Cyber Security (BCC- 301)

Section A

Q No.1 What do you Understand by the term " Cyber Crime "?

Solution:- Almost everyone is aware of the rapid growth of the Internet. Given the unrestricted number of free websites, the internet has opened a new way of exploitation known as cyber crime. **OR**

Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle. **OR**

"a crime conducted in which a computer was directly and significantly instrumental."

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

Q No.2 Who are Cyber Criminals?

Solution:- Most cyber-attacks are spearheaded by individuals or small groups of hackers. However, sizeable organized crime also exploits the internet. These criminals, branded as "professional" hackers, **develop new and innovative ways to commit crimes.** and treat cyber-crime like an income-generating investment.

Cybercriminals involves such activities as

- Child pornography
- Credit card fraud
- Cyber stalking

Q No.3 Identify about Cyber Security?

Solution:- "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.

The term incorporates both the physical security of devices as well as the information stored therein. In other words, It is the body of technologies, Processes and Practices designed to protect networks, devices, programs and data from attack, theft, damage, modification of unauthorized access.

Q No.4 What do you mean by Cyber Stalking?

Solution:- Cyber Stalking is the repeated use of the Internet, email, or related digital electronic Communications devices to alarm, or threaten a specific individual or Groups

of Individuals. In other words, cyber stalking is a crime in which someone harasses or stalks a victim using electronics and digital means such as social media, emai, instant messaging or messages posted to a discussion group or forum. Cyber stalkers take advantage by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected. So, the term “Cyber stalking” and “Cyber Bullying” are often used Interchangebly.

Q No.5 Define Information Security?

Solution:- Lack of information security gives rise to cybercrimes. From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides new focus on **“Information Security in India."**

- Cyber Security covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.
- For anyone trying to compile data on business impact of cybercrime, there are number of challenges. One of them comes from the fact that organizations do not explicitly incorporate the cost of the vast majority of computer security incidents into their accounting as opposed.

Q No.6 What What do you Understand by the term “ Steganography ”?

Solution:- Steganography is a Greek word that means “sheltered writing.” It is a method that attempts to hide the existence of a message or communication. The word “steganography” comes from the two Greek words: steganos meaning “covered” and graphein meaning “to write” that means “concealed writing,” This idea of data hiding is not a novelty; it has been used for centuries all across the world under different regimes. ‘The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messengers head and then tattooing a secret message on it, letting his hair growback and then shaving it again after he arrived at the receiving party to reveal the message.

Q No.7 Who are Key loggers?

Solution:- Keystroke logging, often called key logging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored. It can be classified as software key logger and hardware key logger.

Software Key loggers

Software key loggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software key loggers are installed on a computer system by Trojans or viruses without the knowledge of the user.

Hardware Key loggers

Hardware key loggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each key press on the keyboard of the ATM gets registered by these key loggers.

Q No.8 Identify about Spywares?

Solution:- Spyware is a type of malware that is installed on computers which collects information about users without their knowledge. It is clearly understood from the term Spyware that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system.

Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP).

Q No.9 What do you mean by Backdoors?

Solution:- A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they detect or install themselves as part of an exploit. In some cases, a worm is designed to take advantage of a backdoor created by an earlier attack.

It allows an attacker to create, delete, rename, copy or edit any file, execute various commands, change any system settings; alter the Windows registry; run, control and terminate applications

Q No.10 Define Trojan Horses?

Solution:- Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk.

Some 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 slow down, restart or shutdown the system.
7. They reinstall themselves after being disabled.
8. They gather E-Mail addresses and use them for Spam.

Q No.11 What do you Understand by the term "Digital Forensics Science "?

Digital forensic science is the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/net books, tablets, smart phones, etc., was little-known a few years ago. However, with the growing incidence of cyber crime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations.

Q No.12 Define Indian Cyber Law?

In India, cyber laws are contained in the Information Technology Act, 2000 (IT Act) which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law is referred to as the Law of the Internet.

Like any law, a cyber law is created to help protect people and organizations on the Internet from malicious people on the Internet and help maintain order. If someone breaks a cyber law or rule, it allows another person or organization to take action against that person or have them sentenced to a punishment.

Q No.13 Identify chain of Custody Concept?

A chain of custody is the process of validating how evidences have been gathered, tracked, and protected on the way to the court of law. Forensic professionals know that if you do not have a chain of custody, the evidence is worthless.

The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition to its final disposition. A chain of custody begins when evidence is collected and the chain is maintained until it is disposed off. The chain of custody assumes continuous accountability.

Q No.14 What do you mean by Forensics Analysis of Email?

An E-Mail system is a combination of hardware and software that controls the flow of E-Mail. Two most important components of an email system are:

- E-Mail server
- E-Mail gateway

E-Mail servers are computers that forward, collect, store, and deliver email to their clients.

Q No.15 Define Information Security Policy?

India's cyber space is almost unprotected. Till now, we only have very basic security features. We have started considering advanced features only after the Snowden revelations. All our vital institutions, installations and critical infrastructure need to be protected from cyber-attacks.

The future war will target crucial areas like:

1. Defence installations
2. Sensitive documents related to both internal and external security
3. Communication networks, including satellites
4. ATC management
5. Railway traffic control
6. Financial, services
7. Premier institutions of science, technology and research

Section B

Q No.16 Describe about Botnet attack on wireless devices?

Solution:- A botnet is called as a collection of infected devices which are internet connected and these devices are controlled by the cyber-criminal with the help of malware. Usually, users are unaware of a botnet that is affecting their PC. Botnets normally used to send spam mails, create unusual traffic, etc.

Botnet is installed on the PC which is vulnerable because of outdated firewalls or antivirus. Once the target device gets affected the attacker can control bots with two approaches –

Client server approach – In this approach, first a server is set up which then sends commands to bots via communication protocol. After getting the command bots do the corresponding malicious activity.

Peer to peer approach – This is a decentralized approach in which there is no main server. This approach is very common nowadays because Cyber security is still using the C&C communication to search for these malicious activities. In this approach Infected devices search for the infected website or devices in the same bot. Then they share the updated command of the botnet malware.

Botnet attack to wireless devices

Botnets are not made to trade off only one individual computer; they are intended to contaminatea large number of remote devices. Bot herders regularly send botnets onto computers through a trojan stallion virus. The procedure regularly expects clients to contaminate their own particular frameworks by opening email connections, tapping on malicious fly up advertisements, or downloading hazardous software from a site. In the wake of contaminating devices, botnets are unable to get to and adjust individual data, attack different computers, and perpetrate differentwrong doings.

More mind boggling botnets can even self-engender finding and tainting devices naturally. Such self-governing bots do look for-and-contaminate missions, always scanning the web for defenseless web-associated devices lacking working framework refreshes or antivirus software.

Q No.17 Describe Proliferation of Mobile and Wireless devices?

Solution:- Proliferation (Growth) of Mobile and Wireless Devices:-

- Today, incredible advances are being made for mobile devices.
- The trend is for smaller devices and more processing power.
- A few years ago, the choice was between a wireless phone and a simple PDA.

Now the buyers have a choice between high-end PDAs with integrated wireless modems and smallphones with wireless Web-browsing capabilities.

- A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls.
- As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices.
- Let us understand the concept **of mobile computing** and the various types of devices.

Mobile computing

Mobile computing is "taking a computer and all necessary files and software out into thefield." Many types of mobile computers have been introduced since 1990s.

- They are as follows:

1. Portable computer: It is *a general-purpose computer that can be easily moved from one place to another*, but cannot be used while in transit, usually because it requires some"setting-up" and an AC power source.

2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. Ultramobile PC: It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. Smartphone: It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, ***global positioning system*** **(GPS) and DVD player**. It also contains word processing software and is Bluetooth compatible.

8. Fly Fusion Pentop computer: *It is a computing device with the size and shape of a pen*. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless computing

- Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server)

without a physical connection.

- Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications atthis time.
- Mobile simply describes a computing device that is not restricted to a desktop, that is, not tethered. As more personal devices find their way into the enterprise, corporations are realizing cyber security threats that come along with the benefits achieved with mobile solutions.
- Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all.
- Thus, while "wireless" is a subset of "mobile," in most cases, an application can bemobile without being wireless.
- Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smart phones.

Q No.18 Why Cyber Criminals prefer Cyber Café's?

- **Solution:-** Cyber criminals prefer cyber cafes to carry out their activities.

A recent survey conducted in one of the metropolitan cities in India reveals the following facts :

1.Pirated software are installed in all the computers.

2.Antivirus was not updated with latest patch.

3.Several cyber cafes has installed "Deep Freeze" to protect computer which helps cyber criminals.

4.Annual Maintenance Contract (AMC) was not found for servicing of the computer.

5.Pornographical websites were not blocked.

6.Cybercafe owner have very less awareness about IT security.

7.Cybercafe association or State Police do not seem to conduct periodic visits to cyber cafe.

Q No.19 Discuss about survival mantra for the Netizens?

Solution:- The term "Netizen" was coined by Michael Hauben. Simply, netizens are the Internet users. Therefore, netizen is someone who spends considerable time online and also has a considerable presence online.

The 5P netizen mantra for online security is:

1) precaution,
2) prevention,
3) protection,
4) preservation
5) perseverance.

- For ensuring the motto for the "Netizen" should be "Stranger is Danger!" If you

protect your customer's our employee's privacy and your own company.

- Then you are doing your job in the grander scheme of the things to regulate and enforce rules on the Net through our community.
- NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once.
- This is the reason they have established cyber labs across major cities in India.
- More importantly, users must try and save any electronic information trail on their computers.
- That is all one can do until laws become more stringent or technology more advanced.
- There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.

Q No.20 Examine the term " Social Engineering "?

Solution:- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:

Sabotage: Disrupting or corrupting data to cause harm or inconvenience.

Theft: Obtaining valuables like information, access, or money.

This social engineering definition can be further expanded by knowing exactly how it works.

How Does Social Engineering Work?

Solution:- Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.

The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

1. **Prepare** by gathering background information on you or a larger group you area part of.
2. **Infiltrate** by establishing a relationship or initiating an interaction, started bybuilding trust.
3. **Exploit the victim** once trust and a weakness are established to advance theattack.
4. **Disengage** once the user has taken the desired action.

Q No.21 Why Cyber Criminals attack on Mobile phones?

Solution:- Attacks on Mobile/Cell Phones

Mobile Phone Theft

- Mobile phones have become an integral part of everbody's life and the mobile phone hastransformed from being a luxury to a bare necessity.
- Theft of mobile phones has risen dramatically over the past few years.
- Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.
- Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.
- When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)", that really matter, are lost
- One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement.
- After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones.
- Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.
- The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** Enough terminals or more devices to attack.
2. **Enough functionality:** The expanded functionality ie. *office functionality and applications* also increases the probability of malware.
3. **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Ensure to note the following details about your cell phone and preserve it in a safe place:

1. Your phone number;
2. the make and model;
3. color and appearance details;
4. PIN and/or security lock code;
5. IMEI number.

The International Mobile Equipment Identity (IMEI)

- It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digitnumber and can be obtained by entering *#06# from the keypad.
- The IMEI number is used by the GSM network to identify valid devices and thereforecan be used to stop a stolen phone from accessing the network in that country.
- For example, if a mobile phone is stolen, the owner can call his or her serviceprovider and instruct them to "lock" the phone using its IMEI number.
- This will help to stop the usage of phone in that country, even if a SIM is changed.

Visit the weblink http://www.numberingplans.com/?page=analysis&sub=imeinr to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

- Following are few antitheft software(s) available in the market:

1. **GadgetTrak:** http://www.gadgettrak.com/products/mobile/
2. **Back2u:** http://www.bak2u.com/phonebakmobilephone.php
3. **Wavesecure:** https://www.wavesecure.com/
4. **F-Secure:** http://www.f-secure.com/

<u>Mobile Viruses</u>

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

- *How to Protect from Mobile Malwares Attacks*
- Following are some tips to protect mobile from mobile malware attacks:

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

Mishing

- *Mishing* is a combination of mobile and Phishing.
- Mishing attacks are attempted using mobile phone technology.
- M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
- A typical Mishing attacker uses call termed as *Vishing* or message (SMS) known as

***Smishing*.**

- Attacker will pretend to be an employee from your bank or another organization and willclaim a need for your personal details.
- Attackers are very creative and they would try to convince you with diferent reasons whythey need this information from you.

Vishing

- Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V – **v**oice and Phishing.
- Vishing is usually used to steal credit card numbers or other related data used in ID theftschemes from individuals.
- The most profitable uses of the information gained through a Vishing attack include:

1. ID theft;
2. purchasing luxury goods and services;
3. transferring money/funds;
4. monitoring the victims' bank accounts;
5. making applications for loans and credit cards.

<u>Smishing</u>

- Smishing is a criminal offense conducted by using social engineering techniques similarto Phishing.

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

Q No.22 Discuss about Credit Card frauds in Mobile and Wireless computing?

Solution:- Credit Card Frauds in Mobile and Wireless Computing Era

- These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M- Commerce) and mobile banking (M-Banking).
- Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.
- *Mobile credit card transactions* are now very common; new technologies combine low- cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.
- Today belongs to "mobile computing," that is, *anywhere anytime computing*.
- The developments in wireless technology have fuelled this new mode of working forwhite collar workers.
- Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.
- It is most often used by businesses that operate mainly in a mobile environment.
- Figure 3.4 shows the basic flow of transactions involved in purchases done using creditcards.

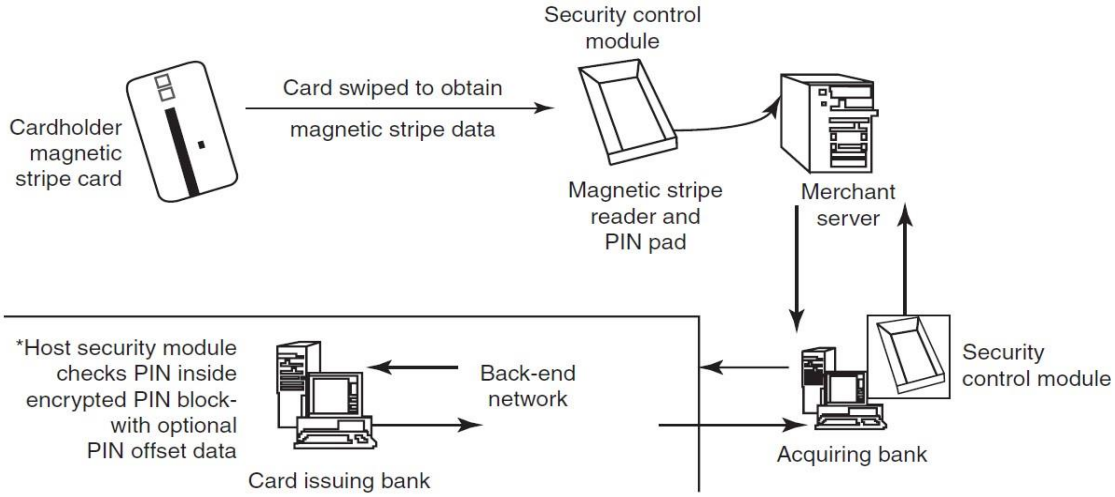


Figure 3.4 | Online environment for credit card transactions.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

- Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions
- Figure 3.5, the basic flow is as follows:

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

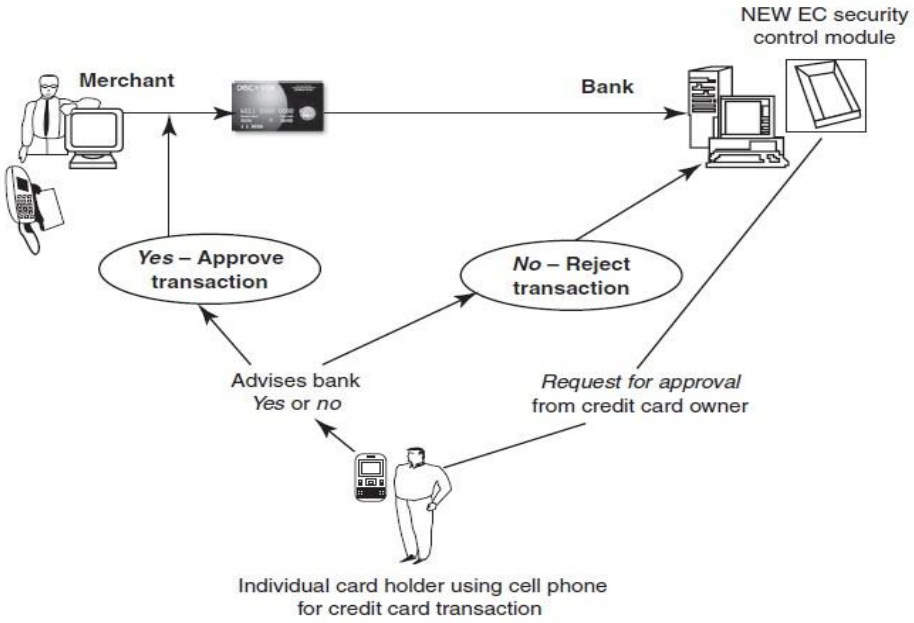


Figure 3.5 | Closed-loop environment for wireless (CLEW).
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Types and Techniques of Credit Card Frauds

Traditional Techniques

- The traditional and the first type of credit card fraud is paper-based fraud – *application fraud*, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) to open an account in someone else's name.
- Application fraud can be divided into

1. ID theft: Where an individual pretends to be someone else

2. Financial fraud: Where an individual gives false information about his or her financial status to acquire credit. Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

Modern Techniques

- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing.
- Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink /website (i.e., they have been scammed).

1. Triangulation: It is another method of credit card fraud and works in the fashion asexplained further.

• The criminal offers the goods with heavy discounted rates through a website designed andhosted by him, which appears to be legitimate merchandise website.

• The customer registers on this website with his/her name, address, shipping address andvalid credit card details.

• The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's website.

• The goods are shipped to the customer and the transaction gets completed.

• The criminal keeps on purchasing other goods using fraudulent credit card details ofdifferent customers till the criminal closes existing website and starts a new one.

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

Q No.23 Examine the term " Trends in Mobility "?

Solution:- Trends in Mobility

- Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking.
- "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction.
- This smart mobile technology is rapidly gaining popularity and the attackers (hackers andcrackers) are among its biggest fans.
- It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cyber security issues in the mobile computing domain.
- Figure 3.3 shows the different types of mobility and their implications

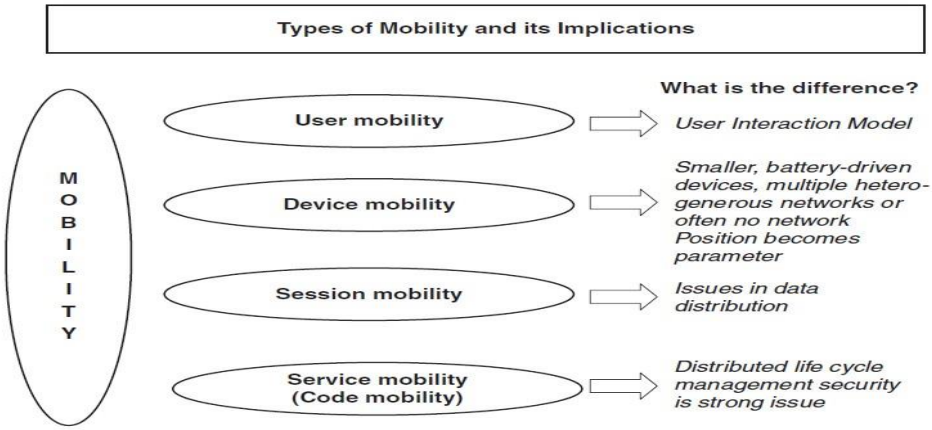


Figure 3.3 | Mobility types and implications.

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

1. Malwares, viruses and worms: Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are fewexamples of malware(s) specific to mobile devices:

- ***Skull Trojan****:* It targets Series 60 phones equipped with the Symbian mobile OS.
- ***Cabir Worm****:* It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The

worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.

• ***Mosquito Trojan****:* It affects the Series 60 Smart phones 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 (refer to Appendix C).

• ***Lasco Worm****:* It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

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

Q No.24 Describe about Patent and Trademarks?

Solution:- <u>Patent and Trademark,</u>

Filing a patent, and trademark, in India involves specific requirements and procedures. Here's an overview of the requirements and steps for filing each type of intellectual property:

Patent Filing in India:

Requirements:

- **Novelty**: The invention must be new and not disclosed or published anywhere in the world before the filing date.
- **Inventive Step**: The invention must involve an inventive step, meaning it is not obvious to a person skilled in the relevant field of technology.
- **Industrial Applicability**: The invention must have practical applicability in an industrial or technical field.

Procedure:

- **Patent Search**: Conduct a thorough search to ensure that the invention is novel and does not infringe upon existing patents.
- **Drafting the Patent Application**: Prepare a detailed description of the invention, including drawings, if necessary. Claims defining the scope of the invention and an abstract should also be included.
- **Filing the Application**: Submit the patent application to the Indian Patent Office either online or through physical filing. Include the necessary forms, fees, and supporting documents.
- **Examination**: The application undergoes a substantive examination to assess its patentability. If any objections or rejections are raised, responses must be filed within the prescribed period.
- **Grant and Publication**: If the application meets all requirements and objections are overcome, the patent is granted and published in the official journal. The term of a patent in India is 20 years from the filing date.

Trademark Filing in India:
Requirements:

- **Distinctiveness**: The trademark must be distinctive, not generic or descriptive of the goods or services it represents.
- **Non-conflict:** The proposed trademark should not conflict with existing registered or pending trademarks.
- **Proper Representation:** The trademark should be capable of graphical representation, such as words, logos, or a combination of both.
- **Trademark Search**: Conduct a comprehensive search to ensure the proposed trademark is available and not already registered or pending.
- **Filing the Application**: Prepare and file the trademark application with the appropriate forms, fees, and supporting documents. The application can be filed online or physically.
- **Examination and Publication**: The trademark application undergoes examination for any conflicting marks or objections. If no objections are raised, the trademark is published in the Trademark Journal.
- **Opposition**: After publication, there is a three-month period during which third parties can oppose the registration of the trademark.
- **Registration**: If no opposition is filed or successfully resolved, the trademark is registered, and a registration certificate is issued. The trademark registration is valid for ten years and can be renewed indefinitely.

Q No.25 Define the Challenges in Computer Forensics?

Solution:- Challenges in Computer Forensic

1. Evolving Technology:

Rapid Technological Advancements: The pace of technological change can outstrip the development of forensic tools and techniques, making it challenging to keep up.

2. Encryption and Security Measures:

Encrypted Data: The widespread use of encryption can make it difficult to access and analyze data during forensic investigations.

Security Mechanisms: Increasingly sophisticated security measures can impede the extraction of evidence from devices.

3. Data Volume and Complexity:

Big Data Challenges: The sheer volume of digital data generated makes it challenging to sift through and analyze relevant information efficiently.

Complex Data Structures: The complexity of data structures and file formats can complicate the extraction and interpretation of evidence.

4. Anti-Forensic Techniques:

Anti-Forensic Tools: Perpetrators may employ anti-forensic tools and techniques to erase or alter digital evidence, making it harder for investigators to reconstruct events.

Data Obfuscation: Deliberate attempts to hide or obfuscate digital trails can pose challenges in uncovering the truth.

5. Legal and Ethical Issues:

Privacy Concerns: Striking a balance between forensic investigations and individual privacy rights poses a significant challenge.

Legal Compliance: Adhering to legal procedures, obtaining proper warrants, and ensuring the admissibility of evidence can be complex.

6. Volatility of Digital Evidence:

Data Volatility: Digital evidence can be volatile and easily altered, requiring swift and careful handling to preserve its integrity.

Live Systems: Analyzing live systems without causing disruption or altering data is a challenge.

7. International Jurisdiction:

Cross-Border Investigations: The global nature of cybercrime requires collaboration across international borders, introducing challenges related to jurisdiction and legal frameworks.

8. Skill Shortages and Training:

Specialized Expertise: Computer forensics demands highly specialized skills, and there may be shortages of qualified professionals.

Continuous Training: Rapid changes in technology necessitate ongoing training for forensic investigators to stay current.

9. Budgetary Constraints:

Resource Limitations: Adequate resources, both in terms of technology and personnel, are crucial, and budget constraints can hinder effective forensic investigations.

10. Digital Forensic Tool Validation:

Tool Reliability: Ensuring the reliability and accuracy of forensic tools is challenging and requires continuous validation and testing.

Open Source Tools: While open-source tools are valuable, their security and reliability need to be carefully assessed.

11. Data Privacy and Consent:

Consent Challenges: Obtaining consent for digital investigations can be complex, especially in corporate environments or when dealing with sensitive personal data.

12. Cloud Computing Challenges:

Data Residency: Data stored in the cloud may reside in different jurisdictions, adding complexity to the legal aspects of investigations.

Access to Cloud Data: Obtaining access to cloud-based evidence can be challenging due to service provider policies and security measures.

13. Forensic Readiness:

Proactive Planning: Organizations may lack proactive forensic readiness plans, hindering their ability to respond effectively to incidents.

Addressing these challenges requires a combination of technical innovation, legal frameworks, collaboration, and ongoing professional development within the field of computer forensics. As technology continues to evolve, these challenges will persist and necessitate adaptability and continuous improvement in forensic practice.

Q No.26 Discuss the Cyber Forensics and Digital Evidence?

Solution:- Cyber Forensics and Digital Forensics

Digital Forensics:

Scope:

Encompasses a broad range of forensic activities involving the recovery, investigation, and analysis of digital artifacts from various digital devices.

Focus:

Primarily focuses on the recovery and analysis of electronic data for legal purposes, often in the context of criminal investigations or litigation.

Applications:

Used in a variety of contexts, including law enforcement, corporate investigations, civil litigation, and data recovery.

Types of Devices:

Involves the examination of a wide array of digital devices such as computers, laptops, smartphones, external storage devices, and more.

Data Types:

Deals with various forms of digital data, including files, documents, images, emails, and other electronic records.

Objectives:

Aims to discover and analyze evidence related to a specific incident, crime, or legal case by examining digital information.

Cyber Forensics:

Scope:

Specialized field within digital forensics that specifically deals with cybercrimes and cyber incidents.

Focus:

Concentrates on the identification, analysis, and response to cyber threats, attacks, and security breaches.

Applications:

Primarily used in the prevention, detection, and response to cybercrimes, including hacking, malware attacks, and data breaches.

Types of Devices:

Focuses on digital devices connected to networks, including servers, routers, firewalls, and IoT (Internet of Things) devices.

Data Types:

Involves the analysis of network traffic, log files, intrusion detection system (IDS) alerts, and other data related to cybersecurity incidents.

Objectives:

Aims to not only gather evidence for legal purposes but also to understand and mitigate cybersecurity threats, protect systems, and improve overall digital security.

Q No.27 Examine Digital Personal Data protection ACT-2023?

Solution:- Objective of the Digital Personal Data Protection Act 2023:

1. **Enhancing Privacy:**
   - Ensure the protection of individuals' digital personal data.
   - Empower individuals with control over their personal information.
2. **Facilitating Trust in Digital Transactions:**
   - Boost confidence in digital services by establishing a framework for responsible data handling.
3. **Promoting Innovation:**
   - Encourage the development of new technologies and services while respecting privacy.
4. **International Compliance:**
   - Align with global data protection standards to facilitate international data flows.
5. **Mitigating Data Breaches:**
   - Establish mechanisms to prevent and respond to data breaches, ensuring swift and effective action in case of security incidents.

6. **Transparent Data Processing:**
- Promote transparency in the collection, processing, and use of personal data by organizations.

7. **Empowering Data Subjects:**
- Grant individuals the right to access, correct, and erase their personal data.

8. **Accountability:**
- Hold organizations accountable for the proper handling of personal data through robust compliance and enforcement mechanisms.

Section C

Q No.28 Discuss about Classifications of Cyber Crime?

Solution:- Cyber crimes are majorly of 4 types:

1. **Against Individuals:** These include e-mail spoofing, spamming, cyber defamation, cyber harassments and cyber stalking.

2. **Against Property:** These include credit card frauds, internet time theft and intellectualproperty crimes.

3. **Against Organisations:** These include unauthorized accessing of computer, denial Of service, computer contamination / virus attack, e-mail bombing, salami attack, logic bomb, trojan horse and data diddling.

4. **Against Society:** These include Forgery, CYber Terrorism, Web Jacking.

Classification Of Cyber Crimes

Cyber crimes can be classified in to 4 major categories as the following:

(1) Cyber crime against Individual

(2) Cyber crime Against Property

(3) Cyber crime Against Organization

(4) Cyber crime Against Society

(1) Against Individuals

(i) **Email spoofing** : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

(ii) **Spamming :** Spamming means sending multiple copies of unsolicited mails or mass e-mailssuch as chain letters.

(iii) **Cyber Defamation** : This occurs when defamation takes place with the help of computersand/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

(iv) **Harassment & Cyber stalking :** Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols

available such as e- mail, chat rooms, user net groups.

(2) Against Property

(i) Credit Card Fraud : As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

(ii) Intellectual Property crimes : These include

Software piracy: Illegal copying of programs, distribution of copies of software.

Copyright infringement: Using copyrighted material without proper permission.

Trademarks violations: Using trademarks and associated rights without permission of the actual holder.

Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

(iii) Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

(3) Against Organisations

(i) Unauthorized Accessing of Computer:

Accessing the computer/network without permission from the owner. It can be of 2 forms:

a) Changing/deleting data: Unauthorized changing of data.

b) Computer voyeur: The criminal reads or copies confidential or proprietary information, butthe data is neither deleted nor changed.

(ii) Denial Of Service :

When Internet server is flooded with continuous bogus requests so as to denying legitimateusers to use the server or to crash the server.

(iii) Computer contamination / Virus attack :

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mailservers thereby ultimately resulting into crashing.

(v) Salami Attack : When negligible amounts are removed & accumulated in to somethinglarger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse : This is an unauthorized program which functions from inside what seems tobe an authorized program, thereby concealing what it is actually doing.

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

(4) Against Society

(i) Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computersand high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people andcarry out the activities of terrorism.

(iii) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Q No.29 How Cyber Criminals plan the Attacks?

Solution:- Cybercriminals commit cybercrimes using different tools and techniques. But, the basic process of performing the attacks is same in general. The process or steps involved in committing the cybercrime can be specified in 6 steps namely:

Reconnaissance

Scanning and scrutinizingGaining Access Maintaining Access Covering the Tracks Launching the attack

Above Six Steps We can Integrate into three phases, involved in planning a cyber-attack. **Reconnaissance** – this is the information gathering stage and is usually considered a passiveattack.

Scanning and scrutinization of the collected data for validation and accurateidentification of existing vulnerabilities.

Launching the attack – entails gaining and maintaining access to the system.

1. Reconnaissance

The first step in how cybercriminals plan attacks is always **Reconnaissance**. The literal meaning of reconnaissance is an act of exploring with an aim or goal of finding someone or something about the target. Concerning cyber security, it's an exploration to gain information about an enemy or a potential enemy. In cyber security, reconnaissance begins with "**Foot printing**", the initial preparation towards the pre attack phase, and entails collecting data about the target's computer infrastructure as well as their cyber-environment.

Foot printing gives an overview of the victim's weak points and suggestions on how they can be exploited. The primary objective of this phase is to provide the attacker

with an understanding ofthe victim's system infrastructure, the networking ports and services, and any other aspect of security required for launching attacks.

Thus, an attacker attempts to source data from two different phases: passive and **active** attacks.

2. Passive attacks

This is the second phase of the attack plan. In this phase, **an attacker secretly gathers information about their target**; the aim is to acquire the relevant data without the victim noticing. The process can be as simple as watching an organization to see when their CEO reports to work or spying on a specific department to see when they down their tools. Because most hackers prefer executing their duties remotely, most passive attacks are conducted over the internet by googling. For example, one may use search engines such as dogpile to search for information about an individual or organization.

Yahoo or Google search: malicious individuals can use these search engines to gather information about employees of the firm they are targeting to breach their system.

Surfing online communities like Twitter, Facebook, Instagram can also prove useful sources to gather information about an individual, their lifestyle, and probably a hint to their weakness that can then be exploited.

The organization's website may also provide useful information about specific or key individualswithin the organization, such as the CEO, MD, head of the IT department, etc. The website can be used to source personal details such as email addresses, phone numbers, roles, etc. With the details, an attacker can then launch a social engineering attack to breach their target.

Press releases, blogs, newsgroups, and so on, are in some cases, used as the primary channels to gather information about an entity or employees.

Going through job requirements for a specific position within a company can also help an attacker identify the type of technology being used by a company and the level of competency oftheir workforce. An attacker can then decide on what method to use when breaching the targeted system from the data.

3. Active Attacks

An active attack involves closely examining the network to discover individual hosts and verify the validity of the gathered information, such as the type of operating system in use, IP address of the given gadget, and available services on the network, collected during the passive attack. It involves the risk of detection and can also be referred to as "**Active reconnaissance**" or "**Rattling the doorknobs**".

Active reconnaissance can be used to confirm the security measures put in place by an attacker, but at the same time, it can alert the victim if not well executed. The process may raise suspicion or increase the attacker's chance of being caught before they execute the full attack.

4. Scrutinizing and Scanning the Gathered Information

Scanning is a key step to intelligently examine after as you collect information about

the networkinfrastructure. The process has the following objectives;

Network scanning is executed to understand better the IP address and other relatedinformation about the computer network system.

Port Scanning – to identify any closed or open ports and services

Vulnerability scanning – to identify existing weak links within the system.

In the hacking world, the scrutinizing phase is also referred to as ***enumeration***. The objectiveof scrutinizing includes:

To validate the authenticity of the user running the given account, be it an individual or a groupof persons. To identify network resources and or shared resources

To verify the operating system and various applications that are running on the computer OS.

5. Attack

The **attack phase** is the last step in the attack process. It involves the hacker gaining and maintaining full control of the system access. It comes immediately after scanning and enumeration, and it launched sequentially as listed in the below steps.

Brute force attack or any other relevant method to bypass the password.Exploit the password.

Launch the malicious command or applications. If requires, then hide the files.

Cover the tracks, don't leave any trail that can lead back to you as the malicious third party. This can be achieved by deleting logs so that there is no trail for your illicit actions.

Q No.30 Discuss about DOS and DDOS Attacks?

Solution:- DoS and DDoS Attacks

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

DoS Attacks

In this type of criminal act, the attacker Hoods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely, The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.e., domain name

The United States Computer Emergency Response Team defines symptoms of DoS attacks toinclude

1. Unusually slow network performance (opening files or accessing websites)
2. Inability to access any website

3. Unavailability of a particular website
4. Dramatic increase in the number of Spam E-Mails received (this type of DoS attack istermed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intendeduser (i.e., legitimate users) of a service from using it. A DoS attack may do the following**:**

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

Classification of DoS Attacks

Bandwidth attacks: Loading any website takes certain time. Loading means complete webpage (ie., with entire content of the webpage — text along with images) appearing on the screen and system is awaiting user's input. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting, say forexample, 50 GB. Now if more visitors consume all 50 GB bandwidth then the hosting of the site can ban this site, The attacker does the same — he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service.

1. **Logic attacks**: These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
2. **Protocol attacks:** Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.
3. **Unintentional DoS**: This is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary sites regular users, potentially hundreds of thousands of people, click that link within a few hours and have the same effect on the target website as a DDoS attack.

Types or Levels of DoS Attacks

1. **Flood attack:** This is the earliest form of DoS attack and is also known as ping flood. Itis based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which result into more traffic than the victim can handle, This requires the attacker to have a faster network connection than the victim(i.e., access to greater bandwidth

than the victim). It is very simple to launch, but to prevent it completely is the most difficult.

2. **Ping of death attack:** The ping of death attack sends oversized Internet Control MessageProtocol (ICMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim.
3. **SYN attack:** It is also termed as TCP SYN Flooding. \n the Transmission Control Protocol (TCP), handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address).
4. **Teardrop attack:** The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various OSs due to a bug in their TCP/IP fragmentation reassembly code
5. **Smurf attack:** It is a way of generating significant computer network traffic on a victim network, This is a type of DoS attack that floods a target system via spoofed broadcast ping messages.
6. **Nuke:** Nuke is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. It is achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop

Tools Used to Launch DoS Attack

Various tools use different types of traffic to flood a victim, but the objective behind the attack and the result is the same: A service on the system or the entire system (i.e., application/website/network) is unavailable to a user because it is keptbusy trying to respond to an exorbitant number of requests. A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service.

l**. Jolt2-** A major vulnerability has been discovered in Windows' networking code. The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines — the attack causes the target machine to consume 100% of the CPU time on processing of illegal packets.

2. **Nemesy-** 'This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.

3. **Targa-** It is a program that can be used to run sight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.

4. **Ctazy Pinger**-This tool could send large packets of ICMP to a remote target network.

DDoS Attacks

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

Tools used to launch DDoS attack

1. **Trinoo** It is a set of computer programs to conduct a DDoS attack, It is believed that Trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit
2. **Tribe Flood** It is a set of computer programs to conduct various DDoS attacks suchas ICMP
3. **Network** (TFN) flood, SYN flood, UDP flood [It combines features of Trinoo with TFN and adds encryption] .
4. **Shaft** This network looks conceptually similar to a Trinoo; it isa packet Hooding attack and the client controls the size of the flooding packets and duration of the attack.
5. **MStream** It uses spoofed TCP packets with the ACK Hag set to attack the target, Communication is not encrypted and is performed through TCP and UDPpackets. Access to the handler is password protected. This program has a feature not found in other DDoS tools. It informs all connected users of access, successful or not, to the handler(s) by competing parties.

How to Protect from DoS/DDoS Attacks

1. Implement router filters. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files
8. Invest in and maintain "hot spares" — machines that can be placed into

service quicklyif a similar machine is disabled.

9.Invest in redundant and fault-tolerant network configurations.

10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.

11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Q No.31 How Cyber Criminals plan the Phishing and ID Theft?

Solution:- Phishing

The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

How Phishing Works?

Phishers work in the following ways

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 which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involvesE-Mail addresses and a webpage.
3. **Attack:** This is the step people are most familiar with the phisher sends a phony message that appears to be from a reputable source.
4. **Collection:** Phishers record the information of victims entering into web pages or pop-up windows.
5. **Identity theft and fraud:** Phishers use the information that they have gathered to make illegalpurchases or commit fraud.

.**Password Cracking**

Password is like a key to get an entry into computerized systems recovering passwords from data that like a lock. Password cracking is a process of have been stored in or transmitted by a computer system.

The purpose of password cracking is as follows:

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

Manual password cracking is to attempt to logon with different passwords. The attacker follows thefollowing 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.

Examples of guessable passwords include:

1. Blank (none)

2. the words like “password,” “pass code” and “admin”

3. series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwerty uiop4.user's name or login name;
5. name of user's friend/relative/ pet;

6. user’s birthplace or date of birth, or a relative’s or a friend's;

7. user’s vehicle number, office number, residence number or mobile number;

8. name of a celebrity who is considered to be an idol (e.g. actors, actress, spiritual gurus) by the user;

9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing.

Password cracking tools

1. **Default password(s):** Network devices such as switches, hubs and routers equipped with “default passwords” and usually these passwords are not changed after commissioning these devices into the network (i.c., into LAN).

2. **Cain & Abel:** This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.

3. **John the Ripper:** ‘This is a free and open-source software — fast password cracker, compatible with many OSs like different favors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.

4. **THC-Hydra:** It is a very fast network logon cracker which supports many different services.

5. **Air crack-ng:** It is a set of tools used for wireless networks. This tool is used for 802.1 1a/b/g wired equivalent privacy (WEP) and Wi-Fi Protected Access (WPA) cracking.

6. **Solar Winds:** It is a plethora of network discovery/monitoring/attack tools and has created dozens ofspecial-purpose tools targeted at systems administrators

7. **Pw dump:** It is a Window password recovery tool, Pw dump is able to extract pw dump NTLM and Lan Man hashes from a Windows target, regardless of whether Sys key is enabled. It is also capable of displaying password histories if they are available.
8. **Rainbow Crack:** It is a hash cracker that makes use of a large-scale time-memory trade-off, A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords.
9. **Brutus:** It is one of the fastest, most flexible remote password crackers available for free. It is availablefor Windows 9x, NT and 2000.

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

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

Online Attacks

The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack.". When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server. This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also used to get the passwords for financial websites that would like to gain the access to banking websites.

Offline Attacks

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

Different types of password Cracking attacks:

- Dictionary attack : Attempts to match all the words from the dictionary to get the password
- Hybrid attack : Substitutes numbers and symbols to get the password
- Brute force attack : Attempts all possible permutation-combinations of letters,numbers and special characters

Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack

.Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak.

Here are some of the examples of "weak passwords":

1. Susan: Common personal name;
2. aaaa: repeated letters, can be guessed;
3. rover: common name for a pet, also a dictionary word;
4. abc123: can be easily guessed;
5. admin: can be easily guessed;
6. 1234; can be easily guessed;
7. QWERTY: a sequence of adjacent letters on many keyboards;
8. 12/3/75: date, possibly of personal importance;
9. nbusr123: probably a username, and if so, can be very easily guessed;
1. p@$$\/\/Ord: simple letter substitutions are preprogrammed into password cracking tools;
11. _ password: used very often — trivially guessed;
12. December12: using the date of a forced password change is very common.

A strong password is long enough, random or otherwise difficult to guess — producible only by the userwho chooses it.

Here are some examples of strong passwords:

1. Convert_£100 to Euros!: Such phrases are long, memorable and contain an extended symbol toincrease the strength of the password.
2. 382465304H: It is mix of numbers and a letter at the end, usually used on mass user accounts and suchpasswords can be generated randomly, for example, in schools and business.
3. 4pReelai@3: Ir is not a dictionary word; however it has cases of alpha along with numericand punctuation characters.
4. MoOoofin245679: It is long with both alphabets and numerals.
5. t3wahSetyeT4: It is not a dictionary word; however, it has both alphabets and numerals.

<u>Random Passwords</u>

Forcing users to use system-created random passwords ensures that the password will have no connection with that user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also includes password aging; the users are required to choose new passwordsregularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training.

The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names orphrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not becoded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed logon attempts. All erroneous password entries shouldbe recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require thepasswords to be re-entered.
8. Successful logons should display the date and time of the last logon and logoff.
9. Logon IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Netizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should bephrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password used previously should not be used while renewing the password.

6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts has been accessed from public Internet facilities such as cyber cafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber attacks.
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the web links displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks.
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

Q No.32 Discuss about Intellectual Property Issues?

Solution:- Several issues in intellectual property (IP) continue to evolve and pose challenges in the modern world. Here are some notable issues:

Globalization:

Challenge: Differing IP laws and standards across countries.

Impact: Difficulty in enforcing and protecting IP globally.

Digital Piracy:

Challenge: Digital piracy is a common problem in the digital age.

Impact: Loss of revenue for creators and businesses.

Open Source and Collaboration:

Challenge: Balancing open-source initiatives with traditional IP protection.

Impact: Altered business models and collaborative innovation.

Biotechnology and Gene Patents:

Challenge: Patenting genes and biotechnological innovations.

Impact: Ethical concerns, potential misuse, and restricted access to genetic information.

Artificial Intelligence (AI) and IP:

Challenge: Determining ownership and protection of AI-generated works.

Impact: Uncertainty in legal frameworks for AI-generated content.

Patent Quality and Patent Trolling:

Challenge: Issues with the quality of granted patents.

Impact: Rise of patent trolls exploiting weak patents for litigation.

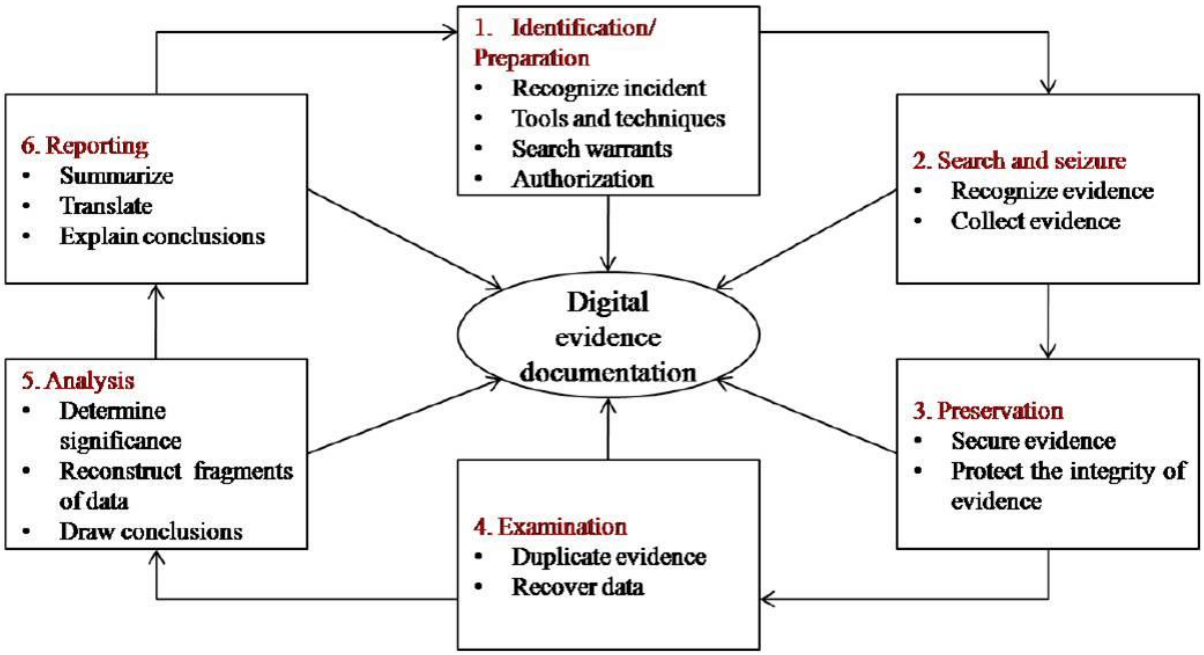
Access to Medicines and Public Health:

Challenge: Balancing IP protection with providing affordable access to medicines.

Impact: Debate over the role of IP in public health crises.

Data Protection and IP:
Challenge: Protecting IP in the age of big data and data-driven innovations.
Impact: Privacy concerns and potential misuse of sensitive data.
Emerging Technologies:
Challenge: Rapid advancements in areas like blockchain, 3D printing, and nanotechnology.
Impact: Struggling to adapt existing IP laws to new technological landscapes.
Fair Use and Digital Rights:
Challenge: Defining the boundaries of fair use in the digital era.
Impact: Confusion over what constitutes fair use, especially in online environments.
Enforcement and Border Control:
Challenge: Enforcing IP rights, particularly in the online space.
Impact: Difficulty in preventing the flow of counterfeit goods across borders.
Cultural Appropriation:
Challenge: Protecting traditional knowledge and cultural expressions.
Impact: Disputes over the use of cultural elements without proper attribution or permission.
Climate Change and Green Technologies:
Challenge: Encouraging innovation in green technologies while protecting IP.
Impact: Balancing environmental concerns with traditional IP incentives.

Q No.33 How Digital Forensics Life Cycle Works?
Solution:- Digital Forensics Life Cycle
The digital forensics process is shown in the following figure. Forensic life cycle phases are:
1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution
6. Reporting
7. Testifying



Preparing for the Evidence and Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras
- Hard drives

- CDs
- USB memory devices

Non-obvious sources can be:

- Digital thermometer settings
- Black boxes inside automobiles
- RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:
Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device.

- Establish and maintain the chain of custody.
- Document everything that has been done.
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)
- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.
Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd

- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter

- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law.