National Chung Cheng University

Department of Information Management

Information Security Overview

Pei-Ju (Julian) Lee

National Chung Cheng University

Information Security

pjlee@mis.ccu.edu.tw

Fall, 2016

Focus areas

- Two areas of this book:
  - Cryptographic algorithms and protocols
  - Network and Internet security

Cryptographic algorithms and protocols

- Symmetric encryption
  - Used to conceal the contents of blocks or streams of data of any size
    - E.g. messages, files, encryption keys, passwords
- Asymmetric encryption
  - To conceal small blocks of data
    - E.g. encryption keys, hash function values
- Data integrity algorithms
  - To protect blocks of data from alteration
- Authentication protocols
  - Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

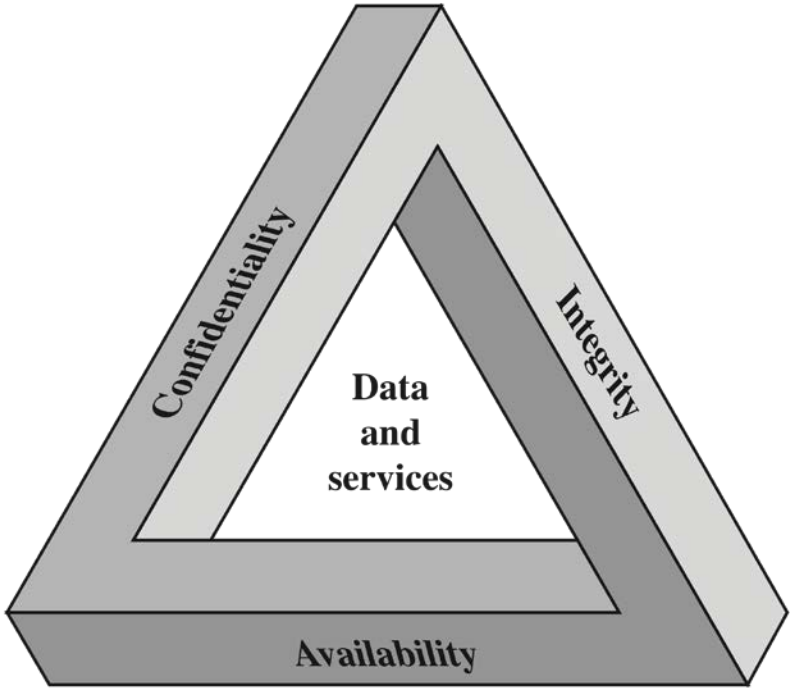
Computer Security

- The NIST *Computer Security Handbook* defines the term Computer Security as:
  - "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" (includes hardware, software, firmware, information/ data, and telecommunications)

- NIST: National Institute of Standards and Technology
  (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.

Computer Security Objectives

- Confidentiality
  - Data confidentiality
  - Privacy
- Integrity
  - Data integrity
  - System integrity
- Availability
- Authenticity
- Accountability



- CIA triad (NIST standard FIPS 199)

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

OSI Security Architecture

- OSI (Open Systems Interconnection)
  - Useful to managers to organize the task of providing security and to vendors to develop their security features under the same international standard
- Focus on:
  - Security Attack
    - Any action that compromises the security of information owned by an organization
  - Security Service
    - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Security Mechanism
    - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack

1. Security Attacks

- Passive attack

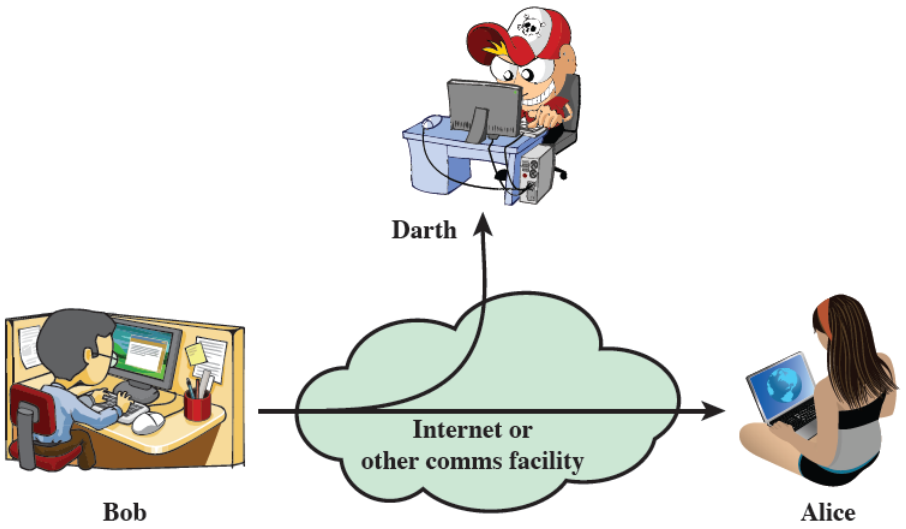
Attempts to learn/make use of information from the system but does not affect system resources
Ex. Eavesdropping, monitoring

– Type1.The release of message contents

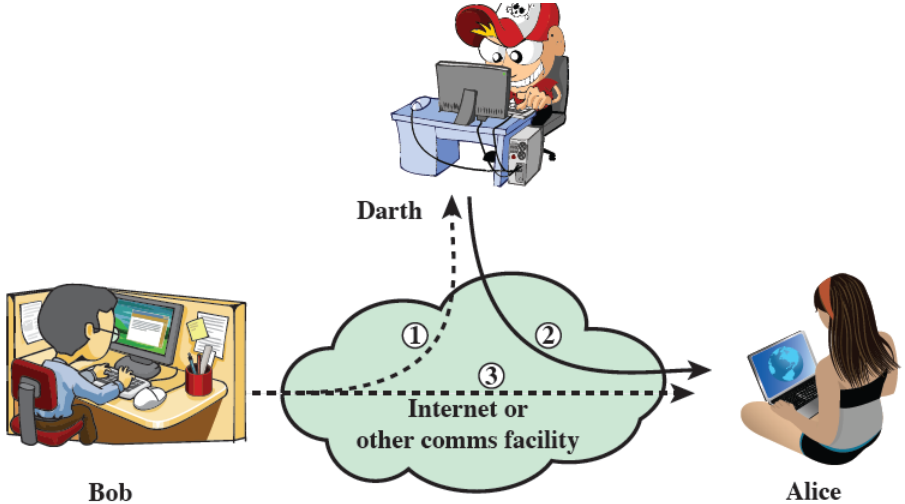
– Type2.Traffic analysis

- Active attack

Attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Active Attacks

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

Active Attacks(cont'd)

- Involve some modification of the data stream or the creation of a false stream
  - Whereas passive attacks are difficult to detect, measures are available to prevent their success
- 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

2. Security Services (SS)

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

- Categories:
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation

Authentication (SS.1)

- 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 Services

- Peer entity authentication:
  - Provides for the corroboration of the identity
  - Peers: if two entities implement to same protocol in different systems E.g. two TCP modules in two communicating systems
  - Use at the establishment of a connection or during the data transfer phase
  - Prevent masquerade or an unauthorized replay of a previous connection
- Data origin authentication:
  - Corroboration of the source of a data unit
  - Does not provide protection against the duplication or modification of data units.

Access Control (SS.2)

- 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 **identified**, or **authenticated**, so that access rights can be tailored to the individual

Data Confidentiality (SS.3)

- 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 (SS.4)

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

Most useful: **total stream protection**

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

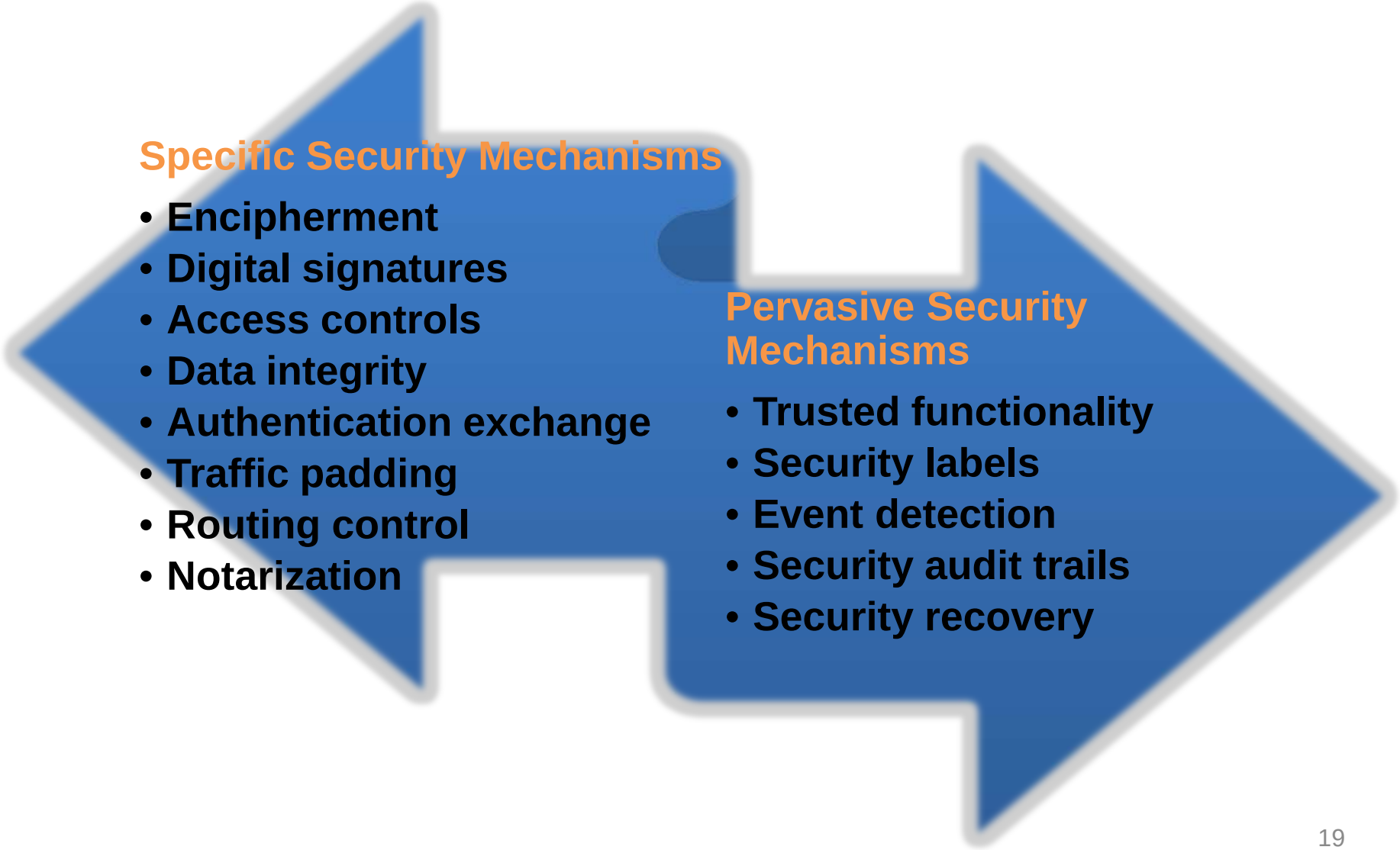
Nonrepudiation (SS.5)

- 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

Table 1.2 Security Services (X.800)

AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-Origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-Flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

3. Security Mechanisms (X.800)



Specific Security Mechanisms

- Encipherment
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible
- Digital signatures
  - Data appended to a data unit that allows a recipient to prove the source and integrity of the data unit and protect against forgery
- Access controls
  - Enforce access rights to resources

Cont'd

- Data integrity
  - To assure the integrity of a data unit
- Authentication exchange
  - To ensure the identity of an entity
- Traffic padding
  - The insertion of bits into a data stream to frustrate traffic analysis attempts
- Routing control
  - Enables selection of particular physically secure routes for certain data
- Notarization
  - The use of a trusted third party to assure certain properties of a data exchange

Security Mechanisms

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

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 (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

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 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.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Security Services and Mechanisms

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
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				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

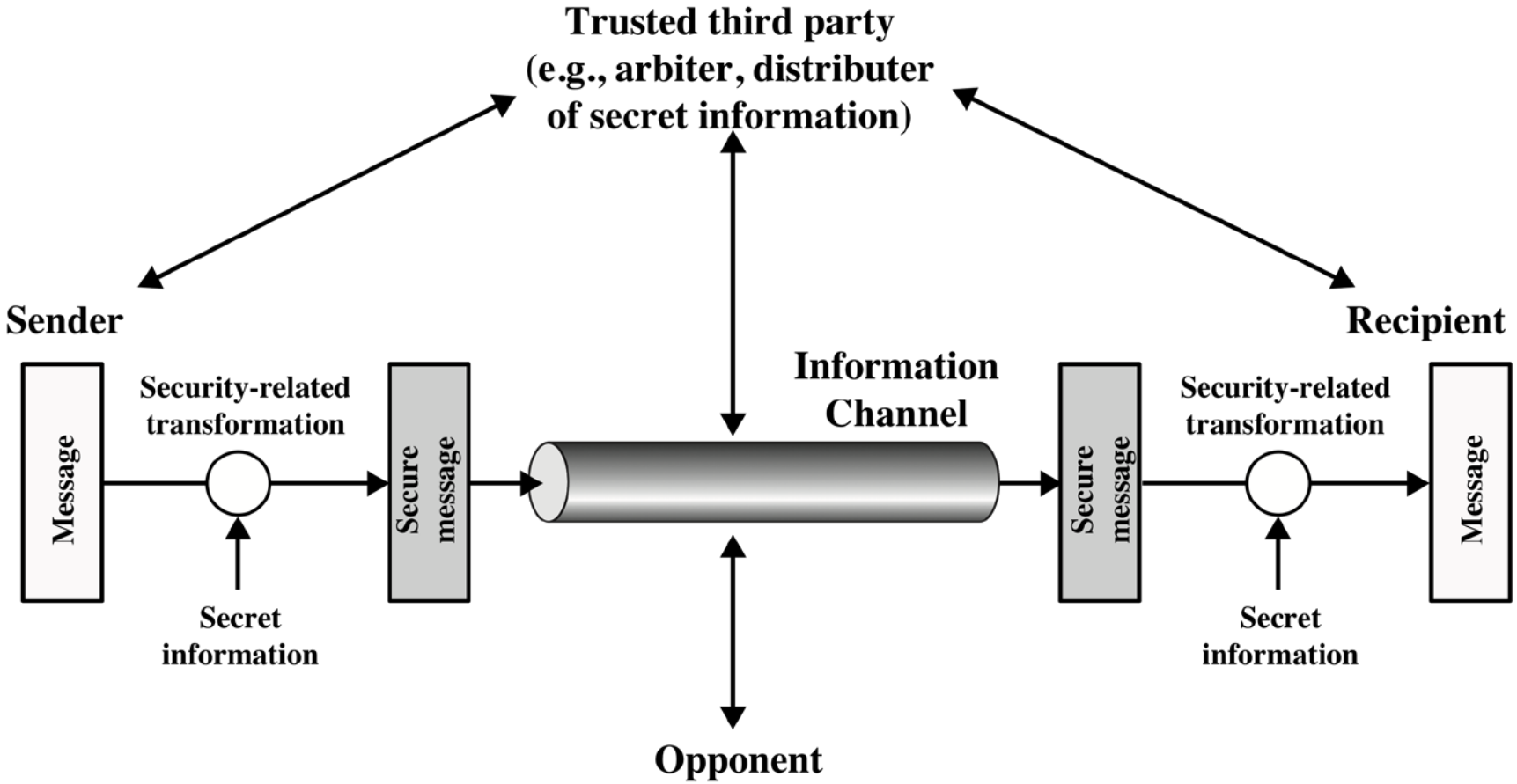


Figure 1.2 Model for Network Security

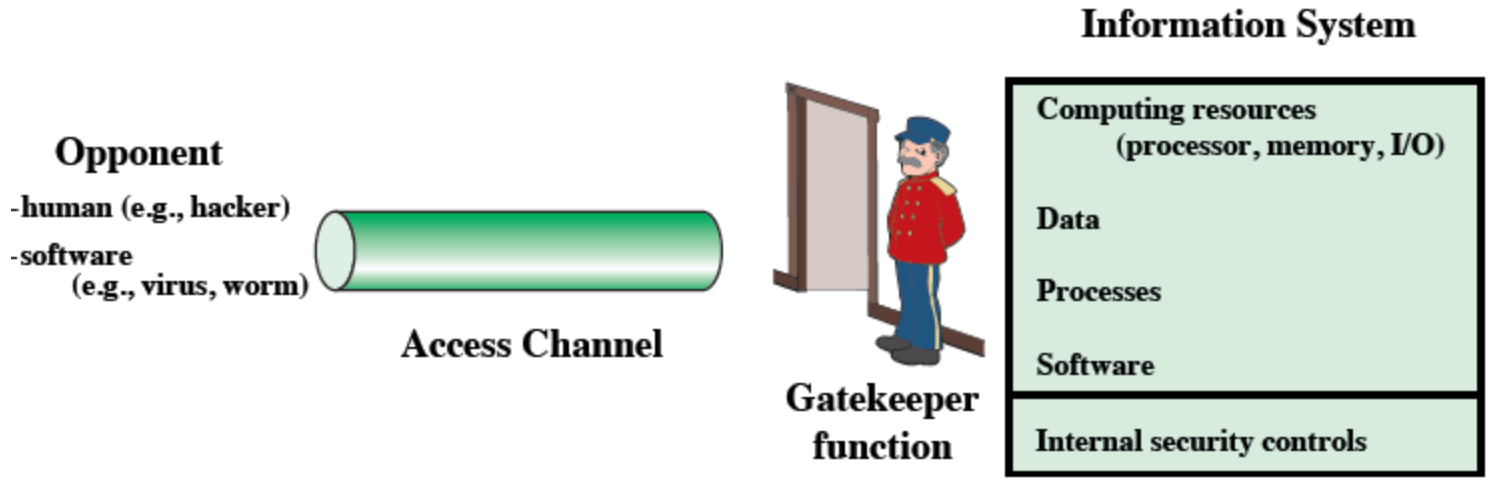
Tasks in Security Service Design

- This general model shows that there are four basic tasks in designing a particular security service:
  - Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose
  - Generate the secret information to be used with the algorithm
  - Develop methods for the distribution and sharing of the secret information
  - Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service

Other security-related situations

- 1.Protect an information system from **unwanted access**
  - E.g. hackers
- 2.The placement in a computer system of **logic that exploits vulnerabilities** in the system
  - Two kinds of threats of program:
    - Information access threats
      - Intercept or modify data on behalf of users who should not have access to that data
    - Service threats
      - Exploit service flaws in computers to inhibit use by legitimate users

Network Access Security Model



- The security mechanisms needed to cope with unwanted access fall into two categories:
  - Gatekeeper function
    - Password-based login procedure
    - Screening logic
  - Internal Control
    - Monitor activity and analyze stored information in order to detect the intruders