# Computer and Network Security Concepts

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Definitions

- Measures to deter, prevent, detect, and correct security violations that involve the transmission of information

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources
  - Hardware – Software – firmware - information/data - telecommunications

# Cryptographic algorithms and protocols

## Data Encryption

- Used to conceal the contents of data, including messages, files,  and passwords

## Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

## Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

# Objectives

## Confidentiality

- **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

## Integrity

- **Data integrity:** Assures that  information and programs are changed only in a specified and authorized manner
- **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

# Security Requirements (CIA)

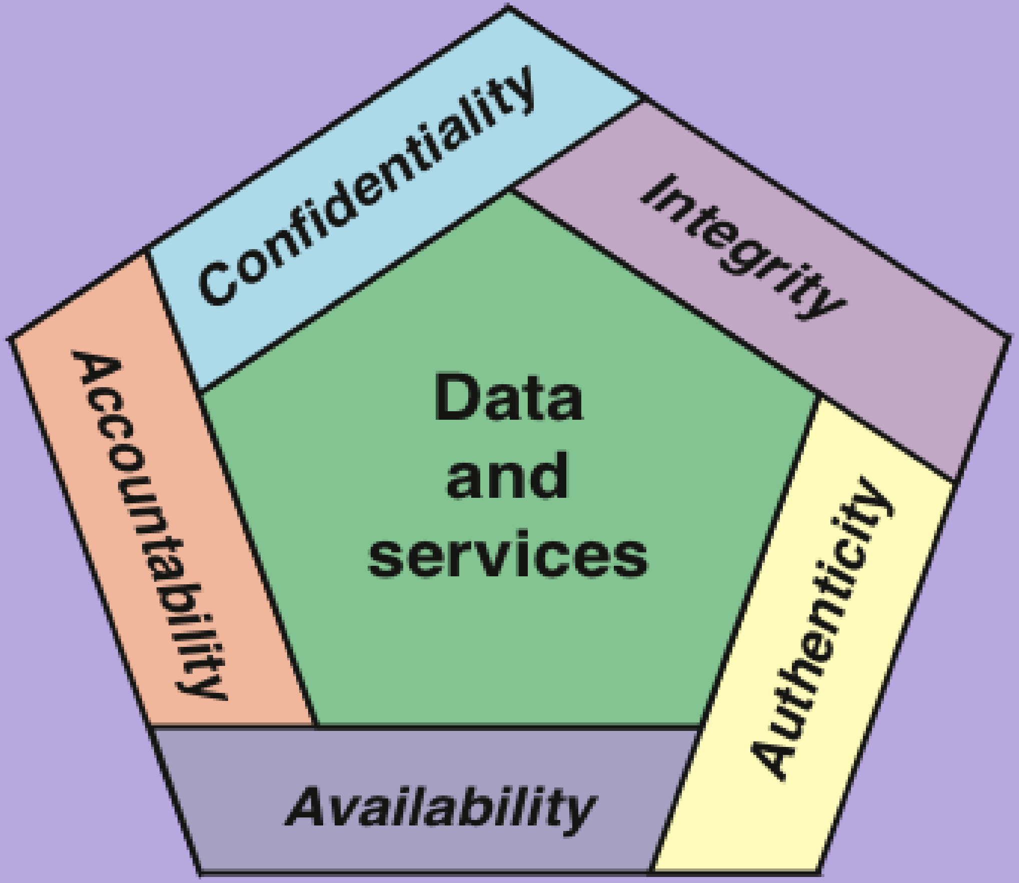


**Figure 1.1 Essential Network and Computer Security Requirements**

# Security Requirements(CIA)

1. **Confidentiality:**

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

# Security Requirements(CIA)

**2- Integrity:**

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

# Security Requirements(CIA)

**3- Availability:**

- Ensuring timely and reliable access to and use of information.
- A loss of availability is the disruption of access to or use of information or an information system.

# Security Requirements(CIA)

**4. Authenticity**:

- The property of being genuine and being able to be verified and  trusted; confidence in the validity of a transmission, a message, or message originator.
- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

# Security Requirements(CIA)

**5. Accountability**:

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.

# Challenges

1. Security is not as simple as it might first appear to the novice.
2. Successful attacks are designed by looking at the problem of a particular security mechanism or algorithm
4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense
5. The creation, distribution, and protection of that secret information such as encryption key.

# Challenges

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
8. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

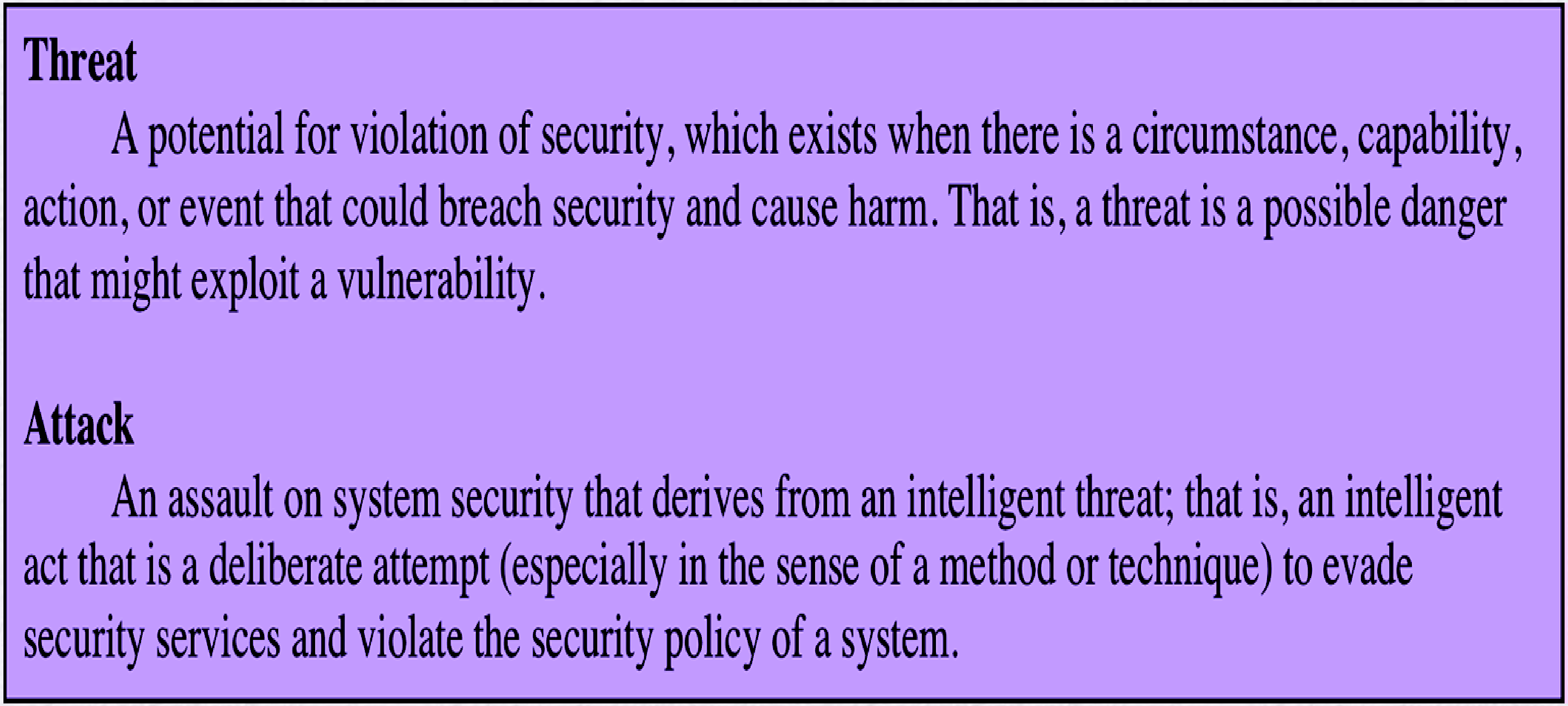
# OSI Security Architecture

- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process  that is designed to detect, prevent, or recover from a security attack
- Security service
  - 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

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Threats and Attacks



**Threat**

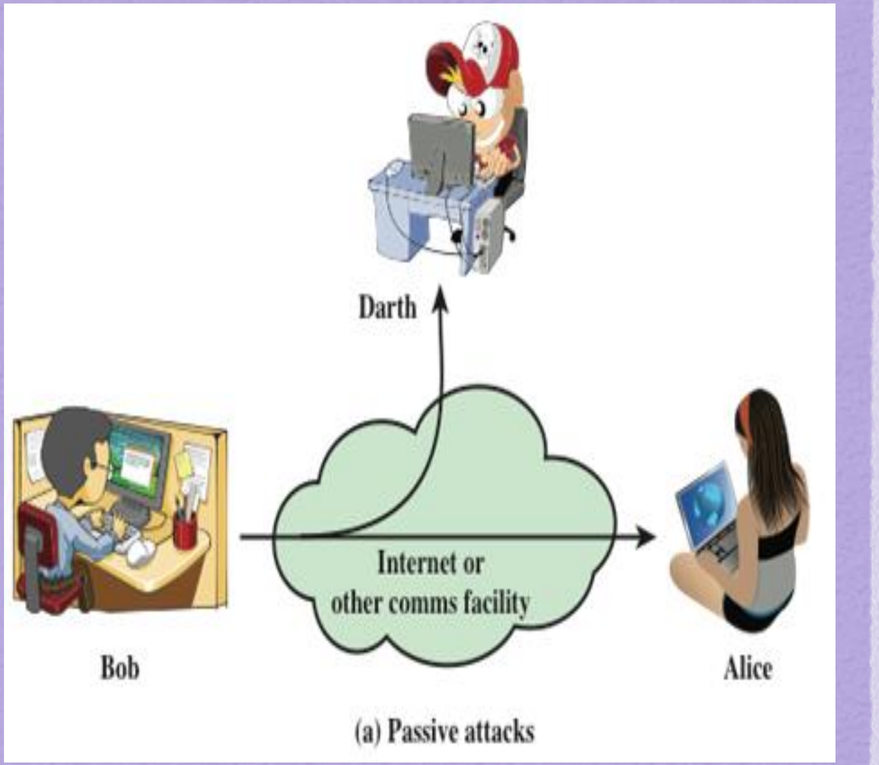
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

**Attack**

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

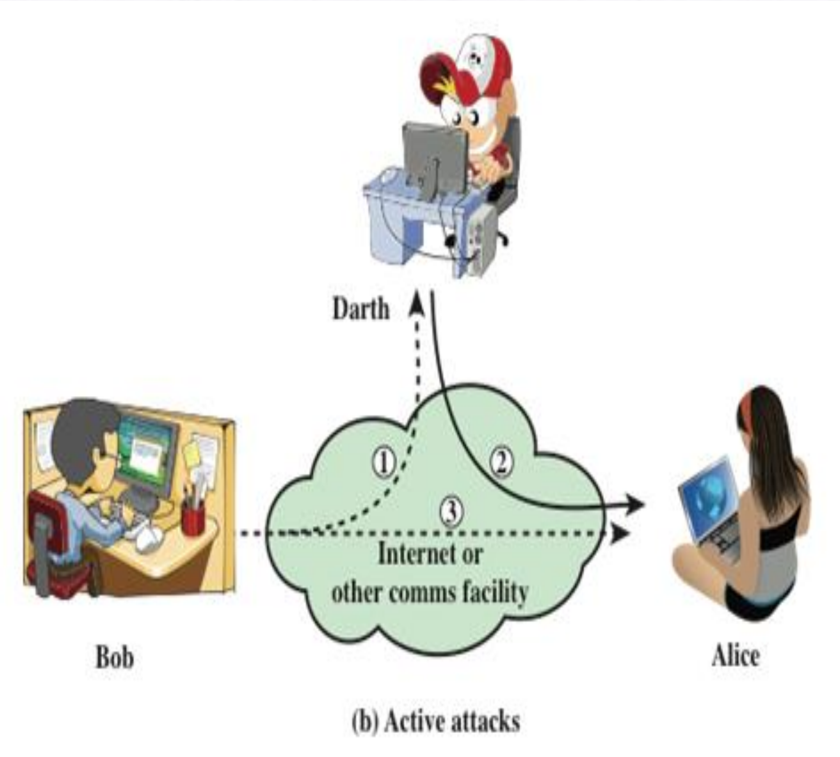
# Security Attacks

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



(a) Passive attacks

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



(b) Active attacks

# 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

**Modification of messages**

- 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

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Security Services

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

# 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

# Access Control

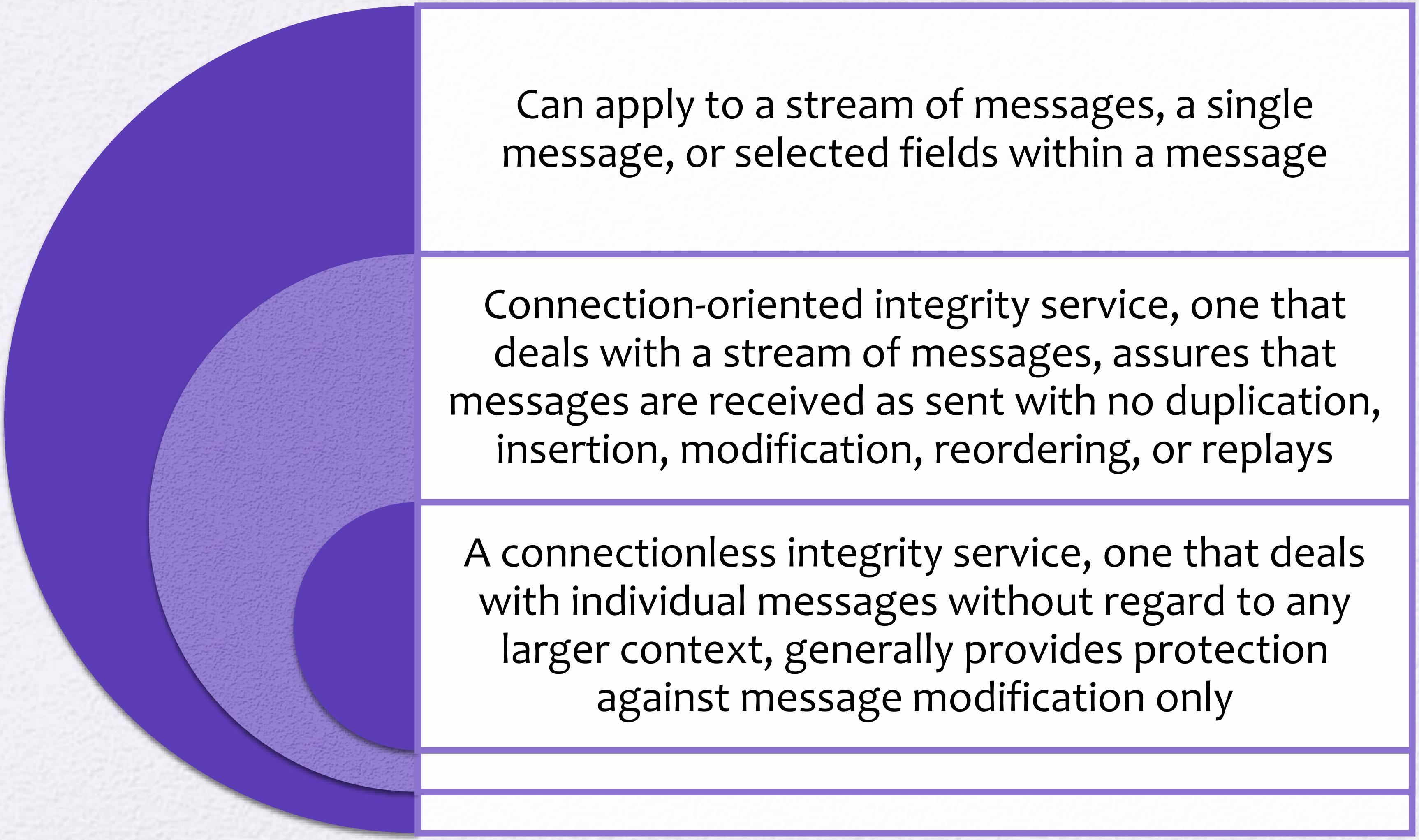
- The ability to limit and control the access to host systems and applications via communications links

- 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

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Model for Network Security

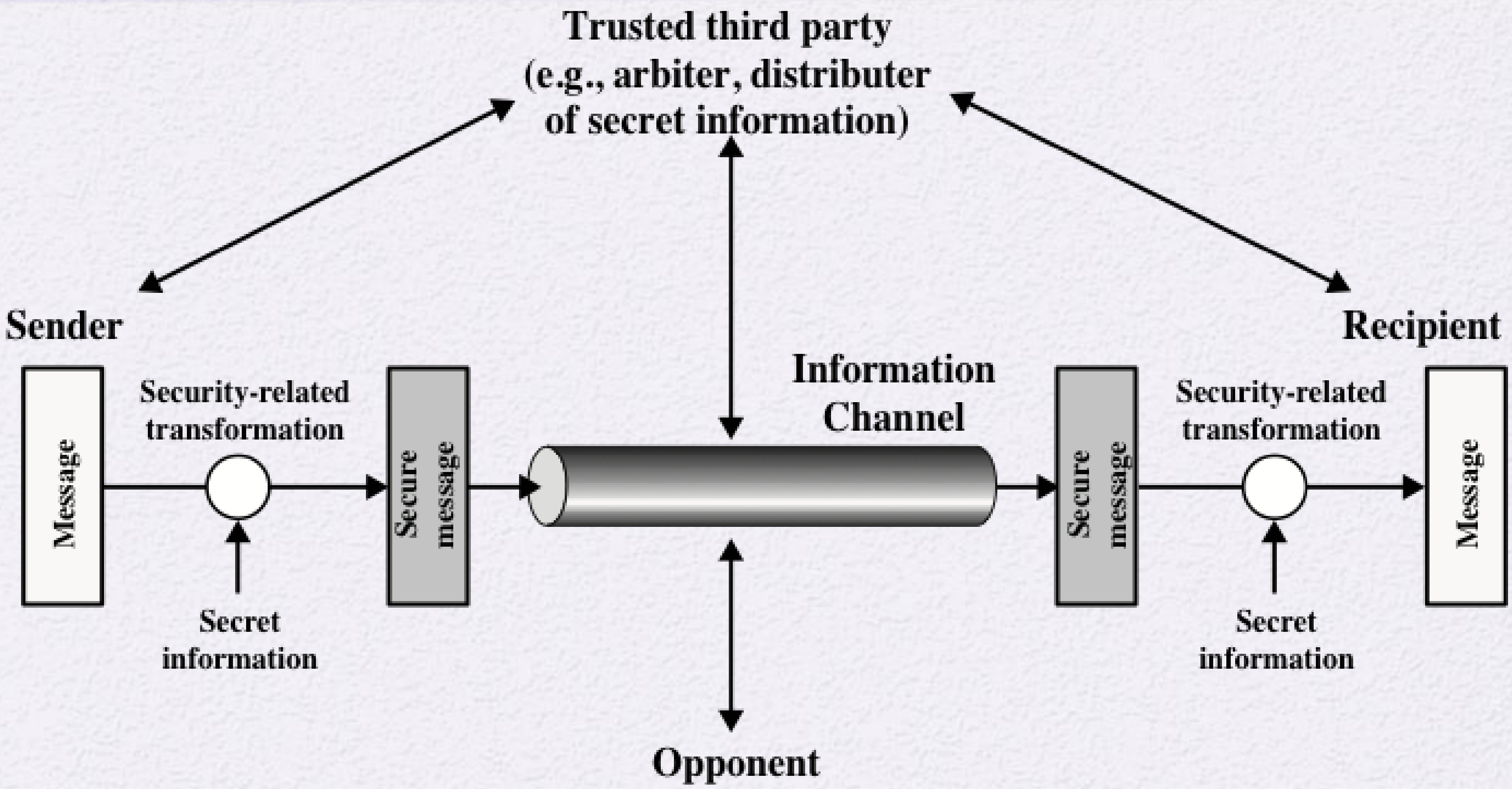


Figure 1.5 Model for Network Security

# Network Access Security Model

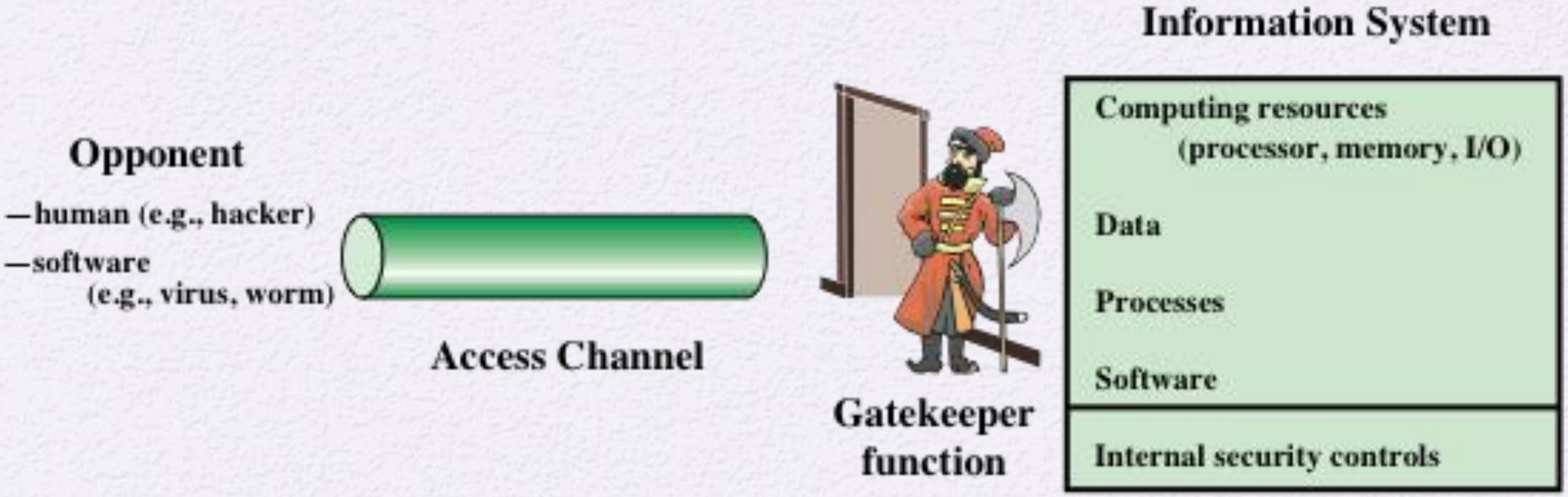


Figure 1.6 Network Access Security Model

# Agenda

1. Computer security concepts
2. The OSI security architecture
3. Security attacks
4. Security services
5. Network security model
6. Standards

# Standards

## National Institute of Standards and Technology

- NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation
- Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

# Standards

## Internet Society

- ISOC is a professional membership society with world-wide organizational and individual membership
- Provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards

# Standards

## ITU-T

- The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services
- The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU and whose mission is the development of technical standards covering all fields of telecommunications

# Standards

## ISO

- The International Organization for Standardization is a world-wide federation of national standards bodies from more than 140 countries
- ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity

Thanks