OSI SECURITY ARCHITECTURE

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

Security attack – Any action that compromises the security of information owned by an organization
Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack
Security service – A service that enhances the security of the data processing systems and the information transfers of an organization.

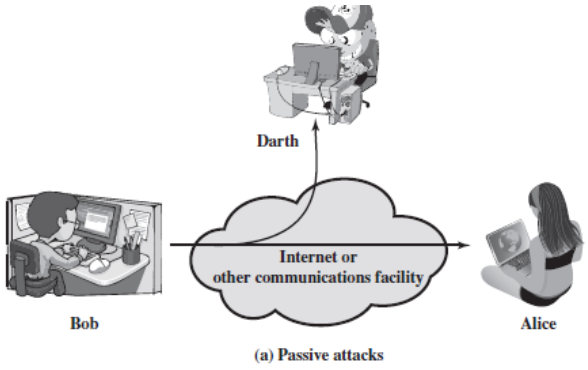
SECURITY ATTACK

There are two types of attacks

- Passive attacks
- Active attacks

Passive attack

Passive attacks attempt to learn or make use of information from the system but do not affect system resources. The goal of the opponent is to obtain information that is being transmitted.



(a) Passive attacks

Passive attacks are of two types

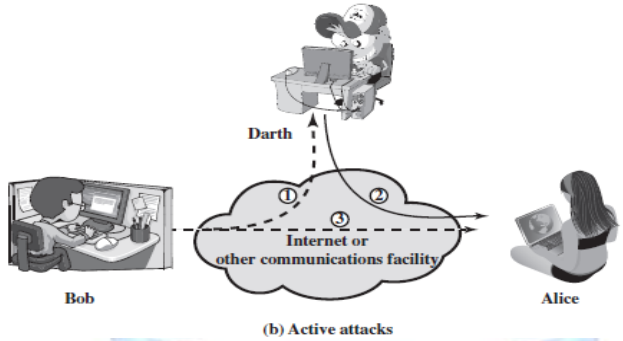
- **Release of message contents**
- **Traffic analysis**

Release of message contents: The opponent would learn the contents of the transmission. A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis: The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Passive attacks are very difficult to detect, because they do not involve any alteration of the data. However, it is feasible to prevent the success of these attacks.

Active attacks

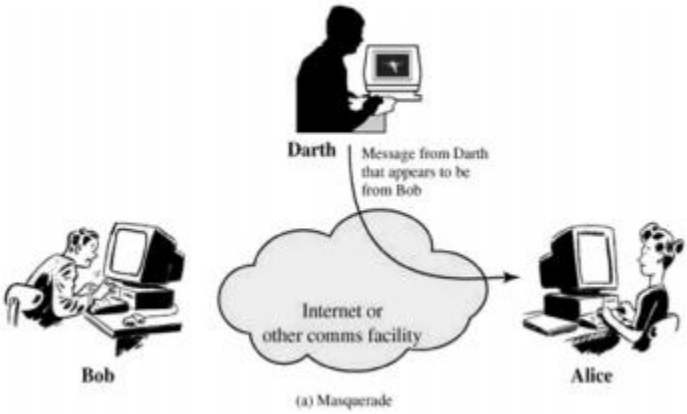
These attacks involve some modification of the data stream or the creation of a false stream.



(b) Active attacks

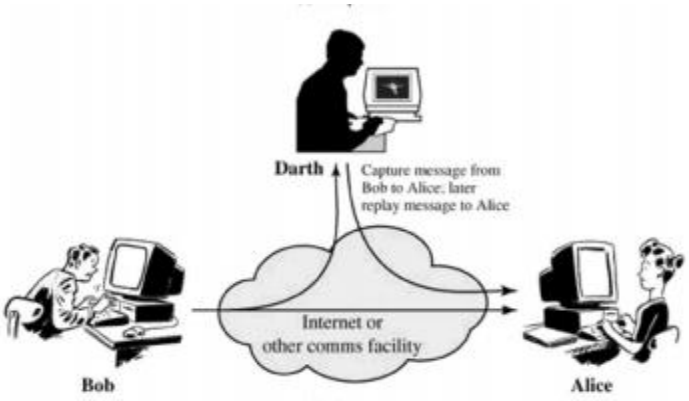
Active attacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity. Here, the attacker capturers the authentication and impersonifies the sender.

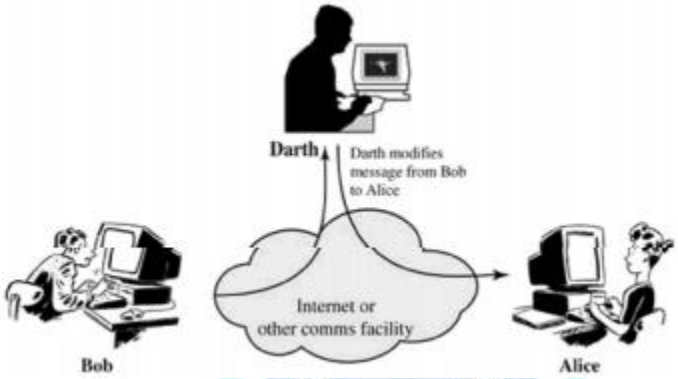


(a) Masquerade

Replay – The attacker captures the message and retransmits the message without modification to produce unauthorized effect.



Modification of messages – The attacker captures the message and retransmits the message with modification to produce unauthorized effect.



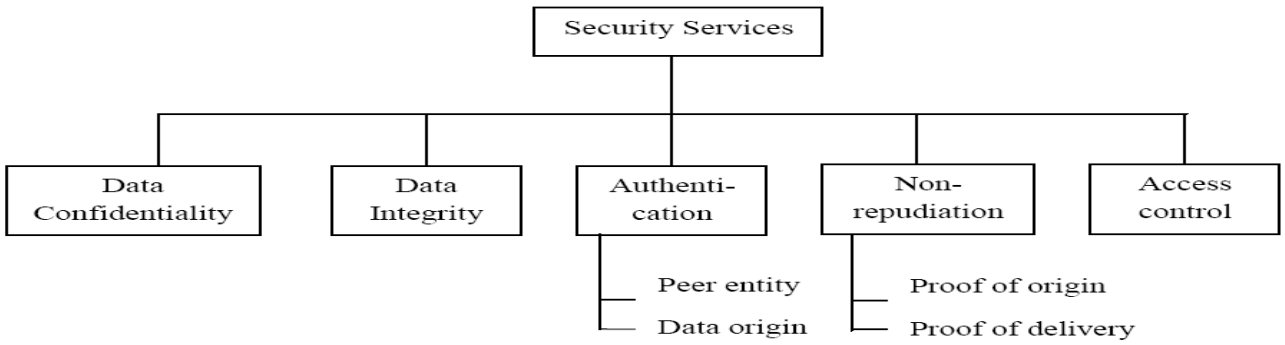
Denial of service – The attacker may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

SECURITY SERVICES

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

The classification of security services are as follows:



(i) Authentication: The authentication service is concerned with assuring that a communication is authentic.

Two specific authentication services are defined in X.800:

- **Peer entity authentication:** Provide confidence in the identity of entities connected.
- **Data origin authentication:** Provide assurance that the source of received data is as claimed.

(ii) Access control: Access control is the ability to limit and control the access to host systems and applications.

(iii) Data Confidentiality: Confidentiality is the protection of transmitted data from passive attacks.

- **Connection Confidentiality**
  The protection of all user data on a connection
- **Connectionless Confidentiality**
  The protection of all user data in a single data block
- **Selective-Field Confidentiality**
  The confidentiality of selected fields within the user data on a connection or in a single data block
- **Traffic-Flow Confidentiality**
  The protection of the information that might be derived from observation of traffic flows

(iv)Data Integrity: The assurance that data received are exactly as sent by an authorized entity.

- **Connection Integrity with Recovery**
  Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery**
  As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity**
  Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity**
  Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity**
  Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

(v)Non repudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

- **Nonrepudiation, Origin**
  Proof that the message was sent by the specified party
- **Nonrepudiation, Destination**
  Proof that the message was received by the specified party

SECURITY MECHANISMS

- **Encipherment:**

  It uses mathematical algorithm to transform data into a form that is not readily intelligible. It depends upon encryption algorithm and key

- **Digital signature:**

  Data appended to or a cryptographic transformation of a data unit that is to prove integrity of data unit and prevents from forgery

- **Access control**

A variety of mechanisms that enforce access rights to resources.

- **Data integrity**

A variety of mechanism are used to ensure integrity of data unit

- **Traffic padding**

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

- **Notarization**

The use of a trusted third party to assure certain properties of a data exchange