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. Also the RFC 2828 defines security services as 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** as shown in the below Table.

Table: Security Services (X.800)

1. AUTHENTICATION: The assurance that the communicating entity is the one that it laims 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.

2. 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).

3. 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.

4. 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.

5. 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 following Table lists the security mechanisms defined in X.800. The security mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms.

A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted.

Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

Table 1.4 indicates the relationship between Security Services and Security Mechanisms.

Table:1.4 Relationship between Security Services and Security Mechanisms (X.800)

Service	Encipherement	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication		Y	Y		Y			
Data origin Authentication		Y	Y					
Access Control			Y					
Confidentiality		Y						Y
Traffic Flow Confidentiality		Y					Y	Y
Data Integrity		Y	Y		Y			
Non-repudation		Y			Y			
Availability					Y	Y		

SPECIFIC SECURITY MECHANISMS

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.

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.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf