Lecture 3

Security services

- **Definition**
  - It is a processing or communication service that is provided by a system to give a specific kind of protection to a system resources.

Five categories :-

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Nonrepudiation

Security Services: Cont..

- **Authentication**
  - Is an assurance that the communicating entity is the one that claims to be
  - Two types
    - **Peer Entity Authentication**
      - Used in association with logical connection to provide confidence in the identity of the entities connected.
    - **Data origin Authentication**
      - In a connectionless transfer, it provides a assurance that the source of received data is as claimed.

Example: Windows Authentication: User/Group Authentication using Active Directory, Domains and Data file authentication using rights

Security Services: Cont..

- **Access Control**
  - Is a prevention of unauthorized use of a resource
  - This service controls
    - who can have a access to a resource,
    - under what conditions access can occur,
    - what those accessing the resource are allowed to do

Security Services: Cont..

- **Data Confidentiality**
  - is the protection of data from unauthorized leak (Disclosure)
  - Has tow types
    - **Connection Confidentiality**
      - Protection of all users data on connection
    - **Connectionless Confidentiality**
      - Protection of all user data in a single block

Security Services: Cont..

- **Data Integrity**
  - Is the assurance that the data received are exactly as sent by an authorized entity
  - Will not allow any modification, insertion, deletion.

Security Services: Cont..

- **Nonrepudiation**
  - Provides protection against denial of any one of the entities involved in communication having participated in communication
  - Has two types
    - **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 Mechanism

- Security mechanism are defined by X.800
  - Implemented by
    - Encipherment
    - Digital signature
    - Access Control
    - Data Integrity
    - Authentication exchange
    - Traffic padding
    - Routing control
    - Notarization

Security Mechanism: Cont.

- Encipherment
  - Use of Mathematical algorithm to transforms data into a form that is not readily intelligible.
  - The transformation is depend upon algorithm and zero, one or more encryption keys.
- Digital Signature
  - It allows a recipient of data unit to prove the data source and integrity of the data unit and protect against unauthorized modification.

Security Mechanism: Cont.

- Access Control
  - Provides access rights to resources (device, files, storage etc)
- Data Integrity
  - Used to assure the integrity of a data unit by means of information exchange.
- Authentication Exchange
  - Identify an entity by means of information exchange.

Security Mechanism: Cont.

- Traffic Padding
  - Insertion of bits in to gaps of data stream to frustrate traffic analysis attempts.
- Routing Control
  - Enables selection of particular physically secured routes for certain data and allows routing changes especially when a breach of security is suspected.
- Notarization
  - Use of trusted third party to assure certain properties of data exchange.

Relationship between security services and mechanism

		Mechanism							
	Service	Encipherment	Digital Signature	Access Control	Data Integrity	Application Exchange	Traffic Padding	Routing Control	Notarization
Security service	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				
	Nonrepudiation		Y		Y				Y
	Availability					Y			