Chapter 1

Information and Network
Security Concepts

Cybersecurity

Cybersecurity *is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets.*

Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment.

The general security objectives comprise the following: availability; integrity, which may include data authenticity and nonrepudiation; and confidentiality

Security Objectives

- The cybersecurity definition introduces three key objectives that are at the heart of information and network security:

  - **Confidentiality:** This term covers two related concepts:

    - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals

    - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Security Objectives

- **Integrity:** This term covers two related concepts:

    - **Data integrity:** Assures that data and programs are changed only in a specified and authorized manner. This concept also encompasses data authenticity, which means that a digital object is indeed what it claims to be or what it is claimed to be, and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information

    - **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

- **Availability:** Assures that systems work promptly and service is not denied to authorized users
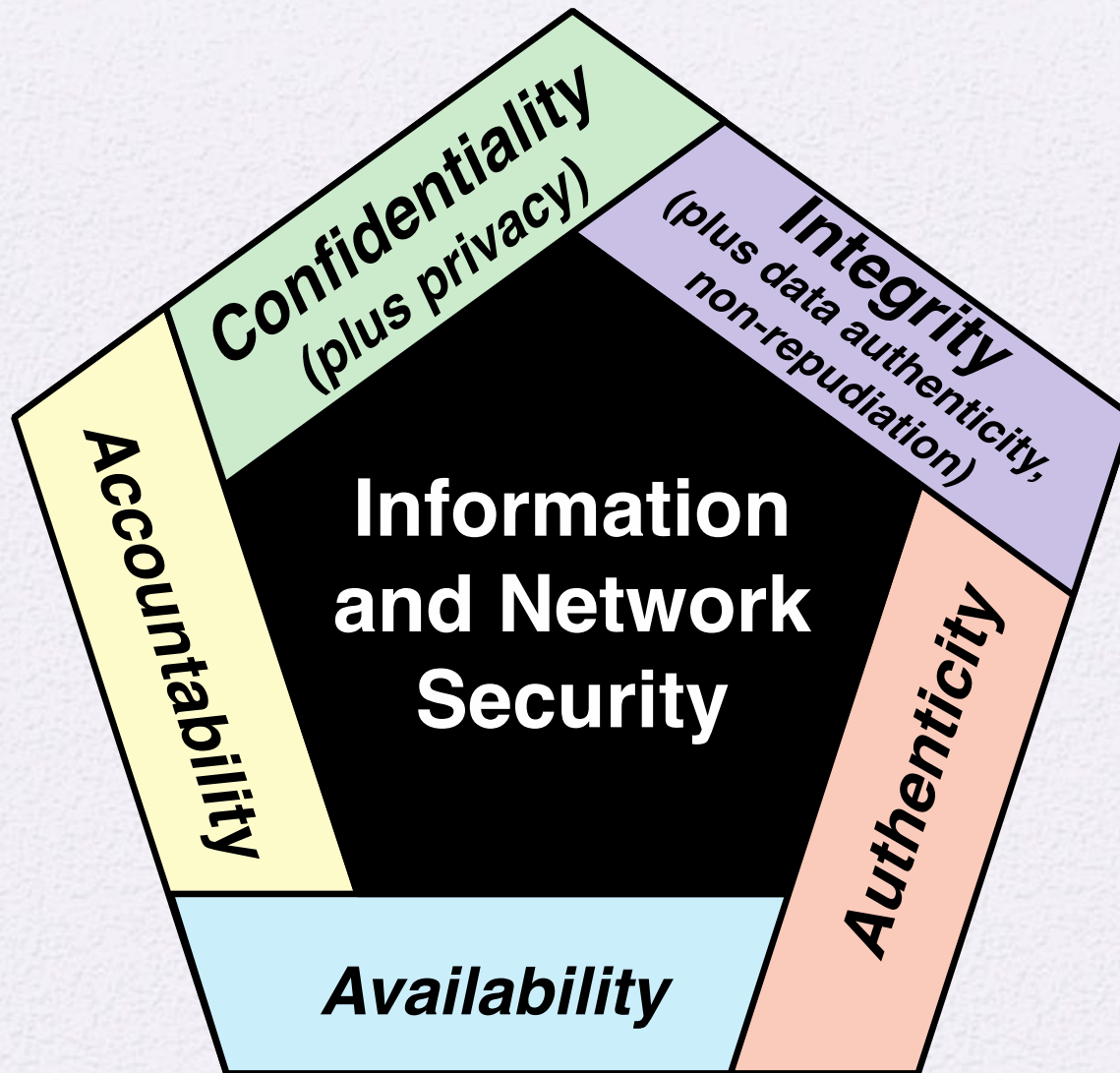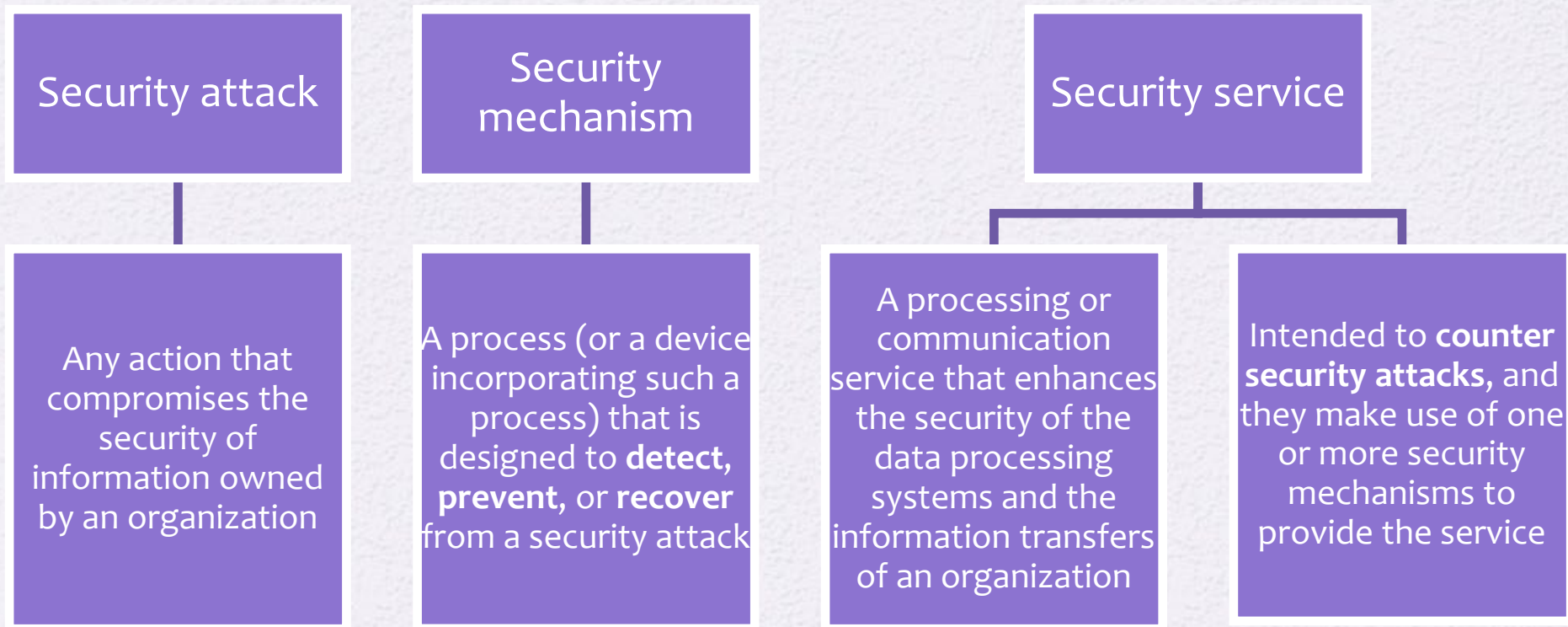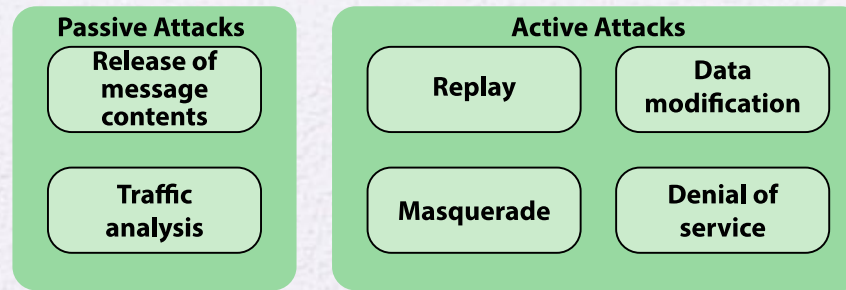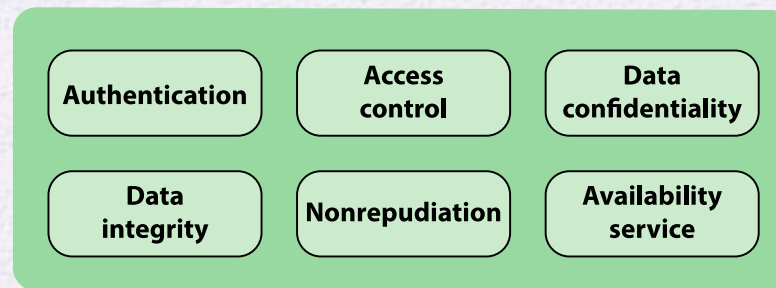
Figure 1.1 Essential Information and Network Security Objectives
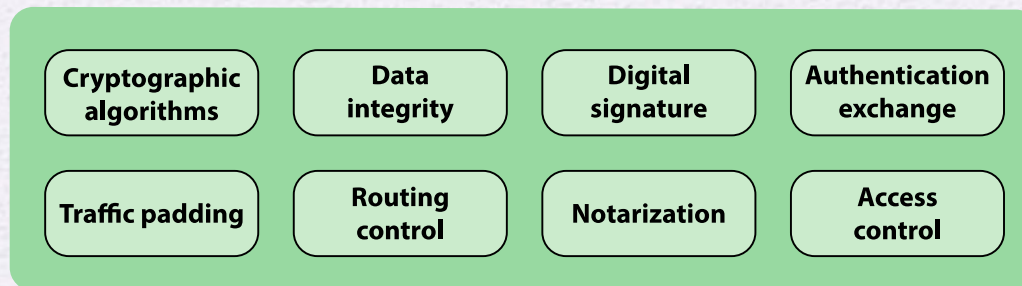
OSI Security Architecture

Security attack	Security mechanism	Security service	
Any action that compromises the security of information owned by an organization	A process (or a device incorporating such a process) that is designed to **detect**, **prevent**, or **recover** from a security attack	A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization	Intended to **counter security attacks,** and they make use of one or more security mechanisms to provide the service

(a) Attacks

(b) Services

(c) Mechanisms

Figure 1.2 Key Concepts in Security

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*

- **A *passive attack*** attempts to learn or make use of information from the system but does not affect system resources

- **An *active attack*** attempts to alter system resources or affect their operation

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions

- Goal of the opponent is to obtain information that is being transmitted

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream

- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities

- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade
- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay
- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Data Modification
- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service
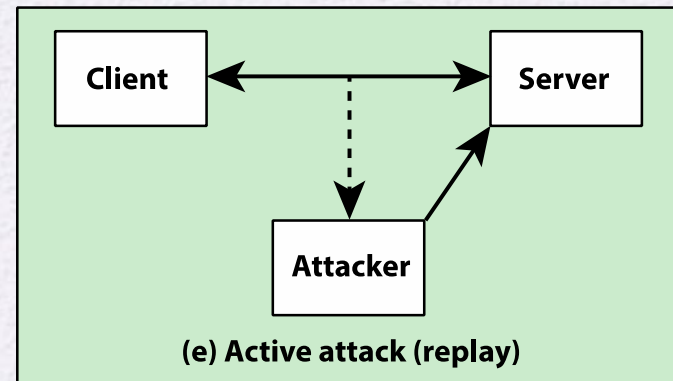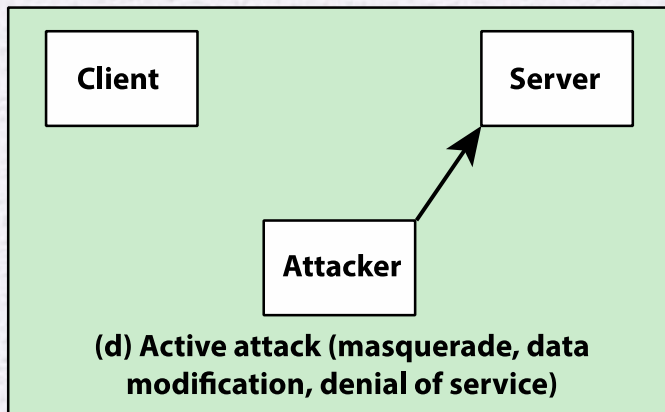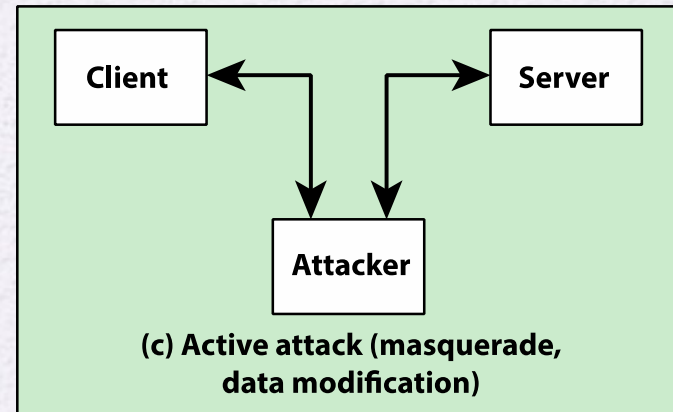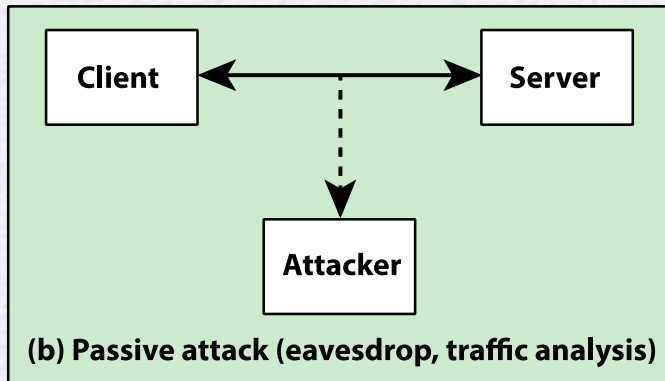- Prevents or inhibits the normal use or management of communications facilities

Figure 1.3 Security Attacks

Security Services

Authentication

Access control

Data confidentiality

Data integrity

Nonrepudiation

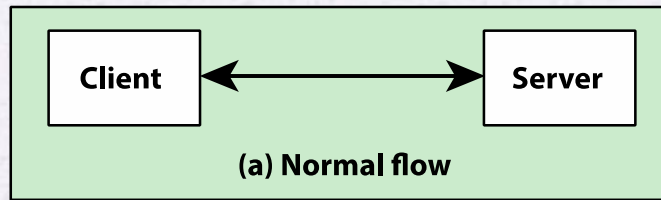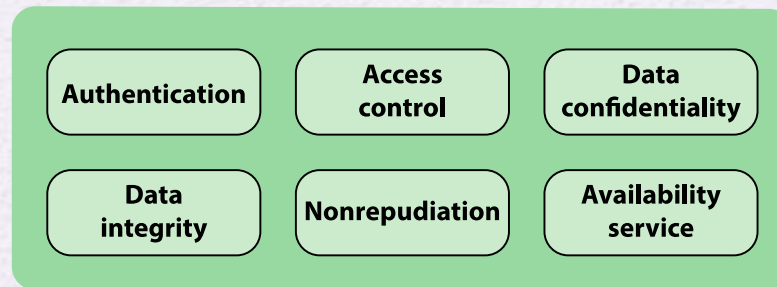Availability service

(b) Services

Authentication

- Concerned with assuring that a communication is authentic

  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from

  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:
• Peer entity authentication • Data origin authentication

Authentication

- ## Peer entity authentication
  - Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement the same protocol in different systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection

- ## Data origin authentication
  - Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no ongoing interactions between the communicating entities

Access Control

- The ability to limit and control the access to host systems and applications via communications links

- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual

Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message

- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity

Can apply to a stream of messages, a single message, or selected fields within a message

Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message

- When a message is sent, the receiver can prove that the alleged sender in fact sent the message

- When a message is received, the sender can prove that the alleged receiver in fact received the message

Availability Service

- Protects a system to ensure its availability

- This service addresses the security concerns raised by **denial-of-service attacks**

- It depends on proper management and control of system resources and thus depends on access control service and other security services

Security Mechanisms

- **Cryptographic algorithms:** We can distinguish between reversible cryptographic mechanisms and irreversible cryptographic mechanisms. A reversible cryptographic mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible cryptographic mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

- **Data integrity:** This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

- **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.

- **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 or logically 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

- **Access control:** A variety of mechanisms that enforce access rights to resources.

Summary

- Describe the key security requirements of confidentiality, integrity, and availability

- List and briefly describe key organizations involved in cryptography standards

- Provide an overview of keyless, single-key and two-key cryptographic algorithms

- Provide an overview of the main areas of network security

- Describe a trust model for information security

- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets