1... Introduction to Cyber Crime and Cyber Security

Learning Objectives...

- To learn about Cybercrime and Cybercriminals.
- To get information of Cyber security.
- To know about Cyber Security Policy and Domains.

1.1 INTRODUCTION

- Cybercrime is a crime which includes computer and network to execute a crime. For example, unauthorized access or modify data or application, intellectual property theft, writing or spreading computer viruses etc. To commit a crime, either computer is involved or it may be a target. Cybercrime, especially through the Internet, has grown because computers are used in every field like commerce, entertainment and government. Cybercrime may put a person' or a nation's security in danger and it is not good for financial health.
- Cybercrime is committed by cybercriminals or hackers who want to make money. It is carried out by individuals or organizations. Some cybercriminals use advanced techniques and are highly technically skilled. Others are novice hackers.
- Cyber security is a way of protecting the computers, network, and other devices from cybercriminals. Cyber security is concern with both physical security of the devices and information stored therein.
- Cyber security means protecting information, devices, computers, computer resource, communication devices and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

1.2 CYBERCRIME: DEFINITION AND ORIGIN OF THE WORD

- Cybercrime is committed using a computer and internet. It is an illegal act where a special knowledge of computer technology is required for its preparation and investigation.
- "Cybercrime is any illegal behaviour, directed by means of electronic operations that target the security of computer system and the data processed by them".
- The term cyber is related to Information technology and the Internet. Origin of the word cyber comes from the word "cybernetics" which deals with information and its use. The term "cybercrime" evolved over the past few years since the adoption of internet and increasing millions of users of internet.

1.3 CYBERCRIME AND INFORMATION SECURITY

- Lack of information security increases cybercrimes. Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be important data of an organization, or personal details or profile on social media, data in mobile phone, biometrics etc. Since these information stores digitally in a computer and generally accessed through internet. Therefore, it is very important to protect this information from cybercriminals. Thus, information security and cybercrime are related to each other.

1.4 WHO ARE CYBERCRIMINALS?

- A cybercriminal is a person who conducts some form of illegal activity using computers or other digital technology such as the Internet.
- In other words, Cybercriminals are those who may be involved in activities like credit card fraud, cyberstalking, defaming people on social media, child pornography, unauthorized access to another computer, ignoring copyright, software licensing, trademark protection, overriding encryption to make illegal copied, software piracy, and stealing another's identity.
- The motive behind cybercrime is greed, desire of publicity, revenge, a sense of adventure, looking for thrill, access information, destructive mindset and desire to sell network security services.
- Cybercriminals are categorized into following three groups:

  Type I: Cybercriminals – hungry for recognition

  Examples:

  - Hobby hackers
  - IT professionals
  - Politically motivated hackers
  - Terrorist Organizations

Type II: Cybercriminals – interested in recognition

Examples:

- Psychological corrupts
- Financially motivated hackers
- Sponsored hackers
- Organized criminals

Type III: Cybercriminals – the insiders

Examples:

- Former employees seeking revenge.
- Companies using employees to gain economic advantages through damage and/or theft.

1.5 CLASSIFICATIONS OF CYBERCRIMES

- Cybercrimes are classified as follows:

1. Cybercrime against individual

- Following are the cybercrimes that come under this category:
  - E-mail spoofing and other online fraud
  - Phishing
  - Spamming
  - Cyber defamation
  - Cyberstalking and harassment
  - Computer sabotage
  - Pornographic offense
  - Password sniffing

2. Cybercrime against property

- Following are the cybercrimes that come under this category:
  - Credit card frauds
  - Intellectual property crime
  - Internet time theft

3. Cybercrime against organization

- Following are the cybercrimes that come under this category:
  - Unauthorized access of computers
  - Password sniffing
  - Denial-of-service attacks
  - Virus attacks
  - E-mail bombing

- Salami attacks
- Logic bomb
- Trojan horse
- Data diddling
- Industrial spying
- Software piracy

4. Cybercrime against society

- Following are the cybercrimes that come under this category:
  - Forgery
  - Cyberterrorism
  - Web jacking

5. Crime arises from Usenet newsgroup

- A Usenet newsgroup is similar to discussion forums, where messages are posted from users in different locations using Internet. They are not devoted to publishing news. Usenet group may carry offensive, harmful, inappropriate messages. Therefore, you should use common sense and proper judgment when using Usenet.

1.5.1 E-mail Spoofing

- E-mail spoofing is a form of cyber-attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. Email spoofing is a popular tactic used in phishing because people are more likely to open an email when they think it has been sent by a known sender.
- The goal of email spoofing is to trick recipients into opening or responding to the message.
- A spoofed email may include a link that installs malware on the user's device if clicked.

1.5.2 Spamming

- Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.
- E-mail spam is popular but it is used in other media also like Instant messaging Spam, Usenet newsgroup Spam, Web search engine Spam, Spam in blog, wiki Spam, online classified ads Spam, Mobile phone messaging Spam, Internet forum Spam, Social networking Spam, File sharing network Spam, Video sharing sites etc.
- Spam can be used to spread computer viruses, Trojan horses or other malicious software. The objective may be identity theft, or worse.
- Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, servers, infrastructures, IP ranges, and domain names, and it is difficult to hold senders accountable for their mass mailings.

1.5.3 Cyber Defamation

- Defamation means giving an "injury to the reputation of a person" by the way of 'Slander' or 'Libel'. The term 'Slander' means "the crime of damaging someone's reputation by false spoken statement", while 'Libel' is "false published or written statement by damaging someone's reputation".
- The term defamation is used in the section 499 of Indian Penal Code, 1860. Cyber defamation occurs when defamation takes place with the help of computer and internet.

1.5.4 Internet Time Theft

- Internet time theft occurs when an unauthorized person uses the internet hours paid by another person. In this, the hackers use another person's user ID and password to access their internet either by hacking or using some illegal means without the knowledge of the person.

1.5.5 Salami Attack/Salami Technique

- This kind of attack is normally widespread in the financial institutions or for the purpose of committing financial crimes. Salami technique is a technique by which cybercriminals steal very small amount of money at a time so that there is no noticeable difference in the overall size. The attacker gets away with these little amounts and thus gathers a considerable amount over a period of time. The principle of this method is the failure to detect the misappropriation.
- For example, a bank employee inserts a program into the bank server that deducts a small amount of money in a month from the account of every customer. No account holder probably notices this unauthorized debit, but the bank employee will make a large amount every month.
- The salami technique can also be applied to collect little information over a period of time, to gather an overall picture of an organisation or individuals. Data can be collected from websites, advertisements, and documents collected from trash cans, and gradually building up a whole database of factual intelligence about the target.
- Since the amount of theft is just below the threshold of perception, we need to be more watchful. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

1.5.6 Data Diddling

- Data Diddling is unauthorised altering of raw data before entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track.
- This type of attack can be done either by a person typing in the data, or a virus that is programmed to change the data, the programmer of the database or application, or

anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

- Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

1.5.7 Forgery

- Forgery is a crime that generally refers to the false making or alteration of a legal document or instrument with the specific purpose to cheat anyone. Currency notes, postage and revenue stamps, marksheets etc., can be forged using computers, printers and scanners.
- Forgery can occur in many forms, from signing another person's name on a check to falsifying one's own academic transcript.

1.5.8 Web Jacking

- This term is derived from the term 'Hijacking'. In these kinds of offences, the hacker gains access and control over the web site of another, by cracking the password and later changing it. He may even change the information on the site. This may be done for fulfilling political objectives or for money.
- The first stage of this crime involves "password sniffing".

1.5.9 Newsgroup Spam/Crimes Emanating from Usenet Newsgroup

Newsgroup Spam:

- Newsgroup spam is a type of spam where the targets are Usenet (USEr NETwork) newsgroups. This is one form of spamming. The meaning of spam is excessive multiple posting, that is, the repeated posting of a message (or similar messages).
- The advent of the large Usenet archive kept as part of the Google Groups website has made Usenet more attractive to spammers than ever.

Cybercrimes emanating from Usenet Newsgroup:.

- Usenet mainly used for following crime :
  - Distribution/sale of pirated software
  - Distribution of hacking software
  - Sale of stolen credit card number
  - Sale of stolen data
- Hackers often communicate with each other through Usenet newsgroups, Following are types of hacker UseNet groups:
  - General-purpose hacking newsgroups focus on stamp collecting or photography. hacker newsgroups tend to stray from their topics.
  - Encryption newsgroups cleverly hide their identity or messages using encryption.
  - Computer virus writers publish their latest creations in newsgroups or post URLs.

- Cracking newsgroups provide limited features until the user pays for a code or key to unlock the additional features.

1.5.10 Industrial Spying/Industrial Espionage

- Espionage or spying is the act of obtaining secret or confidential information from non-disclosed sources without the permission of the holder of the information. A person who commits espionage is called an espionage agent or spy.
- Industrial spying is a form of spying conducted for commercial purposes.
- Industrial espionage takes place in two main forms. The purpose of espionage is to gather knowledge about one or more organizations.
- It may include the acquisition of intellectual property, such as information of industrial manufacturers, ideas, techniques and processes, recipes and formulas. Or it could include proprietary or operational information, such as that on customer datasets, pricing, sales, marketing, research and development, policies, prospective bids, planning or marketing strategies or the changing compositions and locations of production.
- It may describe activities such as theft of trade secrets, bribery, blackmail and technological surveillance. As well as orchestrating espionage on commercial organizations, governments can also be targets. For example, to determine the terms of a tender for a government contract.
- With the growing availability of Trojans and Spyware material, low skilled individuals are now motivated to generate high volume profit out of industrial spying.

1.5.11 Hacking

- Hacking is an act of breaking into a computer and/or network and it is an offense. Hackers (the people doing the 'hacking') are basically computer programmers who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons.
- The main purposes of hacking are as follows:
  1. Greed
  2. Power
  3. Publicity
  4. Revenge
  5. Adventure
  6. Desire to access forbidden information
  7. Destructive mindset
- Some hackers hack credit card information of an individual, transfers money from others bank accounts to their own account. They extort money from corporates also. Government websites are popular on hacker's target list. Attack on Government web site receives wide press coverage.

1.5.12 Online Frauds

- Fraud that is committed using the internet is online fraud.
- Online fraud includes:
  - Financial fraud
  - Identity theft
  - Online scams
  - Spam
  - A scammer buying product online from your account without your knowledge.
  - Viruses that attack computers with the goal of retrieving personal information.
  - Email schemes that attack victims into wiring money to fraudulent sources.
  - "phishing" emails that appear to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit identity theft.

1.5.13 Computer Sabotage

- The use of the internet to obstruct the normal functioning of a computer system through the introduction of viruses, worms or logic bombs, is referred to as Computer Sabotage.
- The purpose of computer sabotage is to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracies, such as drug and human trafficking.

1.5.14 Email Bombing/Mail Bombs

- In Email bombing, an abuser sends high volumes of emails to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters.
- Computer program can be written to instruct a computer to do such activity repeatedly. Sending E-mail repeatedly to specified person's E-mail account by cybercriminal can flood the recipient's mail account and shut down the entire system.

1.5.15 Computer Network Intrusions

- Computer network can get security problem because people can get into them from anywhere. A network intrusion refers to any unauthorized activity on a digital network. Network intrusions often involve stealing valuable network resources and data.

- Hackers can break into a computer system from anywhere in the world and steal data, plant virus, insert Trojan Horses or change username and password.
- Hackers can create a program to capture login ID and password. Therefore, strong password is important.

1.5.16 Password Sniffing

- Password sniffers are the programs that monitor or record the name and password of network users as they login. This often happens on public Wi-Fi networks where it is relatively easy to spy on weak or unencrypted traffic.
- When data is transmitted across networks, if the data packets are not encrypted then data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyse the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.
- Using sniffing tools, attackers can sniff sensitive information from a network, including Email traffic (SMTP, POP, IMAP traffic), Web traffic (HTTP), FTP traffic (Telnet authentication, FTP Passwords, SMB, NFS) etc.

1.5.17 Credit Card Frauds

- Credit card fraud is a fraud committed using a payment card, such as a credit card or debit card. The purpose of this fraud is to make payment to another account which is controlled by a criminal.
- In Credit card fraud 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.

1.5.18 Identity Theft

- Identity theft occurs when someone uses another person's personal identifying information, like their name, ID number, or Credit card number, Bank account details without their permission, to commit fraud or other crimes.
- Identity theft is done to gain financial benefits. Someone involved in identity theft uses the victim's identity to commit other crimes. "Credit card fraud" is a crime involving identity theft, where the criminal uses the victim's credit card to fund his transactions.

1.6 DEFINITION OF CYBER SECURITY

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as Information Technology Security.

- We can divide cyber security into two parts, one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information.
- Some other definitions are:
  - "Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."
  - "Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

1.7 VULNERABILITY, THREATS AND HARMFUL ACTS

- In cyber security, Vulnerability, Threat, and Risk are terms that are related to each other.

1.7.1 Vulnerability

- A vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e., perform unauthorized actions) within a computer system. To exploit vulnerability, an attacker must have at least one tool or technique.

Classification:

- Vulnerabilities are classified according to the asset class that they are related to:

1. **Hardware:**
   - Susceptibility to humidity or dust.
   - Susceptibility to unprotected storage.
   - Age-based wear that causes failure.
   - Over-heating.
2. **Software:**
   - Insufficient testing
   - Insecure coding
   - Lack of audit trail
   - Design flaw
3. **Network:**
   - Unprotected communication lines (e.g., lack of cryptography).
   - Insecure network architecture.
4. **Personnel:**
   - **Inadequate** recruiting process.
   - **Inadequate** security awareness.
   - **Insider** threat.

5. **Physical site:**
   - Area subject to natural disasters (e.g., flood, earthquake).
   - Interruption to power source.
6. **Organizational:**
   - Lack of regular audits.
   - Lack of continuity plans.
   - Lack of security.

Reasons of Vulnerabilities:

- Following are the causes of Vulnerabilities:
  - **Complexity:** Large, complex systems increase the probability of flaws and unintended access points.
  - **Familiarity:** Using common, well-known code, software, operating systems, and/or hardware, increases the probability an attacker has or can find the knowledge and tools to exploit the flaw.
  - **Connectivity:** More physical connections, privileges, ports, protocols, and services increase vulnerability.
  - **Password Management Flaws:** The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.
  - **Fundamental Operating System Design Flaws:** The operating system designer chooses to enforce suboptimal policies on user/program management.
  - **Internet Website Browsing:** Some internet websites may contain harmful Spyware or Adware that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals.
  - **Software Bugs:** The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.
  - **Unchecked user input:** The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-validated inputs).
  - **Not learning from past mistakes:** Repetition of mistakes.

1.7.2 Threats

- A threat is anything that has the potential to disrupt or do harm to an organization. Threats can be intentional or unintentional. The cause of cyber threats can be incidents or activities, or failure to take action.

- Major Security Threats on Information Systems are Hacking, Viruses and Worms, Trojan Horse, Spoofing, Sniffing, Denial of Service(Dos), Malware.

Types of Cyber Security Threats:

1. **Malware:** Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software.
2. **Denial-of-service (DoS):** This attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.
3. **Man in the Middle (MiTM):** A Man-in-the-Middle (MiTM) attack occurs when hackers insert themselves into a two-party transaction and then use malware to install software and use data maliciously.
4. **Virus:** A virus is always hidden in a legitimate software or website and infects your computer as well as the computers of everyone in the contact list.
5. **Computer worm:** A computer worm works on its own, lives in the user's computer, and spreads by sending itself to other computers.
6. **Spyware / Trojan Horse:** A Trojan Horse is a malicious program that looks like a legitimate software. While installed on the computer it runs automatically and will spy on the system, or delete files.

1.7.3 Risk

- Risk refers to the calculated assessment of potential threats to an organization's security and vulnerabilities within its network and information systems.

Example:

- In a system that allows weak passwords,
  - **Vulnerability:** Password is vulnerable for dictionary or exhaustive key attacks
  - **Threat:** An intruder can exploit the password weakness to break into the system
  - **Risk:** The resources within the system are prone for illegal access/modify/ damage by the intruder.
- Cybercriminals use computer as a tool to perform unlawful and harmful acts such as phishing, spoofing, DoS (Denial of Service) attack, credit card fraud, online transaction fraud, cyber defamation, child pornography, kidnapping a person using chat rooms, stalking a person using Internet as medium, unauthorised access to computer system, cyber terrorism, creation and distribution of virus, spamming etc.

1.8 CIA TRIAD

- Confidentiality, Integrity and Availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. Confidentiality, integrity and availability together are considered the three most important concepts within information security. These three principles together can help guide the development of security policies for organizations.
- These three key concepts are described as follows:

1. **Confidentiality:** Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. Here, data is categorized according to the amount and type of damage that could be done, if it fell into the wrong hands. After that, according to those categories, strict measures can then be implemented.

   Example: Requiring an account number when banking online, data encryption, user IDs and passwords (two-factor authentication), biometric verification, take precautions to minimize the number of places where information appears and the number of times it is actually transmitted to complete a required transaction.

2. **Integrity:** Maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people.

   Example: File permissions and user access controls, version control may be used to prevent erroneous changes or accidental deletion by authorized users, detect any changes in data that might occur, using checksums for verification of integrity, backups or redundancies must be available to restore the affected data to its correct state, digital signatures can be used to provide effective nonrepudiation measures.

3. **Availability:** Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

   Example: Repair hardware immediately when needed, maintaining a properly functioning operating system, keep all necessary system upgrades, providing adequate communication bandwidth, safeguards against data loss in case of natural disasters and fire, a backup copy may be stored in a geographically isolated location, perhaps even in a fireproof, waterproof safe, use of firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.

1.9 CYBER SECURITY POLICY AND DOMAINS OF CYBER SECURITY POLICY

1.9.1 What is Cyber Security Policy?

- In general, Cyber security policies are the directives designed to maintain cyber security. Cyber security policy refers to laws and regulations concerning information distribution, private enterprise objectives for information protection, computer operations methods for controlling technology, and configuration variables in electronic devices.
- Cyber security policy is presented as something that set out security goals in support of constituents who are expected to modify their behaviour in compliance with the policy to produce cyber security.
- There is a governance body who establishes laws, rules, and/or regulations that are meant not only to affect constituent behaviour, but also affect others, who thereby become stakeholders in the policy process. Organizations are bound by the governing bodies to obey the policy. Organizations observe cyber security policies issued by governing bodies as well as establish their own internal cyber security policies.

1.9.2 Domains of Cyber Security Policy

- There are different domains of the governance hence cyber security applies to the corresponding governance according to the domain. For example, a nation-state cyber security policy will apply to all citizens within its domain, whereas a corporate cyber security policy will apply only to the staff of the corporation, cyber security policy issued by an industry regulator will apply only to those industries in its regulatory domain.
- The content of security policy will change according to corresponding governing body. The goals of nation-state security are very different from the goals of corporate security, and so policy statements and corresponding expected activities in support of policy will appear very different. Therefore, the content of security policy will change according to the domain.
- Following are the domains of Cyber Security Policy:

1. **Laws and Regulations:**

   Policies are made so that according to the laws and regulations, judgement can be given. Laws and regulations would reflect a wise and thoughtfully framed policy.

2. **Enterprise Policy:**

   In a corporate environment, policies are expected to be followed and if not followed, the employees can be terminated. A mid-level manager supports processes such as staff hiring or expense filing, they may be expected to bring

department activities into compliance with the policies, and often will have to establish department-level metrics for compliance. But in the case of government, sub-organization will decide the policies. Chief Executive Officer will generally apply policies to an entire corporation.

3. **Technology Operations:**

   To assist clients in complying with legal and regulatory information security requirements, the legal, accounting, and consulting professions have adopted standards for due diligence with respect to information security. These were sometimes proprietary to the consulting firm, but were often based on published standards where a standard becomes the preferred mode of operation for securing a technology environment. It will often be referred to as a cyber security policy for technology operations and management.

4. **Technology Configuration:**

   Many technology operations standards use specialized security software and devices. Technology operators refer to the standard-specified technical configuration of these devices as "security policy." These specifications are implemented by vendors and service providers. Vendors label alternative technical configurations for their products as "security policies." Vendor marketing literature presents these technical configurations as "policy".

Summary

- Cybercrime is a crime which includes computer and network to execute a crime.
- Cyber security is a way of protecting the computers, network, and other devices from cybercriminals.
- Email spoofing is a form of cyber-attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source.
- Spam is any kind of unwanted digital communication that gets sent out in bulk.
- Internet time theft occurs when an unauthorized person uses the internet hours paid by another person.
- Salami technique is a technique by which cybercriminals steal very small amount of money at a time so that there is no noticeable difference in overall size.
- Data Diddling is unauthorized altering of raw data before entry into a computer system, and then changing it back after processing is done.
- Forgery is a crime that generally refers to the false making or alteration of a legal document with the specific purpose to cheat anyone.
- In web jacking the hacker gains access and control over the web site of another by cracking the password and latter changing it.

- Hackers are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for unfair reasons.
- In Email bombing an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing.
- Password sniffers are the programs that monitor or record the name and password of network users as they login.
- The purpose of Credit card fraud is to make payment to another account which is controlled by a criminal.
- Identity theft occurs when someone uses another person's personal identification information.
- Vulnerability is a weakness which can be exploited by an attacker, to perform unauthorized actions within a computer system.
- A threat is anything that has the potential to disrupt or do harm to an organization.
- Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. Integrity means maintaining the consistency, accuracy and trustworthiness of data. Availability means information should be consistently and readily accessible for authorized parties.

Check Your Understanding

1. Which of the following is also known as Malicious software?
   (a) Badware (b) Illegalware
   (c) Malware (d) Maliciousware
2. Which of the following is considered as the unsolicited commercial email?
   (a) Virus (b) Spam
   (c) Malware (d) All of the above
3. In any organization, company or firm the policies of information security come under_____.
   (a) CIA Triad (b) Confidentiality
   (c) Authenticity (d) None of the above
4. When you use the word _____ it means you are protecting your data from getting disclose(d).
   (a) Confidentiality (b) Integrity
   (c) Authentication (d) Availability
5. _____ means the protection of data from modification by unknown users.
   (a) Confidentiality (b) Integrity
   (c) Authentication (d) Non-repudiation

6. _____ of information means, only authorized users are capable of accessing the information.
   (a) Confidentiality (b) Integrity
   (c) Non-repudiation (d) Availability
7. Existence of weakness in a system or network is called _____.
   (a) Threat (b) Vulnerability
   (c) Exploit (d) Attack
8. Which of them is not a proper method for email security?
   (a) Use Strong password
   (b) Use email Encryption
   (c) Spam filters and malware scanners
   (d) Click on unknown links to explore
9. _____ are programs or devices that capture the vital information from the target network or particular network.
   (a) Routers (b) Trappers
   (c) Wireless-crackers (d) Sniffers
10. Passwords are used to improve the _____ of a network.
   (a) Performance (b) Reliability
   (c) Security (d) Longevity

ANSWERS

1. (c)	2. (b)	3. (a)	4. (a)	5. (b)	6. (d)	7. (b)
8. (d)	9. (d)	10. (c)				

Practice Questions

Q.I Answer the following questions in short.

1. What is E-mail spamming?
2. Distinguish between hacker and user.
3. What is meant by logic bomb?
4. Define the Malicious program?
5. Define cybercrime?
6. List the cybercrime comes against organization.
7. List the cybercrime comes against individual.
8. What is E-mail spoofing?
9. What is cyber defamation?
10. What is hacking?
11. What do you meant by Password sniffing?

12. Define cyber security.
13. What is Cyber Security Policy?

Q.II Answer the following questions.

1. What is Cyber Security? Explain in detail how to secure information?
2. What is CIA? Discuss three concepts of CIA model.
3. Explain vulnerabilities in network security.
4. How do you classify cybercrime? Explain each one in briefly.
5. Who are cybercriminals? Describe each category with example.
6. Explain Salami attack with example.
7. Explain the following terms in brief:
   (a) Data Diddling, (b)Forgery
8. What is Vulnerabilities? Explain different causes of Vulnerabilities.
9. Write short notes on Domains of Cyber Security Policy.

Q.III Define the terms.

1. E-mail spamming
2. Spoofing
3. Data diddling
4. Salami attack
5. Hacking
6. Computer Sabotage
7. Threats

2...

Cyber Offenses and Cyberstalking

Learning Objectives...

- To know about criminals plan and Cyber Attacks.
- To get information of Cyberstalking.
- To get knowledge about botnets, credit card frauds, security challenges, attacks on mobile.

2.1 CRIMINALS PLAN

- Technology 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 purposes. Computers are also used as target of offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders. Cybercrimes like hacking, cyberterrorism, network intrusions, password sniffing, computer viruses, etc. are the most commonly occurring crimes that target the computer.
- Cybercriminal uses the computer and Internet for all illegal activities like getting 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.
- Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization.
- People who commit cybercrimes are known as "Crackers". A cracker is a person who breaks into computers. The term hacker is often confused with **cracker**. 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 **Brute force hacking** is also used. 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.
- Some of the computer programs that are used to break into other communication systems are called "**Phreaking**". Phreaking sites on the Internet are popular among crackers and other criminals.
- War dialler is a program that automatically dials phone numbers looking for computers on the other end. It catalogues numbers so that the hackers can call back and try to break in.
- Criminals always search the vulnerabilities of their target. Vulnerability is a weakness which can be exploited by an attacker. Since the networks are not adequately protected, the criminal takes advantage of it.

Categories of vulnerabilities:

- The categories of vulnerabilities that hackers typically search for are the following:
  1. Inadequate border protection (border as in the sense of network periphery).
  2. Remote Access Servers (RASs) with weak access controls.
  3. Application servers with well-known exploits.
  4. Misconfigured systems and systems with default configurations.

2.1.1 Categories of Cybercrime

- The crime that involves and uses computer devices and Internet is known as Cybercrime. Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations.
- Cybercrime or Cyberattacks are categorized into five types. It can be categorized based on some factors.
  1. The target of the crime.
  2. Whether the crime occurs as a single event or as a series of events.
- Attack in which Cybercriminals can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).
  1. **Crimes targeted at individuals:** The cyber criminals exploit human weakness such as avidity and innocence. These crimes include financial frauds, sale of non-existent or stolen items, child pornography, copyright violation, harassment, etc. Latest technology development and growth of internet cyber criminals have new attacking tools that make them to expand group of potential victims.
  2. **Crimes targeted at property:** This kind of crime includes stealing devices such as cell phone, laptops, personal digital assistant (PDAs), CDs and pen drives. Sometimes attackers insert harmful programs such as Trojan virus to disturb the function of the hard disk and pen drive. Also, it can wipe out data from the hard disk, and can create the malfunctioning of the attached devices in the system.

3. **Crimes targeted at organizations:** Cyberattacks performed against an organization is also called as Cyber terrorism. Attackers (individuals or groups of individuals) use computer tools and the Internet to perform Cyber terrorism. Attackers steal the private information, and also damage the programs and files or plant programs to get control of the network and/or system.
4. **Single event of Cybercrime:** These types of Cyberattack are performed in a single event from the victim's point of view. For example, mistakenly opened email may contain virus. Representation of incorrect website called as Phishing and steal valuable financial information. This kind of attack is also called as Hacking or Online fraud.
5. **Series of Events:** Sometimes the attacker performs a series of events to track the victim. 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.

2.1.2 Cyber Attacks

- Criminals use many methods and tools to locate the vulnerabilities of their victim. The victim can be an individual or an organization.

I. Criminals plan two types of attacks:

1. **Passive attacks:** Passive attacks attempt to gain information about the target. It exploits confidential information. Passive attacks involve gaining data about a target without the knowledge of the target.
2. **Active attacks:** Active attacks are usually used to alter the system. It may affect the integrity, authenticity and availability of data.

II. Attackers can be categorized as follows:

1. **Inside attacker:** Attacks perform within the organization is called inside attack.
2. **Outside attacker:** Attacker gets information from outside is called outside attack.

Phases in planning cybercrime:

- 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).

2.1.2.1 Reconnaissance

- This is first step towards cyber-attacks; it is one kind of a passive attack. "Reconnaissance" means an act of finding something or somebody. In this phase, the attacker tries to explore and gain the every possible information about the target.

- In the hacking world, reconnaissance phase begins with "Foot printing", hence, this is the pre-attack phase, where the data about the target's environment and computer architecture is collected. Foot printing gives an overview about system vulnerabilities.
- In this phase, the attacker understands 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.

1. **Passive Attack:**

- A passive attack involves gathering information about a target without his/her knowledge.
- Information is collected using Internet and for that the following approaches are used:
  - Google or Yahoo search: People search to locate information about employees.
  - Surfing social media like Facebook to gain information about an individual.
  - Organization's website may provide a personnel directory or information about employees' contact details, E-mail address, etc.
  - Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
  - Using job postings sites, job profiles of technical persons are collected which can provide information about the type of technology like servers or infrastructure devices a company maybe using on its network.

2. **Active Attack:**

- In active attacks, the attacker explores the network of the victim and discovers individual hosts to confirm the information like IP addresses, operating system type and version, and services on the network, gathered in the passive attack phase.
- It 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.

2.1.2.2 Scanning/Scrutinizing gathered Information

- In this phase the attacker validates the collected information to find out the existing vulnerability. It is a key phase before the actual attack happens.
- The objectives of scanning are as follows:
  1. **Port scanning:** Identify all ports and services (open / closed).
  2. **Network scanning:** Verify IP address and network information before cyber-attacks.
  3. **Vulnerability scanning:** Checking loop holes in the system.

2.1.2.3 Attack (Gaining and Maintaining the System Access)

- After completing the first two steps, 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 of the illegal activity.

2.1.3 Social Engineering

- Social engineering is the art of manipulating people, so they give up confidential information. Social engineering is a non-technical strategy used by cyber attackers. It involves human interaction. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- Social engineering relies on the basic human instinct of trust to steal personal and corporate information that can be used to commit further cybercrimes.
- For example, a cybercriminal might use social engineering to convince an employee to tell company passwords. The cybercriminal then uses these passwords to access corporate networks to steal data and to install malware on the company network.
- Social engineering attacks happen in one or more steps. A criminal first investigates the victim to gather necessary background information, such as points of entry and weak security protocols. Then, the attacker gains the victim's trust and breaks security practices, such as revealing sensitive information or granting access to critical resources.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- **A social engineer** usually uses phone or internet to get them to do something.
- The goal of a social engineer is to fool someone into providing valuable information or access to that information. Social engineer studies the human behaviour 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.

  Example: 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.

2.1.3.1 Classification of Social Engineering

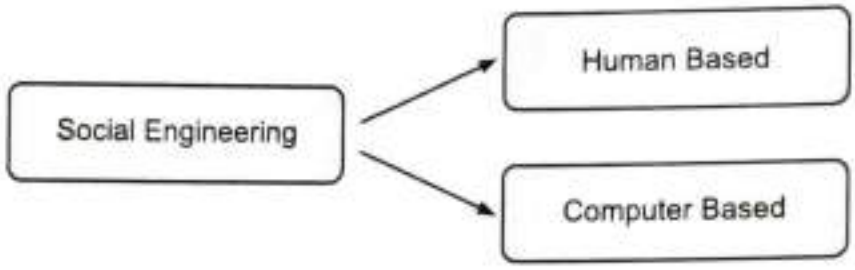

Fig. 2.1: Types of Social Engineering

I. Human-Based Social Engineering

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

1. **Impersonating an employee or valid user:**
   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. So, a lower-level employee such as a help-desk worker will help him/her in gaining access to the system.
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 mostly used 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. It is also called dumpstering, binning, trashing, garbing or garbage gleaning.

II. Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

1. Fake E-mails:

- The attacker sends fake E-mails to users in such a way that the user finds it as a real e-mail. This activity is also called "Phishing". The purpose of fake e-mail is to collect the personal information, such as usernames, passwords and credit card details from organization or an individual. Banks, financial institutes and payment gateways are the common targets.
- Phishing is also carried out through a website where it 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 internet users.
- The term "Phishing" has been evolved from the analogy that Internet scammers are using E-mails to attract fish for passwords and financial data from the sea of Internet users.
- The term was made 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:

- Attachments are sent with E-mail messages which contain malicious code and that code gets inserted into a victim's system automatically. Viruses, Trojans, and worms can be included cleverly into the attachments to attract 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.

2.2 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.
- Cyberstalking is a new form of internet crime in our society, when a person is pursued or followed online. A cyber stalker does not follow his victim physically, but

follows virtually. A cyber stalker follows his online activity to harvest information about the victim and harass him / her and make threats using verbal intimidation. For that cyber stalker uses electronic or digital means, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum.

- Cyberstalking 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 individuals 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, cyber stalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.2.1 Types of Stalkers

- There are two types of stalkers: Online stalkers and Offline stalkers.

1. **Online stalkers:**

   An Online stalker starts an interaction with the victim with the help of the Internet. They use E-mail and chat rooms to get connected with the victim, rather than using traditional instrumentation like phone.

2. **Offline stalkers:**

   An Offline stalker begins 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.

2.2.2 Cases Reported on Cyberstalking

- The majority of cyber stalkers are men and the majority of their victims are women. In some cases, women act as cyber stalkers and men are the victims and there are cases of same-sex cyberstalking as well.
- In many cases, the cyber stalker 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 neighbour. However, there also have been many instances of cyberstalking by strangers.

2.2.3 Working of Stalking

- It is seen that stalking works in the following ways:
  1. Personal information gathering about the victim: Name, family background, contact details, address of residence as well as of the office, E-mail address, date of birth, etc.
  2. Establish a contact with victim through phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
  3. Stalkers will always establish a contact with the victims through E-mail. The stalker may use multiple names while contacting the victim. Some stalkers keep on sending repeated E-mails asking for various kinds of approval or threaten the victim.
  4. The stalker may post the victim's personal information on any website related to illegal 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 for relationships. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
  5. Whosoever comes across the information, start calling the victim on the given contact details for relationships.

2.3 REAL-LIFE INCIDENT OF CYBER STALKING

Case Study

- The Delhi police have registered the first case of cyberstalking – 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 the 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.

2.4 CYBERCAFE AND CYBERCRIMES

- Cybercriminals prefer cybercafés to carry out their activities. In the past several years, many instances have been reported in India, where cybercafés are known to be used for terrorist communication.

- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafés. Cybercafés have also been used regularly for sending obscene mails to harass people.
- In cybercafés, where public computers are used, hold following two types of risks:
  1. You do not know what programs are installed on the computer. There may be malicious programs running at the background that can capture the keystrokes to know the passwords and other confidential information and monitor the browsing behaviour.
  2. Over-the-shoulder surfing can enable others to find out your passwords.
- The criminals tend to identify one particular personal computer (PC) to prepare it for their use. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency maybe alternate day or twice a week.

Facts about cybercrimes in cybercafé:

- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:
  1. Pirated software(s) such as OS, browser etc. are installed in all the computers.
  2. Antivirus software is found to be not updated to the latest patch.
  3. Several cybercafés 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 cybercafés to pick up clues after the Internet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.
  4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence hard disks are not formatted, so cybercriminal can install a malicious software.
  5. Pornographic websites and other similar websites with indecent contents are not blocked.
  6. Cybercafé 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 cybercafé owners.
  8. Cybercafé association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafés.

Safety tips while using the computer in a cybercafé:

- Here are a few tips for safety and security while using the computer in a cybercafé:
  1. Always logout.
  2. Stay with the computer.

3. Clear history and temporary files.
4. Be alert of the surroundings.
5. Avoid online financial transactions.
6. Change passwords.
7. Use Virtual keyboard.
8. Read Security warnings while accessing bank or financial website.

2.5 BOTNETS: THE FUEL FOR CYBERCRIME

2.5.1 Botnet

- The dictionary meaning of Bot is "An automated program for doing some particular tasks, often over a network."
- Botnet is a term used for collection of software that runs autonomously and automatically. Botnet is associated with malicious software but can also be used for distributed computing software.
- A Bot runs automatically in the computer and can gain the control of the 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 used to distribute Spam and viruses to conducting Denial-of-Service (DoS) attacks.

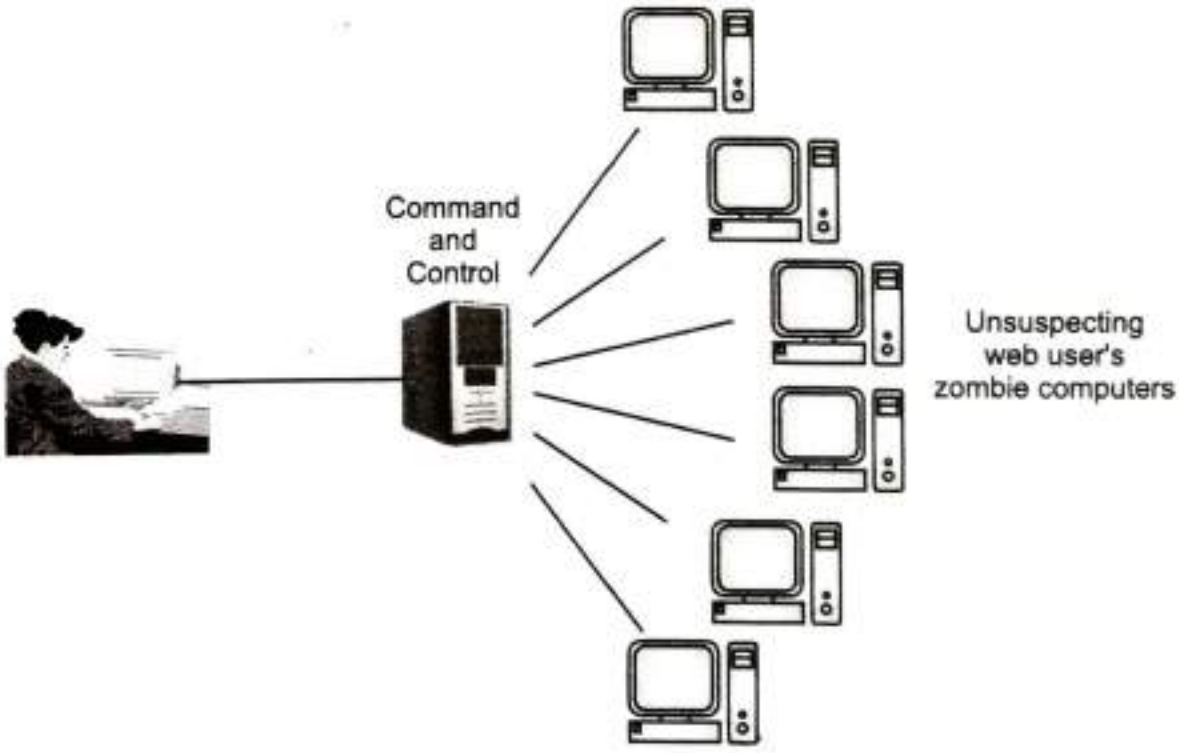

Fig. 2.2: Botnet

- A Botnet is also called as Zombie network. It 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.

Methods to secure the system:

- Following methods can be used 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 are 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 known and trustworthy websites.
  6. Regularly check the mail box and sent items for those messages you did not send.
  7. Take an immediate action if your system is infected.

2.6 ATTACK VECTOR

- An "attack vector" is a path, which an attacker can gain access to a computer or a network server to deliver a 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, except deception, in which a human operator is fooled into removing or weakening system defenses.
- Firewalls and antivirus software can block attack vectors in some extent.
- The attack vectors described here are how most of them are launched.
  1. **Attack by E-mail:** The malicious program is embedded in the message or the message link. Spam is always a carrier for scams, fraud, dirty tricks, or malicious action of some kind.
  2. **Attachments:** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. As soon as you open attachments, the malicious programs install.
  3. **Attack by deception:** Deception is aimed as a vulnerable entry point. It includes Fraud, and scams. Social engineering are other forms of deception that are often an attack vector too.
  4. **Hackers:** Hackers/Crackers use a variety of hacking tools 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 genuine websites. Users give their personal information. 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. 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. Macros can also be used for malicious purposes.
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.
9. **Viruses:** Virus vectors include E-mail attachments, downloaded files, worms, etc.

2.7 CYBERCRIME: MOBILE AND WIRELESS DEVICES

- Mobile devices have become an integral part of business, providing connectivity with the Internet outside the office, but it brings many challenges to secure these devices from being a victim of cybercrime.
- Mobile phones contain personal information also like contact details, bank accounts etc. Some apps may also store credit card information that can allow criminals to buy whatever they want and ship it wherever they want. Phone probably contains direct access to your e-mail, text messages and social media accounts that can be used to steal your identity and providing sensitive information as well.
- Things like these can happen when an attacker physically gets hold of your mobile device. But there are a growing number of exploits that take advantage of your phone's Bluetooth, Wi-Fi and cellular connections to gain virtual access to your phone. Phones can be infected with malware just like a computer can.

2.7.1 Proliferation of Mobile Devices

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

2.7.2 Trends in Mobility

- The third generation (3G) mobile phone 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. This smart mobile technology is popular in attackers (hackers and crackers) also.

- 3G networks are not entirely built with IP data security. There are numerous attacks that can be committed against mobile networks and they can originate from the following two primary vectors:
  1. **Outside the mobile network:** Public Internet, Private networks and other operator's networks.
  2. **Within the mobile network:** Devices such as data-capable handsets and Smartphones, Notebook computers or even Desktop computers connected to the 3G network.
- Popular types of attacks against 3G mobile networks are as follows:

1. **Malwares, Viruses and Worms:**

- Here are few examples of malware(s) specific to mobile devices:
  - **Skull Trojan:** It targets Series 60 phones equipped with the Symbian mobile OS.
  - **Cabir Worm:** It 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.
  - **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
  - **Brador Trojan:** It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-mail file attachments.
  - **Lasco Worm:** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. **Denial-of-Service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users.
3. **Overbilling Attack:** Overbilling involves an attacker hijacking a subscriber's IP address and then using the connection to initiate downloads.
4. **Spoofed Policy Development Process (PDP):** These of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunnelling Protocol].
5. **Signalling-level Attacks:** The Session Initiation Protocol (SIP) is a signalling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services.

2.8 CREDIT CARD FRAUDS IN MOBILE AND WIRELESS COMPUTING ERA

- **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.

- Wireless credit card processing allows a person to process credit cards electronically, virtually anywhere. Wireless credit card processing allows businesses to process transactions from mobile locations quickly, efficiently and professionally.

2.8.1 Types and Techniques of Credit Card Frauds

- Credit card fraud is a form of identity theft in which criminals makes purchases or obtains cash advances using a credit card account assigned to you.
- Following are techniques of credit card frauds:

I. Traditional Techniques:

1. Paper-based application fraud :

- The traditional credit card fraud is paper-based application fraud. In which a criminal use stolen or fake documents such as utility bills and bank statements those can build up useful information to open an account in someone else's name.
- Application fraud can be divided into:
  - **i. ID theft:** Where an individual pretends to be someone else.
  - **ii. Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit.

2. Illegal use of lost and stolen cards:

- In another form of traditional technique, criminal use Illegal use of lost and stolen cards. Credit card can be stolen either by pick pocketer or from postal service before it reaches its final destination.

II. Modern Techniques:

1. Skimming Card information:

- In this technique, criminals produce a fake credit card. Then they use skimming to commit fraud.
- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- Phishing site can also be used. Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink/website.

2. Triangulation:

- The criminal offers goods with heavy discounted rates through a website. The customer registers on this website along with his 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. Such websites are usually available for few weeks/months, so it is not possible to track.

3. **Credit card generators:**
   - It is another modern technique where computer imitation software 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.

2.9 SECURITY CHALLENGES POSED BY MOBILE DEVICES

- Mobility brings two types of challenges to cybersecurity:
  1. Information is being taken outside from the mobile device.
  2. The devices are remotely accessed by the attacker.
- Cybersecurity challenges are important for organizations; hence, they should adopt appropriate security operating procedures.
- As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro-challenges."

Challenges in Mobile Security:

- Some 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.

2.10 AUTHENTICATION SERVICE SECURITY

- There are two components of security in mobile computing:
  1. Security of devices
  2. Security in networks.
- In a secure network, there must be authenticated access between the device and the base stations. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can be inserted by the service provider to trick the device. Thus, the networks also play a crucial role in security of mobile devices.
- Other kinds of attacks in the mobile devices are: Push attacks, Pull attacks and Crash attacks.
- Service security must be authenticated otherwise some typical attacks may happen on mobile devices through wireless networks like: DoS attacks, traffic analysis,

eavesdropping, Man-in-the-Middle attacks and session hijacking. To secure the wireless networks some techniques can be used like: Wireless Application Protocols (WAPs), use of VPNs, Media Access Control (MAC) address filtering and development in 802.xx standards.

2.11 ATTACKS ON MOBILE/CELL PHONES

- Mobile phones have become a necessary part of everybody's life. Theft of mobile phones has risen dramatically over the past few years. Major locations where mobile phone 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.
- After PC, the criminals' target has been cell phones, because the increasing usage of cell phones and availability of Internet in cell phones. Another reason is increasing Wi-Fi zones in the cities and extensive usage of cell phones with lack of awareness/knowledge about the vulnerabilities of the technology.

Factors contribute for outbreaks on Mobile devices:

- The following factors contribute for outbreaks on mobile devices:
  1. Enough terminals or more devices to attack.
  2. The expanded functionality i.e., office functionality and apps also increase the probability of malware.
  3. Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

Types of Mobile security threats:

- Mobile security threats are attacks that are intended to compromise or steal data from mobile devices like smartphones and tablets.

Mobile device attacks have the following four categories:

1. **App-based mobile threats:** These types of attacks can occur when users download malicious apps or grant apps permission to access device data without checking whether or not it's safe to do so.
2. **Web-based mobile threats:** A web-based mobile attack is usually achieved through phishing or spoofing. Attackers will send an email, text, or other instant message that looks as if it was from a trusted source but the message contains a malicious link or attachment. When users click through or provide personal information, the bad actor can then gain unauthorized access to their mobile device or steal credentials to spoof identities.
3. **Network threats:** This attack occurs when bad actors target unsecured or free-to-use public Wi-Fi connections. In some cases, hackers may even set up a fake Wi-Fi

network (known as network spoofing) in an attempt to trick users. Spoofed networks will ask users to create an account with a username and password, giving hackers the opportunity to compromise devices and credentials.

4. **Physical threats:** Lost, stolen, and unattended devices open users up to a range of cell phone security issues. Your phone can easily be hacked if you don't use a strong password, PIN, or biometric authentication, or use unencrypted apps and services.

Summary

- Attack in which Cybercriminals can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).
- Passive attacks attempt to gain information about the target. But, active attacks are usually used to alter the system.
- Attacks perform within the organization is called inside attack. And attacker get information from outside is called outside attack.
- Information gathering (Reconnaissance), Scanning, and Launching an attack are the phases of planning cybercrime.

  Social engineering is the art of manipulating people, so they give up confidential information.
- Human-based social engineering refers to person-to-person interaction to get the desired information. But Computer-based social engineering refers to get the desired information by using computer.
- Cyber stalking is the activity to harvest information about the victim and harass him / her and make threats using verbal intimidation.
- Cybercriminals prefer cybercafés to carry out their activities.
- Botnet is a collection of software that runs automatically in the computer and can gain the control of the computer by infecting them with a virus or other Malicious Code that gives the access.
- An "attack vector" is a path, which an attacker can gain access to a computer or a network server to deliver a malicious outcome.
- The traditional credit card fraud is paper-based-application fraud. In which a criminal use stolen or fake documents such as utility bills and bank statements that can build up useful information to open an account in someone else's name. In Modern technique criminals produce a fake credit card.
- **Mobility** brings two types of challenges to cybersecurity: Information is being taken **outside** from the mobile device, and the devices are remotely accessed by the attacker.

Check Your Understanding

1. In which of the following, a person is constantly followed by another person or group of several peoples?
   (a) Phishing (b) Bulling
   (c) Stalking (d) Identity theft
2. Which of the following is not an example of social engineering?
   (a) Dumpster diving (b) Shoulder surfing
   (c) Carding (d) Spear phishing
3. _____ is an attempt to steal, spy, damage or destroy computer systems, networks or their associated information.
   (a) Cyber-security (b) Cyber attack
   (c) Digital hacking (d) Computer security
4. In _____ attacks an attacker do not contact with authorizing party for stealing password.
   (a) Passive online (b) Active online
   (c) Offline (d) Non-electronic
5. A _____ is a process of breaking a password protected system or server by simply & automatically entering every word in a dictionary as a password.
   (a) Dictionary attack (b) Phishing attack
   (c) Social engineering attack (d) MiTM attack
6. _____ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones.
   (a) Worms (b) Antivirus
   (c) Malware (d) Multimedia files
7. A _____ is a number of Internet-connected systems, where each of them is running one or more bots.
   (a) Trojan (b) Virus
   (c) Worms (d) Botnet
8. Which of the following is/are threats for electronic payment systems?
   (a) Computer worms (b) Computer virus
   (c) Trojan horse (d) All of the above

ANSWERS

1. (c)	2. (c)	3. (b)	4. (a)	5. (a)	6. (c)	7. (d)
8. (d)						

Practice Questions

Q.I Answer the following questions in short.

1. Define Cyber Terrorism.
2. What is social engineering?
3. What is cyberstalking?
4. What is Reconnaissance?
5. Who is online cyberstalker?
6. Who is offline cyberstalker?
7. Define attack vector.

Q.II Answer the following questions.

1. Describe active and passive attacks. Discuss different types of active attack and passive attack?
2. Explain the difference between passive and active attacks. Give an example.
3. Explain how botnets can be used as a fuel to cybercrime.
4. What are the different attacks launched with attack vector? Explain.
5. What kinds of attacks are possible on mobile phone? Explain with example.
6. Explain how criminals plan cyber attacks.
7. Describe 5 categories of cybercrime.
8. Explain Human-based social engineering.
9. Explain Computer-based social engineering.
10. Explain working of stalking with example.
11. What are the risks involve in cybercafés? Mention tips for safety while using the computer in a cybercafé.
12. Explain different techniques of Credit Card Frauds.

Q.III Define the terms.

1. Active attack
2. Passive attack
3. Hacker
4. Cyber stalkers
5. Active vector
6. Botnet

Practice Questions

Q.I Answer the following questions in short.

1. Define Cyber Terrorism.
2. What is social engineering?
3. What is cyberstalking?
4. What is Reconnaissance?
5. Who is online cyberstalker?
6. Who is offline cyberstalker?
7. Define attack vector.

Q.II Answer the following questions.

1. Describe active and passive attacks. Discuss different types of active attack and passive attack?
2. Explain the difference between passive and active attacks. Give an example.
3. Explain how botnets can be used as a fuel to cybercrime.
4. What are the different attacks launched with attack vector? Explain.
5. What kinds of attacks are possible on mobile phone? Explain with example.
6. Explain how criminals plan cyber attacks.
7. Describe 5 categories of cybercrime.
8. Explain Human-based social engineering.
9. Explain Computer-based social engineering.
10. Explain working of stalking with example.
11. What are the risks involve in cybercafés? Mention tips for safety while using the computer in a cybercafé.
12. Explain different techniques of Credit Card Frauds.

Q.III Define the terms.

1. Active attack
2. Passive attack
3. Hacker
4. Cyber stalkers
5. Active vector
6. Botnet

❖❖❖

3... Tools and Methods Used in Cybercrime

Learning Objectives...

- To learn about various Tools and Methods Used in Cybercrime such as
  - Proxy servers and anonymizers
  - Phishing
  - Password cracking
  - Keyloggers and spywares
  - Overview of virus and worms
  - Trojan horses and backdoors
  - Steganography
  - DoS and DDoS attacks
  - SQL injection.

3.1 INTRODUCTION

- In the previous chapter, you have learnt how criminals plan cybercrime against an individual or an organization. In order to protect your system from attack, you need to know about the different ways in which your computer can be attacked and your personal information being stolen.
- In this chapter, few common tools and techniques are discussed which are used by the cyber criminals.
- Let us see various forms of cyber-attacks.
- Following are the steps of attacks through which attackers target the computer systems:

Step 1 : Initial uncovering:

- Initially the attacker performs the following two steps:
  1. Attacker gathers information about the target on the Internet websites. It is called 'reconnaissance'.

2. 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.

Step 2: Network probe (Investigation):

- At this stage, the attacker scans the organization information through a "ping sweep" of the network IP addresses. Then a "port scanning" technique is used to know which services are running on the target system. At this point, the attacker has still not done any abnormal activity on the network.

Step 3: Crossing the line toward electronic crime (E-crime):

- Now the attacker attempts to gain access to the system. Once the attacker is able to access a user account, they will attempt to get an administrator or "root" access. Administrative access is required to run all services and access all files of the system.

Step 4: Capturing the network:

- At this stage, the attacker tries to own the network. The attacker can hack the internal network quickly and easily by compromising low-priority target systems. The next step is to remove any evidence of the attack. Now using some "hacking tools", the attacker replaces the existing files and services with Trojan files and services that have a password.

Step 5: Grab the data:

- At this stage, after capturing the network, an attacker can steal confidential data, credit card information, change webpages, alter processes and launch attacks.

Step 6: Covering attacks:

- This is the last step in any cyberattack. Attackers cover themselves and misuse the system without being-detected. The attacker can remain undetected for long periods.

3.2 PROXY SERVERS AND ANONYMIZERS

3.2.1 Proxy Server

- Proxy server is a computer on a network that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources.
- For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server. It makes the original IP address of the node remain hidden while accessing data from that server.
- In some organizations, there may be a possibility that the information like password or some confidential data can be hacked in case the IP address is accessible easily. To prevent such kind of misuse of Data Proxy servers are set up to prevent tracking of original IP addresses instead data is shown to come from a different IP address.

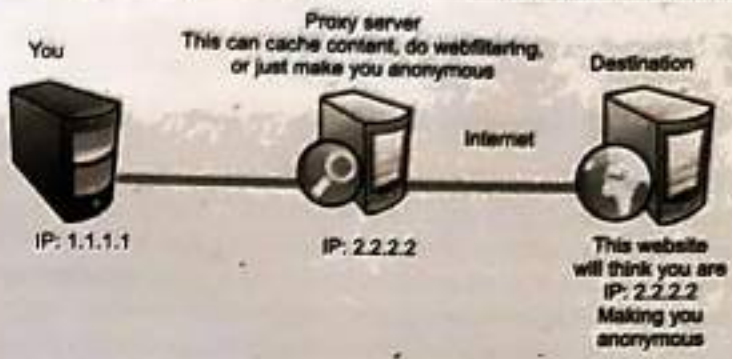

Fig. 3.1: Proxy Server

- The attacker can also connect to the proxy server to access services provided by the target system. The proxy server performs the requests on behalf of the attacker machine. The target machines on the network can see that the request is coming from a proxy machine but cannot see the actual identity of the attacker machine. Generally, attackers use proxies to hide their identity.

Purposes:

- A Proxy Server has the following purposes:
  1. It hides the company servers or systems.
  2. It caches the frequently accessed web pages to improve the response time for the clients accessing those web pages.
  3. It filters inappropriate advertisements or for censoring illegal websites.
  4. It can be used to connect many computers in a LAN or WAN, exposing only one public IP address to the Internet.
  5. It can be used for sorting the traffic going in and out of the network.

3.2.2 Anonymizer

- Anonymizer is an anonymous proxy. It allows the user to browse the Internet anonymously. An anonymizer accesses the Internet on behalf of users, protecting personal information by hiding the source computer's identifying information.
- When an attacker uses an anonymizer, the proxy removes all the identifying information to protect the privacy of the user.

3.3 PHISHING

- 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.
- "Phishing" refers to an attack using mail programs to cheat Internet users and disclosing confidential information that can be then utilized for illegal purposes.

- Phishing is a type of cybersecurity threat. It targets users directly through email, text or direct messages. During one of these scams, the attacker will create a trusted contact to steal data like ID, password, account numbers, and credit card information.

Example:

- An individual receives an email from his bank. The email appears to be sent from that bank because the bank logo is embedded in the email. The email explains there is an urgent issue with the individual's account, instructing him to click on a link to solve the issue right now. Once he clicks on the link, he is brought to a webpage which is a copy of that bank webpage. Unknowingly, he enters his username and password on the website. Hence, the scammer has collected his banking credentials.
- In this scheme, the scammer has collected the individual's banking credentials. Further, by visiting the fraudulent banking site, the individual may have unknowingly downloaded malware to his computer, which will be tracking and collecting other data and sending it to the scammer.

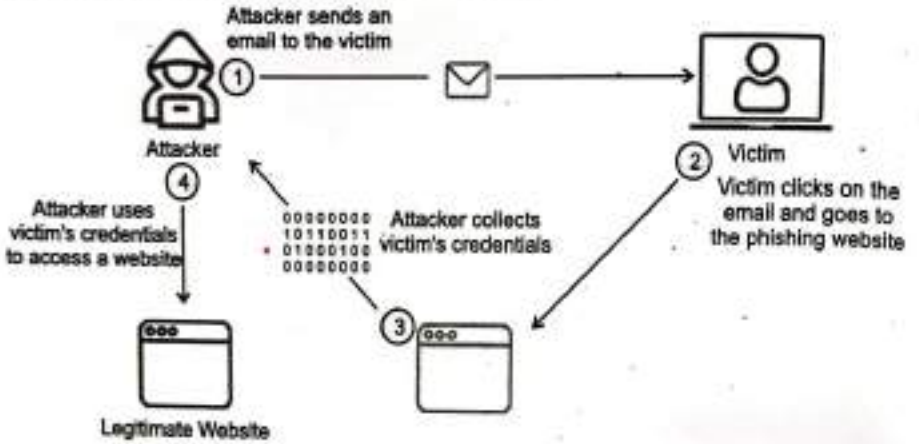

Fig. 3.2: A Phishing Attack

3.3.1 How does Phishing Work?

- Phishers work in the following way:
  1. **Planning :** Criminals, usually called as phishers, decide the target and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
  2. **Setup :** Once phishers know who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.
  3. **Attack :** This is the step people are most familiar with the phisher sends a 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.

3.3.2 Phishing Techniques

1. **Email Phishing:**
- Email phishing is the most common type of phishing, and it has been in use since the 1990s. Hackers send these emails to any and all email addresses they can obtain.
- In Email phishing, an attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam.

2. **Spear Phishing:**
- Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.

3. **Smishing:**
- Smishing is an attack that uses text messaging or short message service (SMS) to get your attention. A message that comes into your cell phone through SMS that contains a link to click or a phone number to call could result in a smishing attack.

4. **Whaling:**
- A whaling email might state that the company is getting litigated and you need to click on the link to get more information.
- The link takes you to a page where you are asked to enter critical data about the company such as tax ID and bank account numbers.

5. **Vishing:**
- This attack is accomplished through a voice call. Hence the "v" rather than the "ph" in the name.
- An example of vishing attack is the caller who claims to be from Microsoft and says you have a virus on your computer. You turn over credit card details to get a better version of anti-virus software installed on your computer. The attacker now has your credit card information and you have likely installed malware on your computer.

3.4 PASSWORD CRACKING

- Passwords are like a key to get an entry into computerized systems. Password cracking is a process of recovering passwords from data that has been stored in or transmitted by a computer system in a scrambled form.
- A common approach, which is called a Brute-force attack, is used repeatedly to guess the password and to check it against an available cryptographic hash of 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 passwords that can be for easily cracks.
  3. To gain unauthorized access to a system.
- The attacker also tries to crack passwords manually, so that they attempts to login with different passwords.
- The attacker cracks password in 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.

3.4.1 Examples of Guessable Passwords

- 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.
  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, and spiritual gurus) by the user.
  9. Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.
- An attacker can also create a script file (a program) which will be executed to try each password in a list. This method is time-consuming and not usually effective.
- Passwords are stored in a database. When a user attempts to login, then the password is verified with the database. To ensure confidentiality of passwords, the password is stored in encrypted format, not in a clear text format.

3.4.2 Classification of Password Cracking Attacks

- Password cracking attacks can be classified under three categories as follows:
  1. **Active Online Attacks:** Attacker performs password cracking by directly communicating with the victim machine.

Examples:

- **Dictionary Attack:** A dictionary file is loaded into the cracking application that runs against user accounts. Attacker tries all dictionary words before trying Brute force attack.
- **Brute Forcing Attack:** The program tries every combination of characters until the password is broken.
- **Rule-based Attack:** This attack is used when the attacker gets some information about the password.
- **Password Guessing:** The attacker creates a list of all possible passwords from the information collected through social engineering or any other way and tries them manually on the victim's machine to crack the password.
- **Hash Injection and Phishing:** Attacker injects a compromised hash into a local session and uses the hash to validate the network resources.
- **Trojan/Spyware/Keyloggers:** Attacker installs Trojan/Spyware/Keyloggers on victim's machine to collect victim's usernames and passwords. Then it runs in the background and sends back all user credentials to the attacker.

2. **Passive Online Attacks:** Attacker performs password cracking without communicating with the authorizing party.

Examples:

- **Wire Sniffing:** Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic.
- **Man-in-the-Middle:** Attacker acquires access to the communication channels between victim and server to extract the information.
- **Replay:** Packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access.

3. **Offline Attack:** Attacker copies the target's password file and then tries to crack passwords in his own system at different locations.

Examples:

- **Pre-Computed Hashes (Rainbow Table):** A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash value.
- **Distributed Network:** Recovering passwords from hashes or password protected files using the unused processing power of machines across the network to decrypt passwords.

4. **Non-Electronic Attacks:** Attackers need not possess technical knowledge to crack passwords, hence known as non-technical attacks.

Examples:

- **Shoulder Surfing:** Looking at either the user's keyboard or screen while he/she is logging in.
- **Social Engineering:** Convincing people to reveal passwords.
- **Dumpster Diving:** Searching for sensitive information at the user's trash bins, printer trash bins, and user desks for sticky notes.

3.4.3 Password Guidelines:

- Password guidelines are as follows:

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.
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 a couple of days, if these E-Mail accounts have been accessed from public Internet facilities such as cybercafés/hotels/libraries.
7. Passwords should not be stored under mobile phones, 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.

3.5 KEYLOGGERS AND SPYWARES

3.5.1 Keyloggeres

- Keystroke logging, often referred to as Keylogging or Keyboard capturing.
- Keyloggers are software programs or hardware devices that track/record the keyboard activities.
- Keyloggers are a form of spyware where users are unaware their actions are being tracked.
- Keyloggers give hackers access to your personal data like the passwords and credit card numbers you type, the web pages you visit – all by logging your keyboard strokes. The software is installed on the computer, and records everything you type. Then the records are stored into a log file, and the log file is sent to a server, where cybercriminals wait to make use of all this sensitive information.

Methods of Keyloggers:

- Most sources describes keyloggers as software programs. But it is not necessary for keyloggers to be software every time, it can be hardware devices some times.

- Following are methods of **Keyloggers:**

1. **Software Keyloggers:**

- These are software programs which are located between the operating system 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 and can obtain the required information about the victim very easily.
- A keylogger is a dynamic link library file (.dll file) or an Executable file(.exe file).

2. **Hardware Keyloggers:**

- These are small hardware devices. To install these, physical access to the computer system is required. 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 PINs. The hardware device looks like an integrated part of such systems; hence, bank customers are unaware of this.

3. **Antikeylogger:**

- An antikeylogger is a type of software specifically designed to detect keystroke logger software. It will also delete or disable hidden keystroke logger software on a computer.

Advantages of using antikeylogger are as follows:

- Firewalls cannot detect; but, antikeyloggers can detect keylogger installed on the system.
- This software does not require regular updates, as compared to antivirus which require regular updates for effective working.
- Prevents Internet banking frauds, ID theft etc.
- It secures E-Mail and instant messaging/chatting.

3.5.2 Spywares

- Spyware is a type of virus that is installed on computers which collects information about users without their knowledge. It is secretly installed on the user's personal computer and it is hidden from the user. Sometimes, like keyloggers, Spywares are installed on shared, corporate or public computers.
- Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited, and sometimes, send this data to advertisers or marketing data firms. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time.

- To overcome the appearance of Spywares, anti-Spyware software is available in the market. Installation of anti-Spyware has become a common element nowadays from a computer security practices perspective.

Guidelines to prevent Spyware:

- Following are some tips to prevent spyware:
  - Download software from trusted sources only.
  - Read all disclosures when installing software.
  - Avoid interactions with pop-up ads.
  - Do not open email attachments or click on links from unknown senders.
  - Use only trusted antivirus software and reputable spyware tools.
  - Enable two-factor authentication (2FA) whenever possible.

Types of Spyware:

Fig. 3.3: Types of Spyware

1. **Adware:**

- Adware is a type of spyware that automatically downloads to track your browsing data with the intent of predicting the products and services you're interested in. It will then display advertisements for those products or services to coax you into clicking and purchasing.

2. **Trojans:**

- Trojans are malicious software programs that mask themselves as a legitimate program (the Trojan horse in Greek mythology). When you're a victim of a Trojan attack, you will unknowingly install a file that is masked as a program, only for it to delete your files, encrypt your data for ransom, or give your personal information to others with the intent of identity theft.

3. **Keyloggers:**

- Keyloggers are used to steal personal information, login credentials, and sensitive data by tracking the keystrokes of the keyboard.

4. **Password stealers:**

- Password stealers are applications designed to collect passwords from infected computers, ranging from email, banking account, or social media accounts.

5. **Mobile spyware:**

- This type of spyware is specific to our mobile devices. It can infect them through an SMS or MMS message, and usually doesn't require any user interaction to initiate. When your mobile is infected, the phone's camera and microphone will be enabled to spy on your activity, record your phone calls, track your browsing activity, and even monitor your keystrokes.

3.6 VIRUS AND WORMS

Virus:

- A computer virus is a malicious piece of program that grows by attaching itself to a host document that will generally be an executable file. Viruses spread themselves, without the knowledge or permission of the users.
- A computer virus passes from computer to computer in a similar manner as a biological virus passed from person to person. Viruses may also contain malicious instructions that may damage the system.
- Viruses can take some typical actions:
  1. Display a message to prompt an action which may set off the virus.
  2. Delete files inside the system into which viruses enter.
  3. Scramble data on a hard disk.
  4. Cause irregular or unstable screen behavior.
  5. Halt the computer system.
  6. Just replicate themselves to propagate further harm.
- In Fig. 3.4, Steps 1 to 3 explain how viruses spread (a) through the Internet, (b) through a stand-alone computer system.
- Computer virus has the ability to copy itself and infect the system. A true virus can only spread from one system to another when a user sends it over the Internet or a network, or carries it on a removable media such as CD, DVD or USB drives.
- Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage.

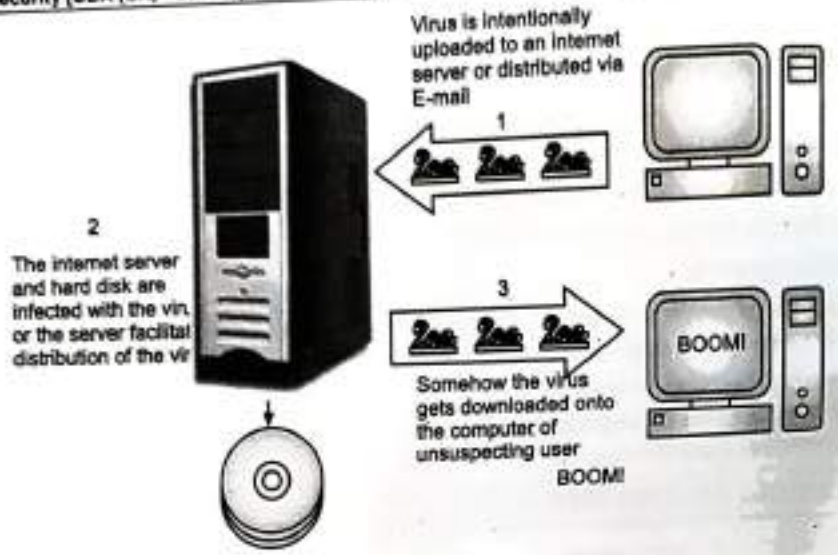

Fig. 3.4 (a): Virus spreads through internet

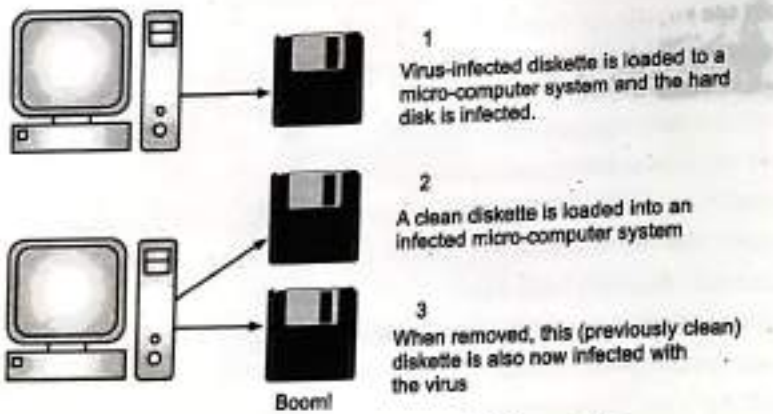

Fig 3.4 (b): Virus spreads through stand-alone system

Worms:

- A computer worm is also like a virus but a worm does not need a host program, it is an independent program. A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a program that appears to be harmless but hides malicious functions.
- Worms are similar to viruses but they do not modify the program. It replicates itself more and more to slow down the computer system. Worms can be controlled remotely. The main objective of worms is to trouble the system resources.

Types of Viruses:

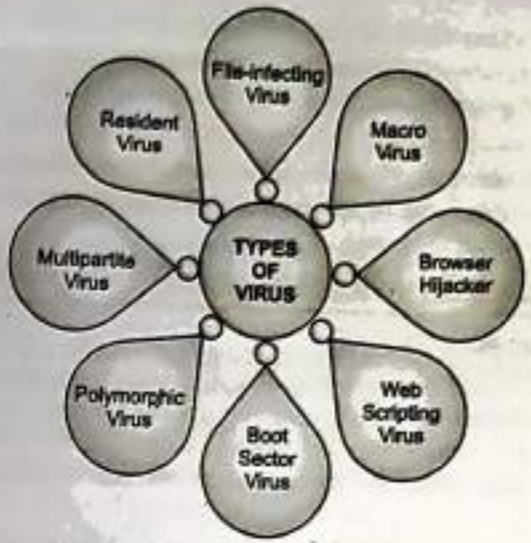

Fig. 3.5: Types of Viruses

- Following are some common types of viruses:

1. **File-infecting Virus:**
- This virus attached itself to an executable file. It is also called a parasitic virus which typically infects files with .exe or .com extensions.
2. **Macro Virus:**
- These viruses are triggered when a program capable of executing a macro is run. For example, macro viruses can be contained in Microsoft Word or Excel files.
3. **Browser Hijacker:**
- This virus targets and alters your browser setting. It is often called a browser redirect virus because it redirects your browser to other malicious websites.
4. **Web Scripting Virus:**
- This virus inserts links that can install malicious software on your device. This virus can steal cookies and post the information to the infected website.
5. **Boot Sector Virus:**
- It infects the boot sector of the system and executes every time the system is booted. Today, these viruses are found distributed in forms of physical media such as external hard drives or USB.
6. **Polymorphic Virus:**
- This virus has the capability to avoid anti-virus programs since it can change codes every time an infected file is performed.

7. **Resident Virus:**

- A resident virus stores itself on your computer's memory which allows it to infect files on your computer. This virus can interfere with your operating system and corrupts files and programs.

8. **Multipartite Virus:**

- A type of virus that is very infectious and can easily spread on your computer system. It can infect multiple parts of a system including memory, files, and boot sector which makes it difficult to contain.

3.7 TROJAN HORSES AND BACKDOORS

3.7.1 Trojan Horses

- A Trojan horse is a program downloaded and installed on a computer that appears harmless, but malicious or harmful code is contained inside it. When Trojan attacks, unexpected changes to computer settings and unusual activity happen, even when the computer is idle. These are strong indications that a Trojan is residing on a computer.
- Typically, the Trojan horse is hidden in an innocent-looking email attachment or in a free download. When the user clicks on the email attachment or free download program, the malware that is hidden inside, is transferred to the user's computer. Then the malicious code can execute whatever task the attacker designed it to carry out.
- The term Trojan horse comes from Greek mythology about the Trojan War. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. It cannot be removed by third party software or antiviruses. Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive.

Fig. 3.6: Trojan Virus

Examples:

- 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 password and credit card numbers.
  8. They display fake website links, and porno sites.
  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.

3.7.2 Backdoors

- A backdoor is a method that allows hackers to remotely access your device without your permission or knowledge. For example, a computer usually requires a username and password. During a backdoor attack, a hacker will bypass the login portal, thus gaining access to the computer's files without entering the username and password.
- In a backdoor, attackers use a vulnerability in a computer or network. Hackers can create a backdoor on a computer or network using malware. Default passwords (or other default credentials) can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.
- A backdoor works in the background and hides from the user. It is very similar to a virus and, therefore, is quite difficult to detect and completely disable.

Functions of Backdoor:

- Following are some functions of backdoor:
  1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands, change system settings, alter the Windows registry, run, control and terminate applications; install malicious software.
  2. It allows an attacker to control computer hardware devices, modify settings, shutdown or restart a computer without permission.
  3. It steals personal information, valuable documents, passwords, 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, and uploads it to a remote computer.

How to keep devices safe from backdoors virus attacks?

- Following are steps to keep devices safe from backdoors virus attacks:
  1. Always use advanced antivirus software that can detect and prevent a wide range of malware.
  2. Always download from official websites, avoid pirate sites.
  3. Use a Firewall.
  4. Use a Password Manager
  5. Stay away from suspect websites/web links.

3.9 STEGANOGRAPHY

- When a file, message, image, or video is concealed (hidden) within another file, message, image, or video that is called Steganography.
- The word steganography comes from Greek word *steganographia*, which combines the words stegano, meaning "covered or concealed", and graphia meaning "writing".
- Steganography is the practice of hiding a secret message inside of something that is not secret. For example, embedding a secret piece of text inside of a picture or hiding a secret message or script inside of a Word or Excel document.
- Steganography can involve the use of any medium to hide messages. It is not cryptography, because it does not involve hiding data using a key. Instead, it is a form of data hiding and can be executed in clever ways. Where cryptography is a science that largely enables privacy, steganography is a practice that enables secrecy.
- 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 helps 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.

Steganography Types:

- Steganography can be divided into five types depending on the nature of the cover object (actual object in which secret data is embedded) as follows:
  1. Text Steganography
  2. Image Steganography
  3. Video Steganography

4. Audio Steganography
5. Network Steganography

- Let's see each of these in detail.

1. Text/Document Steganography:

- This includes focusing on changing the characteristics of documents. A few ways this is done are:
  - By adding white space and tabs to the end of the lines of documents to hide information in plain text.
  - Using a widely available cover source like a book or newspaper and using a code comprising of a combination of numbers, letters, or line number. This way the information inside the cover source will not tell the hidden message and the only way to decode is to gain the key.
  - Another widely used technique for steganography is the use of background color and font. It is used in Microsoft Word documents.

2. Image Steganography:

- Digital images are used widely and since they are available in various formats the algorithm used differ completely.
- Some common types are: Least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter.

3. Video Steganography:

- In this, a video file will be embedded with supplementary data that will hide the secret message.
- Some widely known approaches are: Least Significant Bit Insertion,Real-time Video Steganography.

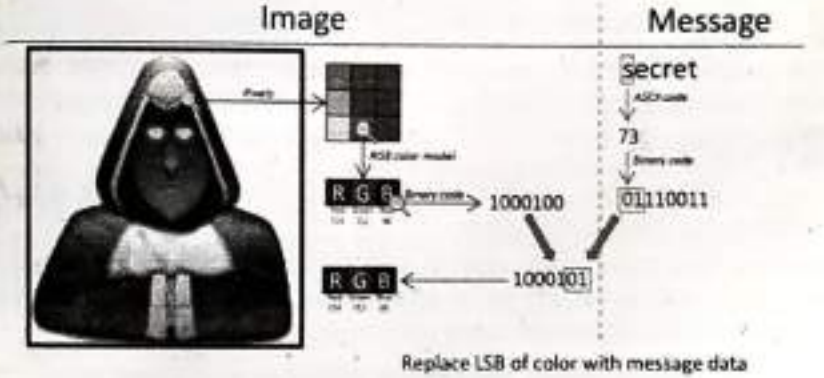

Fig. 3.7: Stegnography

4. Audio Steganography:

- Inserting a secret message in audio is most difficult as the human brain has a wide range of auditory capacity. A few methods used are: Parity coding, LSB coding, Phase coding, Echo hiding.

5. Network Steganography:

- It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

Examples:

1. Playing an audio track backward to expose a hidden message
2. Playing a video at a faster frame rate to show a hidden message.
3. Inserting a message in the red, green, or blue channel of an RGB image.
4. Encrypting a message or image within a photo through the addition of noise or sound.
5. Hiding information with the file header or metadata.

3.9.1 Steganalysis

- Steganalysis is the opposite procedure of steganography. Steganography tries to hide messages while steganalysis tries to detect their existence to retrieve the embedded data.
- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files.
- The main aim of steganography is for a sender to transfer a plaintext to a receiver in such a way that only the receiver can extract the plaintext because only the receiver knows the hidden plaintext exists in the first place & how to look for it.

3.10 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 unavailable to its users.

3.10.1 DoS Attacks

- A DoS attack is an attack, where a computer sends a massive amount of traffic to a victim's computer and shuts it down.
- DoS attack is an online attack which is used to make the website unavailable for its users. This attack makes the server of a website down which is connected to the internet by sending a large number of traffic to it.
- The attacker typically targets sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks. Buffer overflow technique is employed to commit this kind of criminal attack known as spoofing.

- 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 a response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the valid requests and breaks down.

Signs of DoS Attacks:

- Following are the symptoms of DoS attacks:
  1. Unusually slow network performance while 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 E-mail bomb).

Functions:

- A DoS attack may do the following:
  1. Flood a network with 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 time.
2. **Logic attacks:** 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 the network.
4. **Unintentional DoS attack:** A website ends up due to a sudden enormous spike in popularity.

Types or Levels of DoS Attacks:

1. **Flood attack:** An attacker sends a number of packets by using the "ping" command to the victim, which results in more traffic than the victim can handle.
2. **Ping of death attack:** Sending oversized Internet Control Message Protocol (ICMP) packets, using networked computers to send error messages indicating requested service is not available or a host or router could not be reached to the victim.
3. **SYN attack:** Attacker uses the TCP connection sequence to make the victim's network unavailable. The attacker sends SYN requests to the victim's network which then responds with a SYN-ACK response. The sender is then supposed to respond with an ACK response but instead, the attacker doesn't respond (or uses a spoofed source IP address to send SYN requests instead). Every request that goes unanswered takes up network resources until no devices can make a connection.

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.

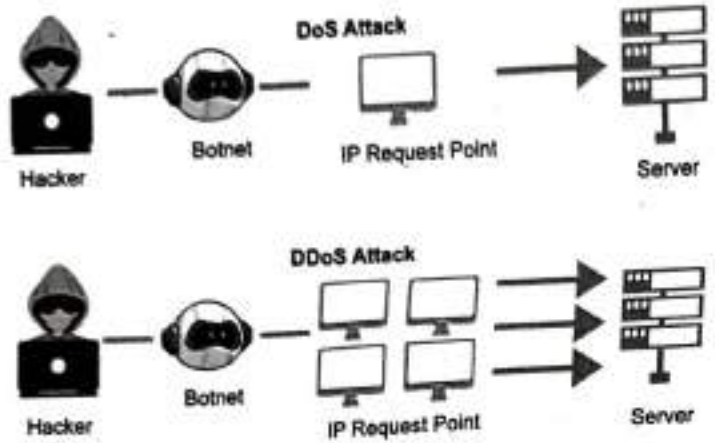

Fig. 3.8: DoS Vs DDoS Attacks

3.10.2 DDoS Attacks

- In this attack, DoS attacks are done from many different locations using many systems. The Victim PC is loaded from the packet of data sent from multiple locations. DDoS attacks are faster than DoS Attack. It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
- **Botnet** is the popular medium to launch DoS/DDoS attacks.

Types of DDoS Attacks are:

1. **Volumetric Attacks:** Volumetric attacks occur when the attacker floods network devices with ICMP echo requests until there is no more bandwidth available.
2. **Fragmentation Attacks:** Attacker sends manipulated packets to a network so that once the network tries to reassemble them, they can't be reassembled. This is because the packets have more packet header information than is permitted. The end result is packet headers which are too large to reassemble in bulk.
3. **Application Layer Attacks:** In this attack the target applications or servers attempt to use up resources by creating as many processes and transactions possible.

How to Protect from DoS/DDoS Attacks?

- Following are steps to protect from DoS/DDoS Attacks:
  1. Implement router filters.
  2. Such filters install patches to guard against TCP SYN flooding.

3. Disable any unused or inessential network service.
4. Observe your system's performance and establish baselines for ordinary activity
5. Routinely examine your physical security with regard to your current needs.
6. Use Tripwire or a similar tool to detect changes in configuration.
7. Establish and maintain regular backup schedules.
8. Establish and maintain appropriate password policies.

3.11 SQL INJECTION

- SQL, or Structured Query Language, is the standard language for interacting with relational databases. In apps and other types of programming, databases are used to store user data such as usernames and passwords. Databases are also often the most effective, secure solution for storing other types of data from public blog posts and comments to confidential bank account numbers.
- SQL statements often use arguments to pass data from users into a secured database or vice versa. Unless the values in these user-supplied SQL arguments are secured, attackers can use the places where your app communicates with a database with a SQL argument to gain access to confidential information and other secured areas.
- Attackers target the SQL servers - common database servers used by many organizations to store confidential data. The main objective behind the 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 to make a system execute a command shell or other arbitrary commands.
- SQL Injection(SQLi) allows attackers to add, edit, and delete notes from the database.
- SQL Injection is a security defect on a database that can impact web applications and websites that use SQL databases like SQL Server, MySQL, and Oracle.
- There are several types of SQL Injection attacks: in-band SQLi (using database errors or UNION commands), blind SQLi, and out-of-band SQLi.

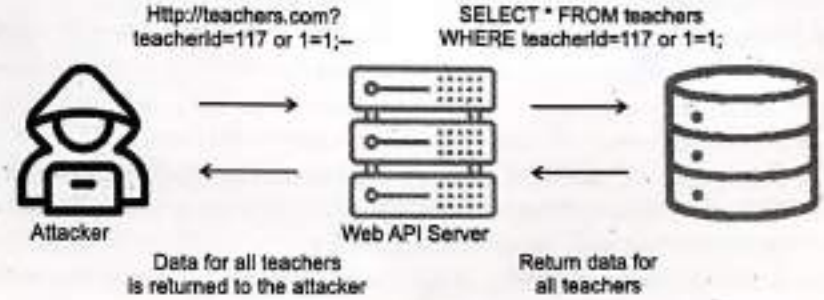

Fig. 3.9: Example of SQL injection

Methods to prevent SQL injection attack:

- Following main methods can be used to prevent SQL injection attack:

1. **Use of Prepared Statements/queries:** Parameterized queries are a means of pre. compiling an SQL statement. You can supply theses parameters in order for the statement to be executed. This method makes it possible for the database to recognize the code and distinguish it from input data.
2. **Escape all user supplied input:** Always use character-escaping functions for user. supplied input provided by each database management system (DBMS). This is done to make sure the DBMS never confuses it with the SQL statement provided by the developer.
3. **Use of Stored Procedures in databases:** Stored procedures (SP) require the developer to group one or more SQL statements into a logical unit to create an execution plan. Subsequent executions allow statements to be automatically parameterized. It is a type of code that can be stored for later and used many times.
4. **Apply Least Privilege:** it's better to enforce least privilege on the database to defend the application against SQL injection. Ensure that each application has its own database credentials and that those credentials have the minimum rights the application needs.
5. **Isolate database server with web server:** This provides added layers of protection that shield us from the negative effects of bad code, human error, or a security vulnerability

Summary

- Different forms of attacks are Initial uncovering, investigation, gain access to the system, capturing the network, steal the data, and covering tracks.
- Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server.
- An anonymizer accesses the Internet on behalf of user's protecting personal information by hiding the source computer's identifying information.
- Phishing refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes.
- Password cracking is a process of recovering passwords from data that has been stored in or transmitted by a computer system in a scrambled form.
- In Active Online Attacks, password cracking is performed by directly communicating with the victim machine. In Passive Online Attacks, password cracking is performed without communicating with the authorizing party.
- Keyloggers are software programs or hardware devices that track the keyboard activities.

- An antikeylogger is a type of software specifically designed to detect keystroke logger software.
- Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.
- A computer virus is a malicious piece of program that propagates typically by attaching itself to a host document that will generally be an executable file.
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities.
- A Trojan horse is a program downloaded and installed on a computer that appears harmless, but malicious or harmful code is contained inside it.
- A backdoor is any method that allows hackers to remotely access your device without your permission or knowledge.
- In Steganography, a file, message, image, or video is concealed (hide) within another file, message, image, or video. Steganalysis is the opposite procedure of steganography.
- A DOS attack is an attack, where a computer sends massive amount of traffic to a victim's computer and shuts it down. DDoS attacks are done from many different locations using many systems.
- 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.

Check Your Understanding

1. Which of the following is not an example of physical data leakage?
   (a) Phishing (b) Dumpster diving
   (c) Shoulder surfing (d) Printers and photocopiers
2. A computer virus may be used to
   (a) Corrupt data in your computer
   (b) Log the user's keystrokes
   (c) Access private data like user id and passwords
   (d) All of the above
3. Which of the following is not an example of malware?
   (a) Virus (b) Worm
   (c) Browser (d) Trojan horse
4. Which type of the following malware does not replicate or clone them self's through infection?
   (a) Rootkits (b) Trojans
   (c) Worms (d) Viruses

5. Which of the following statements is true about the Trojans?
   (a) Trojans perform tasks for which they are designed or programmed.
   (b) Trojans replicates them self's or clone them self's through an infections.
   (c) Trojans do nothing harmful to the user's computer systems.
   (d) None of the above
6. Which of the following is a type of independent malicious program that never required any host program?
   (a) Trojan Horse (b) Worm
   (c) Trap Door (d) Virus
7. _____ is a code injecting method used for attacking the database of a system / website.
   (a) HTML injection (b) SQL Injection
   (c) Malicious code injection (d) XML Injection
8. Which method of hacking will record all your keystrokes?
   (a) Keyhijacking (b) Keyjacking
   (c) Keylogging (d) Keyboard monitoring
9. _____ works in background and steals sensitive data.
   (a) Virus (b) Shareware
   (c) Trojan (d) Adware
10. Spyware collects user's personal data & spreads it to_____ data-firms, or its creator.
   (a) Advertisers (b) Dark-market
   (c) Antivirus company (d) Share market

ANSWERS

1. (a)	2. (d)	3. (c)	4. (b)	5. (a)	6. (b)	7. (b)
8. (c)	9. (c)	10. (a)				

Practice Questions

Q.I Answer the following questions in short.

1. Define a denial-of-service (DoS) attack.
2. What types of resources are targeted by such DoS attacks?
3. What is meant by Trojan horse?
4. What is Phishing?
5. Distinguish between Trojan and Logic Bomb.
6. What is a distributed denial-of-service attack (DDoS)?
7. Define SQL Injection.

8. What is the difference between Proxy server and an anonymizer?
9. What is the difference between virus and worm?
10. What is the difference between Trojan Horse and Backdoor?
11. What is Steganography?
12. Write the purpose of password cracking.
13. Define spyware.

Q.II Answer the following questions.

1. Define virus. Discuss the types of viruses.
2. State the difference between virus and worm.
3. Explain the different phases during the attack on the network.
4. What are the different ways of password cracking?
5. How can be keyloggers used to commit a cybercrime?
6. What is SQL injection and what are the different countermeasures to prevent the attack?
7. What is identity theft? Explain with example.
8. What is proxy server? Also write the purposes of proxy server?
9. Explain how the Phishing works?
10. What is Antikeylogger? Write its advantages.
11. Discuss the functions of backdoor.
12. Explain DoS attack in brief. What are the different types of DoS attack?
13. Discuss how to Protect from DoS/DDoS Attacks.

Q.III Define the terms.

1. Proxy server
2. Anonymizer
3. Rainbow table
4. Keyloggers
5. Steganalysis

❖❖❖

4... Cybercrimes and Cyber Security: The Legal Perspectives

Learning Objectives...

- To understand Cybercrime and the Legal Landscape around the World.
- To learn Why Do We Need Cyberlaws: The Indian Context.
- To know about The Indian IT Act.
- To study Challenges to Indian Law and Cybercrime Scenario in India.
- To know the concept of Digital Signatures and the Indian IT Act.
- To know the concept of Digital Signatures and the Indian IT Act, Cybercrime and Punishment.
- To learn Amendments to the Indian IT Act, Cybercrime and Punishment.
- To learn Cyberlaw, Technology and Students: Indian Scenario.

4.1 INTRODUCTION

- All forms of cybercrimes are rapidly increasing day by day. The cybercrime is the largest illegal industry. In this chapter we focus on knowledge of cyber laws is required for people who may directly or indirectly interact with networked services either over internet or other networks of businesses and enterprises of types - ecommerce, banks, stock brokers, etc.
- The people who are involved in social networking sites must understand the meaning of the term digital evidence that give in that the Indian information Technology Act [ITA 2000] and also the updating takes in IT act in 2008. In ITA2000 there is a clear mention about "special provisions as to 'evidence relating to electronic record' and 'admissibility' of electronic records."
- While maintaining focus on the Indian ITA 2000 and subsequent amendments in year 2008, we have focus on the Indian ITA 2000 (previously known as the IT Bill) and its recent amendments known as the ITA 2008 (Amendments to the IT Ace that came toward the end of year 2008).

- Globally the cybercrime is divided in two categories:
  1. **Cybercrime in a restrictive sense (computer crime):** It means any illegal behavior that is carried out by means of electronic methods targeting the security of computer systems and the data or information processed by them. This can be considered as a simple or narrow definition of the term cybercrime.
  2. **Cybercrime in a general sense (computer-related crime):** It is referred to any illegal behavior that is related to computer system or network, offering or distributing data by means of a computer system or network. This can be a broader definition of the term cybercrime.
- The more concrete example of cybercrime are unauthorized access to computer, causing damage to computer data or programs, an access of computer sabotage, doing unauthorized interception of communications, carrying out computer espionage.
- The law consider computer trespass to be a crime when there is unauthorized access of information. **Computer trespassing** is term that consider a person is guilty of computer trespass, if the person, without authorization, intentionally gains access to a computer system or electronic database.

4.2 CYBERCRIME AND THE LEGAL LANDSCAPE AROUND THE WORLD

- Crime or an Offense is "a legal wrong that can be followed by criminal proceedings which may result into punishment." In this point we discuss the world scenario considering the countries like: the US, Europe, Canada. Asia-Pacific and Africa.

4.2.1 A Broad View on Cyber Crime Law Scenario in the Asia-Pacific Region

- When we consider challenges for handling cybercrime in the Asia-Pacific region, we come to know that the challenges exist mainly due to the general lack of reach of ICT, awareness of information security issues. There are only few countries of the Asia-Pacific region have appropriate legal and regulatory frameworks to meet these challenges. The awareness is increasing and where legislation may be adequate.
- Now we consider the Australian Cybercrime Act 2001. This Cybercrime Act 2001 come into effect in Australia in April 2002. This Act introduces the following new offenses to the Criminal Code Act 1995.
  1. **This section offenses under Division 477 are as bellow:**
     - **Section 477.1:** Unauthorized access, modification or impairment with intent to commit a serious offense.
     - **Section 477.2:** Unauthorized modification of data to cause impairment.
     - **Section 477.3:** Unauthorized impairment of electronic communication.

2. **The other offenses under Division 478 are as bellow:**
   - **Section 478.1:** Unauthorized access to, or modification of, restricted data.
   - **Section 478.2:** Unauthorized impairment of data in a computer disk, etc.
   - **Section 478.3:** Possession or control of data with intent to commit a computer offense.
   - **Section 478.4:** Producing, supplying or obtaining data with intent to commit a computer offense.

- Under the Australian Cybercrime Act, new powers granted for law enforcement which include:
  1. The power to remove "a thing" to another place for the purpose of examination.
  2. The power to "operate electronic equipment" at the warrant premises in order to access data which may contain evidentiary material.
  3. The power to require a person "to provide any information or assistance".
  4. The power to require a "person with knowledge of a computer or a computer system to assist access," etc.

4.2.2 Online Safety and Cybercrime Laws: Detail Perspective on the Current Asia-Pacific Scenario

- The extent and nature of Internet security, safety and privacy legislation in the Asia-Pacific region varies widely. The International Centre for Missing and Exploited Children (ICMEC) has developed authentic model to deal with child pornography crime. This model has been adopted as the benchmark legislation for the online child safety and computer security.
- There are various regional norms, such as the Asia-Pacific Economic Co-operation (APEC) Privacy Framework and the EU's Data Protection Directive, yet an international consensus on the best approach to data protection regulation has not reached.
- Following are the Principle of APEC privacy framework:
  1. Preventing harm
  2. Integrity of personal information
  3. Notice
  4. Security safeguards
  5. Collection limitations
  6. Access and correction
  7. Uses of personal information
  8. Accountability
  9. Choice

Computer Security Law:

- The Singaporean, New Zealand, Australian, Taiwanese and Thai Governments have each enacted robust computer, security laws which cover most of the basics and computer-related offenses in the CoE's (Council of Europe's) Convention on Cybercrime.
- The computer security laws in China, Hong Kong, Japan and South Kore are moderately aligned with the Convention. The enacted law in Malaysia, the Philippines and Vietnam are moderately aligned, with Convention. Malaysia and the Philippines have enacted some computer security offenses; however, the focus of these offences appears to be unauthorized access.
- Although the ITA 2000 in India prohibit many of the activities that involves core offences under Convention. This IT Act merely provides for significant liability in damages.
- **Asia-Pacific region:** Alignment of the countries enacted legislation with regard to the benchmark legislation.

Table 4.1: The countries enacted legislation with regard to the benchmark legislation.

Favorable Alignment	Moderate Alignment	Weak Alignment
Australia	China	India
New Zealand	Hong Kong	Indonesia
Singapore	Japan	
Taiwan	Malaysia	
Thailand	Philippines	
	South Korea	
	Vietnam	

- This degree of alignment varies due to the range of convention offenses covered by the enacted legislation and the restrictive way in which some of the convention offenses are implemented. For example unauthorized access is obtained by use of a telephone line.

Data Privacy and Data Protection:

- Position on privacy laws also greatly varies in the Asia-Pacific region. The Microsoft given a Model of Privacy Bill that serve as the benchmark legislation in data privacy arena. Privacy mature organizations are regulated by prevailing privacy regulation in their respective countries.
- As per the Fair Information Practices (FIPS' organization must give a "privacy notice" before collecting the "Pers able Information (PII)". Privacy

notice is a statement made to a data subject that explains how the organization collect, use, retain and disclose individual information.

- The commonly known examples of PII are the Social Security Number (SSN) in USA, Personal Account Number (PAN) in India. The countries like Australia, Hong Kong, Japan, New Zealand has Moderate Alignment on privacy. Other countries have Weak Alignment.

Spam Laws:

- Spam is nothing but Unsolicited Bulk E-Mail (UBE) or Unsolicited Commercial E-Mail (UCE). The term "Unsolicited" means that there is no prior relationship between the parties concerned and the recipient. The Microsoft checklist conceive an "Opt-Out" anti-spam regime to address commercial electronic messages. This checklist mentions the transactional or relationship messages should be excluded from the scope of regulation. However effective anti-spam legislation needs to also include strong anti-address harvesting and dictionary attack measures.
- In resent time many countries from Asia-Pacific region have enactment of anti-spam legislation. There are now seven countries in this region that have enacted comprehensive anti-spam legislation: Japan, Australia, China, Hong Kong, New Zealand, Singapore and South Korea. Thailand, Philippines and Vietnam have enforced anti-spam measures that are less comprehensive. Legislatures in India, Indonesia and Taiwan are currently considering anti-spam legislative proposals.

Online Protection for Children:

- The International Centre for Missing and Exploited Children (ICMEC) defines the child pornography offences in Title 3 of the convention on cybercrime and the basic elements of this Model Child Pornography Legislation serve as the benchmark.
- Most of the countries developed online child safety law dealing in child pornography.
- Currently, the Indian, Philippine, Indonesian and Japanese legislatures are considering online child safety laws. ITA 2008 addresses child pornography. Most of these pending laws are subsumed in the broader proposals to enact computer security laws.

4.2.3 Anti-Spam Laws in Canada

- Under the Electronic Commerce Protection Act, to address Spam, feck websites and Spyware, the Canadian Government tabled anti-spam legislation Bill-c27 2009. Also raise the proposal of Personal Information Protection and Electronic Documents Act (PIPED Act) which covers online privacy related to E-Mail Marketing. This Act does not apply to the personal information of employees of these provincially regulated organizations or companies.
- The Personal Information Protection and Electronic Document (PIPED) Act is based on the following principals of Fair Information Practices. Which includes

Accountability, Identifying purposes, Consent, Limiting collection, Limiting use, disclosure and retention, Accuracy, Safeguards, individual access and Challenging compliance.

- There are two laws currently being discussed in Canadian legislative assemblies:
  1. **Senate Bill S-220:** Anti-Spam and Phishing attacks.
  2. **Parliamentary Bill C-27:** The bill was given by the government in April 2009, with private right of action, coordination between various enforcement agencies and civil remedies.

4.2.4 Cybercrime and Federal Laws in the US

- The Florida Computer Crimes Act covers unauthorized use of computing facilities is a crime. The Act provides definitions to the various terms related to computer crime: Offenses against intellectual property, offenses against computer equipment or supplies and offenses against computer users. This Act specifies the following type of crimes:
  1. Offenses against intellectual property.
  2. Offenses against computer equipment or supplies.
  3. Offenses against computer users.

4.2.5 The EU Legal Framework for Information Privacy to Prevent Cybercrime

- The European Union is an economic and political union of 27 member states.
- This union believes chat law is the enabler for cruse and confidence in the Information Society. There is a Data Protection Directive known as the EU directive which regulates the processing of personal data within the EU, which is the most important component of EU privacy and human rights law.
- In the EU, cybercrime law is based on the CoE's Convention on Cybercrime (Nov 2001), under the convention, member states are obliged to criminalize:
  1. Illegal access to computer system.
  2. Illegal interception of data to a computer system.
  3. Interfering with computer system and intentional interference with computer, without rights.

4.2.6 Cybercrime Legislation in the African Region

- There is a common agreement that the African regions are in dire need for legislation to fight cybercrime. There is rapid growth in Information Communication Technology (ICT). With this growth, the cybercrime has also become increases. Nigerian scam is known to us.

- Some members of the African Union like Mauritius, South Africa and Zambia, have adopted cybercrime legislation. In Botswana, cybercrime bill passed in Dec 2007 also Information and Communications Bill 2008 has been introduced in Gambia. South Africa has also got legislation governing "Spam" in July 2009.

4.3 WHY DO WE NEED CYBERLAWS: THE INDIAN CONTEXT

- Cyberlaw give legal recognition to all risks arising out of the usage of computers and its networks. Cyberlaw covers various aspects like intellectual property, data protection and privacy, freedom of expression and crimes committed using computers. The Indian Parliament passed its first cyberlaw, the ITA 2000. The main purpose is to provide the legal infrastructure for E-Commerce in India.
- The reasons for enactment of cyberlaws in India are:
  - India lacks in many aspects when it comes to newly developed Internet technology. 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. With grow of Internet, a new concept called Cyberterrorism came in picture. This Cyberterrorism activity effect on the social, ideological, religious, political or similar objectives. Keeping all these factors into consideration, Indian Parliament passed the Information Technology Bill on 17 May 2000, known as the ITA 2000.

4.4 THE INDIAN IT ACT

- The Indian IT Act was published in the year 2000 with the purpose of providing legal recognition for processes carried out by means of electronic data exchange and other means of electronic communication, generally referred to as E-commerce.
- Electronic communications involve the use of alternatives to paper-based methods of communication and storage of data, to facilitate electronic filing of documents with the government agencies. Another intention 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

Cybercrimes and Other Related Crimes Punishable under Indian Laws:

- Under Section 65 of Indian Copyright Act if any person who violate Copyright laws, he/she may get imprisonment which may extend to 2 years with fine.
- Sending pornographic or obscene E-Mails or electronic data are punishable under Section 67 of the IT Act. This punishable offence may extent to imprisonment for 5 years and with fine. Fine may extent to 1 lakh rupees. If same offence happen subsequently, punishment may extend to 10 years and also with fine which may extend to 2 lakh rupees.

- The ITA 2000 Sections 65, 66, 67, 71, 72, 73 and 74 in CHAPTER XI (Offences) of the are relevant to the cybercrime in legal context. The relevant sections from ITA200 as follows:

1. **Section 65: Tampering with computer source documents.**
   Whoever a person who are knowingly or intentionally destroy or alter any computer source code used for a computer, program me, computer system or computer network shall be punishable with imprisonment up to 3 years, or with fine which may extend up to 2 lakh rupees.
2. **Section 66: Computer-related offences.**
   This section of ITA focus on wrongful loss or damage to the pubic or any person destroys or deletes or alters any information residing in a computer or commits hacking shall be punished with imprisonment upto 3 years.
3. **Section 67: Punishment for publishing or transmitting obscene material in electronic form.**
   The publishing or transmitting any material which is lascivious or appeals to the prurient interest is a crime. For this Offence, shall be punished on first time with imprisonment which may extend to 3 years and with fine extend to 5 lakh rupees.
   If same offence happened subsequently, punishment may extend to 5 years' imprisonment and also with fine 10 lakh rupees.
4. **Section 71: Penalty for misrepresentation.**
   In this section, If any one makes any misrepresentation to, or suppresses any material fact from, the controller or the certifying authority for obtaining any license or Digital Signature Certificate, shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees or both.
5. **Section 72: Penalty for breach of confidentiality and privacy**
   This section provided, rules or regulations made for secure access to any electronic record, book register, correspondence, information, document or other material.
   If without the consent of the person discloses of electronic record, book, register, correspondence, information, document or other material to any other person shall be punished.
   The imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh rupees or both.
6. **Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars.**
   This section clearly mentions that other than certifying authority, no any person shall publish a Digital Signature Certificate or make it available to any other.

A person who contravenes the provisions of section 73 shall be punished with imprisonment extend to 2 years, or with fine1 lakh rupees, or with both.

7. **Section 74: Publication for fraudulent purpose.**

In this section any person knowingly creates a Digital Signature Certificate, publishes or it makes available for any fraudulent or illegal purpose shall be punished with imprisonment for a term which may extend to 2 years, or with fine 1 lakh rupees ,or with both.

- The significant changes brought out by the IT Amendment Bill 2008. New Sections added under 66A, 66B, 66C, 66D, 66E and 66F to cover new offences.

1. **Section 66A: Sending offensive messages.**

   Punishment: Imprisonment may extend to 3 years and fine.

2. **Section 66 B: Receiving a Stolen Computer Resource.**

   Punishment: Imprisonment for may extend to 3 years or fine of rupees 1 lakh or both.

3. **Section 66C: Identity Theft.**

   Punishment: Imprisonment for may extend to 3 years or fine of rupees 1 lakh or both.

4. **Section 66D: Cheating by personation.**

   Personation means to pretend to be somebody else.

   Punishment: Imprisonment for may extend to 3 years or fine of rupees 1 lakh or both.

5. **Section 66E: Violation of Privacy.**

   Punishment: Imprisonment for may extend to 3 years or fine of rupees 2 lakh or both.

6. **Section 66F: Cyber Terrorism.**

   Punishment: Imprisonment for may extend for a life or fine of rupees 5 lakh or both. Fine of Rs.10 lakh, for subsequent instance. Imprisonment reduced to 3 years for first instance and 5 years for subsequent instance.

- **New Section 67A: Introduced to cover material containing "sexually explicit act."**

  Punishment: On first conviction with imprisonment for a term which may extend to 5 years and with fine which may rupees 10 lakhs. On second conviction with imprisonment may extend to 7 years.

- **New Section 67B: Introduced to cover child explicit act or conduct.**

  Punishment: On first conviction with imprisonment for a term which may extend to 5 years and with fine which may rupees 10 lakhs. On second conviction with imprisonment may extend to 7 years.

- **New Section 67C: This provision will require intermediaries to preserve and retain certain records for some stated period.**

  Punishment: Imprisonment for a term which may extend to 3 years and also be liable to pay fine.

- **New Section 69A: Introduced to enable blocking of websites**

  Punishment: Imprisonment for 7 years also fine.

- **New Section 69B: Provides powers for monitoring and collecting traffic data, etc. If an Intermediary is not cooperative.**

  Punishment: Imprisonment for 3 years also fine.

- **New Section 70A:** Added to define National Nodal Agency for Critical Information Infrastructure Protection. Indian Computer Emergency Response Team (Cert India) appointed as the nodal agency for incident response.

4.4.1 Positive Aspects of the ITA 2000

1. Before making 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 document in electronic format.
2. As per the legal infrastructure provided by the ITA 2000, the perspective of the corporate sector, companies are able to carry out E-Commerce. Till the coming into effect of the Indian cyber law, the growth of E-Commerce was delay in our country basically because there was no legal infrastructure to regulate commercial transactions online.
3. Organizations will now be able to use digital signatures to carry out their transactions online.
4. If anyone illegally breaks into 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 to rupees 10,000,000.
5. ITA 2000 defined different types of cybercrimes. Prior to the coming into effect of the Indian Cyber Law Act, the corporate or organizations were helpless as there was no legal remedy for such issues. However, making of the ITA 2000, the scenario changed altogether.

4.4.2 Weak Areas of the ITA 2000

1. The ITA 2000 some cases is likely to cause a conflict of jurisdiction.
2. E-Commerce business is based on the system of domain names. The ITA 2000 yet does not any legal remedy to solve issues relating codomain names. Domain name owner rights and liabilities do not find or mention in the law.
3. The ITA 2000 does not support with issues concerning the protection of Intellectual Property Rights (IPR) in the context of the online environment.

4. The ITA 2000 does [illegible] crimes. Mainly include: Theft of internet [illegible] Cyber Fraud Cyber [illegible] Cyberstalking. Cyber defamation, Misuse of credit card number, chat room [illegible] Cyber Squatting (the practice of buying the right to own an internet address with [illegible] same name as that of a well-known organization in order to make money by [illegible] the address to that organization.)
5. The ITA 2000 has not treated vital issues pertaining to E-Commerce business [illegible] privacy and content regulation to name a few.
6. IT Act does not include anti-trust issues.
7. The ITA 2000 is not focus on regulation of Electronic Payments, and [illegible] applicability of IT Act to negotiable Instruments.
8. The major serious concern about the Indian Cyber law relates to its implementation [illegible]

4.5 CHALLENGES TO INDIAN LAW AND CYBERCRIME SCENARIO IN INDIA

- In the above point, weak areas of the Indian IT Act were discussed. In that context found that the Indian IT Law does not provide clear definition to the term cybercrime. The Indian Penal Code (IPC) does not use the cybercrime term even after amendment by the ITA 2000. On the contrary, it has a separate Chapter XI titled "Offences" in that cybercrimes have been declared as penal offenses punishable with imprisonment and fine.
- **The offenses covered under Indian ITA 2000 include:**
  1. Tampering (changing, updating) with the computer resource code or computer source document. Illegal access to Computer (Like "hacking" is one such type of act).
  2. Publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the sexual interest.
  3. Failure to decrypt information if the same is necessary in the interest of the jurisdiction 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 offense.
  4. Attempting to secure access to a protected system.
  5. Falsification, while obtaining, any license to act as a Certifying Authority (CA) or Digital Signature Certificate.
  6. Violation of confidentiality and privacy.
  7. Publication of digital signature certificate, which are false in some cases.
  8. Publication of digital signature certificates for fraudulent purposes.

- **There are some legal drawbacks with regard to cybercrimes:**
  1. The difficulties/drawbacks with most Indians not to report cybercrimes to the law enforcement agencies because they may fear about harassment.
  2. The awareness of people on cybercrime is relatively on the lower side.
  3. The law enforcement agencies in the country are neither well equipped not knowledgeable enough about cybercrime need for training to those agencies.
  4. Cybercrime cell is not present in all cities.
  5. There is a lack of dedicated cybercrime courts in India.
- **To overcome these challenges:**
  1. Need dedicated, continuous and updated training of the law enforcement agencies.
  2. Increasing the count of for cyber-savvy judges.
  3. Arranging the cyber law training to the judges and lawyers.
  4. Updation of cybercrime law and appropriate changes should be made in the IPC and the Information Technology Act.
  5. People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust and without the fear of being harassed.

4.6 CONSEQUENCES OF NOT ADDRESSING THE WEAKNESS IN INFORMATION TECHNOLOGY ACT

- We saw there are many challenges in India to fight the Cybercrime.
- Cyber laws of the country are yet not reach the level of sufficiency and adequate security to support India' E-Commerce business.
- India has lagged behind in keeping pace with the world in this regard, ultimately India's out sourcing sector may get impacted.
- There is some news about overseas customer about data breaches and data leakages in India.
- This can result in breaking India's IT business leadership in international outsourcing marker and the dream of India ruling the world's outsourcing market may not come true.
- Outsourcing is on the rise; if India wishes to maintain its strong position in the global market need, to address the current weaknesses in the Information Technology Act.

4.7 DIGITAL SIGNATURES AND THE INDIAN IT ACT

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

- Digital Signature Certificates or DSC or Digital Signature are being adopted by various government agencies and now is a statutory requirement in various applications.
- Certifying Authorities offers different class of certificates to help organization and individuals secure online transactions with legal validity as per the Indian IT Act, 2000.
- The Indian IT Act mentions "penalty for publishing false digital signature certificate in certain particulars."

4.7.1 Public-Key Certificate

- In cryptography, a public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key.
- A public key certificate is a digitally signed document that serves to validate the sender's authorization and name.
- A trusted organization that issues public key certificates is known as a Certificate Authority (CA).
- A digital signature is a kind of electronic signature that is used to guarantee the originality of the data. When linked to the identity of the signer - using a security token such as X.509 Certificates - a digital signature can be used for non- repudiation, since it links the signer with the signed document.
- The term non repudiation means it assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- An X.509 Certificate includes the information about the certificate subject and the certificate issuer (CA). A certificate is encoded in Abstract Syntax Notation One (ASN. 1), a standard syntax for describing messages that can be sent or received on a internet. The role of a certificate is to associate an identity with a public- key value.
- **A certificate includes following point:**
  1. X.509 version information.
  2. A serial number that use to 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. For example, an extension exists that distinguishes between CA certificates and end-entity certificate.

- One of the useful applications of X.509 Certificates is in Web browsers (such as Netscape Navigator and Microsoft Internet Explorer) that support the Secure Socket Layer (SSL) Protocol.
- SSL is a highly secure protocol that provides privacy and authentication for network traffic.
- Other technologies that rely on X.509 Certificates include:
  1. Code-signing schemes, such as signed Java Archives and Microsoft Authenticode.
  2. Secure E-Mail standards, such as Privacy-Enhanced Mail (PEM) and Secure/ Multipurpose Internet Mail Extensions (S/MIME);
  3. E-Commerce protocols, such as Secure Electronic Transactions (SET).

4.7.2 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 hand written signature form.
- Asymmetric cryptosystem means both private and public keys are used in Digital Signature.
- At the time of drafting of the ITA 2000, there was a slip-up in the drafting of Section 35, subsection (3), which made it compulsory for an applicant of a digital signature certificate to enclose a Certification Practice Statement with his application.
- One of the major low false in the bill, which could obstruct implementation, is the provisions regarding the role and function of the CAs(Certifying Authorities) and the digital certificates issuing process.

4.7.3 Impact of Oversights in ITA 2000 Regarding Digital Signatures

- The oversights, explained in the previous section, result in serious concerns - it is troublesome to imagine what will happen when the new rules under the Act are drafted.
- To keep the situation under control, the Ministry of Information and Technology had to urgently establish a task force to assist them in the drafting of the rules related to cybercrime.
- The task force consisted of experts in the cyber and law field.
- The Information Technology Amendment bill 2006 was drafted on the basis of the recommendation of an " Expert Committee."
- The recommendation of Technical Committee that are:
  (a) The PKI-based system made the law dependent on a sing le authentication technology.
  (b) There was a need to make the law technology Neutral.

- **PKI - Basic Components:**
  1. **Public Key Certificate:** It is on electronic record that binds a public key to the identity of the owner of o public- private key pair and is signed by a trusted authority.
  2. **Certificate Revocation List (CRL):** It is a list of certificates that have been revoked. The list is generally signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example. If the owner's private key has been lost or it the owner's name changes.
  3. **Certification Authority (CA):** A trusted entity that issues and revokes public-key certificates and CRLs.
  4. **Registration Authority (RA):** An entity that is trusted by the CA to register or vouch for the identity of users to a CA.
  5. **Certificate Repository:** An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to repositories.
  6. **Certificate User:** An entity that uses certificates to know with certainty the public key of another entity.

4.7.4 Implications for Certifying Authorities

- Information Technology Amendment Act 2008 of drafting an amendment bill, which was meant for amending a pending bill that was to amend a prevalent act, some serious slip-ups have crept into the Act which is now a law.
- A New Section 3A to define electronic signatures and retained the earlier Section 3 of digital signatures. This has made "electronic signature" a concurrent alternative proposed by law to "digital signature" and both could be used for authentication of electronic documents. As a result, the CAs' regulations also need to be accommodated for both digital signature as well as electronic signature.
- Public should also be able to "affix digital signature" and "affix electronic signature" as the case may be.
- People can acquire two different certificates, one for digital signature and the other for electronic signature, which may involve different CAs. The law, therefore, needs to accommodate all these provisions.
- It appears that the drafting of the bill has resulted in some confusion whereby in some places both the digital signature and electronic signature are mentioned together and in some places they are mentioned differently. The net result is inconsistent treatment giving rise to confusion that could have been avoided.

4.7.5 The Current Scenario Regarding Digital Signatures under the Indian IT Act

- At present, the confusion in electronic signature not clear the present system of digital signatures will continue for the time being and will be the only method of

authentication of an electronic document. When the government needs to introduce a new system, it will have to notify through the Official Gazette the relevant procedure also require the notification to be placed before the Parliament.

- If any technical solutions need to be considered for PKI-based system, then it must put to extensive tests within India as well as in global circles.
- The system has to be Licensed in a similar manner of licensing CAs at present.
- In the near future, the Indian law recognized the digital signature system will continue to be the whole system of authentication.
- The need for "digital signature system" to continue for the time being, results in some serious legal lacuna. In Section 2(d) of the new Act, "affixing of an electronic signature" is defined as "Affixing Electronic Signature" with its grammatical variation and cognate expression mean adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic signature".

4.7.6 Cryptographic Perspective on the Indian IT Act

- In plain language, non-repudiation means the assurance that someone cannot deny something.
- Generally, non-repudiation means one can ensure that a party that performs electronic communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- Technically speaking, the term non-repudiation has a specific meaning in E-Commerce; it means the intent to accept responsibility of submitting or receiving an electronic message and be bound by its substance.
- Non-repudiation in E-Commerce systems and electronic messaging systems is important because it protects a sender against the false assertion of the receiver that the message has not been received, and also protects a receiver against the false assertion of the sender that the message has been sent.
- Mainly, public-key-based digital signatures are "non-repudiable" and this is one of advantage.
- The two cryptographic definitions of repudiation:
  1. **First Definition (General):** The intent to accept one's obligation under a contract and be bound for its performance.
  2. **Second Definition (E-Commerce):** The intent to accept responsibility of submitting or receiving an electronic message and to be bound by its substance.
- The basis for a repudiation of a traditional signature may include:
  1. The signature is a forgery.
  2. The signature is not a forgery but was obtained via,
     - Unconscionable conduct by a party to a transaction;

- Fraud instigated by a third party;
- Undue influence exerted by a third party.

- The common law trust mechanism established to overcome a false claim of non-repudiation is witnessing.
- Following terms gives Crypto-technical meaning of "non-repudiation."
  1. In authentication, a service that provides proof of the data integrity and originality of data, which can be verified by any third party at any time. OR
  2. In authentication, an authentication that with high assurance can be define to be genuine and that cannot subsequently be deny.
- The Indian ITA 2000 puts the liability on the person who accepts the digital signature.

4.8 AMENDMENTS TO THE INDIAN IT ACT

- According to some expert's view, Indian law may satisfy European Union's data protection norms. For example, to do the business in global marker, it is necessary to create appropriate confidence among investors, companies all over the world to assure them that the data send to India for back office operations will indeed be safe and there are appropriate statutory mechanisms in place should a breach of data take place.
- In the amended Indian IT Act, that is, the ITA 2008, there is addition of several new offenses that are included in new paradigm in today's net-centric digital economy.
- The new legal definition chat given to the term cybersecurity under the newly added Section 2(nb) (ITAA 2008).
- Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

4.8.1 Overview of Changes Made to the Indian IT Act

- The newly added section 43(j) tries to expand the cases where compensation can be claimed to cases when a person without the permission of the owner of a computer, computer resource "destroys, conceals, causes any person to steal, or alter any computer source code used far a computer resource with an intention to cause damage."
- Under the newly introduced section 43A, "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource, which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person that affected, there is no upper limit to the liability under this section.

- Under section 72A, a provision has been made for criminal prosecution in the event of breach of information security. This offense is cognizable.
- The amendment in Sections 78 and 80 of the ITA 2000, bringing down the authority of investigation from the level of DSPs to the level of inspectors.
- Under Section 85, the "vicarious liability" on the companies for "data protection" has been hardened. The company as well as its directors or officers in-charge of business "shall be" held guilty of the offense committed" by the company.
- **The Amendment in Section 69B of IT Act of India:** Focus on the need for monitoring "cybersecurity". Any intermediary who intentionally or knowingly contravenes the provisions of subsection, shall be punished with an imprisonment for a term, which may extend co three years and shall also fine.
- **The Amendment in Section 70B(4) of IT Act of India:** The Indian computer emergency response team shall serve as the national agency for per forming functions like analysis of cyber incident, forecast and alert of cyber security incidents etc.
- **The Amendment in Section 70B(6) of IT Act of India :** "For carrying out the provisions of subsection (4), the agency referred to in subsection (I) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person".
- **The Amendment in Section 70B(7) of IT Act of India :** "Any person who fail to provide the information called for or company with the service provider, intermediaries, data centers, corporate body or direction under subsection (6), shall be punishable with imprisonment of one year or with fine of 1 lakh rupees or with both."

4.8.2 Cybercafe-Related Matters Addressed in the Amendment to the Indian IT Act

- The Amendment of Cybercafe Related IT Act was based on case that is on 29 May 2001 two persons Qayesh Thakkar and Sunil Thacker sent a letter to the Chief Justice of the Bombay High Court complaining about the proliferation of pornographic sites on the Internet. The letter was numbered as Writ Petition 2611 of 2001.
- The problem was that the Indian ITA 2000 had not defined cybercafe; so they could only be interpreted as "network service providers" under the erstwhile Section 79.
- The ITA 2008 has now provided a detail definition for the term Cybercafe and also included cybcrcafes under the term intermediaries. Several aspects of the Act therefore become applicable Cybercafe and there is need to take a fresh look at what cybercafes are expected to do for Cyberlaw compliance.

4.8.3 State Government Powers Impacted by the Amendments to the Indian Act

- The Indian ITA 2000 in Section 90 (Power of State Government to Make Rules) the State Government can make rules for the purpose of implementing the provisions of the Act assuming new meaning under ITA 2008.
- There are several more sections of ITA 2008 where State Government needs to exercise its powers.
- Sections 69, 69A and 69B are of crucial importance because they provide powers to State Governments as well as to the Central Government regarding the following:
  1. Appointing an officer or agency of the government specially authorized to intercept, monitor, decrypt, block access to any content, collect traffic data or information generated, transmitted, received or stored in any computer resource.
  2. Notifying procedures and safeguards for exercising the powers as indicates in the above paragraph.
  3. Defining the term traffic data.
- Under the modified Section 70, the appropriate government can declare any "facility of critical information infrastructure" as a "protected system." The State Government has to frame rules and procedures to identify such systems, authorize appropriate persons in writing.
- To able to effectively formulate a strategy for the State Governments, it is necessary to form an advisory body of experts which may be called the Cyber law Advisory Group so that, derailed action plan can be drawn up for the systematic investigation of cyber crime which is looming up as the new menace for the country. We can conclude that the ITA 2008 brings considerable amount of empowerment to the State Governments in India for the implementation of cybersecurity legislation.

4.8.4 Impact of IT Act Amendments on Information Technology Organizations

- Some IT and IT- Enabled Services (IT ES) companies in India seem to be satisfied with the amendments.
- IT act to take into account new technologies, increases in cybercrimes, the growth of the business process outsourcing industry in India and rising global concerns about data privacy and security.
- IT Act 2008 is a significant step forward in establishing a data protection framework in India, and in providing assurances for those doing business with Indian companies much of the detail was left to a rule-making process that has yet to be completed.
- While businesses focus on the new data protection rules, a host of other provisions of the ITAA has also received attention.

- Legal recognition of electronic records and electronic signature, due to this organization get legal support for online communication.
- The Indian Institutes of Information Technology Laws (Amendment) Bill, 2020 was introduced in Lok Sabha by the Minister of Human Resource Development, Mr. Ramesh Pokhriyal Nishank on March 4, 2020. The Bill amends Indian Institutes of Information Technology Act, 2014 and the Indian Institutes of Information Technology (Public-Private Partnership) Act, 2017.
- This Latest Amendment gives broad level of protects for electronic record and signature, so organization can get legal support.

4.9 CYBERCRIME AND PUNISHMENT

- The phenomenal rise in computer crime has caught attention around the world.
- Cybercrimes, which are the harmful acts committed from or against a computer system or network, differ from most terrestrial crimes in four ways:
  1. They are easy to learn how to commit.
  2. They require few resources relative to the potential damage caused.
  3. They can be committed in a jurisdiction without being physically present in it.
  4. They are often not clearly illegal.
- The other problem that comes in way of punishing cybercriminals is that the laws in some countries do nor clearly prohibit cybercrime.
- Often police officers may not realize how cybercrimes are different in nature compared to the traditional forms of crimes. For example, webpages such as the E-Commerce sites hit by widespread, distributed denial-of-service attacks may not be covered by outdated laws as protected forms of property.
- The punishment to cybercriminals by summarizing the following key points:
  1. Reliance on terrestrial laws may not be a reliable approach.
  2. Weak penal ties limit deterrence.
  3. Self-protection remains the first line of defense.
  4. A global patchwork of laws creates little certainty.
  5. A model approach is needed.
- A coordinated public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cybercrime.

4.10 CYBERLAW, TECHNOLOGY AND STUDENTS: INDIAN SCENARIO

- India has a specific scenario given the current educational system.
- Most technology students have either nil or low exposure to cyber law and most law students have only limited exposure to Information Technology.

- In some college a computer science scream student is taught how to develop programs that can automatically transmit data across the Internet using on a TCP/Ip packet, without alerting him on cybercrimes such as hacking or virus introduction.
- In the current educational system, the topic of secure coding is not included in most universities syllabi.
- The Law students should be taught about Trade Marks and Copyrights without recognizing their implications on the electronic documents. As a result, neither the technologist nor the lawyer is trained in his formative years to understand cyber law.
- Near future, Engineering, Commerce and Management colleges need to teach cyber law as an extension of computer science, commerce and management education, even while the law colleges try to enhance their coverage of criminal laws and IPR laws to the cyber world.

Summary

- The people who are involved in social networking sites must understand the meaning of the term digital evidence that give in that the Indian Information Technology Act [ITA 2000].
- Globally the cybercrime is divided in two categories:
  1. Cybercrime in a restrictive sense (computer crime)
  2. Cybercrime in a general sense (computer-related crime)
- Crime or an Offense is "a legal wrong that can be followed by criminal proceedings which may result into punishment."
- The Australian Cybercrime Act 2001come into effect in April 2002. Under this Act, new powers granted for law enforcement.
- The Singaporean, New Zealand, Australian, Taiwanese and Thai Governments have each enacted robust computer, security laws which cover most of the basics and computer-related offenses in the CoE's (Council of Europe's) Convention on Cybercrime.
- In the European Union, cybercrime law is based on the CoE's Convention on Cybercrime (Nov 2001), under the convention, member states are obliged to criminalize:
- Cyberlaw give legal recognition to all risks arising out of the usage of computers and its networks.
- Before making 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 document in electronic format.
- The offenses covered under Indian ITA 2000, but there was some drawback, which was overcome in New Act. 2008.

- Cyber laws of the country are yet not reach the level of sufficiency and adequate security to support India' E-Commerce business.
- Digital Signature Certificates or DSC or Digital Signature are being adopted by various government agencies and now is a statutory requirement in various applications.
- A trusted organization that issues public key certificates is known as a Certificate Authority (CA).
- Some IT and IT- Enabled Services (IT ES) companies in India seem to be satisfied with the amendments.
- IT act to take into account new technologies, increases in cybercrimes, the growth of the business process outsourcing industry in India and rising global concerns about data privacy and security.
- In the amended Indian IT Act, that is, the ITA 2008, there is addition of several new offenses that are included in new paradigm in today's net-centric digital economy.
- Section 66 has now been expanded to include sub Sections :
  - 66A for Offensive Messages.
  - 66B Receiving Stolen Computer, the fast track "adjudication" is restricted to cases where the compensation is up to 5 crore 5,00,00 ,000 , there is no upper limit on the compensation n to be claimed.
  - 66C Identity Theft.
  - 66D Impersonation.
  - 66E Violation of privacy.
  - 66F Cyber Terrorism.
- Section 67 has been expanded to include Sections
  - 67A Sexually Explicit Content.
  - 67B Child Pornography.
  - 67C, there is a further responsibility trusted with "intermediaries." intermediaries now include body "corporate" to retain information for a certain time as specified by the Central Government.-
- Most technology students have either nil or low exposure to cyber law and most law students have only limited exposure to Information Technology.

Check Your Understanding

1. The more concrete example of cybercrime is____.
   (a) unauthorized access to computer
   (b) causing damage to computer data or programs

(c) an access of computer sabotage
(d) All of the Above

2. Which of the following is not a principle of APEC privacy framework?
(a) Preventing harm (b) Integrity of personal in formation
(c) Model (c) Accountability

3. Which of the following is not the ITA 2000 sections in CHAPTER XI (Offences) of the are relevant to the cybercrime in legal context?
(a) 64 (b) 66
(c) 67 (d) 74

4. The ITA 2000 Sections 65 _____.
(a) tampering with computer source documents
(b) computer-related offences
(c) penalty for misrepresentation.
(d) publication for fraudulent purpose.

5. The ITA 2000 Sections 66 _____.
(a) tampering with computer source documents
(b) computer-related offences.
(c) penalty for misrepresentation.
(d) publication for fraudulent purpose.

6. The ITA 2000 Sections 71 _____.
(a) tampering with computer source documents
(b) computer-related offences
(c) penalty for misrepresentation.
(d) publication for fraudulent purpose.

7. The ITA 2000 Sections 74 _____.
(a) tampering with computer source documents
(b) computer-related offences
(c) penalty for misrepresentation.
(d) publication for fraudulent purpose.

8. IT Amendment Bill 2008, New Sections under 66A _____.
(a) sending offensive messages (b) identity Theft
(c) cheating by personation (d) receiving a Stolen Computer Resource

9. IT Amendment Bill 2008, New Sections under 66 B _____.
(a) sending offensive messages (b) identity Theft
(c) cheating by personation (d) receiving a Stolen Computer Resource

10. IT Amendment Bill 2008, New Sections under 66C _____.
(a) sending offensive messages (b) identity Theft
(c) cheating by personation (d) receiving a Stolen Computer Resource

11. IT Amendment Bill 2008, New Sections under 66D _____.
(a) sending offensive messages (b) identity Theft
(c) cheating by personation (d) receiving a Stolen Computer Resource

ANSWERS

1. (d)	2. (c)	3. (a)	4. (a)	4. (b)	6. (c)	7. (d)
8. (a)	9. (d)	10. (b)	11. (c)			

Practice Questions

Q.I Answer the following questions in short.

1. What are the two categories of cybercrime?
2. Write any four principals of APEC privacy framework.
3. What is Spam Laws?
4. What is Cybercrime and Federal Laws in the US?
5. What is Cybercrime Legislation in the African Region?
6. What is ITA section 66?
7. Write IT Amendment Bill 2008, New Sections under 69A and 69B with imprisonment.
8. Write IT Amendment Bill 2008, New Sections under 67A and 67B with imprisonment.
9. What is Public-Key Certificate in Digital Signature?
10. What is "non-repudiation"?
11. Which are problem that comes in way of punishing cybercriminals in many countries?

Q.II Answer the following questions.

1. Explain a Broad View on Cyber Crime Law Scenario in the Asia-Pacific Region.
2. What is Anti-Spam Laws in Canada? Explain in details.
3. Why do we need cyber laws in India?
4. What are the significant changes brought out by the IT Amendment Bill 2008 in section 66?
5. What are the Positive Aspects of the ITA 2000?
6. What are the weak areas of the ITA 2000?
7. What are the challenges to Indian Law and cybercrime scenario in India?

8. Explain the implications for Certifying Authorities.
9. Explain the Cyber law, Technology and Students as per Indian Scenario.
10. What is impact of IT Act Amendments on Information Technology Organizations?
11. Explain in brief the changes made to the Indian IT Act.

Q.III Define the terms:

1. Computer Security Law.
2. Data Privacy
3. Data Protection
4. The ITA 2000 Sections 67.
5. The ITA 2000 Sections 71.
6. The ITA 2000 Sections 72.
7. The ITA 2000 Sections 73.
8. The ITA 2000 Sections 74.
9. IT Amendment Bill 2008, New Sections under 67B and 67C with imprisonment.
10. IT Amendment Bill 2008, New Sections under 66E and 66F with imprisonment.
11. Digital Signatures
12. Certifying Authorities.

❖❖❖

5... Cyber Forensics

Learning Objectives...

- To understand the Fundamental concepts in Cyber Forensic.
- To learn what is Digital Evidence.
- To learn how Cyber Forensics used in cybercrime investigation.
- To understand the legal requirements for Cyber Forensic.
- To understand the challenges faced in Cyber Forensic.

5.1 INTRODUCTION

- Cyber Forensics plays important role in investigation of cybercrime. "Evidence" in the case of "Cyber offence" is legally very important. There are legal aspects involved in the investigation as well as handling of the digital forensic evidence. The only experience and technically trained experts are involved in the forensic activities.
- The data is very important in cyber forensic, so in this chapter the all basic information discussed.

5.2 HISTORICAL BACKGROUND OF CYBER FORENSICS

- The use of computer or digital devices for investigating computer based crime has led to development of a new field called Computer Forensic. It is also called as Digital Forensic.
- As long as people store data inside the computer or on digital media the Computer Forensic or Digital Forensic remain exist.
- Computer forensic is still a relatively new discipline in the domain of computer security, it is rapidly growing discipline and a fast growing profession as well as a business.
- The main aim of digital forensic is to find out digital evidence such as the evidence required establishing whether or not a fraud or a crime has been conducted.
- There is a difference between computer security and computer forensics although computer forensic is generally associated with computer security but both are different.

5... Cyber Forensics

Learning Objectives...

- To understand the Fundamental concepts in Cyber Forensic.
- To learn what is Digital Evidence.
- To learn how Cyber Forensics used in cybercrime investigation.
- To understand the legal requirements for Cyber Forensic.
- To understand the challenges faced in Cyber Forensic.

5.1 INTRODUCTION

- Cyber Forensics plays important role in investigation of cybercrime. "Evidence" in the case of "Cyber offence" is legally very important. There are legal aspects involved in the investigation as well as handling of the digital forensic evidence. The only experience and technically trained experts are involved in the forensic activities.
- The data is very important in cyber forensic, so in this chapter all the basic information discussed.

5.2 HISTORICAL BACKGROUND OF CYBER FORENSICS

- The use of computer or digital devices for investigating computer based crime has led to development of a new field called Computer Forensic. It is also called as Digital Forensic.
- As long as people store data inside the computer or on digital media the Computer Forensic or Digital Forensic remain exist.
- Computer forensic is still a relatively new discipline in the domain of computer security, it is rapidly growing discipline and a fast growing profession as well as a business.
- The main aim of digital forensic is to find out digital evidence such as the evidence required establishing whether or not a fraud or a crime has been conducted.
- There is a difference between computer security and computer forensics although computer forensic is generally associated with computer security but both are different.

- The data required for digital forensic examination by the law enforcement agency which includes investigation into E-mail usage, social media messages, website history, cell phone usage, cellular and voice over internet protocol phone usage, file activity history, file creation or deletion, chat history, account login or logout record etc.
- The term forensic science is the application of science to law and it is ultimately defining by use of court law.
- Forensic means characteristics of evidence that fulfill its suitability for admission as a fact and its ability to persuade based upon proof of evidence.
- The main goal of digital forensic is to determine the value of a crime scene and related evidence.
- The role and contribution of digital forensic or computer forensic experts are almost concurrent to those involved as forensic scientist in other crimes, namely, analysis of evidence, provision of expert testimony, completing training in proper recognition and collection and carefully preservation of evidence.

5.3 DIGITAL FORENSICS SCIENCE

- Digital forensic is the application of analysis technique to the reliable and unbiased collection of digital evidence or proof. The digital evidence uses the analytical and investigative techniques to identify, collect, examine and preserve evidence or information which is store on magnetic material or in encoded form.
- Computer forensic is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and data about data (metadata) derived from digital devices which may contain information.
- **Computer forensic:** It is the collection of techniques and tools used to find evidence in a computer or digital devices.
- **Digital forensic:** It is the use of scientifically derived and proven methods towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence.
- Digital evidence includes the collection and examination of all forms of digital data including the data found in mobile phone, PDAs, iPods and other electronic devices.
- **The role of digital forensic:**
  1. Uncover and document evidence and leaves.
  2. Corroborate evidence discovered in other way.
  3. Assist in showing a pattern of event using the data mining.
  4. Connect attack and victim computers.
  5. Retrieval an end to end path of events leading to the compromise attempt successful or not.
  6. Extract data that may be encrypted, hidden, deleted or not easily available.

- The digital forensic scenario mainly involved following points:
  1. Abuse of internet by employee.
  2. Unauthorized disclosure of corporate information and data.
  3. Corporate spying activities.
  4. After an incident damage assessment.
  5. Criminal fraud and misleading cases.
  6. Criminal cases.
  7. Violation of copyrights.

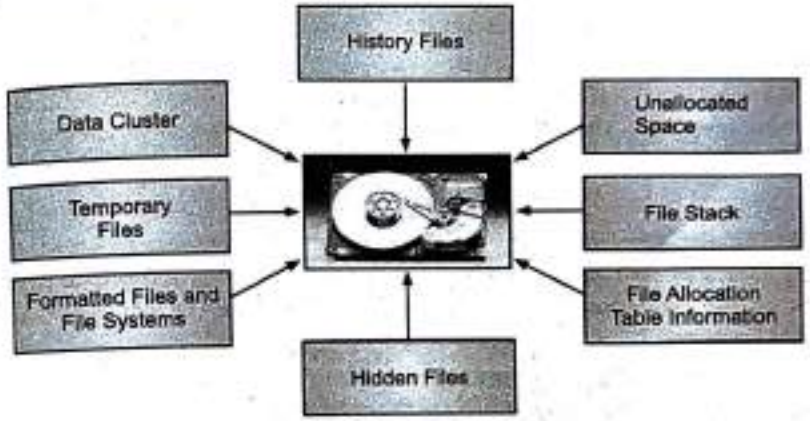

Fig. 5.1: Data seen using Forensic tools

- One can use the digital forensic technique to achieve following things:
  1. Confirm and clarify evidence otherwise discovered.
  2. Generate investigative leads for follow-up and verification in different way.
  3. Provide help to verify and institution assumptions.
  4. Eliminate incorrect assumptions.

5.4 THE NEED FOR COMPUTER FORENSICS

- The large coverage of Information and Communication Technology (ICT) and the vast use of computer worldwide together have brought about many advantages to human being.
- At the same time there is a tremendously all technical capacity of modern computing devices provides unwanted use or misuse devices for committing crimes.
- This will increase address of computer user so there may be a social harm.
- The user in businesses and organizations worldwide have to live with constant thread for or hackers because from many ways hacker can hack a data from computer system.

- The wide view of computer forensic, the result in two factors:
  1. The increasing dependency of law enforcement on digital evidence.
  2. The ubiquity of computers that followed from the microcomputer revolution.
- There are many challenges for the forensic investigator because storage devices are getting very small in nature due to advance in electronic technology. For example, external and mini hard disk and pen drive use are available in amazing shapes. Due to this nanotechnology there is very difficult to find Digital Forensic Evidence (DFE).
- There are many forensic softwares or tools available to find evidence from suspected media as the capacity of medium may varies in GB, TB, PB(Petabyte) or EB(Exabyte).
- These forensic software helps to sieve data from the irrelevant storage mass can be produce as a evidence.
- In larger perspective digital evidence includes all that things used to determine the truth of an assertion. This evidence can be used in court to prove the committed crime.
- There is the need to handle evidence carefully to avoid later allegations of tempering or misconduct that can compromised the case of prosecution.
- The term "chain of custody" is also used in most evidence situations to maintain the integrity of the evidence by proving documentation of the control, transfer and analysis of evidence.
- The main purpose of recording the chain of custody is to develop the alleged evidence is indeed, related to the alleged crime. The chain of custody important when the evidence consist of fungible goods.
- After collection of all evidence the clerk storage it in safe and secure place.
- All evidence collection and its appearance in court need to be completely documented in chronological order to withstand legal challenges to the authenticity of the each any every evidence.

5.5 CYBER FORENSICS AND DIGITAL EVIDENCE

- Cyber forensic can be divided into two different domains:
  1. Computer forensic
  2. Network forensic
- Many security threats are possible through computer networks so computer forensics have importance in the context of cybercrime
- Network forensic is the study of network traffic to find the truth in civil, criminal and administrative matters to protect uses and resources from exploitation, invention of privacy.
- The physical evidence and digital evidence both are in different nature because each has some specific characteristics.

- Digital evidence much easier to change or manipulate. Also the copy of digital evidence can be made without harming or changing original.
- All digital evidence are in the form of image. It is very much possibility to create defensible clone or another copy of storage devices.
- Understanding the importance of digital evidence in its maintenance phase involved in digital forensic investigation and maintaining the chain of custody.
- The digital evidence in cybercrime mainly consists of spreadsheets, memos, letters, emails, chats, files.
- Computer forensic expert knows the techniques to retrieve the data from files which are stored in standard directory, hidden files, deleted files, deleted emails and passwords, login IDs, encrypted files, hidden partitions etc.
- The digital evidence are mainly on computer system, which having following details:
  1. The logical file systems that consists of file system, random access memory, and physical storage media.
  2. User created files which contains address book, audio video files, calendars, database files, email, internet bookmark, documents etc.
  3. Computer or system created files which consist of backups, cookies, configuration file, history file, log files, swap file, system files and temporary files.
  4. Computer networks which consists of main four layers: application layer, transport layer, network layer and data link layer.

5.5.1 The Rule of Evidence

- According to the Indian evidence act 1872, Evidence can be in the form of oral evidence and documentary evidence.
- The Indian IT act amendment mention the electronic evidence is a new type of evidence.
- There are three context in world to identify a piece of digital evidence:
  1. Physical context, that is in the physical form.
  2. Logical context, it identifiable as a logical position.
  3. Legal context that is the evidence must be correct context to read its meaning.
- Following are some guidelines for collection of digital evidence:
  1. Stick to your site's security policy and engage the appropriate incidence handling and law enforcement personnel.
  2. Take a picture of system as accurately as possible, without any mistake.
  3. Maintain details of information with dates and time.
  4. Note the difference between the system clock and coordinated universal time or local time.
  5. Be prepare to [illegible]ify outline all actions you taken time to time.

6. Minimize changes to the data as you are collecting it.
7. Delete external avenues for change.
8. You should do collection first and afterwards do the analysis.
9. Your procedure should be implementable.
10. For every evidence, a systematic approach should be adopted.
11. Proceed for collection of evidence from the volatile to the less volatile.(registers, cache, process table, memory are more volatile whereas disk, network topology, archival media, are list volatile)
12. You should make a bit level copy of systems media. Try to avoid doing for forensic on the evidence copy.

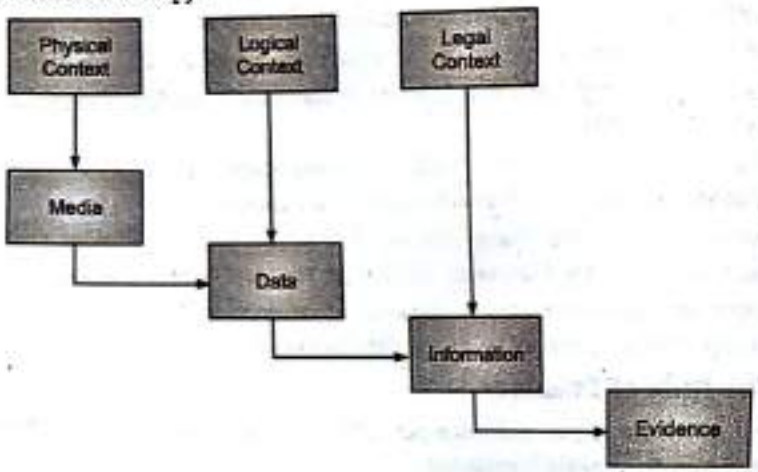

Fig. 5.2: Path of the digital evidence

5.6 FORENSICS ANALYSIS OF EMAIL

- We know that how the criminal can use fake Email for various cybercrime offences.
- Softwares are available that helps to create fake Emails. The forensic analysis of Email is an important aspect of cyber forensic analysis which helps to establish the authenticity of an Email when it is suspected.
- Forensic analysis of Email, you must know the Email component and the Email header structure.
- An Email system is the hardware and software that controls flow of E-mail. Two main components of an E-mail system are Email server and E-mail gateway.
  - E-mail servers are computers that forward, collect, store and deliver email to their clients.
  - E-mail gateway is the conditions between Email servers. The E-mail server software controls the flow of Emails on network server.

- Every mail consists of two parts Header and Body. The header of an Email is very important for forensic point of view.
- Entire header few of an Email provides the total path of Email's journey from its origin to its destination. The header view includes the originating Internet Protocol (IP) addresses and other useful information.
- Following is the E-mail header example.

```
Received: from 10.197.39.76
by atlas108.free.mail.bf1.yahoo.com with HTTPS; Wed, 4 Aug 2021 10:20:52
+0000
Return-Path:<bounces+19798689-ed92
nimbalkar=yahoo.com@em6154.manadesigner.com>
X-Originating-Ip: [167.89.52.239]
Received-SPF: pass (domain of em6154.manadesigner.com designates
167.89.52.239 as permitted sender)
Authentication-Results: atlas108.free.mail.bf1.yahoo.com;
dkim=pass header.i=@manadesigner.com header.s=s2;
. . . . . .
X-Apparently-To: nimbalkar@yahoo.com; Wed, 4 Aug 2021 10:20:52 +0000
X-YMailISG: DtRfRwAWLDsb.9OjJt79WmLgjRLEOEkxYeCxAE47sZ6hEX3n...
. . . . . .
Received: from 167.89.52.239 (EHLO o1678952x239.outbound-mail.sendgrid.net)
by 10.197.39.76 with SMTPs
(version=TLS1_2 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256);
Wed, 04 Aug 2021 10:20:52 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=manadesigner.com;
h=content-type:from:subject:content-transfer-encoding:mime-version:reply-
to:to;
. . . . . .
Received: by filterdrecv-7d5fff68cf-m64np with SMTP id filterdrecv-
7d5fff68cf-m64np-1-610A6A02-70
Received: from [127.0.0.1] (unknown)
Content-Type: text/html; charset=us-ascii
From: Brainovision <it@brainovision.in>
Subject: MoU Proposal.
Message-ID: <c3984460-3622-c547-96bd-c63120eeb869@brainovision.in>
Content-Transfer-Encoding: quoted-printable
Date: Wed, 04 Aug 2021 10:20:50 +0000 (UTC)
MIME-Version: 1.0
Reply-To: it@brainovision.in
To: nimbalkar@yahoo.com
X-Entity-ID: KEJw7VTYEeTaewSrnSLxFA==
Content-Length: 8487
<Body> . . . . . .
```

[You can get above email header details from yahoo, open your email Click on triple dots, select "View raw message" ; for Gmail click on triple dots and click on "Show Original]

- The main purpose serves by Email header is providing information about the sender and recipient and preventing spam, identifying the email route. To analyze it, you need to find the email header and examine the lines of interest. All the code from the beginning, until the <body> tag, represents the header.
- Here are the list main points from the Email header:

1) **"Received:" lines:**
   - They show the address of the computer that received the email, as well as other computers' addresses that an email may have been transferred through. Unlike other Email header elements, "Received:" lines can't be forged.
   - Received By field contains the details of the last visited SMTP server. The following information is disclosed:
     a) Server's IP address.
     b) SMTP ID of the visited server.
     c) Data and time at which the email was received by the SMTP server.
   - Received From is one of the most important fields in an Email header as you can find the IP address of the sender along with other details like the host name. From this information you can find that the Email was first received from with the IP address of the sender. It also shows the date and time when message was send.
2) **MIME-version:**
   - Multipurpose Internet Mail Extensions (MIME) are an Internet standard that extends the format of Email by supporting text and non-text attachments like audio, video, images, message bodies with multiple parts, etc.
3) **Message-ID:**
   - The message-ID is a globally unique identifier used in Email. Message-IDs have a specific format that is generated for a specific Email address and message, thus, no two messages have the same Message-ID.
4) **DKIM Signatures:**
   - Domain Keys Identified Mail (DKIM) confirms the sender's authenticity by connecting the domain name with the email. DKIM is the technology that helps to reduce spam and phishing and allows companies to vouch for their email messages.
   - Here are the various tags of DKIM signature header:
     - **v:** Application version. Only version 1 exists today so this field should always be set to 1.
     - **a:** Algorithms used for encryption. It should be RSA-SHA256 in most cases. Some senders may use RSA-SHA1 but it's not recommended due to security risks.
     - **c:** Algorithms used for canonicalization.

     - **s:** Selector record name used with the domain.
     - **h:** Signed header fields that are used in the signing algorithm to create the hash in b= tag.
     - **bh:** Hash of the message body.
     - **b:** Hash data of the headers listed in the h= tag. It's also called DKIM signature.
     - **d:** Domain used with the selector record.
   - All the above tags are required for DKIM mechanism to work. If any tag is missing, then verification may encounter an error.
5) **Return Path:** This field contains the Email address where the message is returned, in case it fails to reach the intended recipient. This can easily happen if the sender has used a wrong Email address for the recipient.
6) **Received-SPF:**
   - Sender Policy Framework (SPF) is an Email security protocol that's used to verify the sender. The system forwards the message only after the sender's identity is authenticated. The technique uses the domain address for authentication and adds the check status in the header field.
7) **Authentication Results:**
   - Mail Transfer Agents (MTAs) apply a slew of authentication techniques on the email messages before processing them. The results of these techniques are added to the header field of messages and are separated by a semicolon.
   - The Authentication Results field is of great importance in email header analysis forensics as it shares the ID of the authentication performing server. It also shares the authentication techniques along with their results.

- Some email may content CC and BCC. The CC carbon copy and BCC blind carbon copy that is recipients get copies of the message.
- Once you get the IP address next job is to find the internet service provider details.
- The internet service provider plays an important role in email forensic. The internet service provider provides internet access to businesses, organizations, schools, colleges and individuals.
- The details are available from the internet service provider are name, address, and contact number, location of the subscriber of the internet facility, type of IP address and other relevant information related to IP address at the specific date and time.

5.6.1 RFC 2822

- RFC 2822 is the internet message format standard. According to RFSC 2822 there are several formats of valid email addresses like Patil@host.net, Akash@[10.0.3 .19], "S_Kadam"@host.net. Many Email addresses validators on the web fail to recognize some of that valid email address.

- The RFC 2822 standards apply only to the internet message format and some of the semantic of message contents. It does not specify the information of envelop.
- The RFC2822 state that each email must have globally unique identifier.
- As per RFC2822 standard message-ID can be appeared in three header fields:
  1. Message ID header
  2. In-reply-to header
  3. Reference header
- But message-ID of the present Email must be including against the message-ID header. There may be SPAM problem and to that there is no simple solution. E-mail header cannot be trusted, not all email can be traced for authentication. Only legitimate email typically can be traced out.

5.7 DIGITAL FORENSICS LIFE CYCLE

- As per Federal Bureau of Investigation (FBI) view, digital evidence is present in nearly every crime scene.
- The law must know how to identify, seize, transport and store original digital evidence preserve it for forensic examination.
- The fundamental rules to remember are that evidence is admissible, authentic, complete, reliable, understandable and believable.

5.7.1 The Digital Forensics Process

- Digital forensic evidence consists of exhibit. It useful for each member of jury to establish the facts of the case and support or refute legal theories of the case.
- In the court procedure, the exhibit is introduced as evidence by either side.
- Testimony is presented to establish the process which is used to identify, collect, preserve, transport, store, analyze, interpret, attribute and /or reconstruct the information contain in the exhibits.
- The party must show all the evidence to be admitted and also established that the evidence is related, authentic and that the evidence present is not the result of hearsay, original writing for the legal equivalent.
- Generally it assumes that the adequate fact can be established for the introduction of an evidence exhibit. The people involved in the chain of custody need to testify a number of aspects related to the evidence.
- Digital forensic evidence can get details through the use of various tools. People who use these tools properly applied scientific knowledge, skill, experience, training and education.
- People can use the methodology that is reliable to define standard of tool.

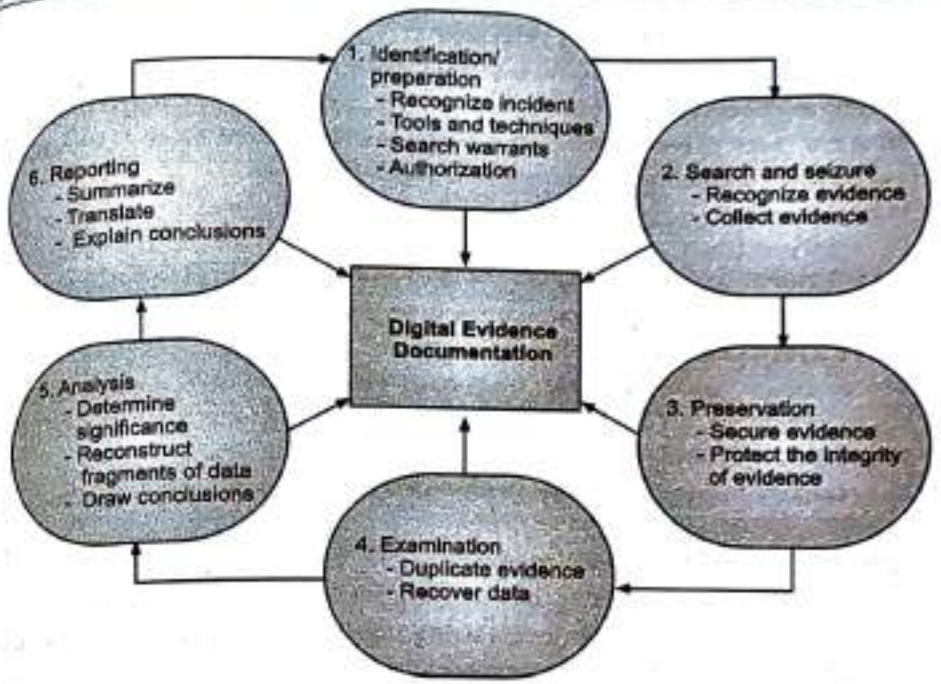

Fig. 5.3: Process model for understanding seizure and handling of forensic evidence legal framework

- Digital forensic evidence can be challenged by establishing that by intent or accident, content, context, meaning, timing, location, relationship, corroboration. This produce false positive or false negatives in the result presented by the other side.
- Forensic examiners are trained to follow a carefully developed set of protocols for acquisition of electronic evidence designed to ensure authenticity and assiduous chain of custody.

5.7.2 The Phases in Computer Forensics/Digital Forensics

- The forensic life cycle involves the following phases:

1. **Preparation and identification of digital evidence:**
   - The evidence must first be identified as an evidence because it may happen that there is a large amount of potential evidence available may never get identified.
   - One can identify the evidence by considering that every sequence of events within the single computer that might be due to interactions with files and file system.
   - If the evidence cannot be identified as a relevant evidence, it is not possible to collect at all and chances of existence of such evidence in digital form are very less.

2. **Collection and recording digital evidence:**
   - Digital evidence can be collected from meaning sources like computers, pen drives, cell phone, digital camera, hard drives, memory sticks and so on.
   - In some cases one can collect the digital evidence from black boxes inside the automobile, digital thermometers, web pages, RFID tags.
   - It is important to take care of digital evidence as they are easily change or update. It is very difficult to detect any change made in the digital evidence. The cryptographic hash functions may be used to detect a change in such cases.
   - The collection of volatile data requires special technical skill because data may be store on RAM and as power off data can be lost.
   - The evidence can be collected from solid state nonvolatile memories like USB sticks, cell phone, SD cards, and multimedia cards. These technologies differ from the normal hard disk.
   - The memory inside the computer also used to collect the evidence, the memory like ROM, PROM, EPROM, and EEPROM.
3. **Storing and transporting digital evidence:**
   - To handle the digital evidence the following practice must be adopted;
     a) Make image of computer media using a write blocking tools to ensure that no data is added or deleted from suspect device.
     b) Properly maintain the chain of custody.
     c) Make a documentation of everything that has been done.
     d) Generally use only those tools and methods that have been tested and you have a dare to validate their accuracy and robustness.
   - In storage center, digital media must be properly maintained over the period of time. Due to humidity or temperature might be damage of media.
   - Sometime digital evidence must be transported from one place to another place. To make secure transportation of the digital evidence, generally making exact duplicates at the level of bits of the original content, sometime also called cloning.
   - In transportation, adequate care must be taken to prevent spoliation. Care must be taken to preserve chain of custody and ensure that a witness can testify accurately about what took place.
4. **Examining or investigating digital evidence:**
   - The only legal forensic authority can seize, copy and examine the data, special care must be taken that unauthorized expert should not access or examine digital evidence.
   - There are two types of analysis, that is dead and live analysis related to investigating digital evidence.

   - The dead analysis can be done by making an image of the media like hard disk, computer forensic investigation perform on data at rest.
   - During the imaging care must be taken that no information is introduced into the evidentiary media during the forensic process.
   - The entire imaging process verified using strong hashing algorithms like *sha1* and *md5*.
   - Nowadays, there has been increasingly an emphasis on performing analysis on live system. For example, the attacker only exploit information in the computer's main memory, so before power of machines evidence must be collected.
5. **Analysis, interpretation and attribution:**
   - Digital investigation may encounter different formats of digital data.
   - There may be several types of analysis based on interpretation or abstraction, layer.
   - The common examples of digital analysis types are:
     1. Media analysis
     2. Media management analysis
     3. File system analysis
     4. Application analysis
     5. Network analysis
     6. Image analysis
     7. Video analysis.
   - There are special tools available to display the information in a format useful to investigation such forensic tools includes Access Data's FTK, Dr.Golden Richard III, Brain Carriers Sleuth Kit etc.
   - Generally forensic analysis includes a manual review of material on the media. For example operating system specific investigation is reviewing the Windows registry.
   - Open source tools are available, can also use for scanning RAM and register information to find recently accessed web based email sites and the login or password combination used.
6. **Reporting:**
   - After completion of complete analysis, a report is generated. This report may be written form or an oral testimony or it may be a combination of both.
   - The evidence, analysis, interpretation and attribution consist in export reports.
   - After complete analyzing of the evidence collected, report are prepared and it will present in various type of audience like law enforcement official, technical expert, legal expert, corporate management.

- Depending on the nature of crime it is necessary to present the findings in front of the court of law.
- Following elements are considered preparation of report:
  1. Identify the suitable reporting agency.
  2. Case identifier or submission number.
  3. Case investigator.
  4. Identity of the submitter.
  5. Date of receipt and report.
  6. Detail list of items submitted for examination which includes serial number, make and model.
  7. Identity and signature of the examiner.
  8. Basic step taken during the examination like string searches, graphical image searches, recovering deleted files.
  9. Final conclusion.

7. **Testifying:**
   - Testifying is nothing but producing evidence as a witness in a law court. This involves presentation and cross examination of expert witnesses. Generally expert witnesses produce digital forensic evidence in a court.
   - Only export witnesses can address issues based on scientific, technical or any other specialized knowledge.
   - A witness qualified as expert by knowledge, skill, experience, training or education main testify in the form of an opinion or if the testimony is based on sufficient fact or data, the testimony is the product of a reliable principle and method, the witnesses has applied the principal and methods reliable to the fact of the case.

5.7.3 Precautions to be taken when Collecting Electronic Evidence

- The collection of the evidence must be done with proper care.
- Special measure must be taken at the time of doing a forensic investigation. The evidence must be accurately collected and that there is in clear chain of custody.
- The integrity of digital evidence must be maintain, for this the following principles are used:
  1. No action taken by the law enforcement agency or their agents should be change data held on a computer or storage media, which may be subsequently produce in court.
  2. In exceptional circumstances, where a person find original data on computer, he must be competent and must able give proper explanation of relevance of evidence.

3. An audit trial or other record of all process applied to computer based electronic evidence should be created and preserve.
4. Investigation in charge has total responsibility for ensuring that the law and these principles are adhered to.

5.8 CHALLENGES IN COMPUTER FORENSICS

- Investigation of cybercrime is by not easy task. Nowadays, computers may have 200GB or more storage capacity. There are more than 5 billion messages are exchanges every day in the US alone. There are more than 4 billion indexed webpages worldwide. There are more than 600 billion documents online. Terabytes of data are stored on electronics devices. Therefore, looking for forensics evidence among these is like looking for the proverbial needle in the haystack.
- Cybercrime investigators are faced by the challenge of how to collect the specific, probative and case related information form huge groups of files.
- Another challenge is most of existing tools and methods allow anyone to alter any attribute associated with digital data.
- The specific data can be finding by techniques called text mining and data mining from very large group of files.
- On the network forensics side, there are many challenges. The networks may fall on multiple time zone and multiple jurisdictions all over the world and this makes it necessary to use absolutely trusted timestamps.
- The Network will be available in both offline and real-time modes, but the current set of computer forensics tools will not be able to handle the real-time and data size/volume.
- The real-time data collection is more complex because it may need to address legalities and privileges involved in surveillance, and must avoid inadvertent damage claims (such as server down condition).

5.8.1 Technical Challenges: Understanding the Raw Data and its Structure

- In digital forensics investigation there are two aspects of the technical challenges faced first is the "complexity" problem and the second is the "quantity" problem involved in a digital forensics investigation.
- The "complexity" problem is due to the data acquired typically in the lowest and most raw format, for non-technical people it is very difficult to understand.
- The "quantity problem" involves the hugeness of digital forensics to analyze data. It is inefficient to analyze every single piece of it. To solve this the Data reduction techniques used. Data reduction is done by grouping data into one larger event or by removing known data.

- The main aim of Digital forensics analysis is to accurately presenting all data at an appropriate layer of abstraction. ASCII is one basic example of abstraction.
- When the ASCII layer of abstraction is applied, the numerical values get mapped to their corresponding characters and the file is displayed as a series of letters, lines, nu rs and symbols. A text editor is an example of a tool operating at this layer of abstraction.
- FAT file system is one of the most basic file systems used for in many system, it has seven layers of abstraction.

  Layer 0: Raw file system image.

  Layer 1: File system image and values from Boot Sector and FAT Entry Size.

  Layer 2: FAT Area and Data Area.

  Layer 3: Starring Cluster, FAT Entries.

  Layer 4: Clusters, Raw Cluster Content and Content Type.

  Layer 5: Formatted Cluster Content.

  Layer 6: List of Clusters.

5.8.2 The Legal Challenges in Computer Forensics and Data Privacy Issues

- The Digital evidence can be easily duplicated or updated; often it can be without even leaving any traces
- Although digital evidence is not unique with regard to relevancy and materiality, there is still a challenge involved
- The digital evidence needs to satisfy the legal admissibility requirements. There is also the problem of locating the relevant evidence within very large amounts of data.
- Actually, the real challenges involve artificial limitations imposed by constitutional, statutory and procedural issues. Due to this we lose the goal of retrieving evidence.
- Data of digital nature can be very easily deleted or modify. One can save data to another platform also.
- The using special tools and techniques, one can identify and review data. If data is not properly recovered or analyzed, it not admissible in court of Law. Therefore, forensics investigators need to be careful in the matter of capturing the perceived evidence. They should understand that before they seize a computer or other electronic hardware they must consider whether they require a search warrant.

Summary

- The main aim of digital forensic is to find out digital evidence such as the evidence required establishing whether or not a fraud or a crime has been conducted.
- The data required for digital forensic examination by the law enforcement agency which includes investigation into E-mail usage, social media messages website

history, cell phone usage, cellular and voice over internet protocol phone usage, file activity history, file creation or deletion, chat history, account it login or logout record etc.

The main goal of digital forensic is to determine the value of a crime scene and related evidence.

Computer forensic is the collection of techniques and tools used to find evidence in a computer or digital devices.

Digital forensic is the use of scientifically derived and proven methods towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence.

A tremendously all technical capacity of modern computing devices provides unwanted use or misuse devices for committing crimes.

There are many challenges for the forensic investigator because storage devices are greeting very small in nature due to advance in electronic technology.

The term "chain of custody" is also used in most evidence situations to maintain the integrity of the evidence by proving documentation of the control, transfer and analysis of evidence.

Cyber forensic can be divided into two domains computer forensic and Network forensic

The Indian IT act amendment mention the electronic evidence is a new type of evidence.

You must know the Email component and the Email header structure for Forensic analysis of Email.

Every mail consists of two parts: Header and Body. The header of an Email is very important for forensic point of view.

The list main points from the Email header: "Received:" lines, MIME-version, Message-ID, DKIM Signatures, Return Path, Received-SPF, Authentication Results.

RFC 2822 is the internet message format standard that is that each email must have globally unique identifier.

Digital foreign evidence consists of exhibit. It useful for each member of jury to establish the facts of the case and support or refute legal theories of the case.

Forensic examiners are trained to follow a carefully developed set of protocols for acquisition of electronic evidence designed to ensure authenticity and assiduous chain of custody.

The forensic life cycle involves the following phases:

Preparation and identification of digital evidence, Collection and recording digital evidence, Storing and transporting digital evidence.

Examining or investigating digital evidence, Analysis, interpretation and attribution, Reporting, Testifying.

- Cybercrime investigators are faced by the challenge of how to collect the specific, probative and case related information form huge groups of files.
- In digital forensics investigation there are two aspects of the technical challenges faced first is the "complexity" problem and the second is the "quantity" problem involved in a digital forensics investigation.
- The real challenges in Data privacy involve artificial limitations imposed by constitutional, statutory and procedural issues. Due to this we lose the goal of retrieving evidence.

Check Your Understanding

1. Which of the following is not a role of Digital Forensic?
   (a) Uncover and document evidence and leaves.
   (b) Corroborate evidence discovered in other way.
   (c) Assist in showing a pattern of event using the data mining.
   (d) Eliminate incorrect assumptions.
2. Which point are/is mainly involved in the Scenario of digital forensic?
   (a) Abuse of internet by employee.
   (b) Unauthorized disclosure of corporate information and data.
   (c) Corporate spying activities.
   (d) All of the Above.
3. One can use the digital forensic technique to achieve _____.
   (a) Develop Digital signature
   (b) Verify Cyber Crime
   (c) Corroborate and verify evidence otherwise discovered
   (d) All of the above
4. Cyber forensic domains consist of _____.
   (a) computer forensic Authentication result
   (b) network forensic
   (c) Both (a) and (b)
   (d) http server
5. What type of context used to identify a piece of digital evidence?
   (a) logical context (b) legal context
   (c) physical context (d) All of the above

6. Which of the following is not the E-mail header attribute?
   (a) Authentication-Results (b) Received
   (c) HTTP (d) MIME
7. Which of the following is not a tag of DKIM header?
   (a) v (b) a
   (c) s (d) e
8. Which of the following is not the fundamental rule to remember the evidence?
   (a) is admissible (b) is authentic
   (c) is complete (d) is legal
9. _____ is not the phases involves in the forensic life cycle.
   (a) Examining or investigating digital evidence
   (b) Analysis, interpretation and attribution
   (c) Implementation.
   (d) Testifying.
10. _____ elements are considered preparation of report.
    (a) Identify the suitable reporting agency
    (b) Case identifier or submission number
    (c) Case investigator
    (d) All of the above

ANSWERS

1. (d)	2. (d)	3. (c)	4. (d)	5. (d)	6. (c)	7. (d)
8. (d)	9. (c)	10. (d)				

Practice Questions

Q1 Answer the following questions in short.

1. What is Digital forensic?
2. What is Digital Evidence?
3. Which is the context in world to identify a piece of digital evidence?
4. What are the phases involves in the forensic life cycle?
5. What are the practices to handle Digital Evidence?
6. Write the elements that are considered in preparation of Digital Forensics report.
7. What are the precautions to be taken when collecting electronic evidence?
8. What are legal Challenges in Computer Forensics?
9. Which are the fundamental rules to remember the evidence?
10. Explain the terms Return Path and Received-SPF from Email Header.

Q.II Answer the following questions.

1. What is the role of Digital Forensic?
2. Why there is need of Computer Forensic?
3. Explain the Rules of Digital Evidence.
4. What are the points involved in the digital forensic scenario?
5. How Forensics Analysis of Email done?
6. What is use of RFC 2822?
7. Explain the process model for understanding seizure and handling of forensic evidence legal framework.
8. Write a note on Digital Forensic Science.
9. What is Cyber forensics? Explain.
10. How data can be see using Forensic tools? Explain with Diagram.

Q.III Define the terms.

1. Cyber Forensics.
2. The digital forensic scenario.
3. Guidelines for collection of digital evidence.
4. DKIM Signatures.
5. Received By.
6. The Digital Forensics Process.
7. Reporting Phases in Computer Forensics/Digital Forensics.
8. Interpretation Phases in Computer Forensics/Digital Forensics
9. Technical Challenges in Computer Forensics
10. Network Forensic.

❖❖❖

6... Cybersecurity: Organizational Implications

Learning Objectives...

- To learn about major web threads faces by the organization.
- To understands why organization carful about Social computing.
- To understand the Intellectual Property Rights related to offences.
- To understand Cloud Computing Challenges.
- To understand the guidelines for safe computing.
- To appreciate Endpoint Security and Incident management system in organization.

6.1 ORGANIZATIONAL IMPLICATIONS: COST OF CYBERCRIMES AND IPR ISSUES

- In the global environment there is a continuous connectivity of internet, due to this there is possibility of cyber-attack from source that are local or remote.
- Due to the cybercrime there is a huge loss to the organization. The benchmark study shows that there are high cost related with malicious code, viruses and web attack.
- The frequency of cybercrime and success of cyber-attack that through the company firewall. This is a main reason for organization or company to worry about the cost of cybercrime.

6.1.1 Organizations have Internal Cost Associated with Cyber Security Incidents

- The internal cost of an organization basically include people cost, overhead cost and productivity losses.

6...

Cybersecurity: Organizational Implications

Learning Objectives...

- To learn about major web threads faces by the organization.
- To understands why organization carful about Social computing.
- To understand the Intellectual Property Rights related to offences.
- To understand Cloud Computing Challenges.
- To understand the guidelines for safe computing.
- To appreciate Endpoint Security and Incident management system in organization.

6.1 ORGANIZATIONAL IMPLICATIONS: COST OF CYBERCRIMES AND IPR ISSUES

- In the global environment there is a continuous connectivity of internet, due to this there is possibility of cyber-attack from source that are local or remote.
- Due to the cybercrime there is a huge loss to the organization. The benchmark study shows that there are high cost related with malicious code, viruses and web attack.
- The frequency of cybercrime and success of cyber-attack that through the company firewall. This is a main reason for organization or company to worry about the cost of cybercrime.

6.1.1 Organizations have Internal Cost Associated with Cyber Security Incidents

- The internal cost of an organization basically include people cost, overhead cost and productivity losses.

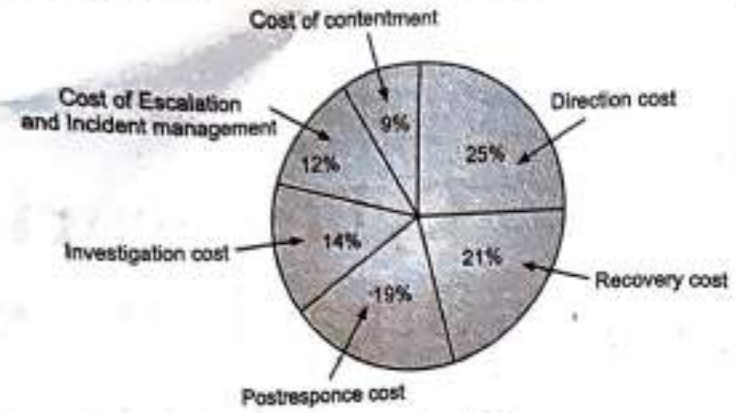

Fig. 6.1: Organizational Cost

- The cost of cybercrime where is based on the attack type, industry type and company size.
- In a global study it is found that the financial and defense sectors worldwide have more cyber-attack than any other organization.
- Following figure shows the consequences of cybercrime and their associated cost.

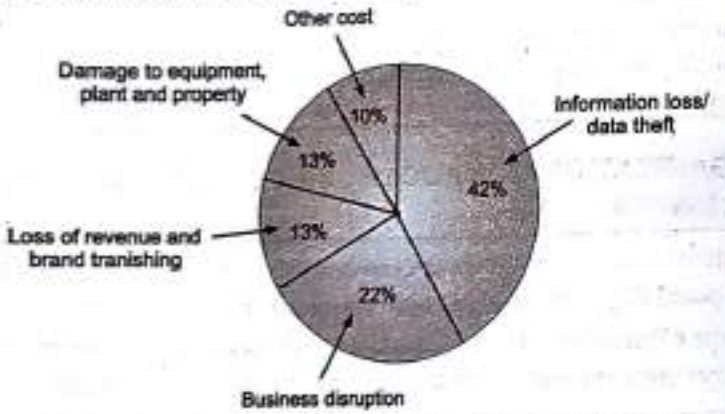

Fig. 6.2: Consequences of Cybercrime and their Associated Cost

- According to study the percentage of organizations impacted by various types of cybercrimes given below:
  1. Viruses, Worms Trojans 100%
  2. Malwares are 80%
  3. Botnets 73%
  4. Web-based attacks 53%

  5. Phishing and social engineering 47%
  6. Stolen devices 36%
  7. Malicious insiders 29%
  8. Malicious code 27%

- To protect data from cyber-attack the following points are to be considered:
  1. **Endpoint Protection:** This is generally ignore but must give the importance for example, IP based printers.
  2. **Secure Coding:** The practice of secure coding is important because that is a good practice to protect organization from malicious code inside the business applications.
  3. **HR Checks:** This is important before employment as well as after employment.
  4. **Access Controls:** This is important because will not allow shared ID and shared laptops. The access privileges must be given carefully to access the confidential and sensitive information.
  5. **Importance of Security Governance:** The good governance is essential for maintaining strong security posture in the company. Indirectly it reduce the crimes incident.

6.1.2 Organizations Implications of Software Piracy

- The software piracy is an Intellectual Property Rights (IPR) violation. The use of pirated software increases serious threats and risk of cybercrime and also computer security. This raise to legal liabilities, violation of copyright law, becomes criminal offence under the cyber Act.
- The use of unlicensed software or pirated software should be discouraged in the organization. The cybercriminals use non-genius computer software malfunctioning in computer.
- The non-genius software can basically disturb smooth functioning organization operations by majorly affecting system security infrastructure.
- Most often people use a pirated software for the following reasons:
  1. Pirated software's are cheaper and easily available.
  2. Many peoples from the organization or society uses pirated software.
  3. Latest and updated versions of pirated software are available.
- The organization should track software license to ensure that only genius copies are used. Also care should be taken that the number of installation is not more than the allowed number.

- If organization not follow rules then there may be a loss of data, confidentiality, integrity and also chance of reduce operational performance.
- The indirect thread to the organization for deploying of non genius software includes increase cost of protection and remediation.

6.2 WEB THREATS FOR ORGANIZATIONS

- The interconnection of web and internet grows the digital economy. Now a day the maximum business applications are web based and adopting the cloud computing concepts.
- The E-Commerce business grows using the web portals. Audio video contain are delivered from the web and corresponding infrastructure and software are delivered from the cloud, due this cyber criminal find it a convenient way to use the internet for cybercrime.

6.2.1 Overview of Web Threats to Organizations

- An internet make us busy. The large number of companies and also individuals has connection to the internet. Mobile internet is more popular in India. The chance of cyber thread for web trade gets increased. Workforce mobility poses challenges for IT manager whose main goal is to protect the business and business assets against the Malware. There is concern about keeping a band width continuously available for business and ensuring uptime of business application and website.
- The web thread can be categorized into two broad categories:
  1. Employees do a various activities online like visiting infected website, accessing pornographic sites, responding to spam mails.
  2. There are many challenges and difficulties in front of IT manager when it comes to manage web using in a secure and efficient way.
- The IT management find some challenges of the top issues are listed below:

1. **Employee time wasted on internet surfing:**
   - Organizations need to make a discipline to an employee for internet use by giving safe computing guideline or internet usage guideline. So it will reduce misuse of Internet.
   - However guidelines are not enough, employees wasting time online is a big issues for most the organization.
2. **Enforcing policy usage in the organization:**
   - An organization has different types of policies. Security policy is the statement produced by the senior management of organization, which help to maintain security inside the organization.

- Fig. 6.3 shows the policy hierarchy chart.

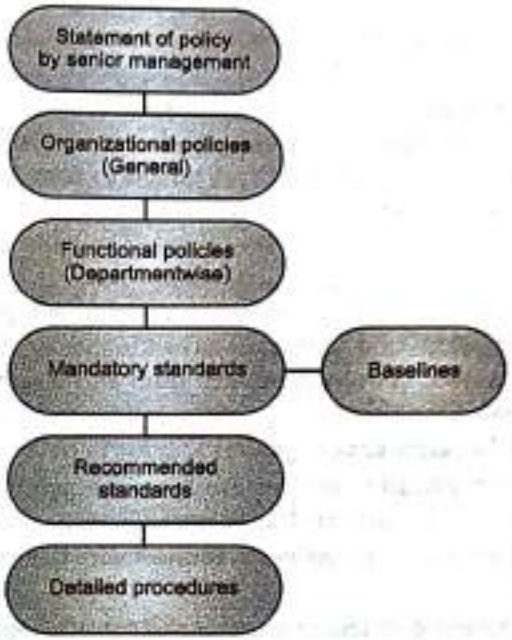

Fig. 6.3: Policy Hierarchy Chart

   - A good system allow a high level of control over the sides, the unwanted sites can be blocked and help to maintain an extensive database of website to ensure safety.

3. **Monitoring and controlling employee's internet surfing:**
   - Every organization controls the internet access to their employees by allowing to access a personal email in a specific time period like in a lunch time.
   - Using some tools organization can manage the web usage by employee by applying the techniques like cookies.
4. **Keeping security patches and virus signature up-to-date:**
   - It is very important and necessary for updating security patches and virus signatures in a regular basis.
   - Typically in house development the web filters, policy engine, spam and anti-malware system required regular updates to get good performance.
5. **Surviving in the era of legal risk:**
   - The employee from the company is visited to inappropriate or offensive website without knowing the company authority. The company director are responsible when employees access pornography website or download pirated softwares. The

organizations are worried about this kind of employees because directors can personally be held liable.

- The organization with effective web filtering and monitoring system may reduce risk.

6. **Bandwidth wastage issue:**
   - Today's applications contain more messages, audio, video contain so it require huge bandwidth. Many of unwanted applications or not required in organization are also downloaded bandwidth usage increases.
   - With the increasing of social networking and the trend towards the social media & the audio video sites, bandwidth requirement is more.
   - The organization should control the bandwidth usage in work hours, so that they can save the bandwidth and ultimately save the money. Also organization can block banned websites, downloads, email, spam and media stream to avoid the bandwidth wastage.
7. **Mobile workers pose security challenges:**
   - Many mobile communication devices like Personal Digital Assistant (PDA) have raise security issues associated with their use.
   - The mobile workers use those devices to connect with their office networks when they are outside.
   - Even if company having system to monitor and control web access and to protect web users from malwares, system they are not capable to cover remote users working on laptop or PDA.
   - Organization needs tool that extend web protection and filtering for remote side users also.
8. **Challenges in controlling access to web applications:**
   - Many organizations have their applications on web. In the future as internet offers wide range of online applications, from webmail or social networking. Cloud computing as huge market in provide online services. At time of development or maintenance online applications the employee often bypass the corporate guideline on security issue. They use the personal email for communication purpose like sending or uploading company data. Afterward it is very difficult to control the access of web. The organization need to decide what type of access control should give to employee.
9. **The bane of Malware:**
   - Many websites contain Malware. Such websites may create security problems. Now most of the organizations are blocking such sites, which declared dangerous. But attacker changes their techniques rapidly to avoid Malware detection.
   - The Malware may create a security issue, now organizations use anti-malware tools.

10. **The need for protecting multiple offices and locations:**
    - An internet connects entire word together. Organization may have various offices worldwide and they can deliver single project from the multiple locations.
    - Protecting information security and data privacy at multiple sites is indeed a major issue to the organization.
    - To overcome this problem the internet base service that can be easily protect many offices worldwide.

6.3 SECURITY AND PRIVACY IMPLICATIONS FROM CLOUD COMPUTING

- There are some issues related to the cloud computing that is, how data handle on cloud?, how and which data encryption methods use?, Who will liable for data integrity and privacy?.
- Basically storing data in cloud main impact the privacy rights, publications and status.
- Organization should think about the privacy scenario in terms of user spheres. There are three kinds of Spheres, their characteristics are as follows:

1. **User Sphere:**
   - In this sphere, data is store on computer, laptop, mobile phone, Radio Frequency Identification (RFID) chips. The organizations responsibility is to give access to users and monitor that access to ensure misuse of data should not happen. There are many challenges related to data storing, transferring from client to data recipient, media of transferring, security issues related to transferring and storing.
2. **Recipient Sphere:**
   - In this sphere, data lies with recipient. Data Share to Servers, network providers, service providers or other parties. In this sphere organizations should minimize user's private risk in data handling by ensuring that unwanted exposure of private data of user do not happened.
   - The challenges in this sphere are: what type of data is shared by data recipient with other parties? Can the user expects on anticipate or transfer of data by the recipient? Is personal data adequately secured? Is there is a way to reduce processing? Is data storage transient or persistent?
3. **Joint Sphere:**
   - In this sphere, data lies with web services provider's servers and databases. In this sphere it is not clear that, to whom the data belong. The challenges in this sphere are: Is the user fully aware of how personal data is used and can individual control this?

6.4 SOCIAL MEDIA MARKETING

- The social computing and social media marketing are same. Importance of social media is faster growing. According to the 2020 survey by marketing professionals, usage of social media sites by large Business to Business (B2B) organization shows the following:
  1. LinkedIn is used by 76% of the organizations.
  2. Facebook is used by 66 % of the organizations.
  3. Twitter is used by 29% of the organizations.
  4. Instagram use by 17 % of the organizations
  5. YouTube used by 11 % of the organizations.
- The data breach offences and data stealing incidents are uncontrolled in most of other countries. Cybercriminal are on watch on sensitive information and they will take the advantages of that information. India has a big usage of internet due to this security breach incidents on the raise. Hackers use a number of internet channels such as Web, E-mail, Instant Messaging, Voice Over Internet Protocol etc. Hackers steal the information for their financial benefits. The Phishing is major threat for the organizations.
- The social media marketing is approach that makes organization to promote products and their services to the user.
- Following figure shows Social Media Online Tools.

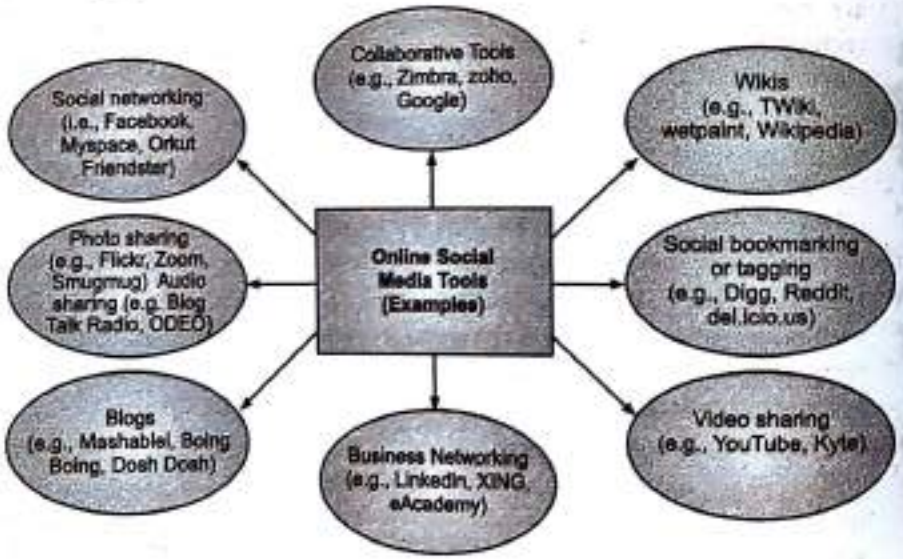

Fig. 6.4: Social Media Online Tools

6.4.1 Understanding Social Media Marketing

- The boost to social media marketing has happened due to growth of the internet.
- Social media marketing uses a number of tools and technologies to reach a large number of users.
- Following are the reasons, why the organizations use the social media marketing to promote their product and services:
  1. To reached to a large number of users fastly.
  2. To increase the traffic of their website by using blogs, social and business networking, so that they will increase their page rank.
  3. To garb other potential revenue benefits and reduces the advertising cost.
  4. To build credibility by participating in relevant product promotion forum and solve customer queries immediately.
  5. To collect rotational customer profile.

6.4.2 Best Practices with use of Social Media Marketing Tools

- It is very important to every organization to establish a social media policy.
- The use of personal blogging for office work related activities should be monitored and minimized.
- Providing continuous information about new security threats and maintaining rules to employees. Network security administrator need to remain up-to-date about the most recent risk on the web.
- The best data access policies reduce the release of information for the money into wrong hand through unauthorized channels.
- The blocking of infected website is the necessary activity in best practice.
- Firewall helps to protect the organization data and using the next generation firewall in organization to keep the security technology up-to-date.
- Protection against vulnerability is possible by carefully planning and vulnerability scanning because vulnerability is a very big challenge to the corporate network.
- The only 'need based' access should be defined for business applications those are on corporate networks or external sites.
- Organizational best practices are listed below:
  1. Organization must have wide policy of information system.
  2. Risk assessment and management.
  3. Configuration / Change control and management.
  4. Security awareness and training to employees.
  5. Standard software configuration that follows the system security policy.
  6. Contingency planning and disaster recovery planning.
  7. Certification and accreditation.

6.5 SOCIAL COMPUTING AND THE ASSOCIATED CHALLENGES OF ORGANIZATION

- The social computing is differ from individual networking and entertainment. It helps thousands of people all over the world to support their work, health, learning, getting entertained and citizenship in different innovative ways.
- With social computing there are different threads involved related to security, safety and privacy.
- If you see, a social computing is related to social media marketing because every business leads in product development, marketing and sale.
- Recommendation is to take special care while using social computing for communicating with internal or external stakeholders such as employee, customer and suppliers.

6.5.1 Protecting People's Privacy in the Organization

- The human issues in privacy and security are the most complex part. Human tendency caused many evils, data theft related to the cyber security context.
- United State Social Security Number (SSN) is used for uniquely identifying all American citizens.
- Similarly in India UID project was started by government. The agency "Unique Identification Authority of India" working on it.
- Aadhar card is the one of the unique identity of Indian people developed by the government of India.

6.6 ORGANIZATIONAL GUIDELINES FOR INTERNET USAGE, SAFE COMPUTING GUIDELINES AND COMPUTER USAGE POLICY

- The organization recognizes that there is a need for protecting the company's identity when online. Every time in employee access the internet, employee may leak data to watch full company competitors. Also Hacker and online predator's leak company data. In such cases organization needs effective solution.
- Organization must develop safety computing guidelines, which may referred to as Organizational Guidelines for the internet usage or computer usage policy.

6.6.1 Developing an Organizational Policy for Computer Usage

- The computer usage policies are focus on following elements:
  - **Mission statement:** The policy should briefly introduce about the organizational mission.
  - **Introduction:** This section should explain content of the policy documents.
  - **Internet Safety:** This section focuses on the technology protection measures.

  - **Confidentiality:** This focus on safe computing information remains confidential.
  - **User responsibilities:** This section mentions the user responsibilities of the safe computing policy.
  - **Disciplinary action for privacy violation and declaimer:** This focus on who violates the computer usage policy, the action should take against.
  - **Miscellaneous:** Apart from above points, the other relieving point should also be specified. Like how long the facility can be used, rule about any ancillary services provider such as printing facility.

6.7 INCIDENT HANDLING

- It is important to have any incident handling, incident response system and structuring the incident response team.

6.7.1 Definitions and Terms

- An incidence is defined as the act of violating an explicit or implicit security policy. Another definition is, any adverse event, which compromise some aspect of computer on network security.
- The definition of incident management is preventing and handling computer security incidence.
- We know the cyber security means protecting information, devices, computer and its resources modification or destruction. This definition provides security in terms of both hardware and software.
- The three important **terms of incident**:
  1. Incident response.
  2. Incident handling.
  3. Incident management.
- These three terms having the relation with each other.
- The incident management activities are performed by:
  1. Computer Security Incident Response Team (CSIRT)
  2. Information Technology Group (IT)
  3. The Security Group
- The **classification of incident** as follows:
  1. **IT security incident:**
     - Illegal usage of organizations asset or resources.
     - Change made with IT systems or controls.
     - Spam and mail forgery.
     - Use of pirated software.

- Downloading unauthorized materials which may infected with viruses Trojan or worms.
- Denial of services.
- Unauthorized sharing of system or application password sharing.

2. **Data incident or data privacy incidents:**
   - All instances of the loss, theft, missing, confidential data, client information, and unattended storage devices like laptop, USB, CD.
   - Unauthorized disclosure or misuse organization data or information.
   - Misuse of customer Personal Id (PI), credit card information or email.
   - Manipulating customer email address for negative purpose.

- The **priority of incidents** are given below:
  1. **High priority incidents:** This incidents having huge impact on the organizational business or services and its customers.
  2. **Medium priority incidents:** This incidents have a significant impact or have potational impact on organizational business or services to customer.
  3. **Low priority incidents:** This incident has impact on the organizational business or service to customers.

6.7.2 Why should Organizations have Incident Response System?

- It is necessary to have incident response system because cyber-attacks frequently cause the compromise of personal and business data.
- Quickly and effectively deface the cyber-attack response system is required. To address threads, the concept of computer security incident response has become widely accepted and implemented in the Federal Government.

6.7.3 Example of Cyber Security Incidents and Information Technology Infrastructure Library (ITIL) Perspective

- Following are the cyber security incident examples:
  1. **Unauthorized access:** An attacker runs special tools to gain access to servers password file. After getting accessing to system file, he may misuse the sensitive data.
  2. **Inappropriate usage:** A user provides illegal copies of software to other through peer to pair file sharing system, a person threatens another person by sending the emails.
  3. **Denial of service:** An attacker sends especially crafted packets to a web server, causing it to crash.
  4. **Malicious code:** Warm use open file shares to quickly infect several hundred work stations within an organization.

6.7.4 What Organization can do to protect their systems from Cyber Security Incidents?

- Every organization needs to protect their information system from the malware through their current IT security planning, management and implementation activities.
- Organization also needs to protect business sensitive information and personal information.

6.7.5 Best practices for organizations

- The organization should do the following best practices against the thread of malwares:
  1. Develop and implement an approach to Malware incident prevention which based on the attack type.
  2. Develop and implement policies that support the prevention of Malware incident by conducting awareness program for user and IT staff.
  3. The awareness program provides the guideline and training to the user so that users are alert to the ways that Malware spread.
  4. The Malware incident can prevent through documented policies, technical process and procedure.
  5. Established thread mitigation capability to assist in containing Malware incidents by detecting and stopping Malware before it can affect the system.
  6. Develop a robust incident response process capability that addresses Malware incident, handle incident through preparation, detection and analysis.
  7. Established Malware incident prevention and handling capability that addresses current and short term future threads that are robust and flexible.

6.7.6 Incident Response Team Work, Capability and Structure

- To handle the incident in using proper method, the incident response team needs to be form.
- The success of team is about skill, competencies, capability and training.
- The response team is responsible for dealing with potential or real information security incident. In response structure an individual can effectively serve as the coordinator of efforts by number of peoples.
- After handling incident, other people involved in the incident are release from their responsibility of that incident.
- The response team has day to day responsibility of handling the incident and we'll always ready to deal with the next incident that may occur in the future.

6.7.7 Benefits from Incident Response System

- The following are the benefits from implementing an effective Incident Response System:
  1. Organization has the ability for responding to incidents in a systematic way, so that accurate steps are taken.
  2. There is a method to help personal to recover quickly and effectively from incident. This method useful to minimize the loss and theft of the information, also reduce disturbance of services.
  3. The information collected while handling the incident that can be used for future incident handling and can provide a strong protection for system and data.
  4. Properly handling the incident will improve user satisfaction.
  5. More efficient utilization of service desk and other staff in incident handling.
  6. Enhance ability to measure and monitor it performer's related Service Level Agreement (SLA).
  7. Better data to support executive decision regarding service quality.
  8. Improved ability to track incident and service request efficiently.

6.7.8 Checklists

- To handle the incident response checklist is useful in the organization.
- Following are the checklists use to handle incident:
  - Checklist for initial handling of incident.
  - Generic checklist for incident handling.
  - Checklist for handling DoS incident.
  - Checklist for handling malicious code incident, unauthorized access, inappropriate usage, multiple component incident.
  - Long review checklist for security incident.
  - Computer incident reporting form.

6.8 INTELLECTUAL PROPERTY IN THE CYBERSPACE OF CYBER SECURITY

- Intellectual Property (IP) is a term referring to creation of the intellect (the term used in studies of the human mind) for which a monopoly (from greek word *monos* means single polein to sell) is assigned to designated owners by law.
- In some foreign countries intellectual property rights is referred to as industrial property, copyright, patent and trademarks, trade secrets. All these cover music, literature and other artistic works, discoveries and inventions and words, phrases, symbols and designs.

- Intellectual Property Rights (IPR) are themselves a form of property called Intangible property.
- Types of Intellectual Property: The term intellectual property is usually thought of as comprising six separate legal fields:
  1. Copyrights
  2. Patents
  3. Trademarks
  4. Trade Secrets
  5. Trade Name
  6. Domain Name

1. Copyrights

- The general definition of copyright "Copyright owner", with respect to any one of the exclusive rights comprised in a copyright, refers to the owner of that particular right.
- Copyright is a form of protection provided by U.S. law to the authors of "original works of authorship" fixed in any tangible medium of expression. The manner and medium of fixation are virtually unlimited. Creative expression may be captured in words, numbers, notes, sounds, pictures, or any other graphic or symbolic media.
- The subject matter of copyright is extremely broad including literary, dramatic, musical, artistic, audiovisual, and architectural works.
- Copyright protection is available to both published and unpublished works. Copyright protection is available for more than merely serious works of fiction or art.
- Marketing materials, advertising copy and cartoons are also protectable.
- Copyright is available for original works. But certain works are not protectable by copyright such as titles, names, short phrases, or lists of ingredients. Similarly, ideas, methods and processes are not protectable by copyright, although the expression of those ideas is.
- Copyright protection exists automatically from the time a work is created in fixed form. The owner of a copyright has the right to reproduce the work, prepare derivative works based on the original work (such as a sequel to the original), distribute copies of the work, and to perform and display the work. Violations of such rights are protectable by infringement actions. Nevertheless, some uses of copyrighted works are considered "fair use" and do not constitute infringement, such as use of an insignificant portion of a work for noncommercial purposes or parody of a copyrighted work.
- Copyrighted works are automatically protected from the moment of their creation for a term generally enduring for the author's life plus an additional seventy years after the author's death. The policy underlying the long period of copyright

protection is that it may take several years for a painting, book, or opera to achieve its true value, and thus authors should receive a length of protection that will enable the work to appreciate to its greatest extent.

2. Patents

- A patent for an invention is the grant of a property right to the inventor which is issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions. Under certain circumstances, patent term extensions or adjustments may be available.
- The right conferred by the patent grant is, in the language of the statute and of the grant itself, "the right to exclude others from making, using, offering for sale, or selling" the invention in the United States or "importing" the invention into the United States.
- Once a patent is issued, the patentee must enforce the patent without aid of the United States Patent and Trademark Office (USPTO).
- There are three types of patents:
  1. **Utility patents** may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.
  2. **Design patents** may be granted to anyone who invents a new, original, and ornamental design for an article of manufacture.
  3. **Plant patents** may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plants.
- The domain of "software patent" is most infested with trouble because software patent does not have a universally accepted definition.
- Software patents involve the following important issues:
  1. Whether software is "patentable."
  2. Whether software can be considered as "piece of invention."
  3. Whether software patents encourage or discourage "innovation."
- The issue is simpler when it comes to business method patents. These are a class of patents that disclose and claim new methods of doing business. This includes new types of E-Commerce, insurance, banking, tax compliance, etc.
- Patent protection exists for twenty years from the date of filing of an application for utility and patents and fourteen years from the date of grant for design patents. After this period of time, the invention fall into the public domain and may be used by any person without permission.

- The inventor is granted an exclusive but limited period of time within which to exploit the invention. After the patent expires, any member of the public is free to use, manufacture, or sell the invention. Thus, patent law strikes a balance between the need to protect inventors and the need to allow public access to important discoveries.

3. Trademarks (Service Marks)

- A trademark or service mark is a word, name, symbol, or device used to indicate the source, quality and ownership of a product or service. A trademark is used in the marketing is recognizable sign, design or expression which identifies products or service of a particular source from those of others.
- The trademark owner can be an individual, business organization, or any legal entity. A trademark may be located on a package, a label, a voucher or on the product itself. For the sake of corporate identity trademarks are also being.
- General Logos:

TM ®

- The Trademark Registration Logo of IBM:

Infosys IBM

- A trademark registration is valid for 10 years and may be renewed for additional 10 year periods thereafter as long as the mark is in used in interstate commerce.
- The registrant is required to file an affidavit with the Patent and Trademark Office (PTO) between the 5th and 6th years after registration and every 10 years to verify the mark is in continued use.
- Marks not in use then are available to others. A properly selected, registered and protected mark can be of great value to a company or individual desiring to establish and expand market share and better way to maintain a strong position in the marketplace.
- A service mark is the same as a Trademark, except that it identifies and distinguishes the source of a service rather than a product.

4. Trade Secrets

- A trade secret consists of any valuable business information. The business secrets are not to be known by the competitor.
- There is no limit to the type of information that can be protected as trade secrets; For Example, Recipes, Marketing plans, Financial projections, and Methods of conducting business can all constitute trade secrets.

- There is no requirement that a trade secret be unique or complex; thus even something as simple and nontechnical as a list of customers can qualify as a trade secret as long as it affords its owner a competitive advantage and is not common knowledge. If trade secrets were not protectable, companies would no incentive to invest time, money and effort in research and development that ultimately benefits the public.
- Trade secret law thus promotes the development of new methods and processes for doing business in the marketplace.
- The trade secrets may last forever. On the other hand, if companies fail to maintain the secrecy of the information, trade secret protection may be lost.
- The companies protect the secret or valuable information is by requiring employee to sign agreements promising not to compete with the employer after leaving the job.

5. Trade Name or Business Name

- A "Trade Name," also known as a "trading name" or "business name," or "assumed name" or "corporate name" is the name that a business trades under for commercial purposes. A Trade name is registered legal name is used for contracts.
- A "Trade Name" identifies the business itself whereas a "Trademark" identifies goods or services or products.
- In some situations, it may be possible that a "Trade Name" can also serve as a "Trademark" if it meets the necessities of a "Trademark." For example, "Parle" is an organization as well as a brand name.
- There are no exclusive rights associated with a Trade Name unless it is used as a Trademark.

6. Domain Name

- Every computer on the Internet has a unique identification number, called an Internet Protocol address (32-bit numeric address). Computers use IP address to find an Internet site.
- Internet Protocol addresses, are "mapped" by the Domain Name System (DNS) to domain names that contain words.
- A domain name is the identity of one or more IP addresses. For example, the domain name google.com points to the IP address "74.125. 127.147". Domain names are invented as it is easy to remember a name rather than a long string of numbers.

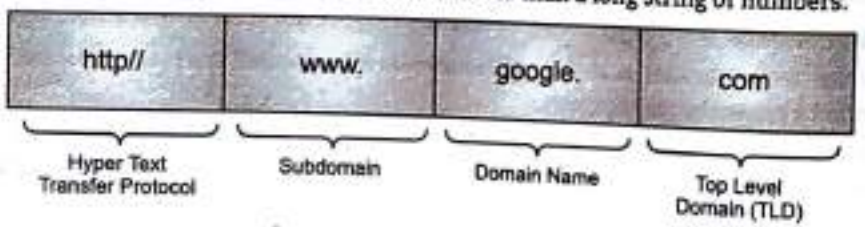

Fig. 6.5: Uniform Resource Locator

- The registration of a domain name does not in itself confer proprietary rights to the use of that domain name. Associated with domain names is a concept of "cybersquatting."
- The term **cybersquatting** refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names.
- Cybersquatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner. Both the federal government and the Internet corporation for assigned names and numbers have taken action to protect the owners of trademarks and businesses against cybersquatting abuses.
- The primary example of anti-cybersquatting legislation is the Anti-cybersquatting Consumer Protection Act (ACPA). The ACPA is a federal law that prohibits domain name registrations that are identical or similar to trademarks or personal names.

Summary

- In the global environment there is a continuous connectivity of internet, due to this there is possibility of cyber-attack from source that are local or remote.
- The cost of cybercrime where is based on the attack type, industry type and company size.
- The software piracy is an Intellectual Property Rights (IPR) violation.
- The non-genius software can basically disturb smooth functioning organization operations by majorly affecting system security infrastructure.
- The interconnection of web and internet grows the digital economy.
- The IT management fined some challenges and solutions of the top issues are: Employee time wasted on internet surfing; Enforcing policy usage in the organization; Monitoring and controlling employee's internet surfing; Keeping security patches and virus signature up-to-date; Surviving in the era of legal risk; Bandwidth wastage issue; Challenges in controlling access to web applications; The bane of Malware ; The need for protecting multiple offices and locations.
- There are some issues related to the cloud computing. Basically storing data in cloud main impact the privacy rights, publications and status.
- Organization should think about the privacy scenario in terms of user spheres, there are three kinds of Spheres, User Sphere, Recipient Sphere and Joint Sphere.
- The social computing and social media marketing are faster growing.
- It is very important to every organization to establish a social media policy.
- Firewall helps to protect the organization data and using the next generation firewall in organization to keep the security technology up-to-date.

- Organization must develop safety computing guidelines, Which may referred to as organizational guideline for the internet usage or computer usage policy.
- The three important terms of incident: First incident response, Second incident handling and Third term is incident management.
- The organization should adopt the best practices against the thread of malwares.
- The response team is responsible for dealing with potential or real information security incident. In response structure an individual can effectively serve as the coordinator of efforts by number of peoples.
- The organization will get benefits after implementing an effective incident response system.
- Types of Intellectual Property : 1. Copyrights, 2. Patents, 3. Trademarks, 4. Trade Secrets, 5. Trade Name, 6. Domain Name.
- There are three types of patents: Utility patents, Design patents and Plant patents.
- A trademark or service mark is a word, name, symbol, or device used to indicate the source, quality and ownership of a product or service. A trademark is used in the marketing is recognizable sign, design or expression which identifies products or service of a particular source from those of others.
- The term cybersquatting refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names.

Check Your Understanding

1. The internal cost of an organization basically include _____.
   (a) people cost (b) overhead cost
   (c) productivity losses (d) All of the above
2. There is no negative impact on organization from the following type _____.
   (a) Virus (b) Malwares
   (c) Phishing (d) DNS
3. Which points are to be considered to protect data for cyber-attack?
   (a) Endpoint protection (b) HR checks
   (c) Access Controls (d) All of the above
4. _____ important because will not allow shared ID and shared laptops.
   (a) Access Controls (b) Hr Check
   (c) Secure coding (d) Endpoint protection
5. _____ is important before employment as well as after employment.
   (a) Access Controls (b) Hr Check
   (c) Secure coding (d) Endpoint protection

6. ____ spheres data lies with web services provider's servers and databases.
   (a) User sphere (b) Joint Sphere
   (c) Recipient Sphere (d) None of the above.
7. The Data incident include _____.
   (a) Misuse organization data (b) Misuse of customer
   (c) Manipulating customer email (d) All of the above
8. IT security incident includes _____.
   (a) Misuse organization data (b) Misuse of customer
   (c) Denial of services (d) Manipulating customer email
9. _____ code warm use open file shares to quickly infect several hundred work stations within an organization.
   (a) Malicious (b) Un-authorized
   (c) Inappropriate usage (d) business
10. _____ protection is available to both published and unpublished works.
    (a) Patent (b) Copyright
    (c) Trademarks (d) Trade Name
11. _____ may be granted to anyone who invents or discovers any new and useful process, machine.
    (a) Design patent (b) Plant patent
    (c) Utility patent (d) None of the above
12. A "Trade Name," also known as _____.
    (a) a "trading name" (b) a "business name,"
    (c) a "assumed name" (d) All of the above

ANSWERS

1. (d)	2. (d)	3. (d)	4. (a)	5. (b)	6. (b)	7. (d)
8. (c)	9. (a)	10. (b)	11. (c)	12. (d)		

Practice Questions

Q.I Answer the following questions in short.

1. What are the reason people uses pirated software?
2. Write the ways that web thread can be categorized?
3. What is the enforcing policy usage in the organization?
4. What is Bandwidth wastage issue?
5. Write the security issues related to the cloud computing.
6. Explain the usage of social media sites by large business to business (B2B) organization.

7. Why the organizations use the social media marketing to promote their product and services?
8. What is the organizational policy for computer usage?
9. What is Incident Handling? Write its important terms.
10. What is the priority of incidents?
11. Why should organizations have incident response system?
12. Write the checklists that use to handle incident.
13. What are the issues involved in Software patents?

Q.II Answer the following questions.

1. What are the consequences of cybercrime and their associated cost?
2. What are various types of cybercrimes that impacted organization?
3. Which points should be considered to protect data for cyber-attack?
4. What are top issues that IT management having challenges? Explain any two.
5. What are kinds of Spheres? Write their characteristics.
6. Explain the best practices with use of social media marketing tools.
7. What are social computing and the associated challenges of the organization?
8. Explain the cyber security incident examples.
9. Explain the best practices of the organization that following against the thread of malwares.
10. What is use of Domain Name? Explain with example.
11. Explain in brief each type of Intellectual Property.

Q.III Define the terms.

1. Domain Name
2. Cybersquatting
3. Software Piracy
4. Secure coding
5. Access controls
6. Malware
7. User sphere
8. Recipient Sphere
9. Joint sphere
10. Social Computing
11. Incident Management
12. Denial of service
13. Malicious code
14. Copyrights
15. Patents
16. Trademarks
17. Trade secrets
18. Trade Name
19. Domain Name

❖❖❖

7... Cybercrime: Illustrations, Examples and Mini-Cases

Learning Objectives...

- To relate the examples, illustrations and mini-cases provided here to the cybercrime categories.
- To learn the practical scenarios of how criminals/fraudsters use methods, tools and techniques.
- To understand how real-life instances of cyber-crimes can impact individuals and organizations if due care is not taken.

7.1 INTRODUCTION

- In the previous chapters you have learnt various categories of cybercrimes, the tools and techniques used by cybercriminals as well as the forensics and legal aspects involved.
- In this chapter some mini-cases, examples and illustrations are discussed which will help you to appreciate the seriousness and implications of computer crime. The mini-cases, examples and illustrations presented here are cybercrime incidents that have taken place in India as well as other countries.

7.2 REAL-LIFE EXAMPLES

- In this section some real-life examples are discussed.

Example 1: Business Liability through Misuse of Organization's Information Processing Assets.

- Criminals can create false E-Mail IDs to perform crime. This is a real-life example where criminal create fake E-Mail Id.

7...

Cybercrime: Illustrations, Examples and Mini-Cases

Learning Objectives...

- To relate the examples, illustrations and mini-cases provided here to the cybercrime categories.
- To learn the practical scenarios of how criminals/fraudsters use methods, tools and techniques.
- To understand how real-life instances of cyber-crimes can impact individuals and organizations if due care is not taken.

7.1 INTRODUCTION

- In the previous chapters you have learnt various categories of cybercrimes, the tools and techniques used by cybercriminals as well as the forensics and legal aspects involved.
- In this chapter some mini-cases, examples and illustrations are discussed which will help you to appreciate the seriousness and implications of computer crime. The mini-cases, examples and illustrations presented here are cybercrime incidents that have taken place in India as well as other countries.

7.2 REAL-LIFE EXAMPLES

- In this section some real-life examples are discussed.

Example 1: Business Liability through Misuse of Organization's Information Processing Assets.

- Criminals can create false E-Mail IDs to perform crime. This is a real-life example where criminal create fake E-Mail Id.

- In one bank, a management trainee of the bank was engaged with a girl working in the same bank. They were to get married in due course of time. During the post-engagement period, the couple exchanged many E-Mails. The boy and the girl used to write the mails during work hours using the company computers. Unfortunately, after some time the relationship went in trouble and the two broke up. The girl created fraudulent E-Mail IDs such as "indianbarassociations". She used that ID to send E-Mails to the boy's foreign clients. The girl used the bank's computer for sending these mails. The mails had negative publicity about the bank. The boy lost a large number of clients assigned in his portfolio. Those clients accuse the bank for doing something illegal. The bank was held accountable for the E-Mails sent using the bank's system.
- This example is a lesson for organizations that they must have well-established computing guidelines in organizations. Organization must watch strictly their computing and communication facilities are being used.

Example 2: The "Piranhas" Tragedy with Children.

- This is the example based on the crime called Web Jacking. In Web Jacking, cybercriminal create a fake page of victim website.
- This incident was reported in the US. There was a hobby website for children. The owner of the site received an E-Mail informing her that a group of hackers had gained control over her website. They demanded a payment of one million dollars from her. The owner was a school teacher. She did not pay due attention to that (threatening) mail because she did not think it was serious. She thought it was just a scare tactic and so she simply ignored the E-Mail. After about three days, she started getting several telephone calls from almost all over the country and then she came to know that the hackers had really web jacked her website. The hackers had altered a portion of the website which was entitled "How to have fun with goldfish." They had replaced the word "goldfish" with the word "piranhas." Piranhas are tiny but extremely dangerous flesh-eating fish. Because of that many children who visited that website believed the contents of the website. Hence, the children followed the instructions and try playing with piranhas fish, which they bought from pet shops and were very seriously injured.

Example 3: E-Mail Bombing Involving a Foreigner.

- This is an example of E-Mail bombing. A foreigner had been residing in Shimla, India for almost 30 years. He wanted to avail a scheme that was introduced by the Shimla Housing Board to buy land at lower rates. His application, however, was rejected on the grounds that the scheme was available only to Indian citizens. The foreigner decided to take revenge. He transmitted thousands of mails to the Shimla Housing Board. He did not stop there. He kept on sending E-Mails till their servers crashed.

Example 4: Pune City Police Bust Nigerian Racket.

- This example shows how even an educated person working in technology field get fooled by the criminal and suffered a big financial loss. It also shows the greed of criminals.
- This fraud happened when the police started probing into a complaint received from a young software engineer working in Pune city. Arjun, a resident in Warje area, was duped with 10.27 lakhs by making him believe that he was going to be offered a high profile job in a London hotel called New Climax.
- In an E-Mail chat with an alleged UK-based Councillor, Arjun was convinced to pack up and leave India for UK. The fraud got exposed when Arjun found that there was no flight to UK. The efforts expended by police were successful and two criminals, including a bank account holder, were arrested. However, the real mastermind Chong-Ching, who is a foreign national, was still absconding. The accused have been charged under various sections of the IPC (Indian Penal Code) and the Indian IT Act.
- The fraud started with the mail Arjun received. In that mail he was offered a job in UK-based hotel "New Climax." A person calling himself Chong-Ching claimed to be authority at the hotel and offered to victim the post of Sales Supervisor with a handsome UK salary. The victim responded to the E-Mail and accepted the offer. There onward, the correspondence continued. In another E-Mail, a person called John Smith Levis introduced himself as UK councillor. John claimed to have been given the responsibility by the hotel to provide Visa. To get the Visa and to pay for journey expenses and accommodation in the UK, John asked the victim for various amounts of money in a number of E-Mails. John gave to the victim several account numbers in different branches of Axis Bank and ICICI Bank. Victim Arjun deposited a total amount of 10.27 lakhs.
- According to the E-Mail, the victim was supposed to catch a flight from Mumbai and a person was going to meet Arjun at the airport with a Visa and an air ticket. During the correspondence, receipts with fake stamps (as it turned out later) and signatures of the British High Commissioner were sent to victim. When victim (Arjun) reached the airport, he found that there was no such person waiting for him. That is when the victim realized that he had been cheated. Arjun returned to Pune and tried to contact the concerned person but the concerned person never replied to his mails. Arjun then decided to approach the police. The investigation revealed that someone hailing from Nigeria asked them to commit the crime.

7.3 MINI-CASES

- In this section some real-life mini-cases are discussed.

Mini-Case 1: Internet Time Stealing.

- This is the case of "Theft of Internet Hours". The fraud described in this case could be detected due to victim's alertness.
- Colonel Bajwa, a resident of New Delhi, asked a nearby net cafe owner to visit for re-installing his Internet connection. For this purpose, the net cafe owner needed to know his username and password. After setting up the connection, the cybercafe owner walked away with the username and password noted down. He then sold this information to another net cafe. After about a week, Colonel Bajwa discovered that his Internet hours were almost over. Out of the 100 hours that he had purchased, more than 90 hours had been used up within the span of that week. He noted that this had happened although he was inactive in that week in terms of his use of the Internet from that connection that was set up with the help of the net cafe owner. Colonel Bajwa reported the incident to the Delhi Police. The Police could not believe that time could be "stolen" because they were not aware of the concept of "time-theft" at all. They could not understand how something "immovable" such as the Internet "hours" could be stolen and so they rejected Colonel Bajwa's report. Colonel Bajwa was not willing to give up and he decided to approach The Times of India, New Delhi. They, in turn, prepared a report about the shortfall of the New Delhi Police in handling cybercrimes. The Commissioner of Police, Delhi took charge of the case and the police under his directions raided the cybercafe and arrested the owner under the charge of theft as defined by the Indian Penal Code. The net cafe owner spent several weeks locked up in jail till the bail was granted.

Mini-Case 2: Indian Cyberdefamation Case of a Young Couple.

- Sujata, a young girl, was about to get married to Sudesh whom she met during a social event. Sudesh seemed to be open-minded and pleasant. They used to meet quite often during the pre-marriage period. One day when Sujata met Sudesh, he looked worried and even a little upset. He did not seem interested in talking to her. When she asked, he told her that members of his family had been receiving E-Mails that contained malicious stories about Sujata's character. Some of them were of her past affairs. He told her that his parents were very upset. Sudesh told Sujata that his parents were considering breaking off the engagement. Sujata was shocked obviously, but fortunately, Sudesh was able to convince his parents and other elders of his house to approach police instead of blindly believing the mails. During investigation, it was revealed that the person sending those E-Mails was none other than Sujata's stepfather. Sujata's father (when he gave in during the police enquiries) admitted that he had sent those E-Mails to break the engagement. He wanted Sujata to remain

with him to continue providing him financial support. He admitted that Sujata's marriage would have caused him to lose control of her property of which he was the guardian till she got married.

- Section 49 of the Indian Penal Code is mentioned in reference to cyber defamation. Cyber defamation is a cognizable offense. Regarding "defamation" there is a mention that "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."
- The investigation traced the criminal through E-Mail forensics.

Mini-Case 3: Indian E-Mail Spoofing Case.

- This is a case of cyberstalking. It means threatening, illegal behavior by one person toward another person using Internet and other forms of online communication channels.
- Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Mumbai and Ahmedabad. These calls created destruction in the personal life, hence destroying mental peace of Mrs. Joshi. She decided to register a complaint with Delhi Police. A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for 4 consecutive days. The person was chatting on the Internet, using her name and giving her address, talking in profane language. The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.

7.4 ILLUSTRATIONS OF FINANCIAL FRAUDS IN CYBER DOMAIN

Illustration 1: Phishing Incidence.

- This is an illustration of Phishing attack in real life. Phishing is an Internet fraud through which cybercriminals illegally obtain sensitive information such as usernames, passwords and credit card details by showing a fake website.
- According to the news posted on 14 April 2010, it could be termed India's first legal adjudication of a dispute raised by a victim of a cybercrime. The judgment for the first case was filed under the IT Act. In this judgment, Tamil Nadu's IT Secretary ordered ICICI Bank to pay 12.85 lakhs to an Abu Dhabi-based NRI within 60 days – in compensation for the loss su ered by him as a result of a Phishing fraud.
- In this case, the compensation, included the travel expenses and the financial loss due to complete lack of involvement of the respondent bank – as per order from Tamil Nadu's IT Secretary. The order came based on a petition that was filed by Umashankar Sivasubramaniam. As per Umashankar's claim, he received an E-Mail in September

2007 from ICICI, asking him to reply with his Internet banking username and password or else his account would become non-existent. He replied and later he found 6.46 lakhs moved from his account to the account of another company. That company did a withdrawal of 4.6 lakhs from an ICICI branch in Mumbai and retained the balance in its account.

- An application was prepared and presented to the state IT Secretary. In that application, Umashankar held the bank responsible for the loss that he suffered. ICICI Bank, however, claimed that the applicant (Umashankar) had failed to protect his confidential information. According to ICICI Bank, Umashankar carelessly disclosed his confidential information such as password. According to the bank, he became the victim of a Phishing attack because of this carelessness. Bank spokesperson said that customers are fully informed on security aspects of Internet banking.
- The bank decided to appeal the order. The bank claims that they continuously upgrade their systems and technology to ensure that customers get the best experience and a safe environment while transacting online.
- Vijayashankarm a techno-legal consultant appeared for the petitioner. According to him, while the order may lead to tightening of cyberlaws in the country, the judgment reflects the lack of accountability of using Internet banking. He further opined that, although Phishing fraud is very common, banks are not accepting the liabilities. In his view, such a ruling will set a good example. In India, most of the Phishing cases do not get tracked under proper legal framework.

Illustration 2: Fake Mails Promising Tax Refunds – Beware.

- This is an illustration of fake E-Mails in the context of "Phishing" and shows how that was used by criminals. If you are a tax payer waiting for refunds at the end of the financial year, beware of fraudulent E-Mails circulating on the Internet. Delhi Police's Economic Offence Wing (EOW) investigated several cases where the complainants claimed to have received E-Mails in which they are asked to provide their bank account details so that the tax refund could be transferred to the accounts.
- Such an E-Mail-based fraud came to light after the Police received a complaint from a south Delhi businessman. The E-Mail claimed that the receiver would receive 2,500 compensations from the Income Tax department if he provided with his bank details, including Net banking password. The person who sent the E-Mail also asked for his credit card details; this raised doubt in the mind of the complainants.
- Additional commissioner of police (EOW) said that this cyber fraud is similar to attempted Phishing. Once the sender receives the details of the bank account, he can easily transfer the money from that account through Internet banking. As a safeguard, one should not respond to such E-Mails. One should report the matter to Police immediately. In this case, officials at the EOW got into tracing of the server

from where these E-Mails originated. They asked the service provider to furnish details about the E-Mail account through which these mails were sent.

- This was for the first time that such a cyber scam report went to Police. In this case, the police approached the income tax department to take steps to create awareness about such fraud E-Mails.

7.5 DIGITAL SIGNATURE-RELATED CRIME SCENARIOS

- In this section, examples of crimes related to "digital signatures" are discussed. Digital signatures are electronic signatures. The fundamental idea in digital signature is to use the concept of traditional paper-based signing and turn it into an electronic "fingerprint." The "fingerprint," or coded message, becomes the unique aspect of both the document and the entity who signs it.
- A digital signature is used for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender, and that the message was not altered in transit.
- The digital signature helps minimize the risk of "non-repudiation," that is, any changes made to the document after it is signed will make the signature invalid thereby protecting against signature forgery and information tampering.
- Following are some situations where authenticity, accountability, data integrity and non-repudiation of digital signature claims:

Situation 1: Digital Signature Certificate – Misinterpretation of Information Provided

- Let us say a person "A" is applying for a digital signature certificate. He fills his name as "B" and also submits photocopies of B's passport, Driving License or PAN Card as proof of identity (which can also be seen as "identity theft"). This situation is liable for misrepresenting information to the Certifying Authority (CA).

Situation 2: Digital Signature Certificate – Suppression of Information by Applicant

- Suppose an organization "XYZ" is applying for a license to become a Certifying Authority (CA). In the application form one of the information required to be filled is "In case any of the company directors been convicted for a criminal offense, then please mention relevant details." Suppose one of the company's directors had been convicted in the past. However, in the submitted form, the company officials do not provide answer to this question, that is, they leave that field on the form blank. Under this circumstance, the officials will be liable for suppressing information from the Controller.

Situation 3: Digital Signature Certificate – False Certificate

- A person creates a fake digital signature certificate with the illegal purpose and make the victim believe that the certificate has been issued by a certain CA. That Person

now plans to use this certificate to carry out some financial frauds with the targeted victim. He posts this certificate on his website. The person shall be liable under this Section 73.

Situation 4: Digital Signature Certificate – Retaining a Rejected Certificate

- Person "A" has applied to a Certifying Authority for a digital signature certificate. In due course of time, the said CA issues the certificate to Person "A". However, Person "A" does not accept it on the basis that some of the details are incorrect in the certificate. In the meanwhile, the CA publishes the certificate in their online repository. In this case, the CA will be liable under Section 73 of the Indian IT Act (Penalty for publishing [Electronic Signature] Certificate false in certain particulars).

Situation 5: Digital Signature Certificate – Retaining a Certificate Beyond its Validity Period

- Person "A" is employed with "XYZ" Company. He obtains a digital signature certificate for official purposes on 1st February in a certain year. He quits the job on 1st November of the same year and the certificate is cancelled on the very same day. Now suppose, "XYZ" Company continues to keep Person A's cancelled certificate in their online repository even after 1st November, that is, even after the person has quit the organization. Under this circumstance, "XYZ" Company is liable under this section. However, they will not be liable if the purpose behind keeping Person A's certificate in their repository is to verify documents signed by the person between 1st February and 1st November. The punishment provided for this Section 73 is imprisonment up to 2 years and/or fine up to 1 lakh.

Situation 6: Digital Signature Certificate – Fraudulent/Unlawful Use

- Person "A" is under possession of a computer with Windows Server operating system running on it. The person also has Certificate Services installed on that computer. Person "A" uses this computer to generate a digital signature certificate for themselves and Person "B". Now the person "A" has created the said certificates. Next, Person "A" puts up Person B's digital signature certificate onto a publicly accessible part of his website. This means that now Person "A" has published Person B's certificate.
- Now, Person "A" using the same computer under his/her possession and running the services as mentioned before on that computer, issues this certificate to Person "C" – knowing or not knowing that Person "C" plans to misuse it to spoof Person B's E-Mails. Under these circumstances, Person "A" has made the certificate available to Person "B" for an unlawful/fraudulent purpose. The punishment provided for violation of Section 74 is imprisonment up to 2 years and/or fine up to 1 lakh.

7.6 DIGITAL FORENSICS CASE ILLUSTRATIONS

- Digital forensics is a science in which material found in digital devices in relation with computer crime are recovered and investigated. In the following illustration a case related with digital forensics is discussed:

Digital Forensics Illustration: Confidential Data Theft Revealed through Forensics Investigation.

- Stealing data is a crime. This illustration shows how an unhappy employ can seek revenge.
- Ajay, an employee of POOR-ME COMPANY receives a poor performance appraisal from his manager. Ajay applied for a job in another company which was a competitor organization, using a company letterhead. Ajay receives a job application from UNSCRUPULOUS_COMPANY (the competitor company).
- In a meeting with UNSCRUPULOUS_COMPANY, they propose a plan to him about getting some urgently required information from POOR-ME COMPANY. Ajay agrees to steal proprietary information in exchange for a job and a payoff. He is given a 4 GB USB Flash drive with detailed guidance describing how to steal and transmit proprietary information. Ajay reads the directions on how to use a "cracker" program.
- Ajay sends a Trojan program as an attachment to E-Mail to members of the Product development team. The attachment appears for a good cause – "donation request". A member of the Product team, Mr. Lele of POOR-ME COMPANY opens the E-Mail and the attachment.
- The attachment sent to Lele is a Trojan Horse program that will allow remote access to and control of Lele's machine. Now Ajay is in a position to access Lele's machine remotely.
- Ajay stole the company confidential information, and transfer it to his soon-to-be new employer, eager to impress them that he has done the "job." In order to conceal his activities, Ajay uses E-Mail and Steganography to hide the stolen data in plain sight.
- After some days, news about Competition Company (UNSCRUPULOUS_COMPANY) appears in the media. The news indicates that the company demonstrate their next version of the product months ahead of the schedule. The news also mentions that the CEO of the company congratulating his R&D team for this fantastic achievement. In the same news, the industry analyst is quoted that through this early prototype development, the company will be able to introduce their competition product to the market very soon and that the product has the potential to take away a major slice of sales revenues from the competition.

- By this news, POOR-ME COMPANY go for forensics investigators to determine whether any fraud occurred that lead to the loss of their data. The investigators monitor POOR-ME COMPANY's Intranet using forensics monitoring devices. With client consent, a document likely to be stolen, is "tagged" to provide tangible proof of intellectual property theft and support later litigation and damages claims.
- Meanwhile, Ajay once again, covertly accesses Lele's computer to steal intellectual property (PRODUCT). Investigators are keeping a close trail and they record Ajay's actions as evidence against him. With his final theft complete, Ajay deletes all stolen documents and exploitation programs from his workstation. Now that Ajay has taken the "bait" document, the investigators perform covert digital evidence recovery on Ajay's employer who is supplied with a Palm Pilot (a kind of hand-held device) and workstation.
- Using a variety of digital forensics tools, the investigators examine Ajay's workstation. The Palm Pilot gave away his passwords and account data and other valuable information such as the use of Steganography.
- With the digital evidence supplied by the investigators, POOR-ME COMPANY filed suit against UNSCRUPULOUS_COMPANY for intellectual property theft.

7.7 ONLINE SCAMS

- In this section, some of the well-known online scams are described.

Scam No. 1 – Follow-up Scamming.

- This trick is used when scammers know that their victim just has been scammed, and is more likely to fall for scamming attempts. Hence the scammer targets the victim just has been scammed rather than a randomly selected victim. Often the scammer contacts the victim after a fraud, then the scammer present himself/herself as a law enforcement officer. The victim is given to understand that a group of criminals has been arrested and that they (i.e., fraudsters who are pretending to be the law enforcement folks) have recovered victim's lost money. Further, fraudster/scammer tells the victim that in order to get the money back, the victim must pay a fee for processing or insurance purposes. Even when the victim realizes the scam, this follow-up scam can be successful because the scammer represents himself/herself as a totally different party and yet knows details about the transactions. For the victim, realization that he/she has lost a large sum of money and the prospect of getting it back often leads to the victim ending up paying even more money to the same scammer.

Scam No. 2 – Purchasing Goods and Services Scam.

- There is a big boom in "Online Marketing" activities even if, it may be at the cost of your personal information being stolen. In this mode of scam, the fraudsters list a

non-existent high value car with a low price as bait to attract buyers eager to buy quickly; specially the young and rich targets. The scammer posts a message like "I am not in the country, but if you pay me first, a friend will drive the car to you." The required payment may be the full price, or a deposit, but it would not be an insignificant fee. The picture of the car is never posted on the website because the car just does not exist. In this type of scam, the scammers use E-Mail only because they are smart enough to know that the sound of their voice and their attitude will give them away as being high risk.

- Another scheme under this type of scam involves advertising fake academic conferences and invite academician to present papers. As a common practice, the conference would typically subsidize the accommodation but would not reimburse the cost of air journey undertaken by the academicians to be at the conference venue for presenting papers. The scammer offer free air travel to the victim, if they agree to pre-pay for hotel accommodation. The scammer can put a number of arguments to support why the accommodation must be pre-paid – primarily that they do not trust the victim will attend the conference unless he/she pays upfront.
- In the first example, fraudster use a goods and in second example fraudster use services. The idea is that they troll the victim with a good deal, and the victim must pay in advance and online.

Scam No. 3 – Foreign Country Visit Bait

- Fraudsters take advantage of the fact that generally people are eager to go overseas with the hope of earning more money. Fraudsters work out for that scenario and attract the victim through an "invitation to visit the country" kind of message. The innocent victims are invited to a country to meet real or fake government officials. Some victims who do travel are instead held for payment. There are a few criminal cases, where they are illegally brought into the country without a visa and threatened into giving additional money as the penalties for being in a foreign country without a visa may be severe. At times victims are taken for ransom or they are killed.

Scam No. 4 – Pyramid Scheme Scams and Ponzi Scheme Scams

- This is called as "pyramid scheme frauds". In this scam the team of fraudsters operate in the structure of a pyramid. A pyramid scheme is considered to be a non-sustainable business model – it involves making payment promises to participants mainly for getting other people into the scheme. Any real investment or sale of products/services to customers/consumers is not intended. Basically, pyramid schemes are a form of fraud.
- The basic concept of pyramid scheme is that "Person A" makes only one payment. To start earning, "Person A" has to get in the chain like others who will also make one

payment each. "Person A" gets paid out of receipts from those new recruits. This way, they go on to recruit others. As each new recruit makes a payment, "Person A" gets his share. As the "business" expands, he is promised increasingly greater benefits.

- The problem in that chain is that, there is no end benefit. The benefits only travel "up the chain." Only the originator and a very few at the top levels of the pyramid make huge amounts of money. The amounts become less and less down the pyramid structure. There is nothing for the individuals at the bottom of the pyramid.

❖❖❖

Bibliography

1. Book : Cyber Security, By Nina Godbole, Sunit Belapure , WILEY publication
2. URL:https://www.rvskvv.net/images/INTELLECTUAL-PROPERTY-RIGHTS_20.04. 2020. pdf

❖❖❖