1. INTRODUCTION TO CYBERCRIME

List of Topics:

- Introduction
- Cybercrime: Definition and Origins of the Word
- Cybercrime and Information Security
- Who are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspective
- Cybercrime and the Indian ITA 2000
- A Global Perspective on Cybercrimes
- Cybercrime Era: Survival Mantra for the Netizens

INTRODUCTION

- **"**Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks**"**.
- **"**Cybersecurity**"** means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- Almost everyone is aware of the rapid growth of the Internet.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomena; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend

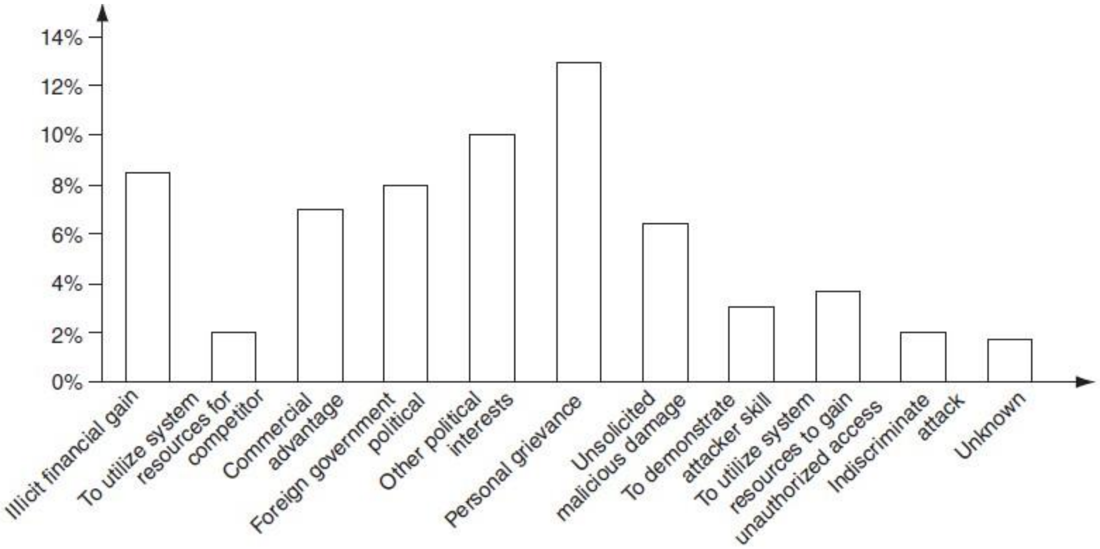


Figure: Cybercrime Trend

- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

Definition:

“A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime.**”**

Alternative definitions of Cybercrime are as follows:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.

5. "Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime. The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security, cybercrime is any criminal activity which uses network access to commit a criminal act. Cybercrime may be internal or external, with the former easier to perpetrate. The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle.

Some people argue that a cybercrime is not a crime as it is a crime against software & not against a person (or) property. However, while the legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:

1. Techno-crime: A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints".
2. Techno-vandalism: These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

There is a very thin line between the two terms “computer crime” and “computer fraud”; both are punishable. Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways:

a. how to commit them is easier to learn,
b. they require few resources relative to the potential damage caused,
c. they can be committed in a jurisdiction without being physically present in it &
d. they are often not clearly illegal.

Important Definitions related to Cyber Security:

Cyberterrorism:

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.

“The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.”

(or)

Cyberterrorism is defined as “any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism.”

Cybernetics:

Cybernetics deals with information and its use. Cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation. Worldwide, including India, cyberterrorists usually use computer as a tool, target for their unlawful act to gain information.

Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes, selling illegal articles, pornography/child pornography, etc. This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

<u>Phishing</u>:

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment.

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain &amp; other fraudulent activities.

(or)

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords, credit card information from users etc.

<u>Cyberspace</u>:

This is a term coined by William Gibson, a science fiction writer in 1984. Cyberspace is where users mentally travel through matrices of data. Conceptually, cyberspace is the nebulous place where humans interact over computer networks. The term “cyberspace” is now used to describe the Internet and other computer networks. In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. Cyberspace is most definitely a place where you chat, explore, research and play.

<u>Cybersquatting</u>:

The term is derived from “squatting” which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.

Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. This term is explained here because, in a way, it relates to cybercrime given the intent of cybersquatting.

Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else’s trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying “domain names” that have existing businesses names.

In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with “Uniform Dispute Resolution Policy” (a contractual obligation to which all domain name registrants are presently subjected to).

Cyberpunk:

This is a term coined by Bruce Bethke, published in science fiction stories magazine in November 1983. According to science fiction literature, the words “cyber” and “punk” emphasize the two basic aspects of cyberpunk: “technology” and “individualism.” The term “cyberpunk” could mean something like “anarchy via machines” or “machine/computer rebel movement.”

Cyberwarfare:

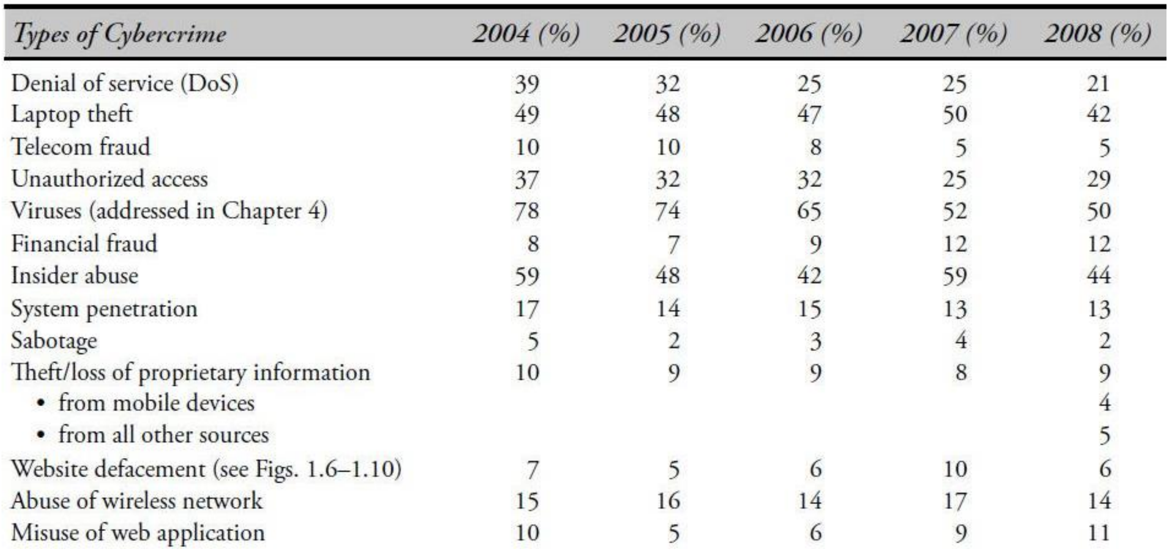
Cyberwarfare means information attacks against an unsuspecting opponent’s computer networks, destroying and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term “information infrastructure” refers to information resources, including communication systems that support an industry, institution or population. These type of Cyber attacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

CYBERCRIME AND INFORMATION SECURITY

Lack of information security gives rise to cybercrimes. Let us refer to the amended Indian Information Technology Act (ITA) 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides a new focus on “Information Security in India". "Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. The term incorporates both the physical security of devices as well as the information stored therein. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.

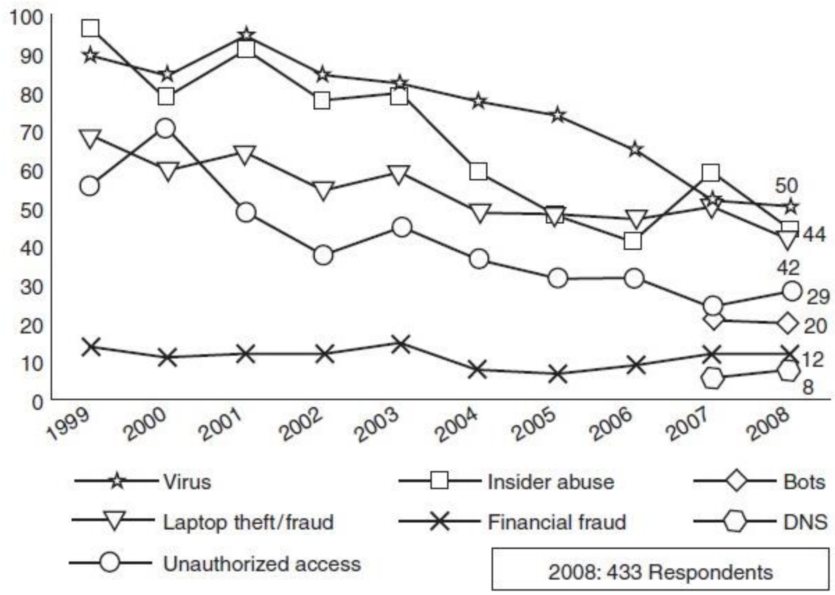
Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Survey on computer crime and security supports this. Cybercrimes occupy an important space in information security domain because of their impact. The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost (through loss/theft of laptops).

Because of these reasons, reporting of financial losses often remains approximate. In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about "security incidents" including cybercrime. In general, organizations perception about "insider attacks" seems to be different than that made out by security solution vendor. However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey. Awareness about "data privacy" too tends to be low in most organizations. When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such "crimes" may not be detected by the victimized organization and no direct costs may be associated with the theft



Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11

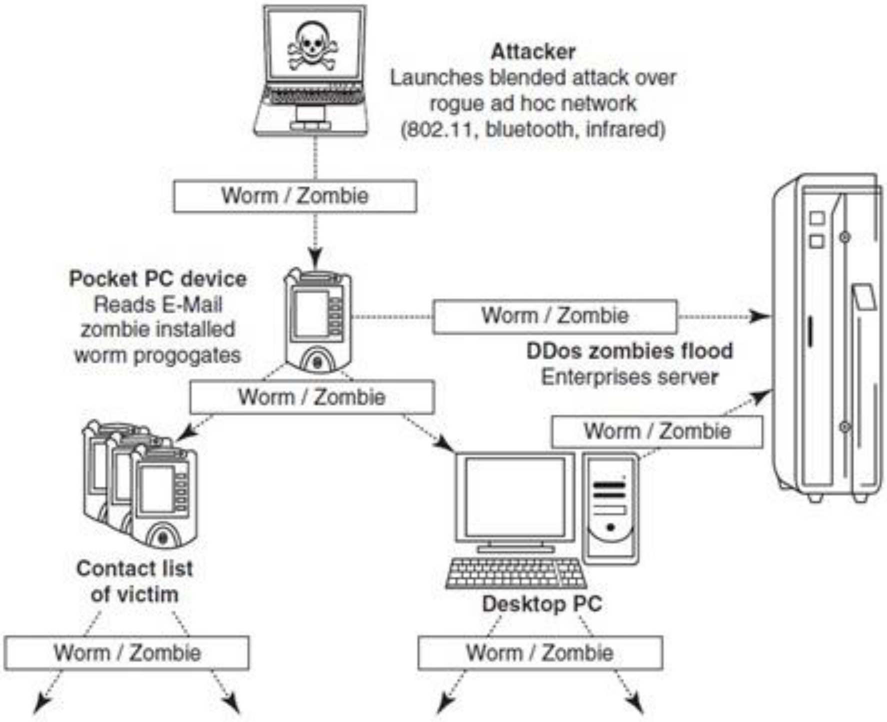
<u>Figure</u>: Cybercrime trend over the years



<u>Figure</u>: shows several categories of incidences – viruses, insider abuse, laptop theft and unauthorized access to systems

<u>The Botnet Menace</u>:

A group of computers that are controlled by software containing harmful programs, without their users' knowledge is called as **<u>Botnet</u>**. The term “Botnet” is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Below figure shows how a “zombie” works.



<u>Figure</u>: How a Zombie works

- A Botnet maker can control the group remotely for illegal purposes, the most common being
    - denial-of-service attack (DoS attack),
    - Adware,
    - Spyware,
    - E-Mail Spam,
    - Click Fraud
    - theft of application serial numbers,
    - login IDs
    - financial information such as credit card numbers, etc.
- An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner’s knowledge that his computer has been compromised.
- The problem of Botnet is global in nature and India is also facing the same.

- India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009.
- Small and medium businesses in the country are at greater risk, as they are highly vulnerable to Bots, Phishing, Spam and Malicious Code attacks.
    - Mumbai with 33% incidences tops the Bot-infected city list,
    - followed by New Delhi at 25%,
    - Chennai at 17% and
    - Bangalore at 13%.
- Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.
- The Internet is a network of interconnected computers. If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country.

WHO ARE CYBERCRIMINALS?

Cybercrime involves such activities

- credit card fraud;
- cyberstalking;
- defaming another online;
- gaining unauthorized access to computer systems;
- ignoring copyright, software licensing and trademark protection;
- overriding encryption to make illegal copies;
- software piracy and stealing another’s identity (known as identity theft) to perform criminal acts

Types of Cybercriminals:

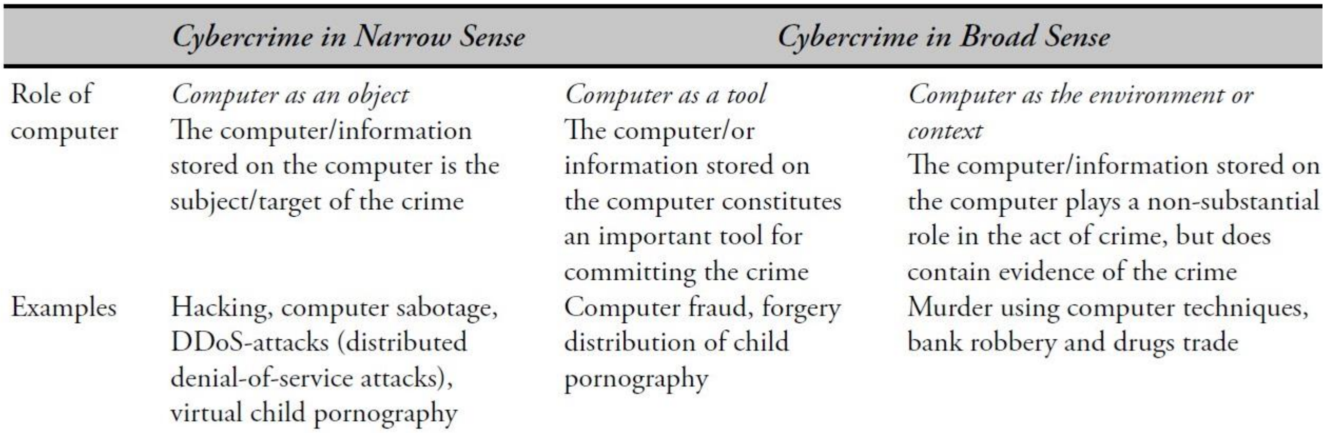
1. **Type I: Cybercriminals – hungry for recognition**
    - Hobby hackers;
    - IT professionals (social engineering is one of the biggest threat);
    - Politically motivated hackers;
    - Terrorist organizations.
2. **Type II: Cybercriminals – not interested in recognition**

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage)
- organized criminals

3. Type III: Cybercriminals – the insiders

- Disgruntled or former employees seeking revenge;
- Competing companies using employees to gain economic advantage through damage and/or theft.

CLASSIFICATIONS OF CYBERCRIMES



	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

__Table__: Classifying Cybercrimes

"Crime is defined as 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 off ender liable to punishment by that law". Cyber crimes are classified as follows:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society
- Crimes emanating from Usenet newsgroup

__Cybercrime against individual__

1. __E-Mail Spoofing__: A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life.

2. Online Frauds: The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spyware and viruses are both malicious programs that are loaded onto your computer without your knowledge. The purpose of these programs may be to capture or destroy information, to ruin computer performance or to overload you with advertising. Viruses can spread by infecting computers and then replicating. Spyware disguises itself as a legitimate application and embeds itself into your computer where it then monitors your activity and collects information.

3. Phishing, Spear Phishing and its various other forms such as Vishing and Smishing:

Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spear Phishing is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company; it could include requests for usernames or passwords. While traditional Phishing scams are designed to steal information from individuals, spear phishing scam works to gain access to a company's entire computer system.

Vishing (voice phishing) is a type of phishing attack that is conducted by phone and often targets users of Voice over IP (VoIP) services like Skype.

It's easy to for scammers to fake caller ID, so they can appear to be calling from a local area code or even from an organization you know. If you don't pick up, then they'll leave a voicemail message asking you to call back. Sometimes these kinds of scams will employ an answering service or even a call center that's unaware of the crime being perpetrated.

Once again, the aim is to get credit card details, birthdates, account sign-ins, or sometimes just to harvest phone numbers from your contacts. If you respond and call back, there may be an automated message prompting you to hand over data and many people won't question this, because they accept automated phone systems as part of daily life now.

Smishing (SMS phishing) is a type of phishing attack conducted using SMS (Short Message Services) on cell phones. Just like email phishing scams, smishing messages typically include a threat or enticement to click a link or call a number and hand over sensitive information. Sometimes they might suggest you install some security software, which turns out to be malware.

Smishing example: A typical smishing text message might say something along the lines of, "Your ABC Bank account has been suspended. To unlock your account, tap here: https://bit.ly/2LPLdaU" and the link provided will download malware onto your phone. Scammers are also adept at adjusting to the medium they're using, so you might get a text message that says, "Is this really a pic of you? https://bit.ly/2LPLdaU" and if you tap that link to find out, once again you're downloading malware.

4. Spamming: People who create electronic Spam are called spammers. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc.

Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low. Therefore, the following web publishing techniques should be avoided:

- Repeating keywords;
- use of keywords that do not relate to the content on the site;
- use of fast meta refresh;
- redirection;
- IP Cloaking;
- use of colored text on the same color background;
- tiny text usage;
- duplication of pages with different URLs;

- hidden links;
- use of different pages that bridge to the same URL (gateway pages).

5. Cyber defamation: It is a cognizable (Software) offense. **"**Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.**"**

Cyber defamation happens when the above takes place in an electronic form. In other words, cyber defamation occurs when defamation takes place with the help of computers and/or the Internet. For example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person.

6. Cyberstalking and harassment: The dictionary meaning of **"**stalking**"** is an **"**act or process of following prey stealthily – trying to approach somebody or something.**"** Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

As the internet has become an integral part of our personal & professional lives, cyberstalkers take advantage of ease of communication & an increased access to personal information available with a few mouse clicks or keystrokes. They are 2 types of stalkers: Online Stalkers: aim to start the interaction with the victim directly with the help of the internet. Offline Stalkers: the stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim.

7. Computer Sabotage: The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage. It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes. Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

8. Pornographic Offenses: Child pornography means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

Child Pornography is considered an offense. The internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime. As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles. Pedophiles are the people who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent too. Here is how pedophiles operate:

- Step 1: Pedophiles use a false identity to trap the children/teenagers.
- Step 2: They seek children/teens in the kids' areas on the services, such as the Games BB or chat areas where the children gather.
- Step 3: They befriend children/teens.
- Step 4: They extract personal information from the child/teen by winning his/her confidence.
- Step 5: Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.
- Step 6: They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- Step 7: At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

9. Password Sniffing: is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.

And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN). IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.

Cybercrime against property

1. **Credit Card Frauds:** Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce

card fraud. Credit card fraud can be authorised, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party.

Credit cards are more secure than ever, with regulators, card providers and banks taking considerable time and effort to collaborate with investigators worldwide to ensure fraudsters aren't successful. Cardholders' money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are becoming increasingly sophisticated making it harder for fraudsters to steal money.

2. **Intellectual Property (IP) Crimes:** With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.

   Copyrights and trade secrets are the two forms of IP that is frequently stolen. For example, stealing of software, business strategies etc. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it. Another major cyber theft of IP faced by India is piracy. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.

3. **Internet time theft:** Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through identity theft.

Cybercrime against Organization

1. **Unauthorized accessing of Computer:** Hacking is one method of doing this and hacking is punishable offense. Unauthorized computer access, popularly referred to as hacking, describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.

2. **Password Sniffing:** Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents. Laws are not yet set up to

adequately prosecute a person for impersonating another person online. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

3. **Denial-of-service Attacks (DoS Attacks):** It is an attempt to make a computer resource (i.e.., information systems) unavailable to its intended users. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with spam mail depriving him of the services he is entitled to access or provide. The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:
    a. Flood a network with traffic, thereby preventing legitimate network traffic.
    b. Disrupt connections between two systems, thereby preventing access to a service.
    c. Prevent a particular individual from accessing a service.
    d. Disrupt service to a specific system or person.
4. **Virus attacks/dissemination of Viruses:**

    Computer virus is a program that can **"**infect**"** legitimate (valid) programs by modifying them to include a possibly **"**evolved**"** copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. Viruses can take some typical actions:

    - Display a message to prompt an action which may set of the virus
    - Delete files inside the system into which viruses enter
    - Scramble data on a hard disk
    - Cause erratic screen behavior
    - Halt the system (PC)
    - Just replicate themselves to propagate further harm
5. **E-Mail bombing/Mail bombs:** E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim**'**s mail servers crash (in the case of a company or an E-Mail service provider). Computer program can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient**'**s personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive.

6. **Salami Attack/Salami technique:** These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed; For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.
7. **Logic Bomb:** A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.
8. **Trojan Horse:** A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
9. **Data Diddling:** A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.
10. **Newsgroup Spam/Crimes emanating from Usenet newsgroup:** This is one form of spamming. The word "Spam" was usually taken to mean Excessive Multiple Posting (EMP). The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever. Spamming of Usenet newsgroups actually predates E-Mail Spam.
11. **Industrial spying/Industrial espionage:** Spying is not limited to governments. Corporations, like governments, often spy on the enemy. The Internet and privately networked systems provide new and better opportunities for espionage. "Spies" can get information about product finances, research and development and marketing strategies, an activity known as "industrial spying."

    However, cyberspies rarely leave behind a trail. Industrial spying is not new; in fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself.

    Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of registered organizations (it is said that they get several hundreds of thousands of dollars, depending on the "assignment"). With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as "Targeted Attacks" (which includes "Spear Phishing").
12. **Computer network intrusions:** "Crackers" who are often misnamed "Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords. Network intrusions are illegal, but detection and enforcement are

difficult. Current laws are limited and many intrusions go undetected. The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords. The practice of "strong password" is therefore important.

13. **<u>Software piracy</u>:** This is a big challenge area indeed. Cybercrime investigation cell of India defines "software piracy" as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. There are many examples of software piracy:
    1. <u>end-user copying</u>: friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
    2. <u>hard disk loading with illicit means</u>: hard disk vendors load pirated software;
    3. <u>counterfeiting</u>: large-scale duplication and distribution of illegally copied software;
    4. <u>Illegal downloads from the Internet</u>: by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:
        - getting untested software that may have been copied thousands of times over,
        - the software, if pirated, may potentially contain hard-drive-infecting viruses,
        - there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
        - there is no warranty protection,
        - there is no legal right to use the product, etc.

<u>Cybercrime against Society</u>

1. **<u>Forgery</u>:** Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates. These are made using computers and high quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.
2. **<u>Cyberterrorism</u>:** Cyberterrorism is a controversial term. Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

3. **Web Jacking:** Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves “password sniffing”. The actual owner of the website does not have any more control over what appears on that website.

Crimes emanating from Usenet newsgroup:

By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

CYBERCRIME: THE LEGAL PERSPECTIVES

- Cybercrime poses a biggest challenge.
- Computer Crime: As per “Criminal Justice Resource Manual (1979)”, computer-related crime was defined in the broader meaning as: “any illegal act for which knowledge of computer technology is essential for a successful prosecution”.
- International legal aspects of computer crimes were studied in 1983.
- In that study, computer crime was consequently defined as: “encompasses any illegal act for which knowledge of computer technology is essential for its commit”.
- Cybercrime, in a way, is the outcome of “globalization.” However, globalization does not mean globalized welfare at all.
- Globalized information systems accommodate an increasing number of transnational offenses.
- The network context of cybercrime makes it one of the most globalized offenses of the present and the most modernized threats of the future.
- This problem can be resolved in two ways.
    a) One is to divide information systems into segments bordered by state boundaries (cross-border flow of information).
    b) The other is to incorporate the legal system into an integrated entity obliterating these state boundaries.

- Apparently, the first way is unrealistic. Although all ancient empires including Rome, Greece and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice.
- In a globally connected world, information systems become the unique empire without tangible territory.

CYBERCRIMES: AN INDIAN PERSPECTIVE

India has the fourth highest number of Internet users in the world. According to the statistics posted on the site (http://www.iamai.in/), there are 45 million Internet users in India, 37% of all Internet accesses happen from cybercafés and 57% of Indian Internet users are between 18 and 35 years. The population of educated youth is high in India. It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007. A point to note is that the majority of offenders were under 30 years. The maximum cybercrime cases, about 46%, were related to incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007" report of the National Crime Record Bureau (NCRB).

Cybercrimes: Indian Statistics:

Cybercrimes: Cases of various categories under ITA 2000: 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year 2006, with an increase of 52.8%. 99 cases of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form known as cyberpornography. There were 76 cases of hacking with computer system which is related to loss/damage of computer resource/utility. India is said to be "youth country" given the population age distribution. However from cybercrime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India.

Cybercrimes: Cases of various categories under IPC Section: A total of 339 cases were registered under IPC sections during the year 2007 as compared to 311 such cases during 2006, thereby reporting an increase of 9%.Majority of the crimes out of total 339 cases registered under IPC fall under 2 categories i.e.., Forgery & Criminal breach of Trust or Fraud.

Incidence of Cybercrimes in cities: 17 out of 35 mega cities did not report any case of cybercrime (neither under the IT Act nor under IPC Sections) during the year 2007. A total of 17 mega cities have reported 118 cases under IT Act and 7 mega cities reported 180 cases under various sections of IPC.

The Indian Government is doing its best to control cybercrimes. For example, Delhi Police have now trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing. As at the time of writing this, the officers were trained for 6 weeks in computer hardware and software, computer networks comprising data communication networks, network protocols, wireless networks and network security.

CYBERCRIME & THE INDIAN ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce. It was enacted taking into consideration UNICITRAL model of Law on Electronic Commerce (1996).

Hacking and the Indian Laws:

Section Ref. and Title	**Chapter of the Act And Title**	**Crime**	**Punishment**
Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer system etc.	Compensation for Rs. 1 Crore
Sec.66 (Hacking with computer system)	Chapter XI Offences	Hacking (with intent or knowledge)	Fine of Rs. 2 Lakhs & Imprisonment for 3 years
Sec.67 (Publishing of information which is obscene in electronic form)	Chapter XI Offences	Publication of obscene material in electronic form	Fine of Rs. 1 Lakh & Imprisonment of 5 years and double conviction on second offence
Sec.68 (Power of controller to give directions)	Chapter XI Offences	Not complying with directions of controller	Fine upto Rs. 2 Lakhs & Imprisonment of 3 years
Sec.70 (Protected System)	Chapter XI Offences	Attempting or securing access to computer of another person without his/her knowledge	Imprisonment up to 10 Years
Sec.72 (Penalty for breach of confidentiality	Chapter XI Offences	Attempting or securing access to computer for	Fine up to Rs. 1 Lakh and Imprisonment up to

and privacy)		breaking confidentiality of the information of computer	2 Years
Sec.73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Chapter XI Offences	Publishing false Digital Signatures, false in certain particulars	Fine of Rs.1 Lakh or imprisonment of 2 years or both
Sec.74 (Publication for fraudulent purpose)	Chapter XI Offences	Publishing of Digital Signatures for fraudulent purpose	Imprisonment for the term of 2 years and fine of Rs. 1 Lakh

Table: The key provisions under the Indian ITA 2000 (before the amendment)

A GLOBAL PERSPECTIVE ON CYBERCRIMES

In Australia, cybercrime has a narrow statutory meaning as used in the Cyber Crime Act 2001, which details offenses against computer data and systems. However, a broad meaning is given to cybercrime at an international level. In the Council of Europe’s (CoE’s) Cyber Crime Treaty, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses.

This wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime. Although this status is from the International Telecommunication Union (ITU) survey conducted in 2005, we get an idea about the global perspective. ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010). The Spam legislation scenario mentions “none” about India as far as E-Mail legislation in India is concerned.

The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began assessment of threats, vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US

constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.

2. In August 18, 2006, there was a news article published “ISPs Wary About ‘Drastic Obligations’ on Web Site Blocking.” European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost joint antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.
3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. More than 40 countries have ratified the Convention to date.

Cybercrime and the Extended Enterprise:

It is a continuing problem that the average user is not adequately educated to understand the threats and how to protect oneself. Actually, it is the responsibility of each user to become aware of the threats as well as the opportunities that “connectivity” and “mobility” presents them with. In this context, it is important to understand the concept of “extended enterprise.” This term represents the concept that a company is made up not just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers.

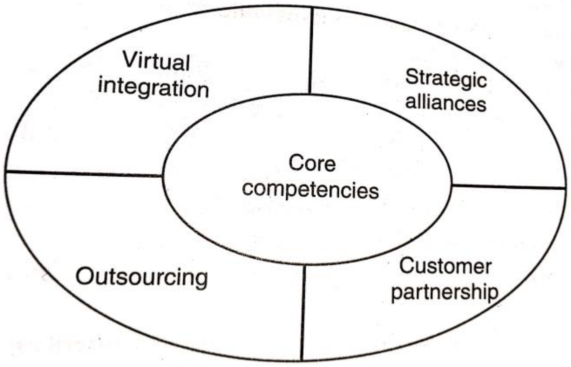


Figure: Extended Enterprise

The extended enterprise can only be successful if all of the component groups and individuals have the information they need in order to do business effectively. An extended enterprise is a **“**loosely coupled, self-organizing network**”** of firms that combine their economic output to provide **“**products and services**”** offerings to the market. Firms in the extended enterprise may operate independently. Seamless flow of “information” to support instantaneous “decision-making ability” is crucial for the “external enterprise”. This becomes possible through the “interconnectedness”. Due to the interconnected features of information & communication technologies, security overall can only be fully promoted when the users have full awareness of existing threats & dangers.

Given the promises and challenges in the extended enterprise scenario, organizations in the international community have a special role in sharing information on good practices and creating open and accessible enterprise information flow channels for exchanging of ideas in a collaborative manner.

CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

The term “Netizen” was coined by Michael Hauben. Quite simply, “Netizens” are the Internet users. Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is:

a. Precaution
b. Prevention
c. Protection
d. Preservation
e. Perseverance

For ensuring cyber safety, the motto for the “Netizen” should be “Stranger is Danger!” If you protect your customer’s data, your employee’s privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community. NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyberlabs across major cities in India

More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.

Unit -II: Cyber Offenses

How Criminals Plan Them – Introduction, How Criminals Plan The Attacks, Social Engineering, and Cyber Stalking, Cyber Cafe And Cybercrimes, Botnets: The Fuel For Cybercrime, Attack Vector Cloud Computing.

Learning Objectives

- ⦿ Understand different types of cyber attacks.
- ⦿ Get an overview of the steps involved in planning cybercrime.
- ⦿ Understand tools used for gathering information about the target.
- ⦿ Get an overview on social engineering – what and how.
- ⦿ Learn about the role of cybercafés in cybercrime.
- ⦿ Understand what cyber stalking is.
- ⦿ Learn about Botnets and attack vector.
- ⦿ Get an overview on cloud computing – what and how.

How Criminals Plan Them –Introduction

- Technology is a “double-edged sword” as it can be used for both good and bad purposes
- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offense.
- In today’s world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter 1 provided an overview of hacking, cyber terrorism, network intrusions, password sniffing, computer viruses, etc. They are the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyber laws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as “Crackers” (Box 2.1).

Box 2.1 | Hackers, Crackers and Phreakers
Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers (refer to Box 2.2).
Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.

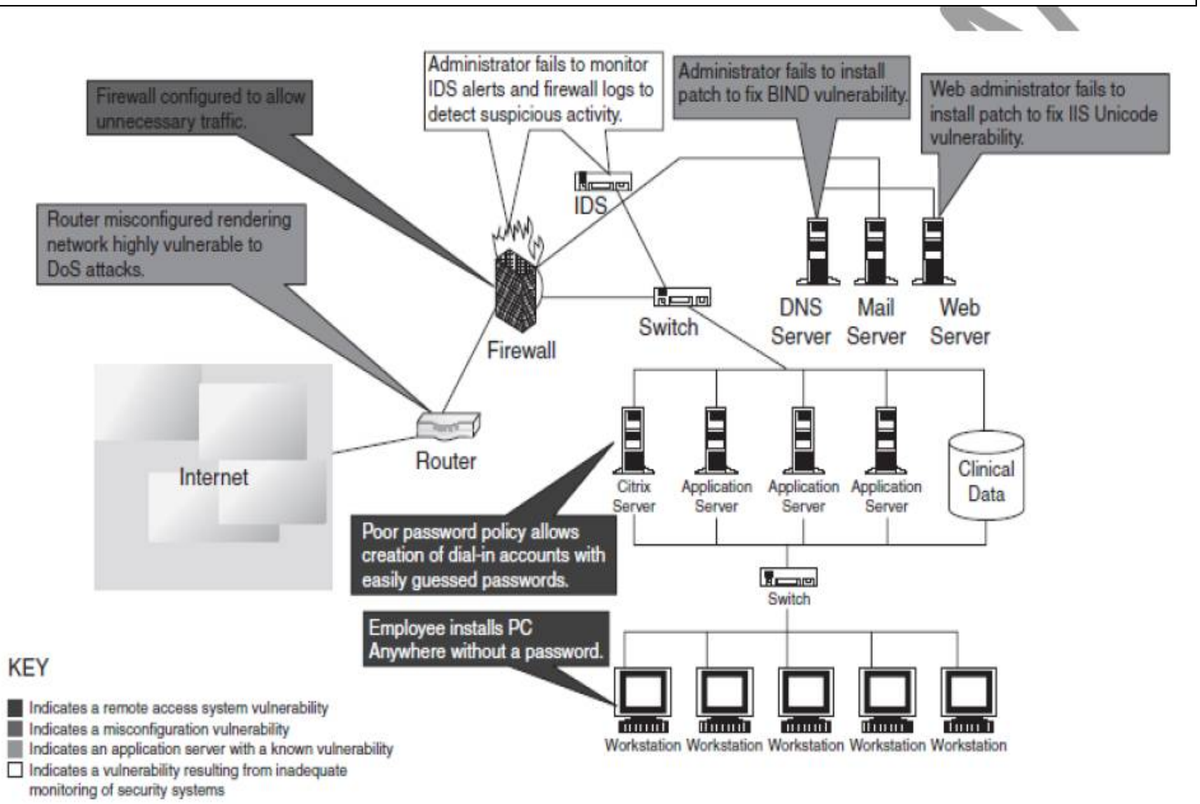
Cracker: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term “cracker” is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.

Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called “phreaking”). These sites usually display warnings such as “These files are illegal; we are not responsible for what you do with them.”

Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.

Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

War dialer: Program automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in. An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.


Firewall configured to allow unnecessary traffic.
Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Clinical Data
Poor password policy allows creation of dial-in accounts with easily guessed passwords.
Switch
Employee installs PC Anywhere without a password.
Workstation
Workstation
Workstation
Workstation
Workstation
KEY
Indicates a remote access system vulnerability
Indicates a misconfiguration vulnerability
Indicates an application server with a known vulnerability
Indicates a vulnerability resulting from inadequate monitoring of security systems

- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection (border as in the sense of network periphery);
  - remote access servers (RASs) with weak access controls;

  - application servers with well-known exploits;
  - misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

Box 2.2 | What Color is Your Hat in the Security World?

A **black hat** is also called a “cracker” or “dark side hacker.” Such a person is a malicious or **criminal hacker**. Typically, the term “cracker” is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of “hacker” can be much broader. The name comes from the opposite of “white hat hackers.”

A **white hat hacker** is considered an **ethical hacker**. In the realm of IT, a “white hat hacker” is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a “white hat” generally focuses on securing IT systems, whereas a “black hat” (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A **brown hat hacker** is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

Cybercrime can be targeted against individuals (**persons**), assets (**property**) and/or **organizations** (government, business and social).

1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Section 1.5.13, Chapter 1), copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.
2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.

3. **Crimes targeted at organizations:** Cyber terrorism is one of the distinct crimes against organizations/ governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system (see Box 2.3).
4. **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. **Series of events:** This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

Box 2.3 | Patriot Hacking

Patriot hacking[1] also known as **Digital Warfare**, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat. Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyber attacks like website defacements (explained in Box 1.4, Chapter1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5. For detailed information visit www.patriothacking.com

2.2 How Criminals Plan the Attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target.
- The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- **Active attacks** are usually used to alter the system (i.e., computer network) whereas **passive attacks** attempt to gain information about the target.
- **Active attacks** may affect the availability, integrity and authenticity of data whereas **passive attacks** lead to violation of confidentiality.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as **passive attacks.**
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

2.2.1 Reconnaissance (reconnaissance= నిఘా)

- The literal meaning of "Reconnaissance" is an act of **finding something or somebody** (especially to gain information about an enemy or potential enemy).
- In the world of "hacking," reconnaissance phase begins with "Footprinting" – this is the preparation toward pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

2.2.2 Passive Attacks

A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees.
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

2.2.3 Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase. It involves the risk of detection and is also called “Rattling the doorknobs” or “Active reconnaissance.” Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

2.2.4 Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target.

The objectives of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

2.2.5 Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password.
2. exploit the privileges.
3. execute the malicious commands/applications.
4. hide the files (if required).
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

2.3 Social Engineering

- Social engineering is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.

- The goal of a social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on… (see Box 2.6).

Box 2.6 | Social Engineering Example

Mr. Joshi: Hello?

The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user’s home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

Mr. Joshi: Ohh … okay. I will be at my home by then, anyway.

Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is “pjoshi.” None of my files will be lost in the move, right?

Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?

Mr. Joshi: My password is “ABCD1965,” all characters in upper case.

Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the files are there.

Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. Impersonating an employee or valid user:

- “Impersonation” is perhaps the greatest technique used by social engineers to deceive people.
- Social engineers “take advantage” of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is

located, or to let someone into the building who “forgot” his/her badge, etc., or pretending to be an employee or valid user on the system.

2. Posing as an important user:

- The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
- The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

3. Using a third person:

- An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

4. Calling technical support:

- Calling the technical support for assistance is a classic social engineering example.
- Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

5. Shoulder surfing:

- It is a technique of gathering information such as usernames and passwords by watching over a person’s shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

6. Dumpster diving:

- It involves **looking in the trash for information written on pieces of paper or computer printouts**.
- This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
- It is also called dumpstering, binning, trashing, garbing or garbage gleaning.
- “Scavenging” is another term to describe these habits.
- In the UK, the practice is referred to as “ binning” or “skipping” and the person doing it is a “binner” or a “skipper.”

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.
- For example, sending a **fake E-Mail to the user** and asking him/her to re-enter a password in a webpage to confirm it.

1. Fake E-Mails:

- The attacker sends fake E-Mails (see Box 2.7) to users in such that the user finds it as a real e-mail.
- This activity is also called “Phishing”.

- It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as **usernames, passwords** and **credit card details** by impersonating as a trustworthy and legitimate organization or an individual.
- Banks, financial institutes and payment gateways are the common targets.
- Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website.
- Thus, Phishing is also an example of social engineering techniques used to fool netizens.
- The term “Phishing” has been evolved from the analogy that Internet scammers are using E-Mails attract to fish for passwords and financial data from the sea of Internet users (i.e., netizens).
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- As hackers have a tendency of replacing “f” with “ph,” the term “Phishing” came into being.

2. E-Mail attachments:

- E-Mail attachments are used to send malicious code to a victim’s system, which will automatically (e.g., keylogger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

3. Pop-up windows:

- Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

2.4 Cyberstalking

- The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.”
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to **harass another individual, group of individuals, or organization**.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- **It involves harassing or threatening behavior that an individual will conduct repeatedly**, for example, following a person, visiting a person’s home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person’s property. As the Internet has become an integral part of our personal and professional

lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. **Online stalkers:**
   - They aim to start the interaction with the victim directly with the help of the Internet.
   - E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
   - The stalker makes sure that the victim recognizes the attack attempted on him/her.
   - The stalker can make use of a third party to harass the victim.
2. **Offline stalkers:**
   - The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
   - Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
   - The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyberstalking

- The majority of cyberstalkers are men and the majority of their victims are women.
- Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking.
- In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor.
- However, there also have been many instances of cyberstalking by strangers.

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.

4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

2.4.4 Real-Life Incident of Cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi – the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved, we have changed their names.

- Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad.
- The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.
- A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.
- This person was chatting on the Internet, using her name and giving her address, talking in obscene language.
- The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.
- This was the first time when a case of cyberstalking was registered.
- Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

Box 2.8 | Cyberbullying

The National Crime Prevention Council defines Cyberbullying as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.
Source: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

2.5 Cybercafe and Cybercrimes

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students.
- Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.
- In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.
- **First**, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
- **Second**, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.
- **Indian Information Technology Act (ITA) 2000,** does not define cybercafes and interprets cybercafes as "network service providers" referred to under the Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer (PC) to prepare it for their use.
- Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:
    1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
    2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
    3. Several cybercafes had installed the software called “Deep Freeze” for protecting the computers from prospective malware attacks. **Deep Freeze** can wipe out the details of all activities carried out on the computer when one clicks on the “restart” button. Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.
    4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
    5. Pornographic websites and other similar websites with indecent contents are not blocked.
    6. Cybercafe owners have very less awareness about IT Security and IT Governance.
    7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
    8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cybercafes across India.

In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe. Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:**
2. **Stay with the computer:**
3. **Clear history and temporary files:**
4. **Be alert:**
5. **Avoid online financial transactions:**
6. **Change passwords:**

7. **Use Virtual keyboard:**
8. **Security warnings:**

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

- The dictionary meaning of Bot is "(computing) an automated program for doing some particular task, often over a network."
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "Zombie networks" have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.
- If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums.
- 'encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.
- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date:
2. Set the OS to download and install security patches automatically:

3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet: A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.
4. Disconnect from the Internet when you are away from your computer:
5. Downloading the freeware only from websites that are known and trustworthy:
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send:
7. Take an immediate action if your system is infected:

Box 2.9 | Technical Terms
Malware: It is malicious software, designed to damage a computer system without the owner’s informed consent. Viruses and worms are the examples of malware.
Adware: It is advertising-supported software, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.
Spam: It means unsolicited or undesired E-Mail messages
Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

2.7 Attack Vector

- **An “attack vector” is a path**, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- **Attack vectors** enable attackers to exploit system vulnerabilities, including the human element.
- **Attack vectors** include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.
- To some extent, firewalls and antivirus software can block attack vectors.
- However, no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.

- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
- In the technical terms, payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the “overhead” data required to get the packet to its destination. Payload may depend on the following point of view: “What constitutes it?” To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles. The attack vectors described here are how most of them are launched.

1. **Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something “free” or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer’s operator to succeed. Social engineering are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use variety of hacking tools, heuristics, Cyberoffenses: How and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.
5. **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.
6. **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file

sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.

7. **Malicious macros:** Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart(IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.
8. **Foistware (sneakware):** Foistware is the software that **adds hidden components** to the system with cunning nature. Spyware is the most common form of foistware. Foistware is partial- legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.
9. **Viruses:** These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

Box 2.10 | Zero-Day Attack

A zero-day (or zero-hour) attack[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package. Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also, visit the weblink http://www.isotf.org/zert to get more information about it.

2.8 Cloud Computing

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.

- Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which make it easier for cybercriminals to attack these systems.
- Cloud computing is Internet (“cloud”)-based development and use of computer technology (“computing”).
- The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- Cloud computing is a term used for hosted services delivered over the Internet.
- A cloud service has three distinct characteristics which differentiate it from traditional hosting:
    1. It is sold on demand – typically by the minute or the hour;
    2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
    3. The service is fully managed by the provider – a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

2.8.1 Why Cloud Computing?

The cloud computing has following advantages.

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user’s computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else’s hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware. The cloud computing services can be either private or public.

2.8.2 Types of Services

Services provided by cloud computing are as follows:

1. **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide **virtual servers** with unique IP addresses and **blocks of storage** on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their

servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.

2. **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. **Google Apps** is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.
3. **Software-as-a-service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The **software interacts with the user through a user interface**. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

2.8.3 Cybercrime and Cloud Computing

- Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years.
- Risks associated with cloud computing environment are as follows
    1. Elevated user access-Any data processed outside the organization brings with it an inherent level of risk
    2. Regulatory compliance-Cloud computing service providers are not able and/or not willing to undergo external assessments.
    3. Location of the data-User doesn't know where the data is stored or in which country it is hosted.
    4. Segregation of data-Data of one organization is scattered in different locations
    5. Recovery of the data-In case of any disaster, availability of the services and data is critical.
    6. Information security- violation reports Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity
    7. Long-term viability- In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.

3. CYBERCRIME: MOBILE & WIRELESS DEVICES

- Introduction
- Proliferation of Mobile and Wireless Devices
- Trends in Mobility
- Credit Card Frauds in Mobile and Wireless Computing Era
- Security Challenges Posed by Mobile Devices
- Registry Settings for Mobile Devices
- Authentication Service Security
- Attacks on Mobile/Cell Phones
- Mobile Devices: Security Implications for Organizations
- Organizational Measures for Handling Mobile Devices-Related Security Issues
- Organizational Security Policies and Measures in Mobile Computing Era
- Laptops

INTRODUCTION

In this modern era, the rising importance of electronic gadgets (i.e., mobile hand-held devices) – which became an integral part of business, providing connectivity with the Internet outside the office – brings many challenges to secure these devices from being a victim of cybercrime. In the recent years, the use of laptops, personal digital assistants (PDAs) and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment. By the end of 2008 around 1.5 billion individuals around the world had the Internet access. In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address.

Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the Smartphone. Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. Although IT departments of organizations as yet are not swapping employees' company-provided PDAs (as the case may be) for the Smartphones, many users may bring these devices from home and use them in the office. Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

PROLIFERATION OF MOBILE AND WIRELESS DEVICES

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities.

A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. As the term “mobile device” includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Below figure helps to understand how these terms are related

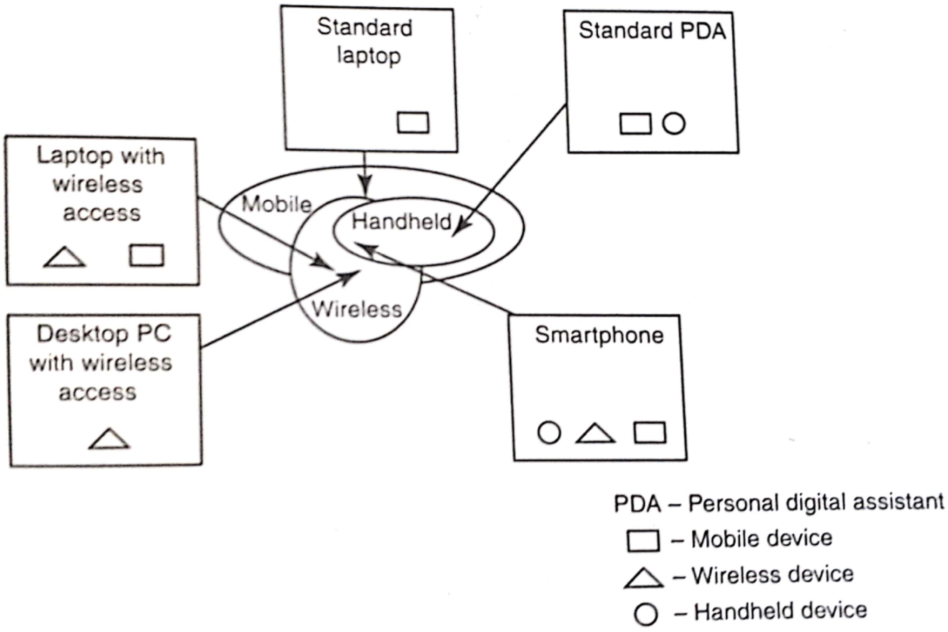


Figure: Mobile, Wireless & Hand-held devices

Mobile computing is “taking a computer and all necessary files and software out into the field.” Many types of mobile computers have been introduced since 1990s. They are as follows:

1. **Portable Computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some “setting-up” and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for

applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. **Internet Tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. **Personal Digital Assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. **Smartphone:** It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. **Fly Fusion Pentop Computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop that is not tethered. As more personal devices find their way into the enterprise, corporations are realizing cybersecurity threats that come along with the benefits achieved with mobile solutions.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all. Thus, while “wireless” is a subset of “mobile,” in most cases, an application can be mobile without being wireless. Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smartphones.

TRENDS IN MOBILITY

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. “iPhone” from Apple and Google-led “Android” phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans. It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.

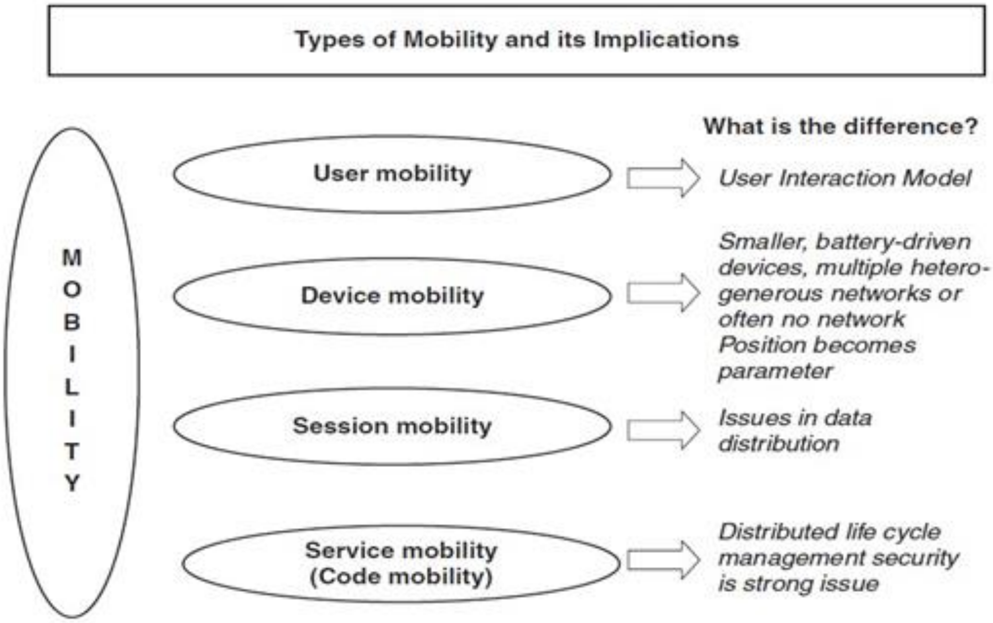

Types of Mobility and its Implications
What is the difference?
MOBILITY
User mobility
User Interaction Model
Device mobility
Smaller, battery-driven devices, multiple hetero-generous networks or often no network Position becomes parameter
Session mobility
Issues in data distribution
Service mobility (Code mobility)
Distributed life cycle management security is strong issue

Figure: Mobility types & implications

Popular types of attacks against 3G mobile networks are as follows:

1. **Malwares, Viruses and Worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:
    a. Skull Trojan: It targets Series 60 phones equipped with the Symbian mobile OS.
    b. Cabir Worm: It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
    c. Mosquito Trojan: It affects the Series 60 Smart phones and is a cracked version of “Mosquitos” mobile phone game.

   d. Brador Trojan: It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments (refer to Appendix C).
   e. Lasco Worm: It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. **Denial-of-Service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable.
3. **Overbilling Attack:** Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct.
4. **Spoofed Policy Development Process (PDP):** These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].
5. **Signaling-level Attacks:** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

CREDIT CARD FRAUDS IN MOBILE AND WIRELESS COMPUTING ERA

These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever- increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Mobile credit card transactions are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal. Today belongs to "mobile computing," that is, anywhere anytime computing.

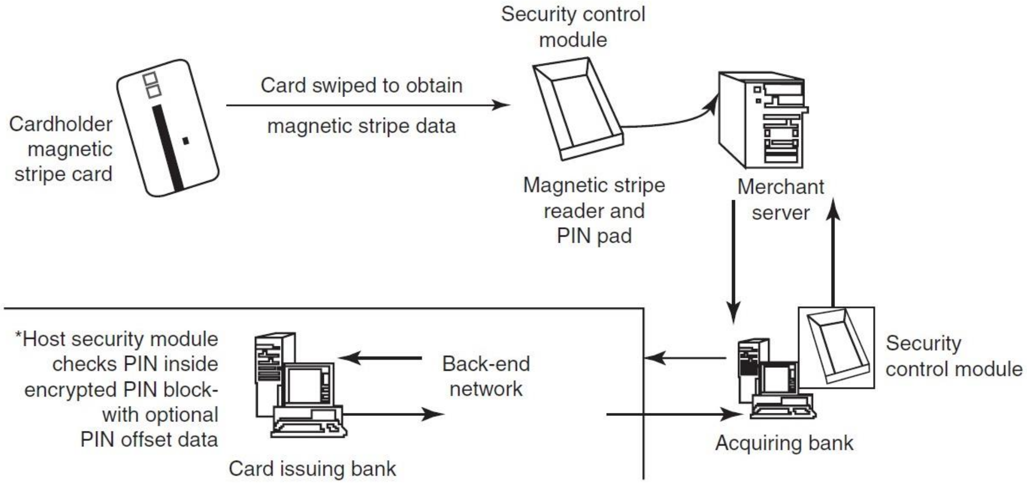

Security control module
Cardholder magnetic stripe card
Card swiped to obtain
magnetic stripe data
Magnetic stripe reader and PIN pad
Merchant server
*Host security module checks PIN inside encrypted PIN block-with optional PIN offset data
Back-end network
Security control module
Card issuing bank
Acquiring bank

Figure: Online Environment for Credit Card Transactions

Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions.

Tips to Prevent Credit Card Frauds:

Do’s

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
3. Change the default Personal Identification Number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Dont’s

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/ to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

There is a system available from an Australian company "Alacrity" called Closed-Loop Environment for Wireless (CLEW). Below figure shows the flow of events

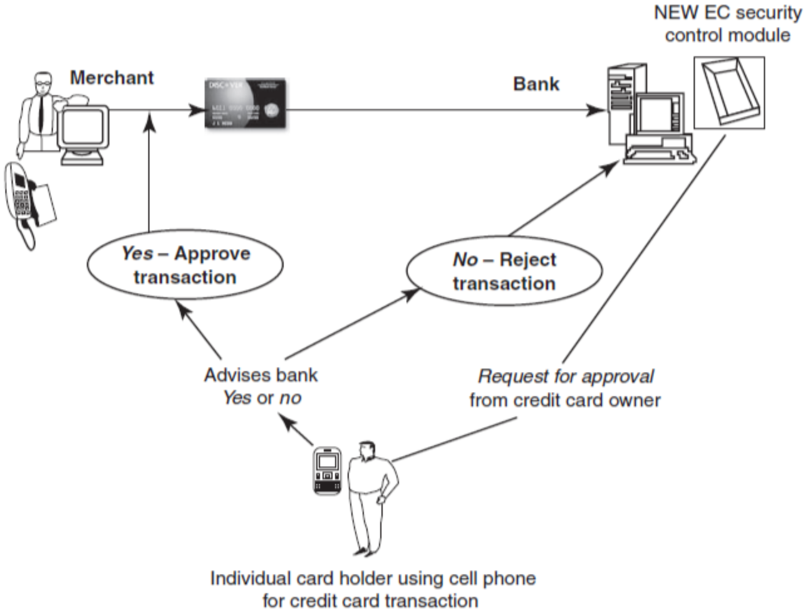

NEW EC security control module
Merchant
Bank
Yes – Approve transaction
No – Reject transaction
Advises bank Yes or no
Request for approval from credit card owner
Individual card holder using cell phone for credit card transaction

Figure: Closed-Loop Environment for Wireless (CLEW)

1. Merchant sends a transaction to bank;
2. The bank transmits the request to the authorized cardholder [not short message service (SMS)];
3. The cardholder approves or rejects (password protected);
4. The bank/merchant is notified;
5. The credit card transaction is completed.

Types and Techniques of Credit Card Frauds:

1. Traditional Techniques
    a. ID theft: Where an individual pretends to be someone else
    b. Financial fraud: Where an individual gives false information about his or her financial status to acquire credit.

2. Modern Techniques
    a. Triangulation:
        - The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.

- The customer registers on this website with his/her name, address, shipping address and valid credit card details.
- The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal’s website.
- The goods are shipped to the customer and the transaction gets completed.
- The criminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

b. Credit card generators: It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

SECURITY CHALLENGES POSED BY MOBILE DEVICES

Mobility brings two main challenges to cybersecurity:

1. on the hand-held devices, information is being taken outside the physically controlled environment and
2. remote access back to the protected environment is being granted

Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. As the number of mobile device users increases, two challenges are presented:

1. at the device level called “microchallenges” and
2. at the organizational level called “macrochallenges”

Some well-known technical challenges in mobile security are:

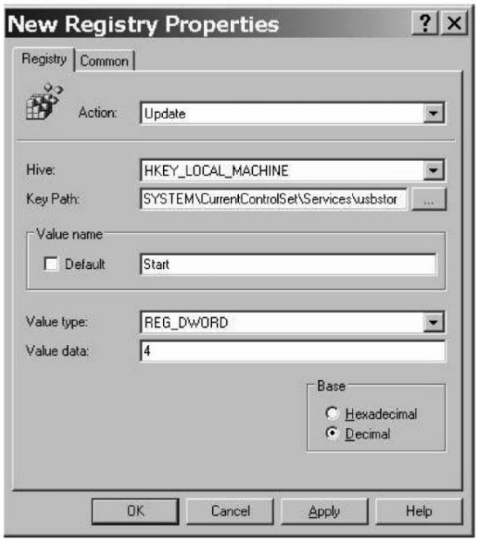
- Managing the registry settings and configurations, authentication service security
- Cryptography security
- Lightweight Directory Access Protocol (LDAP) security
- Remote Access Server (RAS) security
- Media player control security
- Networking application program interface (API) security, etc.

REGISTRY SETTINGS FOR MOBILE DEVICES

Let us understand the issue of registry settings on mobile devices through an example:

- Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook.

- ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user’s desktop to his/her device.
- In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs.
- In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.



Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\usbstor

Value name

☐ Default Start

Value type: REG_DWORD

Value data: 4

Base

○ Hexadecimal

● Decimal

Figure: Registry value browsing

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within “group policy.” Group policy is one of the core operations that are performed by Windows Active Directory.

There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against Spyware, viruses, worms, malware and other Malicious Codes that run through the networks and the Internet. The mobile security issues on a Windows platform is that the baseline security is not configured properly. When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every Control Panel setting and group policy option, they may not get the computer to the desired baseline security.

For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional registry changes that are not exposed through any interface. There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.

Naïve (Innocent) users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of “registry hacks”

AUTHENTICATION SERVICE SECURITY

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves mutual authentication between the device and the base stations or Web servers.

This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate (imitate) the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.

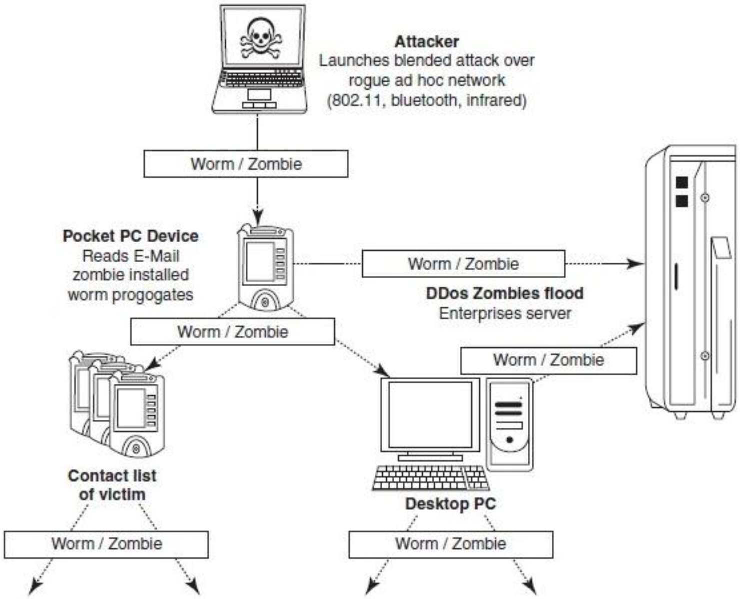


Figure: Push attack on mobile devices. DDoS implies distributed denial-of-service attack

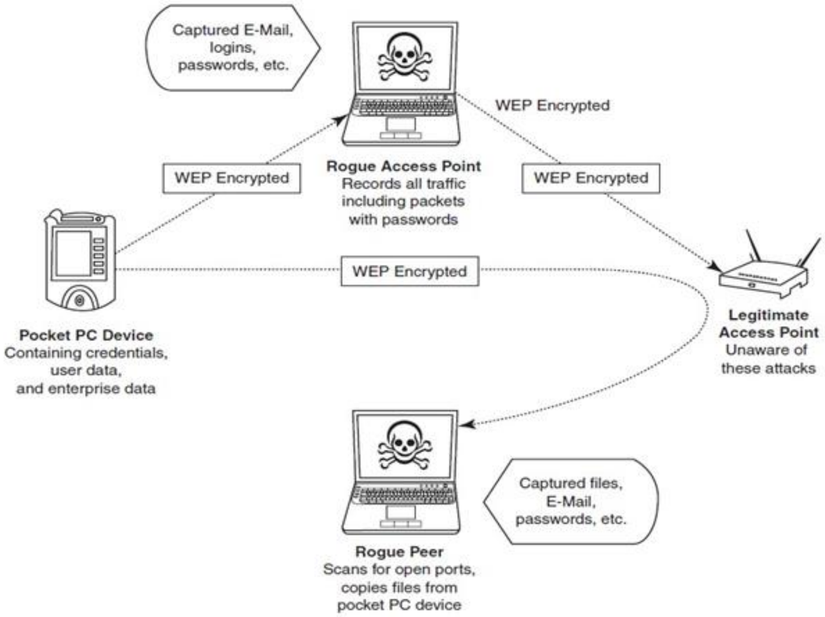

Captured E-Mail, logins, passwords, etc.
WEP Encrypted
WEP Encrypted
Rogue Access Point
Records all traffic including packets with passwords
WEP Encrypted
WEP Encrypted
Pocket PC Device
Containing credentials, user data, and enterprise data
Legitimate Access Point
Unaware of these attacks
Captured files, E-Mail, passwords, etc.
Rogue Peer
Scans for open ports, copies files from pocket PC device

Figure: Pull attack on mobile devices

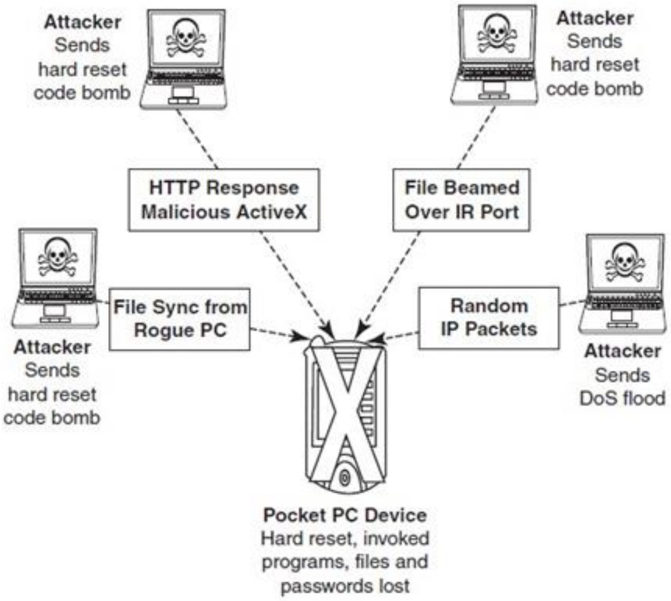

Attacker
Sends hard reset code bomb
Attacker
Sends hard reset code bomb
HTTP Response Malicious ActiveX
File Beamed Over IR Port
File Sync from Rogue PC
Random IP Packets
Attacker
Sends hard reset code bomb
Attacker
Sends DoS flood
Pocket PC Device
Hard reset, invoked programs, files and passwords lost

Figure: Crash attack on mobile devices. DoS- Denial-of-service attack

Authentication services security is important given the typical attacks on mobile devices through wireless networks: DoS attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking.

1. **Cryptographic Security for Mobile Devices:**

- Cryptographically Generated Addresses (CGA) is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.

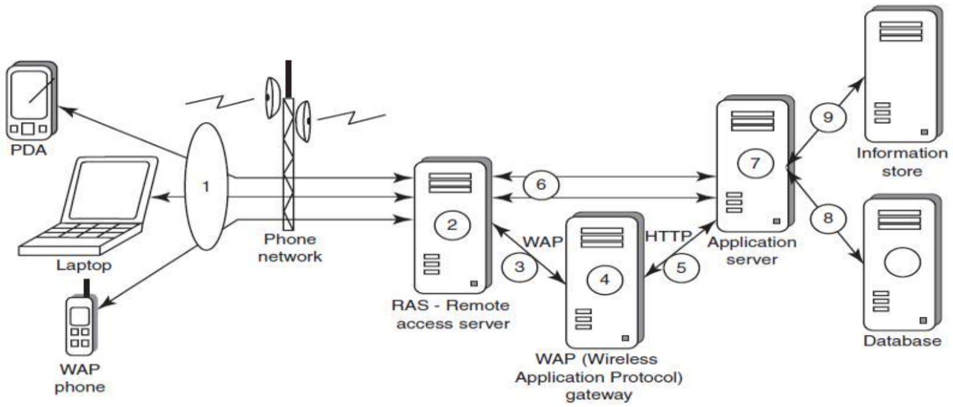
- The address the owner uses is the corresponding private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure.
- Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices.
- CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in context-aware mobile computing applications) and mobility protocols.
- It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm) are one of the most common hand-held devices used in mobile computing.
- Cryptographic security controls are deployed on these devices.
- For example, the Cryptographic Provider Manager (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device.
- The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

2. LDAP Security for Hand-held Mobile Computing Devices:

- LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organizations's Intranet).
- In a network, a directory tells you where an entity is located in the network.
- LDAP is a light weight (smaller Attacker Launches blended attack over rogue ad hoc network (802.11, bluetooth, infrared) amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version.

3. RAS Security for Mobile Devices:

RAS (Remote Access Server) is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices. In terms of cybersecurity, mobile devices are sensitive. Below Figure: organization's sensitive data can happen through mobile hand-held devices carried by employees. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (impersonating or masquerading) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.



Another threat comes from the practice of port scanning:

- First, attackers use a domain name system (DNS) server to locate the IP address of a connected computer. A domain is a collection of sites that are related in some sense.
- Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls.
- For instance, File Transfer Protocol (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers.
- Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID.
- A personal firewall on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection.

4. <u>Media Player Control Security</u>:

Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the “music gateways.” There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this.

- According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people’s computer systems and perform a variety of actions.

- According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

5. **Networking API Security for Mobile Computing Applications:**

- With the advent of electronic commerce (E-Commerce) and its further off -shoot into M-Commerce, online payments are becoming a common phenomenon with the payment gateways accessed remotely and possibly wirelessly.
- Furthermore, with the advent of Web services and their use in mobile computing applications, the API becomes an important consideration.
- Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications
- Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).
- Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.
-

ATTACKS ON MOBILE/CELL PHONES

1. **Mobile Phone Theft:** Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.

   When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)", that really matter, are lost. One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OD virus was seen after the number of Palm OS devices reached 15million. The 1st instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the user's knowledge.
2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data & applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.
3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

2. **Mobile Viruses:**

- A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
- Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays.
- In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified.
- First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
- Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones
- MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

Following are some tips to protect mobile from mobile malware attacks:

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

3. **Mishing:** Mishing is a combination of mobile and Phishing. Mishing attacks are attempted using mobile phone technology.
   - M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
   - A typical Mishing attacker uses call termed as Vishing or message (SMS) known as Smishing.
   - Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
   - Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

4. **Vishing:** Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – Voice and Phishing. Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals. The most profitable uses of the information gained through a Vishing attack include:
   - ID theft
   - Purchasing luxury goods and services
   - Transferring money/funds
   - Monitoring the victims' bank accounts
   - Making applications for loans and credit cards

   How Vishing Works:

   The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

   1. Internet E-Mail: It is also called Phishing mail.
   2. Mobile Text Messaging: Text is being messaged in Mobile.
   3. Voicemail: Here, Victim is forced to call on the provided phone number, once he/she listens to voice mail.
   4. Direct phone Call: Following are the steps detailing on how direct phone call works
      - The criminal gathers cell/mobile phone numbers located and steals mobile phone numbers after accessing cellular company.
      - The criminal often uses a dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.

- When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity.
- The message instructs the victim to call one phone number immediately.
- The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
- When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
- Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
- Such calls are often used to gain additional details such as date of birth, credit card expiration date, etc.

Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

1. Automated message: Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.

- Press 1 if you need to check your banking details and live balance.
- Press 2 if you wish to transfer funds.
- Press 3 to unlock your online profile.
- Press 0 for any other query.

2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: “The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key.”

3. The victim enters his/her bank account number and hears the next prompt: “Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950.”

4. The caller enters his/her date of birth and again receives a prompt from the automated system: “Thank you. Now please type your PIN, followed by the pound key.”

5. The caller enters his PIN and hears one last prompt from the system: “Thank you. We will now transfer you to the appropriate representative”.

At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

How to Protect from Vishing Attacks:

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

5. **Smishing:** Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMs phISHING". SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones.

SMS can be abused by using different methods and techniques other than information gathering under cybercrime. Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to "hook" the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI. Smishing works in the similar pattern as Vishing.

How to Protect from Smishing Attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.

2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

6. **Hacking Bluetooth:** Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile device. Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.

When Bluetooth is enabled on a device, it essentially broadcasts "I'm here, and I'm able to connect" to any other Bluetooth-based device within range. This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software [Bluetooth hacking tools] on a laptop and then installs Bluetooth antenna.

Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

S.No	Name of the Tool	Description
1.	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2.	BlueSniff	This is a GUI-based utility for finding discoverable and hidden Bluetooth enabled devices.
3.	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information
4.	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5.	BlueDiving	Bluediving is testing Bluetooth penetration. It implements

		attacks like Bluebug and BlueSnarf.

Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer are common attacks that have emerged as Bluetooth-specific security issues.

Bluejacking: It means Bluetooth + Jacking where Jacking is short name for hijack – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

Bluesnarfing: It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

Bluebugging: It allows attackers to remotely access a user's phone and use its features without user's attention.

Car Whisperer: It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking.

MOBILE DEVICES: SECURITY IMPLICATIONS FOR ORGANIZATIONS

1. **Managing Diversity and Proliferation of Hand-Held Devices:** Cybersecurity is always a primary concern to most organizations. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether or not the devices have been provided by the organization.

   In addition, close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove logical and physical access to organization networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.
2. **Unconventional/Stealth Storage Devices:** Compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees are the key factors for cyber attacks. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security. It is advisable to prohibit the employees in using these devices.

- Not only can viruses, worms and Trojans get into the organization network, but can also destroy valuable data in the organization network.
- Organization has to have a policy in place to block these ports while issuing the asset to the employee.
- Employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses.
- As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.
- Using “DeviceLock” software solution, one can have control over unauthorized access to plug and play devices.

The features of the software allows system administrator to:

- Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
- Control the access to devices depending on the time of the day and day of the week.
- Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
- Set devices in read-only mode.
- Protect disks from accidental or intentional formatting.

3. **Threats through Lost & Stolen Devices:** This is a new emerging issue for cybersecurity. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. The cybersecurity threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization.

   Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators.

4. **Protecting Data on Lost Devices:** At an individual level, employees need to worry about the importance of data protection especially when it resided on a mobile hand-held device. There are two reasons why cybersecurity needs to address this issue

   - Data that is persistently stored on the device
   - Always running applications

   For protecting data that are stored on the device, there are two precautions that individual can take to prevent disclosure of the data stored on a mobile device:

- Encrypting sensitive data
- Encrypting the entire file system

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss & device owners should be aware of this method.

5. **Educating the Laptop Users:** Often it so happens that corporate laptop users could be putting their company’s networks at risk by downloading non-work-related software capable of spreading viruses and spyware. This is because the software assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options. The perception plays much role in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

ORGANIZATIONAL MEASURES FOR HANDLING MOBILE DEVICES-RELATED SECURITY ISSUES

Encrypting Organizational Databases:

Critical and sensitive data reside on databases and with the advances in technology, access to these data is not impossible through hand-held devices. It is clear that to protect the organization’s data loss, such databases need encryption. Two algorithms that are typically used to implement strong encryption of database files:

- Rijndael (pronounced Rain-dahl or Rhine-doll), a block encryption algorithm, chosen as the new Advanced Encryption Standard (AES) for block ciphers by the National Institute of Standards and Technology (NIST).
- The other algorithm used to implement strong encryption of database files is the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio.

Strong encryption means that it is much harder to break, but it also has a significant impact on performance. Database file encryption technology, using either the AES (or) MDSR algorithms, makes the database inoperable without the key (password). When using strong encryption, it is important not to store the key on the mobile devices, which is equivalent to leaving a key in a locked door. However if you lose the key, data is completely inaccessible. The key is case sensitive and must be entered correctly to access the database.

For greater security there is an option available that instructs the database server to display a dialog box where the user can enter the encryption key. This option is necessary because the encryption key should not be entered on the machine in clear text.

To protect the scenario of information attack/stealing through the mobile devices connecting to the corporate databases, additional security measures are possible through enforcing a self-destruct policy that is controlled from the server. When a device that is identified or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

<u>Including Mobile Devices in Security Strategy</u>:

Organizational IT departments will have to take the accountability for cybersecurity threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection being used. There are technologies available to properly secure mobile devices, which are enough for most organizations.

Although mobile devices do pose unique challenges from a cybersecurity perceptive, there are some genera steps that the users can take to address them such as integrating security programs for mobile and wireless systems into the overall security blue print. A few things that organization can use are:

- Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
- Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
- Develop a system of more frequent and thorough security audits for mobile devices.
- Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company’s overall IT strategy.
- Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

ORGANIZATIONAL SECURITY POLICIES AND MEASURES IN MOBILE COMPUTING ERA

<u>Importance of Security Policies relating to Mobile Computing Devices</u>:

- Growth of mobile devices used makes the cybersecurity issue harder than what we would tend to think.
- People (especially, the youth) have grown so used to their mobiles that they are treating them like wallets!
- For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their hand-held devices
- One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization & also other valuable information that could impact stock values in the mobile devices.

- Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing the sensitive customer data such as credit reports, Social Security Numbers (SSNs) & contact information.
- This not only the Public Relations (PR) disaster, but it could also violate laws & regulations.
- When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure.

Operating Guidelines for Implementing Mobile Device Security Policies:

- By using the following steps we can reduce the risk when mobile device lost or stolen
- Determine whether the employees in the organization need to use mobile computing devices or not.
- Implement additional security technologies like strong encryption, device passwords and physical locks.
- Standardize the mobile computing devices and the associated security tools being used with them.
- Develop a specific framework for using mobile computing devices.
- Maintain an inventory so that you know who is using what kinds of devices.
- Establish patching procedures for software on mobile devices.
- Label the devices and register them with a suitable service.
- Establish procedures to disable remote access for any mobile.
- Remove data from computing devices that are not in use
- Provide education and awareness training to personnel using mobile devices.

Organizational Policies for the Use of Mobile Hand-Held Devices:

There are many ways to handle the matter of creating policy for mobile devices.

- One way is creating a distinct mobile computing policy.
- Another way is including such devices under existing policy.

There are also approaches in between, where mobile devices fall under both existing general policies and a new one. There may not be a need for separate policies for wireless, LAN, WAN etc because a properly written network policy can cover all connections to the company data, including mobiles & wireless.

LAPTOPS

Laptops, like other mobile devices, enhance the business functions. Their mobile access to information anytime and anywhere, they also pose a large threat as they are portable. Wireless capability in these devices has also raised cybersecurity concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Most laptops contain personal and corporate information that could be sensitive. Such information can be misused if found by a malicious user.

Physical Security Countermeasures:

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops.
2. Laptop safes: Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops
3. Motion sensors and alarms: Alarms and motion sensors are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device & the key ring device crosses the specified range.
4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in universal database for verification, which in turn makes the resale of stolen laptops a difficult process.
5. Other measures for protecting laptops are as follows:
   - Engraving the laptop with personal details
   - Keeping the laptop close to oneself wherever possible
   - Carrying the laptop in a different and unobvious bag
   - Creating the awareness among the employees about the sensitive information contained in the laptop
   - Making a copy of the purchase receipt of laptop, serial number & description of laptop
   - Installing encryption software to protect information stored on the laptop
   - Using personal firewall software to block unwanted access and intrusion
   - Updating the antivirus software regularly
   - Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
   - Never leaving the laptop unattended in public places
   - Disabling IR ports and wireless cards when not in use
   - Choosing a secure OS

- Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
- Disabling unnecessary user accounts and renaming the administrator account
- Backing up data on a regular basis

A few logical access controls are as follows:

- Protecting from malicious programs/attackers/social engineering
- Avoiding weak passwords/open access
- Monitoring application security and scanning for vulnerabilities
- Ensuring that unencrypted data/unprotected fi le systems do not pose threats
- Proper handling of removable drives/storage mediums/unnecessary ports
- Password protection through appropriate passwords rules and use of strong passwords
- Locking down unwanted ports/devices
- Regularly installing security patches and updates
- Installing antivirus software/firewalls/intrusion detection system (IDSs)
- Encrypting critical file systems
- Other countermeasures:
    - Choosing a secure OS that has been tested & has high security incorporated into it
    - Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
    - Disabling unnecessary user accounts & renaming the administrator account
    - Disabling display of the last logged in username in the login dialog box
    - Backing up data on a regular basis

UNIT -IV: Tools and Methods Used in Cybercrime

Introduction, Proxy Servers And Anonymizers, Phishing, Password Cracking, Key Loggers And Spywares, Virus And Worms, Trojan Horses And Backdoors, Steganography, DoS And DDoS Attacks, SQL Injection, Buffer Overflow, Attacks On Wireless Networks, Phishing And Identity Theft: Introduction, Phishing, Identity Theft (ID Theft)

1. Introduction
2. Proxy Servers and Anonymizers,
3. Phishing
4. Password Cracking
5. Key loggers and Spywares
6. Virus and Worms
7. Trojan Horses and Backdoors
8. Steganography
9. DoS and DDoS Attacks
10. SQL Injection
11. Buffer Overflow
12. Attacks on Wireless Networks
13. Phishing and Identity Theft: Introduction - Phishing,
14. Identity Theft (ID Theft)

Introduction

Different forms of attacks through which attackers target the computer systems are as follows:

1. Initial uncovering:
   - Two steps are involved here.
     1. In the first step called as reconnaissance, the attacker gathers information about the target on the Internet websites.
     2. In the second step, the attacker finds the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges to steal the data.
2. Network probe (investigation):

- At the network probe stage, the attacker scans the organization information through a “ping sweep” of the network IP addresses.
- Then a “port scanning” tool is used to discover exactly which services are running on the target system.
- At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.

3. Crossing the line toward electronic crime (E-crime):
   - Once the attackers are able to access a user account, then they will attempt further exploits to get an administrator or “root” access.
   - Root access is a UNIX term and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems).
   - “Root” is an administrator or super-user access and grants them the privileges to do anything on the system.
4. Capturing the network:
   - At this stage, the attacker attempts to “own” the network. The attacker gains the internal network quickly and easily by target systems.
   - The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files and services that have a backdoor password.
5. Grab the data:
   - Now that the attacker has “captured the network,” he/she takes advantage of his/her position to steal confidential data
6. Covering tracks:
   - This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
   - The attacker can remain undetected for long periods.
   - During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself.

Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connection with other computers on that network.

- The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy.
- This enables an attacker to surf on the Web anonymously and/or hide the attack.
- A client connects to the proxy server and requests some services (such as a file, webpage) available from a different server.
- The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client.
- Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the web pages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address
    - One of the advantages of a proxy server is that its cache memory can serve all users.
    - If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time.
    - An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
    - Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.

Phishing

"Phishing" refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes.

- While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening to close the bank account if he/she does not reply immediately.
- Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail.
- This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases.
- These messages look authentic and attempt to get users to reveal their personal information.
- It is believed that Phishing is an alternative spelling of "fishing," as in "to fish for information."
- The first documented use of the word "Phishing" was in 1996.

How Phishing Works?

Phishers work in the following ways:

1. Planning: Criminals, usually called as phishers, decide the target.
2. Setup: Once phishers know which business/business house to spoof and who their victims.
3. Attack: the phisher sends a phony message that appears to be from a reputable source.
4. Collection: Phishers record the information of victims entering into webpages or pop-up windows.
5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

Password Cracking

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach – repeatedly making guesses for the password.

The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user’s personal information. Examples of guessable passwords include:

1. Blank (none);
2. the words like “password,” “passcode” and “admin”;
3. series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwertyuiop;
4. user’s name or login name;
5. name of user’s friend/relative/pet;
6. user’s birthplace or date of birth, or a relative’s or a friend’s;
7. user’s vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;

- An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list.
- This is still considered manual cracking, is time-consuming and not usually effective.
- Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource.
- To ensure confidentiality of passwords, the password verification data is usually not stored in a clear text format.
- For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored.
- When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called authentication.

The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Password cracking attacks can be classified under three categories as follows:

1. Online attacks;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving).

Online Attacks

- An attacker can create a script file that will be executed to try each password in a list and when matches, an attacker can gain the access to the system.
- The most popular online attack is man-in-the middle (MITM) attack, also termed as “bucket- brigade attack” or sometimes “Janus attack.”
- It is a form of active stealing in which the attacker establishes a connection between a victim and the server to which a victim is connected.
- When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in- the-middle).

- This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

Offline Attacks

- Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.
- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

Password guidelines.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts and banking/financial user accounts should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts and banking/financial user accounts should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyberattacks.
8. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Keyloggers and Spywares

- Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.
- Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

Software Keyloggers

- Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.
- Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user.
- Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafés, etc) and can obtain the required information about the victim very easily.
- A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.

Some Important Keyloggers are as follows

All In One Keylogger	Stealth Keylogger	Perfect Keylogger
KGB Spy	Spy Buddy	Elite Keylogger
CyberSpy	Powered Keylogger	

Hardware Keyloggers

- Hardware keyloggers are small hardware devices.
- These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.
- Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs.
- Each keypress on the keyboard of the ATM gets registered by these keyloggers.
- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and can remove the tool. (Visit http://www.anti-keyloggers.com for more information)

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chatting.

Spywares

- Spyware is a type of malware (i.e., malicious software) that is installed on computers which collects information about users without their knowledge.
- The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer.
- Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

Some Important Spywares are as follows:

Spy.	**Spector Pro.**	**Spector Pro.**
eBlaster.	Remotespy .	Stealth Recorder Pro.
Stealth Website Logger.	Flexispy.	Wiretap Professional.
PC PhoneHome.	SpyArsenal Print Monitor Pro.	

Box 4.3 | Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code. Malware can be classified as follows:

1. Viruses and worms: These are known as *infectious malware*. They spread from one computer system to another with a particular behavior.
2. Trojan Horses: A Trojan Horse,[14] Trojan for short, is a term used to describe malware that appears,to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system
3. Rootkits: Rootkits is a software system that consists of one or more programs designed to obscurethe fact that a system has been compromised.
4. Backdoors: Backdoor[16] in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.
5. Spyware:
6. Botnets:
7. Keystroke loggers:

Virus and Worms

- Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern.
- Viruses can often spread without any readily visible symptoms.
- A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random.

Viruses can take some typical actions:

1. Display a message to prompt an action which may set of the virus;

2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

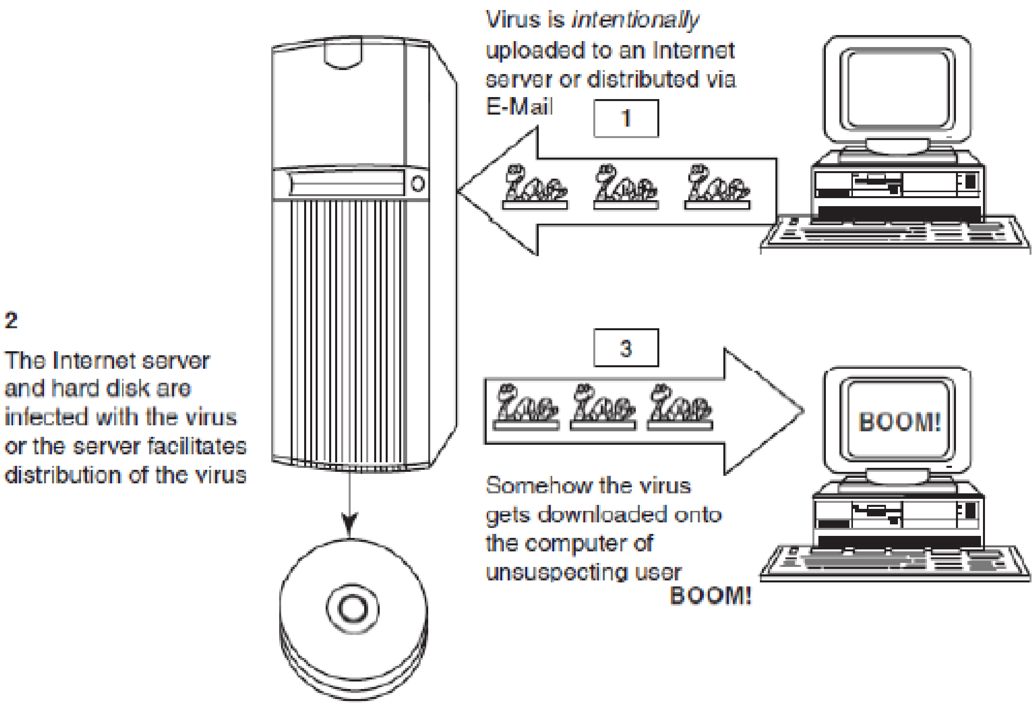

Virus is *intentionally* uploaded to an Internet server or distributed via E-Mail
1
2
The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus
3
BOOM!
Somehow the virus gets downloaded onto the computer of unsuspecting user
BOOM!

Figure: Virus Spread Through Internet

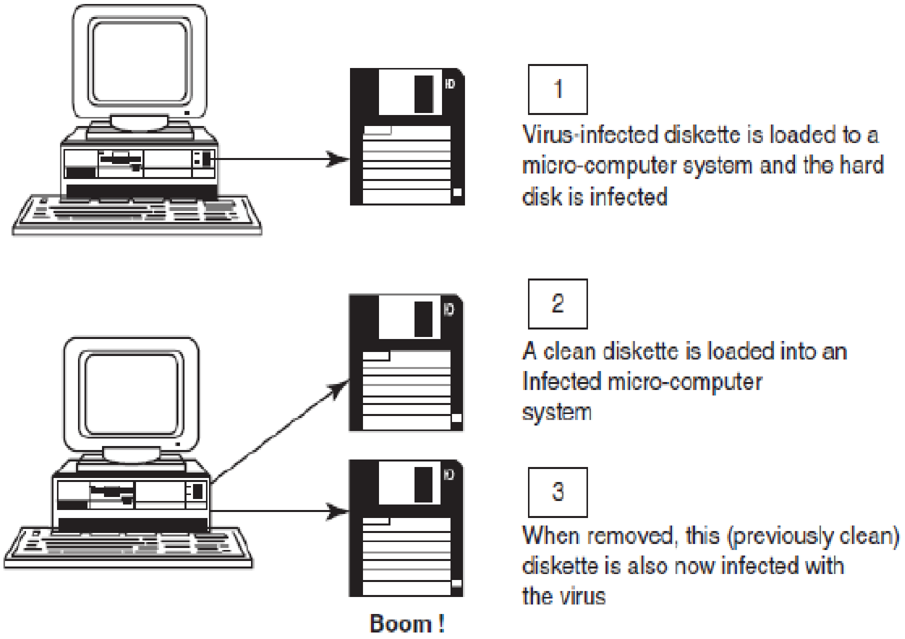

1
Virus-infected diskette is loaded to a micro-computer system and the hard disk is infected
2
A clean diskette is loaded into an Infected micro-computer system
3
When removed, this (previously clean) diskette is also now infected with the virus
Boom !

Figure: Virus Spread Through stand alone System

- **Computer virus** has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sent it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives.
- Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.
- Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses.
- Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm).
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions.

- Worms and Trojans, such as viruses, may harm the system's data or performance.
- Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them.
- Some viruses do nothing beyond reproducing themselves.

Types of Viruses

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system.
2. **Program viruses:** These viruses become active when the program file (usually with extensions .bin, .com,.exe, .ovl, .drv) is excuted
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active.
4. **Stealth viruses:** It hides itself and so detecting this type of virus is very difficult. It can hiding itself such a way that antivirus software also cannot detect it. Example for Stealth virus is "Brain Virus".
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus with the help of an antivirus program.
6. **Macro viruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once macrovirus gets onto a victim's computer then every document he/she produces will become infected.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls.

World's worst worm attacks.

Conficker	INF/AutoRun	Win32 PSW	Win32/Agent
Win32/FlyStudio	Win32/Pacex.Gen	Win32/Qhost	WMA/ TrojanDownloader

The world's worst virus and worm attacks!!!

Morris Worm	ILOVEYOU	Nimda	Jerusalem
Code Red	Melissa	Melissa	
Sobig	Storm Worm	Michelangelo	

Trojan Horses and Backdoors

- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.
- A Trojan Horse may get widely redistributed as part of a computer virus.
- The term Trojan Horse comes from Greek mythology about the Trojan War.
- Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail.
- It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines.
- Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.
- On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.
- For example, waterfalls.scr is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download files without your knowledge.
6. They gather E-Mail addresses and use them for Spam.

7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porno sites, play sounds/videos and display images.
9. They slow down, restart or shutdown the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves as part of an exploit.
- In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.
- A backdoor works in background and hides from the user.
- It is very similar to a virus and, therefore, is quite difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite, as it allows a malicious person to perform any possible action on a compromised system.

Following are some functions of backdoor:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.
2. It allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission.
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and tracks web browsing habits.

4. It records keystrokes that a user types on a computer’s keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.

Following are a few examples of backdoor Trojans:

1. Back Orifice
2. Bifrost:
3. SAP backdoors
4. Onapsis Bizploit:

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. Stay away from suspect websites/weblinks:
2. Surf on the Web cautiously:
3. Install antivirus/Trojan remover software:

Steganography

- Steganography is the practice of concealing (hiding) a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos , meaning "covered, concealed, or protected", and graphein meaning "writing".
- It is a method that attempts to hide the existence of a message or communication.
- Steganography is always misunderstood with cryptography
- The different names for steganography are data hiding, information hiding and digital watermarking.
- Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data.
- *Digital watermarking* is the process of possibly irreversibly embedding information into a digital signal.
- The Digital signal may be, for example, audio, pictures or video.

- If the signal is copied then the information is also carried in the copy.
- In other words, when steganography is used to place a hidden “trademark” in images, music and software, the result is a technique referred to as “watermarking”

Steganalysis

- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.
- The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it.
- Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files.

Box 4.7 | Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, of the message itself is not disguised, but the content is obscured. It is said that terrorists use where the existence steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple.

DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

DoS Attacks

- In this type of criminal act, **the attacker floods the bandwidth of the victim’s network** or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.
- **The attackers typically target sites or services hosted on high-profile web servers** such as banks, credit card payment gateways, mobile phone networks and even root name servers.

- Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*.
- The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the ID of the sender or impersonating another computing system.
- A packet is a formatted unit of data carried by a packet mode computer network.
- The attacker spoofs the IP address and floods the network of the victim with repeated requests.
- As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request.
- This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.
- The United States Computer Emergency Response Team defines symptoms of DoS attacks to include:
    1. Unusually slow network performance (opening files or accessing websites);
    2. unavailability of a particular website;
    3. inability to access any website;
    4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.

A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

Classification of DoS Attacks

1. **Bandwidth attacks:** Loading any website takes certain time. Loading means complete webpage appearing on the screen and system is awaiting user's input.

2. **Logic attacks:** These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3. **Protocol attacks**: Protocols here are rules that are to be followed to send data over network.
4. **Unintentional DoS attack :** This is a scenario where a website ends up denied not due to a attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity.

Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping food*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle.
2. **Ping of death attack:** The ping of death attack **sends oversized Internet Control Message Protocol (ICMP) packets,** and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim.
3. **SYN attack:** It is also termed as ***TCP SYN Flooding***. In the TCP, handshaking of network connections is done with SYN and ACK messages.
   - An attacker initiates a TCP connection to the server with an SYN.
   - The server replies with an SYN-ACK.
   - The client then does not send back an ACK, causing the server to allocate memory for the pending connection and wait.
   - This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system.
4. **Teardrop attack:** The teardrop attack is an attack where **fragmented packets are forged to overlap each other when the receiving host tries to reassemble them**. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim

and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code.

5. **Smurf attack:** This is a type of DoS attack that **floods a target system via spoofed broadcast ping messages.** This attack consists of a host sending an echo request (ping) to a network broadcast address.
6. **Nuke:** Nuke is an old DoS attack against computer networks consisting of **fragmented or invalid packets sent to the target.**

Tools Used to Launch DoS Attack

1. **Jolt2 :** The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines – the attack causes the target machine to consume of the CPU time on processing of illegal packets.
2. **Nemesy :** This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3. **Targa :** It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4. **Crazy Pinger :** This tool could send large packets of ICMP(Internet Control Message Protocol) to a remote target network.
5. **SomeTrouble:** It is a remote flooder and bomber. It is developed in Delphi.

DDoS Attacks

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- The attack is “distributed” because the attacker is using multiple computers, including yours, to launch the DoS attack.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system.

- The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- Malware can carry DDoS attack mechanisms – one of the better-known examples of this is MyDoom.
- Botnet is the popular medium to launch DoS/DDoS attacks.
- Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts.

How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.

1. Implement router **filters**. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, **install patches** to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system’s performance and establish baselines for ordinary activity.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain “hot spares” – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules
11. Establish and maintain appropriate password policies

SQL Injection

- Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS).
- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

- SQL injection attacks are also known as SQL insertion attacks.
- Attackers target the SQL servers – common database servers used by many organizations to store confidential data.
- The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords.
- During an SQL injection attack, Malicious Code is inserted into a web form field or the website's code.
- For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password.
- With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source" – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code.

   Everything between the <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.

   <FORM action=Search/search.asp method=post>

   <input type=hidden name=A value=C>

   </FORM>
3. The attacker inputs a *single quote* under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is interpreted literally by the server. If the response is an error message such as *use "a" = "a"* then the website is found to be susceptible to an SQL injection attack.

4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

Here are few examples of variable field text the attacker uses on a webpage to test for SQL vulnerabilities:

1. *Blah' or 1=1*--
2. *Login:blah' or 1=1*--
3. *Password::blah' or 1=1*--
4. *http://search/index.asp?id=blah' or 1=1*--

Similar SQL commands may allow bypassing of a login and may return many rows in a table or even an entire database table because the SQL server is interpreting the terms literally. The double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

Blind SQL Injection

- Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.
- The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page.
- This type of attack can become time-intensive because a new statement must be crafted for each bit recovered.
- There are several tools that can automate these attacks once the location of the vulnerability and the target information have been established.

How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. **Input validation**
    - Replace all single quotes to two single quotes.
    - Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character

sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack.

- Numeric values should be checked while accepting a query string value. Function – IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values.
- Keep all text boxes and form fields as short as possible to limit the length of user input.

2. **Modify error reports:** SQL errors should not be displayed to outside users
3. **Other preventions**
    - The default system accounts for SQL server 2000 should never be used.
    - Isolate database server and web server.

Buffer Overflow

- Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it.
- This may result unreliable program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.
- Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates.
- They are, thus, the basis of many software vulnerabilities and can be maliciously exploited.

Bounds checking can prevent buffer overflows.

- Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array.
- 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.
- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.
- The knowledge of C, C++ or any other high-level computer language (i.e., assembly language) is essential to understand buffer overflow.

For example,

```
int main () {
int buffer[10];
buffer[20] = 10;
}
```

- This C program is a valid program and every compiler can compile it without any errors.
- However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior.

Types of Buffer Overflow

Stack-Based Buffer Overflow

Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer. Here are the characteristics of stack-based programming:

1. "Stack" is a memory space in which automatic variables (and often function parameters) are allocated.
2. Function parameters are allocated on the stack and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.
3. Once a function has completed its cycle, the reference to the variable in the stack is removed.

The attacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

1. A local variable that is near the buffer in memory on the stack to change the behavior of the program that may benefit the attacker.
2. The return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input-filled buffer.
3. A function pointer, or exception handler, which is subsequently executed.

The factors that contribute to overcome the exploits are

1. Null bytes in addresses;
2. Variability in the location of shell code;
3. Differences between environments.

A shell code is a small piece of code used as a payload in the exploitation of software vulnerability.

It is called “shell code” because it starts with command shell from which the attacker can control the compromised machine.

NOPs

NOP or NOOP (short form of **no operation**) is an assembly language instruction/ command that effectively does nothing at all.

Heap Buffer Overflow

Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. The characteristics of stack based and heap-based programming are as follows:

1. “Heap” is a “free store” that is a memory space, where dynamic objects are allocated.
2. The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions; it is different from the memory space allocated for stack and code.
3. Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zero.

Memory on the heap is dynamically allocated by the application at run-time and normally contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers.

How to Minimize Buffer Overflow

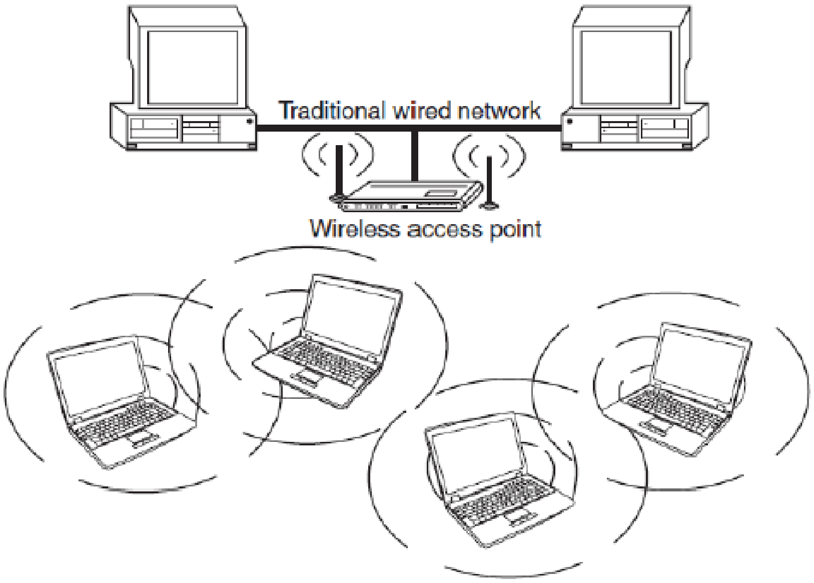
Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

1. **Assessment of secure code manually:** Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of functions like strcpy(), strcat(), sprintf() and vsprintf() in C Language.
2. **Disable stack execution:** Malicious Code causes input argument to the program, and it resides in the stack and not in the code segment. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation.

3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as gets(), strcpy(), etc. Developers should be educated to restructure the programming code if such warnings are displayed.
4. **Dynamic run-time checks:** In this scheme, an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions or it can ensure that return addresses are not overwritten. One example of such a tool is libsafe. The libsafe library provides a way to secure calls to these functions, even if the function is not available.

Attacks on Wireless Networks

- Wireless technologies have become increasingly popular in day-to-day business and personal lives.
- Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
- Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs.
- Wireless networks are generally composed of two basic elements
    - access points (APs) and
    - other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or “connect” with each other.
- APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.
- Wireless access to networks has become very common by now in India – for organizations and for individuals.



Wireless Networks

The following are different types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in semi-tethered (connected) environments where modem use frequently.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office;

Important components of wireless network

1. **802.11 networking standards:** Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication.
2. **Access points:** It is also termed as AP. It is a hardware device and/or software that act as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.

3. **Wi-Fi hotspots:** A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.
    - *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that to without any authentication.
    - *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas.
4. **Service Set IDentifier (SSID):** It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID.
5. **Wired equivalence privacy (WEP):** Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.
6. **Wi-Fi protected access (WPA and WPA2):** WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.
7. **Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network.

Tools used for hacking wireless networks
NetStumbler: This tool is based on Windows OS and easily identifies wireless signals being broadcast within range.
Kismet: This tool detects and displays SSIDs that are not being broadcast which 0is very critical in finding wireless networks.

Airsnort: This tool is very easy and is usually used to sniff and crack WEP keys

CowPatty: This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the “New WEP” for home wireless security.

Wireshark (formerly ethereal): Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.

Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access is termed as *wireless cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. **Sniffing:** The attacker usually installs the sniffers remotely on the victim’s system and conducts activities such as
   - Passive scanning of wireless network;
   - detection of SSID;
   - colleting the MAC address;
   - collecting the frames to crack WEP.
2. **Spoofing:** The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a original network. Different types of Spoofing are as follows.
   - *MAC address Spoofing*
   - *IP Spoofing:*
   - *Frame Spoofing:*
3. **Denial of service (DoS):** We have explained this attack in detail in UNIT-2.
4. **Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host *A* inserts *A* between all communications – between hosts *X* and *Y* without knowledge of *X* and *Y*. All messages sent by *X* do reach *Y* but through *A* and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.

5. **Encryption cracking:** It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

How to Secure the Wireless Networks

Nowadays, security features of Wi-Fi networking products are not that time-consuming and nonintuitive; however, they are still ignored, especially, by home users. Although following summarized steps will help to improve and strengthen the security of wireless network, to know the available tools to monitor and protect the wireless networks:

1. Change the default settings of all the equipments/components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. Enable WPA/WEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the features that are not used in the AP (e.g., printing/music support).
8. Avoid providing the network a name which can be easily identified (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., do not autoconnect to open Wi-Fi hotspots).
10. Upgrade router’s firmware periodically.
11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

Box 4.11 | The New "Wars" in the Internet Era!

1. Warwalking:

2. Warbiking:

3. Warkitting:

4. WAPKitting:

5. WAPjacking:

Phishing and Identity Theft: Introduction , Phishing

Identity theft can be done thorough the following ways.

1. **Spam E-Mails**
    - Also known as "junk E-Mails" they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of Spam.
    - Types of Spam E-Mails are as follows:
2. **Unsolicited bulk E-Mail (UBE):** It is *synonym for SPAM* unsolicited E-Mail sent in large quantities.
3. **Unsolicited commercial E-Mail (UCE):** Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Examples:

1. **HSBC, Santander, CommonWealth Bank:** International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fish.
2. **eBay:** It is a popular auction site, often mimicked to gain personal information.
3. **Amazon:** It was the top brand to be exploited by phishers till July 2009.
4. **Facebook:** Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

   The E-Mail will usually ask the user to provide valuable information about himself /herself or to "verify" information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:

1. **Names of legitimate organizations:** Instead of creating a phony company from scratch, the phisher might use a legitimate company's name and incorporate the look and feel of its website (i.e., including the color scheme and graphics) into the Spam E-Mail.
2. **"From" a real employee:** Real name of an official, who actually works for the organization. This way, if a user contacts the organization to confirm whether "Rajeev Arora" truly is "Vice President of Marketing" then the user gets a positive response and feels assured.
3. **URLs that "look right":** The E-Mail might contain a URL (i.e., weblink) which seems to be original website wherein user can enter the information the phisher would like to steal.
4. **Urgent messages:** Creating a fear to trigger a response is very common in Phishing attacks – the E-Mails warn that failure to respond will result in no longer having access to the account or E-Mails might claim that organization has detected suspicious activity in the users' account or that organization is implementing new privacy software for ID theft solutions.

Here are a few examples of phrases used to entice the user to take the action.

1. "Verify your account":

2. "You have won the lottery":

3. "If you don't respond within 48 hours, your account will be closed":

Let us understand the ways to reduce the amount of Spam E-Mails we receive.

1. Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.
2. Never reply or open any Spam E-Mails.
3. Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT (.); for example, Rajeev**AT**gmail**DOT**com. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.

4. Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses.
5. Do not forward any E-Mails from unknown recipients.
6. Make a habit to preview an E-Mail before opening it.
7. Never use E-Mail address as the screen name in chat groups or rooms.
8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

B. Hoax E-Mails (deceive or trick E-Mail)

- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- It is difficult sometimes to recognize whether an E-Mail is a "Spam" or a "hoax."
- **The websites mentioned below** can be used to check the validity of such "hoax" E-Mails.

1. **www.breakthechain.org: T**his website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails.
2. **www.hoaxbusters.org:** This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy.

Identity Theft (ID Theft)

- This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.
- ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).
- The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as **Identity Theft Resource Center (ITRC)**, with the objective to extend the support to the society to spread awareness about this fraud.

- Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.

1. **Credit card fraud (26%):**
2. **Bank fraud (17%):** Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft
3. **Employment fraud (12%):** In this fraud, the attacker borrows the victim's valid SSN to obtain a job.
4. **Government fraud (9%):** This type of fraud includes SSN, driver license and income tax fraud.
5. **Loan fraud (5%):** It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.

It is important to note the various usage of ID theft information.

1. 66% of victims' personal information is used **to open a new credit account** in their name.
2. 28% of victims' personal information is used **to purchase cell phone service**.
3. 12% of victims end up having **warrants issued in their name** for financial crimes committed by the identity thief.

Personally Identifiable Information (PII)

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

1. Full name;
2. national identification number (e.g., SSN);
3. telephone number and mobile phone number;
4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

The information can be further classified as

a. non-classified and
b. classified.

1. **Non-classified information**
   - **Public information:**
   - **Personal information:**
   - **Routine business information:**
   - **Private information:**
2. **Classified information**
   - **Confidential:** Information that requires protection and unauthorized disclosure could damage national security (e.g., information about strength of armed forces and technical information about weapons).
   - **Secret:** Information that requires substantial protection and unauthorized disclosure could seriously damage national security (e.g., national security policy, military plans or intelligence operations).
   - **Top secret:** Information that requires the highest degree of protection and unauthorized disclosure could severely damage national security (e.g., vital defense plans and cryptologic intelligence systems).

ID theft fraudsters and/or industrial/international spies target to gain the access to private, confidential, secret and top secret information.

Types of Identity Theft

1. Financial identity theft;
2. criminal identity theft;
3. identity cloning;
4. business identity theft;
5. medical identity theft;
6. synthetic identity theft;
7. child identity theft.

Techniques of ID Theft

1. **Human-based methods:**
   - *Direct access to information:*
   - *Dumpster diving:*
   - *Theft of a purse or wallet:*
   - *Mail theft and rerouting:*
   - *Shoulder surfing:*
   - *Dishonest or mistreated employees:*
   - *Telemarketing and fake telephone calls:*
2. **Computer-based technique:**
   - *Backup theft:*
   - *Hacking, unauthorized access to systems and database theft:*
   - *Phishing:*
   - *Pharming:*
   - *Hardware:*

Cybercrimes and Cyber security

1. Why Do We Need Cyber laws: The Indian Context.
2. The Indian IT Act.
3. Challenges to Indian Law and Cybercrime Scenario in India.
4. Consequences of Not Addressing the Weakness in Information Technology Act.
5. Digital Signatures and the Indian IT Act.
6. Information Security Planning and Governance.
7. Information Security Policy Standards and Practices.
8. The information Security Blueprint.
9. Security education, Training and awareness program.
10. Continuing Strategies.

Why Do We Need Cyberlaws: The Indian Context

- Cyberlaw is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks.
- Under the preview of cyberlaw, there are several aspects, such as, *intellectual property*, *data protection and privacy*, *freedom of expression* and *crimes committed using computers*.
- The Indian Parliament passed its first cyberlaw, the ITA 2000, aimed at providing the legal infrastructure for E-Commerce in India.
- ITA 2000 received the assent of the President of India and it has now become the law of the land in India.
- The Government of India felt the need to enact relevant cyberlaws to regulate Internet based computer related transactions in India.
- It manages all aspects, issues, legal consequences and conflict in the world of cyberspace, Internet or WWW.
- In the Preamble to the Indian ITA 2000, it is mentioned that it is an act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as *electronic commerce*.
- The reasons for enactment of cyberlaws in India are summarized below:

1. Although India possesses a very well defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence.

- Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old off ense but in an innovative way.
- Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000.
- It talks about cyberlaws and forms the legal framework for electronic records and other activities done by electronic means.

The Indian IT Act

- As mentioned above, this Act was published in the year 2000 with the purpose of providing legal recognition for transactions carried out by means of electronic data interchange, commonly referred to as *electronic commerce*.
- Electronic communications involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies.
- Another purpose of the Indian IT Act was to amend the Indian Penal Code (IPC), the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, the Reserve Bank of India Act 1934 and matters connected therewith or incidental thereto.
- The Reserve Bank of India Act has got Section 58B about Penalties. Subsequently, the Indian IT Act underwent some important changes to accommodate the current cybercrime scenario; a summary of those changes is presented in Table 6.7 – note

specially the changes to Section 66 and the corresponding punishments for cyber offenses.

- The scope and coverage of the Indian IT Act is briefly described in Section 27.4, Ref. #6, Books, Further Reading.
- The structure of the Indian ITA 2000 is provided in Table 6.6 for readers' immediate reference.
- The sections mentioned in bold italics are relevant in the discussion of cybercrime and information security.

ITA Sections are as follows:

1. Section 65: Tampering with computer source documents
2. Section 66: Computer-related offences
3. Section 67: Punishment for publishing or transmitting obscene material in electronic form
4. Section 71: Penalty for misrepresentation
5. Section 72: Penalty for breach of confidentiality and privacy
6. Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars
7. Section 74: Publication for fraudulent purpose

Positive Aspects of the ITA 2000

The Indian ITA 2000, though heavily criticized for not being specific on cybercrimes, in our opinion, does have a few good points.

1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.

3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000.
4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding ` 10,000,000.
5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

Weak Areas of the ITA 2000

As mentioned before, there are limitations too in the IT Act; those are mainly due to the following gray areas:

1. The ITA 2000 is likely to cause a conflict of jurisdiction.
2. E-Commerce is based on the system of domain names. The ITA 2000 does not even touch the issues relating to domain names.
3. The ITA 2000 does not deal with issues concerning the protection of Intellectual Property Rights (IPR)
4. As the cyberlaw is evolving, so are the new forms and manifestations of cybercrimes. The offenses defined in the ITA 2000 are by no means exhaustive.
5. The ITA 2000 has not tackled issues related to E-Commerce like privacy and content regulations.

Challenges to Indian Law and Cybercrime Scenario in India

The offenses covered under the Indian ITA 2000 include:

1. Tampering with the computer source code or computer source documents;
2. un-authorized access to computer ("hacking" is one such type of act);
3. publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest;

4. 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 off ense;
5. securing access or attempting to secure access to a protected system;
6. misrepresentation while obtaining, any license to act as a Certifying Authority (CA) or a digital signature certificate;
7. breach of confidentiality and privacy;
8. publication of digital signature certificates which are false in certain particulars;
9. publication of digital signature certificates for fraudulent purposes.

- There are legal drawbacks with regard to cybercrimes addressed in India – there is a need to improve the legal scenario.
- These drawbacks prevent cybercrimes from being addressed in India.
- **First**, the difficulties/ drawbacks with most Indians not to report cybercrimes to the law enforcement agencies because they fear it might invite a lot of harassment.
- **Second**, their awareness on cybercrime is relatively on the lower side.
- Another factor that contributes to the difficulty of cybercrime resolution is that the law enforcement agencies in the country are neither well equipped nor knowledgeable enough about cybercrime.
- There is a tremendous need for training the law enforcement agencies in India. Not all cities have cybercrime cells.
- Most investigating officers with the Police force may be well equipped to fight cybercrime we need dedicated, continuous and updated training of the law enforcement agencies.

Consequences of Not Addressing the Weakness in Information Technology Act

- In light of the discussion so far, we can see that there are many challenges in the Indian scenario for fight with cybercrime.
- Cyberlaws of the country are yet to reach the level of sufficiency and adequate security to serve as a strong platform to support India's E-Commerce industry for which they were meant. India has lagged behind in keeping pace with the world in this regard.
- The consequences of this are visible – India's outsourcing sector may get impacted.

- There are many news about overseas customer worrying about data breaches and data leakages in India.
- This can result in breaking India’s IT business leadership in international outsourcing market.
- Outsourcing is on the rise; if India wishes to maintain its strong position in the global outsourcing market, there should be quick and intelligent steps taken to address the current weaknesses in the Information Technology Act.
- If this is not addressed in the near future, then the dream of India ruling the world’s outsourcing market may not come true.

Digital Signatures and the Indian IT Act

A few technical concepts regarding Digital Signature.

Public-Key Certificate

- A public-key certificate is a digitally signed statement from one entity, saying that the public key of another entity has some specific value.
- A digital signature is a type of electronic signature that is used to guarantee the integrity of the data.
- When linked to the identity of the signer – using a security token such as X.509 Certificates – Which is a digital signature.
- An X.509 Certificate contains information about the certificate subject and the certificate issuer (the CA that issued the certificate).
- The role of a certificate is to associate an identity with a public-key value.
- A certificate includes:

1. **X.509 version** information;
2. a **serial number** that uniquely identifies the certificate;
3. a **common name** that identifies the subject;
4. the **public key** associated with the common name;
5. the **name of the user** who created the certificate, known as the subject name;
6. information about the **certificate issuer**;
7. **signature of the issuer**;

8. information about the **algorithm** used to sign the certificate;
9. some optional **X.509 version 3 extensions**.

Representation of Digital Signatures in the ITA 2000

- ITA 2000 had prescribed digital signatures based on Asymmetric cryptosystem and Hash system as the only acceptable form of authentication of electronic documents recognized as equivalent to “signatures” in paper form.
- When the ITA 2000 was drafted, there was a slip-up in the drafting of Section 35, subsection (3), which made it mandatory for an applicant of a digital signature certificate to enclose a *Certification Practice Statement* along with his application.
- One of the major deficiencies in the bill, which could hinder implementation, is the provisions regarding the role and function of the CAs as well as the process of issuing digital certificates.

Impact of Oversights in ITA 2000 Regarding Digital Signatures

- The Ministry of Information and Technology had to urgently establish a task force to assist them in the drafting of the rules.
- The task force consisted of experts in the field.
- It is said that now this blunder has been accompanied by more avoidable confusions.
- The Information Technology Amendment Bill 2006 was drafted on the basis of the recommendations of an “Expert Committee.”
- The Committee took into consideration a recommendation from technical community that
  - the PKI-based system made the law dependent on a single authentication technology and
  - there was a need to make the law *Technology Neutral*

Information Security Planning and Governance

- Strategic planning sets the long-term direction to be taken by the organization and each of its component parts.
- Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined goals.

- After an organization develops a general strategy, it generates an overall strategic plan by extending that general strategy into plans for major divisions.
- Each level of each division then translates those plan objectives into more specific objectives for the level below.
- To execute this broad strategy, the executive team must first define individual responsibilities.
- The executive team is sometimes called the organization's C-level, as in CEO, COO, CFO, CIO, and so on.

Planning Levels

a. **Operational plan:** The documented product of operational planning; a plan for the organization's intended operational efforts on a day-to-day basis for the next several months.

b. **Operational planning**: The actions taken by management to specify the short-term goals and objectives of the organization in order to obtain specified tactical goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

c. **Tactical plan:** The documented product of tactical planning; a plan for the organization's intended tactical efforts over the next few years.

d. **Tactical planning**: The actions taken by management to specify the intermediate goals and objectives of the organization in order to obtain specified strategic goals, followed by estimates and schedules for the allocation of resources necessary to achieve those goals and objectives.

Information Security Governance

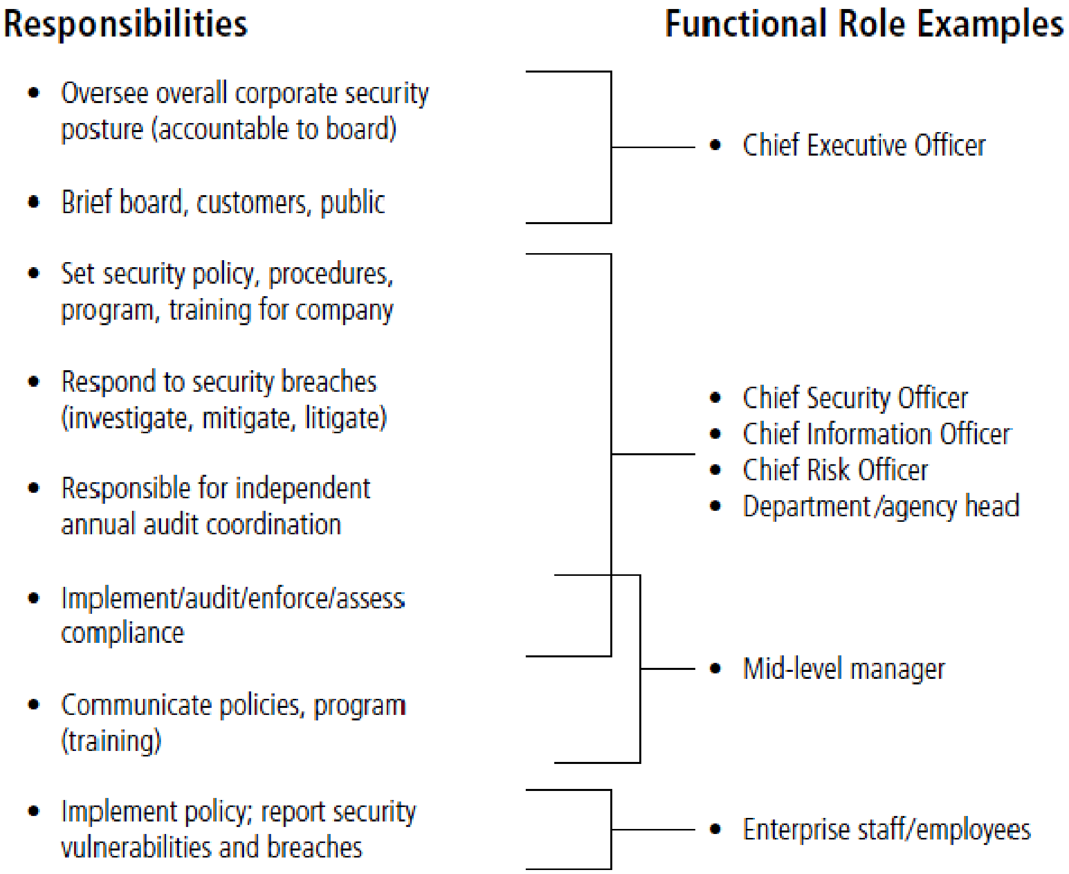
a. **Corporate Governance**: Executive management's responsibility to provide strategic direction, ensure the accomplishment of objectives, oversee that risks are appropriately managed, and validate responsible resource use.

b. **Governance:** "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly.”

c. **Information security governance:** The application of the principles of corporate governance to the information security function.

According to the Information Technology Governance Institute (ITGI), information security governance includes all of the accountabilities and methods undertaken by the board of directors and executive management to provide:

- Strategic direction
- Establishment of objectives
- Measurement of progress toward those objectives
- Verification that risk management practices are appropriate
- Validation that the organization’s assets are used properly


Responsibilities
Functional Role Examples
Oversee overall corporate security posture (accountable to board)
Brief board, customers, public
Chief Executive Officer
Set security policy, procedures, program, training for company
Respond to security breaches (investigate, mitigate, litigate)
Responsible for independent annual audit coordination
Chief Security Officer
Chief Information Officer
Chief Risk Officer
Department /agency head
Implement/audit/enforce/assess compliance
Communicate policies, program (training)
Mid-level manager
Implement policy; report security vulnerabilities and breaches
Enterprise staff/employees

Information Security Governance roles and responsibilities

Information Security Policy, Standards, and Practices

- Management from all communities of interest, including general staff, information technology, and information security, must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and how technologies should be used.
- Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation.
- In addition, policy should never contradict law;
- Policy must be able to stand up in court, if challenged; and policy must be properly administered through documented acceptance. Otherwise, an organization leaves itself..

Policy as the Foundation for Planning

a. **de facto standard :** A standard that has been widely adopted or accepted by a public group rather than a formal standards organization. Contrast with a de jure standard.

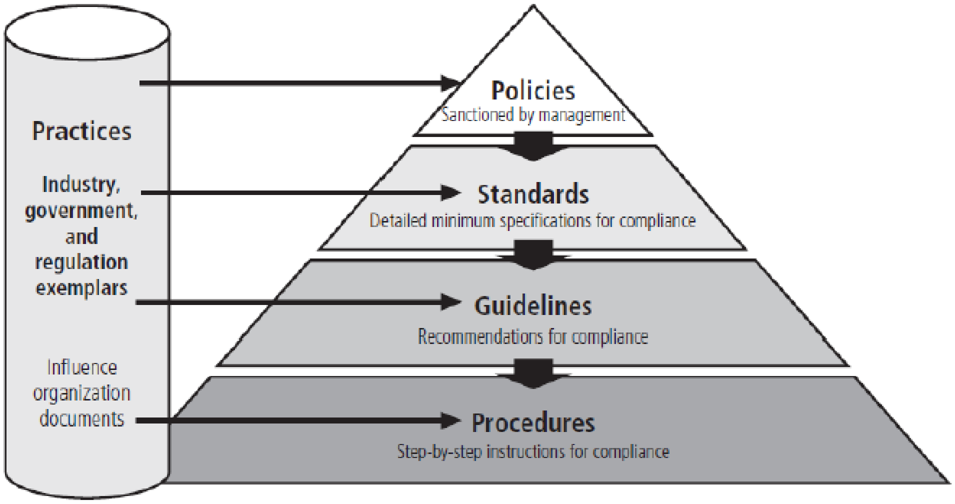
b. **de jure standard** : A standard that has been formally evaluated, approved, and ratified by a formal standards organization. Contrast with a de facto standard.

c. **Guidelines**: Within the context of information security, a set of recommended actions to assist an organizational stakeholder in complying with policy.

d. **Information security policy:** A set of rules that protects an organization's information assets.

e. **Policy**: A set of principles or courses of action from an organization's senior management intended to guide decisions, actions, and duties of constituents.

f. **Practices**: Within the context of information security, exemplary actions that an organization identifies as ideal and seeks to emulate. These actions are typically employed by other organizations.


Practices
Industry, government, and regulation exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance

Policy, Standards, guidelines and Procedures

Enterprise Information Security Policy

- Enterprise information security policy (EISP) is high-level security policy that is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts.
- An enterprise information security policy (EISP) is also known as a general security policy, organizational security policy, IT security policy, or information security policy.
- The EISP is an executive-level document, usually drafted by or in cooperation with the organization's chief information officer.
- This policy is usually 2 to 10 pages long and shapes the philosophy of security in the IT environment.
- The EISP usually needs to be modified only when there is a change in the strategic direction of the organization.

Issue-Specific Security Policy

- Issue-specific security policy (ISSP) is Commonly referred to as a fair and responsible use policy;
- A policy designed to control constituents' use of a particular resource, asset, or activity, and provided to support the organization's goals and objectives.
- As an organization supports routine operations by executing various technologies and processes, it must instruct employees on their proper use.

- In general, the issue-specific security Statement of Purpose Answers the question “What is this policy for?” Provides a framework that helps the reader understand the intent of the document. “This document will:
- Identify the elements of a good security policy
- Explain the need for information security
- Specify the various categories of information security
- Identify the information security responsibilities and roles
- Identify appropriate levels of security through standards and guidelines

The Information Security Blueprint

a. **Information security blueprint:** The basis for all security program elements; a scalable, upgradeable, comprehensive plan to meet the organization’s current and future information security needs.
b. **Information security framework**: An outline or structure of the organization’s overall information security strategy that is used as a road map for planned changes to its information security environment; often developed as an adaptation or adoption of a popular methodology,like NIST’s security approach or the ISO 27000 series.
c. **Information security model**: An established information security framework, often popular among other organizations and backed by a recognized security agency, with exemplar details an organization may want to emulate in creating its own framework and blueprint.
d. Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program.

- If any policies, standards, or practices have not been completed, management must determine whether to proceed nonetheless with the development of the blueprint.
- After the information security team has inventoried the organization’s information assets and then assessed and prioritized threats to those assets, it must conduct a series of risk assessments.
- These assessments, which include determining each asset’s current protection level.

- This information security blueprint is the basis for the design, selection, and implementation of all security program elements.
- The security blueprint builds on top of the organization’s information security policies.
- It is a detailed version of the information security framework.
- The blueprint specifies tasks and the order in which they are to be accomplished, just as an architect’s blueprint serves as the design template for the construction of a building.

The ISO 27000 Series

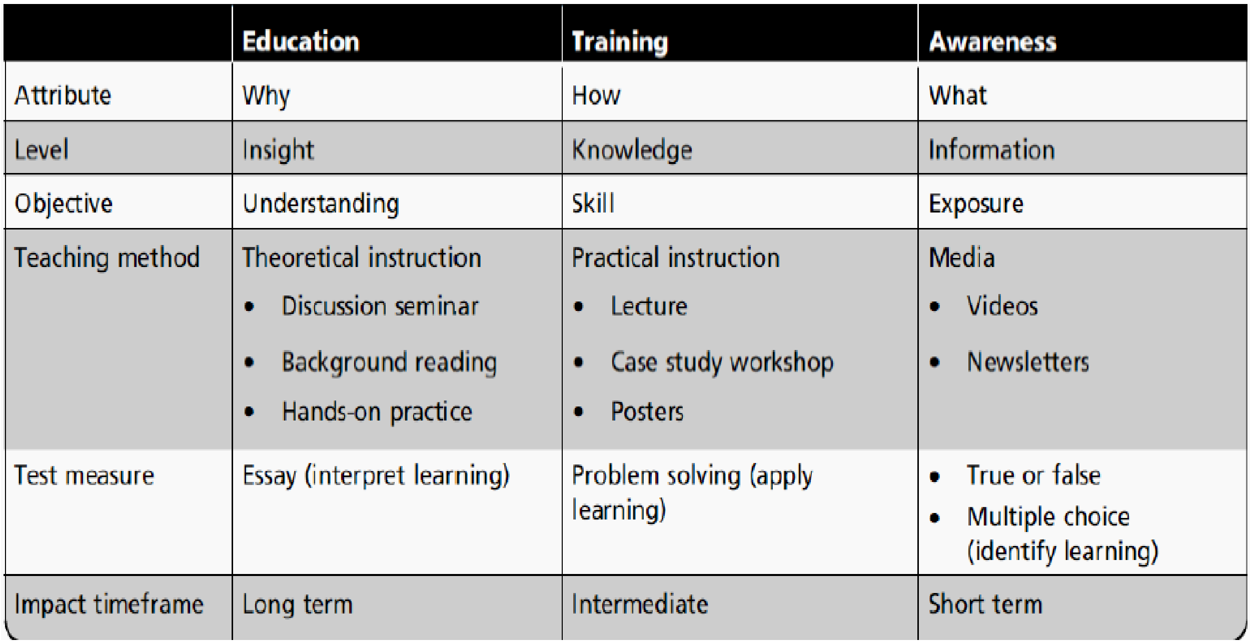
- One of the most widely referenced security models is the Information Technology—Code of Practice for Information Security Management, which was originally published as British Standard BS7799.
- In 2000, this code of practice was adopted as ISO/IEC 17799, an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- The document was revised in 2005 to become ISO 17799:2005

Security Education, Training, and Awareness Program

- Security Education, Training, and Awareness (SETA) is a managerial program designed to improve the security of information by providing targeted knowledge, skills, and guidance for organizations.
- Once your organization has defined the policies that will guide its security program by implementing a security education, training, and awareness (SETA) program.
- The SETA program is designed to reduce incidents of accidental security breaches by employees.
- Employee errors are among the top threats to information assets, so it is well worth developing programs to combat this threat.
- SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff about information security.
- For example, if an organization detects that many employees are opening questionable mail attachments, those employees must be retrained.

- As a matter of good practice, systems development life cycles must include user training during the implementation phase.
- The SETA program consists of three elements: security education, security training, and security awareness.
- An organization may not be able or willing to undertake all three of these elements, and it may outsource elements to local educational institutions.
- The purpose of SETA is to enhance security by doing the following:
  - Improving awareness of the need to protect system resources
  - Developing skills and knowledge so computer users can perform their jobs more securely
  - Building in-depth knowledge as needed to design, implement, or operate security programs for organizations and system.

Comparative Framework is as follows:

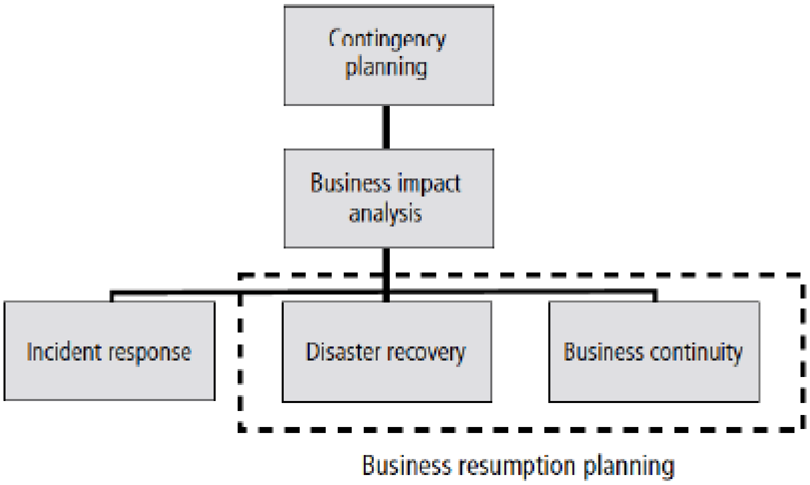


	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Continuity Strategies

- A key role for all managers is Contingency Planning (CP).
- Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems.

- For managers, the probability that some form of attack will occur—from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic—is very high.
- Thus, managers from each community of interest must be ready to act when a successful attack occurs.
- Various types of contingency plans are available to respond to events, including incident response plans, disaster recovery plans, and business continuity plans.
- In some organizations, these might be handled as a single integrated plan.
- In large, complex organizations, each of these plans may cover separate but related planning functions that differ in scope, applicability, and design.
- In a small organization, the security administrator or systems administrator may have one simple plan that consists of a straightforward set of media backup, recovery strategies, and service agreements from the company's service providers.
- Plans for incident response, disaster recovery, and business continuity are components of contingency planning, as shown in the following Diagram.



- Contingency Planning (CP) includes incident response planning (IRP), disaster recovery planning (DRP), and business continuity planning (BCP), in preparation for adverse events that become incidents or disasters.
- The primary functions of these three types of planning are as follows:
    - **The incident response plan** (IR plan) focuses on immediate response.

- **The disaster recovery plan** (DR plan) typically focuses on restoring systems at the original site after disasters occur.
- **The business continuity plan** (BC plan) occurs concurrently with the DR plan when the damage is major or ongoing, and requires more than simple restoration of information.

Unit -VI: Understanding Computer Forensics

INTRODUCTION

Cyber Forensics is simply application of computer investigation and analysis techniques in the interest of determining potential legal evidence. Forensic computing is the process of identifying preserving, analyzing and presenting the digital evidence in a manner that is legally acceptable. It is the study of evidence from attacks on computer system in order to learn what has occurred, how to prevent it from recurring and the extent of the damage.

Cyber Forensics is one of the emerging professions of 21st century. It can be thought of as an investigation of computer based evidence of criminal activity, using scientifically developed methods that attempts to discover and reconstruct event sequences from such activity.

The fascinating part of the science is that the computer operating system invariably leaves behind the computer evidences transparently without the knowledge of computer operator. The information may actually be hidden from view. Any enterprise that uses computer networks should have concern for both security and forensic capabilities (Yasinsac and Manzano, 2001). They suggest that forensic tools should be developed to scan continually computers and networks within an enterprise for illegal activities.

When misuse is detected these tools should record sequence of events and store relevant data for further investigation. Special Forensic software tools and techniques are required in order to recognize and retrieve such evidences. Cyber Forensics involves obtaining and analyzing such digital information for use in civil/criminal or administrative cases. Digital evidence was not considered as tangible evidence in courts until recently but now they are gaining importance.

Terminologies:

1. Disk Forensics: deals with extracting data/information from storage media by searching active, deleted files and also from unallocated and slack space.
2. Network Forensics: It is a sub branch of digital forensics relating to monitoring and analysis of computer network traffic for the purpose of information gathering, legal evidence or intrusion detection. Unlike other areas of digital forensics, network investigation deal with volatile and dynamic information. It is also called Pro-active forensics.
3. Wireless Forensics: It is a sub part of network forensics. The main goal of wireless forensics is to provide the tools required to collect and analyze the data from wireless network traffic. The data collected can correspond to plain data or with the broad usage of Voice over Internet Protocol (VoIP) technologies especially over wireless technology.
4. Database Forensics: is a branch of digital forensics relating to study and examine databases and their related metadata. A forensic examination of a database may relate to the timestamps that apply to the row (update time) in a relational table being inspected and tested for validity in order to verify the actions of a database user.
5. Malware Forensics: deals with analysis and identification of a malicious code, to study their payload, viruses, worms, Trojans, Keyloggers etc.
6. Mobile Phone Forensics deals with examination and analysis of mobile devices, to retrieve phone and SIM contacts, call logs(Dialled, Missed & Received), incoming and outgoing SMS/MMS, Audio, videos, paired device history and in some smart phones, geolocation and calendar information etc.
7. GPS Forensics is also called SatNav Forensics, is a relatively new discipline with the fast paced world of Mobile Device Forensics. It is used for examining and analysing GPS

devices to retrieve information such as TrackLogs, TrackPoints, WayPoints, Routes, Photos, audio etc.

8. Email Forensics: Deals with recovery and analysis of emails including deleted emails, calendars and contacts.
9. Memory Forensics deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
10. E-Discovery: E-Discovery is the process of evaluating solutions for organization. A defensible e-Discovery process is repeatable, systemized and meets legal requirements for proper handling and admissibility of computer evidence. Email archiving can be a useful complement e-Discovery. A defensible e-discovery process is repeatable, systematized and meets legal requirements for proper handling and admissibility of computer evidence. An ideal e-discovery process identifies, collects, preserves, processes, reviews and produces relevant electronically stored information. Relevant information may be found in unmanaged, unstructured, semi-structured or structured data sources dispersed across networks on desktops, laptops, servers, share drives, removable storage media and other devices. As the name implies, email archiving is limited to the contents of email system since they work only with the set of emails and do not extend to data on the network. An effective repeatable and defendable eDiscovery response plan requires an organization to proactively anticipate the type of discovery that could be initiated and develop an offensive strategy that employs both technology and human resources (Scott Carlson, 2009).

DIGITAL SPECTRUM

With the advent of new forms of criminality associated with growth of digital technologies, numbers of terms are used within the forensic community. These include cyber crime, high tech crime, e-crime, new technology crime to indicate new and digitized versions of existing crime. Some crimes can be placed on the spectrum depending upon the extent of digital environment.

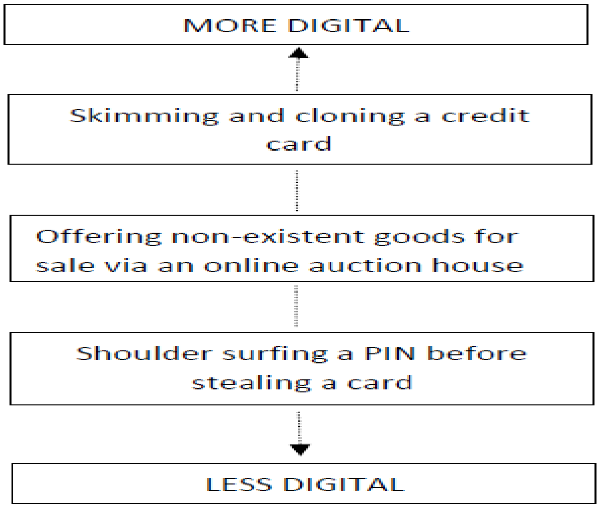

MORE DIGITAL
Skimming and cloning a credit card
Offering non-existent goods for sale via an online auction house
Shoulder surfing a PIN before stealing a card
LESS DIGITAL

Figure: The Digital Spectrum

Consider a street thief who first observes an unwary user input the PIN in an ATM and then steals the card and later withdraws cash; this is not a crime that appears to be particularly digital and it is therefore placed at the less digital end of the spectrum. On the other hand, skimming the magnetic strip, cloning a card Skimming and cloning a credit card and then using it to make transactions is clearly a crime unique to digital era and would appear to be placed at the more digital end of the spectrum.

Similarly, some crimes are more likely to have a digital aspect rather than uniquely exploit digital technologies. For example, a fraud enacted via an e-bay, a fraudster may have had planning for the fraud in the internet, setting up temporary and difficult to trace email accounts, surfing the internet for images, descriptions and prices. These are activities which exploit the advantages of digital technologies but nonetheless arise from a conventional and classic form of crime.

GOOD FIELD PRACTICE IN PROCESSING A CRIME SCENE

Crime Scene: It is crucial to understand the definition of crime scene. For practical purpose, a Crime scene is the aftermath of an event that is considered, by law, to be illegal. For basic understanding the crime scene can be considered the apex of an Inverted pyramid that expands to encompass the five phases, Investigation of crime, the recognition, analysis, interpretation of evidence, and finally, court trial. Crime scene should be processed with due diligence, utmost care and by the application of technology because any mistake made in processing the crime scene are impossible to rectify. Both errors of omission and commission made in processing a crime scene can confound the final resolution in two ways to make thing worse. The investigators use general guidelines for processing crime scene and exercise the use of check sheets, forms lists as templates for search and examination to be counterproductive. Each crime scene is unique and must be approached with knowledge, education and experience of the investigator. Crime scene is the apex of an inverted pyramid. This is illustrated in the Figure.

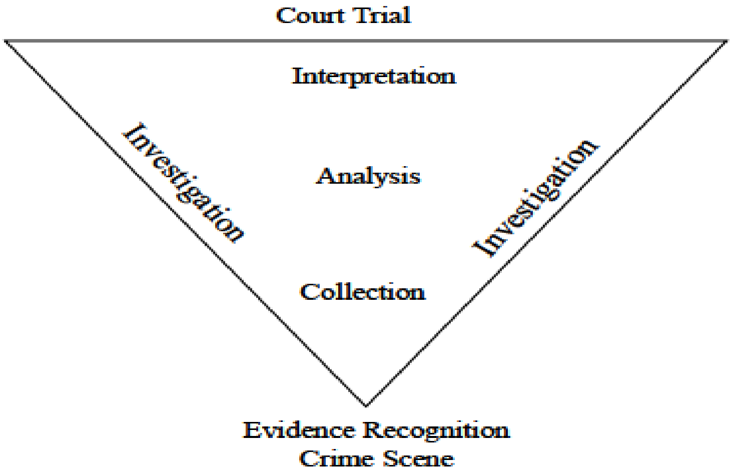


Figure: Crime Scene Pyramid

DIGITAL EVENT AND CASE RELEVANCE

Digital Event is an occurrence that changes the state of one or more objects. If the state of an object changes as a result of an event, then it is an effect of the event. Some types of objects have the ability to cause the events and these called causes (Carrier and Spafford, 2004).

The property of any piece of information, which is used to measure its ability to answer the investigative “who, what, where, when, why and how” questions in criminal investigation

(Rubin and Garrtner, 2005). The authors use this notion to describe the distinction between computer security and forensics even defining degrees of case relevance and the same is given in Figure.

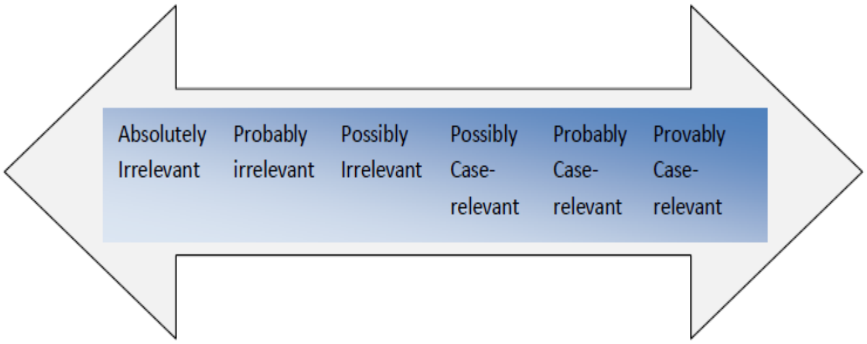


Figure.4. 3: Degrees of Case Relevance

The ultimate purpose of crime scene investigation is to seek to solve the commission of crime inevitably that fall under the umbrella of the six “W” questions:

1. What happened?
2. When did it happen?
3. Where did it happen?
4. Who was involved?
5. How was it done?
6. Why was it done?

In the examination of physical evidence the first five questions are relevant. The question “Why” is irrelevant for laboratory analysis and it is left for the establishment of motive by” “Profilers, “Criminologist” and “Courts”.

LOCARDS PRINCIPLE: TRADITIONAL FORENSICS VS. CYBER FORENSICS

Locard’s Exchange Principle is often cited in forensics publications, “Every contact leaves a trace.” Essentially Locard’s Exchange Principle is applied to crime scenes in which the perpetrator(s) of a crime comes into contact with the scene.

The perpetrator(s) will both bring something into the scene, and leave with something from the scene. In the cyber world, the perpetrator may or may not come in physical contact with the crime scene, thus, this brings a new facet to crime scene analysis.

According to the World of Forensic Science, Locard’s publications make no mention of an “exchange principle,” although he did make the observation *“Il est impossible au malfaiteur d’agir avec l’intensité que suppose l’action criminelle sans laisser des traces de son passage.”* (It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence).

CYBER EXCHANGE PRINCIPLE

“Artifacts of electronic activity in digital devices are detectable through forensic examination, although such examination might require access to computer and network resources involving

expanded scope that may involve more than one venue and geolocation." (Zatyko and Bay, 2012)

Locard's Exchange Principle does apply to cyber crimes involving computer networks, such as identity theft, electronic bank fraud, or denial of service attacks, even if the perpetrator does not physically come in contact with the crime scene. Although the perpetrator may make virtual contact with the crime scene through the use of a proxy machine, we believe he will still "leave a trace" and digital evidence will exist.

Breaking apart the principle into its parts and analyzing the application of Locard's Exchange Principle, one has to determine whether or not the following occurs:

- Are there two items?
- Is there contact?
- Is there an exchange of material?

To illustrate the application of Locard's Exchange Principle to a cyber crime, we take the example of identity theft where someone's identity is stolen and the perpetrator intends to use the stolen information for criminal gain. Let us further suppose the perpetrator steals the identity through the use of a Trojan horse and keyboard logger on the victim's computer. One could contend that during this type of cyber crime Locard's Exchange Principle does not apply. The rationale is that because a human is not at the crime scene there is no trace evidence from the human on the computer or digital media at the scene.

However, in actuality there may be lots of digital evidence such as the Trojan horse itself, changed passwords, digital logs, and so on. Thus, in this example, there is a trace at and from the scene. It may involve finding the trace evidence at other physical locations than just the one scene of the crime. The key logger could be added software or hardware or both, but in both cases it remains behind for an investigator to discover. This examination typically involves bits and bytes of information.

GOALS OF CYBER FORENSICS

In pursuit of finding the truth, the goal of digital forensics moves from specific to abstract. This can be from acquiring the evidence from the storage media in the form of data or information. This information could be represented inside the media as an encoding (i.e) ASCII or binary. The encoded data in the form of information may be involving incidents that transpired in an organization and event reconstruction needs to be made on timeline basis. The correlation or the relationship between events must be established specific to the context for e.g.: an unauthorized exploit. After acquiring the data must be relevant or coincidental to the questioned occurrence. This incident may involve the motivation or the malicious intent of the attacker. The intent may be *information component* or *human component.* It requires the skill, knowledge and ability of the investigator in the process of unraveling the truth. Incident and response time have inverse relationship. Severity and number of attacks/penetrations are high when compared to earlier years as against the time to respond is very low. A graphical representation of the goal from specific to abstract is represented in the Figure.

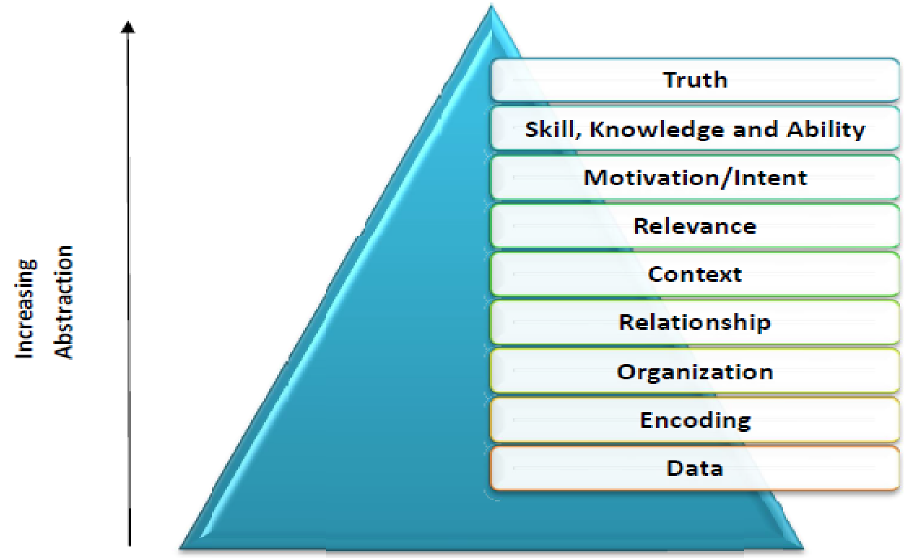


Figure: Goals of Cyber Forensics

EVOLUTION OF CYBER FORENSICS

The field of computer forensics began in the 1980s, shortly after personal computers became a viable option for consumers. In 1984, an FBI program was created. Known for a time as the Magnetic Media Program, it is now known as the Computer Analysis and Response Team (CART). Shortly thereafter, the man who is credited with being "the father of computer forensics" began work in this field. His name was Michael Anderson, and he was a special agent with the criminal investigation division. Anderson worked for the American government until the mid 1990s, after which he founded New Technologies, Inc., a leading computer forensics firm.

EMERGENCE OF CYBER FORENSIC INVESTIGATING AGENCIES

A meeting held in 1988 in Oregon led to the formation of the International Association of Computer Investigative Specialists (IACIS). Shortly after that, the first classes were held to train SCERS (Seized Computer Evidence Recovery Specialists).

Computer Forensic Timeline is illustrated in Figure and it represents the evolution of digital forensics domain as such.

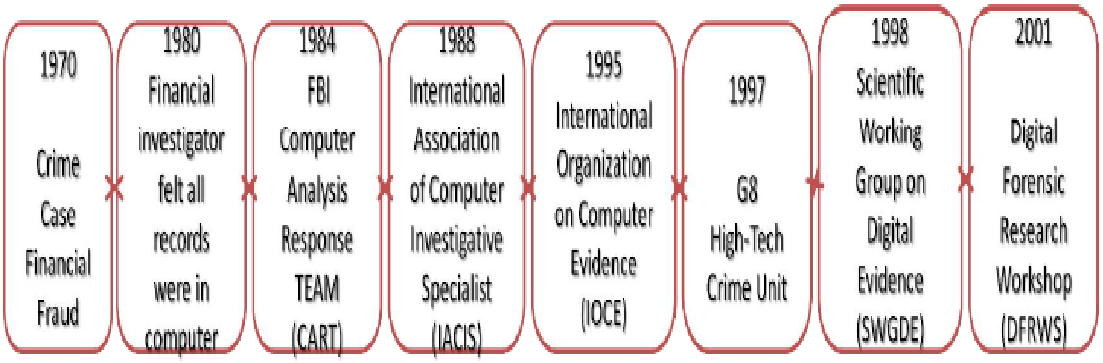

1970 Crime Case Financial Fraud
1980 Financial investigator felt all records were in computer
1984 FBI Computer Analysis Response TEAM (CART)
1988 International Association of Computer Investigative Specialist (IACIS)
1995 International Organization on Computer Evidence (IOCE)
1997 G8 High-Tech Crime Unit
1998 Scientific Working Group on Digital Evidence (SWGDE)
2001 Digital Forensic Research Workshop (DFRWS)

Figure: Computer Forensics Timeline

Different Phases of Cyber Forensics are:

1. Ad-hoc phase which was characterized by lack of structure, lack of clear goals, lack of adequate tools, processes and procedures. Further huge legal issues on how to proceed with digital evidence were seen.
2. Structured Phase is complex solution for computer forensic from accepted procedures, special tools developed and what is more important enabling criminal legislation to wide use of digital evidences.
3. Enterprise phase –Three areas of this phase are real-time collection of evidence, developing field collection tools and forensic becoming a service in companies.

- **International Organization on Computer Evidence:** The discipline continued to grow in the 1990s, with the first conference on collecting evidence from computers held in 1993. Two years later, the International Organization on Computer Evidence (IOCE) was established.
- **Digital Forensic Research Workshop (DFRWS):** DFRWS is a non-profit, volunteer organization dedicated to the sharing of knowledge and ideas about digital forensics research. DFRWS organizes an annual conference and sponsors technical working groups and annual challenges to help drive the direction of research and development.
- **Scientific Working Group on Digital Evidence (SWDGE):** The federal Crime Laboratory Directors group formed SWGDE in 1998. It was noted that the traditional audio and video examination processing was becoming digital and along with digital still photography, was converging with computer forensics. As a result, they formed a group to explore digital evidence as a forensic discipline. This group comprised of members of prominent organizations such as American Association of Forensic Science , Internation Association of Computer Investigative Specialist, High Technology Crime Investigation Association and International Organization on Computer Evidence. SWGDE is focused on the practice of digital evidence forensics primarily in the laboratory setting.
- **Association of Chief Police Officers (ACPO):** Association of Chief Police Officers functioning from Northern Ireland have designed and published a guide with procedures to be followed while collecting computer based evidence to ensure good field practice.

DEVELOPMENT OF CYBER FORENSICS

Computer forensics is the study of extracting, analyzing and documenting evidence from a computer system or network. It is often used by law enforcement officials to seek out evidence for a criminal trial. Government officials and business professionals may also have need of a specialist familiar with computer forensic techniques. The discipline of computers forensics is relatively new, having been founded in the 1980s. This digital evidence consists of data from storage media like hard disk, floppy disks, zip disks, Compact discs, DVDs, emails, data transmitted over communication links (wired and wireless), log files generated by the operating system, logs from perimeter devices like router and switch, PDA, Mobile Phones, MP3 players, USB devices, and even plethora of devices which do not fit into the original concept of computers like the washing machines, engine management system in cars, GPS devices.

In order for evaluation and acceptance of Digital evidence – a new type of evidence, previously not considered by courts, certain basic principles are suggested by research scholars and these are given below:

- Authenticity – the evidence should be authentic that is “it should specifically linked to the circumstances and persons alleged – and produced by someone who can answer questions about such links”
- Accuracy – the evidence should be free from any reasonable doubt about the quality of procedures used to collect the material, analyze the material if that is appropriate and necessary and finally to introduce it into court and produced by someone who can explain what has been done. In the case of exhibits which themselves contain statements – a letter of other document, for example – ‘accuracy’ must also encompass accuracy of content and that normally requires the document’s originator to make a witness statement and be available for cross examination”
- Accuracy – when presented evidence contains statements created in a computer “accuracy must encompass the accuracy of the process which produced the statement as well as the accuracy of the contents
- Completeness - “ tells within Its own terms a complete story of a particular set of circumstances or events”

In addition to these considerations, forensic evidence must exhibit the following properties:

- Chain of custody, transparency and explainable are the other basic principles the needs to be followed among the other principles.

Unlike the physical evidence, the digital evidence, by itself has no informational value. It requires skill and talent in interpreting the latent information which is dependent on the process by which it is unraveled and the process in turn depends on the basic principles of computer science. In order to be legally acceptable in the court of law, it requires a motivated skilled expert who will apply appropriate tools to achieve, efficiency and reliability. Cyber Forensics focuses on three kinds of data namely active data, latent data and archival data.

- **Active Data:** An active data is one that is currently available, visible and that which can be understood using an application within a computer. Active data might also be protected using passwords or some means of encryption. Some of the active data are: word processor files, spread sheets, files and directories, email content, database programs, system files, history files, temporary internet files, cookies, recycle bin and the like.
- **Latent Data:** Latent data also called as ambient data, volatile data may be in the form of deleted files, memory dumps and similar data which reside in swap files, temporary files, printer spool files, metadata, shadow file and so on. It requires an expert talent to bring to light the latent data using specialized tools and techniques.
- **Archival data:** Data that has been stored or backed up to external storage media such as tapes, CDs, DVDs, external hard disks, pen drive, zip disks, network servers or the internet is archival data. Necessary precautions have to be taken while performing forensic examination since the backup peripheral devices do not have all the information. Hence, it is always better to perform forensic examination on original source media because backups do not store latent data.

CARDINAL RULES IN CYBER FORENSICS

The cardinal rules of computer forensics can be expressed as the five ‘A’s

1. Admissibility must guide actions: document everything that is done;

2. Acquire the evidence without altering or damaging the original;
3. Authenticate your copy to be certain it is identical to the source data
4. Analyse the data while retaining its integrity and
5. Anticipate the unexpected.
6. The cardinal rules are designed to facilitate a forensically sound examination of computer media and enable a forensic examiner to testify in court as to their handling of a particular piece of evidence. A forensically sound examination is conducted under controlled conditions, such that it is fully documented, replicable, and verifiable. A forensically sound methodology changes no data on the original evidence, preserving it in pristine condition. The results must be replicable such that any qualified expert who completes and examination of the media employing the same tools and methods employed will secure the same results.

CYBER FORENSIC LAB

The role of cyber forensics will be increasing importance to the legal system as information continues to evolve into purely a digital form and the systems on which such digital information is stored becomes more technologically advanced. Strategic planning for setting a laboratory involves in developing a forensic practice: Operational Perspective, Technological perspective/venue, Scientific Perspectives an artistic perspective. Other areas of significance are Core Mission and Services, Budget and Standard operating procedures.

Cyber Forensics Lab requires adequate infrastructure for examination and analysis of Digital Evidence. Adequate Infrastructure not only includes technical infrastructure but also assets such as workspace, dedicated communication lines, 24/7 internet connection among others which should be made available to the cyber forensic experts.

- **Operational Perspective:** All business venue must have sound business management, financial profitability, core service etc. a police cyber forensics lab may not have profit perse, but the lab has to demonstrate value of service and return of Investment in order to acquire annual budget allocations and training in new technologies to continue fighting crime.
- **Technological Perspective:** Technological advancement calls for sophisticated knowledge in data and data storage technologies. More complex techniques are used by criminals to hide their criminal activity. The commercial market is rolling out a new wave of newest and shiniest technologies available to upkeep the demand for progress; again forensics community is at the front of the line, dismantling and investigating every new gadget that hits the shelves in order to reveal its secrets.
- **Scientific Perspective:** In order reveal facts objectively through empirical observation, deductive reasoning and conversion of hypothesis to demonstrable proof of the fact, examiners have to perform their duties according to reliable, repeatable, valid, objective, consistent and accurate methodologies, thereby enabling the presentation of the findings as acceptable in court of law.
- **An Artistic Perspective:** A great degree of technological prowess or expertise and competency is required in fact finding. Although the investigative process involves a rigid set of procedures, intuitive and creative skills of the forensic examiner is also required. Raw technological skill does not empower an examiner to understand the man and the machine. More artistry and creativity is required to enable a better understanding of how the tools of technology and human nature and thought process interact.

- **Budget:** Every forensic facility be it business organization or government, require funds to function. It has to spend on building, staff, and stock. It has to operate, maintain and grow a facility. Every operation needs to demonstrate return of investment in order to prove viability of the venture.
- **Core Missions and Services:** Primary consideration of forensics facility is the design plan and what services are to be rendered and the scope at which it is to be provided. A firm grasps of a prospective lab core mission and range of service will provide guidance on every aspect of building, functional forensic facility, touching on everything from annual budget to furniture ergonomics. The technical aspects would include the requisite hardware and software tools for examination and analysis. The cyber lab should possess robust operating system software like Microsoft Windows, MAC OS, Linux, SOLARIS etc. It must also have powerful computer workstation with standard peripherals. Another vital requisite would be Uninterruptible Power management software is also required for extensive control and monitoring capabilities. In general, the infrastructure is layered and the same is illustrated in Figure.

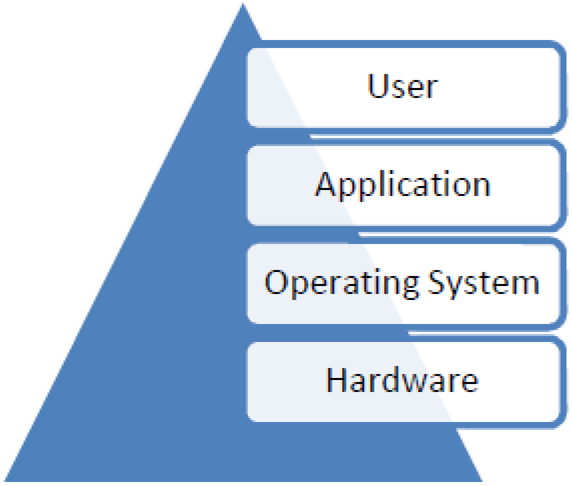


Figure: Layered Infrastructure

CYBER FORENSIC TOOLS

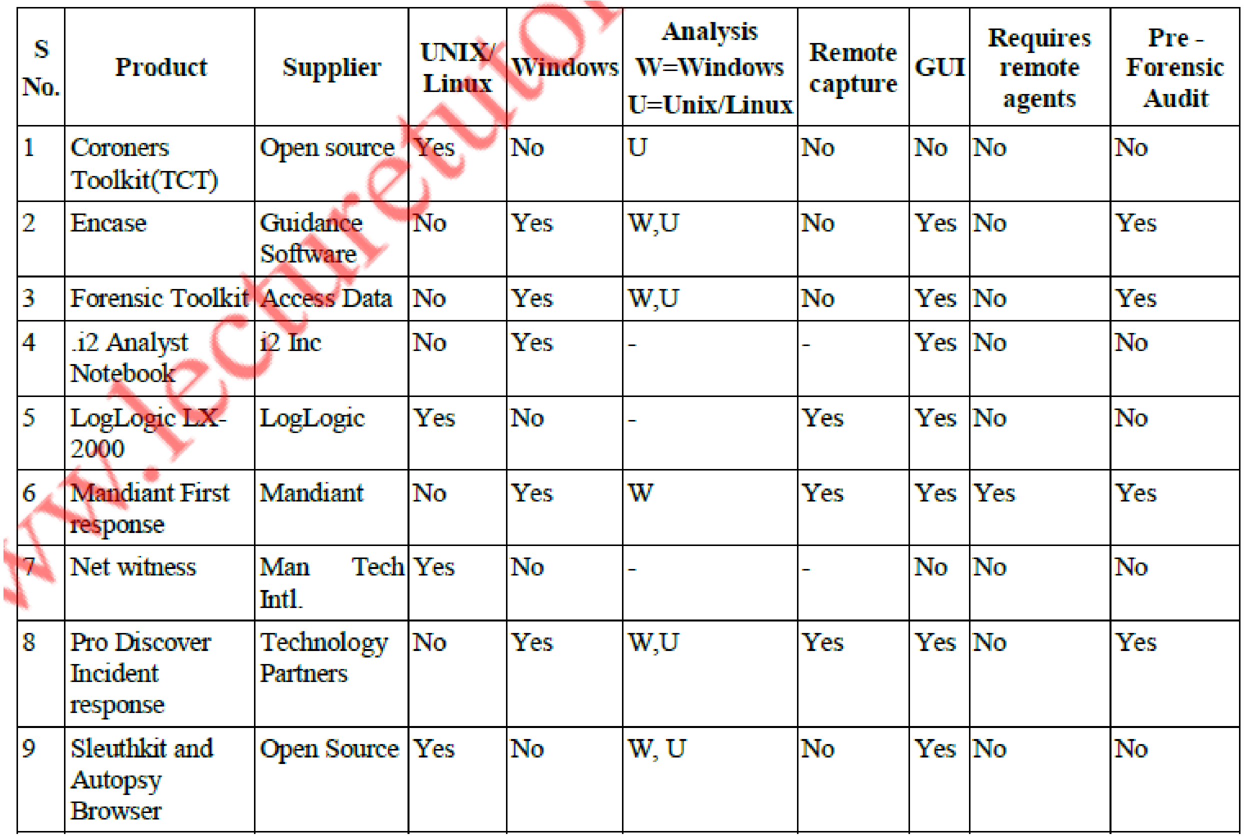
Software packages and hardware devices that qualify as forensic fraternity an there is utilizing cyber forensics tools are hoards of them. The main responsibility lies in the hands of the cyber forensic examiner to have a thorough understanding of this software, hardware and other utilities. Quite often, a combination of tools has to be employed in order to obtain a complete picture. Two-way approach in utilizing the tools exists.

One way is Proactive Forensics and the other is Post Incident Forensics. In another sense, in the current scenario, with increased volume of storage devices and multiple terabytes of data running across in the network or on such devices invites the live examination that is proactive forensics which relates to electronic discovery.

The other way is examining the storage devices after the incident has happened to find out what has actually happened in storage medium like hard disk, memory card, etc,. In proactive forensics, live examination is required without disrupting the business, whereas in post incident forensics, the standalone system and other storage media are examined offline. Choice of the tools should take into consideration the performance, reliability and repeatability and also the caveats. Having considered all these factors, examination should be performed utilizing these tools in a forensically sound manner following the best practices so as to enable admissibility of the evidence in the court of law.

A survey of forensic tools has been compiled by Dr. Peter Stephenson, in July 2006 has been published in the SC Magazine (Marcella and Menendez, 2008). A summary of the findings as to the "best of breed" of forensic tool has been listed in the Table. According to the survey the computer forensic tools sets are categorized as good, the better and best.

Table: Specification for Forensics Tools
(Source: Marcella and Menendez, 2008)



S No.	Product	Supplier	UNIX/ Linux	Windows	Analysis W=Windows U=Unix/Linux	Remote capture	GUI	Requires remote agents	Pre - Forensic Audit
1	Coroners Toolkit(TCT)	Open source	Yes	No	U	No	No	No	No
2	Encase	Guidance Software	No	Yes	W,U	No	Yes	No	Yes
3	Forensic Toolkit	Access Data	No	Yes	W,U	No	Yes	No	Yes
4	.i2 Analyst Notebook	i2 Inc	No	Yes	-	-	Yes	No	No
5	LogLogic LX-2000	LogLogic	Yes	No	-	Yes	Yes	No	No
6	Mandiant First response	Mandiant	No	Yes	W	Yes	Yes	Yes	Yes
7	Net witness	Man Tech Intl.	Yes	No	-	-	No	No	No
8	Pro Discover Incident response	Technology Partners	No	Yes	W,U	Yes	Yes	No	Yes
9	Sleuthkit and Autopsy Browser	Open Source	Yes	No	W, U	No	Yes	No	No

- **Forensic Hardware:** Forensic hardware includes workstation, write blockers, and forensic devices.
- **Forensic Workstations:** Forensic Recovery of Evidence Device **(FRED, Digital Intelligence)** family of workstations consists of integrated forensic processing platforms capable of handling the most challenging computer case. FRED is available in Mobile, Stationary and laboratory configurations. These systems are designed for both the acquisition and examination of Digital evidence. FRED professional forensic systems and the Digital Intelligence Ultrabay universal write protected imaging bay, deliver the ability to easily duplicate evidence directly from IDE/SCSI/SATA hard drives, USB Devices, Firewire devices, floppies, CDs, DVDs, ZIP cartridges, DLT-V4 tapes and PC Card/smart card/SD – MMC/Memory stick/Compact Flash Media in a forensically sound environment. Various categories of FRED workstations are:

a. FRED – Forensic Recovery of Evidence Device an ideal tool for laboratory for imaging and processing
b. FREDDIE – a highly portable solution which meets both imaging and processing requirements FRED interrogation Equipment.
c. FRED- L – The Laptop of FRED family of tools
d. µRED- microFRED the smallest, full powered Forensic Workstation
e. FRED Systems: is the complete forensic hardware and hardware solution. The 19" LCD monitor is included. The available OSs on this system is MS 6.22, Wins 98, Wins XP Pro, and Linux 9.1 Pro. Some software such as Norton GHOST 10.0 & 2003, Nero DVD/CD Authoring Software, DriveSpy, Image, PDWipe, PDBlock, and PART are included.

- **Forensic Network:** Forensic Network is a series of processing and imaging computers connected and integrated directly with a high speed, high capacity server to share resources. The file server operates as the core of the Forensic Network and can be used as a central storage facility for Forensic Images as well as the applications software for use by the client processing and imaging stations.
- **Forensic Write Blockers:** ATA and SCSI hardware write blockers, as well as other custom solutions, to effectively address specific write blocking requirements. Learn how our UltraKit, FireFly, FireBlock, SCSIBlock and FireChief devices can maintain the integrity of evidence.
- **Forensic Devices:**
  1. Fannie - forensic area network numerous imaging enclosure
  2. Rack-a-Tacc password decryption
  3. Tacc1441 Hardware Accelerator
  4. Modular Accessories
  5. Forensic Duplicator
  6. Hardcopy 3 & Hardcopy 2
  7. Shadow 2
- **Forensic Software Tools:** The forensic software tools frequently used for cyber forensics include imaging tools, examination and analysis tools, visualization tools and the like.
- **Digital Intelligence Software:** Digital Intelligence has created several forensic software tools in-house specifically for Forensic use. These tools include DriveSpy, Image, Part, PDBlock and PDWipe.
- **Accessdata:** The forensic tools available are Ultimate Toolkit, Forensic Toolkit, and specialized password recovery based on applied cryptography – Password Recovery Toolkit and Registry Viewer.
- **Guidance Software:** EnCase Forensic Edition, by Guidance Software, is the worlds leading solution for computer investigations and forensics. It is the oldest of GUI Basted IT Forensic Tools, and it includes other useful features including the ability to preview and acquire disks through many types of connections.
- **The Sleuth Kit and Autopsy Browser** powerful forensic tools to work in UNIX or Linux Environments.
- **The Coroner's Toolkit (TCT)** is an open source set of forensic tools for performing post mortem analysis on UNIX system.

- **Mandiant First Response** as a first response tool for gathering snapshot of the network with very limiter intrusiveness prior to a detailed forensic examination.
- **ProDiscover** is a complete IT forensic tool that can access over the network to enable media analysis and network behaviour analysis.
- **i2 Analyst Notebook:** This a very different type of analysis tools from those information security professionals are used to perform Link Analysis, a crucial aspect of incident response is usually done manually or by trying to use log correlators. This is a true link analyser in analysing complex crimes an security incidents. Link analysis is applied to incident response and it is used as a visualization software to link inter relationship between displayed.
- **Nuix Email Investigation** Software is a powerful email investigation software tool that performs link analysis, email information visualization, hierarchical relationship between chain of emails.
- **Paraben Forensic Tools** is a Forensic Software for PDA, Mobile Phone, text searching, data acquisition and email examination.
- **Netwitness** is a network traffic security analyzer (security intelligence) is used as a forensic incident response tool to gather information from connected computers.
- **Forensic Network** is a series of processing and imaging computers connected and integrated directly with a high capacity server to share resources. The file server operates as the core of the Forensic Network and can be used as a central storage facility for Forensic Images as well as applications software for use by the client processing and imaging stations. Workstation clients on the network perform the actual imaging and processing tasks, while the central file server stores the images and case work.
- **CyberCheck Suite** is a suite of forensic software tools to perform data analysis which has a capability of analysing storage media such as hard disks, and optical media images and analyses images for evidences developed by C-DAC Thiruvanathapuram.
- **Hot Pepper Technology:** Authors of EMAIL Detective, a dedicated software solution for recovering and reconstructing AOL email. EMD is the most comprehensive AOL extraction tool available to forensic agencies
- **Stepanet DataLifter:** Suite of products based on investigative experience. These tools have been specifically designed to assist with Computer Forensics, Information Auditing, Information Security and Data Recovery.

DIGITAL FORENSIC LIFE CYCLE

The major issues of cyber forensics involves Identification of potential digital evidence and determine as to where might the evidence be. Which devices were used by suspects? reservation of evidence on the electronic crime scene, prevent loss and contamination and ensure proper documentation and further extract the evidence and present in a legally acceptable manner, taking due care to privacy related issues. The next step is to ensure integrity of evidence. The aim is to try to make an identical copy of the evidence so that it can be analyzed without destroying the original evidence. As a thumb rule, according to various standards, one should never work on the original disk or the storage medium, always make multiple copies and work only on the copies, ensure chain of custody. Different methods of forensic copying are available.

A special device called a write blocker is commonly used. Both Software based write blockers and hardware based write blockers are available. The hardware based write blocker is a small device or a bridge that is connecting the suspect hard disk and the computer system through the hard disk interface. The write blocker functions by analyzing the commands sent from the Hard Disk controller on the motherboard to the hard drive and it filters all the commands that instruct the drive to change its content. That is, it allows the system to “read only” mode. Generally Hardware write blockers are preferred over software based write blockers. Integrity of the evidence can be verified with message digest (MD5) or Secure Hashing Algorithm (SHA) hash algorithm and may be a Global Position System may be used to provide for more reliability indicating the location of imaging process.

The digital forensic life cycle is represented in the Figure.

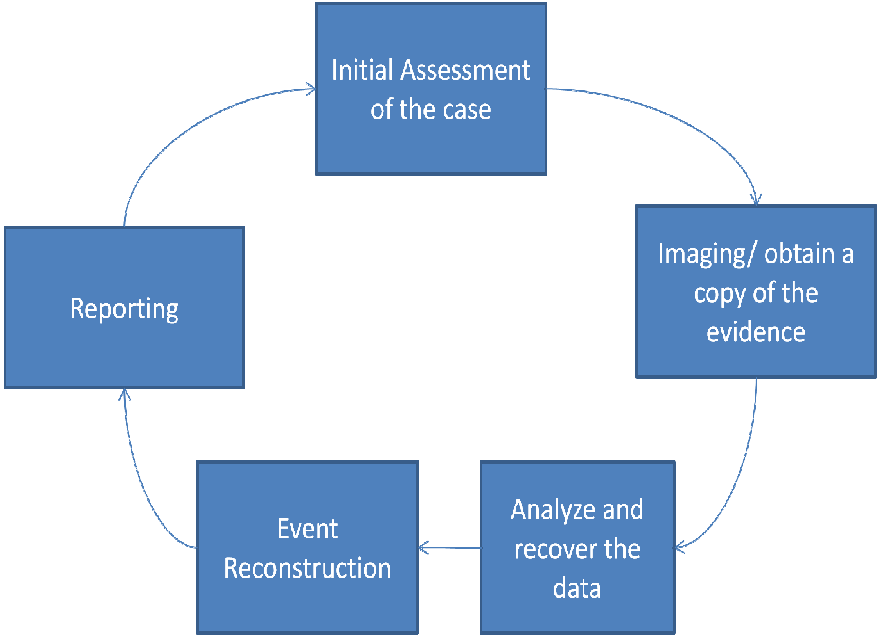

Initial Assessment of the case
Imaging/ obtain a copy of the evidence
Analyze and recover the data
Event Reconstruction
Reporting

Figure: Digital Forensics Life Cycle

DIGITAL FORENSIC EXAMINATION

Digital Forensic examination may be sought for either public or private investigation. What is possible is recovery of deleted data, discovery of when the files were created, modified or deleted, installed and uninstalled application, web browsing habit s of the user etc. What is not possible is recovery of digital media that is physically damaged or destroyed or securely overwritten.

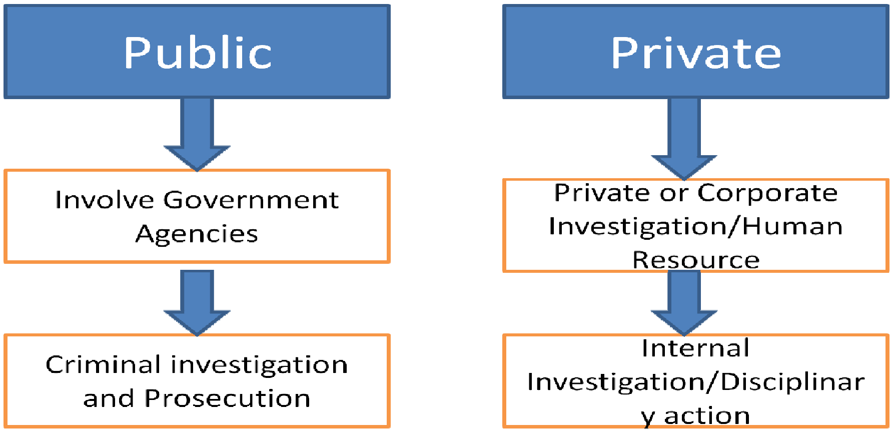

Public
Involve Government Agencies
Criminal investigation and Prosecution
Private
Private or Corporate Investigation/Human Resource
Internal Investigation/Disciplinary action

Figure: Public and Private Investigation

LATENT DEMAND FOR COMPUTER FORENSIC SERVICES IN INDIA

A survey had been done for the “Latent Demand for Computer Forensic Services in India” (Parker P, INSEAD, 2009) Based on the methodology described above, the latent demand for computer forensic services in India is estimated to be $278.1 million in 2009. The distribution of the latent demand (or potential industry earnings) in India, however, is not evenly distributed across regions. Maharashtra is the largest market with $37.8 million or 13.60 percent, followed by Uttar Pradesh with $32.3 million or 11.60 percent, and then Gujarat with $22.9 million or 8.22 percent of the latent demand in India. In essence, if firms target these top 3 regions, they cover some 33.42 percent of the latent demand for computer forensic services in India.

- **The Latent Demand in India Territory Wise** A Study conducted on the latent demand for computer forensic services in India recently (**Philip M. Parker, 2009)** has predicted that the requirement for computer forensic services in India and presents state wise percentage for industry earnings amounting in USD. Table.4.2 represents the latent demand state wise for the year 2009 and in Table.4.3 shows the year wise latent demand and Table 4.3 represents the latent demand for industry earnings in Tamilnadu.

Table.4.2: Latent Demand for Computer Forensic Services in India (2009)
(Source: Philip M. Parker, INSEAD, © 2008, www.icongrouponline.com)

S No	State	USD in millions	Percentage in India
1	Maharashtra	37.816	13.6%
2	Uttar Pradesh	32.260	11.6%
3	Tamil Nadu	26.058	9.4%
4	Gujarat	22.861	8.2%
5	West Bengal	21.716	7.8%
6	Andhra Pradesh	20.216	7.3%
7	Madhya Pradesh	15.935	5.7%
8	Karnataka	14.286	5.1%
9	Rajasthan	12.894	4.6%
10	Delhi	9.804	3.5%
11	Kerala	9.123	3.3%
12	Haryana	8.639	3.1%
13	Orissa	8.066	2.9%
14	Punjab	8.009	2.9%
15	Chhattisgarh	5.661	2.0%
16	Bihar	4.884	1.8%
17	Assam	4.305	1.5%
18	Jharkhand	4.192	1.5%
19	Uttaranchal	2.220	0.8%
20	Himachal Pradesh	1.988	0.7%
21	Jammu & Kashmir	1.689	0.6%
22	Goa	.969	0.3%

23	Chandigarh	.839	0.3%
24	Pondicherry	.735	0.3%
25	Nagaland	.632	0.2%
26	Tripura	.509	0.2%
27	Meghalaya	.506	0.2%
28	Manipur	.427	0.2%
29	Mizoram	.310	0.1%
30	Arunachal Pradesh	.256	0.1%
31	Andaman & Nicobar Islands	.142	0.1%
32	Sikkim	.056	0.0%
33	Daman & Diu	.042	0.0%
34	Dadra & Nagar Haveli	.036	0.0%
35	Lakshadweep	.026	0.0%
	Total	278.109	100.0%

Table.4.3: Year wise Latent Demand/requirement for Computer Forensic Services: 2004 – 2014
(Source: Philip M. Parker, INSEAD, © 2008, www.icongrouponline.com)

Year	India Market US$ Million
2004	103.152
2005	137.641
2006	173.446
2007	208.279
2008	243.141
2009	278.109
2010	313.708
2011	349.845
2012	384.546
2013	421.925
2014	463.050

The data in Table 4.4: represents the requirement in USD demand for computer forensic services in Tamilnadu.

Table.4.4: Latent Demand for Computer Forensic Services in Tamil Nadu: 2004 – 2014
(Source: Philip M. Parker, INSEAD 2008)

Year	US$ Million	Percent in India
2004	10.669	10.34
2005	13.925	10.12
2006	17.186	9.91
2007	20.222	9.71
2008	23.150	9.52

2009	26.058	9.37
2010	28.930	9.22
2011	31.741	9.07
2012	34.308	8.92
2013	37.005	8.77
2014	39.914	8.62

Figure.4.9. represents the district wise requirement in percentage. Accordingly, in Chennai it is 14% followed by Coimbatore, 12%, Trichy and Madurai 4% each.

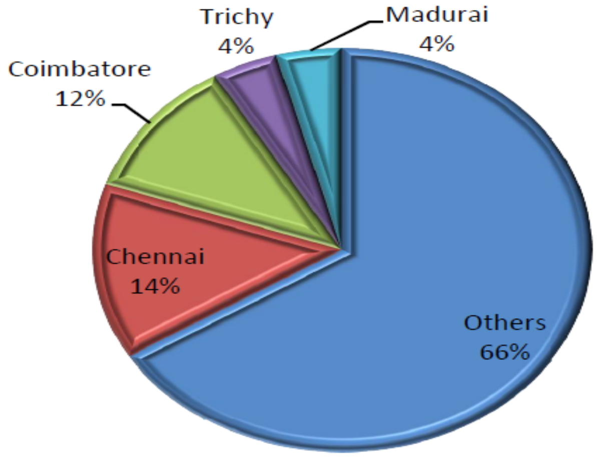


Figure.4.9: Latent Demand for computer forensic services in Tamilnadu

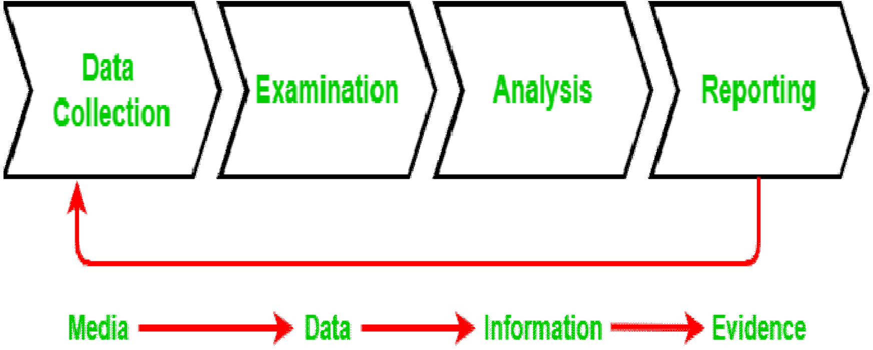
CONCLUSION

Cyber Forensics puts the wheels in motion between the cyber forensic professionals (humanware), the software and the hardware tools of cyber forensics as there is a dire need to develop new methods for analysis and assessment thereof to reflect the focus on competencies. A high quality interdisciplinary collaboration is the need of the hour. In this regard combination of the said factors is envisaged for achieving best practices in cyber forensic investigation. The cyber forensic investigation is confronted with cyber crimes which are heterogeneous in nature. In the next chapter pattern recognition techniques in order to highlight the possible relationships between occurrences of particular crime has been discussed using application of practical forensic methods.

Chain of Custody Concept

- Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases. Each step in the chain is essential as if broke, the evidence may be rendered inadmissible.
- Thus we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.
- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.

- ⦿ It demonstrates trust to the courts and to the client that the evidence has not tampered.
- ⦿ Digital evidence is acquired from the myriad of devices like a vast number of IoT devices, audio evidence, video recordings, images, and other data stored on hard drives, flash drives, and other physical media.
- ⦿ Chain of Custody Process



- ⦿ In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.
- ⦿ Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.
- ⦿ Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
- ⦿ Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.
- ⦿ Reporting: This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:
  - Statement regarding Chain of Custody.
  - Explanation of the various tools used.
  - A description of the analysis of various data sources.
  - Issues identified.
  - Vulnerabilities identified.
  - Recommendation for additional forensics measures that can be taken.
- ⦿ The Chain of Custody Form
  - In order to prove a chain of custody, you’ll need a form that lists out the details of how the evidence was handled every step of the way. The form should answer the following questions:
  - What is the evidence?: For example- digital information includes the filename, md5 hash, and Hardware information includes serial number, asset ID, hostname, photos, description.
  - How did you get it?: For example- Bagged, tagged or pulled from the desktop.
  - When it was collected?: Date, Time
  - Who has handle it?
  - Why did that person handled it?

- Where was it stored?: This includes the information about the physical location in which proof is stored or information of the storage used to store the forensic image.
- How you transported it?: For example- in a sealed static-free bag, or in a secure storage container.
- How it was tracked?
- How it was stored?: For example- in a secure storage container.
- Who has access to the evidence?: This involves developing a check-in/ check-out process.
- The CoC form must be kept up-to-date. This means every time the best evidence is handled off, the chain of custody form needs to be updated

⦿ How can the Chain of Custody be assured?

- A couple of considerations are involved when dealing with digital evidence and Chain of Custody. We shall discuss the most common and globally accepted and practiced best practices.
- Never ever work with the Original Evidence: The biggest consideration that needs to be taken care of while dealing with digital evidence is that the forensic expert has to make a full copy of the evidence for forensic analysis. This cannot be overlooked as when errors are made to working copies or comparisons need to be done, then, in that case, we need an original copy.

⦿ Document any extra scope: During the process of examination, it is important to document all such information that is beyond the scope of current legal authority and later brought to the attention of the case agent. A comprehensive report must contain following sections:

- Identity of the reporting agency.
- Case identifier.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.
- Descriptive list of items submitted for examination: This includes the serial number, make, and model.
- Identity and signature of the examiner
- Brief description of steps taken during the examination: For example- string searches, graphics image searches, and recovering erased files.
- Results.

⦿ Consider the safety of the personnel at the scene: It is very important to ensure that the crime scene is fully secure before and during the search. In some cases, the examiner may only be able to do the following while onsite:

- Identify the number and type of computers.
- Interview the system administrator and users.
- Identify and document the types and volume of media: This includes removable media also.
- Determine if a network is present.
- Document the information about the location from which the media was removed.
- Identify offsite storage areas and/or remote computing locations.

  - Identify proprietary software.
  - Determine the operating system in question.
- The Digital evidence and Digital Chain of Custody are the backbones of any action taken by digital forensic specialists. In this article, we have examined the seriousness of the digital evidence and what it entails and how slight tampering with the digital evidence can change the course of the forensic expert's investigation.

Approaching A Computer Forensics Investigation

- The digital forensic process has the following five basic stages:
  - Identification – the first stage identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
  - Preservation – the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.
  - Collection – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
- The digital forensic process has the following five basic stages:
  - Analysis – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.
  - Reporting – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.
- A crucial activity that accompanies the first four steps is contemporaneous note-taking. This is the documentation of what you have done immediately after you have done it in sufficient detail for another person to reproduce what you have done from the notes alone.
- A Computer Forensic Investigation generally investigates the data which could be taken from computer hard disks or any other storage devices with adherence to standard policies and procedures to determine if those devices have been compromised by unauthorized access or not. Computer Forensics Investigators work as a team to investigate the incident and conduct the forensic analysis by using various methodologies (e.g. Static and Dynamic) and tools (e.g. ProDiscover or Encase) to ensure the computer network system is secure in an organization.
- A successful Computer Forensic Investigator must be familiar with various laws and regulations related to computer crimes in their country (e.g. Computer Misuse Act 1990, the UK) and various computer operating systems (e.g. Windows, Linux) and network operating systems (e.g. Win NT). According to Nelson, B., et al., (2008), Public Investigations and Private or Corporate Investigations are the two distinctive categories that fall under Computer Forensics Investigations. Public investigations will be conducted by government agencies, and private investigations will be conducted by

private computer forensic team. This report will be focused on private investigations, since an incident occurred at a new start-up SME based in Luton.

- This report also includes a computer investigation model, data collections and its types, evidence acquisitions, forensics tools, malicious investigation, legal aspects of computer forensics, and finally this report also provides necessary recommendations, countermeasures and policies to ensure this SME will be placed in a secure network environment.

Computer Forensics and Steganography

- Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication.
- Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme. In summary:
- steganography_medium = hidden_message + carrier + steganography_key
- Types
    - Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
    - Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
    - Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
    - Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
    - Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal [Warchalking 2003]), underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
    - Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of

rules, such as “read every fifth word” or “look at the third character in every word.”

- Steganography Forensics
  - The art and science of steganalysis is intended to detect or estimate hidden information based on observing some data transfer and making no assumptions about the steganography algorithm
  - Steganalysis techniques can be classified in a similar way as cryptanalysis methods, largely based on how much prior information is known (Curran and Bailey 2003; Johnson and Jajodia 1998B).
  - Steganography-only attack: The steganography medium is the only item available for analysis.
  - Known-carrier attack: The carrier and steganography media are both available for analysis.
  - Known-message attack: The hidden message is known.
  - Chosen-steganography attack: The steganography medium and algorithm are both known.
  - Chosen-message attack: A known message and steganography algorithm are used to create steganography media for future analysis and comparison.
  - Known-steganography attack: The carrier and steganography medium, as well as the steganography algorithm, are known.
- Steganography Tools
  - WetStone Technologies’ Gargoyle (formerly StegoDetect) software can be used to detect the presence of steganography software.
  - AccessData’s Forensic Toolkit and Guidance Software’s EnCase can use the HashKeeper, Maresware, and National Software Reference Library (National Software Reference Library 2003) hash sets to look for a large variety of software.
  - Niels Provos’ stegdetect can find hidden information in JPEG images using such steganography schemes as F5, Invisible Secrets, JPHide, and JSteg.

Relevance of the OSI 7 Layer Model to Computer Forensics

- With the development of technology comes the high profile hacking techniques. For this reason, security professionals are in massive demand. But for this, security professionals and analysts have to understand the fundamentals of how network layers work and the key ingredients that can make the security in every layer stronger? This chapter will discuss the security mechanisms and different measures that need to be taken in each layer of the OSI model.
- Before going into security, it is necessary to know the basics of networking and its models - the OSI model. It is a hypothetical networking framework that uses specific protocols and mechanisms in every layer of it. This model is used to divide the network architecture into seven different layers conceptually. These layers are:
  - Physical layer.
  - Data link layer.
  - Network layer.
  - Transport layer.
  - Session layer.

  - Presentation layer.
  - Application layer.

- There also involves some security postures and mechanisms that a security professional must know to detect and put the security method effectively in every layer.
- The first three layers of the OSI model are called the media layers.
- The subsequent four layers are host layers.
- Physical Layer is used for defining the technical qualifications of the data connectivity. Since the security in this layer is critical, so in case of any cyber danger (DoS attack), it is recommended to unplug the cable from the primary system. Safeguarding this layer needs bio-metric security, camera-based surveillance, key cards, and other physical monitoring.
- Data Link Layer comprises of data packets transported from the physical layer. Any malfunctioning in this layer or data breach can impede the working of the network layer. Vulnerabilities that can be used and attacks that can be made in this layer are MAC address spoofing and virtual-LAN circumvention.
  So for protecting your system, common security mechanisms are MAC address filtering, assessment of wireless applications, checking of proper data encryption standards.
- Network Layer is the last of the media layer and has an association with the real world. It deals with the addressing and routing of packets. IP address spoofing is one o the common attack of this phase. Strengthening this layer needs the techniques of firm anti-spoofing, proper implementation of firewalls and routing filters, and secure routing protocols.
- Transport Layer - comes under the logical layer, which helps in transferring variable-length data sequence. The reliability of this layer can be achieved by ensuring the segmentation and de-segmentation mechanism and error control. For security purposes, this layer needs an appropriate firewall, restrictive admission of transmission protocols, and appropriate port number.
- Session Layer - essentially manages the inter-system communication and sessions. The handling of local and remote application's interaction is done in this layer. In case of weak authentication methods, it can help attackers to perform a brute force. So the effective way of securing this layer is by ensuring appropriate encrypted key exchange, along with the restriction of unsuccessful session attempts using timing methods.
- Presentation Layer - is used to standardize data with the help of various conversion schemes. But if there is poor conduct of malicious input, it can help cybercriminals exploit the system or even crash a system. Separate sanitized input and proper input validation can help protect the system from attackers.
- Application Layer - contain the UI and the closest of all layers for the user-end. The widest range of cyber attacks and security breaches is possible in this layer. It can lead to shutting down the network, stealing data, crashing the application, manipulating the information sent from source to destination, and many more.
- Where do Cybersecurity threats happen?
  - Cybersecurity threats exist at all OSI-ISO model layers beginning at Layer 7 – the Application Layer because that’s the place where users begin by interfacing to the network. For the purposes of creating the most comprehensive cybersecurity plan we must actually start BEFORE the Application Layer and address perhaps the biggest vulnerability in the entire network – the user. Users are human and far

more subject to making costly errors than are computers and other digital devices which will perform the same function the same way every time.

- ⦿ The best example is found in one of the top malware attacks or threats in the cyber landscape – ransomware. Fraudsters send out a “phishing” email that looks very authentic, very much as if it actually comes from where it says it does. But somewhere in that email is a link for the user to click or an attachment for the user to open. The text provides powerful inducements to get the user to do so. Once they do their data is either encrypted, corrupted, or stolen. The only way to get it back is to pay a ransom, thus ransomware.
- ⦿ The attackers know the user is their best place to gain access.
- ⦿ Threats at each layer of the ISO-OSI model include:
- ⦿ APPLICATION LAYER THREATS
    - Security software developer F5 tells us, “Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others.” The team at SecurityIntelligence points out that, “The application layer is the hardest to defend.
- ⦿ APPLICATION LAYER THREATS
    - The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world. For the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS).” Other possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, and trojan horses.
- ⦿ APPLICATION LAYER THREATS
    - Your cybersecurity plan must include Application Monitoring which is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source.
- ⦿ PRESENTATION LAYER THREATS
    - The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server.
    - Include in your mitigation plans options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.
- ⦿ SESSION LAYER THREAT
    - DDoS-attackers exploit a flaw in a Telnet server running on the switch, rendering Telnet services unavailable.

- In the regular maintenance portion of your plan be sure to remind operators to check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.

◉ TRANSPORT LAYER THREATS

- According to Network World, “Many businesses use Transport Layer Security (TLS) to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted. TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP.

◉ NETWORK LAYER THREATS

- Routers make decisions based on layer 3 information, so the most common network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.
- The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled. Keep logging enabled and conduct regular auditing of any unusual activity that may occur.

◉ DATA-LINK LAYER THREATS

- Cisco explains that, “The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical, as opposed to logical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure or absent virtual LANs (VLANs, or lack of VLANs). Network interface cards (NICs) that are misconfigured or malfunctioning can cause serious problems on a network segment or the entire network.”

◉ PHYSICAL LAYER THREATS

- Ask any cybersecurity professional to define where the network is and they’ll point at “the wires in the walls.” What they’re saying is that the copper and fiber-optic cables that connect everything together create the actual network that everything else uses. Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits, or other human vandalism.

◉ PHYSICAL LAYER THREATS

- Many companies mitigate these failures by bringing in multiple circuits to the internet. It should be noted that this works well until a backhoe digs up a critical corner through which all carrier circuits run, thus disabling all of the multiple paths. The aftermath of many disasters illustrates the superior strategy being the placement of all network core elements such as servers and storage at multiple redundant cloud data centers. Should a major carrier cable be cut, only users will be affected, and they can switch to wireless access or other locations until repairs are completed.

Forensics and Social Networking Sites

- Social Media needs no introduction. It has taken over the world and our lives like an insidious wave. It is a wave that has brought the world closer, yet not without detrimental effects. At present, over 3.397 billion users are active on social media who spend 116 minutes per day on an average. With abundant personal information available on social media platforms, it is now the hotbed of crimes and malicious activities.
- But, where there's a crime, there's also inspection to bring justice to victims and combat such occurrences in the future. Presenting some common social media crimes and the science of Social Media Forensics. Know how investigators extract social media forensics evidence and engage in forensic analysis of social networking applications on mobile devices.
- The Black Hole called Social Media
- Social media is any application or website that facilitates users to interact and socialize, share ideas and information, upload photos and files, participate in various activities/events, and engage in real-time conversations.
- Online communications in the form of social networking have witnessed a colossal evolution in the last couple of years. From September 2017 to October 2018, the number of social media users grew by 320 million. This spells out a one new social media user every 10 seconds! In fact, WhatsApp and Facebook Messenger handle 60 billion messages every day!
- Type of Social Networking Platforms
    - We all know what social media is. However, what most don't know is that Facebook, Instagram, Twitter, Snapchat and WhatsApp are not the only social media platforms. The classification of social media platforms is based on its primary objective of use Following are the different types of social networking platforms.
- 1. Social Networks
    - Also sometimes called "relationship networks, social networks enable people and organizations to connect online for exchanging information and ideas.
    - Use: To associate with people and brands virtually.
    - Examples: Facebook, Twitter, WhatsApp, LinkedIn
- 2. Media Sharing Networks
    - Media sharing networks enable users and brands to search and share media online. This includes photos, videos, and live videos.
    - Use: To search for and share photos, videos, live videos, and other forms of media online.
    - Examples: Instagram, Snapchat, YouTube
- 3. Discussion Forums
    - One of the oldest types of social media platforms, discussion forums are an excellent repertoire for market research. They provide a wide range of information and discussion on various subjects.

- Use: Serves as a platform to search, discuss, and exchange information, news, and opinions.
- Examples: Reddit, Quora, Digg

⦿ 4. Bookmarking and Content Curation Networks

- Such social networking platforms enable people to explore and discuss trending media and content. These platforms are the epicenter of creativity for those seeking new ideas and information.
- Use: To explore, save, exchange, and discuss new and trending content and media.
- Examples: Pinterest, Flipboard

⦿ 5. Consumer Review Networks

- Consumer review networks enable people to express their opinions/experiences about products, services, brands, places and everything else under the sun!
- Use: To search, review, and share opinions/information about brands, restaurants, products, services, travel destinations, etc.
- Examples: Yelp, Zomato, TripAdvisor

⦿ 6. Blogging and Publishing Networks

- Blogging/publishing networks serve as a platform for publishing online content in a way that facilitates discovery, commenting and sharing. Publishing platforms consist of traditional blogging platforms such as Blogger and WordPress, microblogging platforms such as Tumblr, and even interactive platforms such as Medium.
- Use: To publish, explore, and comment on content online.
- Examples: WordPress, Tumblr, Medium

⦿ 7. Sharing Economy Networks

- It is also known as ‘collaborative economy network’. These networks enable people to connect online for advertising, finding, sharing, trading, buying and selling of products and services online.
- Use: To find, advertise, share, and trade products and services online.
- Examples: Airbnb, Uber, Task rabbit

⦿ 8. Anonymous Social Networks

- As the name itself states, such social networks enable users to share content anonymously. Thus, miscreants are increasingly misusing such platforms for cyberbullying.
- Use: To anonymously spy, vent, gossip, and sometimes bully.
- Examples: Whisper, Ask.fm, After School

⦿ Social Networking Platforms Offers a Lucrative Platform for Executing Social Media Crimes

- On the righteous side, one may use social media platforms to socialize and communicate with near and dear ones. However, it is the anonymous and diverse nature of social networking platforms that miscreants use for unethical activities. Innocent-looking profiles can often be the masquerade for fraudsters, phishers, child predators, lechers, and other cyber criminals.
- In spite of the stringent policies imposed by social media platforms, there are approximately 270 million fake profiles on Facebook!!!

- Additionally, the abundance of personal information available on social networking platforms renders them a favorite of cyber criminals. After the compromise of a profile, a hacker can access, manipulate and misuse its information for various malicious activities. Other unscrupulous activities on such platforms include stalking, bullying, defamation, circulation of illegal or pornographic material etc.
- Following are some types of social media crimes.

⦿ 1. Hacking

- This happens when you are not able to log into your account because someone who has broken into your account and taken complete control over it. Facebook is the most hacked social networking site. Social media hacking usually occurs when:
- One does not log out from the account, especially when using a public computer.
- Sharing of passwords with strangers either unintentionally, or as a result of social engineering. Using easy to predict, or same passwords across multiple platforms.
- Hacking of one’s login email ID.

⦿ 2. Photo Morphing

- Photo morphing is the use of editing to change an image/shape into another without much difficulty. Available data shows that people share nearly 3.2 billion images daily on social media platforms. The widespread availability of media on social networking platforms makes it a cakewalk for miscreants to download and misuse them.
- Miscreants morph the images of popular figures and upload them on adult websites or use them for blackmailing them for sexual or financial favors.

⦿ 3. Offer & Shopping Scams

- Women are usually known to fall for such offer and shopping scams on social networking platforms.
- For example, a miscreant uses a shopping offer to make a user click on a link. Once clicked, it prompts the user to forward it to 20 people to avail the coupon. However, the user does not get any coupon, but the cybercriminal gets his/her personal information!

⦿ 4. Dating Scams

- In such scams, the fraudster connects with the victim using a fake name and picture. Once they befriend the victim, they move to a different platform for further communication. Once they realize that the victim has fallen for them, they first send small gifts like flowers and cards, and later start demanding for emergency monetary help like recharging their phone to talk, booking flight tickets to meet, medical reasons etc. At times, fraudsters may also record video calls or screen, and later use them to blackmail the victim.

⦿ 5. Cyberbullying

- Cyberbullying is an act that involves sending or publishing obscene messages or humiliating content online, or issuing threats to commit violent acts. It includes sending or sharing nasty or false information about another individual for character assassination and causing humiliation. Example: Imposters used social media platforms such as Facebook and WhatsApp for circulating the deadly Blue

Whale and Momo Challenges. These resulted in the death of many teenagers across the globe as they committed suicide as a part of the challenge.

- ⦿ 6. Link Baiting
  - In such scams, the fraudster sends the victim a link that entices the victim to open it. On opening, it leads to a fake landing page which prompts the victim to enter his/her account credentials. This provides the credentials to the cybercriminal who later uses it for illicit activities.
  - Example: The victim gets a message: “Somebody just put up these pictures of you drunk at this wild party! Check ’em out here!”
  - Immediately, the victim clicks on the enclosed link, which leads to his/her Twitter or Facebook login page. Once the victim enters his/her account details, the cybercriminal has the password and can take total control of the account.

Social Media Forensics or Social Network Forensics

- Now that you know how perpetrators can use social networking platforms to wreak havoc, are you considering an exit? Well, let us enlighten you about digital forensics then! The increase in social media crimes has also resulted in the increasing importance of digital forensics for their investigation.
- Precisely known as social media forensics or social network forensics, it focuses on retrieval of electronic evidence from social networking activities. Such evidence often plays a crucial role in the conviction or acquittal of a suspect.
- Social media forensics involves the application of cyber investigation and digital analysis techniques for:
  - Collecting information from social networking platforms such as Facebook, Twitter, LinkedIn etc.
  - Storing,
  - Analyzing, and
  - Preserving the information for fighting a case in the court of law Social Media Forensics is about locating the source of electronic evidence. This is accompanied by collecting it in an unhampered way while complying with all laws.

- ⦿ Evidence Collection in Social Media Forensics
  - The simplest method of evidence collection in social media forensics is a manual collection. It uses basic techniques such as visiting a website and/or taking a screenshot and is quite time-consuming. On the contrary, open source tools and other commercial forensic tools offer a quicker gathering and extraction of evidence. Additionally, since investigators often deal with a lot of live content, they also use content archiving to preserve the nature of the evidence.
  - Above all, e-discovery or evidence collection needs to in compliance with the terms of service agreement. Every social networking platform has specified terms and conditions that define the nature of the information that an investigator can collect and manipulate. Such conditions often inhibit investigations since the defense may cite breach of terms of service to dishonor the evidence.
- ⦿ The Three Basic Stages of Social Media Forensics
  - Social media forensics has three basic stages for the extraction, preservation, and analysis of electronic evidence.

- ⦿ 1. Evidence Identification
  - This step involves a thorough inspection of the crime scene to locate any hardware or software that is worthy of collection. It also includes conducting a basic search to identify all social networking accounts linked to the subject. Additionally, a search of all of the subject's families, friends and associated on social media. A forensic examiner needs to precisely document all sources of evidence along with how and when they found it.
- ⦿ 2. Collection
  - Forensic investigators use various methods to collect electronic evidence. Following are the methods for social media evidence collection.
    - Manual documentation
    - Screen scrape/Screenshot
    - Open source tools (HTTrack)
    - Commercial tool (X1)
    - Web service (Page freezer)
    - Forensic recovery
    - Content subpoena
  - Furthermore, different social media forensic tools kits are available for the logical acquisition of evidence on smartphones. The logical acquisition involves capturing a logical image of all files on the smartphone's internal memory. The files are then analyzed for evidence of various activities.
- ⦿ 3. Examination (Organization)
  - The files obtained during the logical acquisition require specific tools for decoding and viewing of their contents. Once decoded, they provide a vast amount of user data such as call history, sent and received SMS, calendar events, and address book entries. For social media forensics examiners, they provide a huge bank of social networking footprints. These artifacts are then examined and correlated to the actual case in hand.
- ⦿ Facebook Artifacts:
  - Activity logs, Facebook archives, profile information, places visited, locations and geo-locations, friends and family, applications, pages, groups, interests, text and links, the timestamp of all activities, details of friends engaged in active chat sessions with the subject and much more.
- ⦿ Twitter Artifacts:
  - User information, tweets posted, timestamps of the poster tweets, records of people followed by the subject and their tweets along with timestamps.

Social Networking Applications & Mobile Devices

- Due to the increasing use of social applications on smartphones, they are the biggest repertoire of evidence for forensic investigators. Did you know that more than 90% of social media users use mobile devices to access social networking platforms? Thus, they store a lot of potential information that social media forensics professionals can extract with the right tools. Furthermore, with the right inspection methods and tools, such evidence can provide crucial leads in a case.

- In fact, half of Facebook users access Facebook through its mobile applications on their smartphones or tablets. Moreover, such users are twice as active compared to those who use other devices (desktop, laptop) to access Facebook.
- Since millions of users leverage social networking applications on their mobile devices, the probability of misuse is also quite high! Hence, a forensic analysis of the suspect's mobile device offers a great potential to aid in his/her incarceration or exoneration.

- ⦿ Challenges of Forensic Analysis of Social Networking Applications on Mobile Devices
  - As much as the potential they have, smartphones also pose many challenges to social media forensics investigators. Since smartphones are always active and regularly update data, it causes faster loss of evidence. Secondly, the closed source OS of smartphones (except for Linux-based phones) make it difficult to extract evidence using custom tools.
  - To make things worse for forensic examiners, smartphone vendors release OS systems very often. This makes it challenging for social media forensics professionals to keep up with the latest tools and methods for examination.
- ⦿ Incognito Forensic Foundation (IFF Lab) – Social Media Forensics Laboratory in Bangalore
  - We are living in an era where each person has 5.54 social media accounts on an average. In such circumstances, the use of social networking platforms for executing a host of online crimes is inevitable. Incognito Forensic Foundation (IFF Lab) is a digital forensics lab in Bangalore that offers a range of digital forensics services such as social media forensics, mobile phone forensics, and cyber forensics. IFF Lab is a trusted name in the digital forensics industry and boasts of a reputed clientele.

The Security/Privacy Threats

- ⦿ Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.
  - Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.
  - Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.
  - Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or a anything that is designed to perform malicious operations on system. Malware can be divided in 2 categories:
    - Infection Methods
    - Malware Actions
  - Malware on the basis of Infection Method are following:
    - Virus
    - Worms
    - Trojan

    - Bots
- ⦿ Malware based on Actions:
    - Adware – Adware is not exactly malicious but they do breach privacy of the users. They display ads on computer’s desktop or inside individual programs. They come attached with free to use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
    - Spyware – It is a program or we can say a software that monitors your activities on computer and reveal collected information to interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they installs themselves and sits silently to avoid detection.
    - One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
    - Ransomware – It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
    - Scareware – It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
    - Rootkits – are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
    - Zombies – They work similar to Spyware. Infection mechanism is same but they don’t spy and steal information rather they wait for the command from hackers.

Forensics Auditing, and Forensics.

- ⦿ A forensic audit is an analysis and review of the financial records of a company or person to extract facts, which can be used in a court of law. Forensic auditing is a speciality in the accounting industry, and most major accounting firms have a department forensic auditing. Forensic audits include the experience in accounting and auditing practices as well as expert knowledge of forensic audit's legal framework.
- ⦿ Forensic audits cover a large spectrum of investigative activities. There may be a forensic audit to prosecute a party for fraud, embezzlement or other financial crimes. The auditor may be called in during the process of a forensic audit to serve as an expert witness during trial proceedings. Forensic audits could also include situations that do not involve financial fraud, such as bankruptcy filing disputes, closures of businesses, and divorces.
- ⦿ Reasons for Conducting a Forensic Audit?
    - Forensic audit investigations may expose, or confirm, various kinds of illegal activities. Normally, instead of a normal audit, a forensic audit is used if there is a possibility that the evidence gathered would be used in court.
    - The forensic audit process is similar to a traditional financial audit — planning, gathering evidence, and writing a report — with the additional step of a possible

appearance in court. The lawyers on both sides offer evidence that the crime is either discovered or disproved, which decides the harm sustained. They explain their conclusions to the defendant should the case go to trial before the judge.

- A forensic audit comprises the following steps:
  - Planning the Investigation: The forensic auditor and the team will plan their investigation in order to meet their objectives.
  - Collecting Evidence: The evidence gathered should be sufficient to prove in court the identity of the fraudster(s), reveal the details of the fraud scheme and document the financial loss suffered and the parties affected by the fraud.
  - *Reporting: *A forensic audit will need a written report on the crime to be given to the client, so that if they desire, they can continue to file a legal case.
  - *Court Proceedings: *During court proceedings, the forensic investigator must be present to clarify the evidence collected and how the suspect(s) were found by the team.

Challenges for digital forensics

- The increase in the number of people using networked digital devices has led to incidences of crime that call for forensic investigations (Brown, 2015). The existence of Cyber Forensics skills has made it possible to gather evidence from such devices. The evidence collected is used in courts to establish the crime and bring Cyber criminals to justice. Cyber Forensic investigators and analysts are often entrusted with the task of finding, recording, analysing, and reporting of digital evidence. The whole process of gathering forensic evidence has a number of challenges. These challenges are categorized into five broad areas: hardware challenges, software challenges, cloud forensic challenges, legal challenges and human challenges (Karie, & Venter, 2015; Lindsey, 2006; Mohay, 2005).
- HARDWARE CHALLENGES
  - Hardware challenges are linked to the needs of the modulated technology and enhancements of the hardware. Studies suggested that some criminal suspects change the hard disk within their devices before the Cyber Forensic expert can gain access to the device (National Institute of Justice, 2002; Brown, 2015). In such cases, the suspects use the write blockers to shift information between the two hard disks. The main effect is that a forensic examination of the new hard disk, may not display some of the relevant evidence. On the other hand, the evidence gathered from the new hard disk will lack consistency, and may not be apparent (Brown, 2015; Spafford, 2006).
- SOFTWARE CHALLENGES
  - The current era of technological advancements and changes in gathering forensic evidence has resulted into the birth of Platform as a Service (PaaS) and Software as a Service (SaaS), which have brought a number of changes into the computing structure. The use of new software and new technology has brought about a number of challenges. One of the challenges is lined to the well-developed device operating system. The current operating systems have been log enabled, and now requires a Cyber Forensic expert to gather background information on the device, which includes the information on accessibility of the application, usage of the application, and the level of information provided by the specific user of the

application. Even though the new development appears like a progress for the different devices, the development requires some time for it to mature (Spafford, 2006; Giordano & Maciag, 2002).

- CLOUD FORENSIC CHALLENGES
  - Cloud computing is now used by smart mobile devices. The flexibility and scalability of cloud computing poses a huge challenge to forensic investigation (Lopez, Moon, & Park, 2016). The data in these devices, maybe able to be accessed everywhere hence posing another challenge to the investigators. It is a challenge for the investigator to locate the data in a way that ensures the privacy rights of the users. The investigators require the knowledge on anti-forensic tools, practices, and tools that help ensure that the forensic analysis is done accordingly (Spafford, 2006; Lopez, Moon, & Park, 2016).
- LEGAL CHALLENGES
  - There have been some changes in the data protection and privacy regulations in different countries across the globe (Garrie & Morrissy, 2014). Cyber laws and regulations in different jurisdiction vary and many do not take into account, the complexity in collecting forensic evidence. For example, in the machine of a suspect, the information that is available is likely to have some personal information that could be crucial in an investigation. However, accessibility to such private information is likely to be considered as a violation of user privacy (Spafford, 2006)
- HUMAN CHALLENGES
  - Cyber Forensic experts are tasked with collecting and analysing the role of identifying criminals and going through all the evidence gathered against the criminals. These are well-trained professionals working for the public law enforcement agencies or in the private sector to perform roles that are associated to the collection and analysis of forensic evidence. The Cyber Forensic experts also come up with reports that are majorly used in the legal settings for investigations. Besides working in the laboratory, Cyber Forensic experts take up the role of applying the techniques of forensic investigation in the field uncovering the data that is relevant for the court (Karie & Venter, 2015).
- OTHER CHALLENGES
  - Elsewhere, in a literature-based study, Karie and Venter (2015) identified and categorized cyber forensic challenges into four: technical challenges, law enforcement or legal system challenges, personal-related challenges and operational challenges.
  - Technical Challenges were identified as vast volume of data; bandwidth restrictions; encryption; volatility of digital evidence; incompatibility among heterogeneous forensic techniques; the digital media’s limited lifespan; emerging devices and technologies, sophistication of digital crimes; anti-forensics; emerging cloud forensic challenge.
  - Legal Challenges were identified as jurisdiction, admissibility of digital forensic techniques and tools; prosecuting digital crimes; privacy; ethical issues; lack of sufficient support for civic prosecution or legal criminal prosecution.
  - Personnel-related Challenges were identified as semantic disparities in Cyber Forensics; insufficient qualified Cyber Forensic personnel; insufficient forensic

knowledge and the reuse among personnel; strict Cyber Forensic investigator licensing requirements; and lack of formal unified digital forensic domain knowledge.

- Lastly, Operational Challenges were identified as significant manual analysis and intervention; incidence detection, prevention and response; lack of standardized procedures and processes; and trust of Audit Trails.