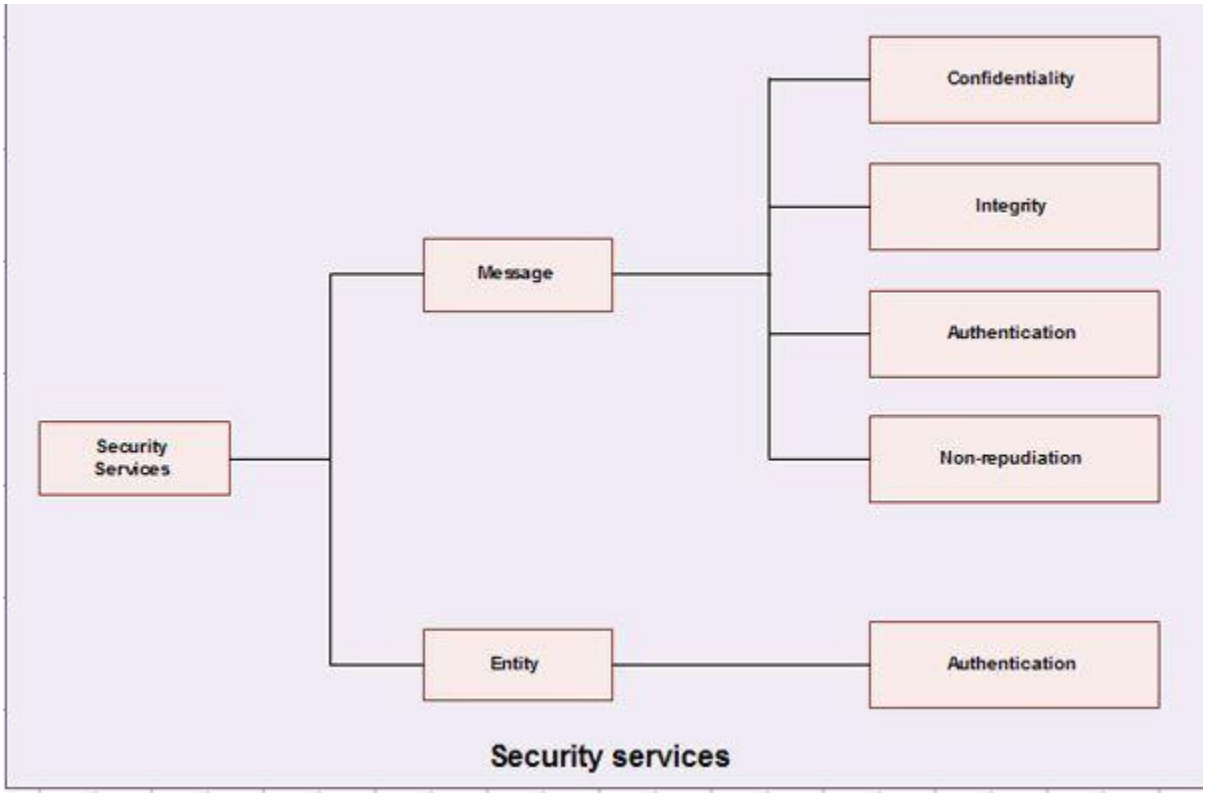
Security Service and Mechanism

Network security can provide the following **services** related to a message and entity.



1. Message confidentiality
2. Message Integrity
3. Message Authentication
4. Message non-reproduction
5. Entity Authentication

1. Message confidentiality

It means that the content of a message when transmitted across a network must remain confidential, *i.e.*, only the intended receiver and no one else should be able to read the message.

The users: therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

2. Message Integrity

It means the data must reach the destination without any adulteration *i.e.* exactly as it was sent.

There must be no changes during transmission, neither accidentally nor maliciously.

Integrity of a message is ensured by attaching a checksum to the message.

The algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

3. Message Authentication

In message authentication the receiver needs to be sure of the sender's identity *i.e.* the receiver has to make sure that the actual sender is the same as claimed to be.

There are different methods to check the genuineness of the sender:

1. The two parties share a common secret code word. A party is required to show the secret code word to the other for authentication.

2. Authentication can be done by sending digital signature.

3. A trusted third party verifies the authenticity. One such way is to use digital certificates issued by a recognized certification authority.

4. Message non-reproduction

Non-repudiation means that a sender must not be able to deny sending a message that it sent.

The burden of proof falls on the receiver.

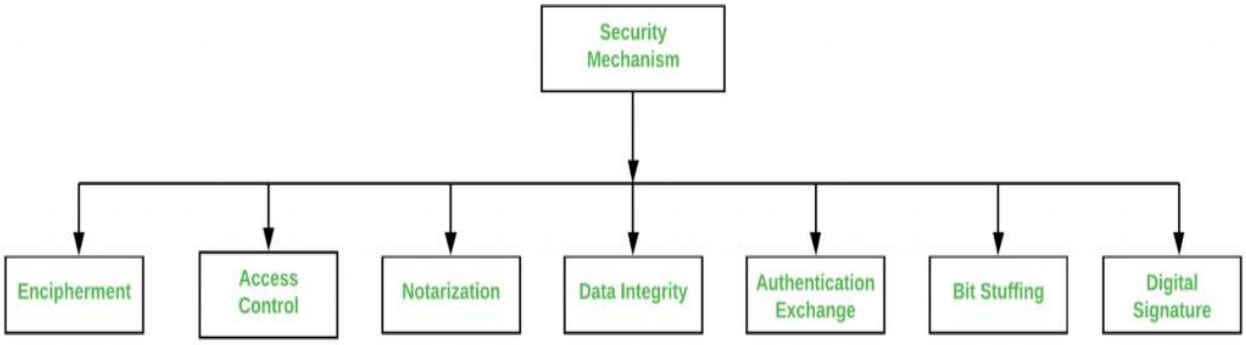
Non-reproduction is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent.

Non-repudiation is achieved by authentication and integrity mechanisms.

5. Entity Authentication

In entity authentication (or user identification) the entity or user is verified prior to access to the system resources.

As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore **security mechanism** can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



Types of Security Mechanism are :

1. **Encipherment :**
   This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.
2. **Access Control :**
   This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
3. **Notarization :**
   This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.
4. **Data Integrity :**
   This security mechanism is used by appending value to data to which is created by data itself. It is like sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
5. **Authentication exchange :**
   This security mechanism deals with identity to be known in

communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

6. **Bit stuffing :**
   This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
7. **Digital Signature :**
   This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential, but sender's identity is to be notified.