Security definition:

Security is referred to protect data during the transmission. It is concerned with making sure that noisy people cannot read message ,or worse yet ,secretly modify messages intended for other recipients. It is concerned with people trying to accesses the remote services that they are not authorized to use. Security also deals with people trying to deny that they sent certain message.

The OSI Security Architecture

ITU-T Recommendation X.800, *Security Architecture for OSI* (open systems interconnection) , defines such a systematic approach.

The OSI security architecture is useful to managers as a way of organizing the task of providing security. 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 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 Attacks

A useful means of classifying security attacks is in terms of ***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.

Passive Attacks:

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.

The **release of message contents**. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, **traffic analysis**. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. 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.

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.

A **masquerade** takes place when one entity pretends to be a different entity .Masquerade attack usually includes one of the other forms of active attack.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized.

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.

The **denial of service** prevents or inhibits the normal use or management of communications facilities.

Security Services:

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures the systems or of data transfers. Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

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

Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

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

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

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).

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.

NONREPUDIATION

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

The lists of security mechanisms defined in X.800 are:

Security Mechanisms (X.800)

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 are 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.