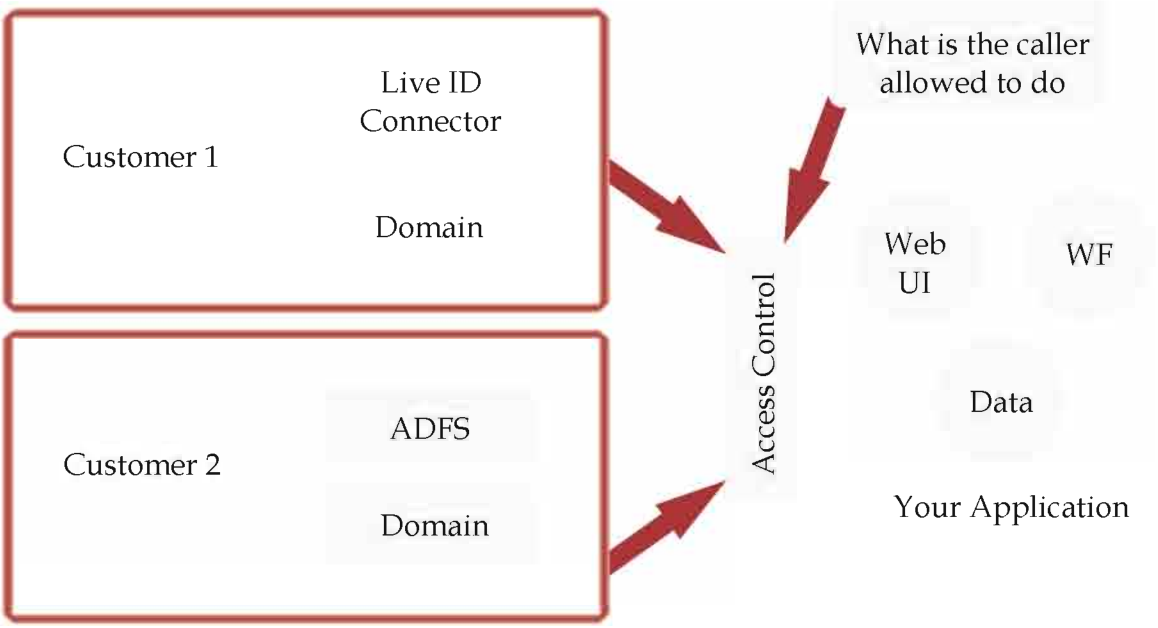


Fig. Access Control

Access control systems are most commonly used to control entry into exterior doors of buildings. Access control systems may also be used to control access into certain areas located within the interior of buildings.

The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people.

Few employers allow all their employees to access all facilities every time. That's why more and more are using electronic access control to limit employees' access to their facilities. At a minimum, an electronic access control system can be used to allow only employees into a building after hours, and provide excellent documentation of when and where employees enter and exit. Access control is the only technology that proactively attempts to keep unauthorized individuals out of a building or areas within a facility, and is a perfect complement to video surveillance, burglar and fire systems in a comprehensive security solution proposal.

Access Control system is generally implemented using firewalls, which provide a Centralized point from where to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

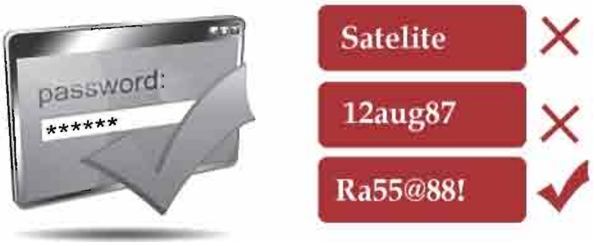


Fig. Password Examples

A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user. Typically, users of a multiuser or securely protected single-user system claim a unique name (often called a user ID) that can be generally known. In order to verify that someone entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user. A password is typically somewhere between 4 and 16 characters, depending on how the computer system is setup. When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

Proof of identity is an essential component to identify intruders. The use of passwords in the most common security for network system includes servers, routers and firewalls. Mostly all the systems are programd to ask for username and password for access to computer system. This provides the verification of user. Password should be changed with regular interval of time andit should be alpha numeric and should be difficult to judge.

2.13.3 Finding the Holes in Network:

Exploiters on the Internet have caused billions of dollars in damages. These exploiters are intelligent cyber terrorists, criminals and hackers who have a plethora of tools available in their war chests ranging from spyware, root kits, Trojans, viruses, worms, bots, and zombies to various other blended threats.

Exploits can be grown and harvested the same day a security hole is announced — in socalled "zero-day attacks" — so they are getting much harder to stop. Open source malware code, freely available on the Internet, is enabling this phenomenon and cannot be reversed. Although the number and types of exploits "in the wild" continues to rise exponentially, there are fewer than a dozen core methodologies used for their execution and proliferation. Most exploits can be removed, but some exist indefinitely and can only be destroyed or removed by loss of data — you've probably heard of these "root kits." Most exploits will re-infect a host if a security hole, also known as the Common Vulnerability and Exposure (CVE), is not removed.

System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

2.13.4 Using Network Scanning Programs:

Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping, returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses.

Scanning is one of the three components of intelligence gathering for an attacker. In the footprinting phase, the attacker creates a profile of the target organization, with information such as its domain name system (DNS) and e-mail servers, and its IP address range. Most of this information is available online. In the scanning phase, the attacker finds information about the specific IP addresses that can be accessed over the Internet, their operating systems, the system architecture, and the services running on each computer. In the enumeration phase, the attacker gathers information such as network user and group names, routing tables, and Simple Network Management Protocol (SNMP) data.

There is a security administration’s tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities including bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.

2.13.5 Using Intrusion Alert Programs:

This tool is designed to facilitate the interactive analysis of alerts reported by Intrusion Detection System (IDS). It was started as a prototype system and was developed to validate who method to correlate intrusion alerts based on the prerequisites and consequences of known attacks (See our paper in CCS '02). Now it has been serving as a platform to test and validate our techniques for intrusion analysis. who would also like to transform our techniques into a practical tool that helps intrusion analysis in real-world applications.

TIAA is written in Java. The current version is an offline tool interacting with DBMS.

As it is important to identify and close existing security holes, you also need to put some watch dogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behaviour on network is caught immediately.

2.13.6 Using Encryption:

Encryption is a process which is applied to text messages or other important data, and alters it to make it humanly unreadable except by someone who knows how to decrypt it. The complexity of the algorithms used means that a strongly encrypted message might require thousands of years of processing by very fast computers to break the encryption.

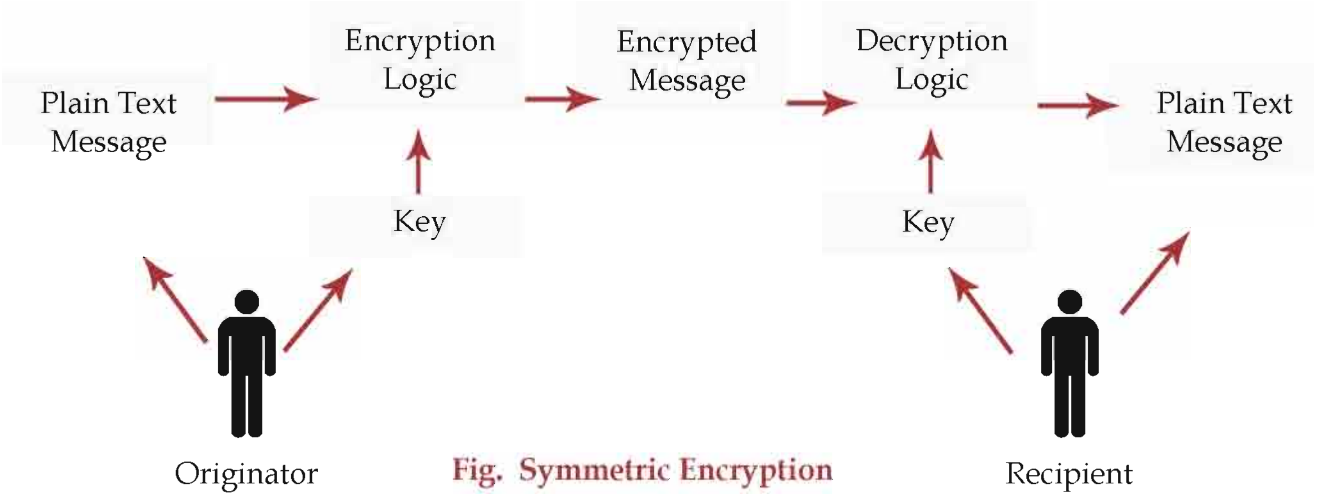


Fig. Symmetric Encryption

The most popular use of encryption is for securing web servers that are accessed by the https protocol not http so that data such as credit cards can be sent safely over the internet. Encryption is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a creditcard purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher — that is, the harder it is for unauthorized people to break it the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to anyone but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will ecome public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

2.14 Problems Related with Cyber Crime:

2.14.1 Jurisdiction:

Power or right of a legal or political agency to exercise its authority over a person, subject matter, or territory. Jurisdiction over a person relates to the authority to try him or her as a defendant. Jurisdiction over a subject matter relates to authority derived from the country's constitution or laws to consider a particular case. Jurisdiction over a territory relates to the geographic area over which a court has the authority to decide cases. Concurrent jurisdiction exist where two courts have simultaneous responsibility for the same case.

Cyber attack have benefited from jurisdictional arbitrage. Because of the sophistication and newness, jurisdictional arbitrage is higher for Cyber Crimes compared to other conventional crimes. Only the US and the UK have laws that come even close to adequate in defining Cyber Crimes and levelling penalties. The lack of a strong rule of law is associated with origination of more cyber attacks. A strong rule of law is characterised by effective punishment of transgressors and regulatory sanctions for defectors and thus enhances the ability to successfully litigate fraudulent online dealings. There are international differences in terms of laws to minimise vulnerability to cyber attacks.

Organised Cyber Crimes are often initiated from countries that have few or no laws directed against Cyber Crimes and little capacity to enforce existing laws. For instance, when a Philippino hacker launched the “Love Letter” virus in 2000, estimated loss of damage in the US was in the range of $4–15 billion. But the US Government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had not enacted laws that prohibited such crimes. Although many countries in world have enacted Cyber Crime.

A nation’s laws also determine what is considered to be a Cyber Crime. National laws also facilitate or restrict law enforcement agencies ability to act on potential ingredients related to Cyber Crimes. In the US, for instance, the FBI considered militant Islamist websites lawful as the First Amendment permits even the most hateful Internet speech, as long as they don’t directly incite violence or raise money. On the contrary, in Singapore in the Cyber conflict with the Think Centre (Asia), an NGO, the State authorities reportedly employed surveillance and intimidation. There are reports that the Government of Singapore actively scans and monitors e-mails and there are in stances of breaking into a number of computers used by various groups and individuals.

Law enforcement agencies responses also differ across types of Cyber Crimes. Experts argue that law enforcement officials in some countries don’t take major actions against hackers attacking international websites and are more interested in protecting national security.

2.14.2 Motivation:

Internal and external factors stimulate desire and energy in people to be continually interested and committed to a job, role or subject, or to make an effort to attain a goal.

Motivation results from the interaction of both conscious and unconscious factors such as the (1) intensity of desire or need, (2) incentive or reward value of the goal, and (3) expectations of the individual and of his or her peers. These factors are the reasons one has for behaving in a certain way. An example is a student who spends extra time studying for a test because he or she wants a better grade in the class.

Given the diversity of computer related crimes, it is not surprising that the various types of behaviour discussed above flow from a wide range of motives. Some of these are as old as human society, including greed, lust, revenge and curiosity. Revenge in the modern era can also entail an ideological dimension. Of considerable significance, if not unique to computer related crime, is the intellectual challenge of defeating a complex system. The motivation for the hackers and crackers could be stealing information or other assets, or merely an act of power wherein he feels powerful in being able to break in a system representing big business or Governmental organization.

2.14.3 Opportunities:

Definition:

Exploitable set of circumstances with uncertain outcome, requiring commitment of resources and involving exposure to risk.

Examples of Opportunity:

1. You'll have an opportunity to ask questions after the presentation.
2. When the opportunity came for her to prove that she could do the job, she was ready.
3. I had the rare opportunity of speaking to the president.
4. Studying abroad provides a great opportunity to learn a foreign language.
5. There are fewer job opportunities this year for graduates.
6. I would like to take this opportunity to thank everyone who helped me with this book.

The exponential growth in connectivity of computing and communications creates parallel opportunities for prospective victims. As the internet becomes increasingly a medium of commerce, it will become increasingly a medium of fraud. There are many technologies which reduce the opportunity to commit computer related crime such as technologies of authentication, from basic passwords, to various biometric devices such as finger print or voice recognition technology, and retinal imaging, which greatly enhance the difficulty of obtaining unauthorized access to information systems. Virus detectors can identity and block malicious computer code; blocking and filter ing programs can screen out unwanted content. A rich variety of commercial software now exist with which to block access to certain sites.

2.14.4 Guardians:

Absence of capable guardianship is also a factor Cyber Crime. Guardianship against Cyber Crime involves preventive efforts on the part of prospective victims, contributions by members of the general public or commercial third parties, as well as the activities of law enforcement agencies. Indeed, it is often only when private efforts at crime prevention fail that the criminal process is mobilised. Capable guardianship has evolved over human history, from feudialism, to the rise of the state and the proliferation of public institutions of social control, to the postmodern era in which employees of private security services vastly out number sworn police officers in many industrial democracies. The basic tenets of the opportunity theory are that the level of crime is determined by the availability of suitable targets, the presence of motivated offenders and the absence of capable guardians.

2.14.5 Enforcement:

In present times, even where the crimes get reported, the prosecution rate is not very high as per worldwide trends available. The criminal justice administration systems are not equipped to deal with the highly technological crimes committed in cyber world. The traditional laws, procedures and the systems are unable to appreciate the nature of crime investigation and evidence in cyberspace for want of necessary technical knowledge. The need for enhancing the understanding about peculiarities of Cyber Crimes and cyber-evidences, by judicial officers. It is the judiciary who has the final word on any criminal prosecution and unless the awareness level among them is built up to meet the challenge of increasing Cyber Crimes, the rate of successful prosecutions will still be less. So to deter prospective offenders from undertaking any crime in cyberspace, the judicial understanding about cyber issues need to be enhanced.

2.15 Types of Cyber Crime:

Cyber Crime IS AN EVIL HAVING ITS ORIGIN IN THE GROWING DEPENDENCE ON COMPUTERS IN MODERN LIFE.

"A simple yet sturdy definition of Cyber Crime would be unlawful acts wherein the computer is either a tool or a target or both". Defining Cyber Crimes, as "acts that are punishable by the information Technology Act" would be unsuitable as the Indian Penal Code also covers many Cyber Crimes, such as e-mail spoofing, cyber defamation, etc

1. Cyber Crime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

2. Cyber Crime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three slots.

- Those against persons.
- Against Business and Non-business organizations.
- Crime targeting the government.

2.15.1 Financial Claims:

This would include cheating, credit card frauds, money laundering etc

2.15.2 Cyber Pornography:

This would include pornographic websites; pornographic magazines produced using computer and the Internet (to download and transmit pornographic pictures, photos, writing etc)

2.15.3 Sale of Illegal Articles:

This would include sale of narcotics, weapons and wildlife etc, by posting information on websites, bulletin boards or simply by using e-mail communications.

2.15.4 Online Gambling:

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

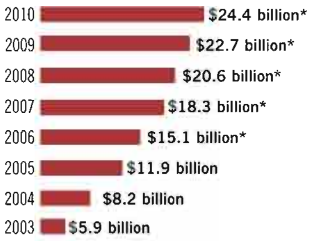


Fig. Global Online Gambing Revenue

2.15.5 Intellectual Property Crimes:

These include software piracy, copyright infringement, trademarks violations etc

2.15.6 E-mail Spoofing:

A spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-mail forging.

2.15.7 Forgery:

Counterfeit currency notes, postage and revenue stamps, mark sheets etc, can be forged using sophisticated computers, printers and scanner.

2.15.8 Cyber Defamation:

This occurs when defamation takes place with the help of computers and or the Internet e.g. someone published defamatory matter about someone on a websites or sends e-mail containing defamatory information to all of that person's friends.

2.15.9 Cyber Stalking:

Cyber stalking involves following a person's movements across the internet by posting messages on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim.

Cyber Stalking

- 75 to 80% of stalkers are men stalking women
- Most Victims are women
- Most Stalkers are men

2.15.10 Unauthorized Access to Computer System or Network:

This activity is commonly referred to as hacking. The Indian Law has however given a different connotation to the term hacking.

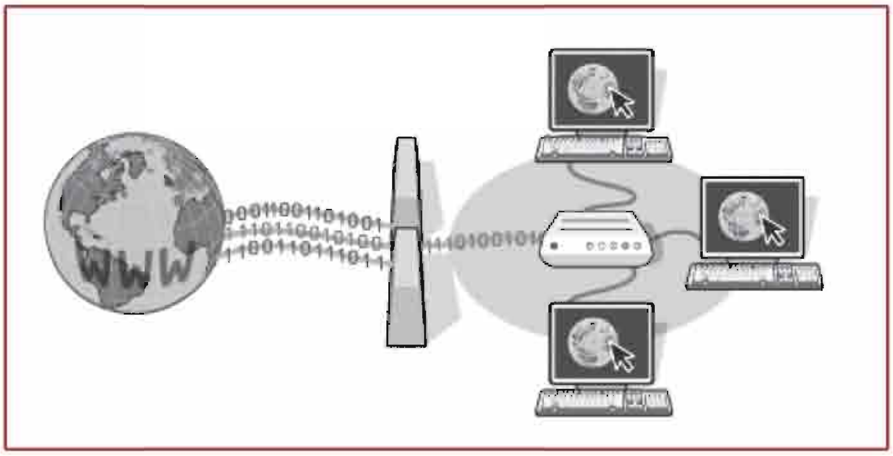


Fig. Unauthorized access to computer system or network

2.15.11 Theft of Information Contained in Electronic Form:

This includes information stored in computer hard disks, removable storage media etc

2.15.12 E-mail Bombing:

Email bombing refers to sending a large amount of e-mails to the victim resulting in the victims' e-mail account or mail servers.

2.15.13 Data Diddling:

This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

2.15.14 Salami Attacks:

Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer.

2.15.15 Denial of Service:

This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

2.15.16 Virus / Worm:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to.

2.15.17 Logic Bombs:

These are dependent programs. This implies that these programs are created to do something only when a certain event occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date.

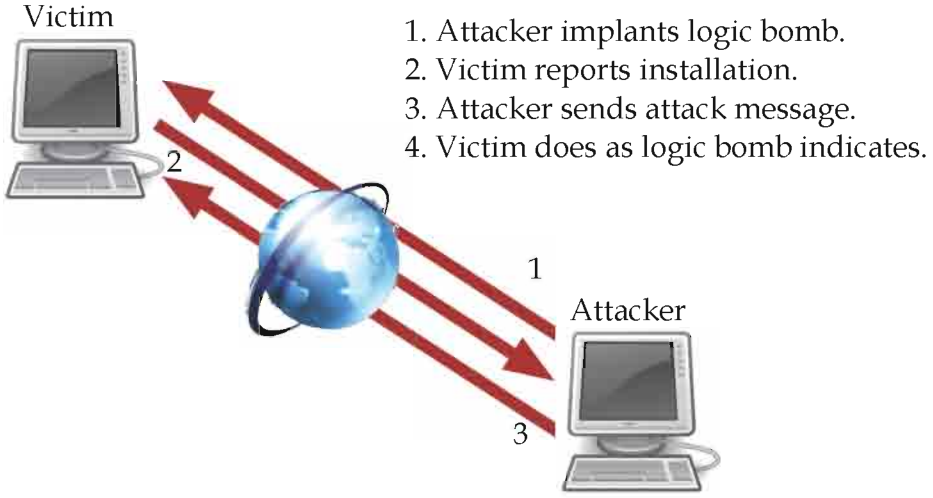

Victim
2
1
Attacker
3
1. Attacker implants logic bomb.
2. Victim reports installation.
3. Attacker sends attack message.
4. Victim does as logic bomb indicates.

Fig. Logic Bombs

2.15.18 Trojan Horse:

A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

2.15.19 Internet Time Theft:

This connotes the usage by unauthorized persons of the Internet hours paid for by another person

2.15.20 Physically Damaging a Computer System:

This crime is committed by physically damaging a computer or its peripherals.

2.16 Threat Perceptions:

Definition:

Threat perception is defined as a deep sense of vulnerability that is assumed to be negative, likely to result in loss, and largely out of one's control.

Threat perception is commonly viewed as a requirement to change organizational inertia.

UK has the largest number of infected computers in the world followed by the US and China. Financial attacks are 16 events per 1000, the highest among all kinds of attacks. The US is the leading source country for attacks but this has declined. China is second and Germany is third. It is hard to determine where the attack came from originally. The number of viruses and worm variants rose sharply to 7,360 that is a 64% increase over the previous reporting period and a 332% increase over the previous year. There are 17,500 variants of Win. 3 viruses. Threats to confidential information are on the rise with 54% of the top 50 reporting malicious code with the potential to expose such information, Phishing messages grew to 4.5 million from 1 million between July and December 2004.

2.17 Tools Used for Cyber Crime:

Botnets are becoming a major tool for Cyber Crime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal botnets, or “Bot Networks”, are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnets have been described as the “Swiss Army knives of the underground economy” because they are so versatile.

Botnet code was originally distributed as infected email attachments, but as users have grown more cautious, Cyber criminals have turned to other methods. When users click to view a spam message, botnet code can be secretly installed on the users’ PC A website may be unknowingly infected with malicious code in the form of an ordinary looking advertisement banner, or may include a link to an infected website. Clicking on any of these may install botnet code. Or, botnet code can be silently uploaded, even if the user takes no action while viewing the website, merely through some un-patched vulnerability that may exist in the browser. Firewalls and anti-virus software do not necessarily inspect all data that is downloaded through browsers. Some bot software can even disable anti-virus security before infecting the PC. Once a PC has been infected, the malicious software establishes a secret communications link to a remote “botmaster” in preparation to receive new commands to attack a specific target. Meanwhile, the malicious code may also automatically probe the infected PC for personal data, or may log keystrokes, and transmit the information to the botmaster.

The Shadow server Foundation is an organization that monitors the number of command and control servers on the Internet, which indicates the number of bot through May 2007, approximately 1,400 command and control servers were found to be active on the Internet. The number of individual infected drones that are controlled by these 1,400 servers reportedly grew from half a million to more than 3 million from March to May 2007, Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006.

2.18 Other Cyber Crime Methods:

Cyber Crime is usually conducted through a connection to the Internet, but can also involve unauthorized removal of data on small, portable flash drive storage devices. Cyber Crime, usually in the form of network hacking, has involved persons with strong technical skills, often motivated by the desire to gain popularity among their technology peers. However, the growing trend is now to profit from these network cyber-attacks by targeting specific systems, often through collaboration among criminals and technical experts. The motives that drive these cybercriminal groups now may differ from those of their paying customers, who may possess little or no technical skills.

New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime intcyberspace, work to the advantage of Cyber criminals who can choose to operate from geographic locations where penalties for some forms of Cyber Crime may not yet exist. Sophisticated tools for cyber-attack can now be found for sale or for rent on the internet, where highly organized underground Cyber Crime businesses host websites that advertise a variety of disruptive software products and malicious technical services. High-end Cyber Crime groups use standard software busi ness development techniques to keep their products updated with the latest antisecurity features, and seek, to recruit new and talented software engineering students into their organizations.

Where illicit profits are potentially very large, some high-end criminal groups have reportedly adopted standard IT business practices to systematically develop more efficient and effective computer code for Cyber Crime. Studies also show that organized crime groups now actively recruit college engineering graduates and technical expert members of computer societies, and sponsor them to attend more information technology (IT) courses to further their technical expertise. However, in some cases, targeted students may not realize that a criminal organization is behind the recruitment offer.

Cyber attacks are increasingly designed to silently steal information without leaving behind any damage that would be noticed by a user. These types of attacks attempt to escape detection in order to remain on host systems for longer periods of time. It is also expected that as mobile communication devices are incorporated more into everyday life, they will be increasingly targeted in the future for attack by Cyber criminals.

2.18.1 Malicious Code:

Definition:

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

Malicious code, such as viruses or Trojan Horses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer if the user opens an email attachment, or clicks an innocent looking link on a website. For example, users who visited the popular MySpace and YouTube websites in 2005, and who lacked important software security patches, reportedly may have had their PCs infected if they clicked on a banner advertisement which silently installed malicious code on their computers to log keystrokes or capture sensitive data. During the first half of 2006, the Microsoft Security Team reported that it had removed 10 million pieces of malicious software from nearly 4 million computers and web servers. Recently, analysis at Google tested several million web pages for the presence of malicious software, and determined that 4.5 million of the web pages examined were suspicious in nature. After further testing of the 4.5 million web pages, over 1 million were found to launch downloads of malicious software, and more than two thirds of those program were “bot” software that, among other things, collected data on banking transactions and then emailed the information to a temporary email account.

Researchers at the San Jose, Calif-based security firm, Finjan Inc., after reviewing security data from the first quarter of 2007, found that more malware is hosted on servers in countries such as the US. and UK, than in other countries with less developed e-crime law enforcement policies.

Findings from the Finjan 2007 Web Security Trends Report are based on an analysis of more than 10 million unique websites from Internet traffic recorded in the UK, and include the following:

1. Attacks that involve the use of code obfuscation through diverse randomization techniques are growing more numerous and complex, making them virtually invisible to patternmatching/ signature-based methods in use by traditional anti-virus products.

2. Criminals are displaying an increasing level of sophistication when embedding malicious code within legitimate content with less dependence on outlaw servers in unregulated countries.

Finjan found that 90% of the websites examined containing malware resided on servers located in the US or UK "The results of this study shatter the myth that malicious code is primarily being hosted in countries where-e-crime laws are less developed," Finjan CTO Yuval Ben-Itzhak reportedly stated.

2.18.2 Identity Theft:

Botnets and other examples of malicious code can operate to assist cyber criminals with identity theft. Current FBI estimates that identity theft costs American businesses and consumers $50 billion a year. Individual users are often lured into clicking on tempting links that are found in email or when visiting websites. Clicking on titles such as "Buy Rolex watches cheap," or "Check out my new Photos", can take advantage of web browser vulnerabilities to place malicious software onto a users system which allows a cybercriminal to gather personal information from the user's computer.

Malicious code can scan a victim's computer for sensitive information, such as name, address, place and date of birth, social security number, mother's maiden name, and telephone number. Full identities obtained this way are bought and said in online markets. False identity documents can then be created from this information using home equipment such as a digital camera, colour printer, and laminating device, to make official-looking driver's licences, birth certificates, reference letters, and bank statements.

Identity theft involving thousands of victims is also enabled by inadequate computer security practices within organizations. MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to US consumers were accessed by computer hackers. Some of these account numbers were reportedly being said on a Russian website, and some consumers have reported fraudulent charges on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related to theft of the MasterCard Information. In June 2006, officials from the US Department of Energy acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen in a network intrusion that apparently took place in 2004. The NNSA did not discover the security breach until one year after it had occurred.

Some sources report that stolen credit card numbers and bank account information are traded online in a highly structured arrangement, involving buyers, sellers, intermediaries, and service industries. Services include offering to conveniently change the billing address of a theft victim, through manipulation of stolen PINs or passwords. Observers estimated that in 2005 such services for each stolen MasterCard number cost between $42 and $72. Other news articles report that, in 2007, a stolen credit card number sells online for only $1, and a complete identity, including a US bank account number, credit-card number, date of birth, and a government issued ID number now sells for just $14 to $18.

As of January 2007, 35 states have enacted data security laws requiring businesses that have experienced an intrusion involving possible identity theft to notify persons affected, and to improve security for protection of restricted data. However, existing federal and state laws that impose obligations on information owners, may require harmonization to provide protections that are more uniform.

2.18.3 Cyber Espionage:

Cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defences, or the unauthorized probing to test a target computer's configuration or evaluate its system defences, or the unauthorized viewing and copying of date files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives, their deliberate intrusions may also quality them, additionally, as cyber criminals. If there is disagreement about this, it is likely because technology has outpaced policy for labelling actions in cyberspace. In fact, industrial cyber espionage may now be considered as a necessary part of global economic competition, and secretly monitoring the computer ized functions and capabilities of potential adversary countries may also be considered essential for national defence.

2.19 Connection between Terrorism and Cyber Crime:

The proportion of Cyber Crime that can be directly or indirectly attributed to terrorists is difficult to determine. However, linkages do exist between terrorist groups and criminals that allow terror networks to expand internationally through leveraging the computer resources, money laundering activities, or transit routes operated by criminals. For example, the 2005 UK subway and bus bombings, and the attempted car bombings in 2007, also in the UK provide evidence that groups of terrorists are already secretly active within countries with large communication networks and computerized infrastructures, plus a large, highly skilled IT workforce. London police officials reportedly believe that terrorists obtained high-quality explosives used for the 2005 UK bombings through criminal groups based in Eastern Europe.

A recent trial in the UK revealed a significant link between Islamic terrorist groups and Cyber Crime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pleaded guilty, and were sentenced for using the Internet to incite murder. The men had used stolen credit card information at online web stores to purchase items to assist fellow jihadists in the field—items such as night vision goggles, tents, global positioning satellite devices, and hundreds of prepaid cell phones, and more than 250 airline tickets, through using 110 different stolen credit cards. Another 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies. The group also laundered money charged to more than 130 stolen credit cards through online gambling websites. In all, the trio made fraudulent charges totalling more than $3.5 million from a database containing 37,000 stolen credit card numbers, including account holders' names and addresses, dates of birth, credit balances, and credit limits.

Cyber criminals have made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups. Drug traffickers are reportedly among the most widespread users of encryption for internet, messaging, and are able to hire high level computer specialists to help evade law enforcement, coordinate shipments of drugs, and launder money. Regions with major narcotics markets, such as Western Europe and North America, also possess optimal technology infrastructure and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups. Officials of the US Drug Enforcement Agency (DEA), reported in 2003 that 14 of the 36 groups found on the US State Department's list of foreign terrorist organizations were also involved in drug trafficking. A 2002 report by the Federal Research Division at the Library of Congress, revealed a "growing involvement, of Islamic terrorist and extremists groups in drug trafficking," and limited evidence of cooperation between different terrorist groups involving both drug trafficking and trafficking in arms. Consequently, DEA officials reportedly argued that the war on drugs and the war against terrorism are and should be linked.

State Department officials, at a Senate hearing in March 2002, also indicated that some terrorist groups may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies in the West through exploiting their desire for addictive drugs. The poppy crop in Afghanistan reportedly supplies resin to produce over 90% of the world's heroin, supporting a drug trade estimated at $3.1 million. Reports indicate that money from drug trafficking in Afghanistan is used to help fund terrorist and insurgent groups that operate in that country. Subsequently, US intelligence reports in 2007 have stated that AL Qaeda in Afghanistan" has been revitalized and restored to its pre-September 11, 2001 operation levels, and may now be in a better position to strike Western countries.

Drug traffickers have the financial clout to hire computer specialists with skills for using technologies which make Internet messages hard or impossible to decipher, and which allow terrorist organizations to transcend borders and operate internationally with less chance of detection. Many highly trained technical specialists that make themselves available for hire originally come from the countries of the former Soviet Union and the Indian subcontinent. Some of these technical specialists reportedly will not work for criminal or terrorist organizations willingly, but may be misled or unaware of their employers' political objectives. Still, others will agree to provide assistance because other well-paid legitimate employment is scarce in their region.

2.19.1 Links between Computer Hackers and Terrorists, or Terrorist Sponsoring Nations may be Difficult to Confirm:

Membership in the most highly-skilled computer hacker groups is sometimes very exclusive and limited to individuals who develop, demonstrate, and share only with each other, their most closely guarded set of sophisticated hacker tools. These exclusive hacker groups do not seek attention because maintaining secrecy allows them to operate more effectively. Some hacker groups may also have political interests that are supra-national, or based on religion, or other socio-political ideologies, while other hacker groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer services, regardless of the political interests in volved. Information about computer vulnerabilities is now for sale online in a hacker's "black market". For example, a list of 5,000 addresses of computers that have already been infected with spyware and which are waiting to be remotely controlled as part of an automated "bot network" reportedly can be obtained for about $150 to $500. Prices for information about computer vulnerabilities for which no software patch yet exists reportedly range from $1,000 to $5,000.

2.19.2 Terrorist Capabilities for Cyber Attack:

Some experts estimate that advanced or structured cyber attacks against multiple systems and networks, including target surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyber attack, causing mass disruption against integrated, heterogeneous systems may require 6 to l0 years of preparation. This characteristic, where hackers devote much time to detailed and extensive planning before launching a cyber attack, has also been described as a "hallmark" of previous physical terrorist attacks and bombings launched by AL Quaeda.

Some observers have stated that AL Quaeda does not see cyber attack as important for achieving its goals, preferring attacks which inflict human casualties. Other observers believe that the groups most likely to consider and employ cyber attack and cyber terrorism are the terrorist groups operating in post-industrial societies (such as Europe and the United States), rather than international terrorist groups that operate in developing regions where there is limited access to high technology.

2.19.3 Possible Effects of a Coordinated Cyber Attack:

In March 2007, researchers at Idaho National Laboratories (INL) conducted an experiment labelled the "Aurora Generator Test" to demonstrate the results of a simulated cyber attack on a power network. In a video released by the Department of Homeland Security, a power generator turbine, similar to many now in use throughout the United States, is forced to overheat and shut down dramatically, after receiving malicious commands from a hacker. The researchers at INL were investigating results of a possible cyber attack directed against a vulnerability that, reportedly, has since been fixed. The video, vulnerabilities could potentially be disabled the same way.

In July 2002, the US Naval War College hosted a war game called "Digital Pearl Harbor" to develop a scenario for a coordinated cyber terrorism event, where mock attacks by computer security experts against critical infrastructure systems simulated state-sponsored cyber warfare. The simulated cyber attacks determined that the most vulnerable infrastructure computer systems were the internet itself, and the computer systems that are part of the financial infrastructure. It was also determined that attempts to cripple the US telecommunications infrastructure would be unsuccessful because built-in system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a "digital Pearl Harbor" in the United States was only a slight possibility.

However, in 2002, a major vulnerability was discovered in switching equipment software that threatened the infrastructure for major portions of the Internet, a flaw in the Simple Network Management Protocol (SNMP) would have enabled attackers to take over internet routers and cripple network telecommunications equipment globally. Network and equipment vendors worldwide raced quickly to fix their products before the problem could be exploited by hackers, with possible worldwide consequences. US government officials also reportedly made efforts to keep information about this major vulnerability quiet until after the needed repairs were implemented on vul nerable Internet systems. According to an assessment reportedly written by the FBI, the security flaw could have been exploited to cause many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems.

While describing possible offensive tactics for military cyber operations, DOD officials reportedly stated that the US could confuse enemies by using cyber attack to open floodgates, control traffic lights, or scramble the banking systems in other countries. Likewise, some of China's military journals speculate that cyber attacks could disable American financial markets. China, however, is almost as dependent on these US markets as the United States, and might possibly suffer even more from such a disruption to finances. As to using cyber attack against other US critical infrastructures, the amount of potential damage that could be inflicted might be relatively trivial compared to the costs of discovery, if engaged in by a nation state. However, this constraint does not apply to non-state actors like AL Qaeda, thus making cyber attack a potentially useful tool for those groups who reject the global market economy.

2.19.4 Organized Cyber Crime:

Some large cyber criminal groups are transnational, with names like Shadow-crew, Carderplanet, and Darkprofits, individuals in these groups reportedly operate from locations all over the world, working together to hack into systems, steal credit card information and sell identities, in a very highly structured, organized network. Organized crime is also recruiting teenagers who indicate that they feel safe doing illegal activity online than in the street. A recent report from the McAfee security organization, titled the 'Virtual Criminology Report', draws on input from Europe's leading high-tech crime units and the FBI, and suggests that criminal outfits are targeting top students from leading academic institutions and helping them to acquire more skills that is essential to commit high-tech crime on a massive scale.

In the future, we may see new and different modes of criminal organization evolve in cyberspace. Cyberspace frees individuals from many of the constraints that apply to activities in the physical world, and current forms of criminal organization may not transition well to online crime. Cyber Crime requires less personal contact, less need for formal organization, and no need for control over a geographical territory. Therefore, some researchers argue that ˝the classical hierarchical structures of organized crime groups may be unsuitable for organized crime on the internet. Consequently online criminal activity may emphasize lateral relationship and networks instead of hierarchies."

Instead of assuming stable personnel configurations that can persist for years, online criminal organization may incorporate the "swarming" model, in which individuals coalesce for a limited period of time in order to conduct a specific task, or set of tasks, and afterwards go their separate ways. The task of law enforcement could therefore become much more difficult. If Cyber criminals evolve into the "Mafia of the moment" or the "cartel of the day," police will lose the advantage of identifying a permanent group of participants who engage in a set of routine illicit activities, and this will only contribute to the future success of organized Cyber Crime.

Cyber terrorist prefer using the cyber attack methods because of many advantages for it:

- It is Cheaper than traditional methods.
- The action is very difficult to be tracked.
- They can hide their personalities and location.
- There are no physical barriers or check points to cross.
- They can do it remotely from anywhere in the world.
- They can use this method to attack a big number of targets.
- They can affect a large number of people.

अध्याय 3

Chapter 3

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

3.1. Fundamentals of Cyber Security

3.1.1. 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.

3.1.1.1. 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 lso 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.

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 controlsfail or are bypassed. They can protect the secrecy of data more completely than cryptography, butif they fail or are evaded, the data becomes visible. Access control mechanisms sometimes concealthe 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 thedata itself. The precise number of people who distrust a politician may be less important thanknowing that such a poll was taken by the politician's staff. How a particular government agencyharassed 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 inappropriateways), 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.

3.1.1.2. 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 adversarytries to find two inputs to the hash function that map to the same output. If hash functions are usedfor signature schemes, a collision attack can allow an adversary to forge a signed message. Mostrecently 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).

3.1.1.3. 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 o 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 themessage 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.

3.1.1.4. 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.

3.1.1.5. 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. O bject-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.

3.1.2. 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.

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. Integrityand 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.

3.1.3. 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.

3.2. Significance of Cyber Security

3.2.1. 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 band width; 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.

3.2.2. 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.

3.2.3. 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.

3.2.4. 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 se curity 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 presi dent 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 preemptivestrike phases of a conflict.

3.2.5. 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 indus try 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.

3.2.6. 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.

3.3. Major Cyber Security Risks for the Common Man

3.3.1. 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 antimalware 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.

3.3.2. 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 informa tion 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 botinfected 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.

3.3.3. 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 TCPbased (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'.

3.3.4. 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 bestcase 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."

3.3.5. 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.

3.3.6. 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 orga nization, 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.

3.3.7. 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-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

3.3.8. 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.

3.3.9. 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 han 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 passwordprotected file.

2. 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.

3.3.10. They Can Attack all Operating Systems

Window's popularity meant that it had to be the prime target of attacks. Mac and Linux user-shave 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.

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 "Per verted Justice," a Portland, Oregonbased 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 casem 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 as 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 com pany 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 wellknown 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 of fenders 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 ac commodation 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.

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. Ltd
- 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 togetherwith 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 ma lignant 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 import ant 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 send ing 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 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. Ltd.

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
- Case Study 47: Scam No.2 : Follow-up scamming
- Case Study 48: Scam No.3 : Purchasing Goods and Services Scam
- Case Study 49: Scam No.4 : Cheque Cashing Scam
- Case Study 50: Scam No.5 : Romance Scam
- Case Study 51: Scam No.6 : Lottery Scam
- Case Study 52: Scam No.7 : The Hitman Scam
- Case Study 53: Scam No.8 : Bomb Scams
- Case Study 54: Scam No.9 : Charity Scams
- Case Study 55: Scam No.10 : Fraud Recovery Scams
- Case Study 56: Scam No.11 : Pet Scams
- Case Study 57: Scam No.12 : Bona Vacantia Scam
- Case Study 58: Scam No.13 : Fake Job Offer Scams
- Case Study 59: Scam No.14 : Rent Scams
- Case Study 60: Scam No.15 : Attorney Debt Collection Scams
- Case Study 61: Scam No.16 : Malware Scams
- Case Study 62: Scam No.17 : The Advantage Fee Fraud
- Case Study 63: Scam No.18 : Babysitting Scams
- Case Study 64: Scam No.19 : Nigerian 419 Scams
- Case Study 65: Scam No.20 : Craiglist Scams
- Case Study 66: Scam No.21 : Pyramid Scheme Scams and Ponzi Scheme Scans

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 offer free air travel to the victim, if they agree to prepay 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 "workat- 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 off, 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 off 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 deduct ible 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 ıoney 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:

- 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."
- 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.
- Never pay any upfront fee for placement services that offer a "dream job."
- 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.
- 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.
- Of course, never depend on oral promises.
- 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.

- 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.

- 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.

- 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 offices in regular business hours.

- Forget about companies with no legitimate street address and companies or agencies that refuse to provide verifiable references.

- 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.

- 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.

- 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.

- 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 difficult. 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:

- 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).

- 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.

- 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.

- 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 fictitiouscharacters 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 men tioned 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 babysitter 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:

- What academic qualifications do you possess?
- Do you have any good certificate to support your prior babysitting/Nanny experience?
- How old are you?
- Are you married?
- Do you have any special aptitude?
- Do you have any crime records?
- Do you have a valid driver's license?
- Tell us more about your temperament.
- Can we have one or two reference(s) from you?
- Can you handle finances if you are given a task to carry out?
- 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:

- 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!

- 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.

- 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!

- 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.

- 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.

- 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:

- 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!

- 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!

- 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.

- 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!

- 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 multilevel 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-tounderstand 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 udaries. 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.

Articles by Cyber Security Experts

Smart Cities & Cyber Security Concerns in India Smart Cities

Rakesh Kumar Raju

Chair Member of National Cyber Defence Research Centre (NCDRC)

According to the Institute for Electrical and Electronics Engineers (IEEE), "A Smart City brings together Technology, Government and Society to enable the following characteristics: A smart economy, smart mobility, a smart environment, smart people, smart living and smart governance."

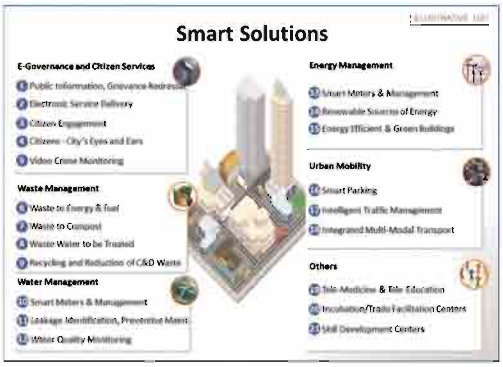
With increasing urbanization, urban areas are expected to have around 40% of India's popula ion and also contribute to 75% of India's GDP by 2030. This needs a solid Economic, Social, Physical & other infrastructure which needs to be built from ground up. All are important in improving the quality of life of general public and also to attract people and investments to the future cities, setting in motion a cycle of growth and development. The dream of our Hon'ble' Prime Minister – Shri. Narendra Modi-ji's development of Smart Cities is a step in that direction.

So going back to the penultimate question - What is a 'Smart City'? The answer lies in what services the Govt. would like to provide to its citizens as part of this program, there is no universally accepted definition of a Smart City. The conceptualisation of Smart City varies from different Cities and countries, depending on the level of development, willingness to change and reform. A Smart City would have a different connotation in India from, say, US / Europe or other parts of the World.

The Smart City project's objective is to provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'smart' / intelligent solutions.

The core infrastructure elements in a Smart City can include:

- Assured 24 / 7 electricity supply using Smart Grids reducing Blackouts,
- Adequate potable water supply & Intelligent Water Management & Recycling capabilities,
- Sanitation, including solid waste management / Zero Waste Management
- Robust IT connectivity and digitization,
- Efficient and environment friendly urban Connected Mobility and public transport which reduces carbon footprint in smart cities and our country,
- Housing which uses resources like HVAC smartly. Also having interconnected home appliances.
- E-Governance.
- Safety and security of citizens using modern devices & equipment which will be connected to centralized devices, which may have access to private data of citizens.


Smart Solutions
E-Governance and Citizen Services
1 Public Information, Grievance Redressal
2 Electronic Service Delivery
3 Citizen Engagement
4 Citizens - City's Eyes and Ears
5 Video Crime Monitoring
Waste Management
6 Waste to Energy & fuel
7 Waste to Compost
8 Waste Water to be Treated
9 Recycling and Reduction of C&D Waste
Water Management
10 Smart Meters & Management
11 Leakage Identification, Preventive Maint.
12 Water Quality Monitoring
Energy Management
13 Smart Meters & Management
14 Renewable Sources of Energy
15 Energy Efficient & Green Buildings
Urban Mobility
16 Smart Parking
17 Intelligent Traffic Management
18 Integrated Multi-Modal Transport
Others
19 Tele-Medicine & Tele Education
20 Incubation/Trade Facilitation Centers
21 Skill Development Centers

(Source : Internet)

Smart cities predominantly rely upon use of Information and Communication Technologies (ICT) to render public services efficiently and intelligently. Wherever applicable, Internet of Things (IoT), Cloud Computing and Virtualisation and machine to machine (M2M) systems are used. However, this omnipresent usage of ICT, IoT, M2M, cloud computing, etc. has a potential drawback as well in the form of indifference towards smart cities cyber security.

Cyber Security Concerns over Smart Cities

It may not be difficult to visualise a scenario of cyber-attacks against critical infrastructures in smart cities that are run by ICT, IoT & Other technologies. Such cyber-attacks can cripple an entire smart city if, well executed. Critical infrastructure protection within India is still at a nascent stage. The national cyber security policy of India 2013, a framework which is developed by Department of Electronics and Information Technology (DeitY), is known to be pretty weak and even that has not been enforced by the Indian government so far. It aims at protecting the public and private infrastructure from cyber- attacks. The policy also intends to safeguard "Information, such as personal information (of web users), financial and banking information and sovereign data". This became important in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. The much awaited cyber security policy of India 2015/16 is also missing so far.

A strong cyber security infrastructure for India is strongly needed, especially when there is no well settled international legal issues of cyber-attacks that can be invoked in the case of cyber incidences.

It is very important that international legal issues of cyber-attacks must be resolved by various government and non-government stakeholders. There is no globally acceptable cyber law treaty and cyber security treaty that can govern the relationships between various countries (some of them are in the pipeline), Even the Tallinn Manual on the International Law Applicable to Cyber Warfare is just an academic document with no legal binding obligations. Tallinn Manual cannot be applied to international cyber-attacks or defence and countries are free to take measures as per their own choices. Some countries like the US consider a cyber-attack to be an Attack on their very nation.

Although this has necessitated that cyber security / cyber warfare related projects in India be expedited, they must also be successfully implemented as early as possible. We have many cyber projects run by different organizations like

- National Critical Information Infrastructure Protection Centre (NCIPC) of India,
- Grid Security Expert System (GSES) of India,
- National Intelligence Grid (Nat grid) Project of India,
- National Cyber Coordination Centre (NCCC) of India,
- Crisis Management Plan Of India For Cyber Attacks And Cyber Terrorism,
- Cyber Attacks Crisis Management Plan of India,
- Cyber Command For Armed Forces & Tri Service Cyber Command for Armed Forces of India,
- Internet Spy System Network And Traffic Analysis System (NETRA) of India,
- Crime and Criminal Tracking Network and Systems (CCTNS) Project of India, etc is still struggling to be implemented successfully by our many different governments.

While the current government is serious about Smart Cities, it must take cyber security for Smart Cities seriously otherwise this may be detrimental in the long run.

This raises the pertinent question as to how Indian government would ensure cyber security of smart cities in India. 100 Smart Cities have already been identified and a notification issued. The cybersecurity challenges will only increase in numbers and complexity as and when Smart Cities are implemented in India and we must be prepared to protect its cyberspace. A comprehensive Policy is need of the hour. Also ,

- By adopting the latest technologies & Encryption techniques, a catastrophic cyber-attack on a smart City/ies can be prevented even before it affects critical Infrastructure.
- Tested & Certified Equipment should be used within Smart Cities. Secure coding for Applications & Devices will be a must.
- PLC’s (programmable logic controllers) in Smart Grids and Nuclear Power Stations, factories etc. & SCADA security needs to be focussed upon.
- There should be a well-defined mechanism for preventing APT’s (Advanced Persistent Threats) & also Web application attacks.
- Improvisation & Protection of Telematics data which may be transmitted by vehicles in a smart transportation environment.
- Skilled workforce is also need of the hour and for this purpose cyber security courses must be introduced at the university level. Online education must be encouraged so that online cyber

security courses can be imparted in India.

Vulnerabilities can be exploited by attackers with different motives and expertise and could cause high levels of damage to the network. Attackers may be script kiddies, elite hackers, disgruntled employees, competitors, customers or even terrorists. Terrorists will view the smart cities / grid as an attractive target as it affects millions of people making the terrorists' cause more visible.

It's crucial for India to establish both offensive and defensive cyber warfare capabilities. This is important to protect critical infrastructures in India that are dependent upon information technology, via ICT; IoT & Cloud based services etc. A cyber warfare policy of India must also be formulated as malware like Ouroboros, Blackshades, FinFisher, Stuxnet, Duqu, Flame, etc. are beyond the reach of current cyber security mechanisms. Some of these may be old, but - very valid due to the subject we are discussing. These malwares are stealthy in nature and by the time they are discovered, an irreparable damage is already done.

WWHW: Pen-Test Organization's Identity

Arulselvar Thomas
Technical Head of National Cyber Defence Research Centre (NCDRC)
Director of Brisk InfoSec

[WWHW: Why, What, How and Where]

Why is that we need to look for real talent with cutting edge technology when it comes to selecting a Pen-Test organization to secure your digital data. Prime objective of hiring a security consulting company is to maximize the value in safeguarding the most critical data related to your business inclusive of industry standard certifications to validate the test preformed. It can be an extremely confusing and frustrating experience in the end if you don't meet the needs or requirements of the security testing in terms of business perspective of your organization.

There are still a lot of inexperienced people out there that are posing themselves off as experts, marketed as "vulnerability scanning", "compliance audit" or "security assessment" often confusing you to pick the right company to partner with for your penetration test. This process can be a gamble if you don't know what you're buying, "Don't Get Pawned before You Sign". Look for consultants who thinks strategically, have agreeable level of flexibility, follow better security practices, Penetration Testing Execution Standard (PTES) compliance. Penetration testing is not an exact science hence validate that if the consultant organization has a work culture comprises of flexibility to follow up on any areas of concern and pursue the path of least resistance.

What is your need for protecting data decides nature of security testing execution plan, however Penetration testing tools can only simulate attacks and help you get an idea of their security vulnerabilities. Penetration testing is the job of a specialist, an expert analyzing large-scale breaches, who can validate the vulnerability assessment reports to their effectiveness with his humongous experience. Moreover, most of the testing tools lack the ability to determine how realistic those risks are. Initial scoping of a penetration test focus on what is the most important information, processing assets that are vulnerable and their business value compromised if attacks might happen.

You don't necessarily need a background on cyber security so that you could understand how penetration testing performed and ethical hacker's work nature. It's all about ensuring that you have the best man [white-hat] in the market to block the middle man [black-hat] from trying an attack. What you need is to identify and understanding the strengths and weak-nesses of your partner organization by learning about their qualities like competency, responsibility, flexibility, reliability, and efficiency to handover the security assessment job and before in hand get a NDA signed. What is the ROI for a Pen-Test? When I meet prospective clients this is the basic question asked by management heads and it's important for security professionals to understand how business views and justifies expenditures. It is important for the security professional to teach business to think in terms of information asset valuation and correlate that to potential loss.

How is your data protected during and after Penetration testing is a critical parameter before any discussion about developing effective relationships with security consultants. Often very reputed firms are difficult to handle with, and can be hard to schedule their services because they are very busy. Also they are often unable to perform anything but basic web testing. Technical competency of the employees is one of the important items in the checklist and a good Pen-Testing firm will showcase you the list of certifications and/or experience of their testers.

How specialized is the consultant? Do their consultants have passed an independent penetration testing assessment. How strictly do they adhere to the methodology? You want a good balance that establishes a “baseline” level of coverage but allows sufficient time for the consultant to try more creative attacks. This doesn’t mean that you should literally meet the consultants or have a phone interview but you have to get rid of people who talk convincingly about pen testing without actually having the expertise to do it. Penetration testing has become big business because systems are so complicated and poorly understood. We don’t know what’s dangerous today, and what will be dangerous tomorrow. So we hire penetration testers because penetration testing is a key component of a security assessment.

Where to start assessing your Pen-Test consultant organizations efficiency? A poorly executed pen test is even worse than not doing one at all because you get that false sense of security. A decade ago, a penetration test was generally a “black box” test that took place at the network level however attackers are now sophisticated enough that they will probably know a vast amount about your technology in advance of an attack. The OSI model, antiquated as it may seem, offers a good way to define the scope of a penetration test. Gray-box testing is a mix of black-box and white-box testing, involves close communication and information sharing between your technology group and pen testers. Whereas Black-box testing may be performed by an attacker!

Most importantly check if they perform penetration testing in a methodical and repeatable series of tests, working through many different types of vulnerabilities to avoid an inefficient scattergun approach. Once you have decided who will do the testing, make sure that they have time to complete a thorough evaluation. Without any doubt, the final report should detail the tests completeness, key discoveries on vulnerabilities and recommendations to mitigate the risk. Remember that the report is what you are paying for, and you will want time to discuss it with the tester to understand their findings.

Finally, at this point if you are thinking that little more technical details would make you likely scrutinize and tie-up with partners then talk to security experts. The concern is that without professional recommendation, the more risk the targeted system personnel will blindly follow it, potentially wreaking havoc in a production environment.

Are you Mr. Robot – The State Surveillance

Aditya Mukherjee

Member of National Cyber Defence Research Centre (NCDRC)

With the right set of skills and technology almost Anyone can Pwn you!!

I still remember the day, when one of my close friends watched Mr. Robot for the first time and went into a paranoid frenzy to set up security measures in her mobile, laptop and hard disk. To be honest, I was always aware of these techniques in the back of my mind but somehow watching it on the show made me reconsider my lax too.

In one the recent episode - eps2.7_init_5.fve, we saw Elliot hack into a sim using crackSIM to eavesdrop on a cell phone call. Although this was a frictional technique that was used, it is in fact technically possible.

In the show, the hack was done using the OTA update to send malware to the phone via a malicious text message. We all know that using a remote administrative tool (RAT) malware could allow a remote attacker to eavesdrop on a victim using an android device's microphone. Cracking the OTA key would allow that sort of malware to be injected into the phone by masquerading as the carrier. That approach is entirely plausible, though it may not have been carried out as quickly as in the episode, despite the use of a cloud-based DES cracking tool.

In the past we have seen security experts demonstrate that if an attacker has physical access to the SIM, along with pre-computed potential keys and knowledge of OTA update message, it is possible to grab a single 56-bit DES encryption key from the SIM. Even SIMs that use Triple DES encryption sometimes downgrade their key to just normal DES when the service they're connected to requests it.

This is the sort of attack that is used in "Stingray" boxes (which can be bought easily in black market), devices used by law enforcement around the world to track cell phones and intercept calls. (Stingrays lower cellular connections to 2G, weakening encryption on calls, to make it easier to monitor calls.)

We can also utilize an exploit to use a known weakness in the SS7 phone network routing protocol. An attacker can read text messages, listen to phone calls and track mobile phone users' locations with just the knowledge of their phone number.

Another alternative would require proximity to the victim - using a femtocell (a very small mobile phone base station which is connected to the phone network via the Internet, typically used in areas where the mobile signal is weak) to intercept the calls. A hacked femtocell would allow direct monitoring of the call without having to crack the SIM, because the femtocell decrypts signals it receives to route them over the Internet.

In the wake of the various exigent factors such as the rise of global Islamic terrorism, covert espionage, enormous economic and social paradigm shifts that we have seen in the last 15 years, surveillance has transformed from a pet project to a major tactical and strategic wing in almost every law enforcement agency across the globe. With the advancement in the technology, we have moved from a target specific monitoring to a mass surveillance model, where every day collection systems intercept and store more than 5 billion e-mails, phone calls and other types of communications.

Today, no digital communication is secure by the virtue that any communication is susceptible to government interception as it happens but far beyond that: all digital communications - meaning telephone calls, emails, online chats and the like - are automatically recorded and stored and accessible to the government after the fact. To describe that is to define what a ubiquitous, limitless Surveillance State is.

Coming from Law enforcement associated background, I understand the need and paramount importance of surveillance but how it is being exercised is not only astonishing but also a serious concern for privacy violations. The problem haunting the intelligence is not the lack of data but the ability to analyse them to produce an actionable output. This is why proper democratic oversight is needed to put a check to it.

This is partly what the German Federal Intelligence Service BND is doing now, there was a proposal to implement SAP Hana which is known as an in-memory database. As a result, Hana can answer complex search queries to draw conclusion based on connection between several different data to identify patterns and make analytic predictions. This kind of technology is required whenever one wants to analyse huge amounts of metadata. But there needs to be focus on factors such as how this metadata is intercepted, stored, shared and utilized.

The U.S. Government has specifically moved into a more aggressive mode with clandestine operation such as PRISM, INDECT, MYSTIC, ECHELON, XKeyscore(Real-Time Internet Monitoring Capability), Carnivore, Bullrun and any more to gather information from internet traffic, email content, contact list, data storage, social media and various backend databases additional to already established data request from corporations like Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple to name a few. This in turn has turned the microscope from targeted audience to the general public as a whole, gives direct access to audio, video, photographs, e-mails, documents and connection logs for each of these systems.

At this point you might think that at least the cloud is safe from these prying eyes, but think again. The NSA MUSCULAR program allows them to conveniently conduct large-scale data gathering outside the jurisdiction of the Foreign Intelligence Surveillance Court by secretly tapping into the communication links between Google's data centres outside the U.S. The Special Source Operations (SSO) group discovered a clever way around Google's security measures giving them full access to the rich data Google stores on the cloud for its users.

Above and beyond this you have the ANT catalogue, Operation CHAOS, ICREACH, Hawk owl project, Project Crisscross and programs like shenanigans (close to what we saw in the show Narcos), Undersea Cable Tapping Strategy, Persistent Surveillance Systems and many more potential data feeds like Pokemon Go.

Despite of this, the question remains that has this made any difference in making the world a safer place. A case in point one of the Boston marathon bomber was already on the watch list of the FBI. Even ex-NSA director William Binney has warned that Mass surveillance and bulk data collection won't prevent terrorism. If you are looking for a needle in a hay stack, increasing the amount of hay doesn't make it easier, instead the focus should be deriving sophisticated methods to find the same.

What happens is you get so many matches it's like getting a Google return. Every time you use a Google query you could get a hundred, a thousand, a million or more returns. And that's on just the input for that day and every day is the same. That means analysts can't get through it, they fail to see the threats. The end result is dysfunctional of the analyst and no prediction capabilities for stopping any attacks. The alternative, he suggested is targeted surveillance, which has been used to great effect, but sometimes only after events such as the Paris attacks.

People die and when they die you find out who did it, then focus on those people. That's when you do the targeted approach and now, like the French are doing, they're going after people and raiding them because they went after the people who did the attack, looked at the people they had relationships with. They could have got all that data from a targeted approach and could have had the opportunity to stop them before the attacks. Targeted data collection provides a rich environment of information to figure out what attacks are going to happen, and that is cheaper and more effective than bulk collection - and of course less intrusive.

If we did everything through analysis and collection smartly, in a targeted way, we'd give privacy to everybody in the world because you don't take in their data. Referring to the 9/11 attacks, Binney suggested that targeted surveillance rather than bulk surveillance could have stopped the whole tragedy from happening. All of these people were in knowledge bases already. If they'd taken a targeted approach from the beginning, keeping the data finite, the analysts would have found the threats," he claimed.

Figures go on to show that the total number of terrorist attack plots in united states post 9/11 are close to almost 60, approx. 31 of which were unsuccessful due to the inception based on intelligence using the conventional methods rather than intel from general surveillance.

With the inception of these programs for terrorist surveillance, they soon turn into mass surveillance projects that have been misused by authorities countless times in the past. For an example since the 9/11, law enforcement had apprehended over thousands of individuals based on ethnic profiling and guilt by association, none of which were later convicted of any crimes or conspiracy.

Security agencies often justify surveillance by stating that if you have nothing to hide, you have nothing to fear…. but this reasoning only creates a state of oppression which itself undermines the essence of freedom and democracy. We have seen in the past that governments have used these methods to oppress the freedom of speech and expression along with suppression of government opposition in countries like Turkey, Bahrain and Iran, among many others. None of which are helping us fight terrorism.

The central argument disseminated is that privacy and freedom from government surveillance is the fundamental premise of individual determination: the right to choose, to think, to ask and to pursue on our own terms – free from recorded, analysed and interpreted thoughts.

Don't agree? okay, I want you to voluntarily give me all of your passwords, a copy of all your text messages, work and personal emails, your browsing history together with your bank and medical records just so that I can have a quick 'gander' through them.

I'm not telepathic, but I already guess the nuanced response: 'err…no.' That's none of your business.

Exactly!

So why do you continue to voluntarily give the government, or more exactly individual security agents sitting at their desks. The problem doesn't just end there. These scenarios and techniques are not just limited to state spy agencies. We have seen in the past how hackers and other foreign government sponsored agencies have been able to retrieve and steal sensitive data from them, making it publicly available.

One key scenario that played out in the recent times was the request for backdoor to defeat the encryption in iPhone by NSA after the terror attack in San Bernardino, although Apple rejected the request citing that it would compromise the privacy of billions of law abiding citizens worldwide. Nevertheless, what turned out to be a major concern was that few weeks later NSA admitted that they hacked the iPhone anyway, this along with the existing capabilities of spy agencies by which they can covertly turn on the microphone / Camera of an iPhone or Android device, capture call logs, text messages and even get the location of the phone (via a technique known as Implant – Dropout Jeep) or access the data and camera of your laptop. This means that someone sitting in a dark room somewhere can have the ability to look at your 12 year old daughter in her room, without you having any control to stop it. That is a little farfetched but very much possible. This is not just limited to the NSA, but also to other advanced cyber security agencies from Israel, UK, Russia and China. Even countries like Norway have also thrown their hats in the ring. A number of the important state institutions like the Prime Minister's office, the Ministry of defence, the Parliament and the Central Bank are under constant watch. Ministers, state secret agencies, members of parliament, state officials, business executives and other essential staff engaged in protecting the nation's security, the military are all under the observation.

But passers-by are hardly aware of the following Constantly fact: In several locations someone has installed secret transmitters wooden wine probably behave like fake mobile base stations. These so called IMSI catchers can monitor all mobile activity in the vicinity. The people who run these surveillance equipment march in principle monitor every person moving in and out of the parliament building, the government offices or other institutions in the area. They can also select certainties person for eavesdropping and collecting data from their smartphones and laptops.

Not far from the chaos, India on the other hand has created the Central Monitoring System, abbreviated to CMS, which is a centralized telephone interception provisioning system installed by the Centre for Development of Telematics (C-DOT), an Indian Government owned telecommunications technology development centre, and operated by Telecom Enforcement Resource and Monitoring (TERM) Cells. The CMC system is going to be set up in each major state collocated with the TERM Cells. Telecom operators in India are required by law to give access to their networks to law enforcement agencies. The interconnection between LEA and Telecom Operators prior to CMS.

The interconnection between TERM Cell, LEA and Telecom Operators post CMS setup Government has set up the Centralized Monitoring System (CMS) to automate the process of Lawful Interception & Monitoring of telecommunications. CMS has got the approval from government. Cabinet Committee on Security has approved the project of CMS with government funding of Rs 400 Crores. Pilot trials have been completed and the system is anticipated to be progressively operationalized from the endof the financial year. Not to mention the IT Act of 2008 – Section 69 and the NATGRID. The need of the hour is not more collecting random data, building backdoors into software and acquiring keys to break encryption, but actionable intelligence being derived from the data that is available based on significant inputs. The erosion of privacy with increase in mass surveillance has not been the silver bullet we believed it would be.

Creating master keys to monitor billions of cell phones is not the same as targeted inspection. Surprisingly most countries already have various laws the place for targeted surveillance, instead what is needed is better application of the present laws instead of newer and stricter ones that undermine our freedom. Let us not out of fear destroy what we are most proud of – our democracy, liberty and our core fundamental rights to privacy and security. Amid this wildfire the only sight of relief is that they so far have been extensively done only on a targeted basis and not on the mass public, but what's the assurance that in future the tables won't be turned on us.

Let’s face it the game is rigged. We can’t beat them but we don’t have to lose to them ether maybe there is a way that we can stop them winning They are the ever silent observer, watching us at all times even when we can’t see them. Listening in our conversations, they might be a step ahead of us, but we can counter it….and maybe in the process outgrow the problem itself.

Cyber Security

Dr. T. Subbulakshmi
Professor of VIT University

Today's Internet is the fastest developing infrastructure and the most recent advancements in cloud computing, social networking and mobile computing has made internet as the integral part in every day's life. Most of the transactions are online and all the product vendors are hosting their website in the cloud for higher reachability. The internet infrastructure is based on a distributed and multi-user architecture where security threats imposes the major risk in providing cyber security. Security concerns are raising with growth in adoption of current IT deployment models. Inspite of the flexibility, resource availability and scalability of the recent IT technology there is always security and privacy risks associated with delivery of critical services. The other challenges include

- Application constraints due to the shift in operational paradigm.
- Licensing and portability
- Data confidentiality, security and accessibility in dynamic environment.
- Loss of control over servers and other data centers affects the IT/ITES sector.

The cyber space is facing new threats and the hackers are utilizing most sophisticated tools to launch attacks against the internet infrastructure. It disrupts the normal operation of the critical services deployed in the internet servers. The biggest attacks of 2016 [1] are listed as below.

- Major denial of service attack against the Ukraine power grid.
- Ransomware attacks against business competitors.
- Ransomware attacks against data storage with the patient records.
- Tax fraud and Phishing
- Poor authentication and data theft
- Man in the cloud attacks
- SSL attacks

Assocham-Mahindra SSG report says that cyber-crimes are growing at the greater level in India and it is has revealed some shocking figures. The over utilization of the internet is highly dangerous and the study clearly investigates the increase in the Cyber Crimes enormously. According to the statistics, the number of Cyber Crime in India registered is 13,301 in 2011, 22,601 in 2012, 71,708 in 2013, 1,49,254 in 2014 and 55-60 percent increase in 2015 as shown in Figure 1[2].

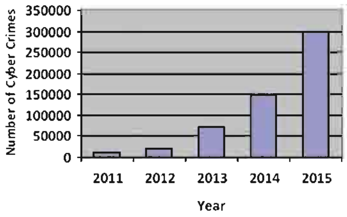


Figure : Cyber Crimes Growth in India

The statistics have provided proven facts showing the significance of Cyber Crimes in India. The country has witnessed 107% of the annual growth rate in the amount of cases that has been recorded in previous years. It addition to this, the report states that mobile devices have been evolved as the vital part in the Cyber Crimes because majority of the transactions are carried out using the mobile applications. The impact of the cyber attacks in India is manifold such as financial loss, loss of reputation, unavailability of the services, threatening to the physical safety of the personnel and individual asset. The Cyber Crime report has illustrated 47% of the business disruption, 49% repudiation loss to the to the institution. 65% report the e-mail servers are possible victim of attacks and 46% predict end machines are the potential victim. Financial and pharmaceutical industries are also found be the target [3].

The major challenge is to how to stop the attacks and provide a secure cyber space. Government is taking sincere efforts to detect the cyber-attacks and block the source after the onset of the first Counterfeit Access Device and Computer Fraud and Abuse Act in 1984. Like other countries, India is also facing cyber risks and other security challenges since the day it has emerged as the one of the biggest market in Asia. The gap between the time the attack initiated and till the original source is tracked down is where many dreadful ransomware attacks happen making the detection tedious.

The attackers use one or more computers to hack into the critical system to compromise privileged data. He/she might also use phishing attacks, malware attacks or Trojans to carry out identity theft. The only thing that an internet user can do is to protect himself using strong authentication and access controls mechanisms. Staying cautious, informed and vigilant in observing malicious e-mails, encrypting personal information, strong passwords, and updating anti-virus software can be the preventive measures.

Cyber security awareness must be created across universities and the current technology and practical solutions to the security shall be shared in an open community constituting the professionals of government, public/private sectors and academia. The universities should bring proper syllabus for cyber security in collaboration with the cyber security industry so that the finishing school students are directly deployed at the live security projects. The skillsets of the candidates will be enhanced us-ing certification programs and research projects to empower them with innovative ideas and problem solving skills in the cyber security world. Also, the students should be facilitated with workshops, symposium, training programs, scholarships, internships at research labs, research projects, industryacademia projects, certification and semester abroad programs.

The government, IT Industry and academia can create more awareness for students in cyber security and best practices that offer remarkable career and also solves the skill deficiency in the domain. This following are the key aspects that are to be considered for brining global awareness.

- PhD & MS programs
- Working groups with government, IT and academia
- Security projects for societal benefits
- Research labs connecting the leading institutions and government agencies
- Risk, compliance and policy framework

Worldwide Cloud Security

Ilyas Mohamed Rajak
Sr.Network and Security Expert,
Member of National Cyber Defence Research Centre (NCDRC)

Cloud services security threats around the world. Nowadays major companies moved to cloud services at the same time companies face security threats while using cloud services. Shared technology posture a significant threat to cloud computing. Cloud service providers share infrastructure, applications and platforms. If vulnerability increases in any of these layers, it affects everyone. A single misconfiguration or vulnerabilities can lead to a compromise across an entire provider's cloud. CSA (Cloud Security Alliance) warned, due to industry applies whether the organization is trying to migrate to the cloud or working with another company in the cloud. For example, organizations that fail to inspect a contract may not be aware of the provider's responsibility in case of data loss or breach.

Operated and architectural issues arise if a company's development team lacks familiarity with cloud technologies as applications are deployed to a particular cloud. The CSA reminds organizations they must perform extensive due industry to understand the risks they assume when they subscribe to each cloud service.

I just shared my experience and explain about some of top most threats in cloud services.

Malicious insiders

The insider threat has many faces: employee, system admin, contractor or business partner. The malicious program varieties from data theft to pay back. In a cloud scenario, a hell-bent insider can destroy whole infrastructures or operate data's. Systems that depend only on the cloud service provider for security. The CSA mentions that organizations control the encryption process and keys, separating duties and minimizing access given to users. Effective logging, monitoring, and auditing admin activities are also dangerous. As the CSA notes, it's easy to misconstrue a bungling attempt to perform a routine job as "malicious" insider activity. Example is an admin who accidentally copies a delicate customer database to a publicly accessible server. Good training and management to prevent such mistakes becomes more critical in the cloud, due to greater potential exposure.

Account Stealing

Fraud, phishing and software exploits are silent successful, and cloud services add a new measurement to the threat because attackers can snoop on activities, operate transactions, and modify data's. Attackers may also be able to use the cloud application for performance another attack very easily. Shared protection plans can contain the damage experienced by a breach. Companies should ban the sharing of account credentials between users and services, as well as enables multifactor authentication schemes anywhere available. Accounts, even service accounts, should be monitored so that every transaction can be traced. As per CSA says the key is to protect account credentials from being stolen.

APT Issue in Cloud

Advanced Persistent Threats (APTs) "parasitical" forms of attack. APTs penetrate systems to establish a position, intellectual property over an extended period of time. APTs typically move across through the network and the mixture in with normal traffic, so they're difficult to detect. The major cloud providers apply advanced techniques to prevent APTs from infiltrating their infrastructure, but customers need to be as hard working on detecting APT compromises in cloud accounts as they would in on-premises systems. Mutual points of entry include spear phishing, direct attacks, USB drives with malware, and compromised third-party networks. The CSA recommends training users to recognize phishing techniques. Frequently reinforced awareness programs keep users alert and less likely to be tricked into letting an APT into the network and IT departments need to update of the latest advanced threats and attacks. It should be required training for all IT department members like security controls, process management, incident response plans. Companies should consider these training costs against the possible economic damage exacted by successful APT attacks.

Data Breaches

Cloud settings face many of the same threats as traditional corporate networks, but due to the huge amount of data stored on cloud servers, providers become a gorgeous target. The severity of potential damage inclines to depend on the sensitivity of the data exposed. Exposed personal financial information tends to get the headlines, but breaches involving health information, trade secrets, and intellectual property can be more shocking. When a data breach occurs, companies may experience penalties, or they may face complaints or criminal charges. Breach investigations and customer notifications can rack up significant costs. Indirect effects, such as brand damage and loss of business, can impact organizations for some years. Cloud providers typically organize security controls to protect their settings, but ultimately, organizations are responsible for protecting their own data in the cloud. The CSA has recommended organizations to use multifactor authentication and encryption to protect against data breaches. In every organization should prevent own network. ATP (Advanced Threat Production) it should be placed on customer inside the network (LAN) , ATP will help to prevent threats to the local network.

Credentials Sliced

Data breaches and other attacks often happened and result was authentication, weak passwords, and poor significant. Companies are often fighting with identity management as they try to allocate permissions appropriate to the user's job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization. Multifactor authentication, one-time passwords, phone-based authentication and smartcards protect cloud services because they make it harder for attackers to log in with stolen passwords. The Anthem breach (https://www.anthemfacts. com/) which exposed more than 80 million customer records was the result of stolen user credentials. Anthem had failed to deploy multi factor authentication, so once the attackers obtained the credentials, attackers was taken everything. Some Developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing sources such as GitHub. ISP blockage. On December 17, 2014, the Indian Department of Telecom issued an order to ISPs to block 32 websites. The notice was made public on December 31, 2014 and it included GitHub, GitHub's Gist, Vimeo, the Internet Archive, and various paste bin services.

The CSA said, Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary. They also need to be rotated occasionally to make it harder for attackers to use keys they've obtained without permission. Organizations planning to merge identity with a cloud provider need to understand the security procedures the provider uses to protect the identity platform. Unifying identity into a single source has its risks. Organizations need to consider the trade-off of the expediency of unifying identity against the risk of having that repository become an extremely high-value target for attackers.

Cloud Service Exploitation

Cloud services can be seized to support wicked activities, such as using cloud computing resources to break an encryption key in order to present an attack. Other examples, including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content. Providers need to identify these types of abuse such as inspecting traffic to recognize DDoS attacks and offer tools for customers to monitor the health of their cloud environments. Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service exploitation can still result in service availability issues and data loss.

DOS Attacks

Denial of Service as it is often truncated is a malicious attack on a network. This attack is basically designed to bring a network to its laps by flooding it with useless traffic. Systems may slow to a crawl or simply time out. DOS attacks consume large amounts of processing power, a bill the customer may eventually have to pay. While high-volume DDoS attacks are very common, organizations should be aware of unequal, application-level DOS attacks, which target Web Servers and database vulnerabilities. CSA said, Cloud providers incline to be better composed to handle the DOS attacks than their customers. The key is to have a plan to mitigate the attack before it occurs, so admin has access to those resources when they need them. Detection systems, applying the concept of least privilege, network segmentation, and repairing shared resources.

Bitcoin Forensics

Amandeep Singh Chawla, Nitya Shukla, Dr. Shubha Jain
Axis Colleges, Kanpur, Email: shubhajain@axiscolleges.in

Abstract: Bitcoin is a cryptocurrency and a digital payment system invented by an unknown programmer or a group of Programmers who are totally anonymous till date. Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

Keywords—**Forensics, Bitcoins, Digital Information, Investigation, Evidence, Artefacts**

1. Introduction

Cryptocurrencies such as Bitcoin among private users and Black hat Hackers have opened a new avenue of research in the field of Digital Forensics. Since creation of Bitcoin since 2008 the Cryptocurrencies have begun to make presence in the world of ecommerce. Cryptography serves as the underlying foundation for Bitcoin which provides the benefits of Confidentiality, integrity, and authentication. Thus by above three factors keeping in mind Bitcoin have payment freedom, security, low fees and fewer risks for merchants.

This research paper seeks to find what forensic artifacts are recoverable from a user's system with Bitcoin wallet applications installed and actively used. As well as recover any evidence of Bitcoin mining that would be present on a user's system due to the use of such software or applications.

2. Role of Cryptocurrency in Bitcoin

Cryptocurrency, by definition is a type of digital currency based on cryptography, or the process of converting plaintext into cipher text, thus making readable text no decipherable. The use of cryptography in the transfer of data has four main objectives: Confidentiality, Integrity, Non repudiation, Authentication.

3. How Bitcoin Works

In order for a consumer to begin interacting and conducting transactions utilizing Bitcoin, he or she must first download and setup a Bitcoin wallet. A Bitcoin wallet can show the total balance of all Bitcoins it controls and let a user pay a specified amount to a specific person, just like a physical wallet. Once the wallet is installed and configured, an address is generated which is similar to an e-mail or physical address, in that it provides other users a numerical location to send Bitcoins to. In addition, the wallet contains a user's private key, which allows for the spending of the Bitcoins, which are located in the block chain [1].

4. Bitcoin Artifacts

When the user tries to get involved in Bitcoins, the first step they need to do is to set up a bitcoin wallet. The main purpose of this wallet is to do transactions like sending and receiving bitcoins this wallet acts same like other wallets like Paytm and all. Although there are numerous Bitcoin wallet software applications out in the market, the most notable is Bitcoin-Qt because it is the original Bitcoin P2P open source software created by the creator of Bitcoin. It is not only a Bitcoin wallet, but it also contains the public ledger that lists every Bitcoin transaction in the system [3].

Forensics Approach

On examining suspect's hard disk the following information in the Bitcoin Qt Wallet may be be extracted that the suspect was using:

Blocks: The "blocks/index subdirectory" is a database that contains metadata about all known blocks, and where to find them on disk. Without this, finding a block would be very slow. – This subdirectory contains block chain data and contains a "blk.dat" file and a "blocks/index" subdirectory. The "blk.dat" stores actual Bitcoin blocks, in network format, which is dumped to disk in raw format.

Databases: This directory contains database journaling files.

Chainstate: It is a database with a compact representation of all currently unspent transactions Chainstate: It is a database with a compact representation of all currently unspent transactions

5. Additional Discovered Files

Lock File: A file whose work is to lock/protect the database from an unauthorized source.

Debug.log: It is the Bitcoin's extensive logging file.

Peers.dat: This file is storage for peer information to make a reconnect easier. It also utilizes a Bitcoin specific file format, which is unrelated to any other database system.

Wallets.dat: This file is storage for keys, transactions, metadata, and options relating to Bitcoin.

In addition to the evidentiary artifacts that can be located on the user's computer, investigators can also locate artifacts by conducting an in-depth examination of the block chain. Recall that the block chain is a public record of Bitcoin transactions in chronological order and verifies the permanence of Bitcoin transactions. Thus, if an investigator has the Bitcoin private key of the suspect, they can search for that particular key on the Block chain to trace the purchases to other potential suspects [1].

6. Building a case with Bitcoin Artifacts

In forensics a case is meant to be successful only when a case involving digital evidence depends upon the content of the case as well as the knowledge, experience, expertise and curiosity of the investigator in charge of the case.

In addition to a well-rounded investigator, the success of a digital case rests on a foundational model that provides phases by which the investigator can progress through. The Investigation Process for Digital Forensic Science model is the foundation for a successful digital investigation. This model contains six key phases [7]:

1. Identification

2. Preparation

3. Collection

4. Examination

5. Analysis

6. Presentation

6.1 Brief Steps to Perform Bitcoin Forensics

In order to perform forensics analysis on bitcoin the foremost step is collection phase in which the investigator needs to search for document and collect any object or data that could potentially contain digital evidence. Since Bitcoin transactions occur via network connection, an investigator should seize any physical object that can be connected to Internet. These objects include: Cell phones, iPod, laptops or desktop computers. During the Identification and observation phases if the investigator finds that the suspect computer is one he must take the live imaging of the whole system especially the system's physical memory because many type of evidence could be available in the volatile memory relating to Bitcoin these types of evidence may include:

- Running Bitcoin processes and services
- System information
- Information about logged in users
- Registry information
- Remnants of chats, communications in social networks and Bitcoin forums
- Recent Bitcoin web browsing activities
- Recent communications via webmail systems involving Bitcoin
- Information from cloud services
- Decryption keys for encrypted volumes mounted at the time of the capture
- Running Bitcoin malware/Trojans

Upon collecting the evidence, either physically or through extraction or imaging, the investigator can now begin the process of examining the data and assigning the level of importance of each individual piece. Although the Bitcoin artifacts reside on the suspect's hard drive and can be recovered using robust forensic tools such as Access Data's Forensic Toolkit or EnCase, Internet Evidence Finder permits the investigator to view just the Bitcoin artifacts [1].

6.2 Alternatives for Investigator

Two different options are available that enable an investigator to recover the Bitcoin evidentiary artifacts utilizing Internet Evidence Finder.

- The first option is that the investigator can export the entire Bitcoin file folder from the suspect's drive and have Internet Evidence Finder analyze just that folder for Bitcoin artifacts
- The second option is that the investigator can point Internet Evidence Finder at the entire image of the suspect's drive and the program will return not only the Bitcoin artifacts, but also Internet and chat history, e-mail and web searches.

7. Bitcoin Forensics Artifact Examination

In order to do an examination on bitcoin Artifact we need a designated computer with a fresh installation of Windows 7, Multibit, Bitcoin-QT, Bitminter and a basic USB ASIC BITCOIN mining rig.

A Bitcoin mining rig is typically a computer system used for mining bitcoins. At the conclusion of the testing process, an image of the system's RAM and hard drive were examined with Encase 6.19.9 and Internet Evidence Finder 6.1. The goal of the examination is to see the interaction between the Bitcoin mining software and wallet, with the operating system, registry, and RAM. By analyzing each of those areas in depth with forensic software, the forensic community will gain a working knowledge of the Bitcoin forensic artifacts that are present and their importance in an investigation [6].

7.1 Hardware Setup

The below listed items are the specific items of hardware that were used during the experiment. The 120 GB hard drive was wiped and a fresh installation of Windows 7 was installed to ensure a clean experimental environment. The individual ASIC Mining drives were individually plugged in to the USB hub that was then plugged in to the Gateway laptop via USB connection [6].

- Gateway laptop ML6720 with power supply
- 120 GB Western Digital hard drive
- (4) USB ASIC Mining drives
- 7 port USB hub
- USB powered cooling fan
- 32 GB USB thumb drive

7.2 Tools Used

During the Experiment, several tools are to be used in order to maintain a running Bitcoin mining computer as well as populate the system's file and registry with Bitcoin Evidently Artifacts. Each of the tools utilized in the experiment had a specific purpose and were chosen based on their platform design and ease of use. Under given are the tools used [1]:

- Bitminter
- Multibit
- Bitcoin-qt
- Tableau Imager
- EnCase

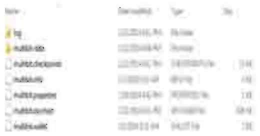
8. Testing Results

The second phase of testing involved configuring the test system to mine and interact with Bitcoins. The first step in this process was to install the Bitcoin wallets that would house the Bitcoin transactions, addresses, and private keys utilized during the testing. The Multibit Bitcoin wallet application was downloaded in the test system’s Internet Explorer web browser and saved in the Downloads folder of the test system.

The Multibit application was located in the Downloads folder and installed by double-clicking on the “multibit-0.5.16-windowssetup.exe” file. This action installed the application with the default settings in the following location “C:\Program Files\MultiBit-0.5.16.” Upon successful installation of the Multibit Bitcoin wallet, the application was opened and the Bitcoin address associated with the wallet was:

“1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6.”

In addition to verify the address of the Multibit wallet, the folder structure of the installation was documented for reference when conducting further examination with EnCase and Internet Evidence Finder. Figure 1 given depicts the folder structure of the Multibit wallet application on the test system.



Name	Date modified	Type	Size
log	[illegible]	[illegible]	
[illegible]	[illegible]	[illegible]	
multibit.checkpoints	[illegible]	[illegible]	[illegible]
multibit.info	[illegible]	[illegible]	[illegible]
multibit.properties	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
multibit.wallet	[illegible]	[illegible]	[illegible]

Fig.: Folder structure of the Multibit wallet application

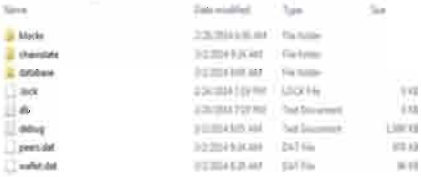
In order to gain an understanding of the various artifacts resulting from different Bitcoin wallets, Bitcoin-Qt was downloaded and installed via Internet Explorer to the test system as an additional wallet software application. The Bitcoin-Qtapplication was installed with the default settings.

After noting the Bitcoin address associated with the wallet as [3]:

"14igLoRYLjmqc9H5ZSxWqBvdNT3Ro1QeUJ,"

Was then labeled as "Suspect" and saved within the Bitcoin-Qt wallet**.**

To verify the address of the Bitcoin-Qt wallet, the folder structure of the installation was documented for reference when conducting further examination with EnCase and Internet Evidence Finder. Figure 2 depicts the folder structure of the Bitcoin-Qt wallet application on the test system.



Name	Date modified	Type	Size
blocks	[illegible]	File folder	
chainstate	[illegible]	File folder	
database	[illegible]	File folder	
.lock	[illegible]	LOCK File	[illegible]
db	[illegible]	Text Document	[illegible]
debug	[illegible]	Text Document	[illegible]
peers.dat	[illegible]	DAT File	[illegible]
wallet.dat	[illegible]	DAT File	[illegible]

9. Transactions Details Extracted

After installing and configuring both of the Bitcoin wallets, an account was created utilizing the G-Mail address of "forensicminer@gmail.com" at website "https://bitminter.com." The account was created in order to run the software application from the test system and to store pertinent information such as Bitcoin addresses and worker identities. Upon signing on to the Bitminter mining pool for the first time, all of the default account settings were left.

With the Multibit and Bitcoin-Qt wallets installed and the Bitminter account created, the Bitcoin mining rig was configured. For the testing environment, the rig consisted of four ASIC Block Erupters plugged in to a seven-port USB hub. An ASIC Block Erupter is a tool utilized to mine Bitcoins that uses an Application Specific Integrated Chip and mines at 330 mega hashes a second (MH/s).

Internet Explorer was used to visit the website https://bitminter.com, logging in with the username of "forensicminer@gmail.com," and clicking on the "Start Engine" button that launched the Bitminter control panel and showed the miners actively working.

While the test system was actively mining for Bitcoins and the Bitminter account had accrued enough Bitcoins in order to conduct a transaction, three separate transactions were made from the "forensicminer" Bitminter account to the address of the Multibit wallet as well as the Bitcoin-Qt wallet.

The transactions occurred on separate dates and times and the respective wallet application logged each. Figure 3 depicts the transactions conducted within the Multibit wallet on the dates of January 25, February 8, and February 28.

Fig.3: Transactions conducted within the Multibit wallet on Jan 25, Feb 8, and Feb 28

The figure 4 depicts the transactions conducted within the Bitcoin-Qt wallet on the dates of February 28, 2014

It is important to note that the address listed as "Suspect" is actually the address of the Multibit wallet [3],

"1FdhjMV8s2kzfAdU6TXVS35xkCGcbxAiM6."

Date	Type	Address	Amount
✓ [illegible]	Sent to	Suspect	[illegible]
✓ [illegible]	Received with	[illegible]	[illegible]
✓ [illegible]	Received with	[illegible]	[illegible]

Fig.4: Transactions conducted within the Bitcoin-Qt wallet on February 28, 2014

Glossary

Access Control

Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL)

A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service

A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access

Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Matrix

An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting

Account Harvesting is the process of collecting all the legitimate account names on a system.

ACK Piggybacking

ACK piggybacking is the practice of sending an ACK inside another packet going to the same destination.

Active Content

Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors

Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standard (AES)

An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm

A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Applet

Java programs; an application program that uses the client's web browser to provide a user interface.

Arpanet

Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetric Cryptography

Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric Warfare

Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

Auditing

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Authentication

Authentication is the process of confirming the correctness of the claimed identity.

Authenticity

Authenticity is the validity and conformance of the original information.

Authorization

Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System

One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Availability

Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

Backdoor

A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

Bandwidth

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

Banner

A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

Basic Authentication

Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

Bastion Host

A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

BIND

BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

Biometrics

Biometrics use physical characteristics of the users to determine access.

Bit

The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbolsÑ"0" (zero) and "1" (one) - that are used to represent binary numbers.

Block Cipher

A block cipher encrypts one block of data at a time.

Boot Record Infector

A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

Border Gateway Protocol (BGP)

An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

Botnet

A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.

BOTS

Programs that are installed covertly on a user's system which allows the attacker to remotely control the targeted computer through a communication channel such as Internet relay chat(IRC), peer-to-peer (P2P), or HTTP.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

Broadcast

To simultaneously send the same message to multiple recipients. One host to all hosts on network.

Broadcast Address

An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

Browser

A client computer program that can retrieve and display information from servers on the World Wide Web.

Brute Force

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Business Continuity Plan (BCP)

A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Business Impact Analysis (BIA)

A Business Impact Analysis determines what levels of impact to a system are tolerable.

Byte

A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.

Cache

Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Cache Cramming

Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning

Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Call Admission Control (CAC)

The inspection and control all inbound and outbound voice network activity by a voice firewall based on user-defined policies.

Carnivore Software

Software that uses packet sniffing at the ISP level to monitor data flow through ISPs. Carnivore is designed to monitor email and electronic communications. It is known as a customized packet sniffer which can be used to monitor all of the internet traffic of a particular user.

Cell

A cell is a unit of data transmitted over an ATM network.

Certificate-Based Authentication

Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

CGI

Common Gateway Interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

Chain of Custody

Chain of Custody is the important application of the Federal rules of evidence and its handling.

Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

Checksum

A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

Cipher

A cryptographic algorithm for encryption and decryption.

Ciphertext

Ciphertext is the encrypted form of the message being sent.

Circuit Switched Network

A circuit switched network is where a single continuous physical circuit connected two end-points where the route was immutable once set up.

Client

A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Cloud Bursting

A process where a service provided by a private cloud can automatically access and use resources from a public cloud when it needs to ramp up and handle peak demand.

Computer-related forgery

Computer-related forgery involves the unauthorized creating or altering or manipulation of stored data so that they acquire a different evidentiary value in the course of legal transactions which relies on the authentically of information contained in the data.

Computer-related fraud

The causing of loss of property to another person by manipulating or altering, deleting any computer data, with fraudulent or dishonest intention to gain economic benefit without right, is considered as computer-related fraud.

Collision

A collision occurs when multiple systems transmit simultaneously on the same wire.

Competitive Intelligence

Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

Computer Emergency Response Team (CERT)

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Network

A collection of host computers together with the sub-network or inter-network through which they can exchange data.

Confidentiality

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Configuration Management

Establish a known baseline condition and manage it.

Cookie

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent clientside state information for HTTP-based applications, retrieving the state information in later
connections.

Corruption

A threat action that undesirably alters system operation by adversely modifying system functions or data.

Cost Benefit Analysis

A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

Counter Measure

Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ counter measures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.

Covert Channels

Covert Channels are the means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.

Cron

Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

Crossover Cable

A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

Cryptanalysis

The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

Cryptographic Algorithm or Hash

An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cut-Through

Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

Cyclic Redundancy Check (CRC)

Sometimes called “cyclic redundancy code.” A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

Daemon

A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

Data Aggregation

Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

Data Custodian

A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data Encryption Standard (DES)

A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Interference

Data interference means damaging, deletion, deterioration, alteration or suppression of computer data, intentionally and without a right to do so and input of malicious codes, such as viruses and Trojan horses.

Data Mining

Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

Data Owner

A Data Owner is the entity having responsibility and authority for the data.

Data Preservation

Data preservation means keeping data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate.

Data Retention

Data retention means the accumulation of data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate.

Data Warehousing

Data Warehousing is the consolidation of several previously independent databases into one location.

Datagram

Datagram's or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

Day Zero

The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one"-> day at which the patch is made available).

Decapsulation

Decapsulation is the process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

Decryption

Decryption is the process of transforming an encrypted message into its original plaintext.

Deep Packet Inspection

Interception of online data from emails, internet phone calls, as well as images on social networking sites, such as Facebook and Twitter. Every digitized packet of online data is intercepted, de-constructed, examined for keywords and then reconstructed within a few milliseconds.

Defacement

Defacement is the method of modifying the content of a website in such a way that it becomes "vandalized" or embarrassing to the website owner.

Defence In-Depth

Defence In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

Denial of Service

The prevention of authorized access to a system resource or the delaying of system operations and functions.

Dictionary Attack

An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication

Digest Authentication allows a web client to compute MD5 hashes of the password to prove it has the password.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Envelope

A digital envelope is an encrypted message with the encrypted session key.

Digital Signature

A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Digital Signature Algorithm (DSA)

An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Standard (DSS)

The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Disassembly

The process of taking a binary program and deriving the source code from it.

Disaster Recovery Plan (DRP)

A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

Discretionary Access Control (DAC)

Discretionary Access Control consists of something the user can manage, such as a document password.

Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Distance Vector

Distance vectors measure the cost of routes to determine the best route to all known networks.

Distributed Scans

Distributed Scans are scans that use multiple source addresses to gather information.

Domain

A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Hijacking

Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name

A domain name locates an organization or other entity on the Internet. For example, the domain name “www.nationalcybersafety.com” locates an Internet address for “nationalcybersafety.com” and a particular host server named “www”. The “com” part of the domain name reflects the purpose of the organization or entity (in this example, “commerce”) and is called the top-level domain name.

Domain Name System (DNS)

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-toremember “handle” for an Internet address.

Due Care

Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

Due Diligence

Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

DumpSec

DumpSec is a security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

Dumpster Diving

Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

Dynamic Link Library

A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

Dynamic Routing Protocol

Allows network devices to learn routes. Ex. RIP, EIGRP Dynamic routing occurs when routers talk to adjacent routers, informing each other of what networks each router is currently connected to. The routers must communicate using a routing protocol, of which there are many to choose from. The process on the router that is running the routing protocol, communicating with its neighbour routers, is usually called a routing daemon. The routing daemon updates the kernel's routing table with information it receives from neighbour routers.

Eavesdropping

Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

Echo Reply

An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request

An echo request is an ICMP message sent to a machine to determine if it is online and how long traffic takes to get to it.

Egress Filtering

Filtering outbound traffic.

Emanations Analysis

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Encapsulation

The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Ephemeral Port

Also called a transient port or a temporary port. Usually is on the client side. It is set up when a client application wants to connect to a server and is destroyed when the client application terminates. It has a number chosen at random that is greater than 1023.

Escrow Passwords

Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

Ethernet

The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

Event

An event is an observable occurrence in a system or network.

Exponential Backoff Algorithm

An exponential backoff algorithm is used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

Exposure

A threat action whereby sensitive data is directly released to an unauthorized entity.

Extended ACLs (Cisco)

Extended ACLs are a more powerful form of Standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

Extensible Authentication Protocol (EAP)

A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

Exterior Gateway Protocol (EGP)

A protocol which distributes routing information to the routers which connect autonomous systems.

False Rejects

False Rejects are when an authentication system fails to recognize a valid user.

Fast File System

The first major revision to the Unix file system, providing faster read access and faster (delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fast Flux

Protection method used by botnets consisting of a continuous and fast change of the DNS records for a domain name through different IP addresses.

Fault Line Attacks

Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP)

A TCP/IP protocol specifying the transfer of text or binary files across the network.

Filter

A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Filtering Router

An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

Fingerprinting

Sending strange packets to a system in order to gauge how it responds to determine the operating system.

Firewall

A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Flooding

An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly.

Forest

A forest is a set of Active Directory domains that replicate their databases with each other.

Fork Bomb

A Fork Bomb works by using the fork() call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Form-Based Authentication

Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Forward Lookup

Forward lookup uses an Internet domain name to find an IP address.

Forward Proxy

Forward Proxies are designed to be the server through which all requests are made.

Fragment Offset

The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

Fragmentation

The process of storing a data file in several “chunks” or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Frames

Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that “frame” the data.(Some control frames contain no data.)

Framing

An act of fraudulent display of contents of one website within another person’s website with the purpose of making the user believe that he is actually viewing the former’s website. Third party content is used intentionally within the frames of the website.

Full Duplex

A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

Fully-Qualified Domain Name

A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain name.

Fuzzing

The use of special regression testing tools to generate out-of-spec input for an application in order to find security vulnerabilities.

Gateway

A network point that acts as an entrance to another network.

Gethostbyaddr

The gethostbyaddr DNS query is when the address of a machine is known and the name is needed.

Gethostbyname

The gethostbyname DNS quest is when the name of a machine is known and the address is needed.

GNU

GNU is a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. The GNU project was started I n 1983 by Richard Stallman and others, who formed the Free Software Foundation.

Gnutella

An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

Hacking

Gaining of unauthorized access to the data stored in computer systems. Hacking is an intentional act of breaking into a computer system with the objective of stealing data that can be used for purposes of identity theft or other fraud.

Hactivism

Hactivism is a term which combines the concepts of 'hacking' and 'activism' which means the hacking into the computer system of another for a social or a political purpose.

Hardening

Hardening is the process of identifying and fixing vulnerabilities on a system.

Hash Function

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Hash Functions

(cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHAL.

Header

A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack

A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honey Client

see Honeymonkey.

Honey pot

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Honeymonkey

Automated system simulating a user browsing websites. The system is typically configured to detect web sites which exploit vulnerabilities in the browser. Also known as Honey Client.

Hops

A hop is each exchange with a gateway a packet takes on its way to the destination.

Host

Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

HTTP Proxy

An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

HTTPS

When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Hub

A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

Hybrid Attack

A Hybrid Attack builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid Cloud

A hybrid cloud is a composition of two or more clouds (private or public) that remain separate cloud entities but share certain technology which permits interoperability.

Hybrid Encryption

An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Hyperlink

In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by colour or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link.

Hypertext Mark-up Language (HTML)

The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

Hypertext Transfer Protocol (HTTP)

The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

Identity

Identity is whom someone or what something is, for example, the name by which something is known.

Incident

An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling

Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incremental Backups

Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

Inetd (xinetd)

Inetd (or Internet Daemon) is an application that controls smaller internet services like telnet, ftp, and POP.

Inference Attack

Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

Information Warfare

Information Warfare is the competition between offensive and defensive players over information resources.

Ingress Filtering

Ingress Filtering is filtering inbound traffic.

Input Validation Attacks

Input Validations Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

Integrity

Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Integrity Star Property

In Integrity Star Property a user cannot read data of a lower integrity level then their own.

Internet

A term to describe connecting multiple separate networks together.

Internet Control Message Protocol (ICMP)

An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Engineering Task Force (IETF)

The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

Internet Message Access Protocol (IMAP)

A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for or extension to the Post Office Protocol (POP). It is defined in RFC 1203 (v3) and RFC 2060 (v4).

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec)

A developing standard for security at the network or packet processing layer of network communication.

Internet Standard

A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Interrupt

An Interrupt is a signal that informs the OS that something has occurred.

Intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intrusion Detection

A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address

A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Flood

A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP Forwarding

IP forwarding is an Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Spoofing

The technique of supplying a false IP address.

ISO

International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

Issue-Specific Policy

An Issue-Specific Policy is intended to address specific needs within an organization, such as a password policy.

ITU-T

International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations."

Jitter

Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.

Jump Bag

A Jump Bag is a container that has all the items necessary to respond to an incident inside to help mitigate the effects of delayed reactions.

Kerberos

A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

Kernel

The essential centre of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

Key Loggers

A software program or a device designed to secretly monitor and log all keystrokes. Key logging devices are small devices that can be fixed to the keyboard, or placed within a cable or the computer itself. Key logging software is made up of programs dedicated to tracking and logging keystrokes.

Lattice Techniques

Lattice Techniques use security designations to determine access to information.

Layer 2 Forwarding Protocol (L2F)

An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP)

An extension of the Point-to-Point Tunnelling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

Lawful Interception

Legally sanctioned official access to private communications such as telephone calls and email messages

Location Data

Data which provide the geographic position of the mobile phone user.

Least Privilege

Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legion

Software to detect unprotected shares.

Lightweight Directory Access Protocol (LDAP)

A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Link State

With link state, routes maintain information about all routers and router-to-router links within a geographic area, and create a table of best routes with that information.

Linking

Linking occurs where the URL, that is, the website address provided connects to a specific page on a website rather than the home page.

List Based Access Control

List Based Access Control associates a list of users and their privileges with each object.

Loadable Kernel Modules (LKM)

Loadable Kernel Modules allow for the adding of additional functionality directly into the kernel while the system is running.

Log Clipping

Log clipping is the selective removal of log entries from a system log to hide a compromise.

Logic bombs

Logic bombs are programs or snippets of code that execute when a certain predefined event occurs. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

Logic Gate

A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. As digital circuits can only understand binary, inputs and outputs can assume only one of two states, 0 or 1.

Loopback Address

The loopback address (127.0.0.1) is a pseudo IP address that always refer back to the local host and are never sent out onto a network.

MAC Address

A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

Malicious Code

Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware

A generic term for a number of different types of malicious code.

Mandatory Access Control (MAC)

Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

Masquerade Attack

A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

MD5

A one way cryptographic hash function. Also see "hash functions" and "shAL"

Measures of Effectiveness (MOE)

Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

Meta Tags

A meta tag is an encoded statement in the Hypertext Mark-up Language (HTML) that provides information regarding some of the content of a webpage. The meta tag is placed near the top of the HTML in a web page as a part of the heading. Based on the information fed into a meta tag by the net surfer, search engines index the pages which could be of interest to an internet user.

Monoculture

Monoculture is the case where a large number of users run the same software, and are vulnerable to the same attacks.

Morris Worm

A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November, 1988, causing problems for thousands of hosts.

Multi-Cast

Broadcasting from one host to a given set of hosts.

Multi-Homed

You are "multi-homed" if your network is directly connected to two or more ISP's.

Multiplexing

To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

NAT

Network Address Translation. It is used to share one or a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses. Typically home or small business networks use NAT to share a single DLS or Cable modem IP address. However, in some cases NAT is used for servers as an additional layer of protection.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology, a unit of the US Commerce Department.

Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Disaster

Any “act of God” (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Netmask

32-bit number indicating the range of IP addresses residing on a single IP network/subnet/ supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.

Network Address Translation

The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Network Mapping

To compile an electronic inventory of the systems and the services on your network.

Network Taps

Network taps are hardware devices that hook directly onto the network cable and send a copy of the traffic that passes through it to one or more other networked devices.

Network-Based IDS

A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication (like phone lines) can’t be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it’s attached to. Packets are considered to be of interest if they match a signature. Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

Non-Repudiation

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn’t been modified.

Null Session

Known as Anonymous Logon, it is a way of letting an anonymous user retrieve information such as user names and shares over the network or connect without authentication. It is used by applications such as explorer.exe to enumerate shares on remote servers.

Octet

A sequence of eight bits. An octet is an eight-bit byte.

One-Way Encryption

Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

One-Way Function

A (mathematical) function, f, which is easy to compute the output based on a given input. However given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

Open Shortest Path First (OSPF)

Open Shortest Path First is a link state routing algorithm used in interior gateway routing. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

OSI

OSI (Open Systems Interconnection) is a standard description or “reference model” for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

Overload

Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

Packet

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Switched Network

A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

Partitions

Major divisions of the total physical hard disk space.

Password Authentication Protocol (PAP)

Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

Password Cracking

Password cracking is the process of attempting to guess passwords, given the password file information.

Password Sniffing

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch

A patch is a small update released by a software manufacturer to fix bugs in existing programs.

Patching

Patching is the process of updating software to a different version.

Payload

Payload is the actual application data a packet contains.

Penetration

Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Penetration Testing

Penetration testing is used to test the external perimeter security of a network or facility.

Permutation

Permutation keeps the same letters but changes the position within a text to scramble the message.

Personal Data

The information or data which relate to a living individual who can be identified from that information or data, whether collected by any Government or any private organization or agency.

Personal Firewalls

Personal firewalls are those firewalls that are installed and run on individual PCs.

Pharming

This is a more sophisticated form of MITM attack. A user's session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading website's IP. Almost all users use a URL like www. worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

Phishing

The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

Phreaking

The word 'phreaking' is a combination of the two words 'phone' and 'freak'. Phreaking refers to people who tamper with systems of telecommunications such as the public telephone networks and various phone system audio frequencies.

Ping of Death

An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Ping Scan

A ping scan looks for machines that are responding to ICMP Echo Requests.

Ping Sweep

An attack that sends ICMP echo requests (“pings”) to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

Plaintext

Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer’s TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

Point-to-Point Tunneling Protocol (PPTP)

A protocol (set of communication rules) that allows corporations to extend their own corporate network through private “tunnels” over the public Internet.

Poison Reverse

Split horizon with poisoned reverse (more simply, poison reverse) does include such routes in updates, but sets their metrics to infinity. In effect, advertising the fact that there routes are not reachable.

Polyinstantiation

Polyinstantiation is the ability of a database to maintain multiple records with the same key. It is used to prevent inference attacks.

Polymorphism

Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port

A port is nothing more than an integer that uniquely identifies an endpoint of a
communication stream. Only one process per machine can listen on the same port number.

Possession

Possession is the holding, control, and ability to use information.

Post Office Protocol, Version 3 (POP3)

An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

Practical Extraction and Reporting Language (Perl)

A script programming language that is similar in syntax to the C language and that includes a number of popular Unix facilities such as sed, awk, and tr.

Pretty Good Privacy (PGP)TM

Trademark of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

Private Addressing

IANA has set aside three address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in RFC 1918. The reserved address blocks are: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255

(172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Private Cloud

A private cloud (also called internal cloud) is one in which the computing environment is operated exclusively for a particular company or organization. The private cloud providers services to a limited number of users behind a firewall.

Processing

Processing means obtaining, recording or holding the personal data or information of an individual and carrying out any operation on the information including alteration, disclosure, transmission, dissemination and destruction.

Program Infector

A program infector is a piece of malware that attaches itself to existing program files.

Program Policy

A program policy is a high-level policy that sets the overall tone of an organization's security approach.

Promiscuous Mode

When a machine reads all packets off the network, regardless of who they are addressed to. This is used by network administrators to diagnose network problems, but also by unsavory characters who are trying to eavesdrop on network traffic (which might contain passwords or other information).

Proprietary Information

Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Protocol

A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.

Protocol Stacks (OSI)

A set of network protocol layers that work together.

Proxy Server

A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Cloud

A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the internet.

Public Key

The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Encryption

The popular synonym for "asymmetric cryptography".

Public Key Infrastructure (PKI)

A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Public-Key Forward Secrecy (PFS)

For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

QAZ

A network worm.

Race Condition

A race condition exploits the small window of time between a security control being applied and when the service is used.

Radiation Monitoring

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Reconnaissance

Reconnaissance is the phase of an attack where an attackers finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.

Reflexive ACLs (Cisco)

Reflexive ACLs for Cisco routers are a step towards making the router act like a stateful firewall. The router will make filtering decisions based on whether connections are a part of established traffic or not.

Registry

The Registry in Windows operating systems in the central set of settings and information required to run the Windows computer.

Regression Analysis

The use of scripted tests which are used to test software for all possible input is should expect. Typically developers will create a set of regression tests that are executed before a new version of a software is released. Also see "fuzzing".

Request for Comment (RFC)

A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Resource Exhaustion

Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

Response

A response is information sent that is responding to some stimulus.

Reverse Engineering

Acquiring sensitive data by disassembling and analyzing the design of a system component.

Reverse Lookup

Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.

Reverse Proxy

Reverse proxies take public HTTP requests and pass them to back-end webservers to send the content to it, so the proxy can then send the content to the end-user.

Risk

Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment

A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

Risk Averse

Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail in order to avoid risks associated with e-mail may be considered "Risk Averse"

Rivest-Shamir-Adleman (RSA)

An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Role Based Access Control

Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

Root

Root is the name of the administrator account in Unix systems.

Root kit

A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

Router

Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.

Routing Information Protocol (RIP)

Routing Information Protocol is a distance vector protocol used for interior gateway routing which uses hop count as the sole metric of a path's cost.

Routing Loop

A routing loop is where two or more poorly configured routers repeatedly exchange the same packet over and over.

RPC Scans

RPC scans determine which RPC services are running on a machine.

Rule Set Based Access Control (RSBAC)

Rule Set Based Access Control targets actions based on rules for entities operating on objects.

S/Key

A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Safety

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Scavenging

Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Secure Electronic Transactions (SET)

Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SSH)

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Segment

Segment is another name for TCP packets.

Sensitive Information

Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties

Separation of duties is the principle of splitting privileges among multiple individuals or systems.

Server

A system entity that provides a service in response to requests from other system entities called clients.

Session

A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking

Take over a session that someone else has established.

Session Key

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

SHAL

A one way cryptographic hash function. Also see "MD5"

Shadow Password Files

A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

Share

A share is a resource made public on a machine, such as a directory (file share) or printer (printer share).

Shell

A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

Signals Analysis

Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Signature

A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

Simple Integrity Property

In Simple Integrity Property a user cannot write data to a higher integrity level than their own.

Simple Network Management Protocol (SNMP)

The protocol governing network management and the monitoring of network devices and their functions. A set of protocols for managing complex networks.

Simple Security Property

In Simple Security Property a user cannot read data of a higher classification than their own.

Skimming

Skimming is the capturing of personal information on the credit card by using skimming device to scan the card details on the magnetic strip.

Smartcard

A smartcard is an electronic badge that includes a magnetic strip or chip that can record and replay a set key.

Smurf

The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer

A sniffer is a tool that monitors network traffic as it received in a network interface.

Sniffing

A synonym for "passive wiretapping."

Social Engineering

A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

Socket

The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

Socket Pair

A way to uniquely specify a connection, i.e., source IP address, source port, destination IP address, destination port.

SOCKS

A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. SOCKS uses sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software

Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source Port

The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

Spam

Electronic junk mail or junk newsgroup postings.

Spanning Port

Configures the switch to behave like a hub for a specific port.

Split Horizon

Split horizon is a algorithm for avoiding problems caused by including routes in updates sent to the gateway from which they were learned.

Split Key

A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

Spoof

Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

SQL Injection

SQL injection is a type of input validation attack specific to database-driven applications where

SQL code is inserted into application queries to manipulate the database.

Stack Mashing

Stack mashing is the technique of using a buffer overflow to trick a computer into executing arbitrary code.

Standard ACLs (Cisco)

Standard ACLs on Cisco routers make packet filtering decisions based on Source IP address only.

Star Property

In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

State Machine

A system that moves through a series of progressive conditions.

Stateful Inspection

Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Static Host Tables

Static host tables are text files that contain hostname and address mapping.

Static Routing

Static routing means that routing table entries contain information that does not change.

Stealthing

Stealthing is a term that refers to approaches used by malicious code to conceal its presence on the infected system.

Steganalysis

Steganalysis is the process of detecting and defeating the use of steganography.

Steganography

Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is “invisible” ink.

Stimulus

Stimulus is network traffic that initiates a connection or solicits a response.

Store-and-Forward

Store-and-Forward is a method of switching where the entire packet is read by a switch to determine if it is intact before forwarding it.

Straight-Through Cable

A straight-through cable is where the pins on one side of the connector are wired to the same pins on the other end. It is used for interconnecting nodes on the network.

Stream Cipher

A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

Strong Star Property

In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

Sub Network

A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

Subnet Mask

A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

Subscription Encryption

In subscription encryption, the message is encrypted by substituting one character for another. In the most basic form, this involves replacing and rotating each character by a certain number of letters of the alphabet.

Switch

A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

Switched Network

A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. Any network providing switched communications service.

Symbolic Links

Special files which point at another file.

Symmetric Cryptography

A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

Symmetric Key

A cryptographic key that is used in a symmetric cryptographic algorithm.

SYN Flood

A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

Synchronization

Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

Syslog

Syslog is the system logging facility for UNIX systems.

System Interference

System interference is defined as the serious hindering, without right, of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

System Security Officer (SSO)

A person responsible for enforcement or administration of the security policy that applies to the system.

System-Specific Policy

A System-specific policy is a policy written for a specific system or device.

T1, T3

A digital circuit using TDM (Time-Division Multiplexing).

Tamper

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

TCP Fingerprinting

TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

TCP Full Open Scan

TCP Full Open scans check each port by performing a full three-way handshake on each port to determine if it was open.

TCP Half Open Scan

TCP Half Open scans work by performing the first half of a three-way handshake to determine if a port is open.

TCP Wrapper

A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

TCP/IP

A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

TCPDump

TCPDump is a freeware protocol analyzer for Unix that can monitor network traffic on a wire.

TELNET

A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment

A threat assessment is the identification of types of threats that an organization might be exposed to.

Threat Model

A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector

The method a threat uses to get to the target.

Time to Live

A value in an Internet Protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

Token Ring

A token ring network is a local area network in which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

Token-Based Access Control

Token based access control associates a list of objects and their privileges with each user. (The opposite of list based.)

Token-Based Devices

A token-based device is triggered by the time of day, so every minute the password changes, requiring the user to have the token with them when they log in.

Topology

The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. The specific physical, i.e., real, or logical, i.e., virtual, arrangement of the elements of a network. Note 1: Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Note 2: The common types of network topology are illustrated

Trace Route (tracert.exe)

Trace route is a tool the maps the route a packet takes from the local machine to a remote destination.

Transmission Control Protocol (TCP)

A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transport Layer Security (TLS)

A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

Triple DES

A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

Triple-Wrapped

S/MIME usage: data that has been signed with a digital signature, and then encrypted, and then signed again.

Trojan Horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Trunking

Trunking is connecting switched together so that they can share VLAN information between them.

Trust

Trust determine which permissions and what actions other systems or users can perform on remote machines.

Trusted Ports

Trusted ports are ports below number 1024 usually allowed to be opened by the root user.

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link - i.e., an OSI layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunnelling can move data between computers that use a protocol not supported by the network connecting them.

UDP Scan

UDP scans perform scans to determine which UDP ports are open.

Unicast

Broadcasting from host to host.

Uniform Resource Identifier (URI)

The generic term for all types of names and addresses that refer to objects on the World Wide Web.

Uniform Resource Locator (URL)

The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, http://www.pcwebopedia.com/ index-.html.

Unix

A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programrs, UNIX was designed to be a small, flexible system used exclusively by programrs.

Unprotected Share

In Windows terminology, a “share” is a mechanism that allows a user to connect to file systems and printers on other systems. An “unprotected share” is one that allows anyone to connect to it.

Unsolicited Commercial Communications

A communication in any form with commercial content that is sent to a recipient who has not requested data.

User

A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

User Contingency Plan

User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

User Datagram Protocol (UDP)

A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/ IP provides very few error recovery services, offering instead a direct way to send and receive datagram’s over an IP network. It’s used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get a datagram from one computer to another but does not divide a message into packets (datagram’s) and reassemble it at the other end. Specifically, UDP doesn’t provide sequencing of the packets that the data arrives in.

Virtual Private Network (VPN)

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall; the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Vishing

The term ‘vishing’ coined from the words voice and phishing, is the criminal practice of using voice over phone systems to gain access to details about account numbers, PIN date of birth and expiry date of credit card holders and using it for fraudulent activities.

Voice Firewall

A physical discontinuity in a voice network that monitors, alerts and controls inbound and outbound voice network activity based on user-defined call admission control (CAC) policies, voice application layer security threats or unauthorized service use violations.

Voice Intrusion Prevention System (IPS)

Voice IPS is a security management system for voice networks which monitors voice traffic for multiple calling patterns or attack/abuse signatures to proactively detect and prevent toll fraud, Denial of Service, telecom attacks, service abuse, and other anomalous activity.

War Chalking

War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

War Dialer

A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing

War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

War Driving

War driving is the process of travelling around looking for wireless access point signals that can be used to get network access.

Web of Trust

A web of trust is the trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

Web Server

A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

WHOIS

An IP for finding information about resources on networks.

Windump

Windump is a freeware tool for Windows that is a protocol analyzer that can monitor network traffic on a wire.

Wired Equivalent Privacy (WEP)

A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

Wireless Application Protocol

A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat.

Wiretapping

Monitoring and recording data that is flowing between two points in a communication system.

World Wide Web ("the Web", WWW, W3)

The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Zero Day

The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero days" exploit is referred to an exploit for which no patch is available yet. ("day one" - day at which the patch is made available).

Zero-day Attack

A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zombies

A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

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
- Google & Wikipedia
- Investigation of Cyber Crimes By Alex Samuel & A.K. Upadhyay (Dwivedi & Company)
- Corporate Computer and Network Security (2nd Edition) By Raymond R. Panko
- “Cyber Crimes, Law Enforcement, Security & Surveillance in the Information Age.” By D. Thomas & B.D. Loader
- https://www.sans.org/