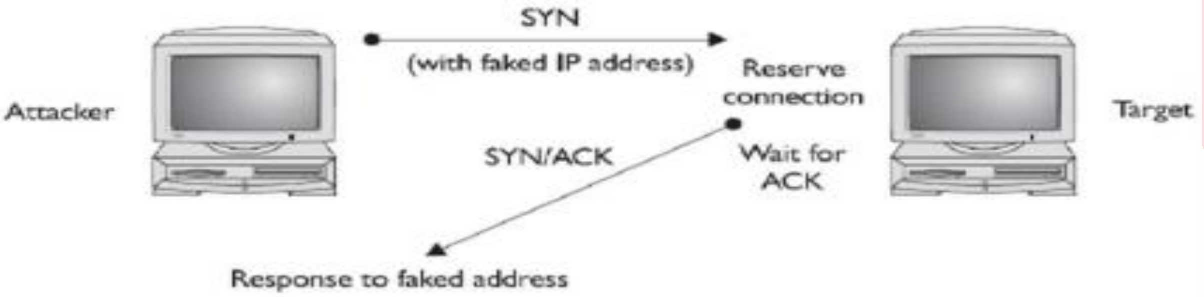
SUPER 25

important questions

(Write point wise, Draw neat diagrams wherever possible)

1) Explain DOS with neat diagram.

Denial Of Service Attack: Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself. The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems. In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come, as shown in Figure.



The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.

2) Explain Public Key Infrastructure with example.

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage publickey encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them. PKI identifies a public key along with its purpose.

It usually consists of the following components:

- A digital certificate also called a public key certificate
- Private Key tokens
- Registration authority
- Certification authority
- CMS or Certification management system

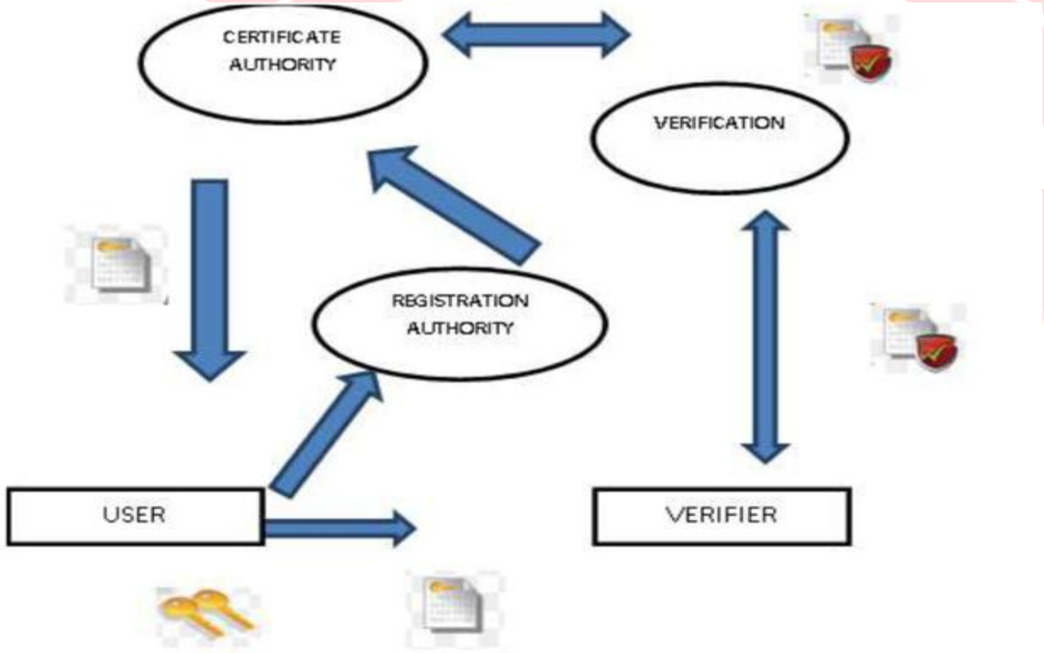
Working on a PKI:

PKI and Encryption: The root of PKI involves the use of cryptography and encryption techniques. Both symmetric and asymmetric encryption uses a public key. There is always a risk of MITM (Man in the middle). This issue is resolved by a PKI using digital certificates. It gives identities to keys in order to make the verification of owners easy and accurate.

Public Key Certificate or Digital Certificate: Digital certificates are issued to people and electronic systems to uniquely identify them in the digital world.

- The Certification Authority (CA) stores the public key of a user along with other information about the client in the digital certificate. The information is signed and a digital signature is also included in the certificate.
- The affirmation for the public key then thus be retrieved by validating the signature using the public key of the Certification Authority.Certification Authority:
- **Certification Authority:** A CA issues and verifies certificates. This authority makes sure that the information in a certificate is real and correct and it also digitally signs the certificate. A CA or Certifying Authority performs these basic roles:
- Generates the key pairs This key pair generated by the CA can be either independent or in collaboration with the client.

- Issuing of the digital certificates When the client successfully provides the right details about his identity, the CA issues a certificate to the client. Then CA further signs this certificate digitally so that no changes can be made to the information.
- Publishing of certificates The CA publishes the certificates so that the users can find them. They can do this by either publishing them in an electronic telephone directory or by sending them out to other people.
- Verification of certificate CA gives a public key that helps in — verifying if the access attempt is authorized or not.
- Revocation In case of suspicious behavior of a client or loss of trust in them, the CA has the power to revoke the digital certificate.



The most popular usage example of PKI (Public Key Infrastructure) is the HTTPS (Hypertext Transfer Protocol Secure) protocol. HTTPS is a combination of the HTTP (Hypertext Transfer Protocol) and SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols to provide encrypted communication and secure identification of a Web server. In HTTPS, the Web server's PKI certificate is used by the browser for two purposes:

Validate the identity of the Web server by verify the CA's digital signature in the certificate.

Encrypt a secret key to be securely delivered to the Web server. The secret key will be used to encrypt actual data to be exchanged between the browser and the Web server.

Other examples of PKI (Public Key Infrastructure) are:

Digital signature - The sender of a digital message uses his/her private key to generate a digital signature attached to the message. The receiver uses the sender's certificate to verify the digital signature to ensure the message was sent by the claimed sender.

Encryption of documents - The sender of a digital message uses the receiver's certificate to encrypt the message to protect the confidentiality of the message. Only the receiver who can use his/her private key decrypt the message.

Digital identification - User's certificate is stored in a smart card to be used to verify card holder's identities.

(CONSIDER ANY ONE EXAMPLE)

3) Explain Policies, configuration & limitations of firewall. (VVIP)

Policies of firewall:

All traffic from inside to outside and vice versa must pass through the firewall. To achieve this all access to local network must first be physically blocked and access only via the firewall should be permitted. As per local security policy traffic should be permitted. The firewall itself must be strong enough so as to render attacks on it useless. **Configuration of firewall**

There are 3 common firewall configurations.

1. Screened host firewall, single-homed bastion configuration
2. Screened host firewall, dual homed bastion configuration
3. Screened subnet firewall configuration

1. Screened host firewall, single-homed bastion configuration

In this type of configuration a firewall consists of following parts

i)A packet filtering router

(ii)An application gateway.

The main purpose of this type is as follows:

- Packet filter is used to ensure that incoming data is allowed only if it is destined for application gateway, by verifying the destination address field of incoming IP packet. It also performs the same task on outing data by checking the source address field of outgoing IP packet.
- Application gateway is used to perform authentication and proxy function. Here Internal users are connected to both application gateway as well as to packet filters therefore if packet filter is successfully attacked then the whole Internal Network is opened to the attacker.

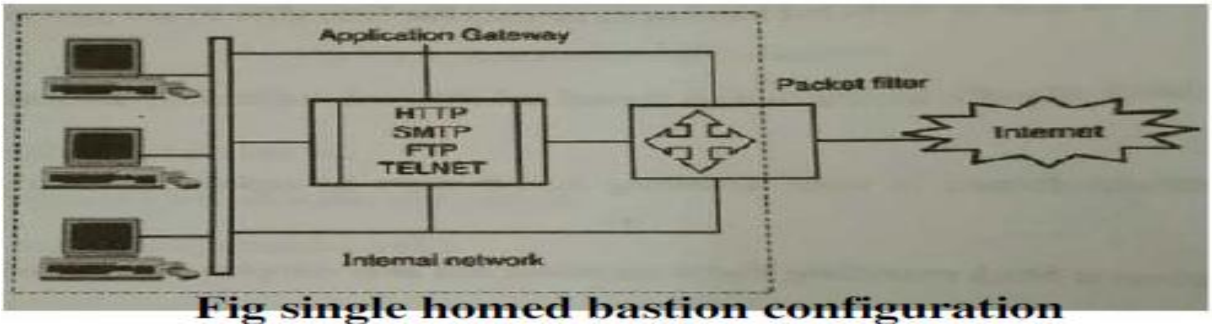


Fig single homed bastion configuration

2. Screened host firewall, dual homed bastion configuration

To overcome the disadvantage of a screened host firewall, single homed bastion configuration, another configuration is available known as screened host firewall, Dual homed bastion. n this, direct connections between internal hosts and packet filter are avoided. As it provide connection between packet filter and application gateway, which has separate connection with the internal hosts. Now if the packet filter is successfully attacked. Only application gateway is visible to attacker. It will provide security to internal hosts.

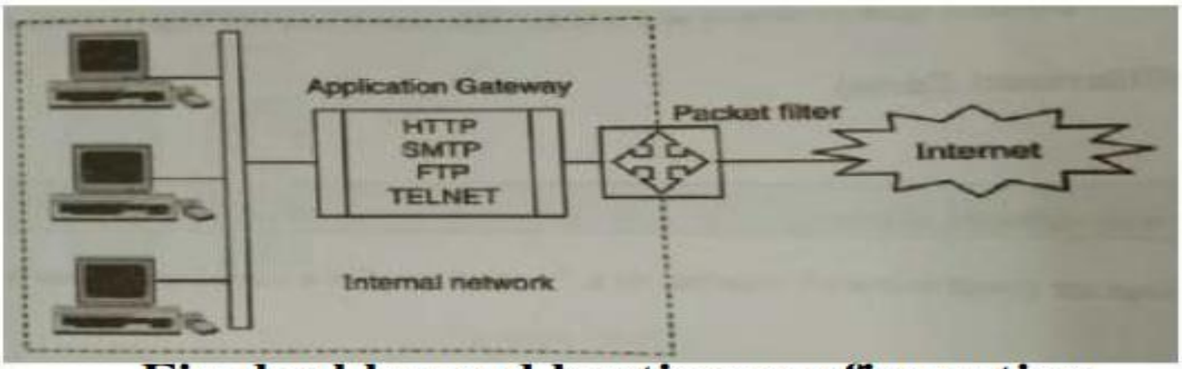


Fig dual homed bastion configuration

3. Screened subnet firewall configuration

It provides the highest security among all firewall configurations. It is improved version over all the available scheme of firewall configuration. It uses two packet filters, one between the internet and application gateway and another between the application gateway and the internal network. Thus this configuration achieves 3 levels of security for an attacker to break into.

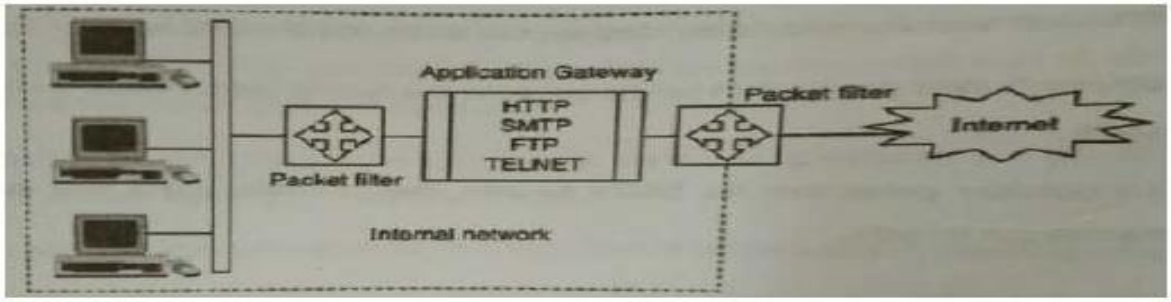


Fig Screened subnet firewall configuration

Limitations: (one mark)

1. Firewall do not protect against inside threats.
2. Packet filter firewall does not provide any content based filtering.
3. Protocol tunneling, i.e. sending data from one protocol to another protocol which negates the purpose of firewall.
4. Encrypted traffic cannot be examine and filter.

4) Explain Kerberos with help of suitable diagram.

Kerberos: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It uses secret key cryptography. It is a solution to network security problems. It provides tools for authentication and strong cryptography over the network to help you secure your information system.

There are 4 parties involved in Kerberos protocol :

i) User

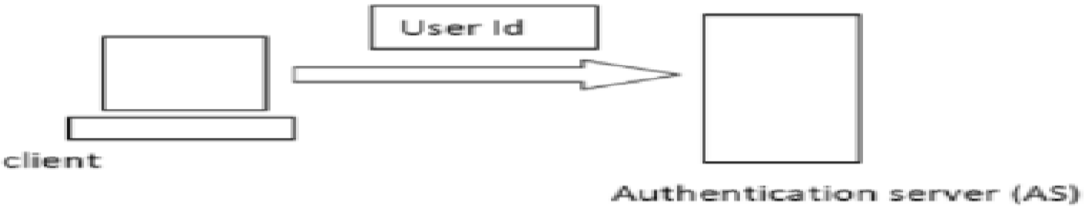
ii) Authentication service (AS)

iii) Ticket granting server (TGS)

iv) Service server

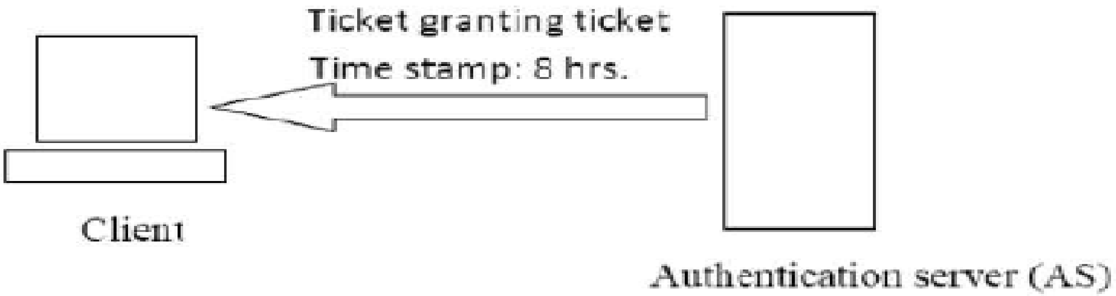
Working of Kerberos:

1. The authentication service, or AS, receivers the request by the client and verifies that the client is indeed the computer it claims to be. This is usually just a simple database lookup of the user"s ID.

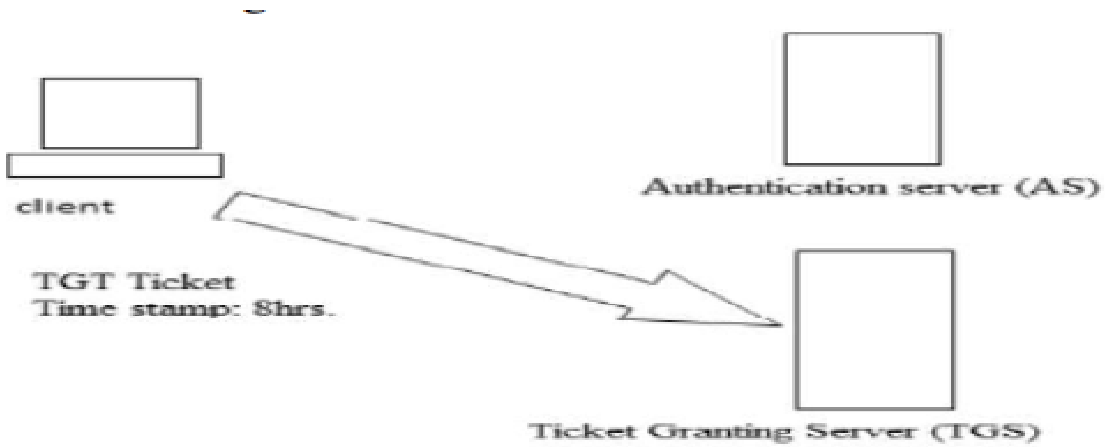


2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless.

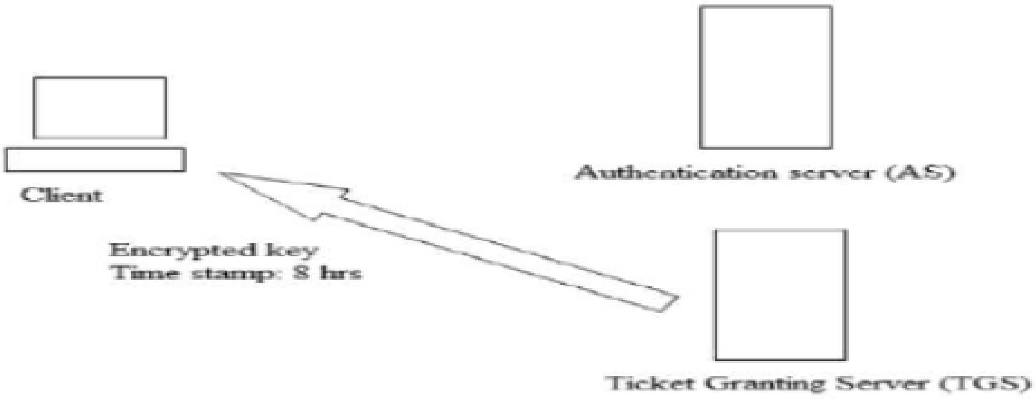
3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.



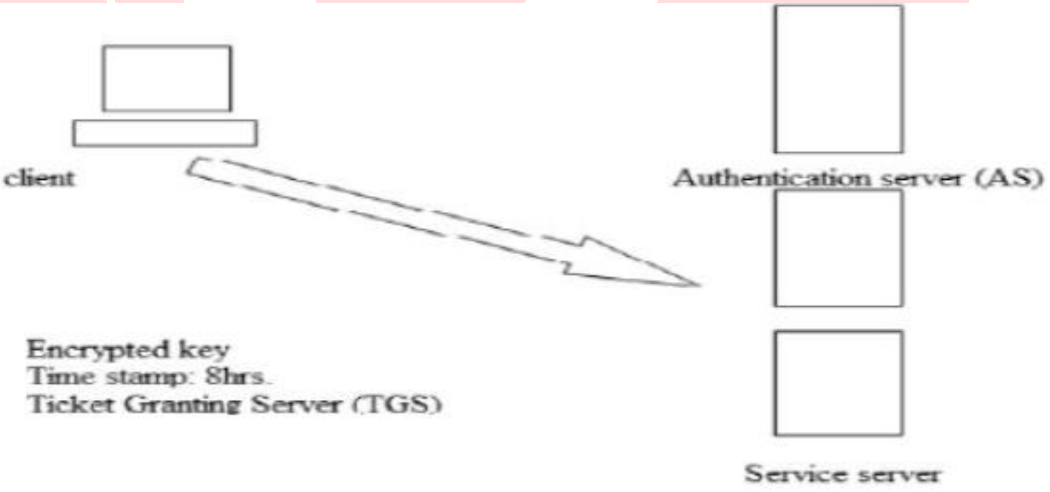
4. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.



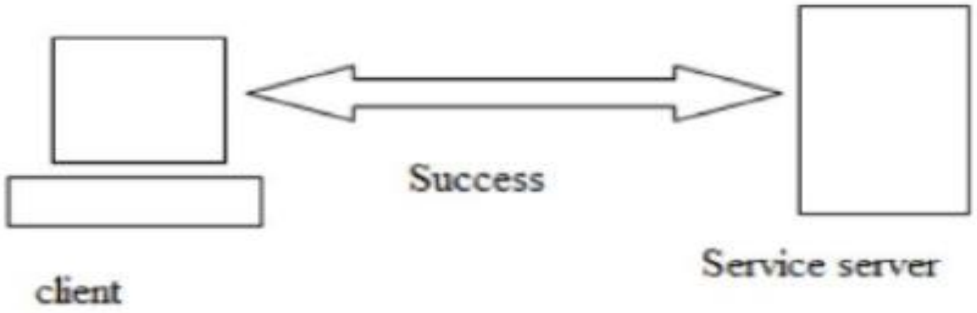
5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.



6. The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service.



7. The service decrypts the key, and makes sure the timestamp is still valid. If it is, the service contacts the key distribution center to receive a session that is returned to the client.



8. The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.

5) Define virus and describe the phases of virus.

Definition: Virus is a program which attaches itself to another program and causes damage to the computer system or the network. It is loaded onto your computer without your knowledge and runs against your wishes.
During the lifecycle of virus it goes through the following four phases:
1. **Dormant phase**: The virus is idle and activated by some event.
2. **Propagation phase**: It places an identical copy of itself into other programs or into certain system areas on the disk.
3. **Triggering phase:** The virus is activated to perform the function for which it was intended.
4. **Execution phase:** The function of virus is performed.

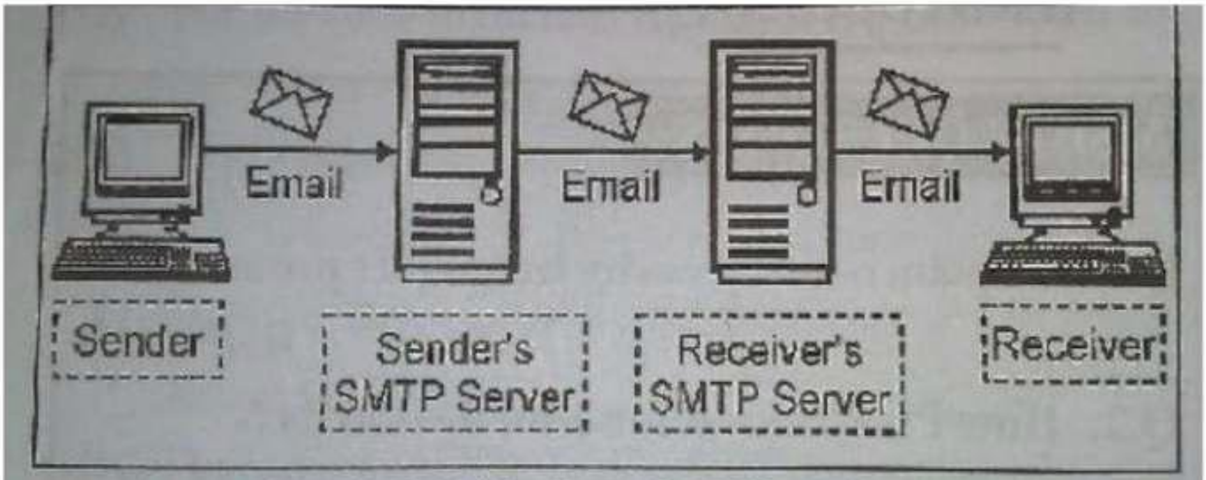
6) Explain working principle of SMTP in detail.

Composition of Mail: A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
1) Submission of Mail: After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
2) Delivery of Mail: E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name. If the domain name of the recipient's email

address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message

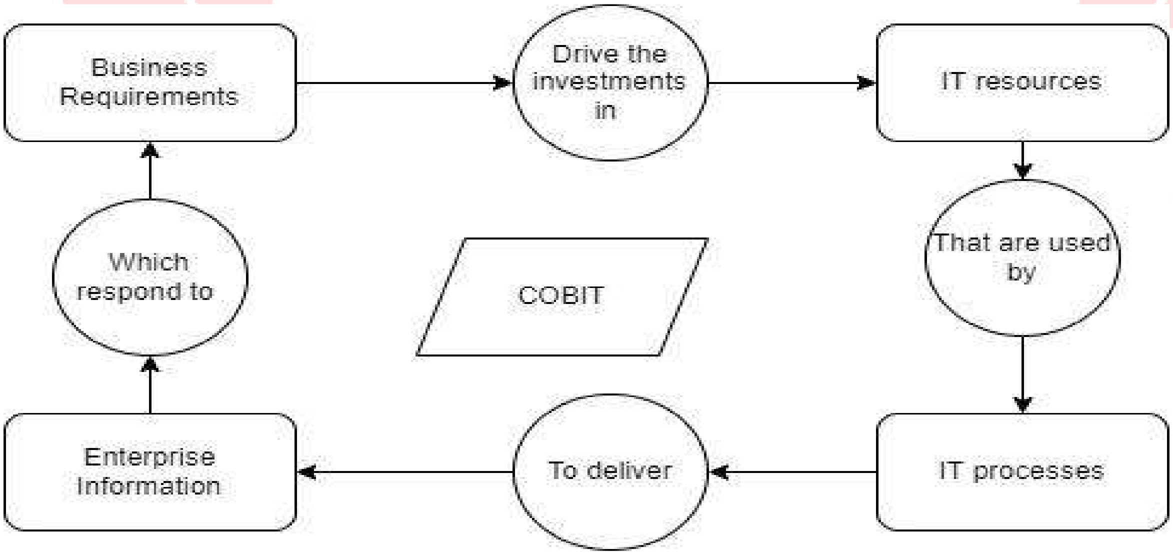
3) Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.

4) Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.



Working of SMTP protocols

7) Describe COBIT framework with neat sketch.



COBIT stands for —Control Objectives for Information and related Technology, it is a framework that was developed by ISACA (Information System Audit and Control Association). It is a set of guidance material for IT governance to manage their requirements, technical issues, and business risks.

COBIT connects IT initiatives with business requirements, monitors and improves IT management practices, and ensures quality control and reliability of information systems in an organization.

- Plan and Organize: This domain addresses direction to solutions, Information architecture, managing IT investments, assess the risks, quality, and project.
- Acquire and Implement: This domain acquires and maintains application software and technology infrastructure, develops as well as maintains procedures and manages changes, implements desired solutions and passes them to be turned into services.
- Deliver and Support: This domain defines and manages service levels, ensures the security of the system, educates or trains, and advises users. It receives solutions and makes them usable for end users.
- Monitor and Evaluate: This domain monitors the process, assesses internal control capability, finds independent assurance, and provides independent audit. Principle of COBIT:
- Providing service of delivering information that an organization requires.
- Undesired events will be prevented, detected, and corrected.

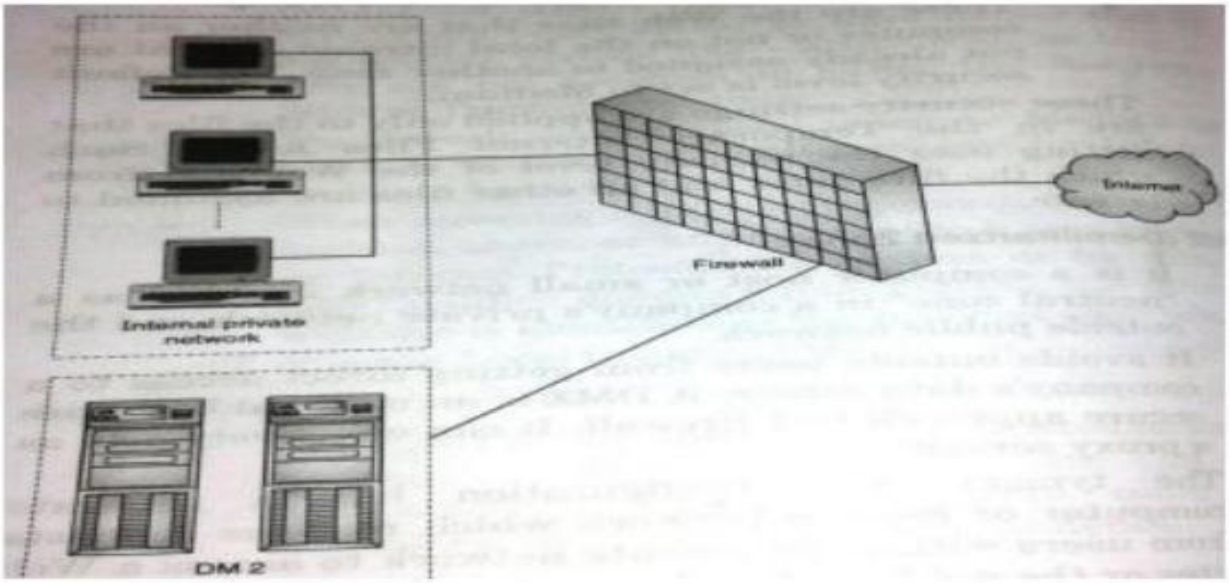
Managing and controlling IT resources using a structured set of processes. Fulfilling client’s requirements. Note: Any other relevant framework shall be considered.

8) Describe the DMZ with suitable example.

DMZ (Demilitarized Zone):

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 public network. Then DMZ host initiates sessions for such requests on the public network but it is not able to initiate a session back 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 the other company‟s data. By any way, if an outsider penetrates the

DMZ‟s security the web pages may get corrupted but other company‟s information can be safe.



9) List Need and Importance of Information? State the Information Classification.

i) Useful life

A data is labelled „more useful‟ when the information is available ready for making changes as and when required. Data might need to be changed from time to time, and when the „change‟ access is available, it is valuable data.

ii) Value of data

This is probably the most essential and standard criteria for information classification. There is some confidential and valuable information of every organization, the loss of which could lead to great losses for the organization while creating organizational issues. Therefore, this data needs to be duly classified and protected.

iii) Personal association

It is important to classify information or data associated with particular individuals or addressed by privacy law.

iv) Age

The value of information often declines with time. Therefore, if the given data or information comes under such a category, the data classification gets lowered.

10) Define Information. Explain the basic principle of information security.

Information is organized or classified data, which has some meaningful values for the receiver. Information is the processed data on which knowledge, decisions and actions are based. For the decision to be meaningful, the processed data must qualify for the following characteristics

□ **Timely** − Information should be available when required.

□ **Accuracy** − Information should be accurate.

□ **Completeness** − Information should be complete.

Basic Principles of information security

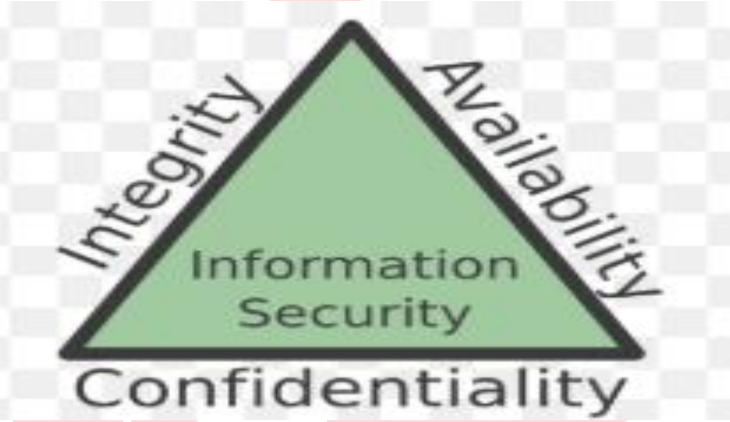


Fig CIA Triad of information security

1. Confidentiality: The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.

2. Authentication helps to establish proof of identities. Authentication process ensures that the origin of a message is correctly identified. Authentication deals with the desire to ensure that an individual is who they claim to be.

3. Integrity: Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information. When the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

11) Explain active attack and passive attack with suitable example.

1) Active Attack:

▪ Definition: Involves an attacker altering or manipulating the data being transmitted.

▪ Example: Man-in-the-Middle (MITM) Attack, where an attacker intercepts communication between two parties and modifies the data before forwarding it.

2) Passive Attack:

▪ Definition: The attacker only monitors or eavesdrops on communication without altering the data.

▪ Example: Eavesdropping on network traffic to capture sensitive information like login credentials

12) State the features of the following IDS :

a. **Host based IDS**
b. **Network based IDS**
c. **Honey pots**

Host Based IDS (HIDS)

- Checks- log files, audit trails, network traffic (incoming/outgoing)
- HIDS – operates in real me- observes activities, batch mode on periodic basis
- It is self-contained-
  - commercial versions take help of central system
  - they also take local system resources to operate
  - Older version-
    - work on batch mode hourly or daily basis
    - looking for the events in system log files
  - New versions-
    - processor speed is increased-
    - it looks for log files in real time –
    - examines data traffic
- **Windows examined logs:** -applications, system and security event logs
- **UNIX examined logs:** - message, kernel, error logs
- **Application specific HIDS**- examine traffic from specific services
- **HIDS is looking for certain log files like:**
  - Logins at odd hours
  - Login authentication failure
  - Adding new user account

- Modification of access of critical system files
- Modification or removal of binary files
- Starting or stopping processes
- Privilege escalation (rapid increase)
- Use of certain programs

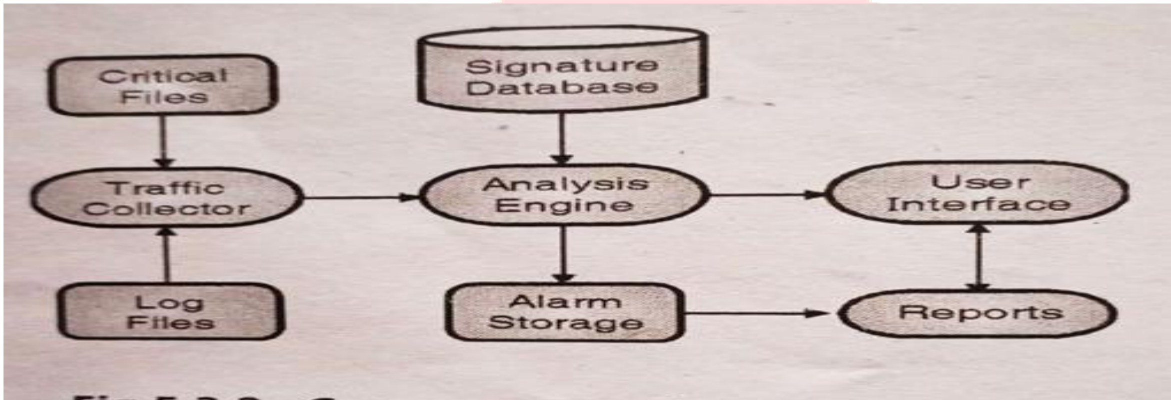


Fig.5.3.2 : Components of Host-based IDS

Advantages

- OS specific and detailed signatures
- Examines data after decryption
- Very application specific

Disadvantages

- Needs to be installed on every host spot
- High-cost ownership and maintenance
- Uses local system resources
- Very focused view and cannot relate to activity around it
- Excluded from the network
- Passive in nature, so it just informs about the attack without doing anything about it.

<u>Network Based IDS (NIDS)</u>

- Focuses on n/w traffic
- Bits and bytes travelling along cables interconnecting system
- Checks traffic according to – protocol, type, amount, source, destination, content, traffic already seen
- analysis occurs quickly at the speed network operates to be effective
- Examines traffic in/out- internet, remote offices, partners etc.
- NIDS looks for certain activities like:
- Denial of service attack (DOS)
- Port scans or sweeps

- Malicious content in data in packet
- Vulnerability scanning
- Trojans, viruses, worms
- Tunneling
- Brute-force attacks

Layout of NIDS

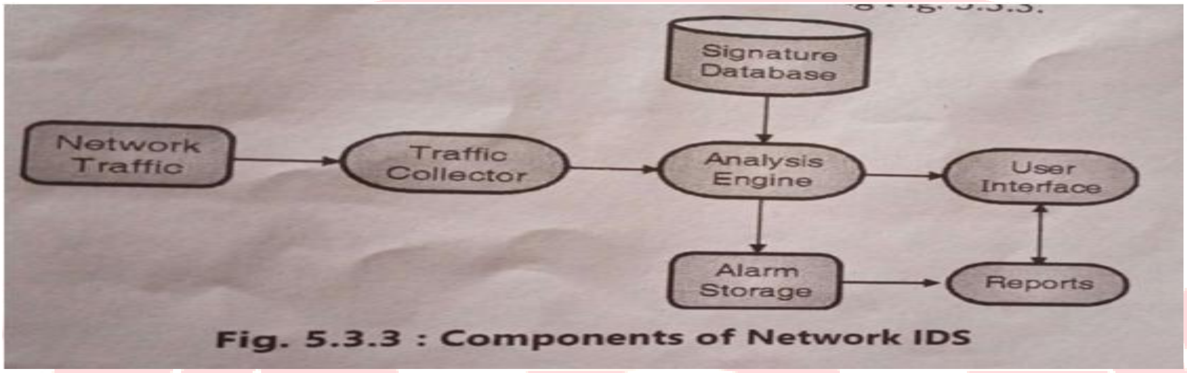


Fig. 5.3.3 : Components of Network IDS

Advantages

- Provides coverage of fewer systems(not single like HIDS)
- Low cost – deployment, maintenance, upgrade
- Visibility into all n/w traffic
- Can corelate multiple systems

Disadvantages

- Ineffective for encrypted traffic
- Can't see traffic that does not pass through it
- it might be slow as compared to the network speed.

Honeypots

- Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.
- The honeypot is designed to do the following:

1. Divert the attention of potential attacker.
2. Collect information about the intruder's action.
3. Provide encouragement to the attacker so as to stay for some time, allowing the administrations to detect this and swiftly act on this.

- Honeypots are designed for 2 important goals

1. Make them look-like full real-life systems.
2. Do not allow legitimate users to know about or access them.

• Different types of honeypots:

1. **Research Honeypot** – A Research Honeypot is used to study about the tactics and techniques of the intruders. It is used as a watch post to see how an attacker is working when compromising a system.

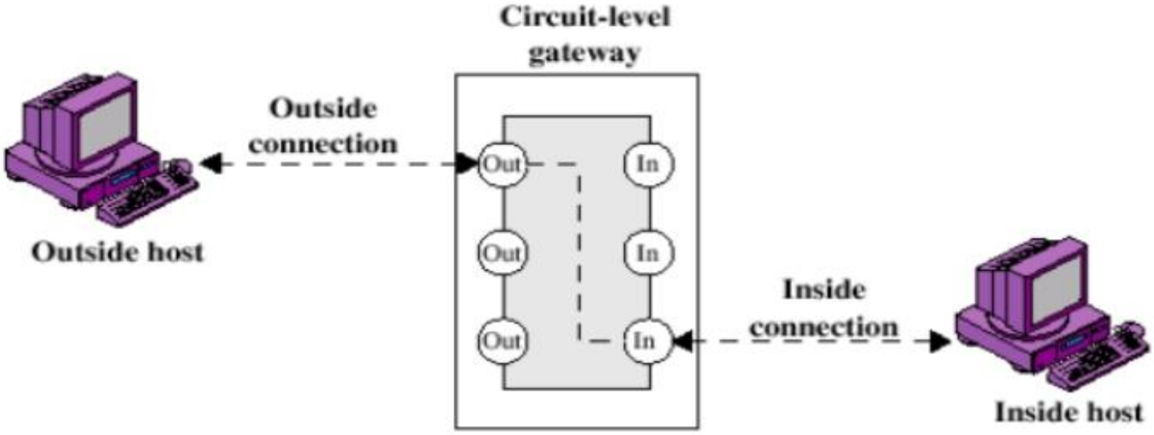
2. **Production Honeypot** – These are primarily used for detection and to protect organizations. The main purpose of a production honeypot is to help mitigate risk in an organization.

13) Define & explain.

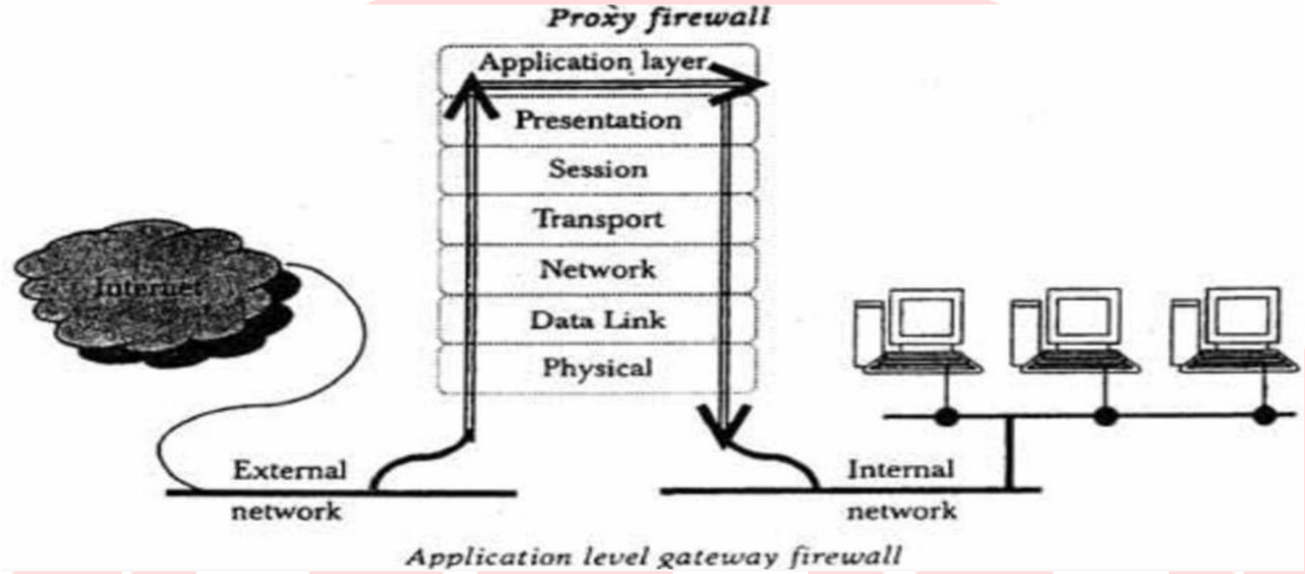
a. Circuit Gateway

b. Application Gateway

Circuit level gateway Firewalls: The circuit level gateway firewalls work at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate. And the information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. So, there is no way for a remote computer or a host to determine the internal private ip addresses of an organization, for example. This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet). This way, the packets are tagged with only the Public IP address (Firewall level) and the internal private IP addresses are not exposed to potential intruders.



Application level gateway Firewalls: Application level firewalls decide whether to drop a packet or send them through based on the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. So, any suspicious data or connections are dropped by these proxies. Application level firewalls ensure protocol conformance. For example, attacks over http that violates the protocol policies like sending Non-ASCII data in the header fields or overly long string along with Non ASCII characters in the host field would be dropped because they have been tampered with, by the intruders.



Application level gateway firewall

14) Explain the following attacks using an example:

a. **Sniffing**
b. **Spoofing**
c. **Phishing**

Sniffing: This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. It can be used to view all traffic or target specific protocol, service, or string of characters like logins. Some network sniffers are not just designed to observe the all traffic but also modify the traffic. Network administrators use sniffers for monitoring traffic. They can also use for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses.

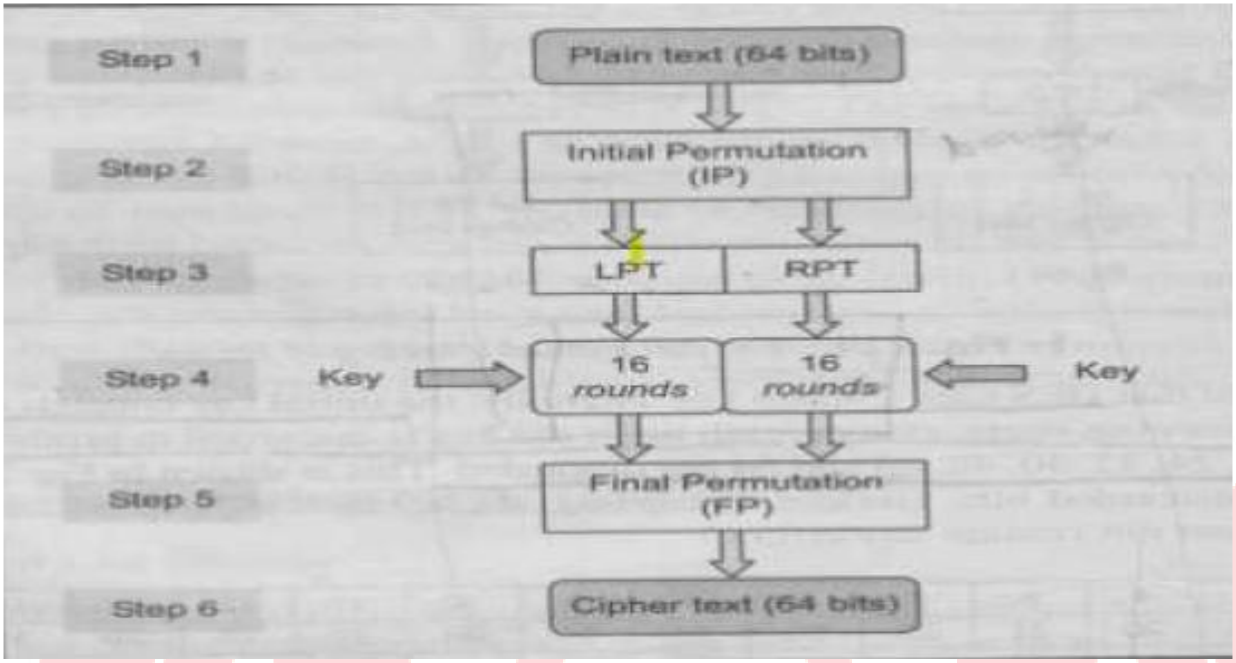
Spoofing: In the context of network security, a **spoofing attack** is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage spoofing involves packet can be captured , data can be modified as per the requirement of third party and may sent to recipients. Following are the types of spoofing
IP Address spoofing

GPS spoofing
Caller id spoofing
Mail spoofing
Third party may use any spoofing technique as per requirement & may get

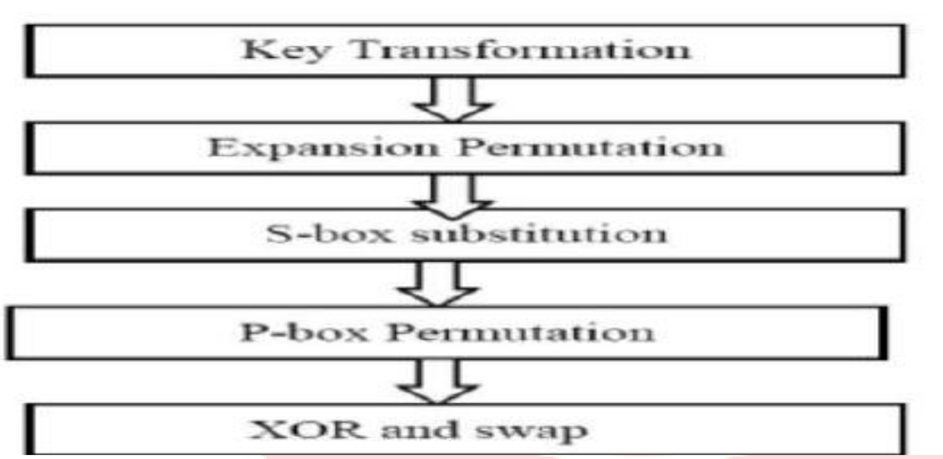
<u>Phishing:</u>

- It is an attempt to steal sensitive information like:
  - Username
  - Password
  - Credit Card Details
  - Bank Account Information
  - Other critical data
- Attacker can – use or sell stolen information
- Attacker- pretend to be trusted source and makes attractive offer to trick victim
- How Phishing works?
  - Planning:
    - Phisher selects the target based on – victims' potential vulnerability and likelihood of them of responding to the fake message
  - Setup:
    - Create methods for delivering the message
    - To collect data about the target
  - Attack:
    - Phisher sends fake message to trick the victim into revealing sensitive information
  - Collection:
    - Phisher records victims' information such as – login credentials or personal details after tricking the into providing them
  - Identify theft and fraud:
    - They use gathered information –
      - to make illegal purchase
      - commit fraud
      - accessing bank accounts
      - making unauthorized transactions
      - opening credit accounts in victims name

Q15) Explain DES in detail



Initial Permutation (IP): It happens only once. It replaces the first bit of the original plain text block with the 58th bit of the original plain text block, the second bit with the 50th bit of original plain text block and so on. The resulting 64-bits permuted text block is divided into two half blocks. Each half block consists of 32 bits. The left block called as LPT and right block called as RPT.16 rounds are performed on these two blocks. Details of one round in DES.



Step 1: key transformation: the initial key is transformed into a 56 bit key by discarding every 8th bit of initial key. Thus ,for each round , a 56 bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation Expansion Permutation Key Transformation

S-box substitution

XOR and swap

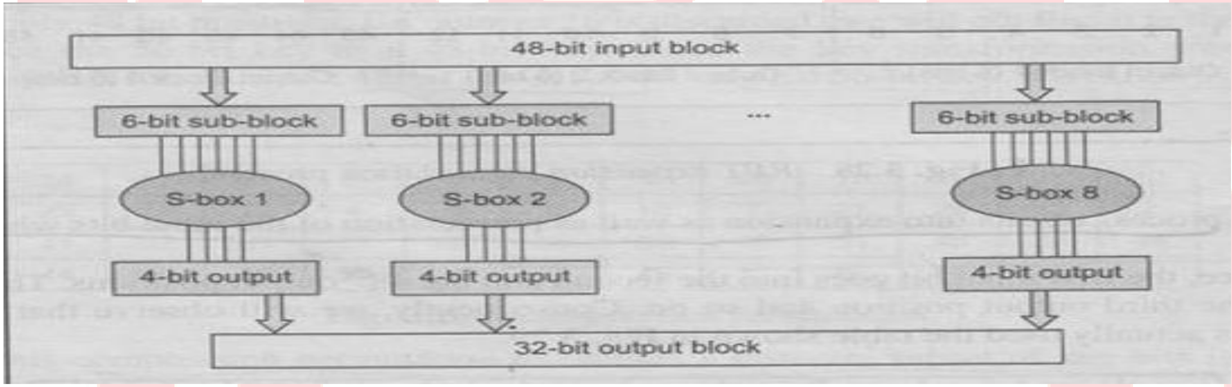
P-box Permutation

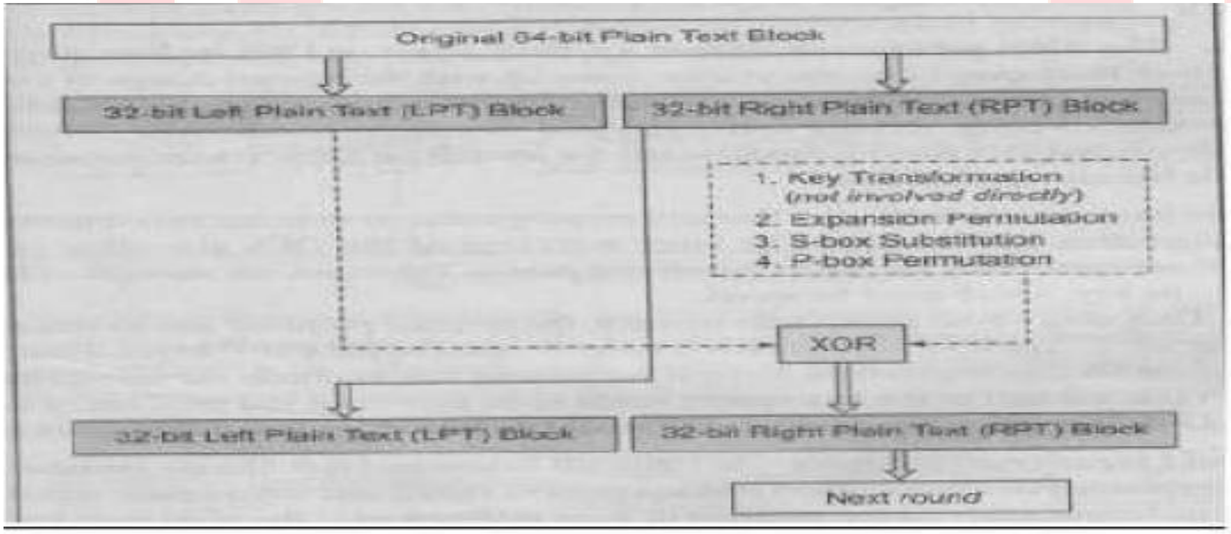
Step 2: Expansion permutation: During Expansion permutation the RPT is expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4-bits. Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block, per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block. The 2nd and 3rd bits are written as they were in the input. The 48 bit key is XOR ed with the 48-bit RPT and the resulting output is given to the next step.

Step 3: S-box substitution: It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques. Each of the 8 S-boxes has a 6-bit input and a 4-bit output. The output of each S-box then combined to form a 32-bit block, which is given to the last stage of a round

Step 4: P- box permutation: the output of S-box consists of 32-bits. These 32-bits are permuted using P-box.

Step 5: XOR and Swap: The LPT of the initial 64-bits plain text block is XORed with the output produced by P box-permutation. It produces new RPT. The old RPT becomes new LPT, in a process of swapping.



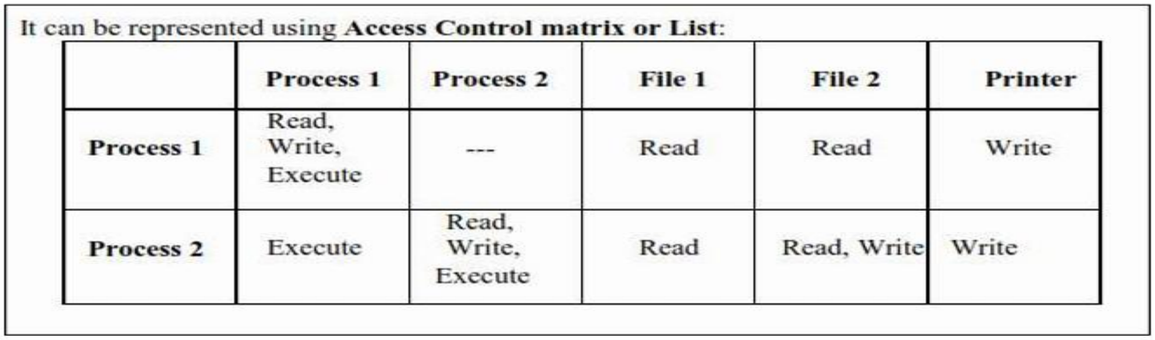

Original 64-bit Plain Text Block
32-bit Left Plain Text (LPT) Block
32-bit Right Plain Text (RPT) Block
1. Key Transformation (not involved directly)
2. Expansion Permutation
3. S-box Substitution
4. P-box Permutation
XOR
32-bit Left Plain Text (LPT) Block
32-bit Right Plain Text (RPT) Block
Next round

Final Permutation: At the end of 16 rounds, the final permutation is performed. This is simple transposition. For e.g., the 40th input bit takes the position of 1st output bit and so on.

16) Explain access control policies – DAC, MAC, RBAC

Policies –DAC, MAC, RBAC, & ABAC

Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.



It can be represented using **Access Control matrix or List**:

	Process 1	**Process 2**	**File 1**	**File 2**	**Printer**
Process 1	Read, Write, Execute	---	Read	Read	Write
Process 2	Execute	Read, Write, Execute	Read	Read, Write	Write

Discretionary Access control (DAC): Restricting access to objects based on the identity of subjects and or groups to which they belongs to, it is conditional, basically used by military to control access on system. UNIX based System is common method to permit user for read/write and execute

Mandatory Access control (MAC): It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity based restriction, formal authorization subject to sensitivity. In MAC the owner or User cannot determine whether access is granted to or not. i.e. Operating system rights. Security mechanism controls access to all objects and individual cannot change that access.

Role Based Access Control (RBAC): Each user can be assigned specific access permission for objects associated with computer or network. Set of roles are defined. Role in-turn assigns access permissions which are necessary to perform role. Different User will be granted different permissions to do specific duties as per their classification.

ABAC – Attribute based access control

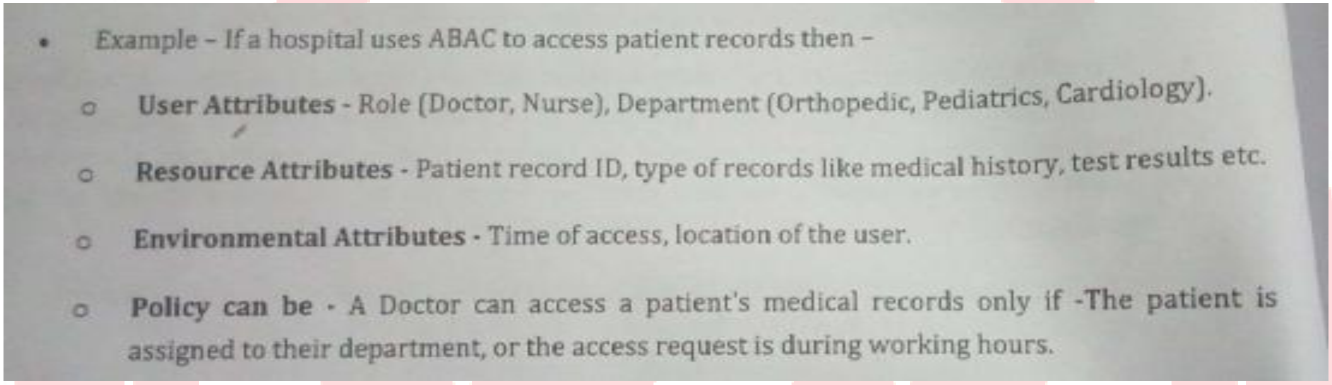
- New control policy
- Based on attributes associated with identity
- Attributes-

1. user details
2. resource information

3. environmental factors (location or me)
4. user credentials

Definition of ABAC:

- “an access control method where subject requests to perform operations on the objects which are granted or denied based on assigned attributes of the subjects, assigned attributes of the objects, environmental conditions, and set of policies that are specified in terms of those attributes or conditions”
- ABAC – implemented using standards like eXtensible Access Control Markup Language(XACML)
- Uses attributes and policies to decide access rights
- E.g.



- Example – If a hospital uses ABAC to access patient records then –
  - **User Attributes** - Role (Doctor, Nurse), Department (Orthopedic, Pediatrics, Cardiology).
  - **Resource Attributes** - Patient record ID, type of records like medical history, test results etc.
  - **Environmental Attributes** - Time of access, location of the user.
  - **Policy can be** - A Doctor can access a patient's medical records only if -The patient is assigned to their department, or the access request is during working hours.

Q17) Explain digital signature in Cryptography.

<u>Digital Signature:</u>

1. Digital signature is a strong method of authentication in an electronic form.
2. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols.
3. Digital Signature is used for authentication of the message and the sender to verify the integrity of the message.
4. Digital Signature may be in the form of text, symbol, image or audio.
5. In today‟s world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster.
6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature.
7. Digital signature algorithms are divided into two parts-

a. Signing part: It allows the sender to create his digital signature.

b. Verification part: It is used by the receiver for verifying the signature after receiving the message.

Generation and Verification of digital signatures:

Working:

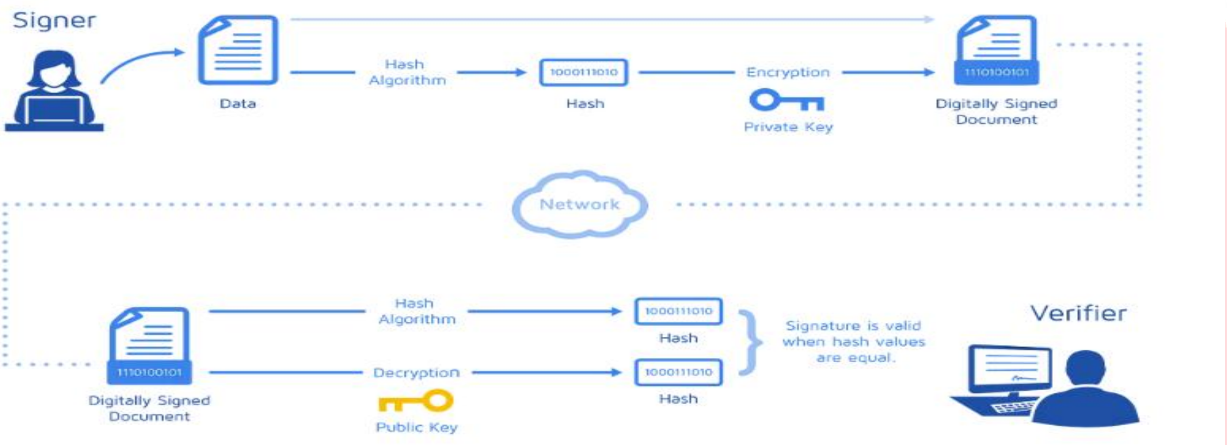
1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.

2. The message digest is encrypted using user"s private key.

3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.

4. The receiver calculates the message digest from the plain text or message he received.

5. Receiver decrypts the encrypted message digest using the sender"s public key. If both the MDs are not same then the plaintext or message is modified after signing.



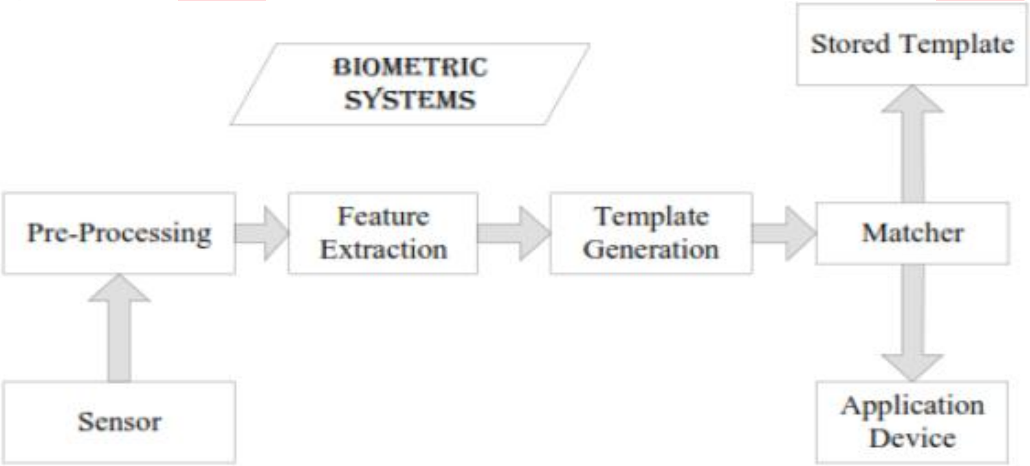
Advantages of Digital Signatures

- Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.
- Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
- Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.
- Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.
- Non-Repudiation: Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.
- Time-Stamp: By time-stamping your digital signatures, you will clearly know when the document was signed.

Q18) Enlist types of Biometrics & explain any one Biometrics type in detail.

Different types of Biometrics

1. Finger print recognition
2. Hand print recognition
3. Retina/iris scan technique
4. Face recognition
5. Voice patterns recognition
6. Signature and writing patterns recognition
7. Keystroke dynamics



Above figure shows the block diagram of biometric system.

Finger print recognition

Fingerprint registration & verification process

1. During registration, first time an individual uses a biometric system is called an enrollment.
2. During the enrollment, biometric information from an individual is stored.
3. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment.
4. The first block (sensor) is the interface between the real
5. world and the system; it has to acquire all the necessary data.
6. The 2nd block performs all the necessary pre-processing
7. The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way.
8. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both).

9. If a matching phase is being performed the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm.
10. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.

Q19) Define Hacking. Explain different types of Hackers.

Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage.

OR

Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Hacking is not always a malicious activity, but the term has mostly negative connotations due to its association with cybercrime.

Different Types of Hackers:

1. Black Hat Hacker - Black hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals.

2. White Hat Hacker -White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world. These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system.

3. Gray Hat Hacker - Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

20) Define computer security and its need.

Computer Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization.

Need of computer Security:

1. For prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc.
2. To make data remain safe and confidential.

3. To provide confidentiality which ensures that only those individuals should ever be able to view data they are not entitled to.
4. To provide integrity which ensures that only authorized individuals should ever be able change or modify information.
5. To provide availability which ensure that the data or system itself is available for use when authorized user wants it.
6. To provide authentication which deals with the desire to ensure that an authorized individual.
7. To provide non-repudiation which deals with the ability to verify that message has been sent and received by an authorized user.

OR

1. Confidentiality: The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message. Example of compromising the Confidentiality of a message is shown in fig:

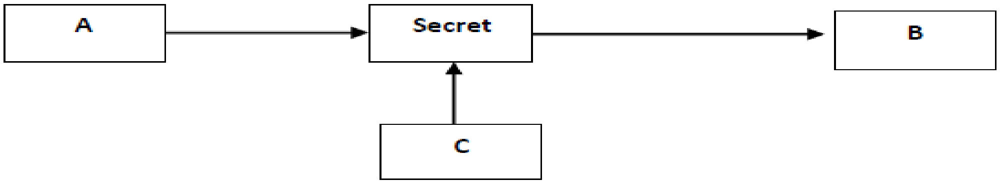


Fig. Loss of confidentiality

Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of Confidentiality. This type of attack is also called as **interception.**

2. Integrity: when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change. This type of attack is called as **modification**.

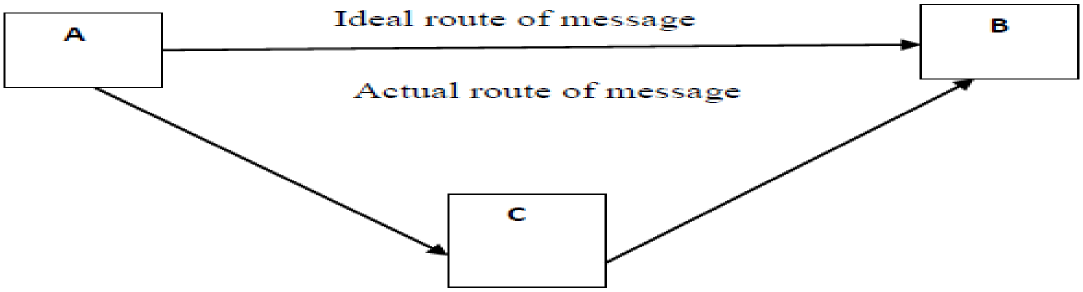


Fig. Loss of Integrity

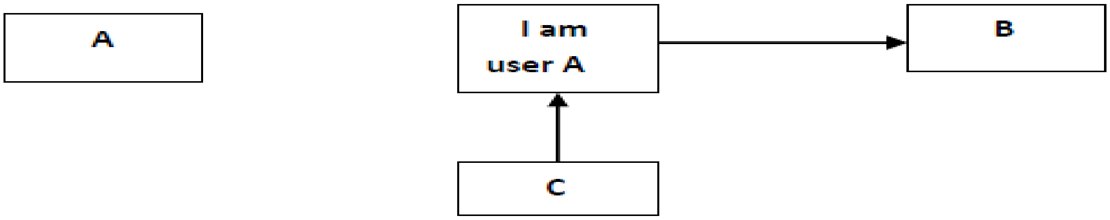


Fig. Absence of authentication

3. Authentication: Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified. For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A? This concept is shown in fig. below. This type of attack is called as **fabrication.**

4. **Availability:** The goal of availability s to ensure that the data, or the system itself, is available for use when the authorized user wants it.

21) Define Risk. Describe qualitative and quantitative risk analysis.

Risk: A computer security risk is any event or action that could cause a loss or damage to computer hardware, software, data, or information

OR

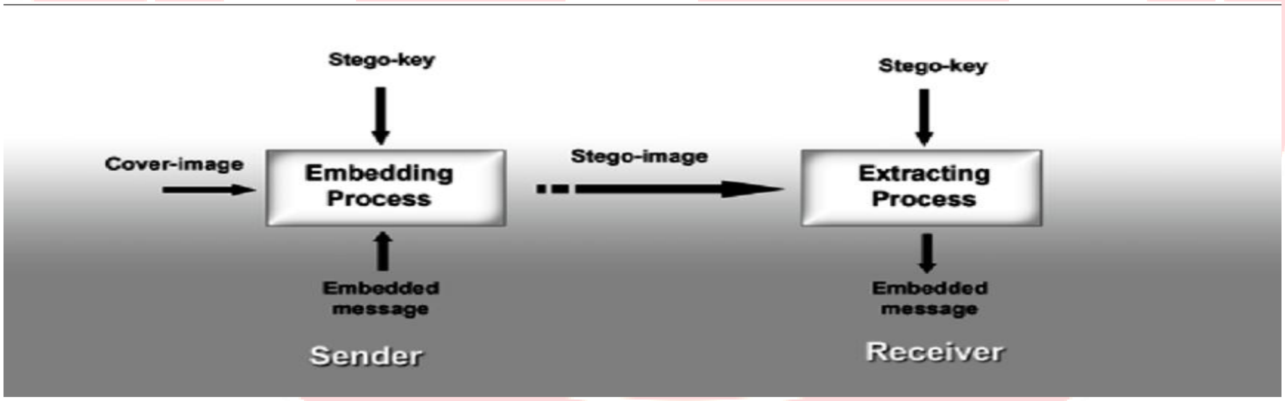
Risk is probability of threats that may occur because of presence of vulnerability in a system.

Quantitative Risk Analysis: A Process of assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats. It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation. In this 100% quantitative risk analysis is not possible.

Qualitative Risk Analysis: A collaborative process of assigning relative values to assets, assessing their risk exposure and estimating the cost of controlling the risk. It utilizes relative measures and approximate costs rather than precise valuation and cost determination. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc. In this 100% qualitative risk analysis is feasible.

Q22) Write a short note on steganography.

Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, html or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text or even images. In modern steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image.



Steganography 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.
Advantages:

1. With the help of steganography we can hide secret message within graphics image.
2. In modern Steganography, data is encrypted first and then inserted using special algorithm so that no one suspects its existence.

Drawbacks:

1. It requires lot of overhead to hide a relatively few bits of information.
2. Once the system is discovered, it becomes virtually worthless.

Q23) Describe piggy backing and shoulder surfing, dumpster diving.

Piggybacking: It is the simple process 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. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. i.e. Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission, it means when an authorized person allows (intentionally or unintentionally) others to pass through a secure door. Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. Piggybacking is sometimes referred to as "Wi-Fi squatting." The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network.

Shoulder surfing: Shoulder surfing a similar procedure in which attackers position themselves in such a way as to- be-able to observe the authorized user entering the correct access code. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision enhancing devices. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.

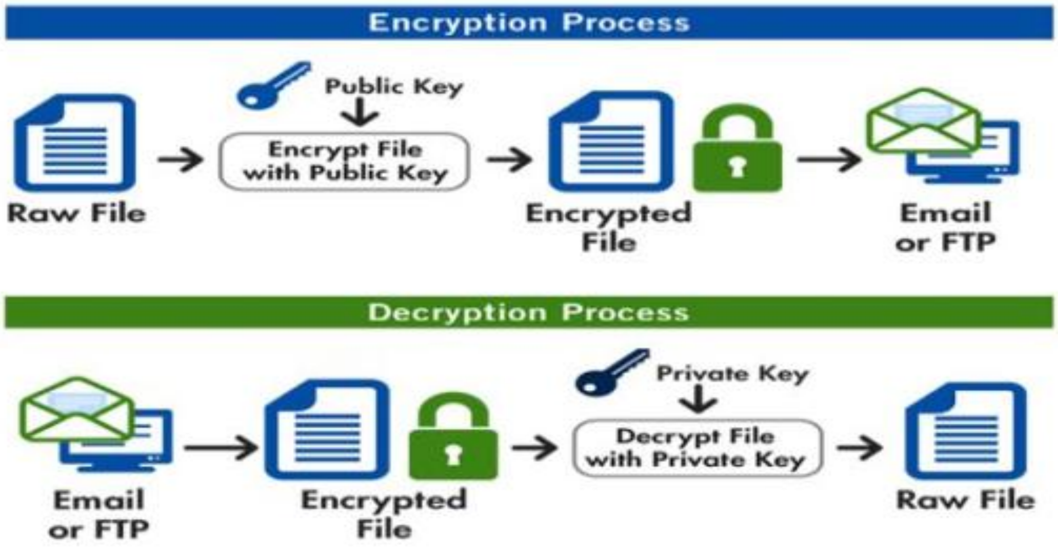
Dumpster diving: It is the process of going through a target's trash in order to find little bits of information. It refers to a form of reconnaissance where attackers search through an organization's discarded waste to gather information that can be used for malicious purposes. This includes anything from sensitive documents like passwords and access codes to less obvious items like employee contact lists, which can be used in social engineering attacks.

Q24) Describe any four password selection criteria.

Password: Password is a secret word or expression used by authorized persons to prove their right to access, information, etc.
Components of good password:
1. It should be at least eight characters long.
2. It should include uppercase and lowercase letters, numbers, special characters or punctuation marks.
3. It should not contain dictionary words.
4. It should not contain the user's personal information such as their name, family member's name, birth date, pet name, phone number or any other detail that can easily be identified.
5. It should not be the same as the user's login name.
6. It should not be the default passwords as supplied by the system vendor such as password, guest, and admin and so on.

Q25) Describe PGP with suitable diagram.

PGP is Pretty Good Privacy. It is a popular program used to encrypt and decrypt email over the internet. It becomes a standard for email security. It is used to send encrypted code (digital signature) that lets the receiver verify the sender's identity and takes care that the route of message should not change. PGP can be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders It is available in Low cost and Freeware version. It is most widely used privacy ensuring program used by individuals as well as many corporations.



There are five steps as shown below:

1. Digital signature: it consists of the creation a message digest of the email message using SHA-1 algorithm. The resulting MD is then encrypted with the sender's private key. The result is the sender's digital signature.

2. Compression: The input message as well as p digital signature are compressed together to reduce the size of final message that will be transmitted. For this the Lempel -Ziv algorithm is used.

3. Encryption: The compressed output of step 2 (i.e. the compressed form of the original email and the digital signature together) are encrypted with a symmetric key.

4. Digital enveloping: the symmetric key used for encryption in step 3 is now encrypted with the receiver's public key. The output of step 3 and 4 together form a digital envelope.

5. Base -64 encoding: this process transforms arbitrary binary input into printable character output. The binary input is processed in blocks of 3 octets (24-bits).these 24 bits are considered to be made up of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into an 8 bit output character in this process.