UNIT-1

1. What is Information and CIA Triad?

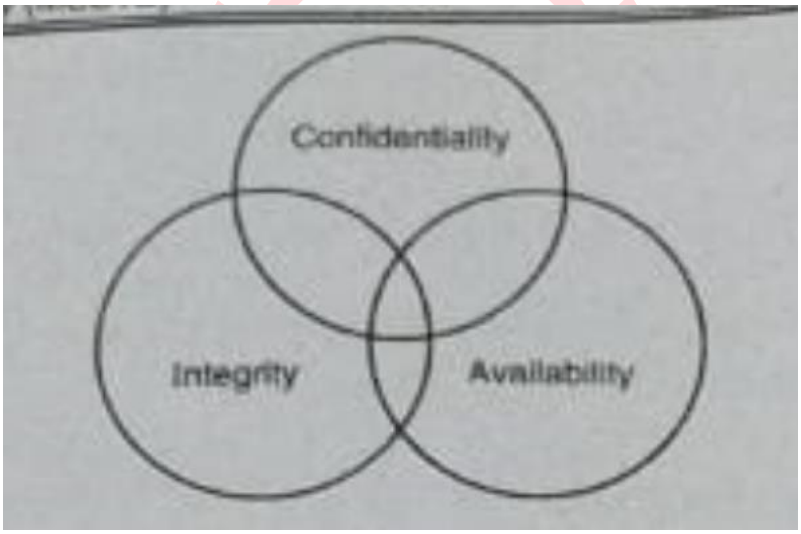
Ans:

Information:

- Information is an asset of any organization.
- Information is classified according to the sensitivity and its vulnerability for theft or misuse
- Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company
- In order to protect their data against any security threats using:
- Risk Assessment Methodology to identify its critical resources and possible areas of risk
- If any risks are identified then the company should develop an extension plan to mitigate the attacks.
- A Company should also have Business Continuity Plan and Disaster Recovery Plan ready so that the business operations can be continued in case of a Security attack.

CIA Triad:

CIA Triad is a well-known securely model used for the development of security policies



Confidentiality:

❑ Confidentiality means that only the authorized individuals or systems can view sensitive or classified information

❑ The data being sent over the network should not be accessed by unauthorized individuals

❑ Attacker may try to capture the data using different tools available on the Internet and gain access to the sensitive information.

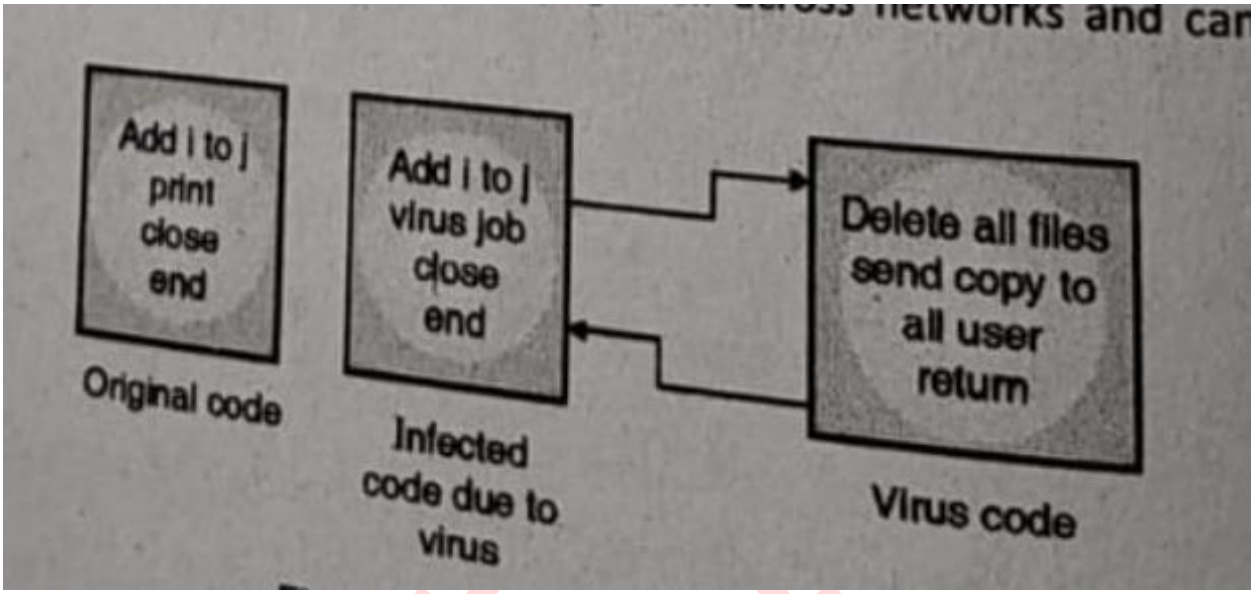
Integrity :

❑ Integrity means that the data has not been altered in an unauthorized way.
❑ Main goal of integrity controls is to block the ability of unauthorized people to make changes to data, and to provide a means of restoring data back to the original state.
❑ Corruption of data is a failure to maintain data integrity

Availability :
❑ Availability means that the data should be readily available to its users when needed. This applies to systems and to data.
❑ Availability can be ensured by implementing high-availability or continuous service controls on computer networks, and storage, making regular upgrades, having a plan for fail over like backups etc. and prevent bottleneck in a network.

2. What is Virus , types of virus and different phases of virus? How to deal with virus?
Ans:

- A virus is a code that attaches itself to another code which causes damage to the computer system
- It is a piece of code which is loaded onto the computer without individuals knowledge and runs against their wishes.
- It can replicate them
- Any simple virus can be dangerous because it will quickly use all available memory space and bring the system to an halt.
- Whereas, dangerous viruses are capable of transmitting itself across networks and can be able to avoid security systems.



Phases of Viruses

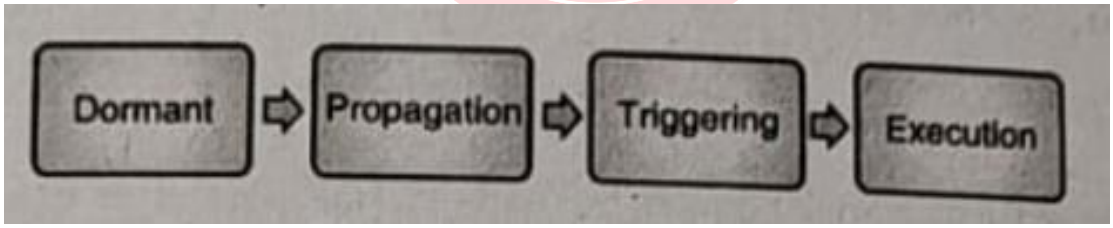
During its lifetime, a typical virus goes through the following four phases:

❑ Dormant Phase :- The virus is idle and eventually activated by some event

❑ Propagation Phase :- The virus places are identical copy to itself into other programs or into certain system areas on the disk

❑ Triggering Phase :- The virus is activated to pearform the function for which it was intended.

❑ Execution Phase :- The function is performed



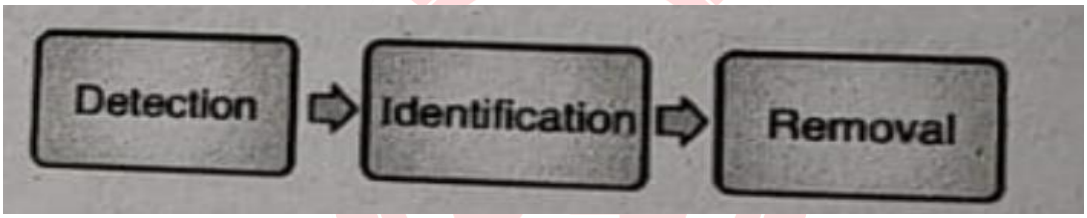
Types of Virus

- Parasitic Virus :- It attaches itself to executable code and replicates itself. When the infected code is executed, it will find other executable code or program to infect.
- Memory resident virus :- This type of virus lives in the memory after its execution. It inserts themselves as a part of operating system or application and can manipulate any file that is executed, copied or moved.

- Boot Sector Virus:- This type of virus infects the boot record and spread through a system when system is booted from disk containing virus
- Overwriting Virus:- This type of virus overwrites the code with its own code.
- Macro Virus:- These viruses are not executable,it affects Microsoft Word like documents. They can spread through emails.
- Companion virus:- This is the virus which creates a new program instead of modifying an existing file.
- Email Virus:- Virus gets executed when email attachment is open by recipient. Virus send itself to everyone on the mailing list of the sender.

Dealing with virus :

- Preventing the virus is always a good option.
- There is no direct way to test/ find the hidden code but we can attempt to detect, identify and remove viruses.



- Detection:- Find out the location of virus
- Identification :- Identify the specific virus that has attached.
- Removal :- After identification, it is necessary to remove all traces of the virus and restore the affected file to the original state with the help of anti virus.

3. Difference between Worms and Virus?

Table 1.3.1 : Difference between worm and virus

Sr. No.	Virus	Worm
1.	A virus is a piece of code that attaches itself to legitimate program.	A worm is a malicious program that spread automatically.
2.	Virus modifies the code.	Worm does not modify the code.
3.	It does not replicate itself.	It replicate itself.
4.	Virus is a destructive in nature.	Worm is non destructive in nature.

4. What is Trojan , insider and intruders?

Ans:

Trojan:

- Trojan horse is a hidden piece of code, it allows an attacker to obtain confidential data.

- Main purpose of Trojan Horse is to reveal confidential information to an attacker.
- For example:- Trojan Horse can hide in code for login screen. When the user enters the user id and password, the trojan horse captures the details and transfer it to the hacker without knowledge of authorized user.
- The attacker then can use the information to gain the access to the system.

Insider:

- Insiders have the access and necessary knowledge to cause immediate damage to an organization. Hence, Insiders is more dangerous than outside intruders.
- Many securities are designed to protect the organization against outside intruders and so they lies at the boundary between the organization and the rest of the world.
- Insiders may already have all the access to carry out criminal activity like fraud. Also frequently the insiders have knowledge of the security systems in place and will be better able to avoid detection.
- Employees are not the only insiders within the organization but there are number of other individuals who have physical access to facilites like contractors or partners, may not have physical access to the organizations facilities but may also have access to computer systems and networks.

Intruders:

- An intruder is a person who enters the territory that does not belongs to that person.
- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system.
- This is one of the most publicated threats to security. There are three classes of intruders:-
  - Masquerader :- An individual who is not authorized to use the computer and who enters a systems access controls to use a legal user's account
  - Misfeasor :- A legitimate user who accesses data, programs or resources for whom these access is not authorized , or who is authorized for such access but misuse his or her privilege.
  - Clandestine/ Secret User :- An individual who hold managerial control of the system and uses this control to avoid auditing and access controls or to suppress audit collections.
- Generally, the masquerader is an outsider, Misfeasor is an insider and Secret User can either be insider or outsider.

5. What is attack and types of attack?

Ans:

Attack is a path or way by which hacker can gain access to computer system without your prior knowledge:

Types:-

1. Active Attack:- In active attacks, the contents of the original message are modified in some way. These attacks cannot be prevented easily.

Interruption:

- It causes when an unauthorized user pretends to be another user

Modification:

- It contains replay attack and alterations. A user captures a sequence of event and re-sends it. Alteration involves some modification/changes to the original message.

Fabrication:

- It is an attempt to prevent authorized users from accessing some services. E.g. Denial of Service (DoS) attacks.

2. Passive Attack:- Passive attacks are those, where attacker aims to obtain information that is in transit. In passive attack, attacker does not involve any modifications to the contents of an original message. So, the passive attacks are hard to detect.

Release of Message Contents:

- Release of message contents means a confidential message should be accessed by authorized user otherwise a message is released against our wishes.

Traffic Analysis:

- Traffic analysis is a passive attacker may try to find out similarities between encodes message for some clues regarding communication and this analysis is knows as traffic analysis.

6. What is DoS and explain the different types of DoS?

Ans:

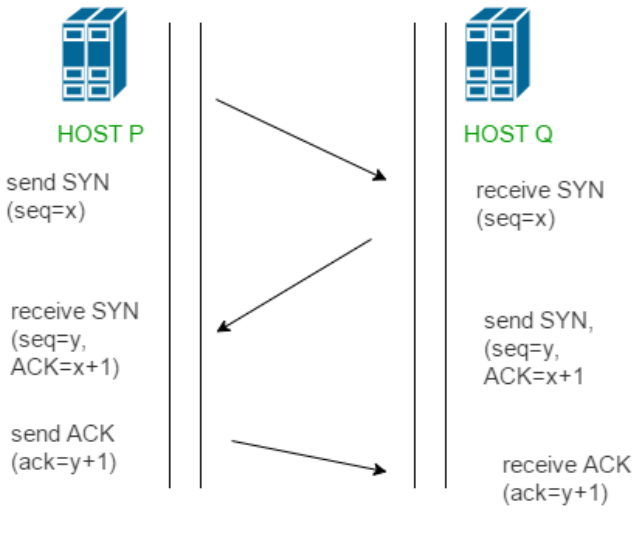
- DoS attack is a type of attack which can exploit a know vulnerability in a specific application or OS, or may attack features or weaknesses in particular protocols or services.
- Using this attack, attacker attempts to deny unauthorized access to specific information or to the computer system or network itself.
- Aim of this attack is to simply prevent access to the target system, or the attack can be used in combination with other actions in order to gain unauthorized access to a computer or network. E.g:- SYN Flooding attack and POD attack.
- DoS attacks are conducted using a single attacking system.

SYN Flooding Attack:

- SYN Flooding attack, used to prevent the services to the system. It takes the advantage of trusted relationship and TCP/IP networks design. This attack uses TCP/IP three-ways handshake for connection between two systems.

Three-way Handshake:

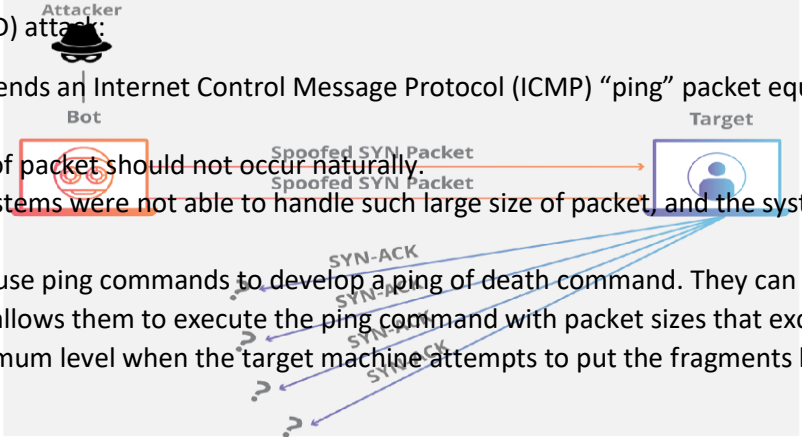
- Step 1(SYN):- In first step, the clients want to establish a connection with a server, so it sends a segment with SYN which informs the server that the clients wants to start a communication and with that sequence number it starts the segments with.
- Step 2(SYN + ACK):- Server responds to the client request with SYN ACK signal bit set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with.
- Step 3(ACK):- In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.



SYN Flooding Attack:

- In SYN Flooding Attack, the attacker sends a high volume of SYN packets to the targeted server, often with Spoofed IP Addresses.
- The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
- While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, once all the available ports have been utilized the server is unable to function normally.

Ping-of-death (POD) attack:

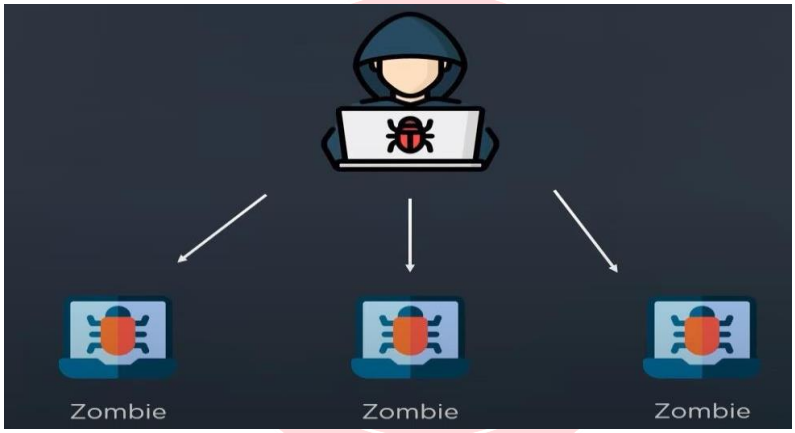


- Attacker sends an Internet Control Message Protocol (ICMP) “ping” packet equal to or exceeding 64 kB.
- This type of packet should not occur naturally.
- Certain systems were not able to handle such large size of packet, and the system would hang or crush.
- Attackers use ping commands to develop a ping of death command. They can write a simple loop that allows them to execute the ping command with packet sizes that exceed the 65,535-byte maximum level when the target machine attempts to put the fragments back together.

7. What is DDoS?

Ans: Distributed Denial of Service (DDoS):

- Denial of Service attack is using multiple attacking system which are known as Distributed Denial of Service (DDoS) attack.
- Goal is to deny the use or access to specific service or system.
- In DDoS attack the method is used to deny a service by simply overwhelm the target with traffic from many different systems.
- This attack is a two-step process.
- In the first step, the attacker creates multiple botnet also called as Zombies.
- Attacker uses this zombies to attack on the targeted system whenever the attacker initiates it using malware infusion.



- Then these bots flood the target with continuous requests that causes the server system to crash.
- One important thing of a DDoS attack is that with just a few messages to the agents, the attacker can have a flood of messages sent against the targeted system.
- To stop or mitigate the effects of DoS and DDoS attack, one important precaution is to be taken that is apply the latest patches and upgrades to your system ad the application running on them.

8. What is Sniffing, Spoofing, Man-in-middle, replay and TCP/IP Hijacking attacks?

Ans:

Sniffing:

- Sniffer is an application that can capture network packets. Sniffers are also known as network protocol analyzers.
- Objective of Sniffing is to steal:
  - ❑ Password (from Email, Web Site, FTP, TELNET, etc.)
  - ❑ Email Text
  - ❑ Files in transfer
- A network sniffer is a software or hardware that is used to observe the traffic, it passes through a network on shared broadcast media.
- These devices can be used to view all traffic, or it can target a specific protocol, service, or even string of characters like logins.
- Network administrators for monitoring network performance can use network sniffers. They can be used to perform traffic analysis. For example, in order to determine what type of traffic is most commonly carried on the network and to determine which segments are mot active.
- They can also be used for network bandwidth analysis and to troubleshot certain problems such as duplicate MAC addresses.
- Contents of the email messages can be viewed by the sniffers which travel across the network
- Packet Sniffing:- It is a passive attack, attacker does not hijack the conversation but he will observe the packets as they passed by.

- In order to prevent sniffing:-
  - ❑ The information that is travelling can be encoded.
  - ❑ The transmission link can be encoded.

Spoofing:

- Spoofing is making data similar to it has come from a different source. This is possible in TCP/IP because of the friendly assumptions behind the protocols.
- The assumption at the time of protocol development is that an individual who is having access to the network layer will be privileged users who can be trusted.
- When a packet is sent from one system to another, it includes not only the destination IP address and port but the source IP address as well. This is one of the several forms of spoofing.
- Spoofing Email
  - • E-mail spoofing can be easily accomplished, and there are several different ways to do it and programs that can assist you in doing so.
  - • E-mail Spoofing refers to a mail that appears to have been originated from one source but, it was actually send from another source. Best example of Email spoofing is Spam Mail and Junk mails.
  - • There are simple ways to determine that an e-mail message was probably not sent by the source, but most users do not question their e-mail and will accept it.
- URL Spoofing:-
  - An attacker acquires a URL to close to the one they want to spoof so, that e-mail sent from their system appears to have come from the official site.
  - For example, if attackers wanted to spoof XYZ Corporation, which owned XYZ.com, the attackers might take access to the URL XYZ.Corp.com. An individual receiving a message from the spoofed corporation site would not normally suspect it to be spoof but would take it to be official.

Man-in-Middle Attack:

- A man-in-middle Attack, generally occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view and/or modify the traffic.
- This will do by making sure that all communication going to or from the target host is routed through the attackers host.
- Then the attacker can be able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received.

Replay:

- A replay attack is an attacker captures a portion of a communication between two parties and retransmits it after some time.
- For example, an attacker might replay a series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times.
- The best way to prevent replay attacks is with encryption, Cryptographic authentication, and time stamps.

TCP/IP Hijacking:

- TCP/IP hijacking is the process of taking control of an already existing session between a client and a server.
- Main benefit to an attacker of hijacking over attempting to enter a computer system or network is that the attacker doesn't have to avoid any authentication mechanisms, since the user has already authenticated and established the session.
- When the user completed its authentication sequence, the attacker can then take the session and carry similar to the attacker, and not the user, had authenticated with the system.
- To prevent the user from noticing anything unusual the attacker may decide to attack the users system and perform DoS attack on it, so that the user and the system, will not notice any unusual traffic that is taking place.

9. What is security and need of Security ?

Ans:

- Information is a resource fundamental to the success of any business information is a combination of following three parts:-
    1. Data:- It is a collection of all types of information which can be stored and used as per requirement. For example:- personal data, medical information, accounting data, etc.
    2. Knowledge:- It is based on data that is organized, synthesized or summarized and it is carried by experienced employees in that organization
    3. Action:- It is used to pass the required information to a person who needs it with the help of in format
- Information is a important asset and need to be protected all the time.

10. What is Operating System Updates?

Ans:

- Operating systems are large and complex mixture of interconnected software modules written by several of separate individuals.
- when operating systems is continually growing and introduces new functions then the potential Tor problems with that code will also increase.
- It is almost not possible for an operating system vendor to test their product on each possible platform under every possible situation, so the functionality and security issues are occurred after released of operating system.
- To the standard user or system administrator is constant stream of updates designed to correct problems, replace sections of code, or even add new features to an installed operating system. Vendors typically follows a hierarchy fo software updates given below :

Hotflix:

- Normally this is a term given to a small software update designed to address a particular problem like buffer overflow in an application that exposes the system to attacks.
- Hotfixes are typically developed in reaction to a discovered problem; they are produced and then released rather quickly.

Patch:

- This terms generally applied to a more formal larger software update that may address several or many sower problems.
- Patches often contain improvements or additional capabilities and fixes for known bugs. Patches are usually developed over a longer period of time.

Service pack:

- Usually this term is given to a large collection of patches and hotfixes that are rolled into a single, rather large package.
- Service packs are designed to bring a system up to the latest known, good level all at once, rather than requiring the user or system administrator to download several of updates separately.

- Like from LINUX to Windows each and every operating system needs software updates, and every operating system has different methods of helping users in keeping their system up-to-date. For example, Microsoft provides updates, which needs to be downloaded from web site.
    - By selecting Windows Update from the Tools menu in Internet Explorer users will be taken to the Microsoft web site.
    - By selecting Scan for Updates, users can allow their systems to be examined for needed or required updates.
- The web site will identify which updates the user's system needs and will provide the user with the option to download and install. Although this typically requires admin or powerful user level access for update process for most users.
- Microsoft also provides an automated update functionality that will, once configured, locate any required updates, download that update to your system, and also install the updates. The active Internet connection is required for both the web-based updates and automatic updates to retrieve information and updates from Microsoft's site.
- Not only Microsoft is providing such utilities for users in keeping their systems up-to-date and secure but also the latest versions of Red Hat Linux contain a utility called the Red Hat Update Agent, which does the same thing.
- By registering your system and user profile with Red Hat, you can get a customized list of updates for your specific system.
- It is important to keep the system updated, regardless of the method used to update the operating system. Much like the steps taken to baseline and initially secure an operating system, keeping every system patched and up-to-date is critical to protecting the system and the information.

UNIT-2

1. What is Identification and Authentication?

Ans:

- When user logged on to a computer, he performs two tasks:
    - Identification: Enter username and password.
    - Authentication : Prove that you are who claim to be.
- After entering username and password, the computer will compare this input against the entries stored in password file.

- Login is successful if username and password is valid and if wrong then login is fail.
- Many systems count the fail login attempts and prevent or deny next attempt when threshold has been reached.
- Now a day, many computer systems use identification and authentication through username and password as first step of protection.
- This mechanism is widely accepted because it is not very difficult to implement.
- But managing password security can be quite expensive and obtaining a valid password is a common way of gaining unauthorized access to a computer system.
- A password must be set to user account or else attacker can:
  - Intercept the password when a new user account is created.
  - Attempt to guess the password.
  - Get password from user through attacks like spoofing or phishing.
  - Get password from system by social engineering attack or by accessing password file.
- User plays an important role in password protection. Authentication can be compromised when user disclose their passwords either by telling to someone or by writing it down in some place where people can find it.

2. What is Guessing password and how to prevent it?

Ans:

- Password selection is critical issue because of attacks of guessing a valid password.
- Generally attackers are following two basic password guessing strategies:
  - Exhaustive Search : Here attacker tries all possible combinations of valid symbols till certain length. For Example - Brute Force attack.
  - Intelligent Search : Here attacker searches a password with the help of user's personal information like name, birth date, family members name, phone number etc. Many times attacker tries popular passwords.
  - For Example - Dictionary attack (trying all passwords from dictionary).
- Hence, following are some protections techniques which can be used by users:
  - Default password : Many times the default accounts like admin has default passwords like admin. If such passwords are not changed by system admin then it will help attacker to enter into the system easily.

- Length of Password: To avoid exhaustive search, set the length of password like in UNIX system password length is 8 characters long.
- Format of Password : Password should have at least combination of the following elements.

1. One or more uppercase letters (A-Z)

2. One or more lowercase letters (a - z)

3. One or more numerals (0 - 9)

4. One or more special characters or punctuation marks (! @#$%A and*,:;?)

- Avoid obvious passwords : May attackers have list of popular passwords and they can use dictionary attacks to catch the obvious passwords, hence it is best practice to avoid such kind of passwords.
- Here are some techniques that system can follow to improve password security.
  - Password Checkers: In this scheme the system periodically runs its own password I cracker program to find out guessable or weak passwords. If the systems find any such a password, then system cancels it. Here System can notify and prevents the user from selecting such passwords. This scheme will prevent dictionary attacks against the system. This method has a number of drawbacks - It is resource intensive if the job is done right. Because a strong-minded opponent who is able to steal a password file can dedicate full CPU time to the task for hours or even days.
  - Password Generation : Many operating systems can produce Computer-generated passwords. The passwords are reasonably random in nature and can be pronounceable. In scheme, users are not allowed to select the own passwords. Drawback of this scheme is Even though the password is pronounceable, the user may have difficulty in remembering it.
  - Password Aging : In many systems, the password can be set with its expiry dates. In such systems, they force their users to change passwords at regular intervals. Some additional mechanisms can be provided to prevent users from selecting previous password. For Example -list previous 10 passwords used by user.
  - Limit login attempts : In many systems, monitoring mechanisms can be used to check unsuccessful login attempts. If found, then lock the user account completely or at least for certain time period. This will prevent and discourage further attempts.
- Many time users not in favour of remembering long and complicated passwords. Hence, they write it down on a piece of paper which is kept near the computer, where it is useful for both legitimate users and to potential intruders.

- So, this will add a task to security manager to search for such password notes posted on computer terminals and notify to the user.
- When passwords are changing frequently and users who find it difficult to change password are tempted to choose passwords which are easy to remember.
- If password is forgotten by user and asked for new password then user should follow all password precautions. When changing any password, it is good advice to type it several times as well as not to change password before weekends or holidays.

3. What are the types of password attacks and explain it and also how to prevent it?

Ans:

Piggybacking:

- Piggybacking is the simple approach of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.
- In this way an attacker can gain access to the facility without knowing the access code or acquiring an access card. E.g. Access of Wireless Internet connection by bringing one's own computer within range of another's Wireless connection and using that without subscriber's explicit permission.

Shoulder Surfing:

- Shoulder surfing is a similar procedure, where an attackers position themselves in such a way that he is able to observe the authorized user entering the correct access code.
- This attack is by direct observation techniques, like looking over some one when he is entering a PIN or password etc.
- Both of these attacks can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions.

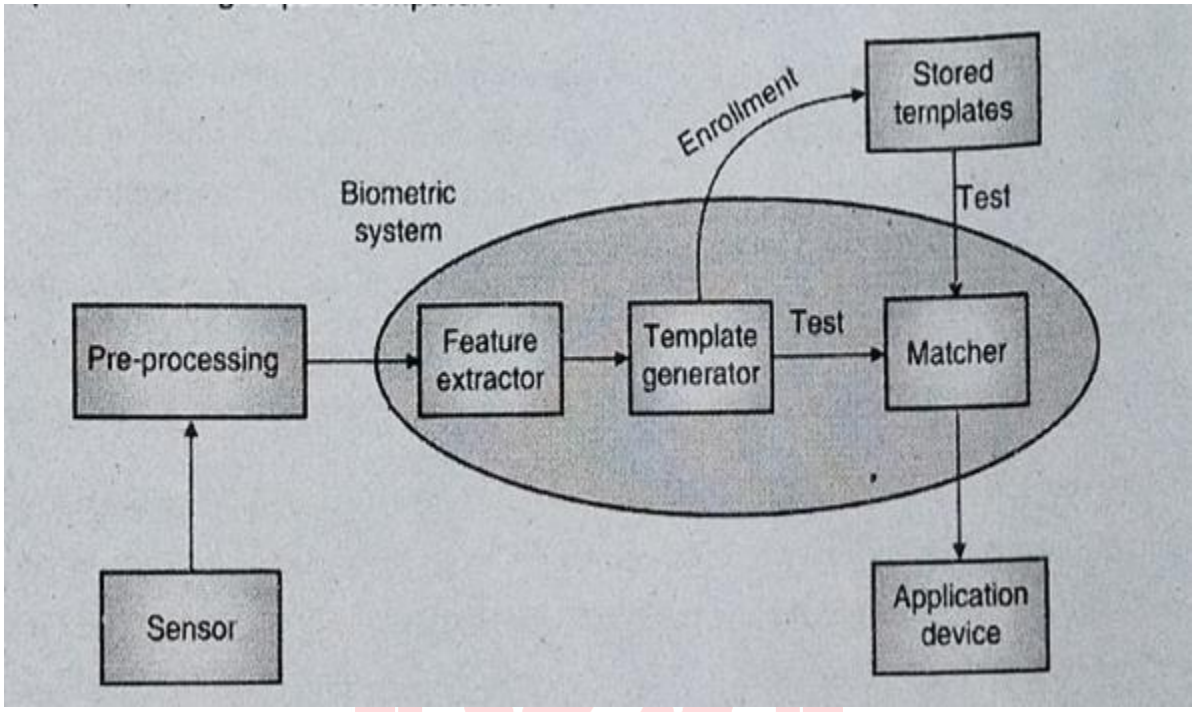
Dumpster Diving:

- Dumpster diving Is the process of going through a target's trash in order to find little bits of information. In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry Out an attack on a computer network.

- Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Innocent information like a phone list. calendar, or organizational chart can be used to assist an attacker to gain access to the network.
- To prevent dumpster divers from learning anything valuable from the trash, experts recommend that the company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.
- Attackers always need a certain amount of information before attack. If the attacker is in the surrounding area ot the target, one common place to find this information is to go through the target's trash in order to find little bits of information that could be useful. This process of going through a target's trash is known as dumpster diving.
- If the attackers are very lucky, and the target's security procedures are very poor, they may actually find user IDs and passwords. We have studied earlier that the users sometimes write their password down. When the password is changed, they discard the paper where the old password was written on without shredding it and in this way the lucky dumpster diver can get a valuable clue.
- Even though the attacker is not lucky enough to obtain a password directly, they can found the name of employee and from that it's not hard to determine user IDs for attackers.
- From hardware or software manuals, which is purchased by user may also provide clues as what vulnerabilities exist on the target's computer systems and networks. Like this by many ways the attacker may gather a variety of information, which can be useful in a social engineering attack.

4. What is Biometric Access control? Explain it with diagram and also advantage and disadvantage of the same? (explain with diagram).

Ans:



- Access controls are not the only methods to limit the unauthorized access to the system. Some new approach is to utilize something unique about the individual, like their fingerprints to identify them. The something you are method is known as biometrics.
- The idea of biometrics is very simple to grasp, but the implementation can be e very difficult to realize. The difficulty does not come from the gathering of the actual measurements but from the analysis of these measures. Other methods to accomplish biometrics include handwriting analysis, retinal scans, iris scans, voiceprints, hand geometry, systems and networks and also and facial geometry etc. Biometrics can be used to control access to computer as a physical access control device.
- Biometrics is the idea to map measurements of human physical characteristics to human uniqueness. If this can be accomplished in a reliable, repeatable fashion, the verification and identification of human individuals by machine becomes a reality. To that end, biometrics is a combination of human physiology, pure mathematics, and engineering.
- Hand geometry requires a fairly large device. This device can he easily placed outside of a door to control access to the room but this will not be convenient to control access to a computer system, because a reader need to placed with each computer or with groups of computers.

- Simply verifying someone's identity is much less complex than identifying a person. Verification vs. Identification might seem like semantics, but think about the difference between checking someone's driver's license photo and recognizing someone in a room who you have not meet yet.
- For example, verification involves telling a biometric system that she is actually Marry and then uses one or more set of biometric information to verify that she is actually Marry. Identification will be Marry walking up to a set of Biometric sensors and being recognized as Marry.
- Depending on the application and objective. different "form factors" are more appropriate.

5. Explain the types of Biometric?

Ans:

1. Fingerprint:

- A fingerprint is the pattern of ridges and furrows on the surface of the fingertip and it is unique across the entire human population.
- Fingerprint involves a finger size identification sensor with a very low cost biometric chip.
- Automated fingerprint recognition and matching system extract a number of features from the fingerprint for storage as a numerical substitute for the full fingerprint pattern.
- This is the best option for most uses of biometric verification and it is specially attached to specific Computer and network assets.

2. Hand Print:

- Handprint is usually most appropriate for fixed physical locations requiring very high assurance to identify, since it combines the hand biometric with essentially five different fingerprints biometrics.
- These systems identify features of the hand, including shape, and lengths and widths of fingers.
- Handprints are used primarily for the traditional applications like data rooms, sensitive office zones/buildings, national security/intelligence facilities, and vaults etc.

3. Retina:

- Retina scan involves the examination of the unique patterns on the back of a person's eye.
- The Retina pattern formed by veins beneath the retinal surface. It is unique and hence suitable for identification.

- A retinal biometric system obtains a digital image of the retinal pattern by projecting a low-intensity beam of visual o infrared light into the eye.

4. Voice/Speech Patterns:

- This type of verification using speech/voice is uniquely interesting because no specialized recording device required.
- Voiceprint verification is completely a part of the algorithms and analysis software. This mechanism can be able to use for phone-based applications such as voice response systems and time card entry.
- The use of voice verification will increase the possibility to protect remote data reporting applications and hence t will be more convenient in the criminal justice and healthcare industries.
- Many databases could be made much more reliable if each criminal had to call in periodically to provide updated contact information. The entry could be authenticated via his or her unique voice pattern and recorded. Any offenders who missed their deadline to call in would be flagged for further investigation.

5. Signature and Writing Patterns:

- Every individual has a unique style of handwriting.
- This is reflected especially in the signature, which is typically a frequently written sequence.
- However, multiple signature samples from a single individual will not be identical. This complicates the task of developing a computer representation of the signature that can be matched to future samples.
- Biometric verification via handwriting or signature must be distinguished from simple signature capture pads.
- A signature capture pad, which simply records an image of what the person wrote, biometric enabled capture pads actually record the pressure, distance of strokes, and speed of writing.
- These data points enable biometrically verifying whether the person writing the signature is indeed the same person who supplied the original enroll1ment sample.
- Biometric signature verification is particularly interesting to the financial and legal communities because it is substantially less obtrusive and requires less behavior modification. It still feels like a signature- just digitally captured.

6. Keystrokes:

- Keystroke biometrics refers to the art and science of recognizing an individual based on an analysis of his typing patterns.

- Biometric authentication and classification procedures have traditionally been implemented using physiological traits such as fingerprints, retinas, and face, or using behavioural traits such as voice. The concept of keystroke biometrics has arisen as a hot topic of research only in the past two decades.
- Biometrics based on typing patterns is distinctive in that they are cheaper to implement, more distributed, and more unobtrusive than conventional biometric procedures.
- Collecting data regarding a person's typing patterns simply requires a keyboard and some basic software to collect data.
- Data collection software is easily replicable whereas hardware is not. Because the primary hardware requirement for keystroke biometrics is a keyboard, keystroke biometrics can be collected from virtually anywhere throughout the world via an Internet connection without requiring an individual to be at certain locations with access to specialized hardware.
- Moreover, because each keystroke is captured entirely by the key pressed, the press time, and the release time, the data can also be transmitted using low bandwidth.
- The growth or Internet connectivity thus makes distributed mechanisms for authentication increasingly feasible and attractive.
- A final advantage of keystroke biometrics is that it is a relatively unremarkable measure. Fingerprint, retina, and face scans all inconvenience the user by requiring him to place a particular body feature either within or in-front of some machinery. By contrast, typing on a keyboard is already a daily activity for many people; thus, keystroke biometrics can be easily integrated into a person's daily routine.

6. Explain access control with respect to security?

Ans:

- Use of physical access controls is the same as that of computer and network access controls - to restrict access to unauthorized users. Physical access controls can be based on following points:
    1. Something the individual has,
    2. Something they know, or
    3. Something they are
- The most common physical access control device is a lock. Combination locks are depends on something the individual knows i.e. combination and the Locks with keys depend on something the individual has ie. key. Each of these has some advantages and disadvantages.
- In addition to locks, there are some other common physical security devices like video cameras and sign-in logs.

- Sign-in logs provides a record of access, and when these are used in combination with a security guard who checks an individual's identity, they can put off potential adversaries from attempting to gain access to a facility.
- Most common access control mechanism is a human security guard.
- Many organizations employ a guard to provide an extra level of checking of individuals who want access. A human guard can apply common sense to situations that might have been unexpected but other devices are limited to their designed function. Having security guards also addresses the common practice of piggybacking.
- Suppose one employee enters the combination and then opens the door. another individual may follow the employee before the door closes to avoid re-entry of the combination. A security guard checking each individual's identification will eliminate such a type of problem.

7. Difference between Authentication and Authorization?

Ans:

8. What is Access Control Matrix and Access Control List ?

Ans: Access Control Matrix:

- Activity in the system is initiated by entities known as subjects to access an object.
- Subjects are typically users or programs executing on behalf of users. An object is a passive entity that contains the information like -Computer, Database, File, Program etc.
- A user may sign on to the system as different subjects on different occasions, depending on the privileges the user's wishes to exercise in a given session.
- The subject-object difference is basic to access control. Subjects initiate actions or operations on objects. These actions are permitted or denied according to the authorizations established in the system.
- Authorization is given in terms of access rights or access modes. The meaning of access rights depends upon the object in question. For example, Files -the typical access rights are Read, Write, Execute and Own.
- An Access Control Matrix (ACM) provides the simplest framework for showing the process. It is a conceptual model which specifies the rights that each subject possesses for each object.
- There is a row in this matrix for each subject, and a column for each object. Each cell of the matrix specifics the access authorized for the subject in the row to the object in the column.

- The task of access control is to ensure that only those operations authorized by the access control matrix that actually get executed. This is achieved by means of a reference monitor, which is responsible tor mediating all attempted operations by subjects on objects.
- The access control matrix model clearly separates the problem of authentication from that of authorization.
- An example of an access control matrix is provided in Table 2.3.1.

Table 2.3.1

User	Process 1	Process 2	File 1	File 2	Printer
John	Read, Write, execute	–	Read, Write	Read	Write
Alice	Execute	Read, Write, execute	Read, write	Read, write	Write

- In Table 2.3.1, the system is having a track of two processes, two files, and one hardware device.
- John can read both File 1 and File 2, but can write only to File 1, John cannot access Process 2, but he can have the ability to write to the printer.
- Alice can execute Process 1 and Process 2. Alice can read as well as write both files.
- In a large system the access matrix will be huge in size, and most of its cells are likely to be empty.
- The access control matrix is rarely used in computer systems because it is extremely costly in terms of storage space and processing.

Access Control List (ACL):

- The implementation of access Controls in a system may vary, but the Access Control Lists (ACLs) are common.
- An ACL is nothing more than a list that contains the subjects that have access rights to a particular object as shown in Fig. 2.3.2. The list will identify not only the subject but also the specific access for the object.

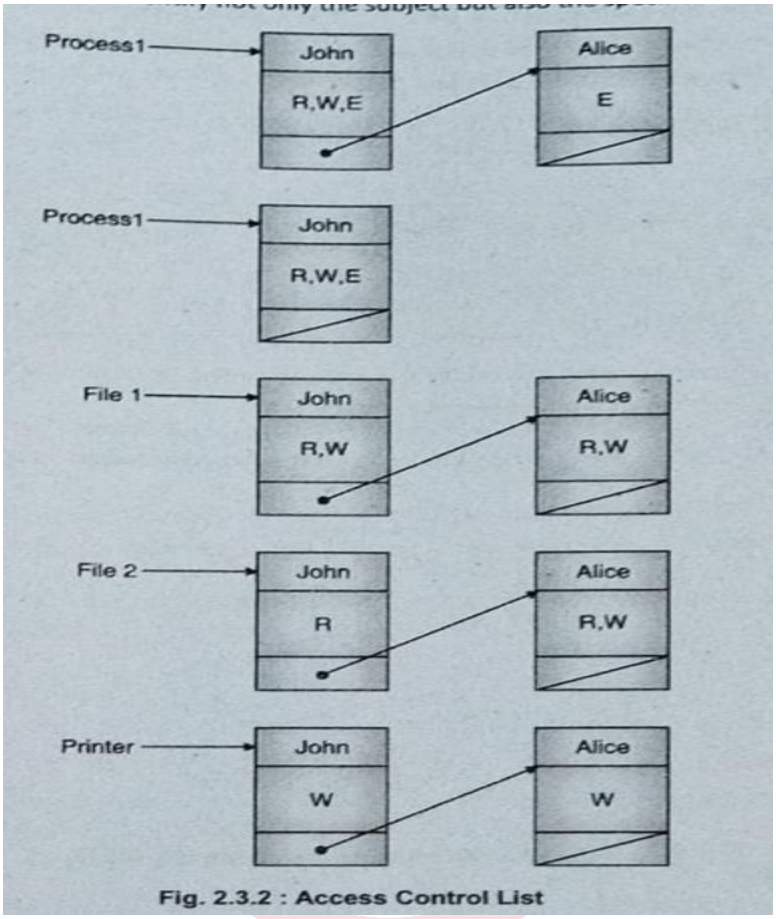


Fig. 2.3.2 : Access Control List

- Typical types of access include read, write, and execute as indicated in our example access control matrix.
- In ACL, it is easy to determine what access the subjects are currently authorized for the object.
- Means it is provided for convenient access review with respect to an object. Also, it is easy to revoke all access to an object by replacing the ex0sting ACL with an empty one.
- It is very important to examine the ACL of each object in the system to do access review win respect to a subject.
- Hence, the ACL has small fixed size sand it can be stored using a few bits associated with the file.
- The mechanism used to implement access controls in a computer system or network is not important but the controls should be based on a specific access model.

9. What is DAC, MAC and RBAC?

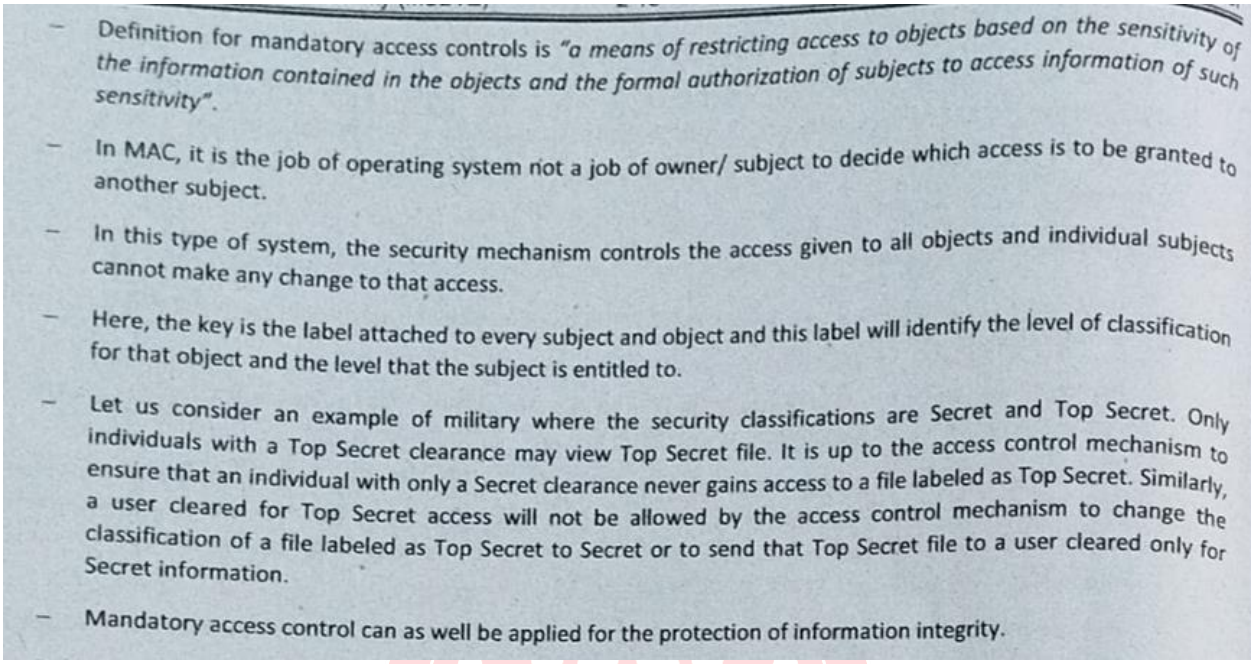
Ans:

1. **Discretionary Access Control (DAC)**

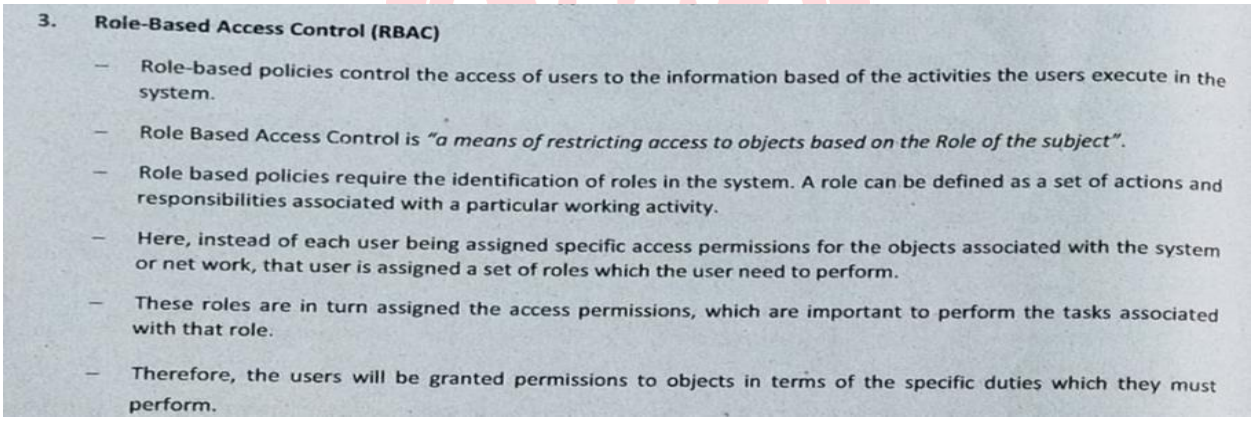
- Discretionary access controls are "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong."
- It controls the access based on the identity of the requestor and on access rules (authorizations) stating what requestors are or are not allowed to do.
- Discretionary protection policies decide the access of users to the information on the basis of the user's identity and authorizations (or rules) that specify, for each user (or group of users) and each object in the system, the access modes (e.g., read, write, or execute) the user is allowed on the object. Each request of a user to access an object is checked against the specified authorizations.
- The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission indirectly on to any other subject.
- If the system is having discretionary access controls then, the owner of an object can decide which other subjects may have access to the object and what specific access they may have.
- The permission bit used in UNIX-based systems is the common method to accomplish this. The owner of a file can specify what permissions (read/ write/execute) members in the same group may have and also what permissions all others may have.
- Access Control Lists (ACL) is another common mechanism used to implement discretionary access control.
- The flexibility of discretionary access control policies makes them suitable for a variety of systems and applications.
- For these reasons, they have been widely used in a variety of implementations, especially in the commercial and industrial environments.
- However, discretionary access control policies have the drawback that they do not provide real assurance on the flow of information in a system. It is easy to bypass the access restrictions stated through the authorizations.
- For example, a user who is able to read data can pass it to other users not authorized to read it without the knowledge of the owner.

2. **Mandatory Access Control (MAC)**

- Mandatory policies decide access on the basis of classification of subjects and objects in the system. Each user and each object in the system is assigned a security level.
- Generally, this system is used in environments where different levels of security classifications are there and is much more restrictive of what a user is allowed to do.



- Definition for mandatory access controls is *"a means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity"*.
- In MAC, it is the job of operating system not a job of owner/ subject to decide which access is to be granted to another subject.
- In this type of system, the security mechanism controls the access given to all objects and individual subjects cannot make any change to that access.
- Here, the key is the label attached to every subject and object and this label will identify the level of classification for that object and the level that the subject is entitled to.
- Let us consider an example of military where the security classifications are Secret and Top Secret. Only individuals with a Top Secret clearance may view Top Secret file. It is up to the access control mechanism to ensure that an individual with only a Secret clearance never gains access to a file labeled as Top Secret. Similarly, a user cleared for Top Secret access will not be allowed by the access control mechanism to change the classification of a file labeled as Top Secret to Secret or to send that Top Secret file to a user cleared only for Secret information.
- Mandatory access control can as well be applied for the protection of information integrity.



3. **Role-Based Access Control (RBAC)**

- Role-based policies control the access of users to the information based of the activities the users execute in the system.
- Role Based Access Control is *"a means of restricting access to objects based on the Role of the subject"*.
- Role based policies require the identification of roles in the system. A role can be defined as a set of actions and responsibilities associated with a particular working activity.
- Here, instead of each user being assigned specific access permissions for the objects associated with the system or net work, that user is assigned a set of roles which the user need to perform.
- These roles are in turn assigned the access permissions, which are important to perform the tasks associated with that role.
- Therefore, the users will be granted permissions to objects in terms of the specific duties which they must perform.

UNIT-3

1) What is Plaintext and Cipher text with Diagram.

Ans:

Plaintext:

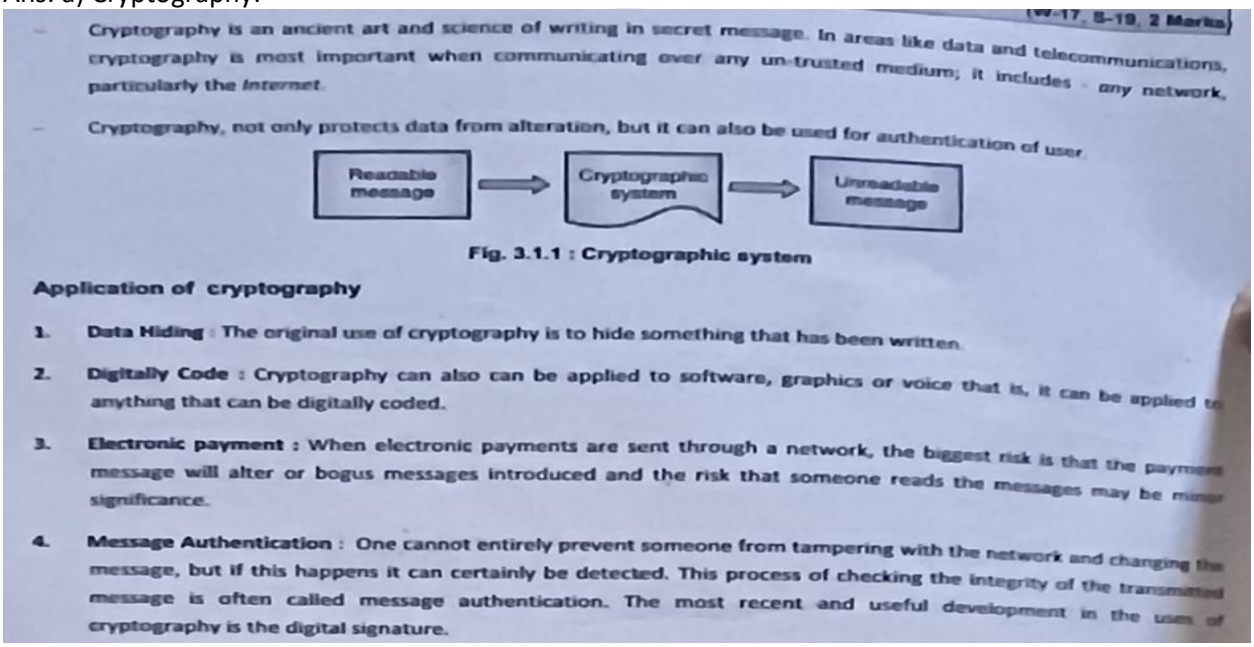
- The Plaintext is also known as clear text mean anyone who knows the language can easily read the message.
- The original message is known as plaintext.

Cipher text:

- When the Plaintext is codified with the help of any suitable scheme, then the resultant message is known as Ciphertext.
- The coded message is known as Ciphertext.

2) Define the terms with diagram:
a) Cryptography
b) Cryptanalysis
c) Cryptology
d) Encryption
e) Decryption

Ans: a) Cryptography:



Cryptography is an ancient art and science of writing in secret message. In areas like data and telecommunications, cryptography is most important when communicating over any un-trusted medium; it includes any network, particularly the *Internet*.

Cryptography, not only protects data from alteration, but it can also be used for authentication of user.

Fig. 3.1.1 : Cryptographic system

Application of cryptography

1. **Data Hiding :** The original use of cryptography is to hide something that has been written.
2. **Digitally Code :** Cryptography can also can be applied to software, graphics or voice that is, it can be applied to anything that can be digitally coded.
3. **Electronic payment :** When electronic payments are sent through a network, the biggest risk is that the payment message will alter or bogus messages introduced and the risk that someone reads the messages may be minor significance.
4. **Message Authentication :** One cannot entirely prevent someone from tampering with the network and changing the message, but if this happens it can certainly be detected. This process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the digital signature.

b) Cryptanalysis:

- The process of trying to break any Ciphertext message to obtain the original message itself is known as cryptanalysis.
- It is the technique of decoding message from a non-readable format back to readable format without knowing how they are converted into non-readable format.

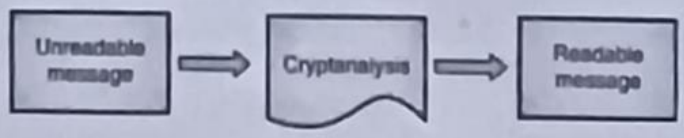


Fig. 3.1.2 : Cryptanalysis

c) Cryptology:

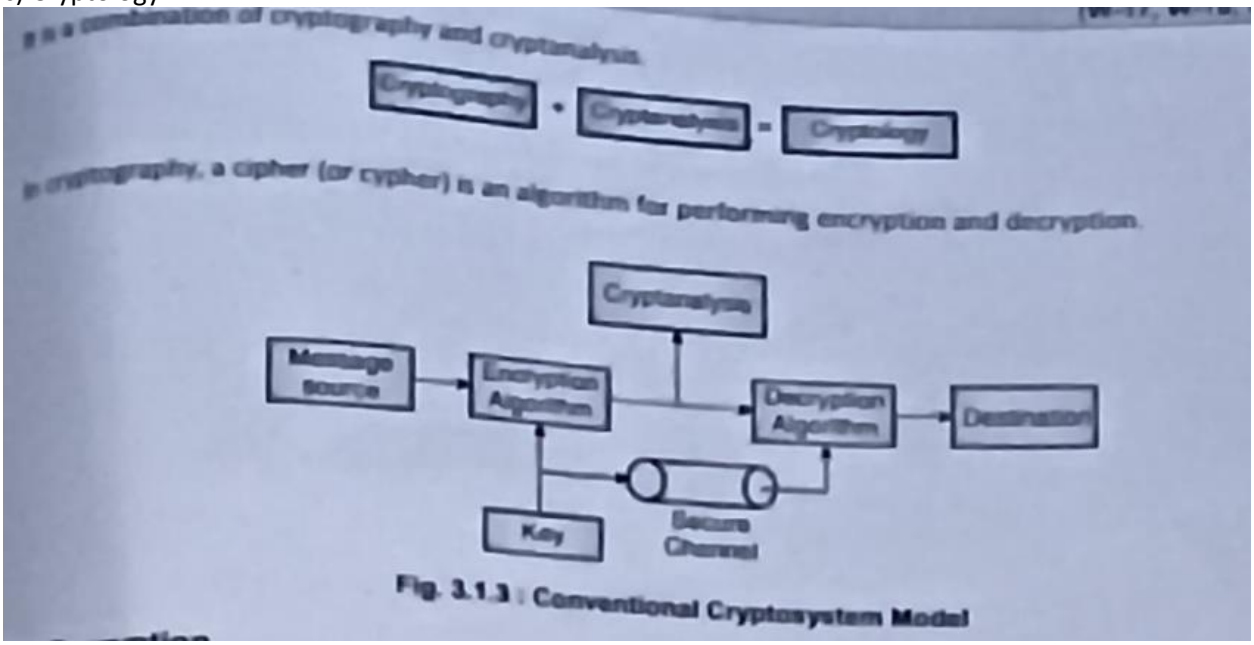


Fig. 3.1.3 : Conventional Cryptosystem Model

d) Encryption:

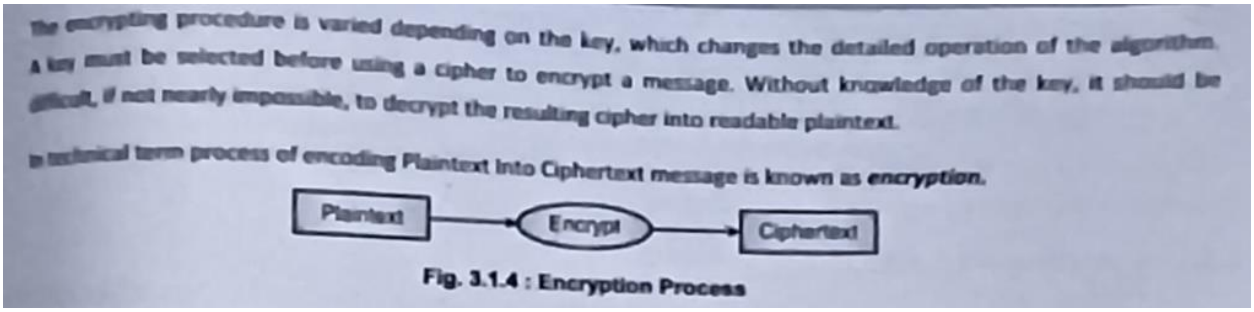


Fig. 3.1.4 : Encryption Process

e) Decryption:

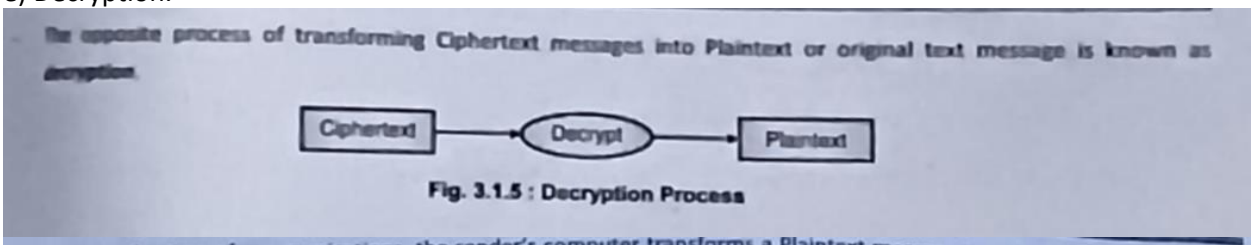


Fig. 3.1.5 : Decryption Process

- At the time of communications, the sender's computer transforms a Plaintext message into Ciphertext with the help of encryption.
- Then the encrypted Ciphertext message is sent to the receiver over a network i.e. Internet.
- The computers at receiver's end then takes this encrypted message, and perform the reverse of encryption means the decryption process to get original Plaintext message.
- For encrypting a plaintext message, the sender performs encryption with the help of different encryption algorithms.
- For decrypting a received encrypted message, the recipient performs the decryption with the help of decryption algorithms.

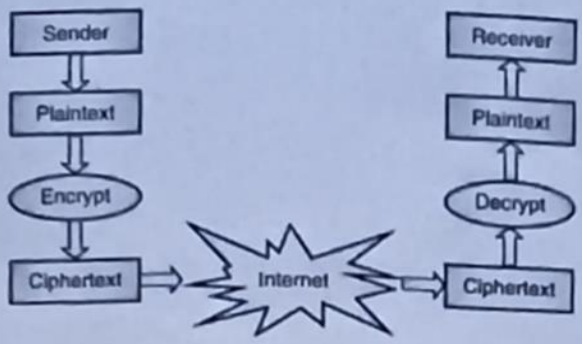


Fig. 3.1.6 : Encryption and Decryption

3) What is Substitution Technique and also explain the types of substitution with Example.

Ans:

4) What is Transposition Technique and also explain the types of Transposition technique with Example
Ans:

Transposition technique does not replace alphabets from plaintext with other whereas; it performs some permutation on alphabets of plaintext.

1. **Simple Columnar Transposition**

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the length of the rows and the permutation of the columns are usually defined by a keyword.

the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword.

In this case, the order would be "6 3 2 4 1 5".

Plaintext = WELCOME HOME with Key = ZEBRAS (Length is 6).

Consider the rectangle with 6 columns because the length of key is 6.

Write the message in rectangle in row-by-row manner.

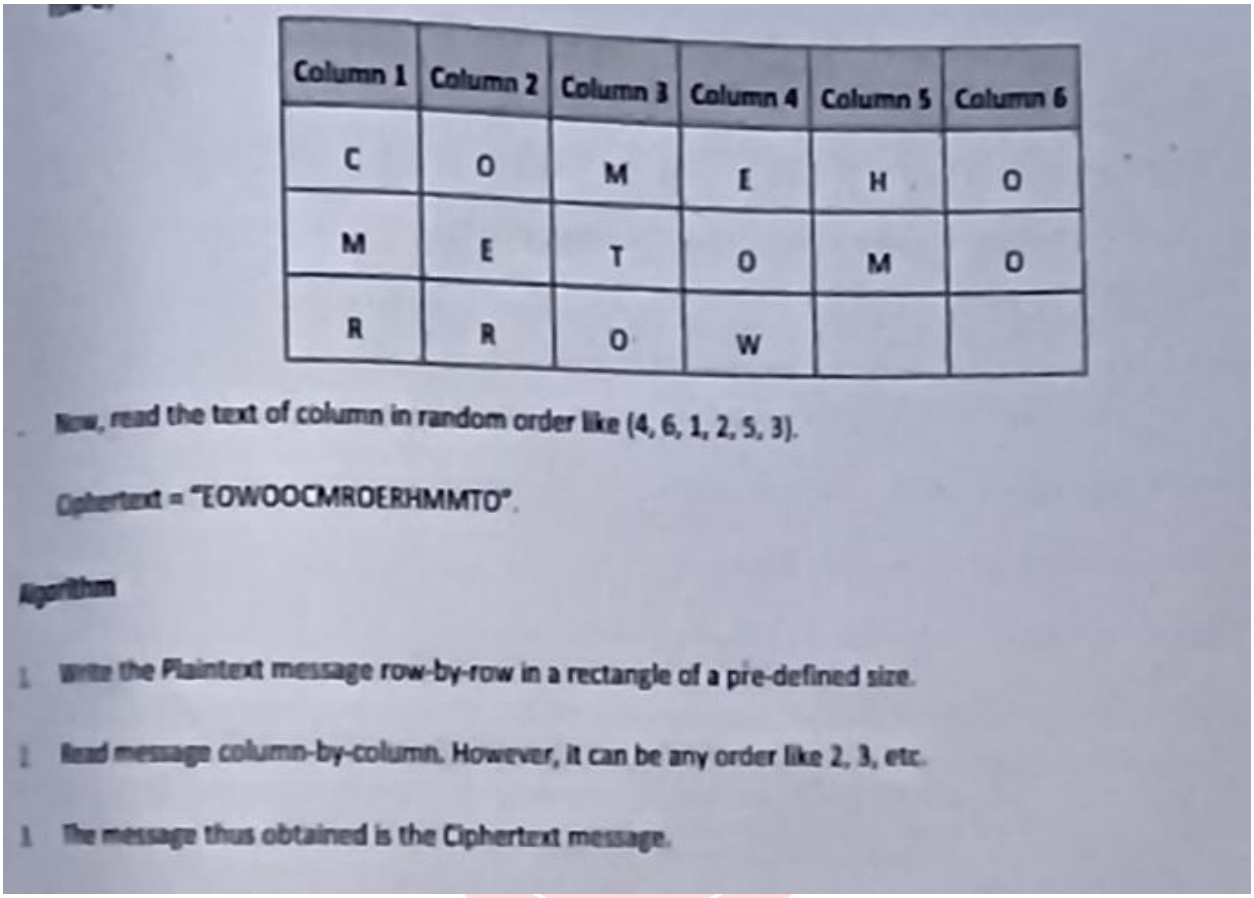
1	2	3	4	5	6
W	E	L	C	O	M
E	H	O	M	E	

Now, read it with some random order of (4, 6, 1, 2, 5, 3).

The Ciphertext is "CMMWEEHOELO".

Plaintext = Come Home Tomorrow with key = 6.

As length of key is 6, the rectangle should be of 6 columns. Now write Plaintext message in these columns row-by-row.



Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
C	O	M	E	H	O
M	E	T	O	M	O
R	R	O	W		

Now, read the text of column in random order like (4, 6, 1, 2, 5, 3).

Ciphertext = "EOWOOCMROERHMMTO".

Algorithm

1. Write the Plaintext message row-by-row in a rectangle of a pre-defined size.
2. Read message column-by-column. However, it can be any order like 2, 3, etc.
3. The message thus obtained is the Ciphertext message.

5) What is Steganography and also explain the procedure?
Ans:

- Steganography is a technique of hiding a large amount of secret message within an ordinary message and the extraction of it at its destination.
- Steganography takes cryptography a step further by hiding an encrypted message; so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.
- In modern digital steganography, data is encrypted using Encryption algorithm.
- Encrypted data is inserted into cover media (JPEG images).
- Encrypted data will be added in cover media using Stego-key.

The following formula provides the description of Steganographic process.

Cover-media + Hidden-data + Stego-key = Stego-medium

- Cover media is the file in which we will hide the hidden-data, which may also be encrypted using stego-key. The resultant file is stego-medium. Cover-media can be image or audio file.

Think of all the bits that represent the same color pixels repeated in a row. By applying the encrypted data to the redundant data in some random or non-conspicuous way, the result will be data that appears to have the "noise" patterns of regular, non-encrypted data. A trademark or other identifying symbol hidden in software code is sometimes known as a watermark.

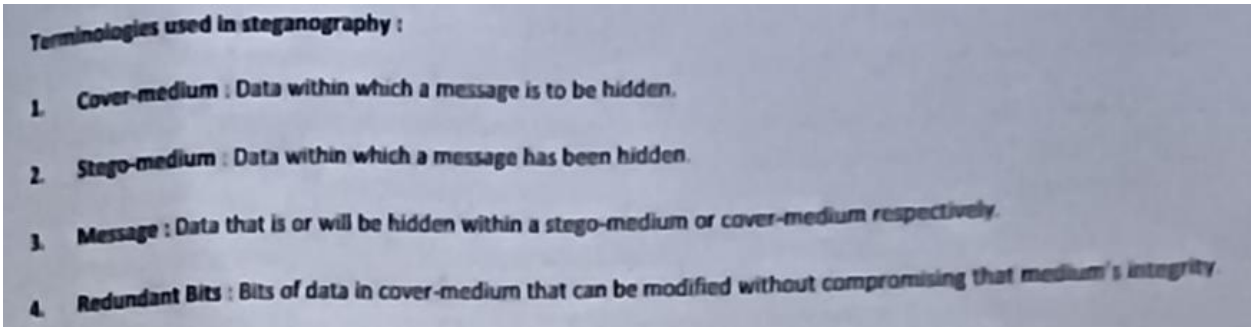
Disadvantage is it requires a lot of overhead to hide a few bits of information.

Once the system is discovered, it becomes virtually worthless. This problem is solved by insertion method which uses some sort of key.

Alternative is, first encrypt the message and then hide using Steganography.

Advantage is that it can be employed by parties who have something to lose should the fact of their secret communication be discovered.

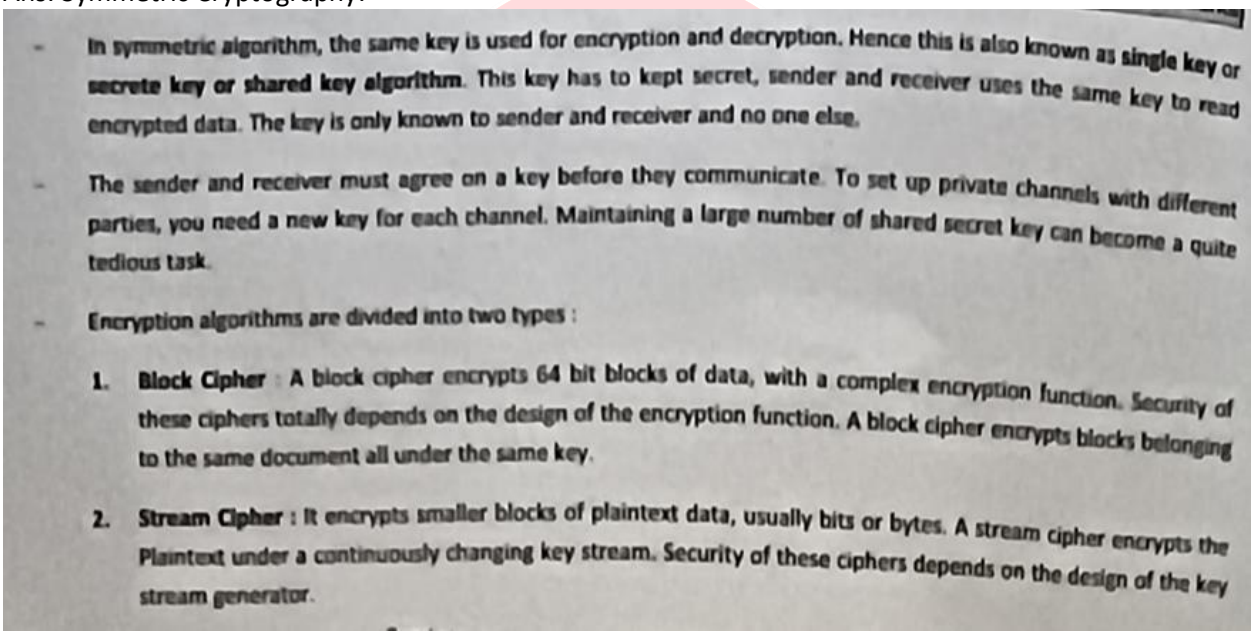
Encryption flags are important or secret or may identify the sender as someone with something to hide.



Terminologies used in steganography :

1. **Cover-medium** : Data within which a message is to be hidden.
2. **Stego-medium** : Data within which a message has been hidden.
3. **Message** : Data that is or will be hidden within a stego-medium or cover-medium respectively.
4. **Redundant Bits** : Bits of data in cover-medium that can be modified without compromising that medium's integrity.

6) What is symmetric and asymmetric Cryptography with examples?
Ans: Symmetric Cryptography:



- In symmetric algorithm, the same key is used for encryption and decryption. Hence this is also known as **single key** or **secrete key or shared key algorithm**. This key has to kept secret, sender and receiver uses the same key to read encrypted data. The key is only known to sender and receiver and no one else.
- The sender and receiver must agree on a key before they communicate. To set up private channels with different parties, you need a new key for each channel. Maintaining a large number of shared secret key can become a quite tedious task.
- Encryption algorithms are divided into two types :
  1. **Block Cipher** : A block cipher encrypts 64 bit blocks of data, with a complex encryption function. Security of these ciphers totally depends on the design of the encryption function. A block cipher encrypts blocks belonging to the same document all under the same key.
  2. **Stream Cipher** : It encrypts smaller blocks of plaintext data, usually bits or bytes. A stream cipher encrypts the Plaintext under a continuously changing key stream. Security of these ciphers depends on the design of the key stream generator.

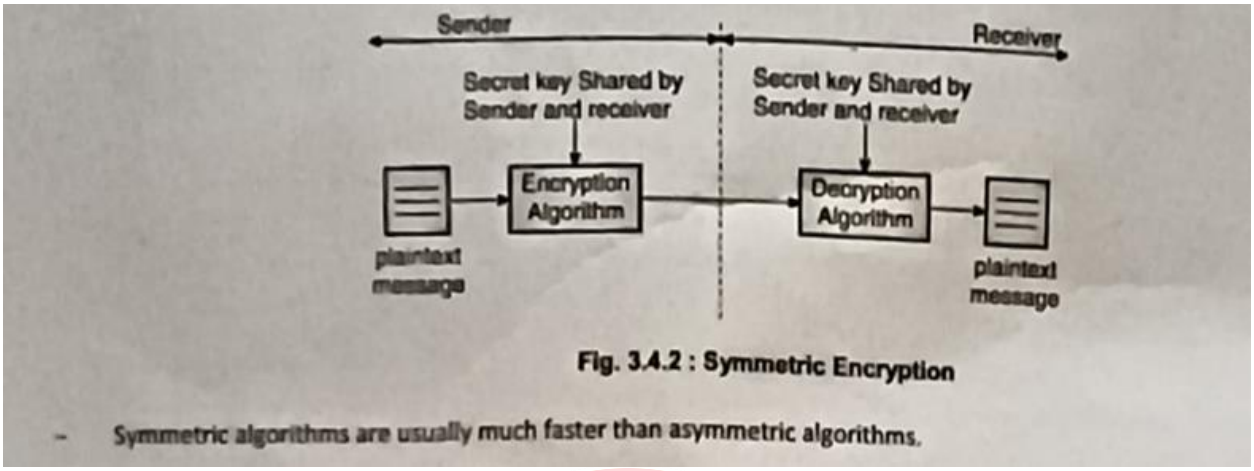


Fig. 3.4.2 : Symmetric Encryption

- Symmetric algorithms are usually much faster than asymmetric algorithms.

Asymmetric Cryptography:

- Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.
- Frequently the keys are interchangeable, in the sense that if key A encrypts a message, then B can decrypt it, and if key B encrypts a message, then key A can decrypt it. While common, this property is not essential to asymmetric encryption.
- Asymmetric Encryption is also known as **Public Key Cryptography**, since users typically create a matching key pair, and make one public while keeping the other secret.
- Users can 'sign' messages by encrypting them with their private keys. This is effective since any message recipient can verify that the user's public key can decrypt the message, and thus prove that the user's secret key was used to encrypt it.

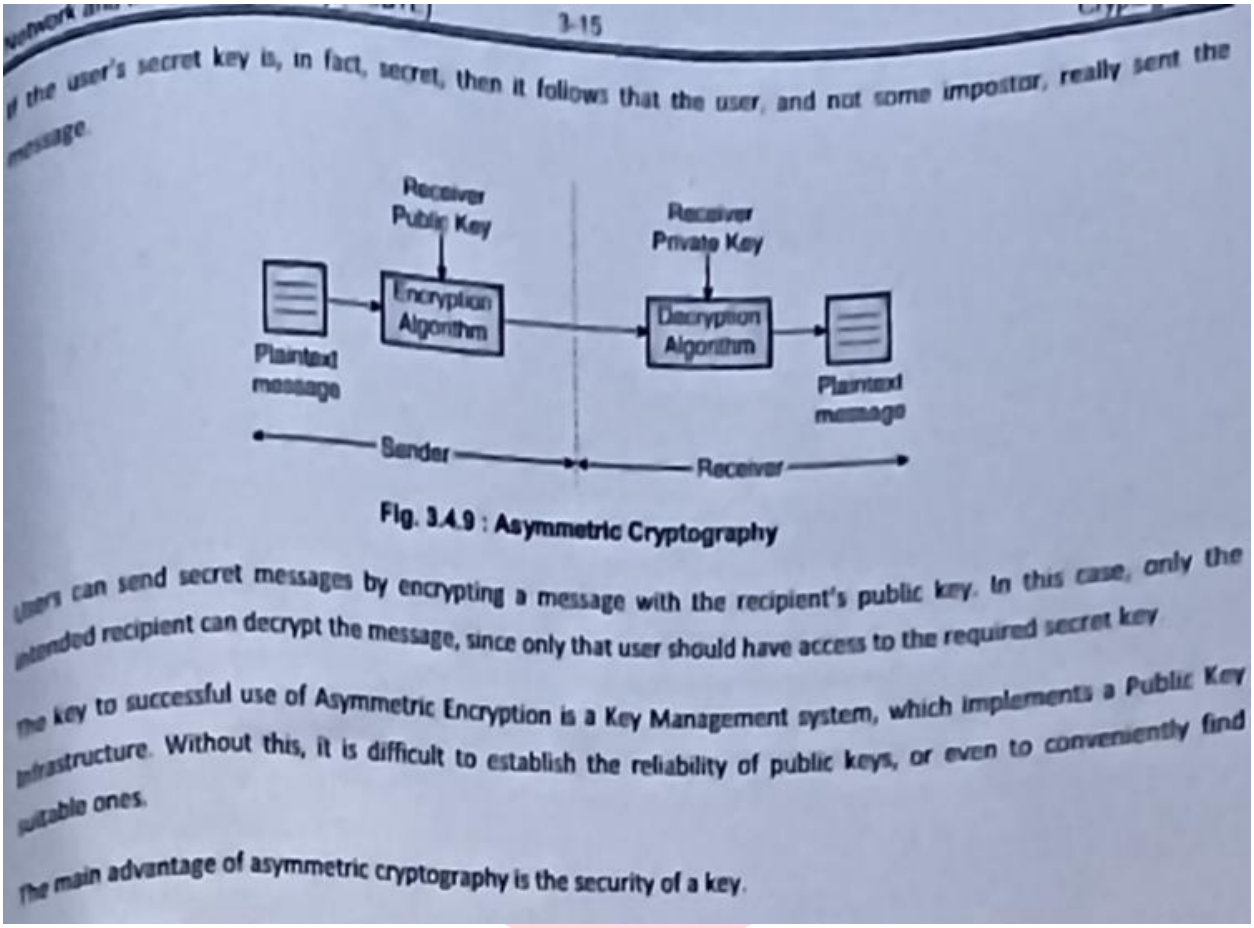


Fig. 3.4.9 : Asymmetric Cryptography

Users can send secret messages by encrypting a message with the recipient's public key. In this case, only the intended recipient can decrypt the message, since only that user should have access to the required secret key.

The key to successful use of Asymmetric Encryption is a Key Management system, which implements a Public Key Infrastructure. Without this, it is difficult to establish the reliability of public keys, or even to conveniently find suitable ones.

The main advantage of asymmetric cryptography is the security of a key.

7) What is Block and Stream Cipher?
Ans:

8) What is DES? Explain DES cryptography step by step?

Ans:

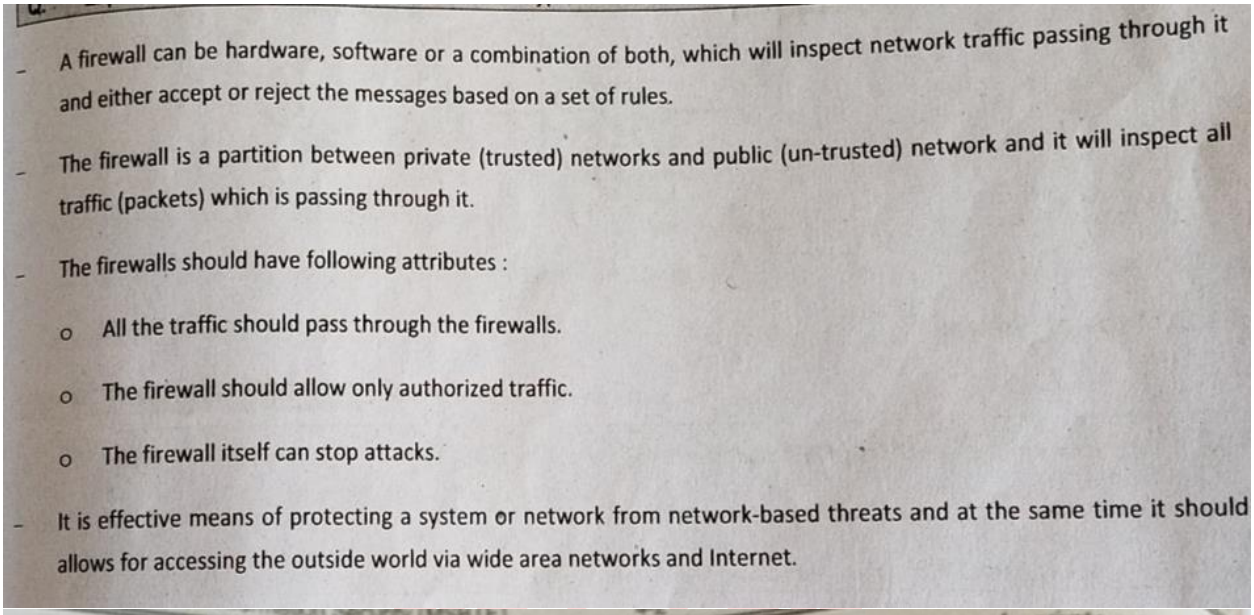
9) Comparison between Symmetric and Asymmetric Cryptography?
Ans:

Sr. No.	Symmetric Key Cryptography	Asymmetric Key Cryptography
1.	Single key is used for encryption and decryption.	Two separate keys are used for encryption and decryption.
2.	Also known as Single Key cryptography.	Known as Public and Private Key encryption.
3.	Key should be agreed by both- sender and receiver.	No need to agree on keys.
4.	Less Security.	More Security.
5.	Simple to implement.	Hard to implement as compare to symmetric key cryptography.
6.	For example - Data Encryption Standard (DES).	For example - Digital Signature.

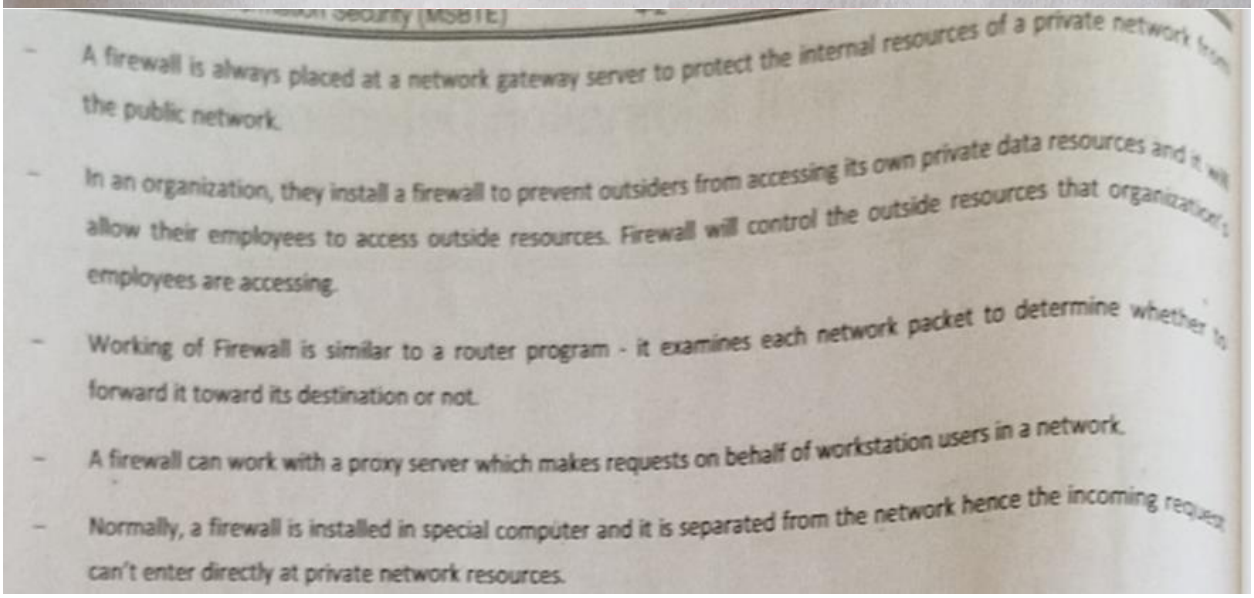
UNIT-4

1) What is firewall and the need of firewall ?

Ans:



- A firewall can be hardware, software or a combination of both, which will inspect network traffic passing through it and either accept or reject the messages based on a set of rules.
- The firewall is a partition between private (trusted) networks and public (un-trusted) network and it will inspect all traffic (packets) which is passing through it.
- The firewalls should have following attributes :
  - All the traffic should pass through the firewalls.
  - The firewall should allow only authorized traffic.
  - The firewall itself can stop attacks.
- It is effective means of protecting a system or network from network-based threats and at the same time it should allows for accessing the outside world via wide area networks and Internet.



- A firewall is always placed at a network gateway server to protect the internal resources of a private network from the public network.
- In an organization, they install a firewall to prevent outsiders from accessing its own private data resources and it will allow their employees to access outside resources. Firewall will control the outside resources that organization's employees are accessing.
- Working of Firewall is similar to a router program - it examines each network packet to determine whether to forward it toward its destination or not.
- A firewall can work with a proxy server which makes requests on behalf of workstation users in a network.
- Normally, a firewall is installed in special computer and it is separated from the network hence the incoming request can't enter directly at private network resources.

- Firewall uses different screening methods - the simple one is to screen the requests to ensure that the traffic is from trusted domain name and Internet Protocol addresses.
- For mobile users, firewall allows remote access in to the private network with the help of secure logon procedures and it authenticates the certificates.

Design Goals

- All traffic must pass through the firewall either from inside to outside, and vice versa. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic which is defined by the local security policy will be allowed to pass through the firewall. Different types of firewalls will implement different types of security policies.
- The firewall itself is immune to penetration.

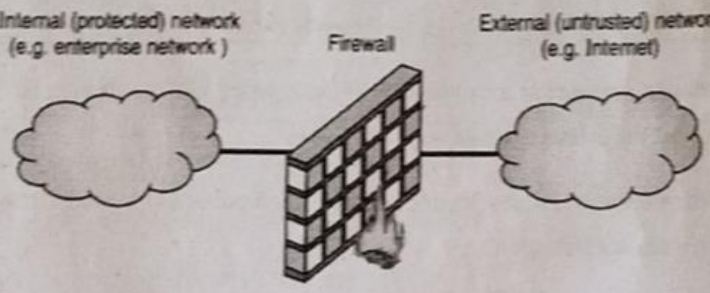


Fig. 4.1.1 : Firewall

2) What are the types of firewall and explain the types with diagram ?
Ans:

1. **Packet Filter**

- A router as part of a firewall usually performs packet Filtering.
- A packet filtering router applies a set of rules to each and every incoming IP packet and then decides either to forward or discard the packet.
- Typically the router is configured to filter packets going towards and coming from the internal network.
- Filtration rules are based on information of a network packet.

- **Source IP address :** The IP address of the system who generates the IP Packet.
- **Destination IP address :** The IP address of the other system where the IP packet is trying to reach.
- **Source and destination transport-level address :** The transport level port number TCP or UDP to define applications such as SNMP or TELNET.
- **IP protocol field :** It tells the transport protocol.
- **Interface :** It is for a router who uses three or more ports from which interface the packet came from or which interface the packet is destined for.

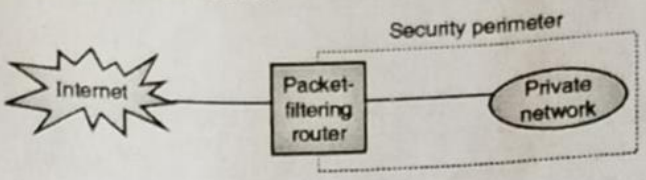


Fig. 4.1.2 : **Packet Filtering Router**

2. **Stateful Packet Filter**

- Stateful packet filters understand request and reply system.
- Usually the rules of stateful packets are specified only for the first packet in one direction, and then new rule is created dynamically after the first outbound packet.
- All other packets in the communication are then processed automatically.
- Stateful firewalls can support for a wider range of protocols like FTP, IRC, or H323.

3. Application Gateways

- An application-level gateway is also known as proxy server. This is because it acts like a proxy and decides about the flow of application level traffic.
- An internal user contacts the application level gateway using a TCP/IP application, such as Telnet or FTP or HTTP.
- The application level gateway will asks the user/host about the remote host with which the he wants a connection for communication.
- When the user provides all information like a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- The service is not supported and cannot be forwarded across the firewall, if the gateway does not implement the proxy code for a specific application.
- Generally, the gateways are configured to support only specific features that the network administrator considers acceptable while denying all other features.
- An application level gateway is more secure than packet filtering. Here, it is very easy to audio or logs all incoming traffic.

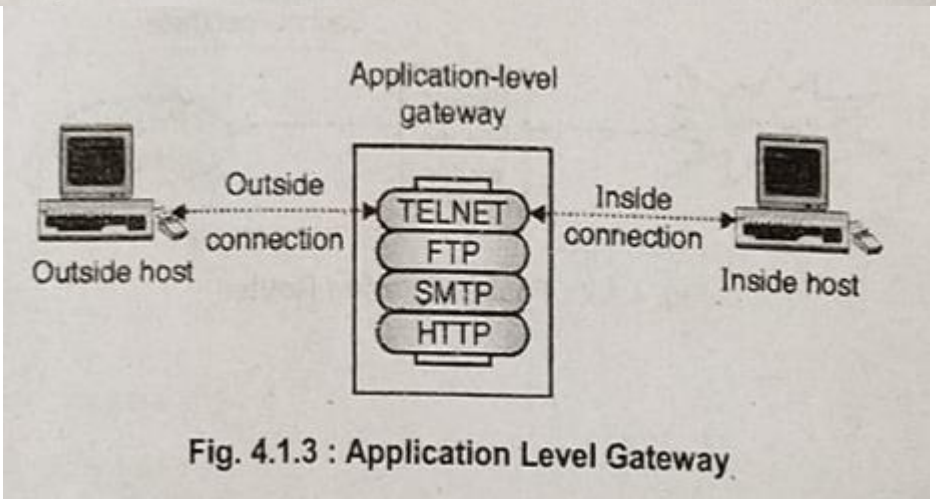


Fig. 4.1.3 : Application Level Gateway

4. Circuit Gateways

- It can be a specialized function that performs an application level gateway for certain applications.
- I will not allow an end-to-end TCP connection, but it will set up two TCP connections :
  - One between a TCP user on an inner host and a gateway.
  - One between a gateway and a TCP user on an outside host.
- After establishing the two connections, the gateway transmits the TCP segments from one connection to another without examining the contents. The security function will check which connection is allowed.
- The use of circuit level gateways is in a situation, where the system administrator trusts the internal users.

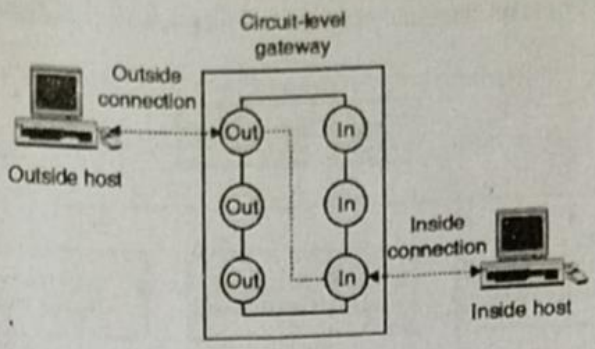
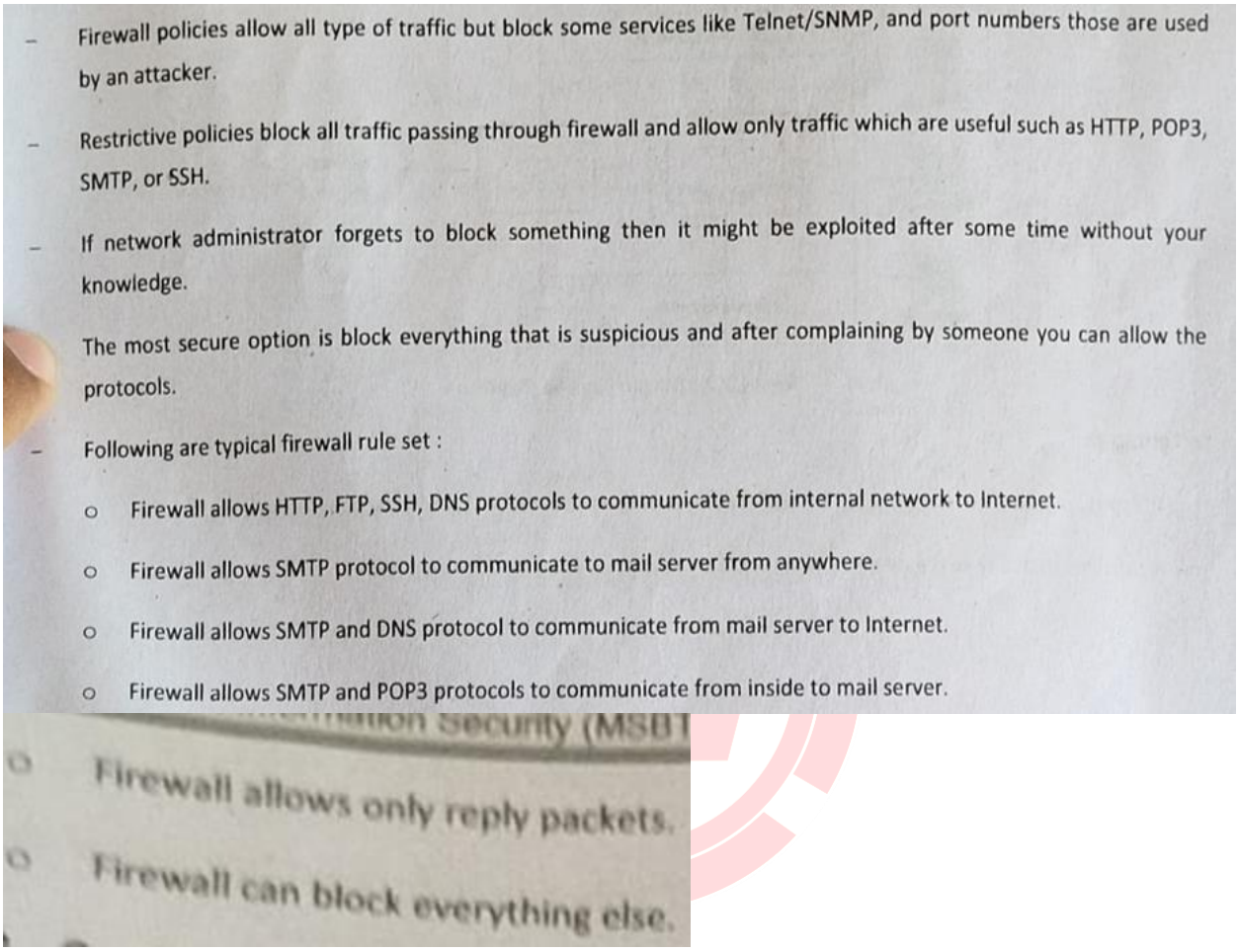


Fig. 4.1.4 : Circuit Level Gateway

- The gateway can be configured to support application level or proxy service on inbound connections and circuit-level functions for outbound connections.
- In this, the gateway can acquire the processing overhead of examining incoming application data for prohibited functions but does not acquire that overhead on outgoing data.

3) What are firewall policies?

Ans:



- Firewall policies allow all type of traffic but block some services like Telnet/SNMP, and port numbers those are used by an attacker.
- Restrictive policies block all traffic passing through firewall and allow only traffic which are useful such as HTTP, POP3, SMTP, or SSH.
- If network administrator forgets to block something then it might be exploited after some time without your knowledge.
- The most secure option is block everything that is suspicious and after complaining by someone you can allow the protocols.
- Following are typical firewall rule set :
  - Firewall allows HTTP, FTP, SSH, DNS protocols to communicate from internal network to Internet.
  - Firewall allows SMTP protocol to communicate to mail server from anywhere.
  - Firewall allows SMTP and DNS protocol to communicate from mail server to Internet.
  - Firewall allows SMTP and POP3 protocols to communicate from inside to mail server.
  - Firewall allows only reply packets.
  - Firewall can block everything else.

4) What is Firewall configuration? Explain the types of firewall configuration with Diagram?
Ans:

guration

- A firewall is a combination of packet filter and application level gateway. Based on these, there are three types c configurations.

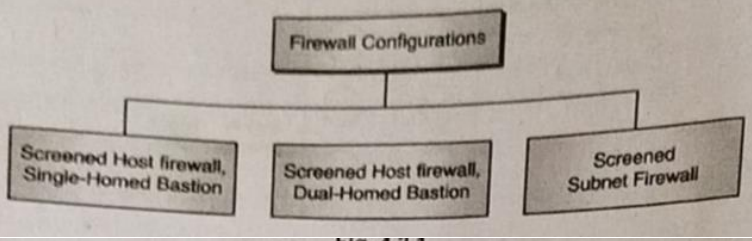


Fig. 4.2.1

1. **Screened Host firewall, Single-Homed Bastion**

- Here, the firewall configuration consists of two parts - ***a packet filter router*** and an ***application level gateway***.
- A packet filter router will ensure that the incoming traffic is allowed only if it is intended for the application gateway, by examining the destination address field of each incoming IP Packet.
- It will also ensure that the outgoing traffic is allowed only if it is originated from application level gateway, by examining the source address field of every outgoing IP Packet.
- An application level gateway performs authentication as well as proxy functions.

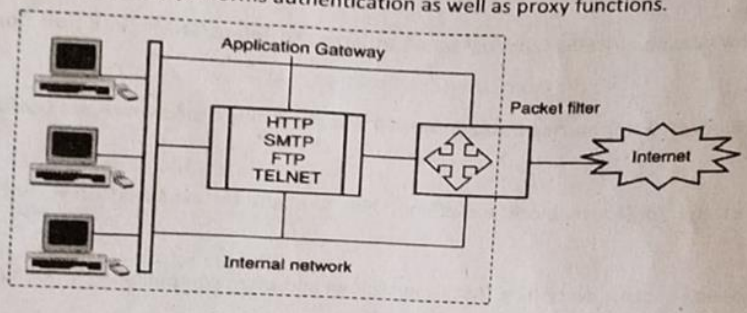


Fig. 4.2.2 : Single Homed Bastion

Advantages

- It improves security of the network by performing checks at both levels- packet and application level
- It provides flexibility to the network administrator to define more security policies.

Disadvantages

Internal users are connected to the application gateway as well as packet filter router. So, if any how the packet filter is attacked, then the whole internal network is exposed to the attacker.

2. **Screened Host firewall, Dual-Homed Bastion**

- In this type of configuration, the direct connections between the internal hosts and the packet filter are avoided.
- Here, the packet filter connects only to the application gateway, which in turn has a separate connection with the internal hosts.
- Hence, if packet filter is successfully attacked, then only application gateway is visible to the attacker.

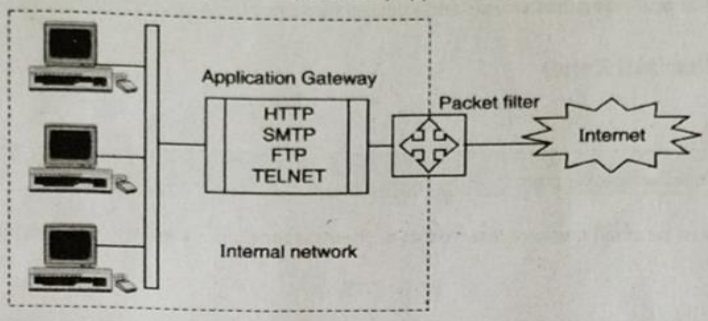


Fig. 4.2.3 : Dual-Homed Bastion

3. **Screened Subnet Firewall**

- This type of configuration offers highest security among the possible configurations.
- In this type, two packet filters are used, one between the Internet and application gateway and other in between application gateway and the Internal network.
- This configuration achieves 3 levels of security for an attacker to break into.

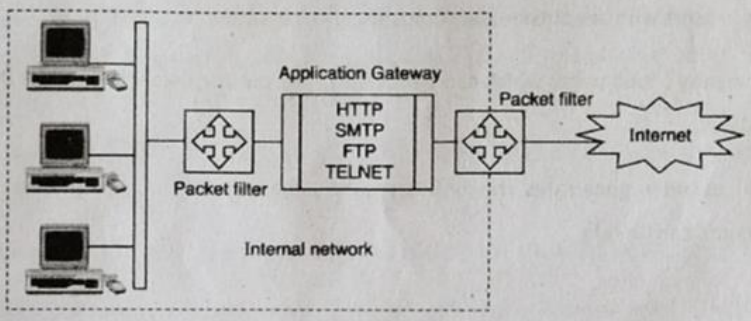


Fig. 4.2.4 : Screened Subnet Firewall

5) What is DMZ? Explain with Diagram?

Ans:

- It is a computer host or small network inserted as a, "neutral zone" in a company's private network and the outside public network.
- It avoids outside users from getting direct access to a company's data server. A DMZ is an optional but more secure approach to a firewall. It can effectively acts as a proxy server.
- The typical DMZ configuration has a separate computer or host in network which receives requests from users within the private network to access a Web sites or the public network.
- Then a DMZ host initiates sessions for such requests on the public network but it is not able to initiate a session into the private network. It can only forward packets which have been requested by a host.
- The public network's users who are outside the company can access only the DMZ host.
- It can store the company's Web pages which can be served to the outside users. Hence, the DMZ can't give access to other company's data.
- By any way, if an outsider penetrates the DMZ's security, then the Web pages may get corrupted but other company's information can be safe.

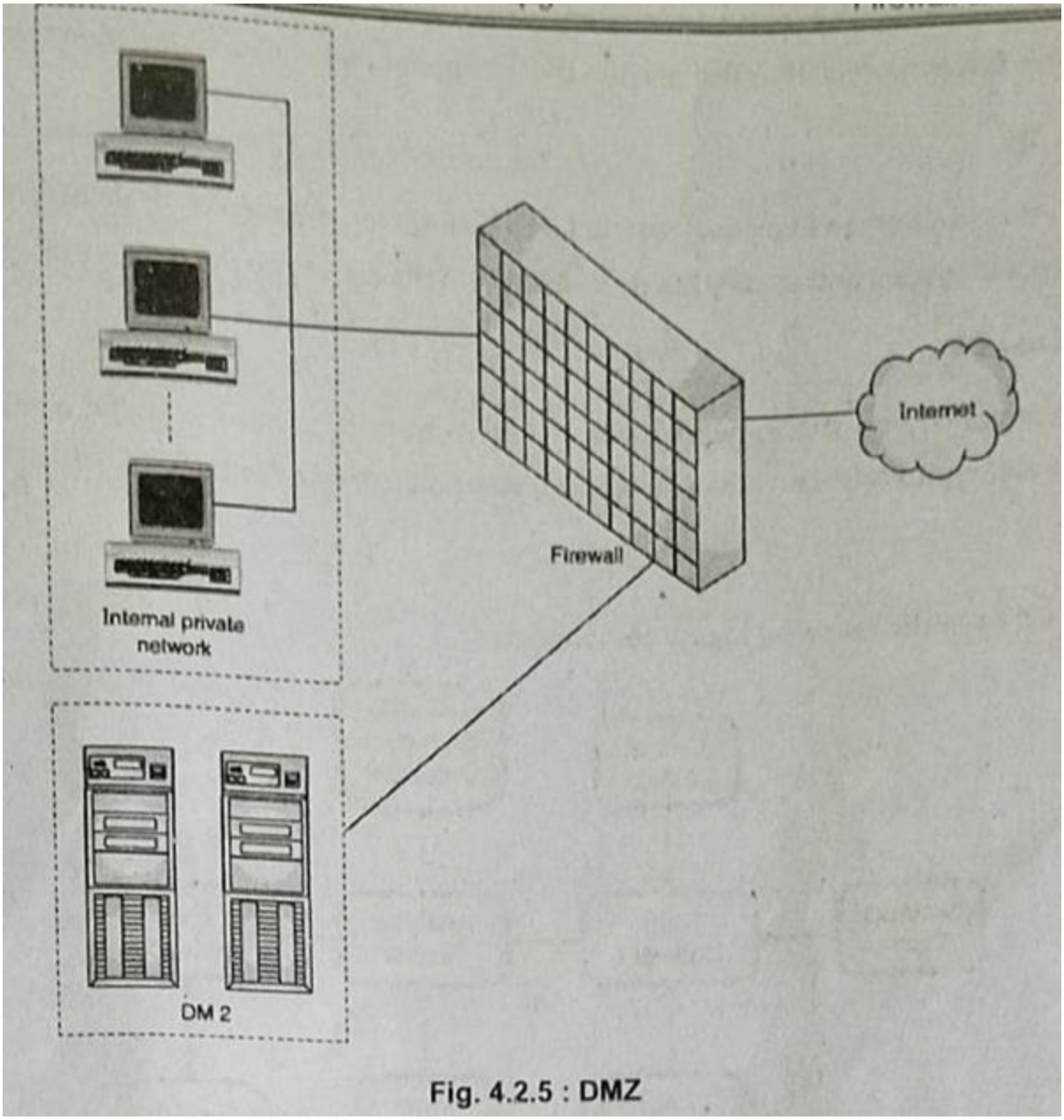
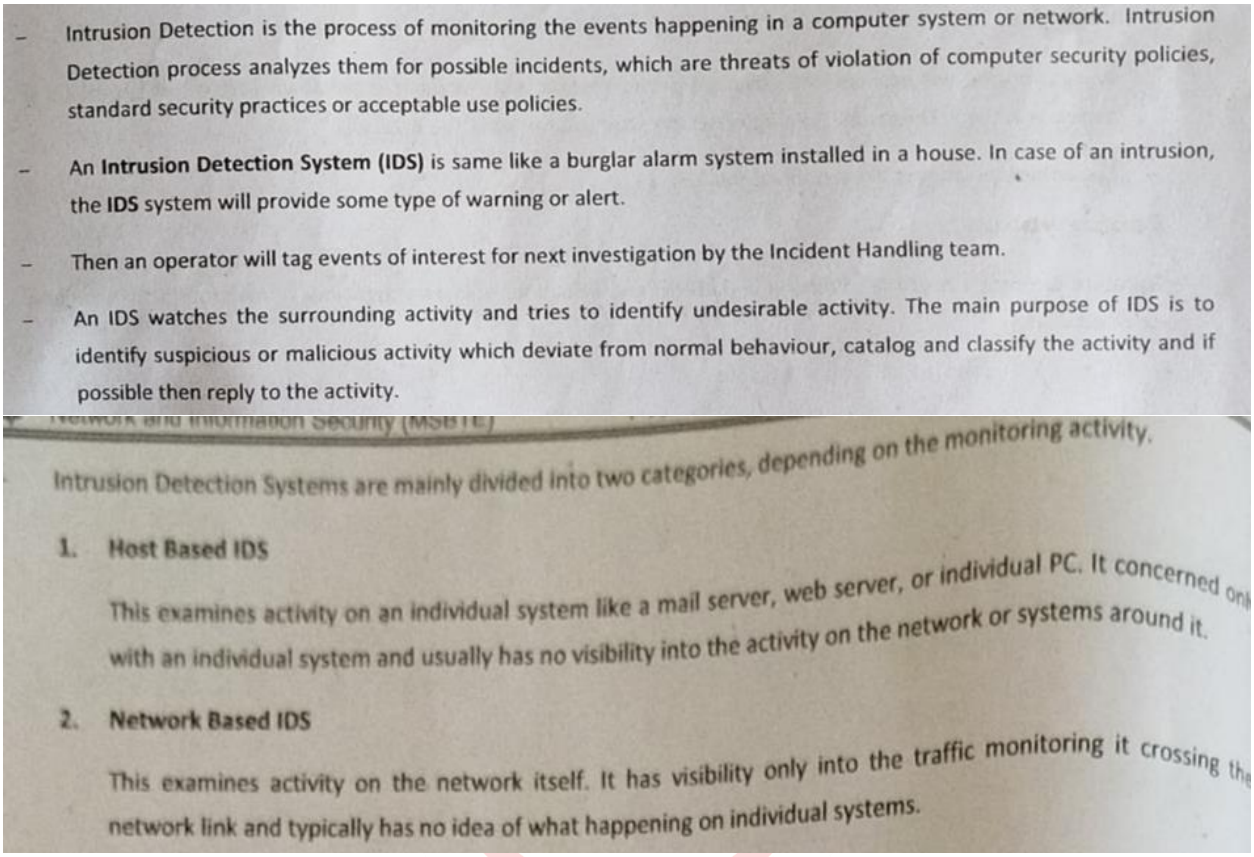


Fig. 4.2.5 : DMZ

6) What is IDS? Explain the types of IDS ?
Ans:



- Intrusion Detection is the process of monitoring the events happening in a computer system or network. Intrusion Detection process analyzes them for possible incidents, which are threats of violation of computer security policies, standard security practices or acceptable use policies.
- An **Intrusion Detection System (IDS)** is same like a burglar alarm system installed in a house. In case of an intrusion, the **IDS** system will provide some type of warning or alert.
- Then an operator will tag events of interest for next investigation by the Incident Handling team.
- An IDS watches the surrounding activity and tries to identify undesirable activity. The main purpose of IDS is to identify suspicious or malicious activity which deviate from normal behaviour, catalog and classify the activity and if possible then reply to the activity.

Intrusion Detection Systems are mainly divided into two categories, depending on the monitoring activity.

1. **Host Based IDS**

   This examines activity on an individual system like a mail server, web server, or individual PC. It concerned on with an individual system and usually has no visibility into the activity on the network or systems around it.

2. **Network Based IDS**

   This examines activity on the network itself. It has visibility only into the traffic monitoring it crossing th network link and typically has no idea of what happening on individual systems.

7) Explain the Components of IDS?
Ans:

Components of IDS

Typically, an IDS will have the following logical components :

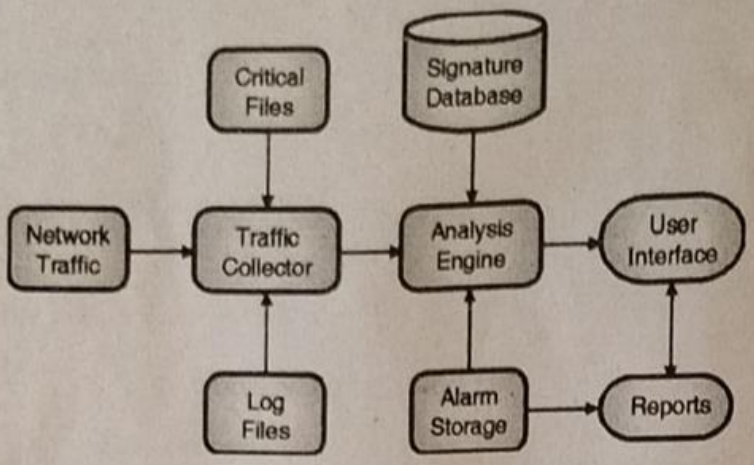


Fig. 4.3.1 : Components of IDS

1. **Traffic collector**
   - The job of traffic collector is used to collect the activity or events from the IDS for examination.
   - Host-based IDS - the events can be log files, audit logs, or traffic coming to or leaving a specific system.
   - Network-based IDS - the events can be a mechanism for copying traffic of the network link.
2. **Analysis Engine**
   - Analysis engine will examine the collected network traffic and compares it to known patterns of suspicious or malicious activity. These malicious activities are stored in the signature database.
   - The analysis engine act like a brain of the IDS.
3. **Signature database**

   Signature database stores the collection of patterns and definitions of known suspicious or malicious activity on host or on network.

4. **User Interface and Reporting**

Its job is to provide interface with the human element and provide alert whenever required. Because of this user can interact with and operate the IDS.

8) Explain Host Based and Network Based IDS with Diagram ?
Ans: Host Based IDS:

- A host based IDS check log files, audit trails and network traffic coming into or leaving specific host.
- HIDS can operate in real time, looking for activity as it arises, or batch mode, looking for activity on a periodic basis.
- Typically Host based systems are self contained, but many new commercial products are designed for reporting to and be managed by a central system. These systems are also taking local system resources to operate.
- Older version of host-based IDSs was operating in batch mode, looking for suspicious activity on an hourly or daily basis and typically looked for particular events in the system's log files.
- In the new version of host-based IDS, processor speed is increased and IDSs start looking through the log files in real time and the ability to examine the data traffic the host was generating and receiving is also added.
- Many host-based IDS focus on the log files or audit trails produced by local operating system. On windows systems, the examined logs are typically Application, System and Security event logs. On Unix system, the examined logs are generally message, kernel and error logs.
- Some host based IDSs have the ability to cover specific applications by examining the logs produced by that specific applications or examining the traffic from the services themselves like FTP, or web services.
- HIDS is looking for certain activities in the log file are :

- Logins at odd hours.
- Login authentication failure.
- Adding new user account.
- Modification or access of critical system files.
- Modification or removal of binary files.
- Starting or stopping processes.
- Privilege escalation.
- Use of certain programs.

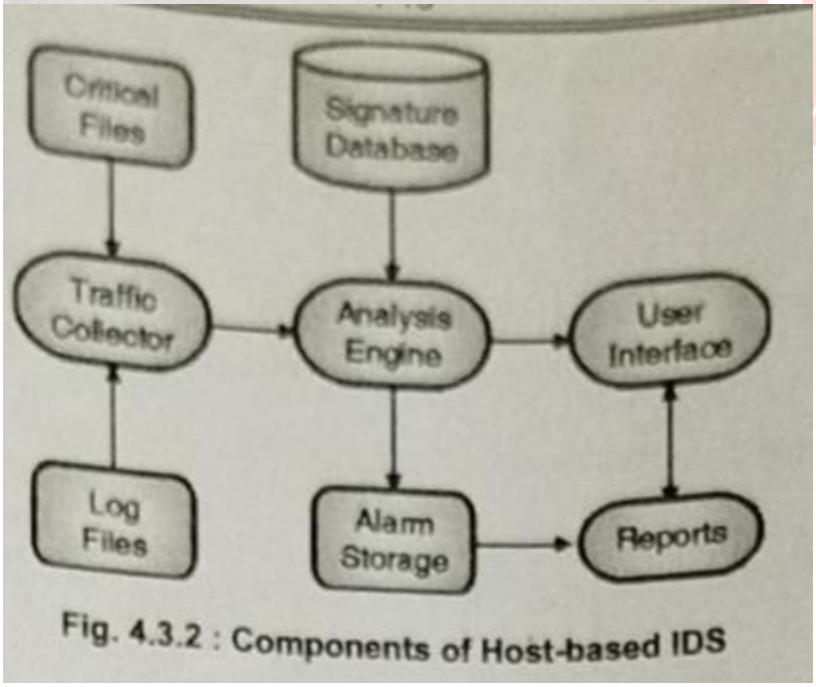


Fig. 4.3.2 : Components of Host-based IDS

Network Based IDS:

- Network based IDS focuses on *network traffic* - the bits and bytes travelling along the cables and wires that interconnect the system.
- A network IDS should check the network traffic when it passes and it is able to analyze traffic according to protocol, type, amount, source, destination, content, traffic already seen etc.
- Such an analysis must occur quickly and the IDS must be able to handle traffic at any speed the network operates on to be effective.
- Network based IDSs are generally deployed so that they can monitor traffic in and out of an organization's major links like connection to the Internet, remote offices, partner etc.

Network-based IDSs looks for certain activities like :

- Denial of service attacks
- Port scans or sweeps
- Malicious content in the data payload of a packet or packets
- Vulnerability scanning
- Trojans, viruses, or worms
- Tunneling
- Brute-force attacks.

– The logical layout of Network-based IDS is shown in following Fig. 4.3.3.

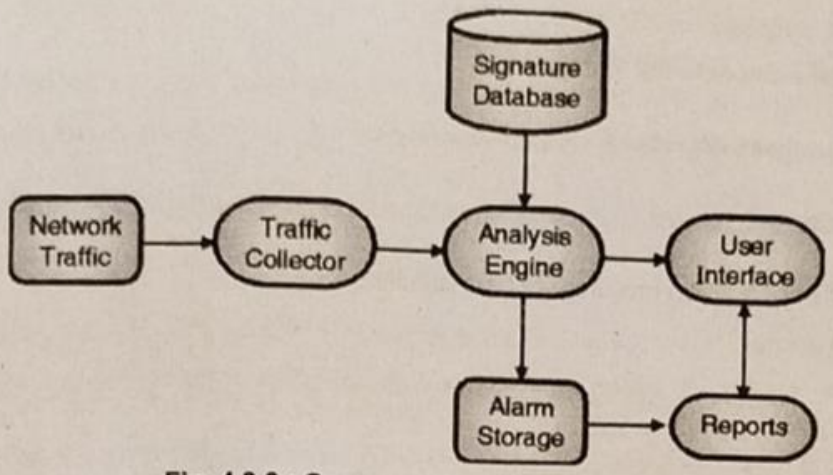


Fig. 4.3.3 : Components of Network IDS

9) Explain Vulnerability Assessment, Misuse Detection and Anomaly Detection?
Ans:

4.3.2 Vulnerability Assessment

- Vulnerability assessment is examining the state of network security.
- Data about open ports, software packages running, network topology etc. are collected and then prioritized the list of vulnerabilities.
- Vulnerability assessment needs to be updated regularly to handle new threats to security.
- In many organizations, they keep the track of security vulnerabilities and list of available patches.

4.3.3 Misuse Detection

- Misuse detection looks for patterns of network traffic or activity in log files that are suspicious, it is known as attack signature.
- Attack signature may contain number of failed login to sensitive host, bits in IP address of buffer overflow attack, TCP SYN packet of SYN flooding attack etc.
- For monitoring the system, IDS can check security policy and database to known vulnerabilities and attacks.
- It is necessary to discover and exploit new vulnerabilities.
- Vendors need to update with the latest attacks and update the issue database and customers need to install the updates.

4.3.4 Anomaly Detection

- To detect potential intrusions, statistical anomaly detection uses statistical techniques.
  - (i) The baseline is established (i.e. normal behaviour).
  - (ii) During the operation, a statistical analysis of the data monitored is performed
  - (iii) If the difference from the baseline is measured and a threshold is exceeded, then an alarm is raised
- Anomaly every time is not an attack. For example - a failed login attempt can be due to administrator forgetting the password or due to an attack.
- The careful attacker can remain undetected without being noticed by IDS when the baseline is adjusted dynamically and automatically.
- A patient attacker will slowly change the 'normal behaviour' over time until his planned attack no longer generates an alarm.

- Thus need to be concerned about :

  (i) False positives – when an attack is flagged however nothing has happened.

  (ii) False negatives – when an attack is missed because it is within the range of normal behavior.

10) Explain HoneyPots with types and also Diagram?
Ans:

– Honeypots are the innovation in Intrusion Detection technology.

- A honeypot is a computer system on the Internet which is specifically set up to attract and "trap" people who are attempting to penetrate (attackers) other critical systems.
- Honey pots are designed :
  1. To purposely divert hackers from accessing critical systems.
  2. To identify malicious activities performed over the Internet by attacker.
  3. To engage the attacker for longer time, so he will stay on the system for administrators to respond.
- The Honeypot system is designed with sensitive monitors and event loggers, which will detect the accesses and collect the information about the attacker's activities.
- There are two different kinds of honeypots. They are classified based on their deployment method :
  1. **Production Honeypot**

     Used by companies and corporations for the purpose of researching the aims of hackers as well as diverting and mitigating the risk of attacks on the overall network.
  2. **Research Honeypot**

     Used by non-profit organizations and educational institutions for the sole purpose of researching the motives and tactics of the hacker community for targeting different networks.
- Overall, honey pots are considered as an effective method to track hacker behaviour and heighten the effectiveness of computer security tools.

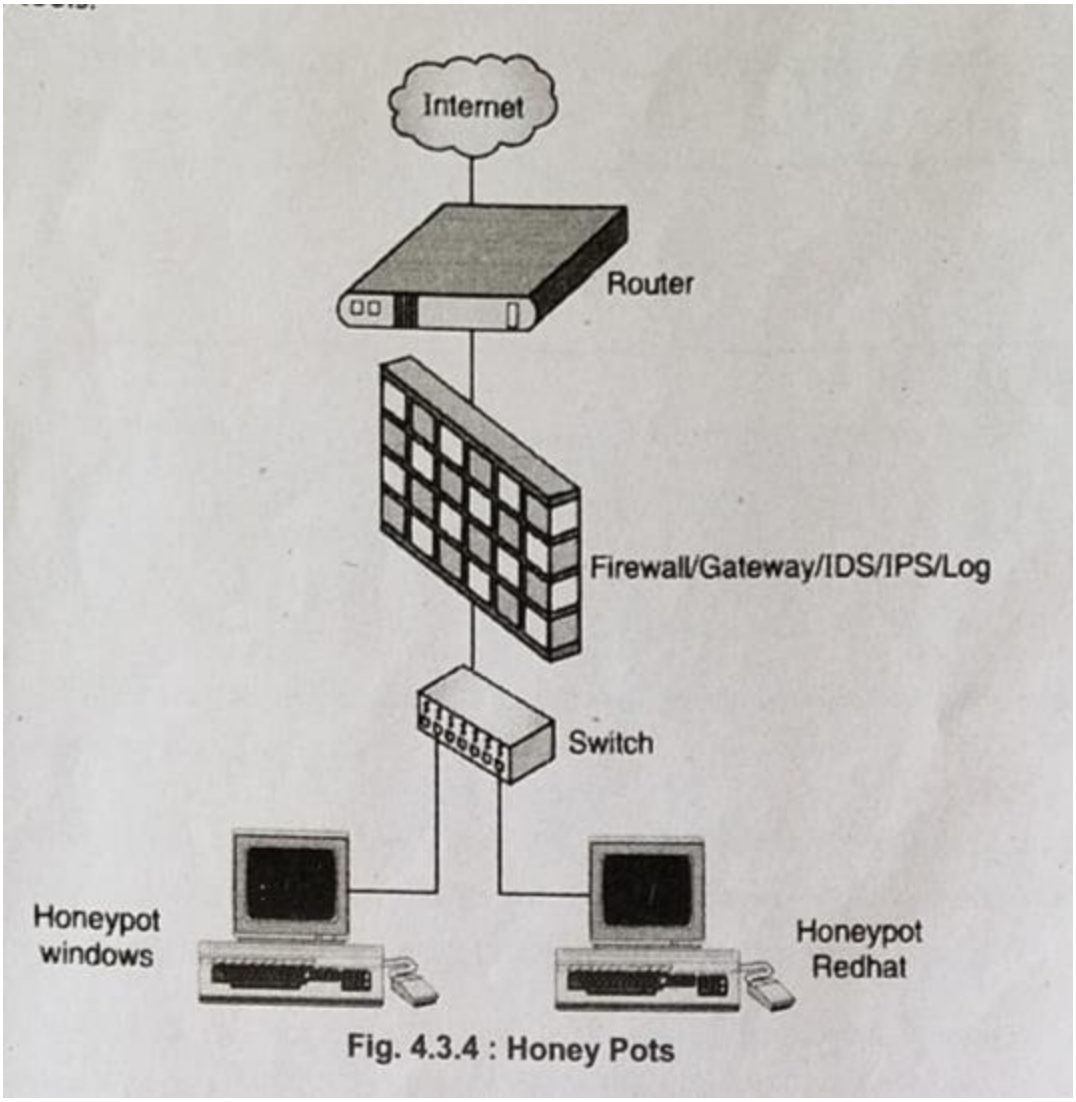


Fig. 4.3.4 : Honey Pots