4.2 The OSI Security Architecture

ITU-T Recommendation X.800, *Security Architecture for OSI*, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security.

OSI : Open Systems Interconnection

ITU-T : The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) is a United Nations sponsored agency that develops standards.

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 process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security violations:

1. When data is transmitted from one system to other, the data would be access by other user.
2. An unauthorized user may access and change the original message (data).
3. Duplicate message may be sent by unauthorized user by discarding the original message.
4. Delaying the message during transmission.
5. Denying about sent message, i.e. user who sent the message itself can deny it.

- Nearly all modern multiuser computer and network operating systems employ passwords at the very least to protect and authenticate users accessing computer and/or network resources. But passwords are *not* typically kept on a host or server in plaintext, but are generally encrypted using some sort of hash scheme.

Security Threats

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

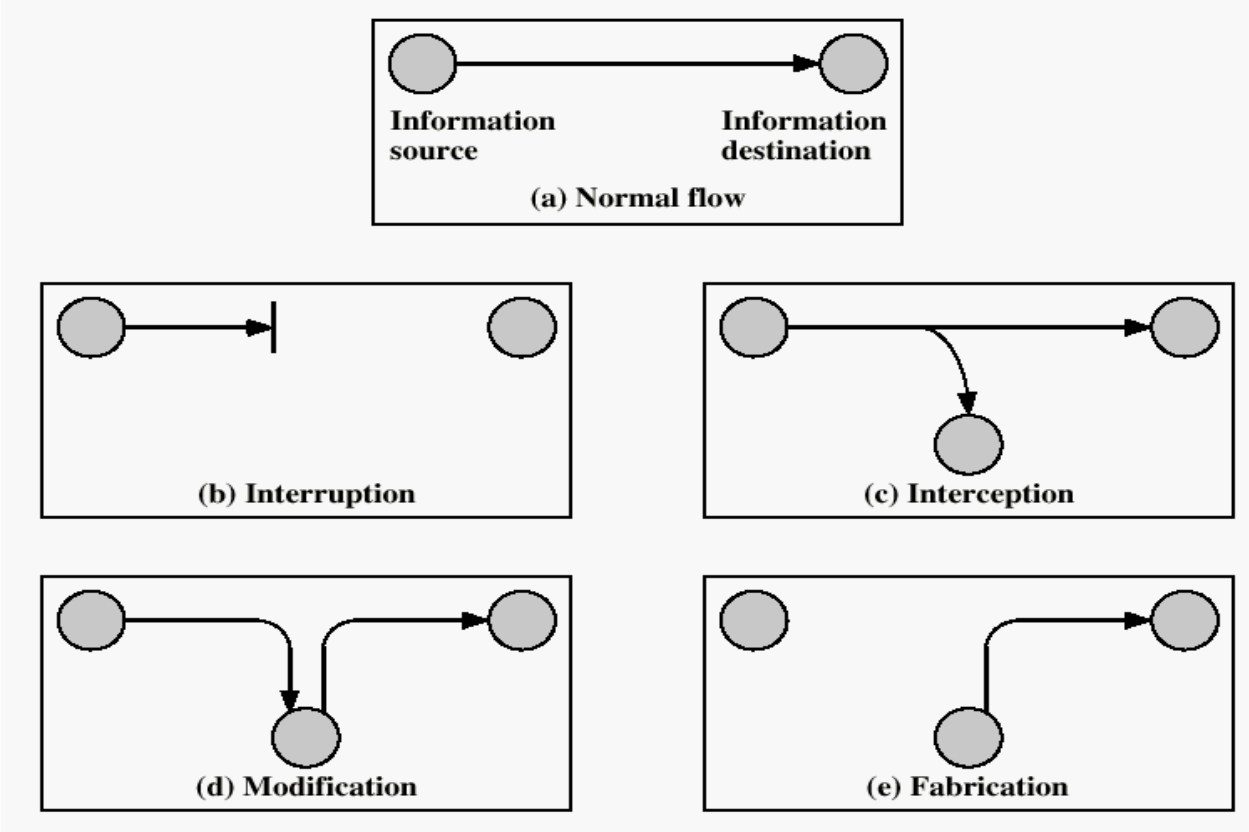

Fig 1: Security Threats

Interruption: an asset of the system is destroyed or becomes unavailable. This is an attack on unavailability. E.g: cutting the communication line.
Interception: an unauthorized user gain access to an asset. This is an attack on confidentiality. Eg: wiretapping.
Modification: an unauthorized user not only gains access to, but tampers with an asset. This is an attack on integrity. Eg: changing values in data file.
Fabrication: an unauthorized user inserts counterfeit objects into the system. This is an attack on authenticity. Eg: insertion of spurious messages.

Security Attacks

In computer networks, an **attack** is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Types of attacks: passive attacks and active attacks. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

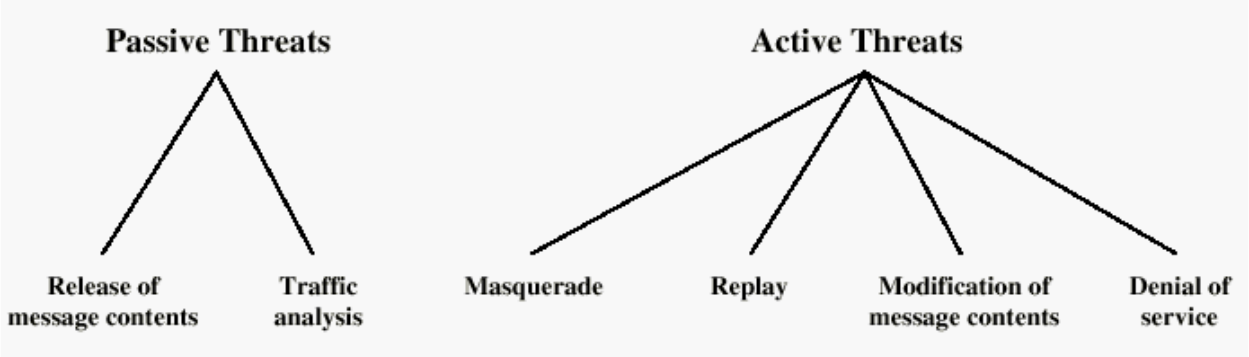

Fig 2 : Types of attacks

Passive attack: This attack is just accessing the message and not altering the message. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

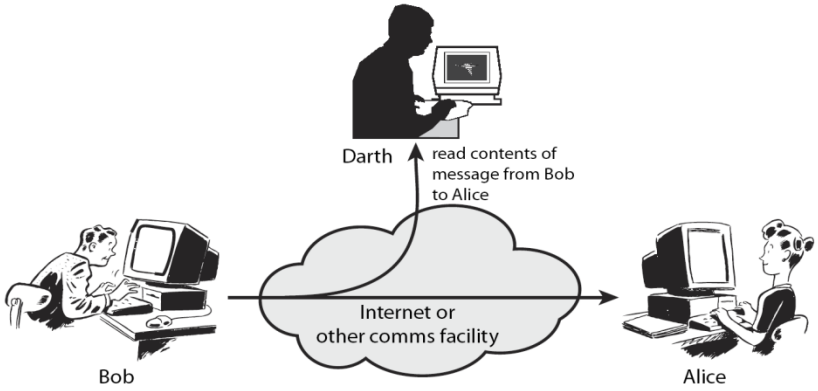

Fig 3: Passive attack – release of message contents

The **release of message contents** is easily understood (Figure 3). i.e, to read the contents of message. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

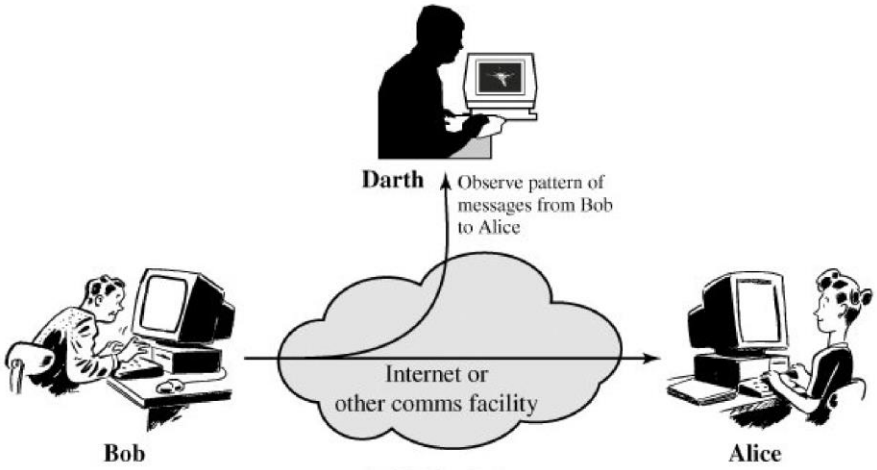

Fig 4: Passive attack – Traffic analysis

Traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. 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.

Active attacks: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

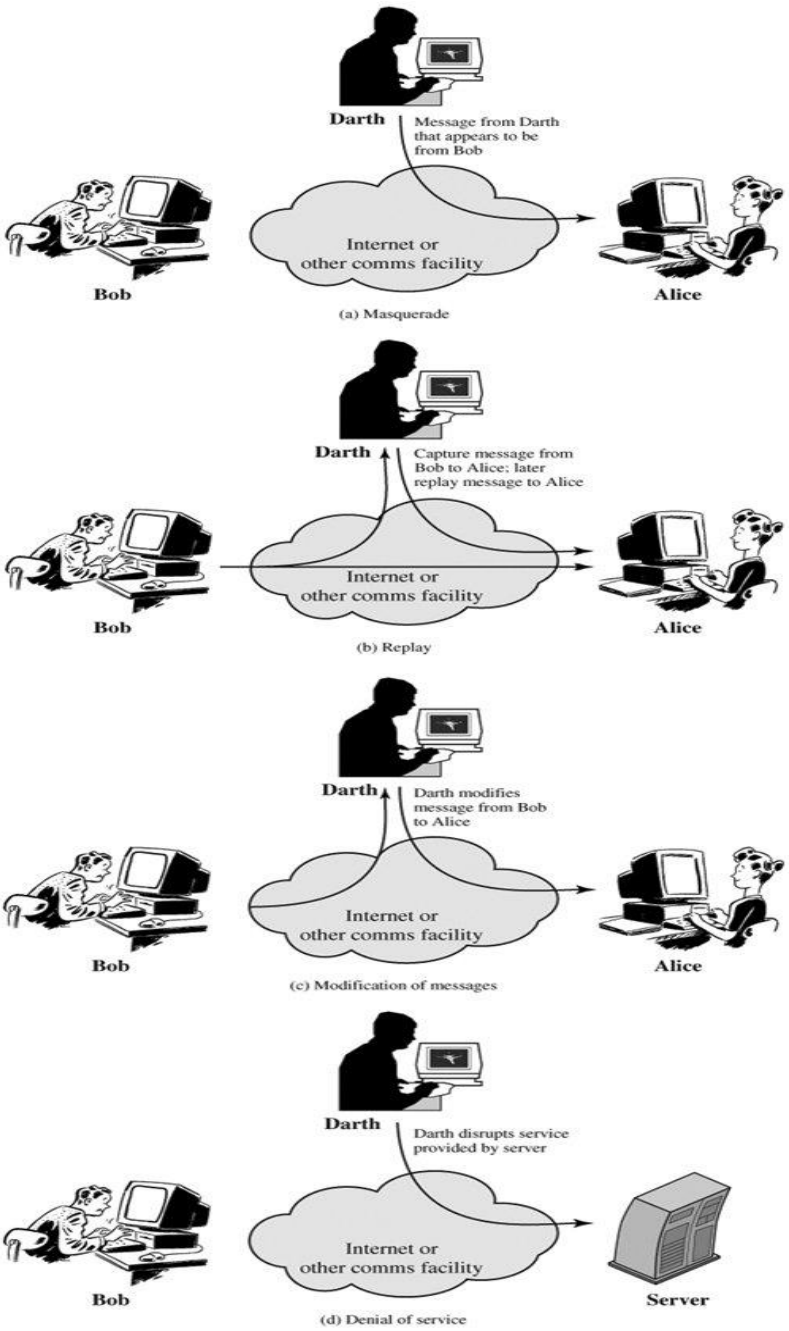

Fig 5: Active attacks

A **masquerade** takes place when one entity pretends to be a different entity (Fig 5a). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Fig 5a).

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Fig 5c). For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Fig 5d). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). 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.

Security services:

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

X.800 divides these services into five categories and fourteen specific services

1. Authentication (who created or sent the data)
2. Access control / Availability (prevent misuse of resources)
3. Confidentiality (privacy)
4. Integrity (has not been altered)
5. Non-repudiation (the order is final)

- **Authentication** - assurance that the communicating entity is the one that it claims to be.
  - The process of proving one's identity.
  - **Peer Entity Authentication**
    - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - **Data Origin Authentication**
    - In a connectionless transfer, provides assurance that the source of received data is as claimed.

- **Access Control/Availability** - prevention of the unauthorized use of a resource

- **Data Confidentiality** –protection of data from unauthorized disclosure.
  - *Privacy* - Ensuring that no one can read the message except the intended receiver.
  - **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.

➢ **Data Integrity** - The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
❖ Assuring the receiver that the received message has not been altered in any way from the original.
❖ **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.

➢ **Non-Repudiation** - protection against denial by one of the parties in a communication. A mechanism to prove that the sender really sent this message.
❖ **Non-repudiation, Origin**
- Proof that the message was sent by the specified party.

❖ **Non-repudiation, Destination**
- Proof that the message was received by the specified party.

Security Mechanism

➢ A security mechanism is a means to provide a service
❖ **E.g.** encryption, cryptographic protocols

➢ **Specific Security Mechanisms**
✓ May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

❖ **Encipherment**
✓ The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

❖ **Digital Signature**
✓ Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

❖ **Access Control**

- ✓ A variety of mechanisms that enforce access rights to resources.

❖ **Data Integrity**

- ✓ A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

❖ **Authentication Exchange**

- ✓ A mechanism intended to ensure the identity of an entity by means of information exchange.

❖ **Traffic Padding**

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

❖ **Routing Control**

- ✓ Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

❖ **Notarization**

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

➢ **Pervasive Security Mechanisms**

- ✓ Mechanisms that is not specific to any particular OSI security service or protocol layer.

❖ **Trusted Functionality**

- ✓ That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

❖ **Security Label**

- ✓ The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

❖ **Event Detection**

- ✓ Detection of security-relevant events.

❖ **Security Audit Trail**

- ✓ Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

❖ **Security Recovery**

- ✓ Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.