Basic concepts in Security

CNS, sections 2.1 – 2.2
NSE, sections 1.1 – 1.4

Security Architecture for OSI

- ITU-T Recommendation X.800, *Security Architecture for OSI* defines systematic way to
  - *Defining the requirements for security*
  - *Characterizing the approaches to satisfying those requirements*

ITU-T – international Telecommunication Union Telecommunication Standardization Sector

OSI – Open Systems Interconnection – an effort started in 1977 to standardize computer networking

OSI Security Architecture

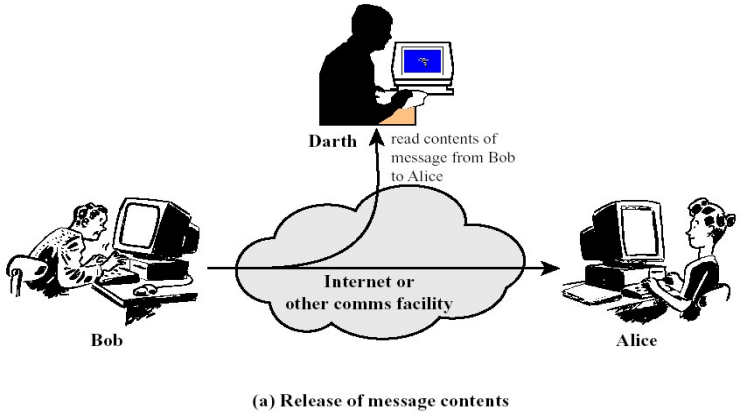
- **The following concepts are used:**

- **Security attack:** Any actions that compromises the security of information owned by an organization (or a person)
- **Security mechanism:** a mechanism that is designed to detect, prevent, or recover from a security attack
- **Security service:** a service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service

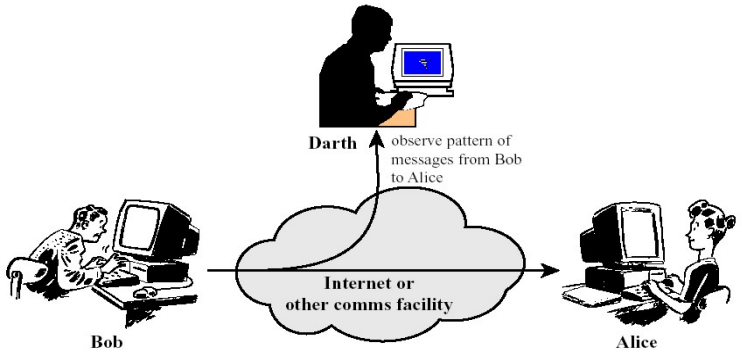
Security attacks

- **Passive attack:** aims to learn or make use of information from the system but does not affect system resources.
- **Active attack:** attempts to alter system resources or affect their operation

Passive attacks



(a) Release of message contents



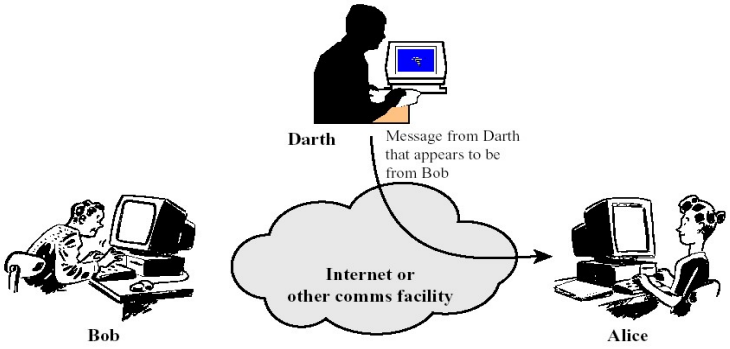
(b) Traffic analysis

Figure 1.1 Passive Attacks

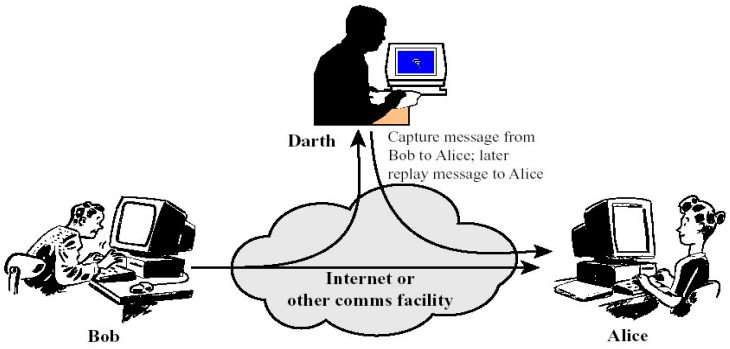
How to deal with?

Prevention rather than detection.

Active Attacks

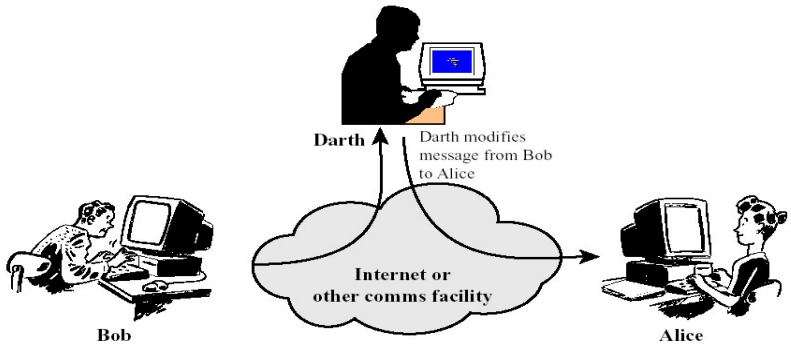


(a) Masquerade

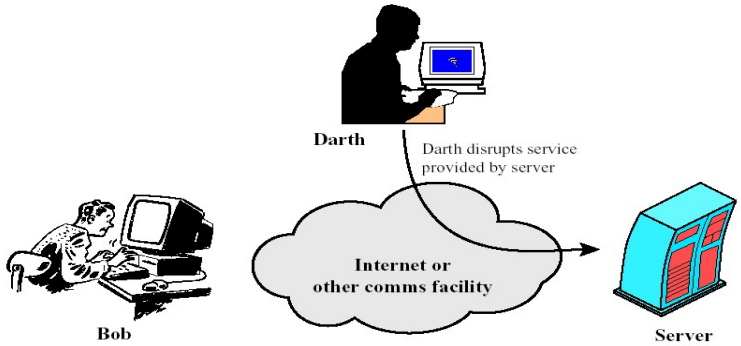


(b) Replay

Figure 1.2 Active Attacks (page 1 of 2)



(c) Modification of messages



(d) Denial of service

Figure 1.2 Active Attacks (page 2 of 2)

Active Attacks

- How to deal with?

- Detect and recover from disruption or delay
- It is more feasible than prevention

Security services/security attributes

- Security service is a service which ensures adequate security (a particular *security attribute*) of the systems or of data transfers
- X.800 Recommendation divides security services into 5 categories:
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - *Availability service*

Authentication

- The authentication service is concerning with
- assuring that a communication is authentic:
  - The recipient of the message should be sure that the message came from the source that it claims to be
  - All communicating parties should be sure that the connection is not interfered with by unauthorized party.
- **Example:** consider a person, using online banking service. Both the user and the bank should be assured in identities of each other

Access control

- This service controls
  - who can have access to a resource;
  - under what conditions access can occur;
  - what those accessing are allowing to do.

- **Example:** in online banking a user may be allowed to see his balance, but not allowed to make any transactions for some of his accounts

Data confidentiality

- The protection of data from unauthorized disclosure
- (from passive attacks).
  - Connection confidentiality
  - Connectionless confidentiality
  - Selective field confidentiality
  - Traffic-Flow Confidentiality

Data Integrity

- The assurance that data received are exactly as sent by an authorized entity, i.e. contain
  - no modification
  - no insertion
  - no deletion
  - no replay
- Protection from active attacks
- It may be
  - integrity with recovery, or
  - Integrity without recovery (detection only)

Nonrepudiation

- Protection against denial by one of the entities involved in a communication of having participated in the communication.
- Nonrepudiation can be related to
  - Origin: proof that the message was sent by the specified party
  - Destination: proof that the message was received by the specified party

- **Example**: Imagine a user of online banking who has made a transaction, but later denied that. How the bank can protect itself in a such situation?
-

Availability service

- Protects a system to ensure its availability
- Particularly, it addresses denial-of-service attacks
- Depends on other security services: access control, authentication, etc

Attacks and Security services

	Attack					
Service	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation						
Availability						Y

Security mechanisms

- Security mechanisms are used to implement security services. They include (X.800):
- Encipherment
- Digital signature
- Access Control mechanisms
- Data Integrity mechanisms
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarisation