Lecture 2 Title : Security Services, Mechanisms and Techniques.

Lecture Outlines:

2.1 Security Services.

2.2 Security Mechanism

2.3 Security Techniques

Objectives :

After studying this lecture, you will be able to discuss:

- ✓ Essential Security services to be provided by communication system.
- ✓ Methods/mechanisms that can ensure various services.
- ✓ Techniques to realize security goals.

2.1 Security Services.

Security Service is 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.

X.800 (Security Architecture for OSI)* divides these services into many categories and specific services (see Table 2.1). Figure 7 below shows all specific services and the category they belong to.

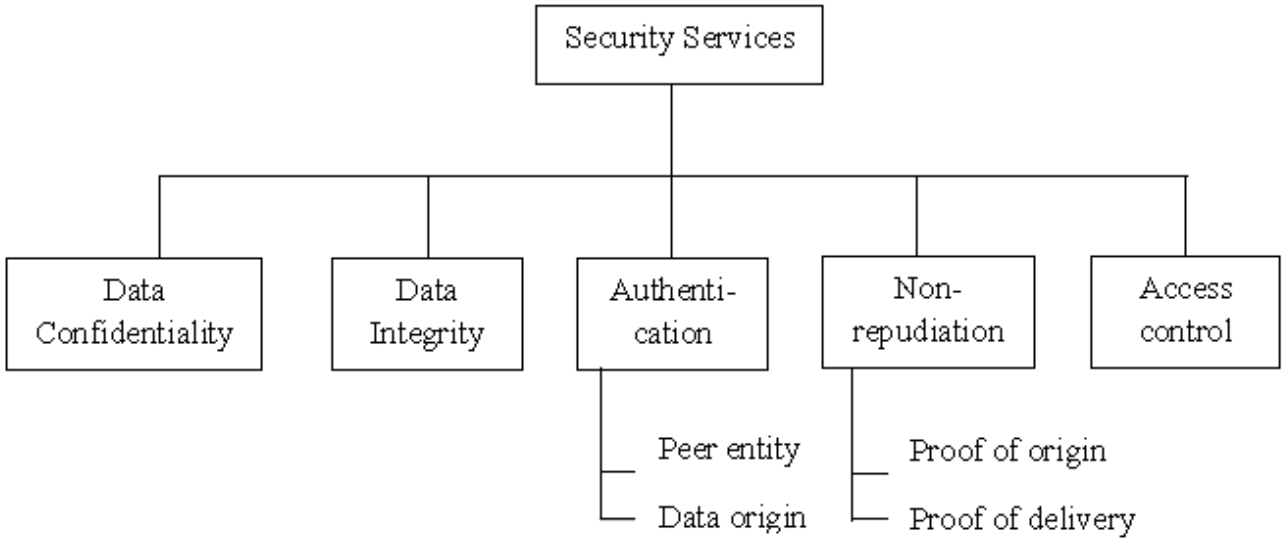

Figure 6 : All specific services and the category they belong to

* Used as references to systematically evaluate and define security requirements.

Table 2.1: Category of services and specific tasks

Service and Definition	Specific Tasks
Data Confidentiality - Protection of data from unauthorized disclosure (from passive attacks)	1. Connection confidentiality (prevents the release of any user data transmitted over the TCP connection). 2. Connectionless confidentiality. 3. Selective field confidentiality (message or even specific fields within). 4. Traffic flow confidentiality (protection of traffic flow from analysis).
Data Integrity - Assurance that data is as sent by authorized entity (contains no modifications, insertion, deletion, or replay) (As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message)	1. Connection integrity with recovery. 2. Connection integrity without recovery. 3. Selective field connection integrity. 4. Connectionless integrity. 5. Selective field connectionless integrity.
Authentication - Assurance that communicating entity is the one that it claims to be from.	1. Peer entity authentication (for participating entities). 2. Data origin authentication (for the corroboration of the source of a message (sender)
Non repudiation -provides protection against one of the entities from denying all or part of the communication. (It prevents either sender or receiver from denying message transmission or receipt of message)	1. Non repudiation of origin 2. non repudiation of destination

Access Control - Prevention of unauthorized use of a resource. (each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual)	
Availability of Service - A system is available if it provides services according to the system design whenever users request them).	

2.2 Security Mechanisms

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

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service. These mechanisms are called "**specific security mechanisms"** and **"pervasive security mechanism**".

2.2.1 Specific Security Mechanisms

Some techniques for realizing security are listed here.

1. **Encripherment:** This is the process of using mathematical algorithms to transform data into a form that is not readily intelligible.
2. **Digital Signature:** Data or cryptographic transformation of a data unit is appended to the data, so that the recipient of the data unit is convinced of the source and integrity of the data unit and this can also serve to protect the data against forgery (e.g., by the recipient).
3. **Access Control:** A variety of mechanisms are available that enforce access rights to resources.
4. **Data Integrity:** A variety of mechanisms may be used to assure the integrity of

a data unit or stream of data units.

5. **Authentication Exchange:** This is a mechanism intended to ensure the identity of an entity by means of information exchange.
6. **Traffic Padding:** The insertion of bits into gaps in a data stream is called traffic padding. This helps to thwart traffic analysis attempts.
7. **Routing Control:** enables selection of particular physically secure routes for certain data transmission and allows routing changes, especially when a breach of security is suspected.
8. **Notarization:** This is the use of a trusted third party to assure certain properties of a data exchange.

2.2.2 Pervasive Security Mechanisms

These are the mechanisms that are not specific to any particular OSI security service or protocol layer.

1. **Trusted Functionality:** The process that which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
2. **Security Label:** This is the technique of marking of a bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
3. **Event Detection:** Detection of security-relevant events such as forgery, denial of sending or receiving of data, alteration of data etc. is another important essential mechanism.
4. **Security Audit Trail:** Data can be collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
5. **Security Recovery:** This deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Table 2.2, based on one in X.800, indicates the **relationship between security services and security mechanisms.**

Service	Encipherment	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 repudiation		Y		Y				Y
Availability				Y	Y			

2.3 Security Techniques

Mechanisms discussed in the previous section are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: one (**cryptography**) is very general and the other one (**steganography**) is specific.

2.3.1 Cryptography

Some security mechanisms listed in the previous section can be implemented using cryptography. Cryptography, a word with Greek origin, means "secret writing". However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks. Although in the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: symmetric-key

encripherment, asymmetric-key encripherment, and hashing. We will briefly discuss these three mechanisms here.

- **Symmetric-key Encipherment :**

In symmetric encipherment, an entity, say Alice, can send a message to other entity, say Bob, over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply eavesdropping over the channel. Alice encrypts the message using an encryption algorithm. Bob decrypts the message using a decryption algorithm. Symmetric-key encipherment uses a single secret key for both encryption and decryption. Encryption/decryption can be thought of as electronic locking system. In symmetric-key enciphering, Alice puts the message in a box and locks the box using the shared secret key; Bob unlocks the box with the same key and takes out the messages.

- **Asymmetric Encipherment**

In asymmetric encipherment, we have the same situation aas the symmetric-key encipherment, with a few exceptions. First, there are two keys instead of one; one public key and one private key. To send a secure message to Bob, Alice firsts encrypts the message using Bob‟s public key. To decrypts the message, Bob uses his own private key.

- **Hashing**

In hashing, a fixed-length message digest is created out of a variable-length message. The digest is normally much smaller than the message. To be useful, both the message and the digest must be sent to Bob. Hashing is used to provide check values, which were discussed earlier in relation to providing **data integrity**.

2.3.2 Steganography

This is the art of hiding messages in another form. Message is not altered as in encryption. A text can hide a message. For example, “red umbrella needed” may mean the message “run”. The first letter of each word in the text becomes the message. An image can also be used for hiding messages. Digital images are after all binary information. Suppose the image is grey image. The least significant bit of consecutive eight pixels may be altered to be a specific bit pattern of a character. We will discuss this technique of steganography in detail in the unit to come.