



Information Security Systems

EC-615-F

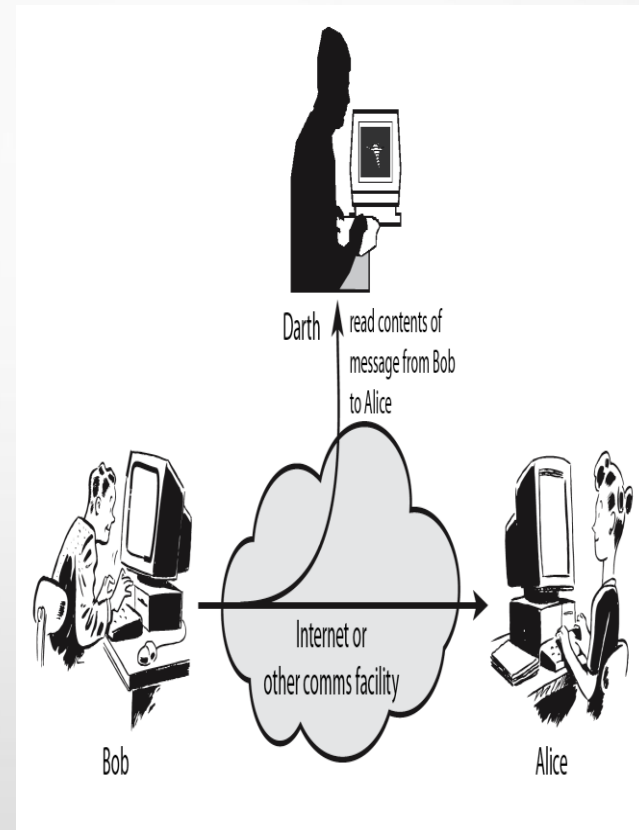
Lecture No 3

Topics To be Covered

❖ Security Attacks

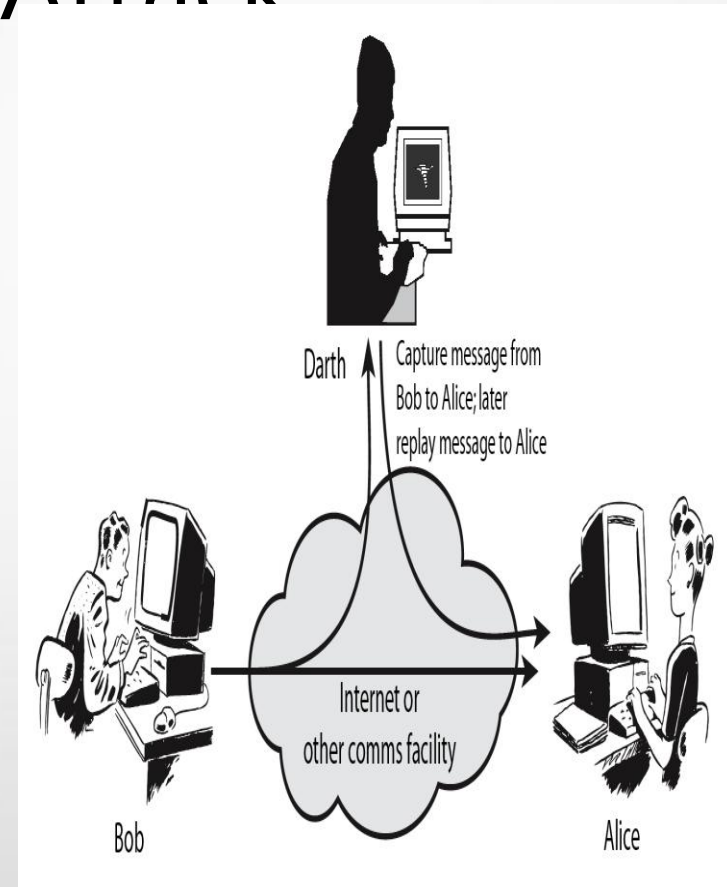
Security Attack

- **Passive Attack**
 - attempts to learn or make use of information from the system but does not affect system resources.
- Two types of passive attacks are:
 1. Release of message contents
 2. Traffic analysis.



Active Attack

- **Active Attack**
 - modification of the data stream or the creation of a false stream
- Four types of active attacks
 1. masquerade,
 2. Replay
 3. modification of messages,
 4. denial of service.



OSI Security Structure

- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- Define Security Services and mechanism

OSI Security Structure – Security Services

- **Authentication** (التثبت من الهوية) - assurance that communicating entity is the one claimed
 - have both peer-entity & data origin authentication
- **Access Control** (التحكم في الوصول) - prevention of the unauthorized use of a resource
- **Data Confidentiality** (سريّة المعلومات) – protection of data from unauthorized disclosure
- **Data Integrity** (التأكد من صحة المعلومات) - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** (عدم الإنكار) - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

OSI Security Structure – Security Mechanism

- specific security mechanisms (OSI model)
 - Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

OSI Security Structure – Security Mechanism

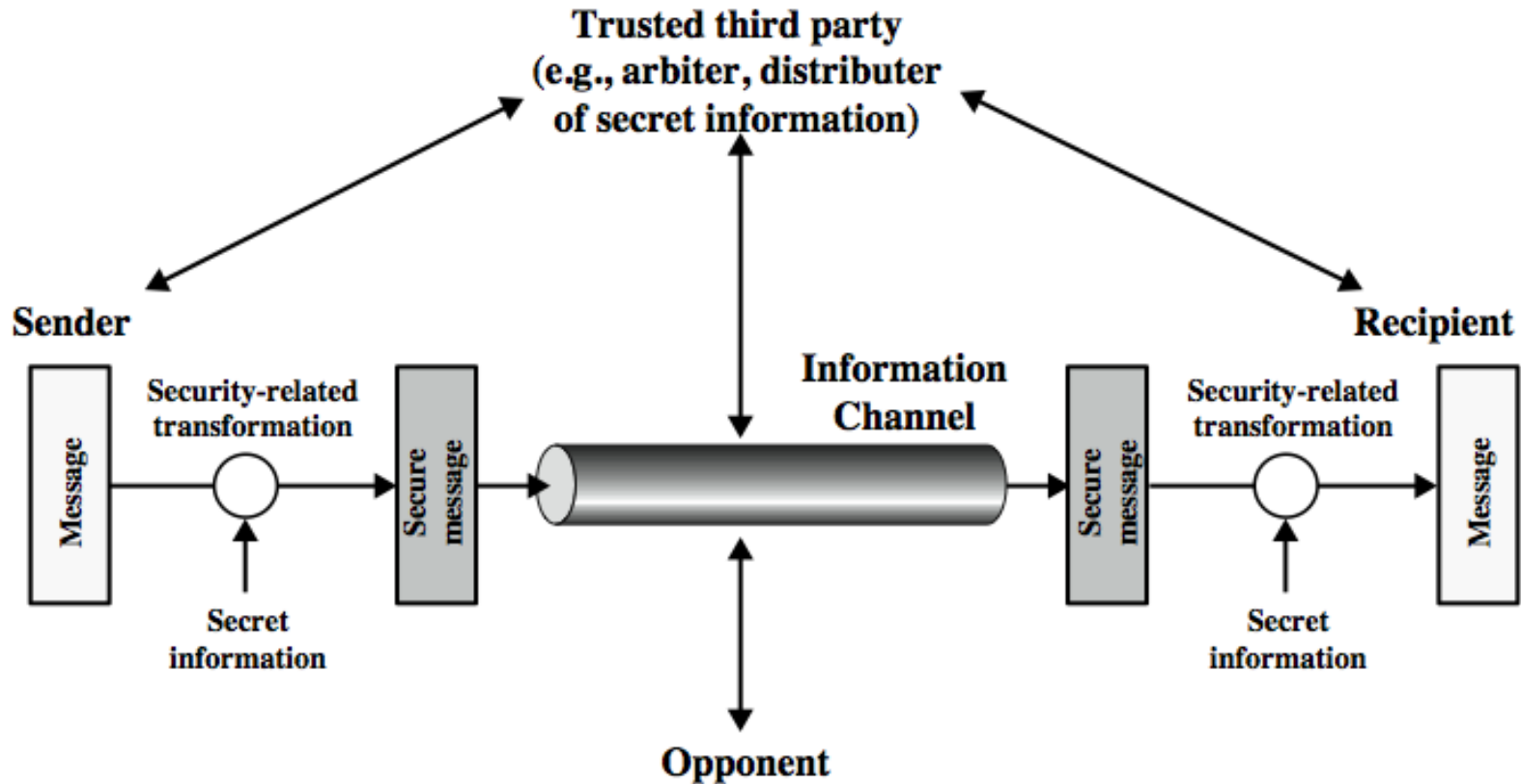
Table 1.4 Relationship Between Security Services and Mechanisms

Service	Mechanism					
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Notari- zation
Peer entity authentication	Y	Y			Y	
Data origin authentication	Y	Y				
Access control			Y			
Confidentiality	Y					
Data integrity	Y	Y		Y		
Nonrepudiation		Y		Y		Y
Availability				Y	Y	

OSI Security Structure – Security Mechanism

- pervasive security mechanisms:
 - trusted functionality: functionality that can be trusted to perform as intended.
 - security labels: every item is associated with a security label. For example : a label for sensitivity level.
 - event detection : detective and could be corrective mechanism m for security event.
 - security audit trails: Review and Examination of system records and activities
 - security recovery : implementing corrective security mechanisms and putting them in appropriate place.

Model for Network Security

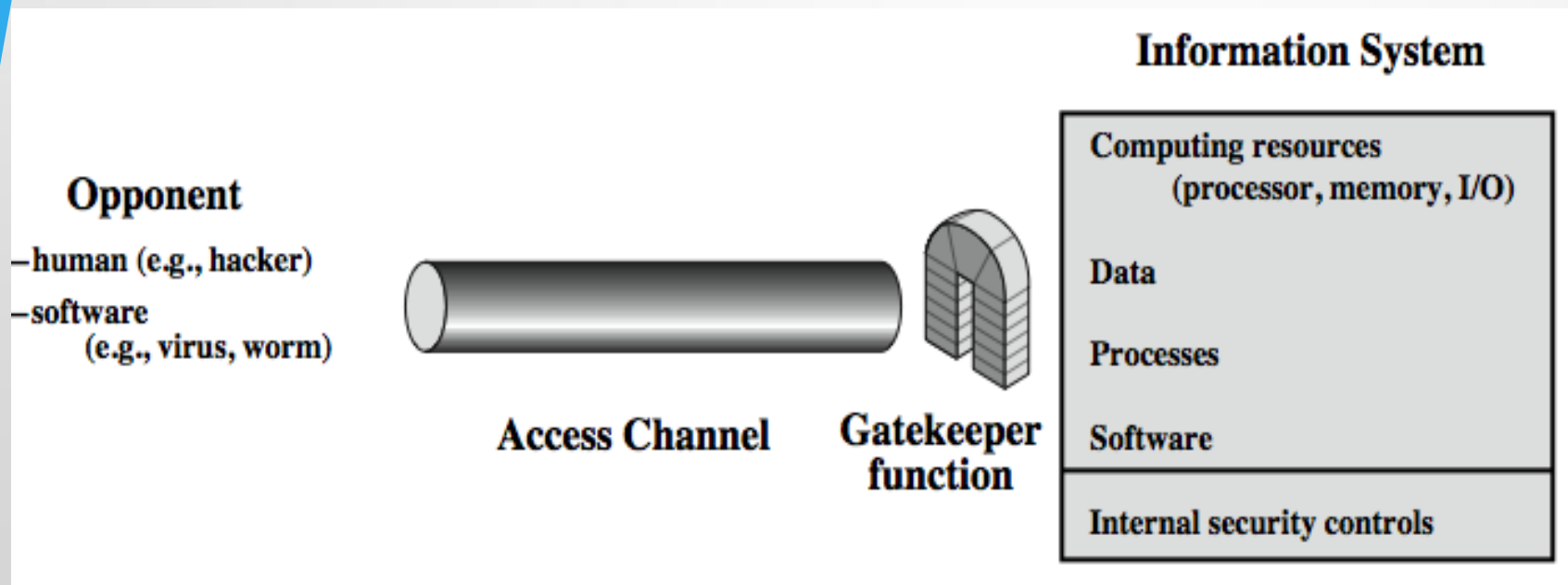


Model for Network Security

using this model requires us to:

1. design a suitable algorithm for the security transformation
2. generate the secret information (keys) used by the algorithm
3. develop methods to distribute and share the secret information
4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Security



Model for Network Security

using this model requires us to:

1. select appropriate gatekeeper functions to identify users
2. implement security controls to ensure only authorised users access designated information or resources