UNIT – 1

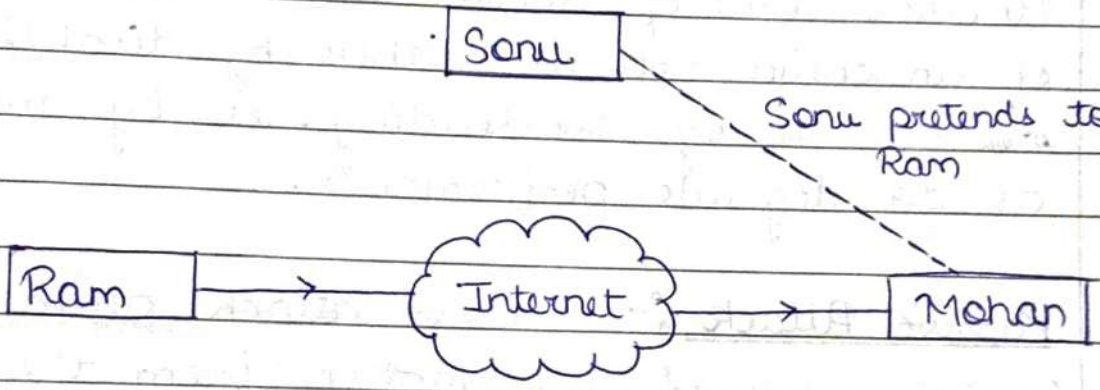
Introduction

★ **Attacks :-**

(1.) **Active attack** – An active attack attempts to alter system resources or affect their operations. Active attack involve some modification of data stream or creation of false statement.

Types of active attacks are as follows –

1- **Masquerade** – This attack takes place when one entity pretends to be different entity.



2- **Modification of messages** – It means that some portion of a message is altered or that message is delayed or recorded to produce an unauthorised effect.
For example – "Mohan is allowed to read confidential file x" is modified as "Sonu is allowed to access confidential file x".

3- **Repudiation** – This attack is done by either sender or receiver. The sender or receiver can deny later that he or she has send or receive a message.

Example – Customer ask his bank "to transfer an amount to someone" and later on the sender (customer) deny that he had made such a request. This is repudiation.

4- **Replay** – It involves the passive capture of a message and its sub-sequent the transmission to produce an authorised effect.

5- **Denial of Service** – It prevents normal use of communication facilities. This attack may have a specific target.
Example- An entity may suppress all messages directed to a particular destination.
Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it by messages so as to degrade performance.

(2) **Passive Attack** :- Passive attack attempts to learn or make use of information from the system but does not affect system resources.
Passive attacks are in the nature of monitoring of transmission. ~~The release~~

1- **The release of message content** – Telephonic conversation, e-mail message or a transfered message contain sensitive or confidential information. We would like to prevent an opponent from learning the content of these transmissions.

2- **Traffic analysis** – We tend to make encryption of

information so that the attacker even if captured, the ~~message~~ attacker could not extract any information from the message.

The opponent could determine the location and identity of communicating host, and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

★ **Security Services** :- Security services are the methods used to enhance the security of the network. It helps in implementing security policies and uses various security mechanisms. A security mechanism is a method which is used to protect your message from unauthorised entity. There are four types of security services -

1- **Authentication** — Authentication ensures that the entity sending or receiving the messages is the one, It is actually pretending to be. Two types of authentications mainly used in network are -

(i) Peer entity authentication used in association with a logical connection to provide confidence in the identity of the entities connected.

(ii) Data origin authentication, in a connectionless transfer, provides assurance that the source of received data is as claimed.

2- **Access Control** — Access control prevents the unauthorized use of resources. This service control who can have

access to a resource, under what conditions access can occur and what those accessing that resource are allowed to do.

In other words, access control can be defined as the ability to permit or deny the use of something by someone.

3- **Data confidentiality** — Data confidentiality avoids unauthorization by ensuring that the data is being received safely by the original receiver, for whom it was actually meant for. Various types of confidentiality are as follow -

(i) **Connection Confidentiality** - The protection of all user data on a connection.

(ii) **Connectionless Confidentiality** — The protection of all user data in a single data block.

(iii) **Selective field Confidentiality** — The confidentiality of selected fields within the user data on a connection or a single data-block.

(iv) **Traffic flow Confidentiality** — The protection of the information that might be derived from observation of traffic flow.

4- **Data Integrity** — Data integrity ensures that data received is exactly the same as sent by an authorised entity (i.e. contains no modification, insertion, deletion or replay).

* **Security Mechanism :-** Security mechanism deals with identification of any break in security and also helps in removing it. It is different from security services. Security mechanisms are also used to identify and recover from various security attacks.

Security mechanisms are as follows -

1- **Encipherment :** Encipherment is also known as encryption. It is the process of using mathematical formulas, algorithms and the keys to transform the simple message into a message that is not easily understood by each and everyone.

2- **Digital Signatures :** These are similar to signatures on paper done in real life but these are done in computer documents and in cryptographic format to ensure the source and integrity.

3- **Access Control :** Access control includes variety of techniques used to avoid unauthorized access or granting only limited access to data or network resources.

4- **Data Integrity :** It ensures that the data received on receiver side is same as sent by the original data transfer.

5- **Routing Control :** Routing control is a computer network technique that uses various mechanisms to avoid the traffic congestion in the network. It helps in denial of service attack.

★ **Cryptography** :- Cryptography is a science which is used in encryption and decryption of data. Cryptography enables us to store sensitive information or transmit it across insecure networks (like internet) so that it cannot be read by anyone except the intended receipent.

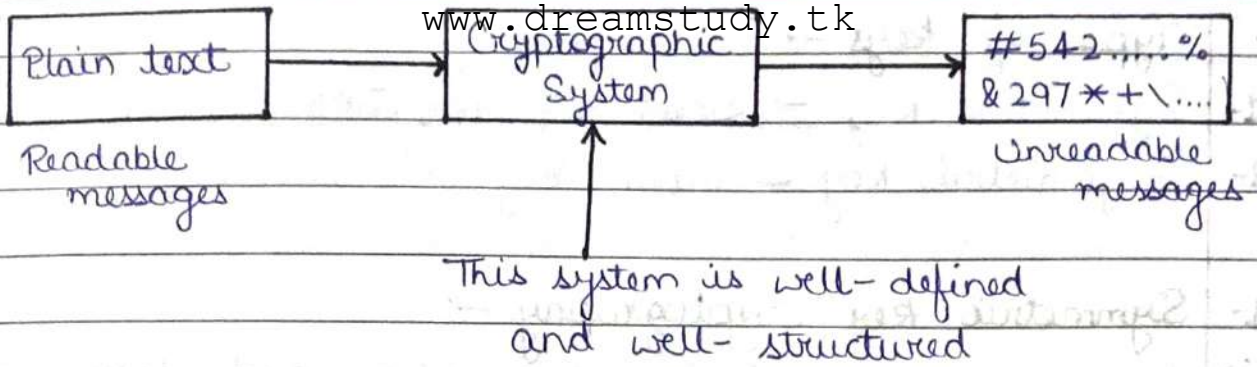
Cryptography is a Greek word which means secret writing.

The sender encrypts a message using a secret key and the receiver decrypts it before reading. Someone who intercepts the message sees only a apparently random symbols. Without the key he cannot read it. Cryptography is a practice and study of hiding information.

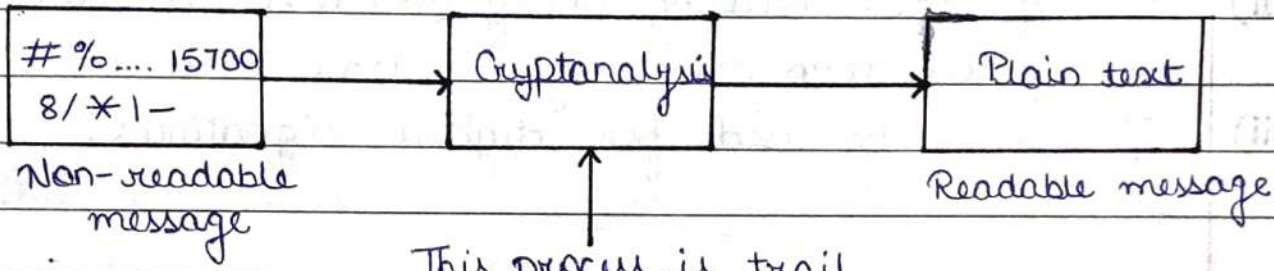
Example –

It is the art and science of achieving security by encoding messages to make them non-readable. Cryptography has been defined as the 'UMBRELLA' word used to describe the entire field of secret communication.

The purpose of cryptography was to hide something that had been written. It can also be applied to software, graphics, voice i.e. it can be applied to anything. That can be digitally coded.



* **Cryptanalysis :-** It is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.



Cryptology – It is the combination of cryptography and cryptanalysis.

Cryptography + Cryptanalysis = Cryptology

* **Key :-** In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text or to decrypt encrypted text.

In database content, a key is a unique field that is used for sorting or selecting record.

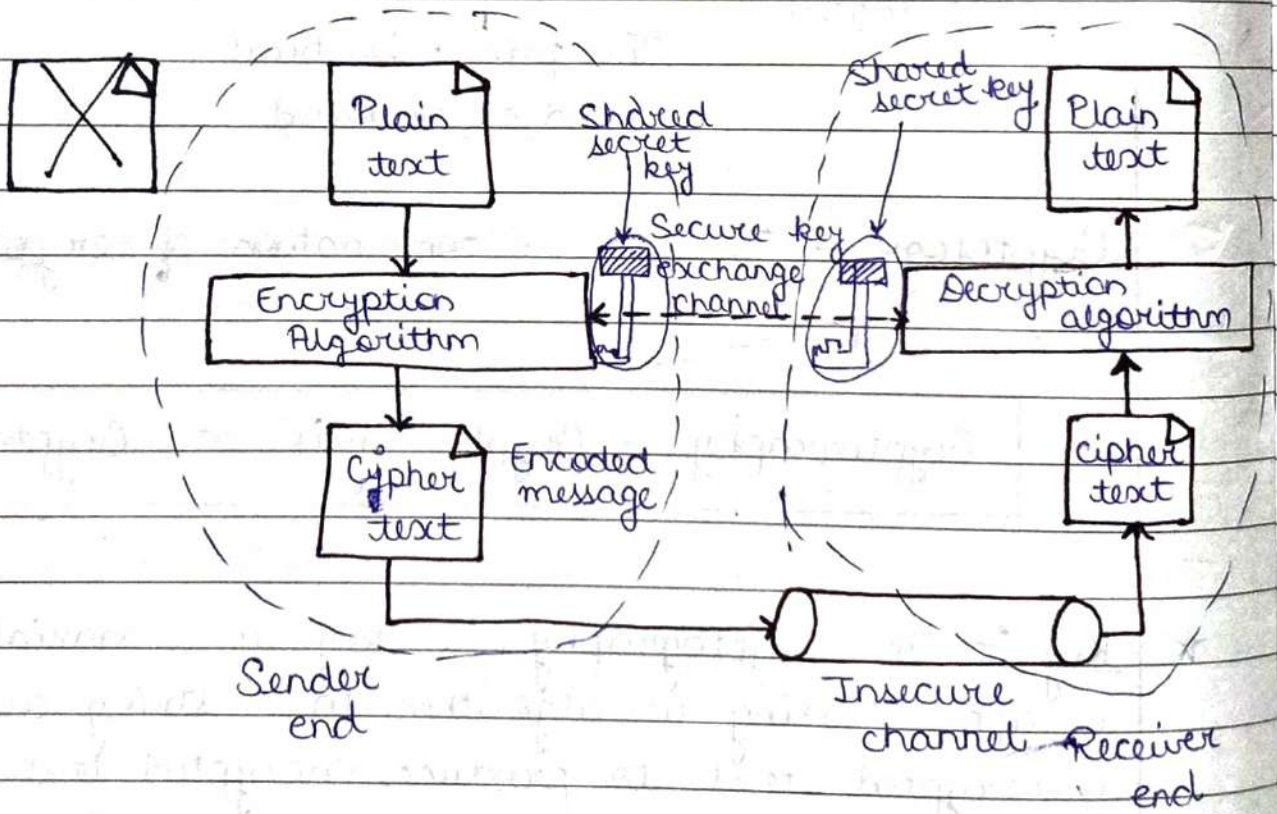
1. Symmetric key
2. Asymmetric key

• Types of keys –

1- Symmetric key – Secret key encryption
2- Asymmetric key – Public key encryption

1- Symmetric key cryptography –

(i) Same key is used for encryption and decryption.
(ii) It is very fast.
(iii) Key exchange is a big problem.
(iv) It is also called secret key encryption.
(v) The sender and receive must share the algorithm and the key.
(vi) Size of the resulting encrypted text is usually same as or less than the original clear text size.
(vii) It cannot be used for digital signatures.



2- Asymmetric key cryptography –

(i) One key for encryption and other key for decryption are used.

(ii) It is slower than symmetric key encryption.
(iii) Key exchange is not a problem.
(iv) One of the two keys must be kept secret.
(v) The sender and the receiver must each have one of the matched pair of keys.
(vi) Size of the resulting encrypted text is more than original clear text size.
(vii) It can be used for digital signature.

★ **Public Key Encryption / Public key Cryptography :-**

→ It is also called assymmetric key encryption. It uses two keys - public key and private key.

→ Public key of a user is used to encrypt message. Public key is also known as encryption key.

→ Private key of the receiver is used to decrypt the message. Private key is also called decryption key.

→ It is asymmetric because those who encrypt the message or verify signatures cannot decrypt messages or create signatures.

→ A message can be encrypted with the public key and decrypted by the private key, to provide security.

→ Each system generates a pair of keys. Each system publishes its public key and keeps its private key as secret. The keys are generated in such a way that it is impossible to derive the private key from the public key.

→ The private key is kept secret and it not sent over the message to the receiver, although the public key is.

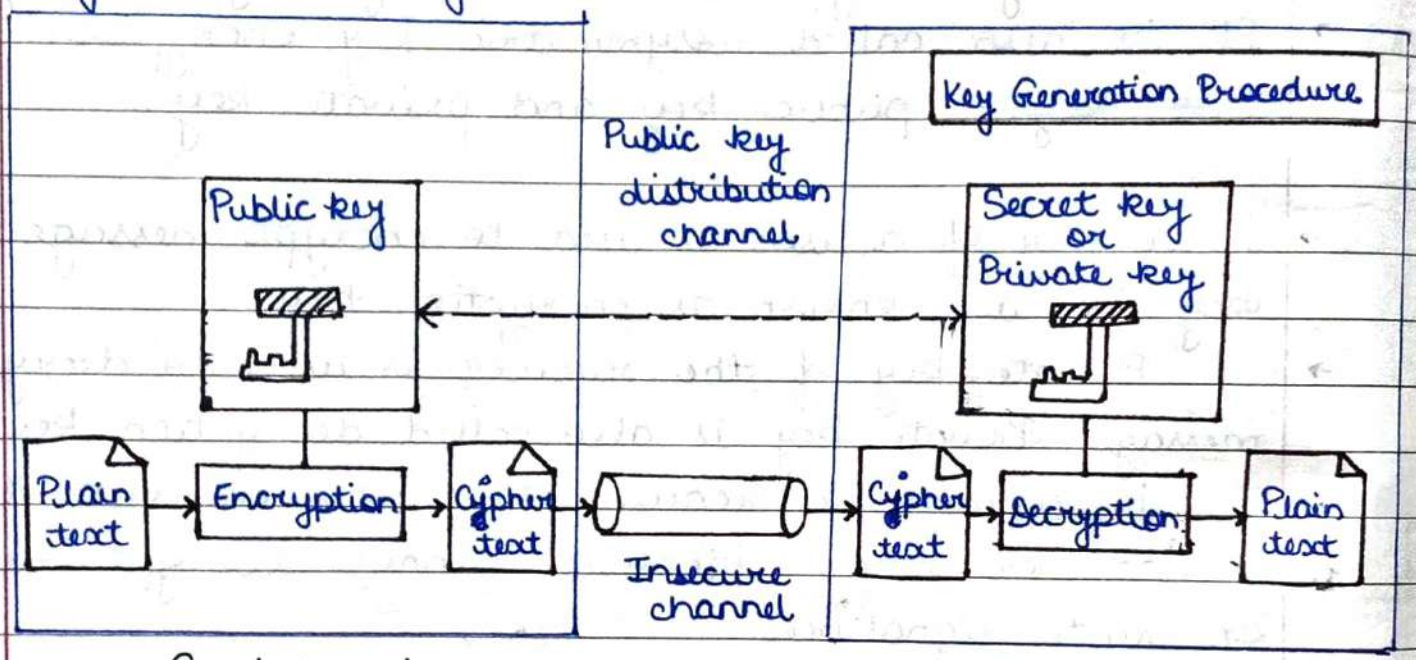
8 → Public key encryption is also used for authentication.

Advantages –

1- It provides strong security, because of two keys are used.
2- They can provide a method for digital signature.
3- There is no need for exchange keys, so it reduces key distribution problem.

Disadvantages –

1- Encryption and decryption takes long time.
2- Not suitable for long messages.
3- Key size is larger.



2- Discuss the role of digital signature in modern communication. Also discuss the differences between digital certificates and digital signatures in authentication.

★ Digital signature and authentication :-

- Digital signature is same as a person's signature on a document. A digital signature on a message is required for the authentication and identification of right sender.
- Digital signature supposed to be unique to an individual and serves as a means of identification of the sender.
- Any public key cipher can be used for digital

signature. Digital signature standard (DSS) is a digital signature format that has been standardized by NIST (National Institute of Standards and Technology) a unit of US commerce department.

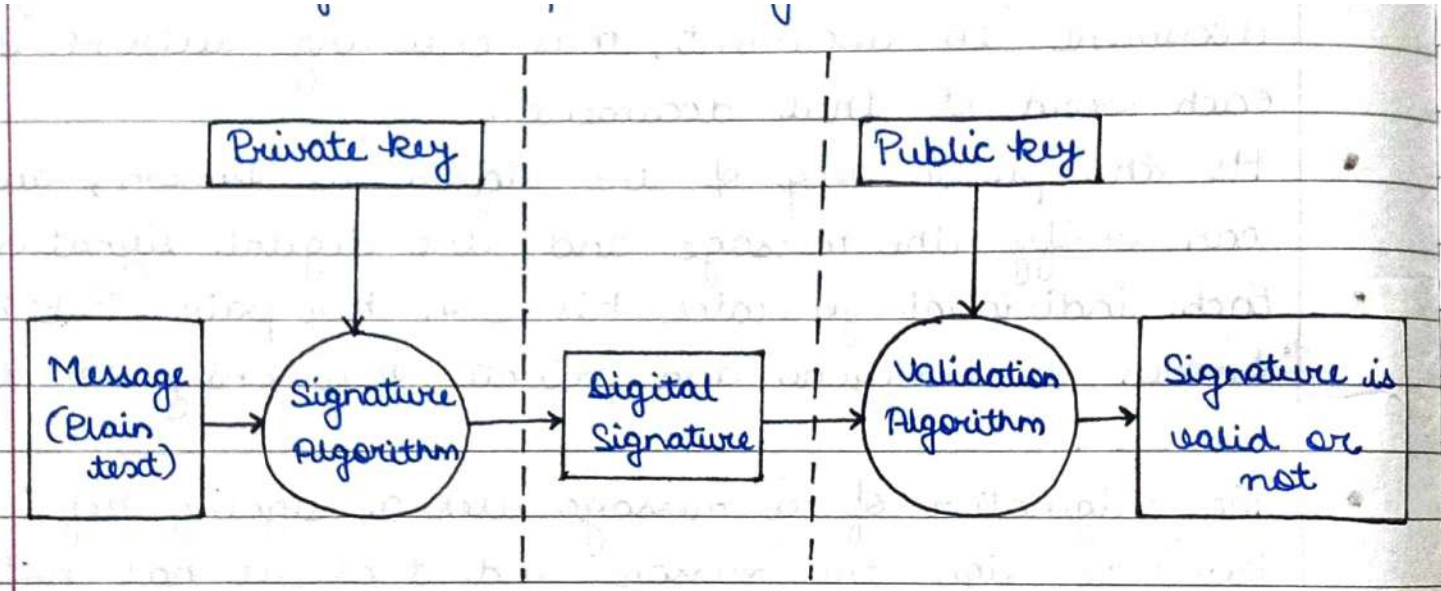
- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-document.
- Digital signature of a person therefore varies from document to document, thus ensuring authenticity of each word of that document.
- As the public key of the signer is known, anybody can verify the message and the digital signature.
- Each individual generates his own key-pair. Public key is known to everyone and private key only to the owner.
- The originator of a message uses a signing key (private key) to sign the message and that it has not been tempered with while in transmit.
- Digital signatures uses three algorithm -

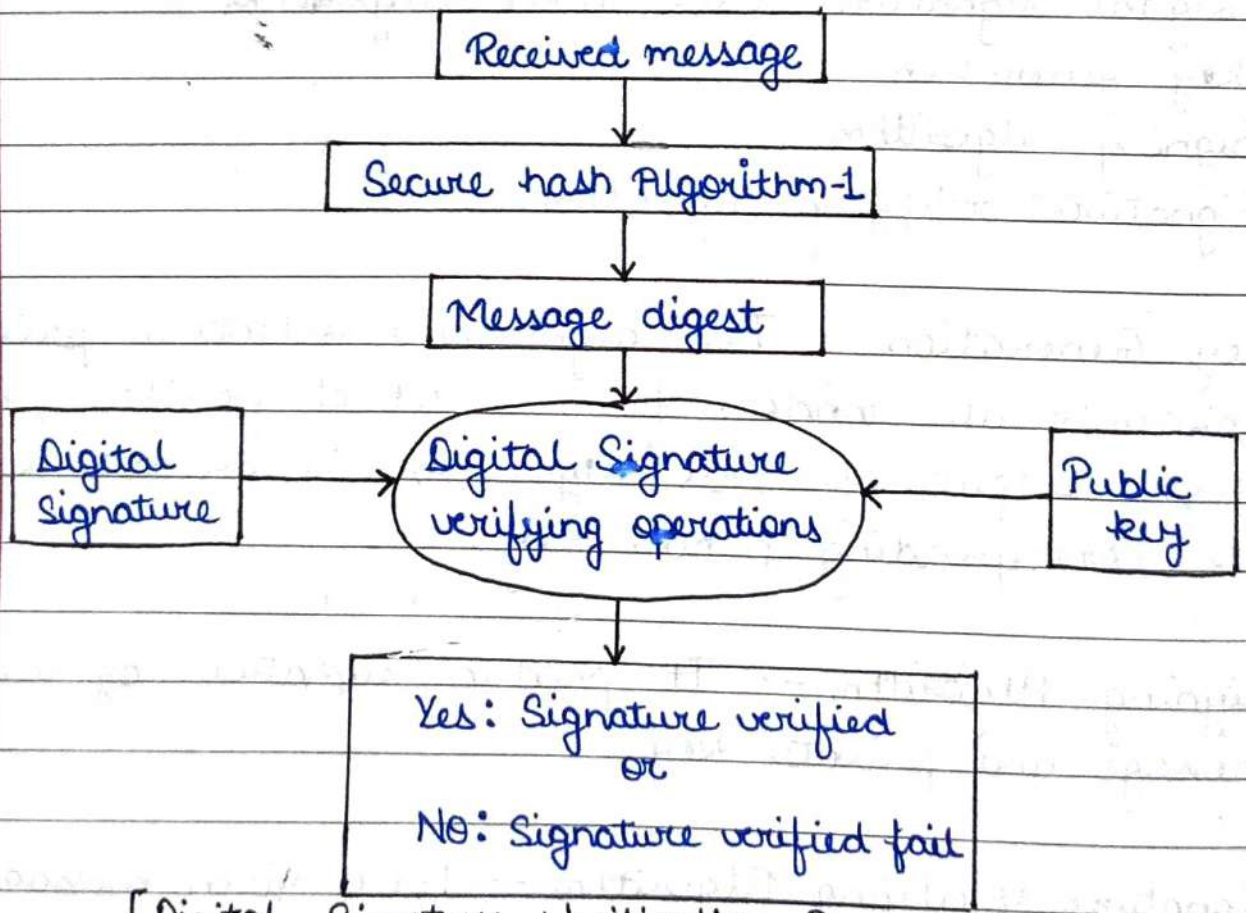
1. Key generation
2. Signing algorithm
3. Signature verifying algorithm

1- Key Generation — This algorithms selects a private key uniformly at random from a set of possible private keys. Output of this algorithm is private key and its corresponding public key.

2- Signing Algorithm — It produce signature by using message and private key.

3- Signature Verifying Algorithm — For a given message,



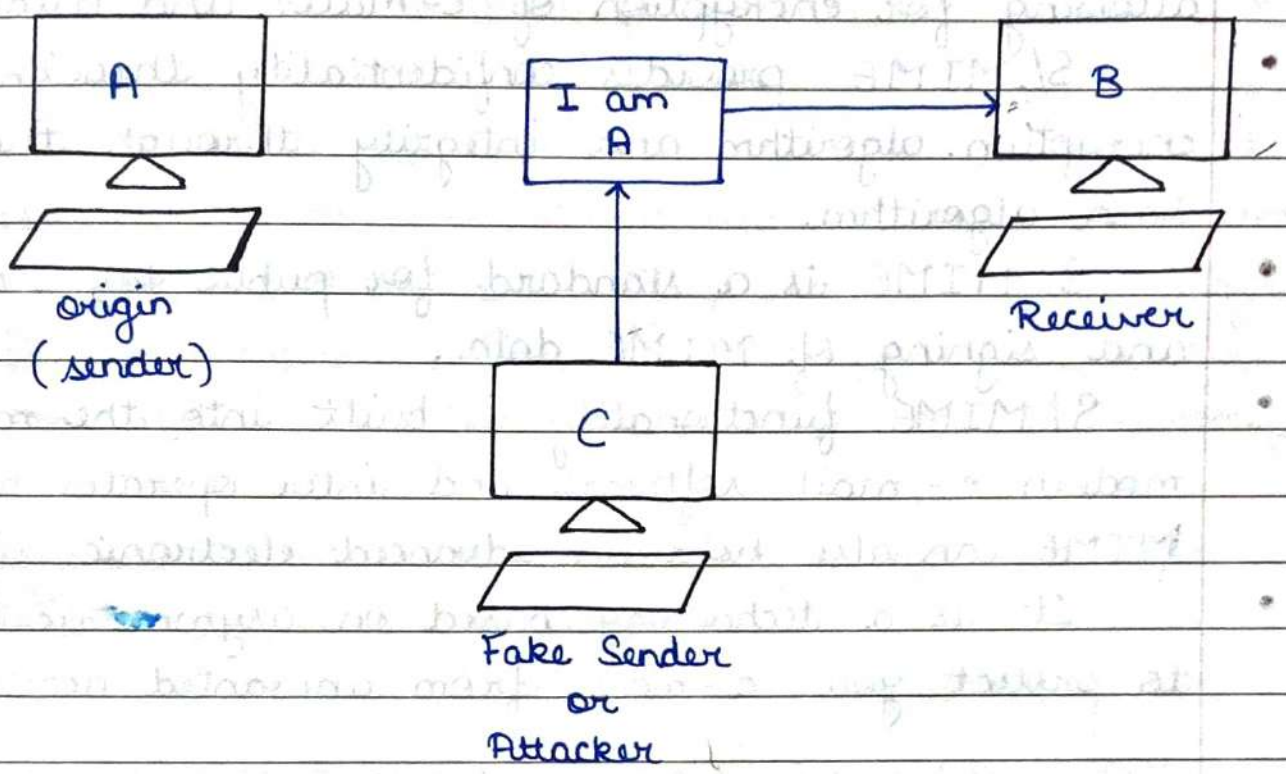


[Digital Signature Verification Process]

today for safe business - transaction online.

Authentication - Authentication helps in proof of identities. It ensures that the origin (sender) of an electronic message or document is correctly identified.
For example:

In absence of Authentication



* MIME (Multipurpose Internet Mail Extension):-
This is a technical specification indicating how multi-media data and e-mail attachments are to be transfered.

Internet has e-mail standards that dictate how a mail is to be formatted, encapsulated, transmitted and opened.

If a message or document contains a multimedia attachments, MIME dictates how that portion of the message should be handled.

★ S/MIME (Secure Multipurpose Internet Mail Extension):-

- It is a standard for encryption and digitally signing e-mails that contains attachments and providing secure data transmission.
- S/MIME extends the MIME standard by allowing for encryption of e-mails and attachments.
- S/MIME provides confidentiality through the user's encryption algorithm and integrity through the user's hash algorithm.
- S/MIME is a standard for public key encryption and signing of MIME data.
- S/MIME functionality is built into the majority of modern e-mail software and inter operates between them. MIME can also hold an advanced electronic signature.
- It is a technology based on asymmetric cryptography to protect your e-mails from unwanted access.

★ Authentication Application : Kerberos :-

- Kerberos provides a centralised authentication server whose function is to authenticate users to servers and servers to users.
- Kerberos relies exclusively on conventional encryption, making no use of public key encryption. The following are the requirements of kerberos -

Secure

1- Secure - A network eaves-dropper should not be able to obtain the necessary information to impersonate a user. More generally kerberos should be strong enough that a potential opponent does not find it to be the weak line.

2- Reliable — For all services that relie on kerberos for access control, lack of availability of the kerberos service means lack of availability of the supported services. Hence, kerberos should be highly reliable and should employ a distributed server architecture with one system able to backup another.

3- Transparent, 4- Scalable

- Kerberos is a network authentication protocol. It is designed to provide strong authentication for client-server applications by using secret key cryptography. A free implementation of this protocol is available from the MIT (Massachusettes Institute of Technology).

- Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice-versa), across insecure internet connection.

- Kerberos is freely available from MIT under copyright permission very similar those used for the BSD operating system.

Kerberos works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one-another in a secure manner. It provides mutual authentication — both the user and the server verify each other's identity.

Kerberos uses UDP port 88 by default.

★ X.509 :- In cryptography, X.509 is a standard which is used to define the format of public key certificates. X.509 certificates are used in many internet protocols such as - https.

- It is also used in digital signatures.
- An X.509 certificate contains a public key and an identity (a host name, or an organisation or an individual) and is either signed by a certificate authority or self-signed.
- X.509 is defined by ITU-T (International Telecommunication Union's) Standardisation sector.
- X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

★ Directory Authentication Service :-

- It is an external authentication directory service (also called an enterprise directory or authentication login domain) to provide a single sign-on for group of users instead of maintaining individual local login accounts.
- Each user in a group is assigned the same role (for example - infrastructure administrator). An example of an authentication directory service is a corporate directory that uses LDAP (Light-weight Directory Access Protocol).
- After the directory service is configured, any user in the group can log into the application or appliance. On the login windor the user -

→ Enters their user-name (CN, common name attribute)
→ Enter their password.
→ Selects the authentication directory service. This box appears only if you have added an authentication directory service to the appliance.

When you add an authentication directory service to the appliance, you provide such criteria so that the appliance can find the group by its DN (Distinguished Name)

★ Pretty Good Privacy (PGP) :-

It is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting, decrypting e-mails to increase the security of e-mail communications.

PGP is a popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files.

PGP is based on public key method, which uses two keys - one is a public key that you disseminate to anyone from whom you want to receive a message. The other key is a private key which is used to decrypt messages.

PGP consist five services -

1- Authentication
2- Compression
3- Confidentiality
4- Email compatibility
5- Segmentation

1- Authentication — A hash code of message is created. using SHA-1. This message digest is encrypted using RSA with a sender's private key. and included with the message.

2- Compression — As a default PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for email transmission and for file storage.

3- Confidentiality — Message is encrypted using IDEA or 3DES with a one-time session key generated by the sender. The sender key is encrypted using diffiehellman or RSA with a recepient's public key and included with the message.

4- Email compatibility — Email systems only permit the use of blocks consisting of ASCII text. To accomodate this restriction PGP provides the service converting the raw it with binary stream to a stream or printable ASCII characters.

Following

5- Segmentation — To accomodate maximum message size limitations, PGP performs segmentation and re-assembly. PGP documentation often uses the term secret keys do refer to a key-paired with a public key encryption scheme.

UNIT – 3

IP Security and Architecture

Page No : 5 | Mar | 2020

- **IP Security :-**

IP Security is a capability which provides security mechanisms that include secure datagram authentication and encryption mechanisms within IP. It can be added to current versions of Internet Protocol (IPv4 or IPv6) by means of additional headers. IP security encompasses three functional areas –
Authentication, confidentiality and key management.

The principle feature of IP security that enables it to support these varied application is that it can encrypt or authenticate all traffic at the IP level. When IP security is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
IPSec is a set of protocols to support secure exchange of packets at IP layer.

- **Applications of IP Security :-**

It provides the capability to secure communications across a LAN, across private and public WAN and across the internet. Some important applications are as follows –

(a) **Secure branch office connectivity over the internet** – A company can build a secure virtual private network over a public WAN.

(b) Secure remote access over the internet – An end user whose system is equipped with IP security protocols can make a local call to an internet service provider (ISP)

c) Establishing extranet and intranet connectivity with partners

IP security can be used to secure communication with other organisations, ensuring authentication and confidentiality and providing key exchange mechanism.

(d) Enhancing electronic-commerce security — Even though some web and e-commerce applications have built-in security protocols. The use of IP security enhances that security.

★ IP Security Architecture :- IP sec architecture uses 2 protocols - ESP, AH to secure the traffic or data flow.
The IP security specification consist of numerous documents. The most important of these issued in November of 1998 are RFCs 2401, 2402, 2408. The documents are divided into seven groups -

1. Architecture
2. Encapsulating security payload (ESP)
3. Header (Authentication header) (AH)
4. Encryption algorithm
5. Authentication algorithm
6. Key management
7. Domain of interpretation

1- Architecture — It covers the general concepts, security requirements, definitions and mechanisms defining IP security technology.

2- Encapsulating security payload (ESP) — It covers the packet format & general issues related to the use of the the encapsulating security payload for packet encryption and optionally authentication.

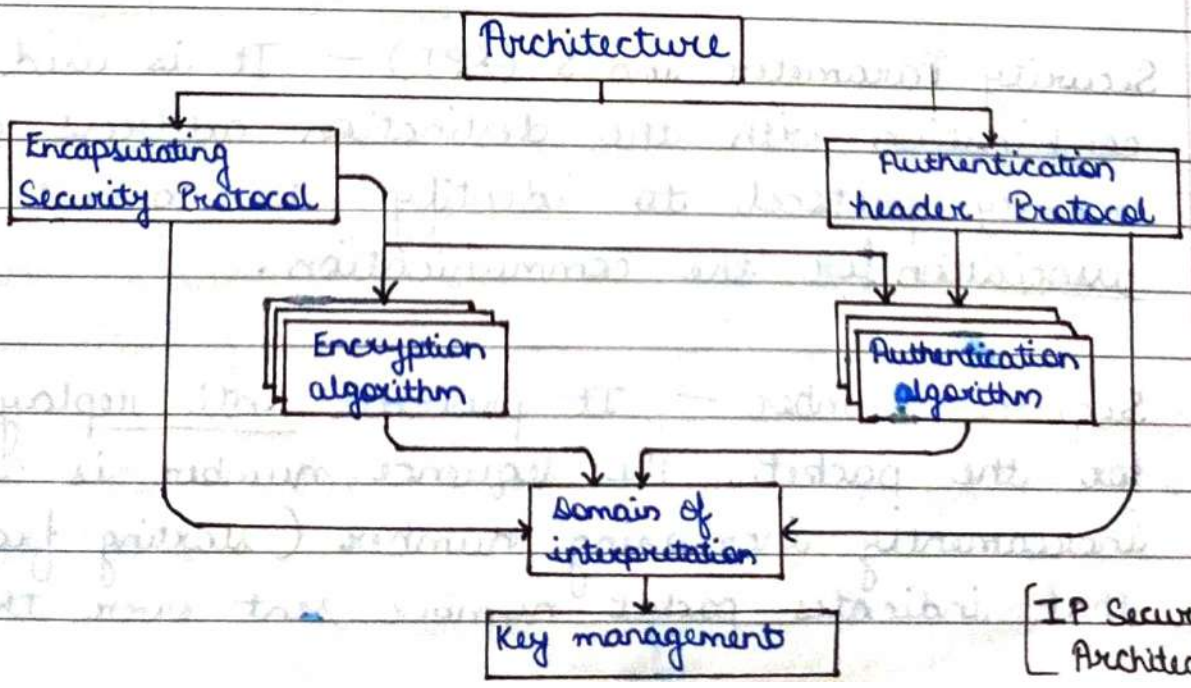
3- Authentication header (AH) — It covers the packet format of general issues related to the use of authentication header (AH) for packet authentication and integrity.

4- Encryption algorithm — A set of documents that describes how various encryption algorithms are used for encapsulating security payload (ESP).

5- Authentication algorithm — A set of documents that describes how various authentication algorithms are used for authentication header (AH) and for the authentication option of encapsulating security payload.

6- Key management — Key management contains the Documents that describe key management schemes and describes how the keys are exchanged between sender and receiver.

7- Domain of interpretation — It contains value needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms as well as operational parameters such as key lifetime. DOI is the identifier which supports both ESP and AH protocols.



[IP Security Architecture]

★ Authentication header :-

It provides authentication, integrity & and anti-replay protection for the entire packet (Both the IP header and the data payload carried in the packet).

It doesn't provide confidentiality, which means that it doesn't encrypt the data. The data is readable but protected from modification.

It contains following fields -

1. Next header
2. Length
3. Sequence number
4. Authentication data
5. Security parameter index (SPI)

★ ~~Encapsulation Security Payload~~

1. Next header - It identifies the IP payload by using the IP protocol ID.

2. Length - It indicates length of AH header.

3. Security Parameter index (SPI) - It is used in combination with the destination address and the security protocol to identify the correct security association for the communication.

4. Sequence number - It provides anti-replay protection for the packet. The sequence number is a 32-bit, incrementally increasing number (starting from 1) that indicates packet number sent over the security

association for the communication.

5- Authentication data — It contains the integrity check value (ICV), also known as the message authentication code, which is used to verify both message authentication and integrity. The receiver calculates the ICV values and checks it against this value (which is calculated by the sender) to verify integrity.

★ Encapsulating Security Payload (ESP) :-
ESP provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.

ESP can also provide an authentication service. ESP contains following feilds -

1. Security parameter index (32-bits)
2. Sequence number (32-bit)
3. Payload data (variable)
4. Padding (0-255 bytes)
5. Pad length (8-bit)
6. Next header (8-bit)
7. Authentication data

1- Security parameter index (32-bit) — It identifies a security association for the communication when used in combination with the destination address and the security protocol.

2- Sequence number (32-bit) — It provides anti-replay function.

3- Payload data — This is a transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.

4- Padding (0–255 bytes) — The purpose of this field is to make message of fixed length.

5- Pad length — It indicates the number of pad bytes immediately preceding this field.

6- Next header — It identifies the type of data contained in the payload data field by identifying the first header in that payload.

7- Authentication data — It is a variable length field that contains ICV value (Integrity Check Value) computed over the encapsulating security payload (ESP) packet (—) the authentication data field.

★ Security association —

It is a key concept that appears in both the authentication and confidentiality mechanisms for IP.

An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.

A security association is uniquely identified by three parameters -

(a) Security parameter index
(b) IP destination address
(c) Security protocol identifier

Following are the parameters for defining security associations -

1- **Sequence number counter** — It is a 32-bit value to generate the sequence number field in authentication header(AH) or encapsulating security payload (ESP) header.

2- Sequence counter flow — It is a flag indicating overflow of the sequence counter.

3- Anti-replay window — It is used to determine replay attack.

4- Authentication header information — It includes authentication algorithms, keys or key lifetimes.

5- Encapsulating security payload information — It contains encryption and authentication algorithm, keys, initial values, key lifetimes and other related parameters.

6- Duration — It contains lifetime of security association.

7- IP security protocol mode — It is also called tunnel mode

8- Path — Any observed path maximum transmission unit (MTU).

* Security association bundle :-
It refers to a sequence of security associations through which traffic must be processed to provide a desired set of IP security services.

- **Combined Security Associations :-**

Security associations may be combined into bundles in two ways -

1. Transport adjacency
2. Iterated tunneling

1. Transport adjacency — It refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining authentication header (AH) and ESP allows for only one level of combination.

2. Iterated tunneling — It refers to the application of multiple layer of security protocols affected through IP tunneling. This approach allows for multiple level of nesting, since each tunnel can originate or terminate at a different IP security site along the path.

Imp. Key-

★ **Management :-**

The key management portion of IP Security involves the determination and distribution of secret keys.

A typical requirement is four keys for communication between two applications — transmit and receive pairs for AH and ESP.

IP security architecture document mandates support for two types of key management -

1. Manual
2. Automated

1. Manual – A system administrator manualy configure each system with its own keys and with the keys of other communication systems. This is practical for small and static environment.

2. Automated – An automated system enables the on demand creation of keys and facilitates the use of keys in a large distribution system with an involving configuration.

The default automated key management protocol for IP security is refered to as ISAKMP/Oakley.

- Features of Oakley –

1- It employs a mechanism known as cookies to transfer/thwart clogging attacks.
2- It enables the two parties to negotiate a group, this in essence, specifies the global parameters of the diffie Hellman key exchange.
3- It uses nonces to ensure against replay attacks.
4- It enables the exchange of Diffie Hellman public key values.
5- It authenticates the Diffie Hellman exchange to thwart man-in-middle attack.

- ISAKMP — (Internet Security Association and Key Management Protocol)

An ISAKMP message has a fixed header format. This format has following fields –

1. **Initiater cookie (64-bit)** – It is a cookie of entity that initiated security association establishment, security association notification or security association deletion

2- Responder cookie (64-bit) — It is a cookie of responding entity, null in first message from initiater.

3- Next Payload (8 bit) — It indicates the type of first payload in the message.

4- Major version (4 bit) — It indicates major version of internet security association and key management protocol (ISAKMP).

5- Exchange type (8 bit) — It indicates type of exchange

6- Flag (8 bit) — It refers to bit of information.

7- Message Id (32 bit) —

UNIT – 4

Web Security

* **Web Security :-** Web security is a branch of computer security specifically related to the internet often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

* **Web Security Threats :-**

- Web security threats are that type of security threats which faced when using the web. One way to group these threats is in terms of passive and active attacks.
- Passive attacks include eavesdropping (to listen secretly) on network traffic between browser and server and gaining access to information on a website that is supposed to be restricted.
- Active attacks include impersonating another user altering messages in transmit between client and server and altering information on a website.
- Another way to classify web security threats is in terms of the threats, web server, web browser and network traffic between browser and server. Issues of server and browser security fall into the category of computer system security.

- Possible web security threats and their consequences. counter measures are as follows –

Page No :

	Threats	Consequences	Counter measure
Integrity	(a) Modification of user data. (b) Trojan horse browser (c) Modification of memory (d) Modification of message traffic transmit.	Loss of info Compromise of machine Vulnerability to all other threats	Cryptographic checksums
Confidentiality	(a) Eavesdropping on the net. (b) Theft of information from server. (c) Theft of data from client. (d) Information about network configuration. (e) Information about which client talks to server	Loss of info Loss of privacy	Encryption, web proxies
Denial of Service	(a) Killing of user threats (b) Flooding machine with bogus threats (c) Filling up disk or memory. (d) Isolating machine by DNS attacks.	Disruptive Annoying Prevent user from getting work done.	Difficult to prevent.

Page No :

Authentication	(a) Impersonation of legitimate users. (b) Data forgery	Misrepresentation of users. Belief that false information is valid.	Cryptographic techniques

* Secure Socket Layer (SSL) :-

SSL is the standard security technology for establishing an encrypted link between a web server and browser. This link ensures that all data passed between the web server and browsers remain private and integral.

- SSL Architecture :-

→ SSL is designed to make use of TCP to provide a reliable end to end ~~and~~ security services.

→ SSL is not a single protocol but rather two layers of protocols, as illustrated in figure.

→ The "SSL record protocol" provides basic security services to various higher-layer protocols.

→ In particular, the HTTP, which provides the transfer service for web client / server interaction, can operate on top of SSL.

→ Three higher-layer protocols can defined as part of SSL, the handshake protocol, the change cipher spec protocol and the alert protocol.

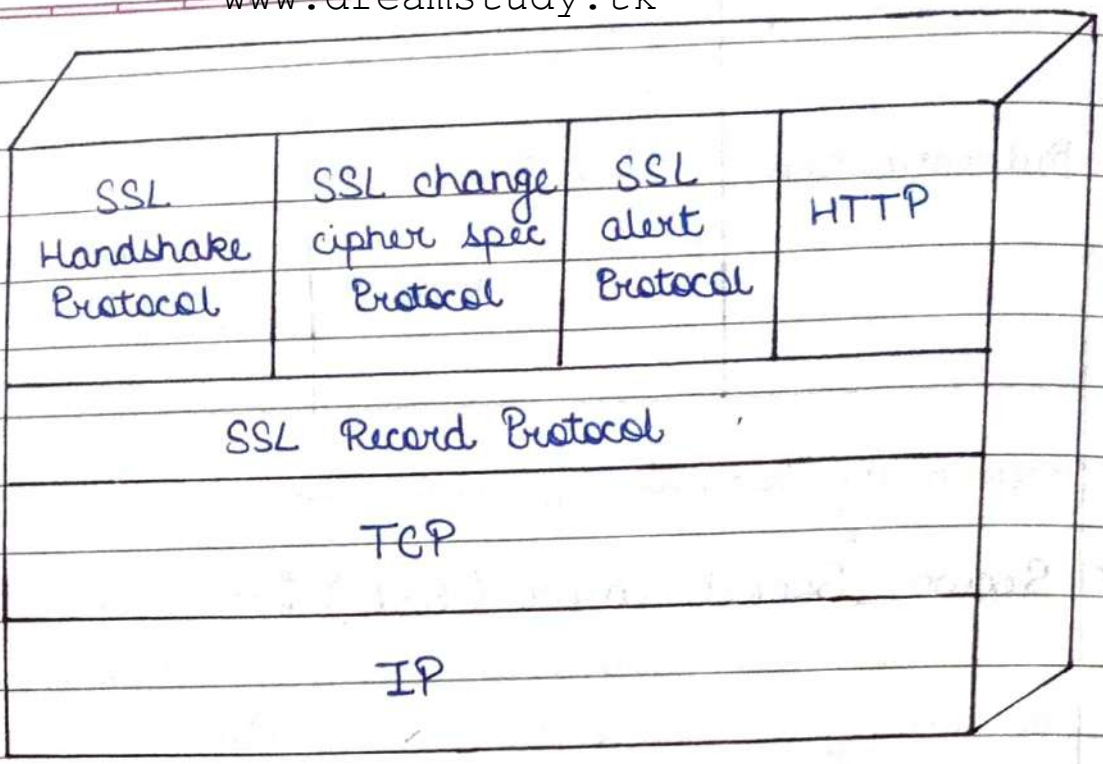


fig :- SSL Protocol Stack

- **SSL Session State :-**

→ SSL session is an association between a client and a server.

→ Sessions are created by the handshake protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections.

→ The session state is defined by the following parameters-

1- Session Identifier — An arbitrary type sequence chosen by the server to identify an active or resumable session state.

2- Peer Certificate — An X.509 v3 certificate of the peer. This element of the state may be null.

3- Compression method — The algorithm used to compress data prior to encryption.

4- Cipher spec — Specifies the bulk data encryption algorithm (such as null) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as hash- size.

5- Master secret — 48 byte secret shared between the client & server.

6- Is resumable — A flag indicating whether the session can be used to initiate new connections.

* SSL Connection State :-

→ A connection is a transport (in the OSI layer model definition) that provides a suitable type of service.

→ This is a logical client / server link, associated with the provision of a suitable type of service. In SSL, it must be a peer to peer connection with two network nodes.

→ A connection state is defined by the following parameters-

1- Server and client random — Byte sequence that are chosen by server and client for each connection.

2- Server write MAC secret — The secret key used in MAC operations on data sent by the server.

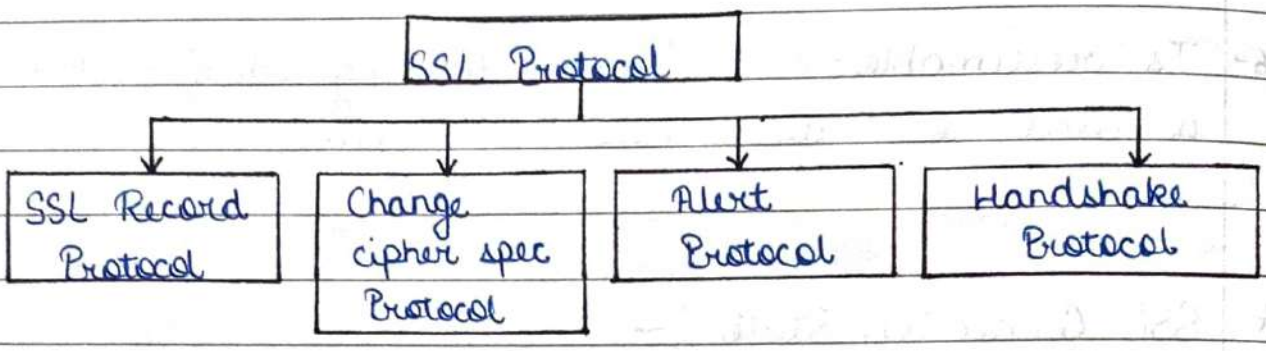
3- Client write MAC secret — The secret key used in MAC operations on data sent by the client.

4- Server write key — The conventional encryption key for data encrypted by the server and decrypted by the client.

5- Client write key — The conventional encryption key for data encrypted by the client and decrypted by the server.

★ SSL Protocols :-

There are four protocols used in SSL.

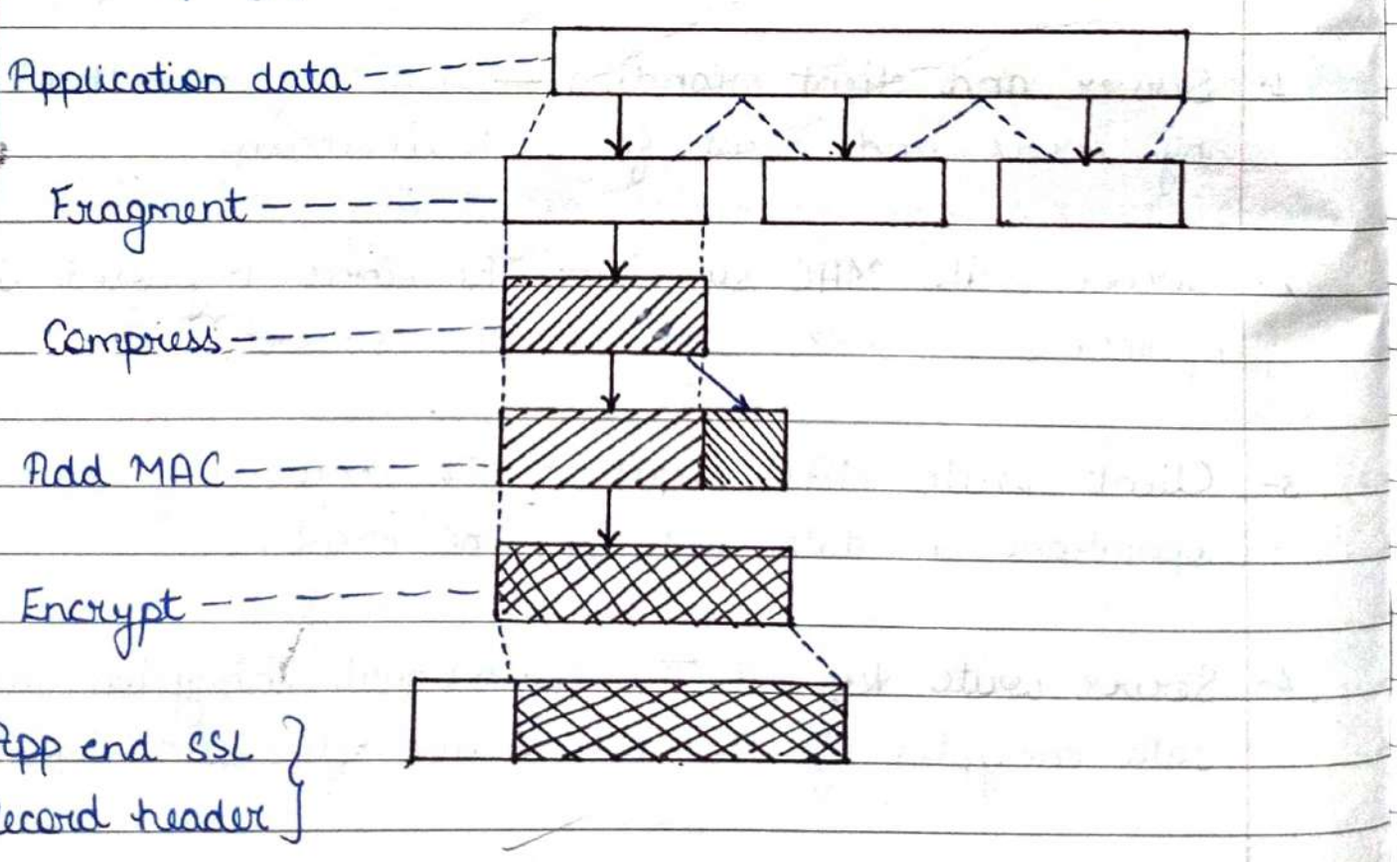


1. SSL Record Protocol :-

It provides two services for SSL connection —

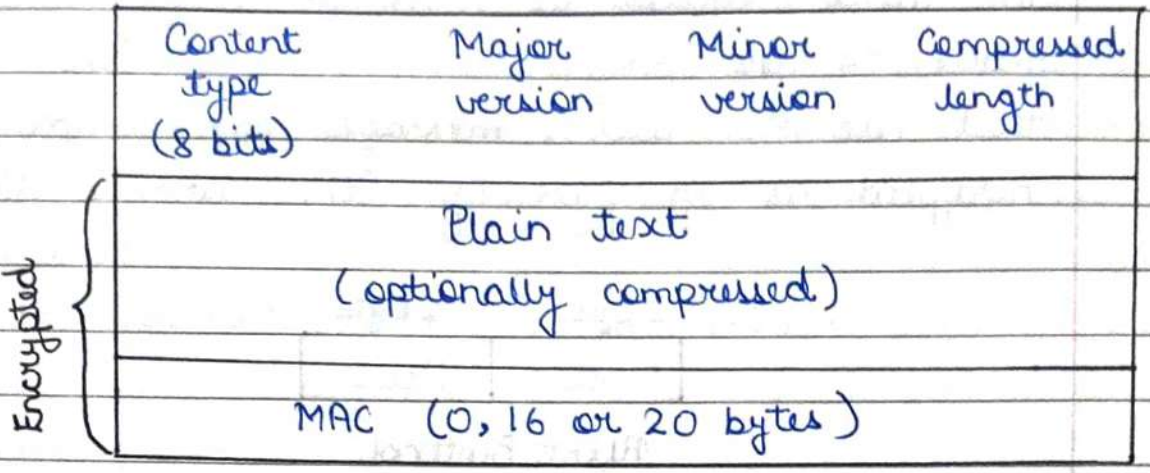
1- Confidentiality
2- Message Integrity

Following figure shows SSL Record Protocol operation —



Page No :

Following is SSL record format –



2- SSL change cipher spec protocol :-

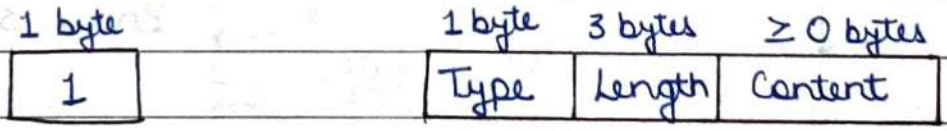
→ The change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the just negotiated cipher spec and keys.

→ There are two states for the change cipher spec message –

(a) Read current

(b) Read pending

→ The sole purpose of this message is to cause the pending state to be copied into the current state.



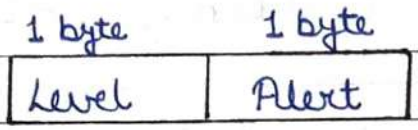
(a) change cipher spec protocol

(b) Handshake Protocol

→ This change cipher spec message is normally sent at the end of the SSL handshake.

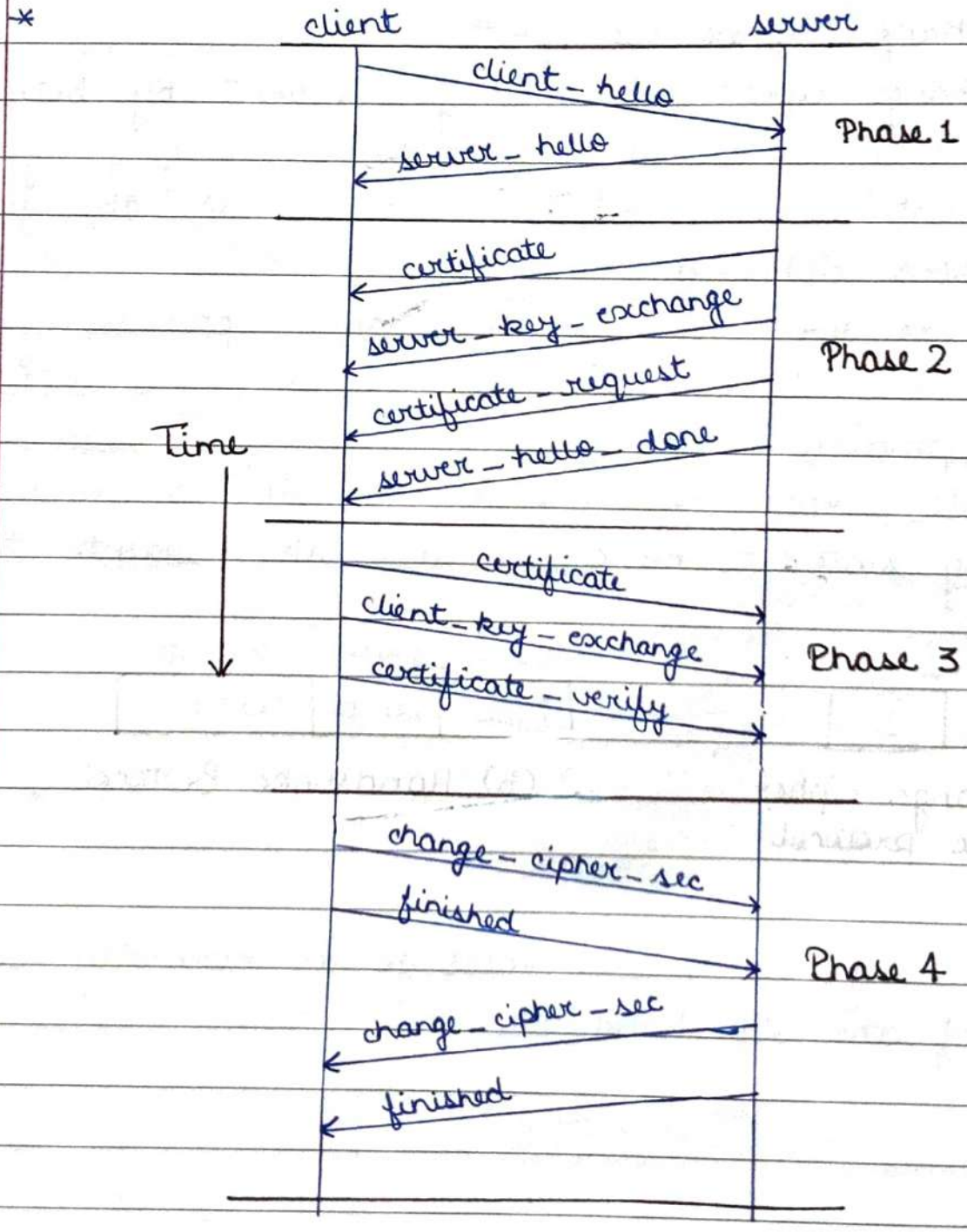
3. SSL Alert Protocol :-

The alert protocol is used to convey SSL related alerts to the peer entity. As with other applications that use SSL alert messages are compressed and encrypted as specified by the current state.



Alert Protocol

4. SSL Handshake Protocol :-



→ Handshake protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in a SSL record. Handshake protocol is used before any application data is transmitted.

→ Handshake protocol action is as follows —

★ Transport Layer Security (TLS) :-

1 → TLS is a protocol that provides communication security between client / server applications that communicate with each other over the internet.

2 → It enables privacy, integrity and protection for the data that's transmitted between different nodes on the internet.

3 → TLS primarily enables secure web browsing, applications access, data transfer and most internet based communication.

4 → It prevents the transmitted / transported data from being eavesdropped or tempered.

5 → TLS is used to secure web browsers, web servers, VPNs, database servers and more.

6 → TLS protocols consist of two different layers of sub-protocols :

(a) TLS Record Protocol

(b) TLS Handshake Protocol

(a) TLS Record Protocol ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable.

(b) TLS Handshake Protocol allows authentication between the server and client, and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

★ Secure Electronic Transactions (SET) :-

→ SET is a standard that will enable secure credit card transactions on the internet.

→ SET has been endorsed by virtually all the major players in the electronic commerce arena, including microsoft, visa, netscape and mastercard.

→ SET provides three services :

(a) It provides a secure communication channel among all parties involved in a transaction.

(b) It provides trust by the use of X.509 v3 digital certificate.

(c) It ensures privacy because the information is only available to parties in a transaction when and where necessary.

→ SET is a system for ensuring the security of financial transactions on the internet.

→ It was initially supported by mastercard, visa, microsoft, netscape and others.

→ With SET, a user is given an e-wallet (digital signature) and a transaction is conducted and verified using a combination of digital certificates and combination of digital certificates and digital signature among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and

confidentiality.

→ SET is a specification defined in three books issued in May of 1997.
Book 1 : Business description (80 Pages)
Book 2 : Programmer's guide (629 Pages)
Book 3 : Formal protocol definition (262 Pages)

→ SET is not a payment system rather is security protocols.

- Key features of SET :-

SET incorporates the following features -

1- Confidentiality of information.
2- Integrity of data.
3- Cardholder account authentication.
4- Merchant authentication.

SET overview and its Requirements :-

→ Book 1 of the SET specification lists the following business requirements for secure payment processing with credit cards over the internet and other network.

1- Provide confidentiality of payment and ordering information.
2- Ensure the integrity of all transmitted data.
3- Provide authentication that a cardholder is a legitimate user of a credit card account.
4- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.
5- Ensure the use of the best security practices and system

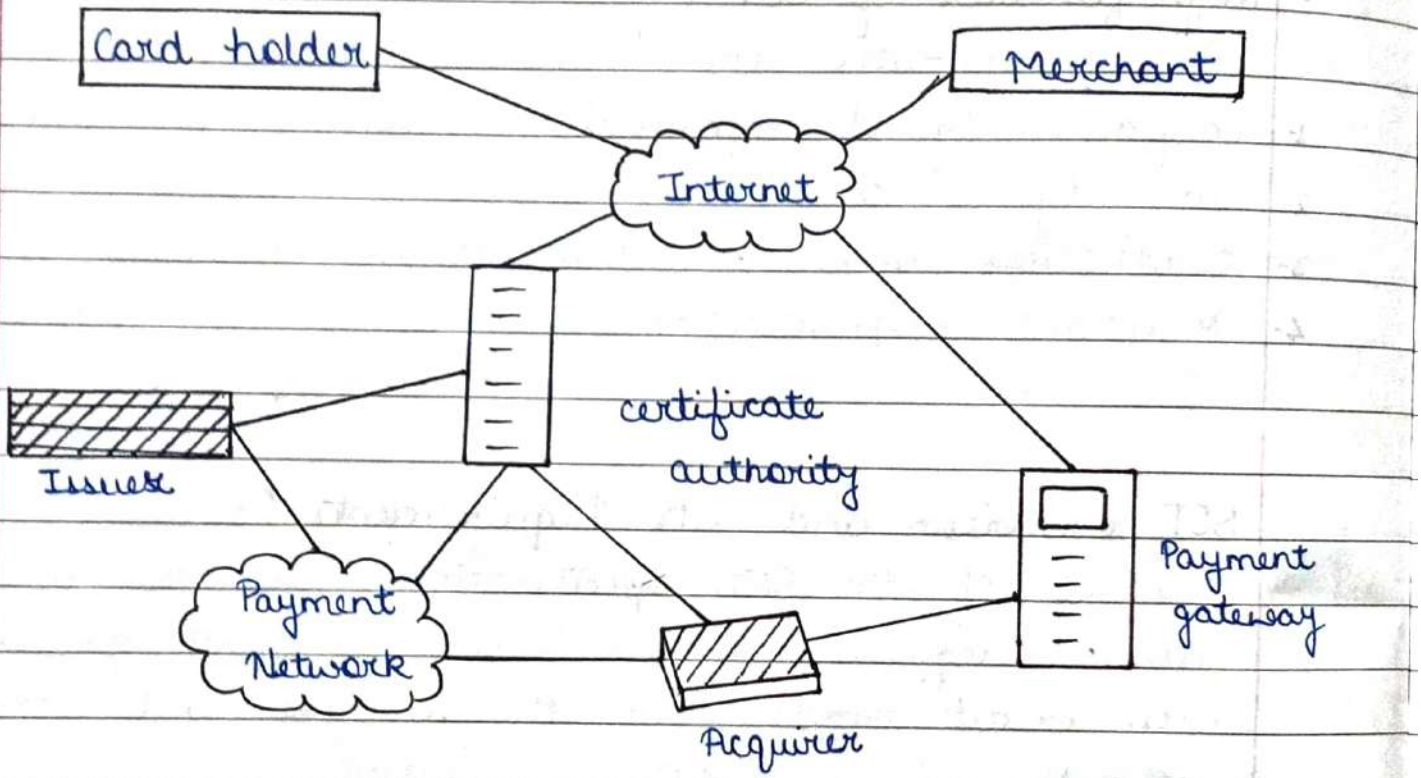
design techniques to protect all legitimate parties in an e-commerce transaction.

6- Create a protocol that neither depends on transport security mechanisms nor prevents their use.

7- Facilitate and encourage interoperability among software and network providers.

- Components of SET :-

Following figure indicates the component in SET system.



1. Card holder — In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the internet. A card holder is an authorised holder of a payment card (e.g. master card, visa) that has been issued by an issuer.

2. Merchant — A merchant is a person or organisation

that has goods or services to sell to the cardholder.

3- Payment Gateway — This is a function operated by the acquirer or a designed third party that processes merchant payment messages. It provides authorisation and payment functions.

4- Certification Authority (CA) — This is an entity that is trusted to issue X.509 v3 public key certificates for cardholders, merchants and payment gateways.

5- Issuer — This is a financial institution such as a bank, that provides the cardholder with the payment card. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder.

6- Acquirer — This is a financial institution that establishes an account with a merchant and processes payment card authorisations and payments.

Acquirer provides authorisation to the merchant and that a given card account is active and that the proposed purchase does not exceed the credit limit.

Acquirer also provides electronic transfer of payments to the merchant's account.

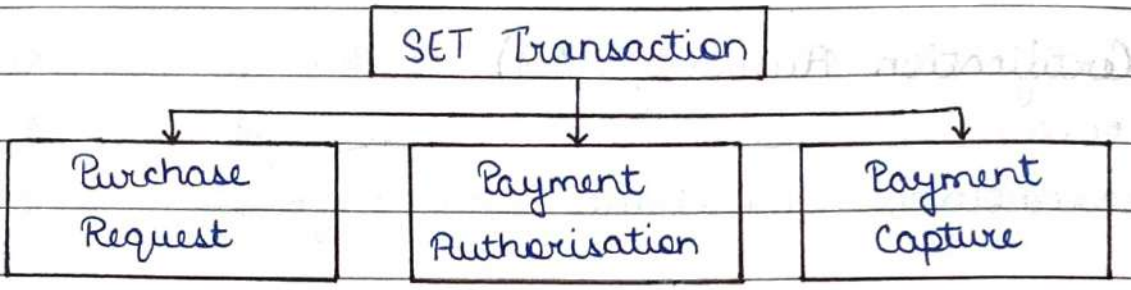
★ Dual Signature in SET :-

→ The purpose of the dual signature is to link two messages that are intended for two different recipients.

→ In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank.

→ The merchant does not need to know the customer's credit card number and the bank does not need to know the details of the customer's order.

★ SET Transaction Type :-



1- Purchase Request — Before the purchase request exchange begins, the cardholder has completed browsing, selecting and ordering. The end of this preliminary phase occurs when the merchant sends a completed order form to the customer. The purchase request exchange consists of four messages :
Initiate request , Initiate response
Purchase request , Purchase response

2- Payment Authorisation — During the processing of an order from a cardholder, the merchant authorises the transaction with the payment gateway.

The payment authorisation ensures that the transaction was approved by the issuer. The authorisation guarantees that the merchant will receive payment. The merchant can therefore provide the services or goods to the customer.

The payment authorisation exchange consist of two messages :
Authorisation request

Authorisation response
Purchase-related information
Authorisation-related information
Certificate

3- Payment Capture —

→ The merchant engages the payment gateway to obtain the payment in a payment capture transaction, consisting of a capture request and a capture response message.

→ For the capture request message, the merchant generates signs and encrypts a capture request block, which includes the payment amount and the transaction ID. The message also includes the encrypted capture token received earlier for this transaction, as well as the merchant's signature key and key-exchange key certificates.

→ When the payment gateway receives the capture request message, it decrypts and verifies the capture request block and capture token. It then creates a clearing request that is sent to the issuer over the private payment network.

→ The gateway then notifies the merchant of payment in a capture response message. The message includes a capture response block that the gateway signs and encrypts, also includes the gateway's signature key certificates.

UNIT – 5 mgmt
Computer Network Security

★ Network Management System :–

→ It is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

→ Network management system components assist with –

1. Network device directory — It is used to identifying what devices are present on a network.

2. Network device monitoring — It is used to monitoring at the device level to determine the health of network components.

3. Network performance analysis — It is tracking performance indicators such as bandwidth utilisation, packet loss, latency, availability and up time of routers, switches and other simple network management protocol (SNMP) enabled devices.

4. Intelligent notifications — It is some configurable alerts that will respond to specific network scenarios by paging, e-mailing, calling or texting a network administrator.

★ SNMP Architecture :–

→ The fullform of SNMP is "Simple Network Management Protocol."

→ In 1988, the specification for SNMP was issued and rapidly became the dominant network management standard.

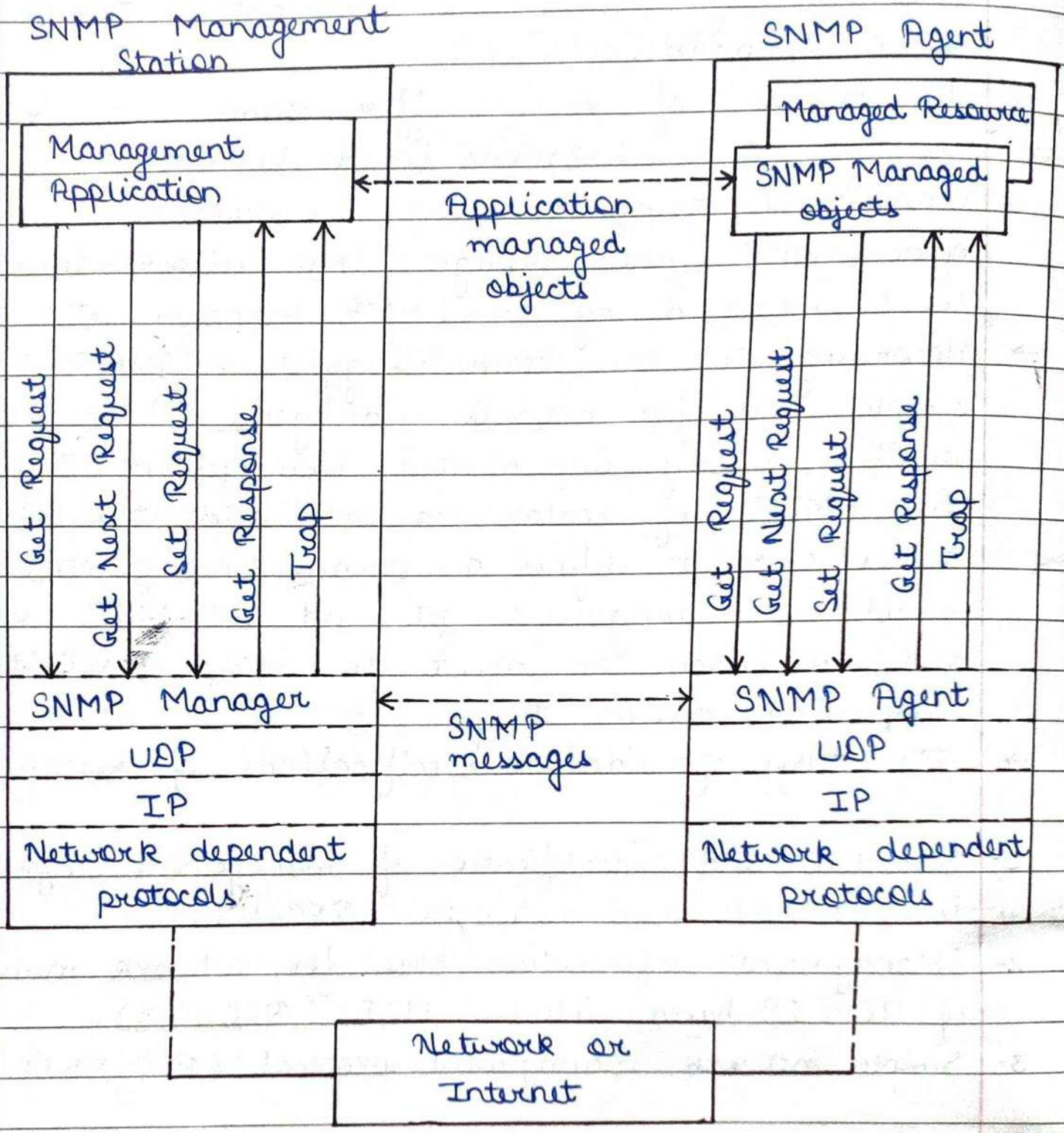
→ The number of vendors offer stand-alone network management workstations based on SNMP, most vendors of bridges, routers, workstations and PCs, offer SNMP agent packages that allow their products to be managed by an SNMP management station.

→ According to the name suggests, SNMP is a simple tool for network management. It defines a limited, easily implemented Management Information Base (MIB) of scalar variable and two dimensional tables and it defines a stream lined protocol to enable a manager to get and set MIB variables and to enable an agent to issue unsolicited notification called traps.

→ The three foundation specifications of SNMP are—

1- Structure and identification of management information for TCP/IP based networks (RFC 1155).
2- Management Information Base for network management of TCP/IP based internet MIB (RFC 1213).
3- Simple network management protocol (RFC 1157).

- SNMP Architecture Diagram —



SNMP Entity :- Each SNMP entity includes a single SNMP engine. An SNMP engine implements functions for sending and receiving messages, authenticating and encrypting / decrypting messages and controlling access to managed objects.

Page No :

★ SNMPv1 Community Facility —

→ SNMP v1, as defined in RFC 1157, provides only a very basic or simple rudimentary security facility based on the concept of community. This facility gives a certain level of security but is open to various attacks.

→ The application involves a one to many relationship between a manager and a set of agents, the manager is able to get and set objects in the agents and is able to received traps from the agents.

→ Thus, from an operational or control point of view, the manager "manages" a number of agents.

→ We also need to be able to view SNMP, network management as a one to many relationship between an agent and a set of managers.

→ Each agent controls its own local MIB and must be able to control the use of that MIB by a number of managers.

→ There are three aspects of this control —

1. Authentication service
2. Access service
3. Proxy service

1- Authentication service in SNMPv1 community facility-

→ The purpose of the SNMPv1 authentication service is to assure the recipient that an SNMPv1 message is from the source that it claims to be from.

→ SNMPv1 only provides for a trivial scheme for authentication. Every message (get or put request) from a manager to an agent includes a community name, this name functions as a password, and the message is assumed to be authentic if the sender knows

the password.

→ The community name could be used to trigger an authentication procedure, with the name functioning simply as an initial password screening device. The authentication procedure could involve the use of encryption/decryption for more secure authentication functions. This is beyond the scope of RFC 1157.

2- Access policy in SNMP — By defining a community, an agent limits access to its MIB to selected set of managers. By the use of more than one community, the agent can provide different categories of MIB access to different managers. There are two aspects to this access control —

(a) SNMP MIB view — A subset of the objects within an MIB. Different MIB views may be defined for each community.

(b) SNMP access mode — An element of the set [READ-ONLY, READ-WRITE]. An access mode is defined for each community. The combination of an MIB views and access mode is referred to as an SNMP community profile. Thus a community profile consists of a defined subset of the MIB at the agent, plus an access mode for those objects. An SNMP community profile is referred to as an SNMP access policy.

3- Proxy service in SNMP — The community concept is also useful in supporting the proxy service.

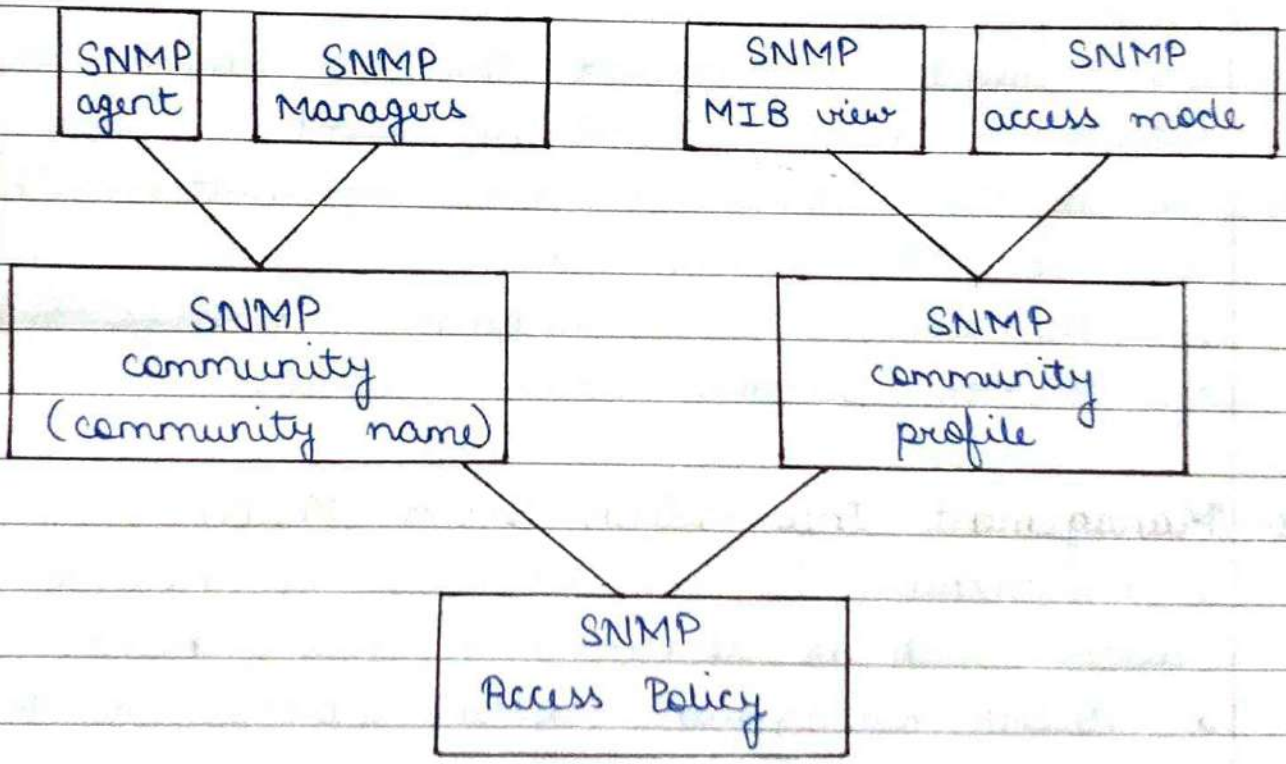
→ Proxy is an SNMP agent that acts on behalf of

other devices. Typically, the other devices are foreign. In this sense, that they do not support TCP/IP and SNMP.

→ In some cases, the proxied system may support SNMP but the proxy is used to minimize the interaction between the proxied device and network management system.

→ For each device that the proxy system represents, it maintains an SNMP access policy. Thus the proxy knows which MIB objects can be used to manage the proxied system (the MIB view) and their access mode.

Diagram of SNMPv1 administrative concepts —



Key Elements of SNMP:-

1. Management Station
2. Management Agent
3. Management information base
4. Network management protocol

1- Management Station — It is typically a stand alone device, but may be a capability implemented on a shared device. It serves as a interface for the human network manager into the network management system. It is a set of management applications for data analysis, fault recovery and so on. It is an interface by which the network may monitor and control the network.

2. Management, Managers & Agents —

→ A management stations, called a manager. It is a host that runs the SNMP client program.

→ A managed station, called an agent. It is a router (or a host) that runs the SNMP server program.

→ Management is achieved through simple interaction between a manager and an agent.

→ The agents keeps performance information in a database. The manager has access to the values in the database. The manager can also make the router perform certain actions.

3- Management Information Based (MIB) — MIB is a hierarchical virtual database of network objects (devices such as routers, switches, hubs) describing a network management system (NMS). An MIB is used by SNMP and Remote Monitoring 1 (RMON1)

4- Network Management Protocol —

→ The management station and agents are linked by a network management protocol.

→ The protocol used for the management of TCP/IP

networks is the SNMP. It involves following key capabilities.

Get – Enables the management station to retrieve the value of objects at the agent.

Set – Enables the management station to set the value of objects at the agent.

Notify – Enables an agent to notify the management station of significant events.

★ SNMPv3 :-

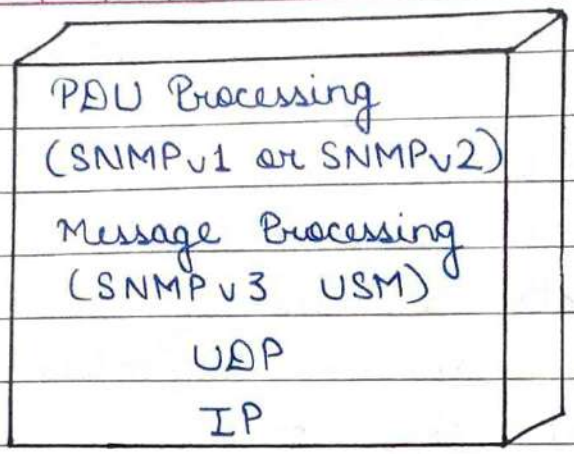
→ In 1998, the IETF, SNMPv3 working group produced a set of proposed internet standards, currently RFC, 2570 through 2576.

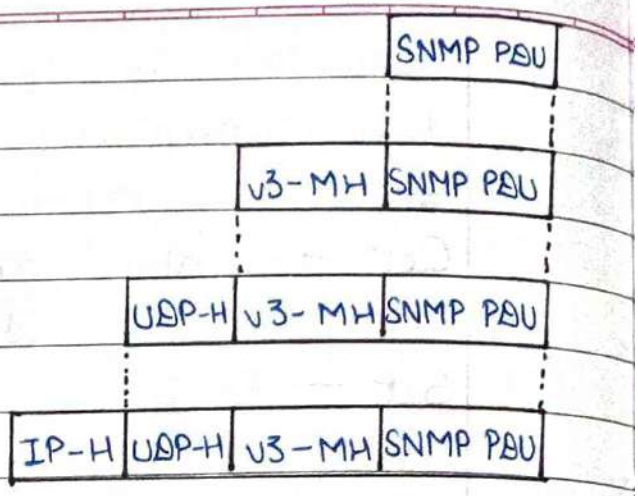
→ This documents set defines a framework for incorporating security features into an overall capabilities that includes either SNMPv1 or SNMPv2 functionality. In addition the documents define a specific set of security and access control.

→ It is important to realise that SNMPv3 is not a stand-alone replacement per SNMPv1 and/or SNMPv2. SNMPv3 defines a security capability to be used in conjunction with SNMPv2 (preferred) or SNMPv1.

→ In addition RFC 2571 describes an architecture within which all current and future version of SNMP fit.

→ RFC 2575 describes an access control facility, which is intended to operate independently of the core SNMPv3 capability.





here IP-H = IP header
UDP-H = UDP header
v3-MH = SNMPv3 message header
PDU = Protocol data unit

→ Information are exchanged between a management station and an agent in the form of SNMP message.

- SNMPv3 Terminology :-
Some SNMPv3 terms are introduced in RFC 2271. Some important SNMPv3 terms are as follows-

1- SNMP Engine ID — Unique and unambiguous identifier of an SNMP engine, as well as the SNMP entity that corresponding to that engine.

2- Context Engine ID — Uniquely identifies as SNMP entity that may realise an instance of a context with a particular context name.

3- Context Name — Identifies a particular context within an SNMP engine. It is passed as a parameter to the dispatcher and access control subsystem.

Page No :

4- Scoped PDU — A block of data consisting of a context engine ID, a context name and an SNMP PDU. It is passed as a parameter to/from the security subsystem.

5- SNMP Message Processing Model — Unique identifier of a message processing model of the message processing subsystem. Possible values include SNMPv1, SNMPv2, SNMPv3.

6- SNMP Security Model — Unique identifier of a security subsystem. Possible values include SNMPv1, SNMPv2 and USM.

7- SNMP Security Level — A level of security at which SNMP messages can be sent or with which operations are being processed, expressed in terms of whether or not authentication and/or privacy are provided. The alternative values are no authpriv, authNoPriv and auth priv.

8- Principal — The entity on whose behalf services are provided or processing takes place. A principal can be an individual acting in a particular role, a set of individuals, with each acting in a particular role, an application or set of applications and combinations thereof.

9- Security Name — A human-readable string representing a principal. It is passed as a parameter in all of the SNMP primitives (dispatcher, message processing, security, access control).

★ VACM (View Based Access Control Model) :-

→ It is an SNMPv3 mechanism regulates access to MIB objects by providing a fine-grained access control mechanism associating users with MIB views.

→ The VACM facilities are essential in ensuring a completely secure agent.

→ There are five elements defined in VACM model -

(a) Groups
(b) Security level
(c) Contexts
(d) MIB views
(e) Access policy

→ VACM has two important characteristics -

1- VACM determines whether access to a managed object in a local MIB by a remote principal should be allowed.

2- VACM makes use of an MIB that -

(a) define the access control policy for this agent.
(b) makes it possible for remote configuration to be used.

- Motivation in VACM — The concept that make up VACM appear to result in a rather complex definition of access control. The motivations for introducing those concepts are to clarify the relationship involved in accessing management information and to minimize the storage and processing requirements at the agent.

★ SNMPv2 :—

→ The strength of SNMPv2 is its simplicity. SNMP provides a basic set of network management tools in a package that is easy to implement and easy to configure.

→ However, as users have come to reply its deficiencies have become all the apparent.

→ These defficiencies fall into three categories—

(1-) Lack of support for distributed network management.

(2-) Functional deficiencies

(3-) Security deficiencies

→ The first two categories of defficiencies are addressed in SNMPv2 which was issued in 1993, with a revised version issued in 1996 (currently RFCs 1901, 1904 through 1908, 2578 & 2579).

→ SNMPv2 quickly gained support and a number of vendors announced products within months of the issuance of the standard. The security defficiencies have been address in SNMPv3.

Q- Compare and contrast — SNMPv1 and SNMPv3

★ Comparision between SNMPv1 & SNMPv3 :—

	Basis of comparision	SNMPv1	SNMPv3
1-	Version	It was the Ist version of SNMP.	It is the newest version of SNMP.
2-	Goal	Open and standard protocol.	Uses SNMPv2 protocol operations.

Page No :

3-	Support	Smaller RTUs commonly support SNMPv1.	Net guardian 832A is one RTU that supports SNMPv3.
4-	Security	No security from someone with access to the network.	Enhanced security
5-	Complexity	Performance and security limitations.	Focuses on improving the security aspect.
6-	Message format	Five messages - Get Request, Get Next Request, Set Request, Trap, Response.	Implements SNMPv1 and SNMPv2 specifications along with proposed new features.

UNIT – 6
System Security

★ Intruders :–

→ An intruder is a person who attempts to gain unauthorised access to a system, to damage that system, or to disturb data on that system.

→ In summary, this person attempts to violate security by interfering with system availability, data integrity or data confidentiality.

→ One of the two most publicised threats to security is the intruder (the other viruses) generally referred to as a hacker or cracker. In an important early study of Intrusion Anderson (ANDE80) identified three classes of intruders –

1. Masquerader
2. Misfeasor
3. Clandestine user

1- Masquerader – An individual who is not authorised to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

2- Misfeasor – A legitimate user who accesses data, programs or resources for which such access is not authorised or who is authorised for such access but misuses his or her privilages.

3- Clandestine user – An individual who seizes supervisary control of the user/system. This control is used to evade auditing and access controls or

to suppress audit collection.

The Masquarader is likely to be an outsider, the misfeaser is generally is an insider and the clandestine user can be either an outsider or an insider.

★ Intrusion Techniques :-

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. In some cases, this can be protected in one of two ways —

1- One-way Function — The system stores only the value of a function based on the user's password when the user presents a password, the system transforms that password and compares it with the stored value.

2- Access Control — Access to the password file is limited to one or a very few accounts. On the basis of a survey of the literature and interviews with a number of password crackers, reports the following techniques have been fixed for learning passwords —

(a) Try default passwords used with standard accounts that are shipped with the system.
(b) Exhaustively try all short passwords (those of one to three characters).
(c) Try words in the system's online dictionary or a list of likely passwords.
(d) Collect information about users, such as their

full names, the names of their spouse and children, picture in their office and books in their office that are related to hobbies.

(e) Try user's phone numbers, social security numbers and room numbers.

(f) Try all legitimate licence plate numbers for this state.

(g) Use a trojan horse to bypass restrictional access. Tap the line between a remote user and the host system.

→ The first six methods are various ways of guessing a password, if an intruder has to verify the guess by attempting to log in. It is a tedious and easily countered means of attack.

★ Intrusion Detection System (IDS) :—

→ IDS is used to detect where the intrusion occur.

→ IDS can be hardware or software based security service that monitors and analyses system events that may indicate a network system attack.

→ Following factors motivate efforts on intrusion detection-

(a) The sooner it is able to detect an intrusion, the quicker we can act. The hope of recovering from attacks and losses is directly propotional to how quickly we are able to detect an intrusion.

(b) Intrusion detection can help collect more information about intrusions, strengthening the intrusion prevention methods.

(c) Intrusion detection system can act as good deterrents prevention to intruders.

★ Categories of IDS :-

1. Misuse detection
2. Anomaly detection
3. Network based IDS (NIDS)
4. Host based IDS (HIDS)
5. Passive IDS
6. Reactive IDS

1- Misuse Detection — Here, the IDS analyses the information it gathers and compares it to the database of attack signatures.

2- Anomaly Detection — In this IDS, a baseline is maintained such as traffic load state, breakdown protocol and packet size, which is compared with the present network segments to identify analysis. If baseline is choosen protocol, then this is called protocol IDS.

3- Network Based IDS (NIDS) — NIDS monitor network traffic and analyze the individual packets that are flowing through the network.
It detects malicious packets that are designed by an attacker to be overlooked by the simplistic filtering rule of many firewalls.

4- Host Based IDS (HIDS) — HIDS can be installed on individual workstations or servers to examine the activity on each individual computer mode or host.

It evaluates modifications to important system files, abnormal or excessive central processing

unit (CPU) activity and misuse of root or administrative rights.

5- Passive IDS— Here, the IDS detects a potential security breach, logs the information, and signal and alerts. Here, no direct action is taken by the system.

6- Reactive IDS— Here IDS can respond in several ways to the suspicious activity such as by loging a user off the system, closing the connection or even reprogramming firewall to block network traffic from the suspected malicious source.

* Approaches of IDS :—

1- Knowledge Based IDS— Knowledge Based IDS uses a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities is found.

2- Behaviour Based IDS— It uses dynamic approach in the sense that they detect deviations from the learned patterns of user behaviour.

An alarm is triggered when any activity that is considered outside of normal system use takes place.

3- Statistical Anomaly IDS— It involves the collection of data relating to the behaviour of legitimate users over a period of time. Then statistical

tests are applied to observe behaviour of determine with a high level of confidence whether that behaviour is not legitimate user behaviour.

It fall into two categories —

(a) Threshold detection

(b) Profile-based anomaly detection

(a) Threshold Detection — This approach involves defining thresholds, independent of users for the frequency of occurance of various events.

(b) Profile-Based anomaly detection — A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.

4- Rule Based IDS — Rule-based techniques detect intrusion by detecting (observing) events in the system and applying a set of rules that lead a decision regarding whether a given pattern of activity is or is not suspicious.

It involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.

5- Rule-Based Penetration Identification IDS —

→ It takes a very different approach to intrusion detection, one based on expert system technology.

→ The key feature of such system is the use of rules for identifying known penetrations that would exploit know ~~us~~ weakness.

→ The penetration identification scheme used in IDES

is representative of the strategy followed.

→ Audit records are examined as they are generated and they are matched against the rule base. If a match is found then the user's suspicious rating is increased.

→ If enough rules are matched, then the rating will pass a thresholds that results in the reporting of an anomaly.

6- Distributed IDS — It needs to defend a distributed collection of hosts supported by a LAN or internetwork. Porras points out the following major issues in the design of a distributed intrusion detection system.

→ A distributed IDS may need to deal with different audit record formates.

→ One or more nodes in the network will serve as collection and analysis points for the data from the system on the network.

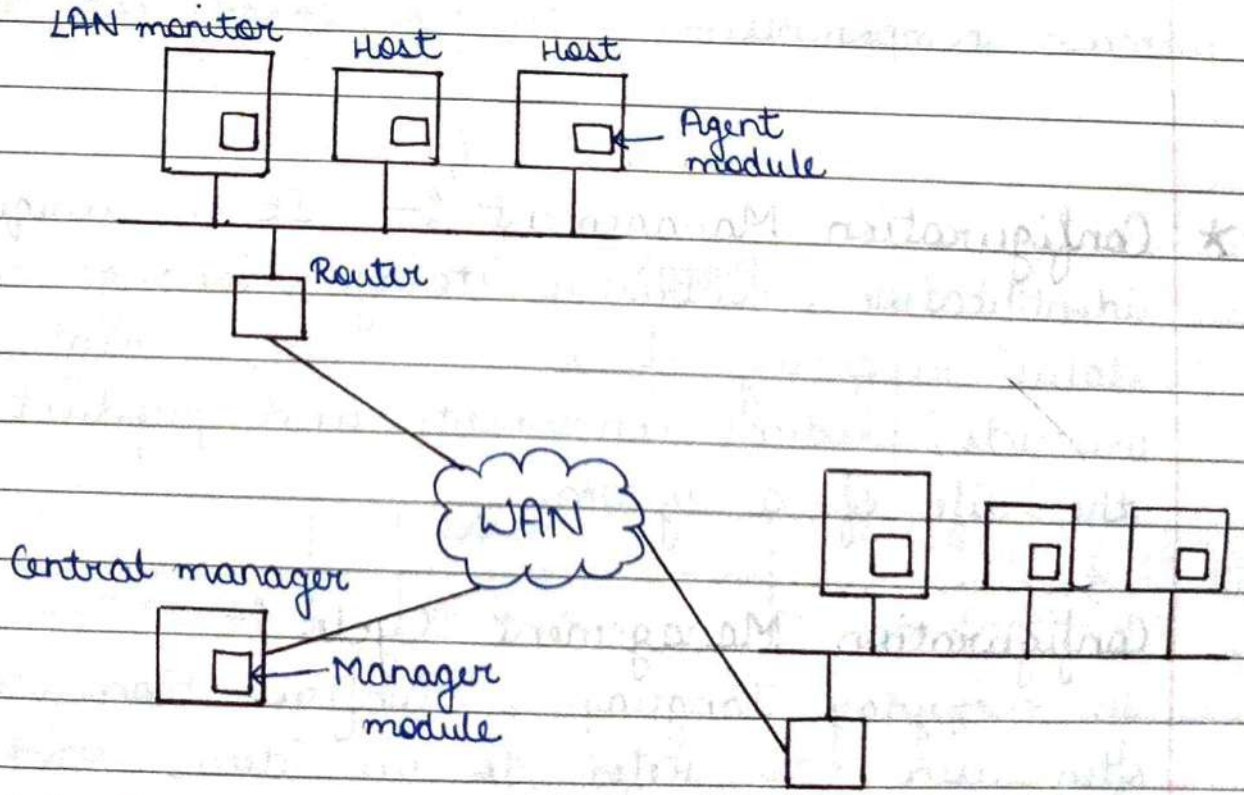


fig (a)- Architecture for distributed intrusion detection

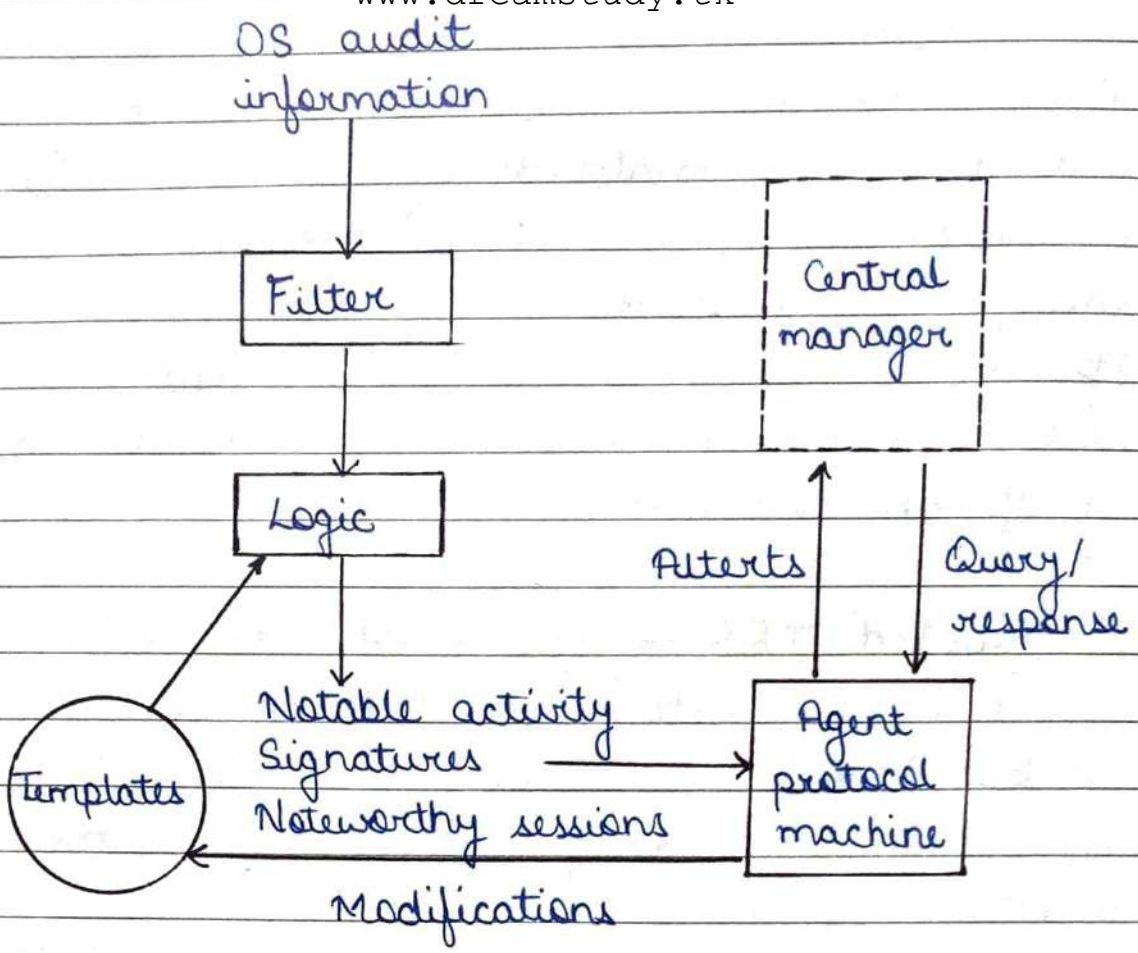


fig (b) Agent architecture

Either a centralised architecture can be used. Figure shows the overall architecture, which consist of three main components —

★ Configuration Management :— It is unique identification, controlled storage, change control and status reporting of selected intermediate work products, product components and product during the life of a system.

Configuration Management Cycle :-
In everyday language, "Configuration item" is often used to refer to an item, which is then said to be produced in several versions. This is

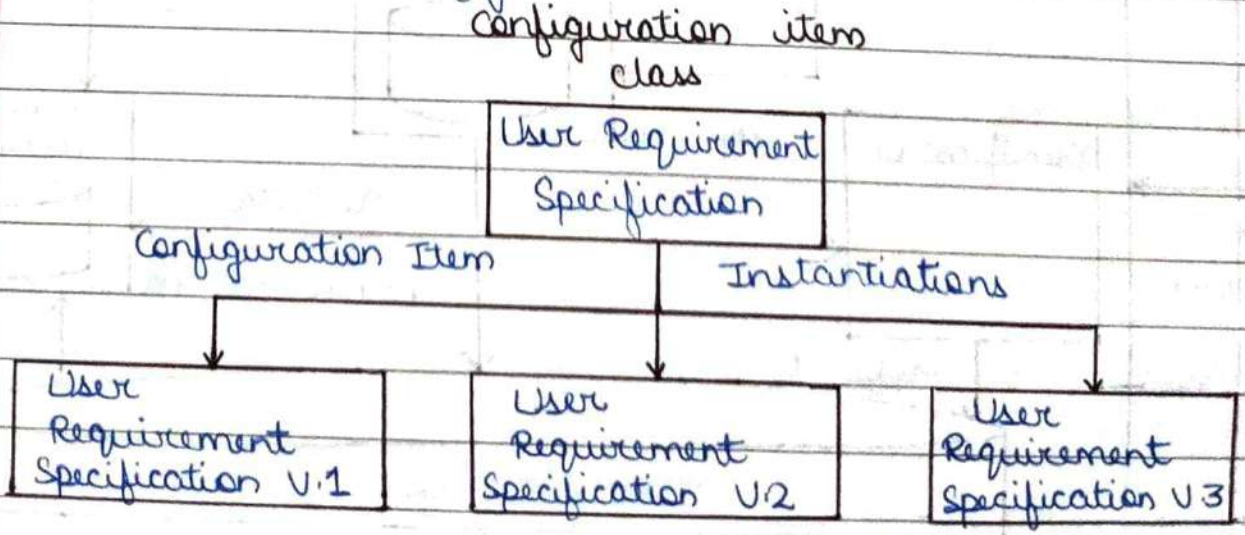
not strictly correct but it's acceptable as long as the reference is clearly understood by all involved. In fact, each new version of a configuration item is a new configuration item in its own right.

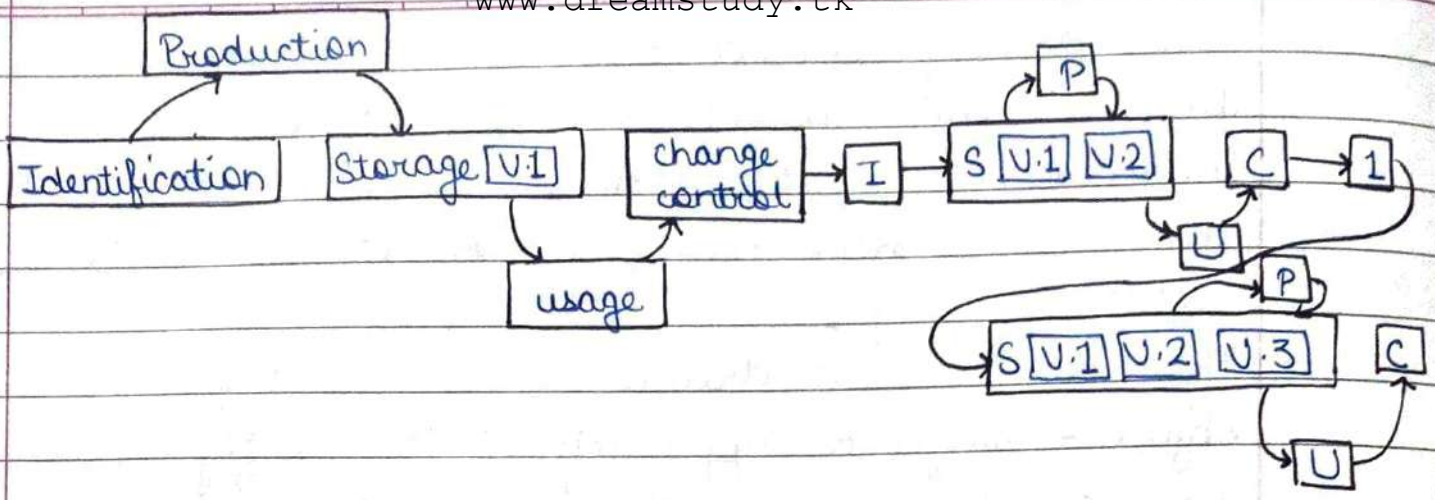
→ This can be illustrated by an analogy to an object - oriented approach. "The configuration item" may be seen as a class and the versions as instantiations of the class as shown in fig.

→ Version chains of configuration item i.e., versions 1, 2, 3 and so on may be formed by indicating which configuration item a given configuration item is derived from or based on.

→ Configuration management activities may be viewed as cyclic for each item class placed under configur-ation management. This means that a configuration item class continuously goes "through the mile."

→ The first cycle is initiated by a (planned) need for a configuration item, and later the driving force is change request (and only this!). This is illustrated in fig —





→ Configuration items are that are different versions of the same original item are obviously strongly related but each one is an individual item, which will be identified and may be contracted and used independ-ently. This is one of the main points of configurati-on management to be revert to an earlier version of an item class.

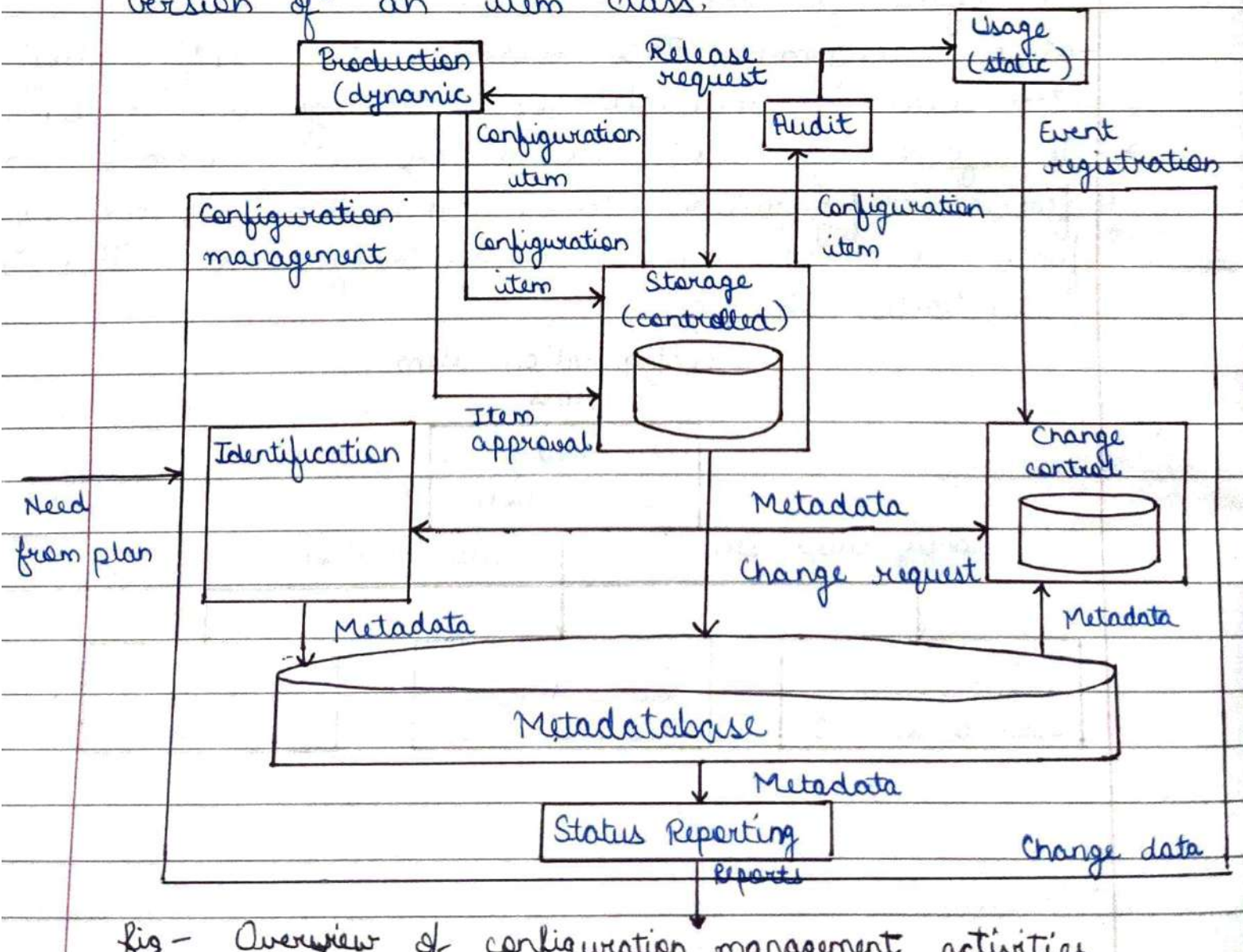


fig- Overview of configuration management activities

★ Virus :-

→ A virus is a piece of program code that attaches itself to legitimate program code and runs when the legitimate program runs. It can then infect other programs in that computer or in another computer in a same network.

→ Usually viruses cause damage to computer and network systems to the extent that it can be repaired assuming that the organisation deploys good backup and recovery procedures.

→ During its lifetime, a virus goes through four phases :-

(a) Dormant phase — Here, the virus is idle. It gets activated based on certain action or event. This is optional phase.

(b) Propagation phase — In this phase, a virus copies itself and each copy starts creating more copies of itself, thus propagating the virus.

(c) Triggering phase — A dormant virus moves into this phase when the action / event for which it was waiting is initiated.

(d) Execution phase — This is the actual work of the virus, which could be harmless or destructive.

★ Categories of Viruses :-

1- Parasitic virus — Such virus attaches itself to executable files and keeps replicating whenever files

the infected file is executed, the virus looks for other executable files to attach itself and spread.

2- Memory - Resident Virus — The virus first attach itself to an area of the main memory and then infects every executable program.

3- Boot Sector Virus — This virus infects the master boot record of disk and spread on the disk when operating system starts booting the computer.

4- Stealth Virus — This virus has intelligence built-in, which prevent anti-virus software program from detecting it.

5- Polymorphic Virus — A virus that keeps its signature on every execution, changing making it very difficult to detect.

6- Metamorphic Virus — In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

Q- What do you mean by firewalls? Discuss the need of firewall in VPN along with its types.

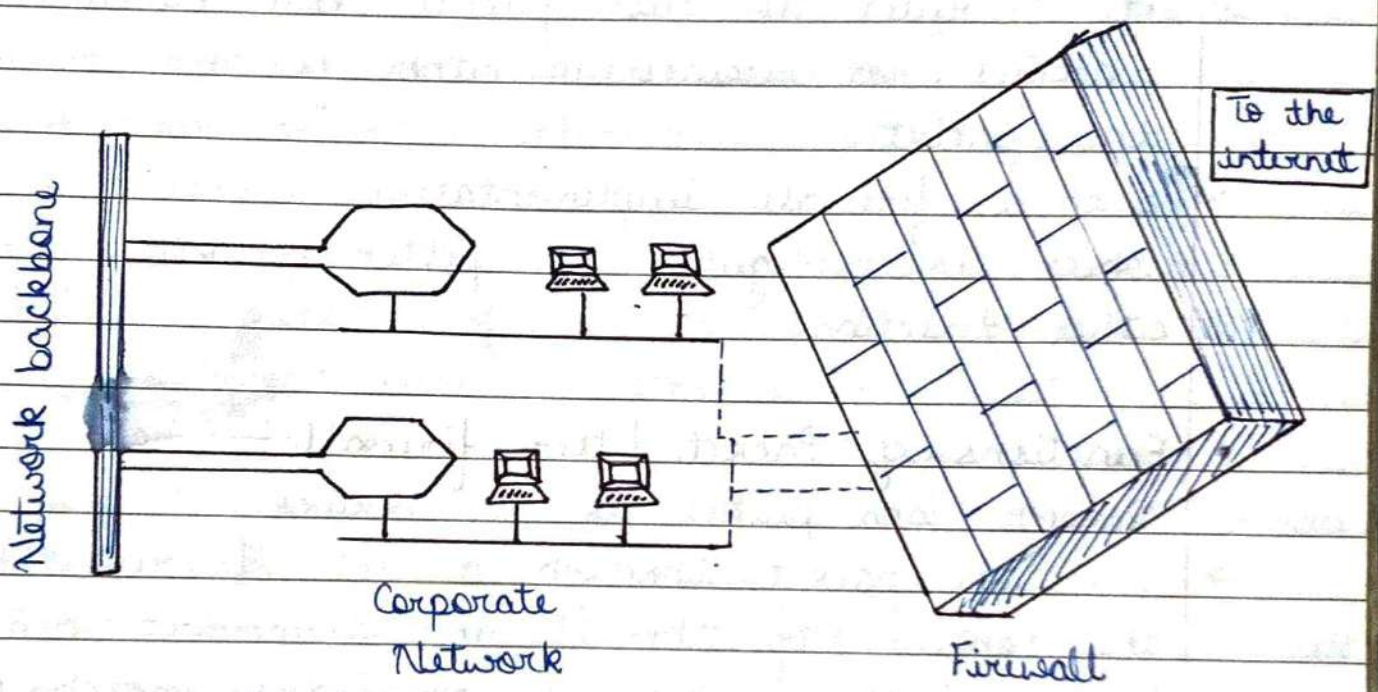
★ Firewall :-

→ A firewall acts like a sentry for a corporate network. Firewall stands between corporate network and the outside world and prevent the network from outsider's attack.

→ All the traffic between the network and the internet in either direction must pass through the firewall.

→ The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.

→ Technically, a firewall is a specialized version of router. Apart from a basic routing function and rules, a router can be configured to perform the firewall functionality with the help of additional software resources.



Characteristics of a good firewall :-

All traffic from inside to outside and vice-versa must pass through the firewall. To achieve this, all the access to the local network must first be physically blocked and access only via the firewall should be permitted.

→ Only the traffic, authorized as per the local security policy should be allowed to pass through.

→ The firewall itself must be strong enough so as to render attacks on it useless.
prevent

- Types of Firewall :- Depending on criteria used for filtering traffic, firewall are generally classified into two types -

(1.) Packet filter firewall
(2.) Application gateways firewall

1- Packet Filter Firewall — Packet filter also known as screening router or screening filter, applies a set of rules to each packet and based on the outcomes, it decides to either forward or discard the packet.

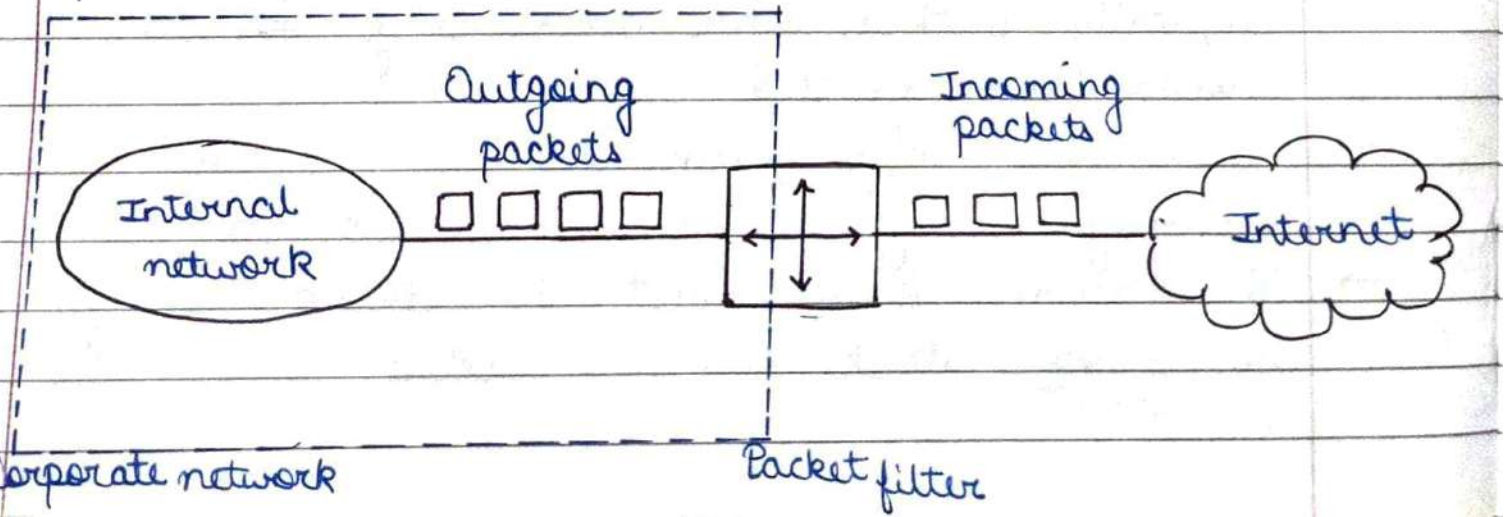
→ Such a firewall implementation involves a router, which is configured to filter packets going in either direction.

- Functions of Packet filter firewall —

→ Receive each packet as it arrives.

→ Pass the packet through a set of rules based on the contents of the IP and transport header fields of the packet. If there is match with one of the set of rules, decide whether to accept or discard the packet based on that rule.

→ If there is no match with any role, take the default action. The default action can discard all packets or accept all packets.



2- Application Gateways Firewall —

→ An application gateway is also called as a 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 gateway using a TCP/IP application such as HTTP or TELNET.

→ The application gateway asks the user about remote host with which the user wants to set up a connection for actual communication.

→ The user provides information to the application gateway.

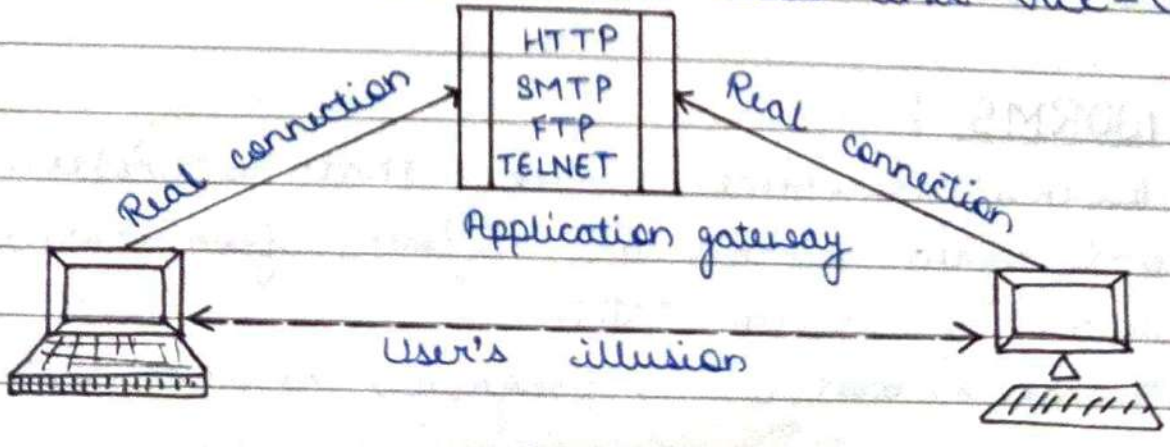
→ The application gateway now accesses the remote host on behalf of the user and passes the packets of the user to the remote host.

→ A variation of application gateway is called "circuit gateway", creates a new connection between itself and the remote host.

→ The circuit gateway changes the source IP address in the packets from the end user's IP address to its own.

→ This way, the IP addresses of computers of the internal users are hidden from outside world.

→ The application gateway acts like a proxy of the actual end-user and delivers packets from the user to the remote host and vice-versa.



★ Hardware Firewall :-

→ Hardware firewall is a stand alone product such as a broadband router.

→ It uses packet filtering as the method to transfer data. It compares the header of the packets and determines the destination and source address.

→ A hardware firewall is a device placed in between server computer and the internet. They are harder to configure than software firewalls.

→ Hardware firewall still protect the computer when the operating system crashes.

→ Hardware firewall does not consume CPU time and memory of server.

★ Software firewall :-

→ Software firewall are program based applications that run on a computer.

→ They work by monitoring all open ports on a computer and checking all the information that is received on them.

→ Software firewall is cheaper than a hardware firewall and easier to configure than hardware firewalls.

→ This firewalls consumes lot of memory and CPU time. It is not possible to protect whole network on single firewall.

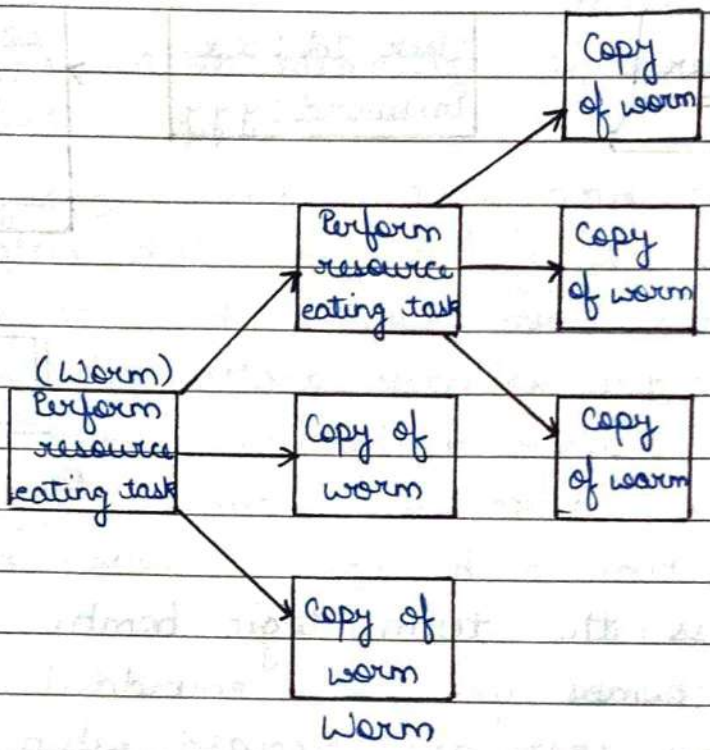
★ WORMS :-

1- Worms are piece of code that replicates itself again and again. Worms are different from viruses in terms of implementation.

2. A virus modifies a program, however a worm does

not modify a program.

3- A worm replicates so much itself that ultimately the computer or the network on which the worm resides become very slow, finally coming to a halt



4- Thus, the basic purpose of worm is different from virus. Virus used for destructive actions whereas worm does not perform any destructive action, only consumes system resources to make system unusable.

Ques – What is trojan horse?

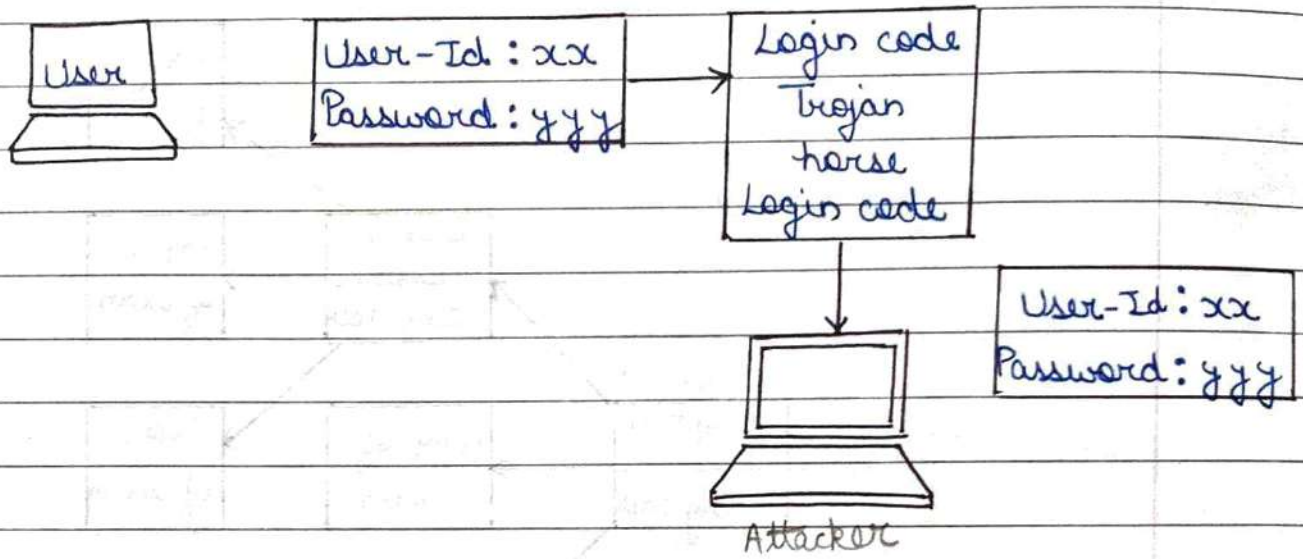
Ans – Trojan Horse :–

1- A trojan horse is a hidden piece of code, which allows attacker to obtain or reveal some confidential information about a computer or a network.

2- The name trojan horse is due to Greek soldiers, who hide inside a large hollow horse, which was pulled by Troy citizens and opened gates for rest of Greek soldiers.

3- In a similar way, trojan horse could attack to the

code of login screen. When user enters user id and password, the trojan could capture these details and send this information to attacker. Then attacker can use this information to gain access to the system.



Que- Discuss the term logic bomb.

Ans- Logic bombs are codes embedded in some legitimate program that are executed when a predefined event occurs.

2. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date or a particular user running the application.
3. These bombs display a message to the user and occur at time when either the user is accessing the internet or making use of a word processor application.
4. Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.
5. The logic bomb initiation is a four-step process-

(a) Attacker implants the logic bomb.
(b) Victim reports the installation.
(c) Attacker sends the attack message.

Ques- What is e-mail virus ?

Ans- 1- An e-mail virus is computer code sent as an e-mail note attachment which if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on hard disk and causing the attachment to be re-mailed to everyone in address book.

2- Although not the only kind of computer virus, e-mail viruses are the best known and undoubtedly cause the greatest loss of time and money overall.

3- The best two defenses against e-mail viruses for the individual user are—

(a) A policy of never opening (eg. double clicking on) an e-mail attachment unless you know who sent it and what the attachment contains.

(b) Installing and using antivirus software to scan any attachment before opening it.

Ques- What is macro virus ?

Ans- 1- A macro virus is a computer virus written in the same macro language used for software applications like word processors. It effects is to release a chain of events in conjunction with the application.

2- Microsoft word is an example of an application susceptible to macro viruses, this explains why it is a bad idea to open suspicious or unknown attachment even if they may appear legitimate.

3- Because macro programs embedded in these document run automatically when the document is opened, it is a likely mechanism to spread viruses.

4- Once triggered, the macro virus can embed itself in other documents including any future

documents created after the virus attack. as well as conceivably download software to the target computer.

5- Because a macro virus works using the application rather than an operating system, it can infect non windows computers as well.

6- Macro viruses are also known as script viruses and can also be embedded within web pages. The best defense against being infected by a macro virus, besides being very careful of what e-mail attachments you open, is having a quality updated antivirus.

Ques - What is malicious software or malware?

OR

Explain characteristics of malicious software (malware)

Ans- 1- Malicious software (malware) is any software that gives partial to full control of computer to do whatever the malware creator wants. Malware can be virus, worm, trojan etc.

2- Most malware requires the user to initiate its operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks OK on pop-up and from vulnerabilities in the operating system or programs.

Characteristics of malwares —

1- Self replicating malware actively attempts to propagate by creating new copies, or instances of itself. Malware may also be propagated passively by a user copying it accidentally, but this is not self

replication

2- The population growth of malware describes the overall change in the number of malware instance due to self replication.

3- Malware that does not self replicate will always have a zero population growth, but malware with a zero population growth may self replicate.

4- Parasitic malware requires some other executable code in order to exist. "Executable" in this context should be taken very broadly to include anything that can be executed such as boot block code on a disk, binary code.