Cryptography and Security

Lecture 1

Mosarrat Jahan
mosarratjahan@cse.du.ac.bd

course Website:
https://sites.google.com/cse.univdhaka.edu/cse-4137/cryptography-and-network-security

Security and Standards Organizations

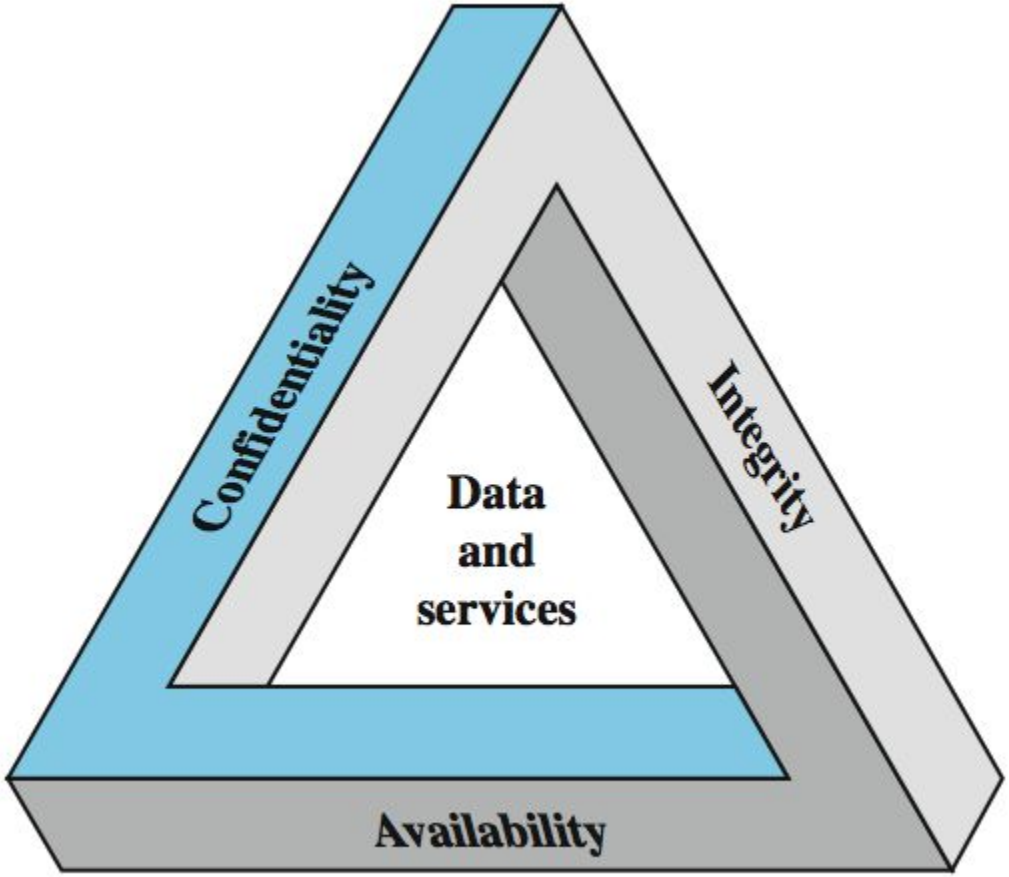
- **National Institute of Standards & Technology (NIST):**
  - NIST FIPS (Federal Information Processing Standard) and SP(Special Publication)
- **Internet Society (ISOC)**
  - Internet Engineering Task Force (IETF)
  - Internet Architecture Board (IAB)
  - Request for Comments (RFC)
- **International Telecommunication Union**
  - Telecommunication Standardization Sector (ITU-T)
  - Recommendation
- **International Organization for Standardization (ISO)**
  - ISO is a nongovernmental organization that promotes the development of standardization and related activities to facilitates the international exchange of goods and services.

Computer Security Concept

According to NIST *Computer Security* Handbook

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).*

Key Security Concepts



Key Security Concepts

- Confidentiality
  - Private information should not be disclosed to unauthorized individuals.
  - Ensures privacy.
- Integrity
  - Guard data against improper modification including information non-repudiation and authenticity.
- Availability
  - Timely and reliable access to and use of information.

Additional Security Concepts

- Authenticity
  - Property to verify the user's originality and that the date arriving is from a trusted user.
- Accountability
  - Ability to trace the action of an entity.
  - This supports non-repudiation, fault isolation, intrusion detection and prevention, after-action recovery and legal actions.

Attacker/Adversary

- “Computer security studies how systems behave in the presence of an adversary.”
- The adversary

  a.k.a. the attacker

  a.k.a. the bad guy
- An intelligence that actively tries to cause the system to misbehave.

Levels of Impacts of Security Breaches

Three levels of impact from a security breach

- Low
- Moderate
- High

Impacts are defined in terms of

- Organizational operation
- Organizational asset
- Financial loss
- Individuals

Examples of Security Requirements

- Confidentiality – Student grades
- Integrity – Patient information
- Availability – Authentication service

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived of benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

OSI Security Architecture

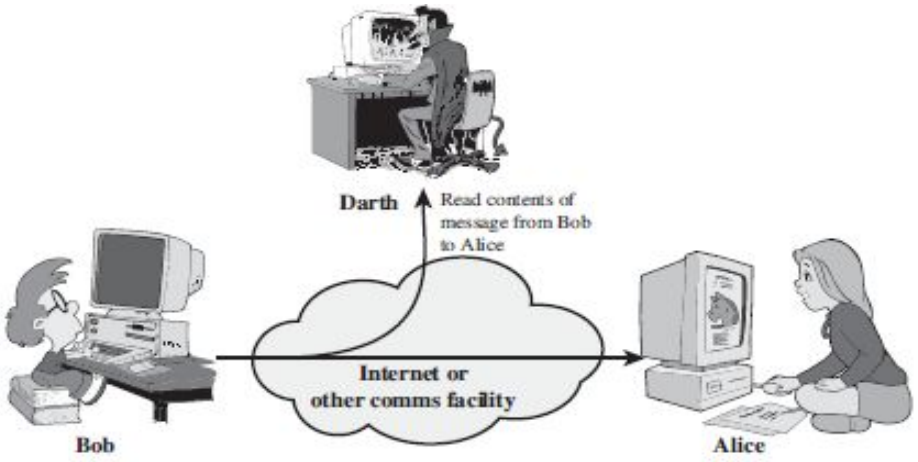
- ITU-T X.800 *"Security Architecture for OSI"*
- Defines a systematic way of defining and providing security requirements
- It provides a useful, if abstract, overview of concepts we will study

OSI Security Architecture

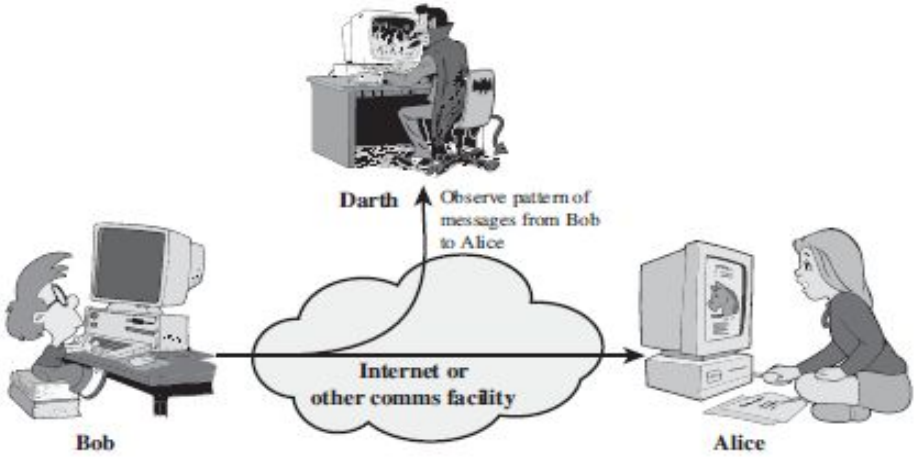
Consider three aspects of information security:

- **security attack**
- **security mechanism**
- **security service**

Passive Attack



(a) Release of message contents

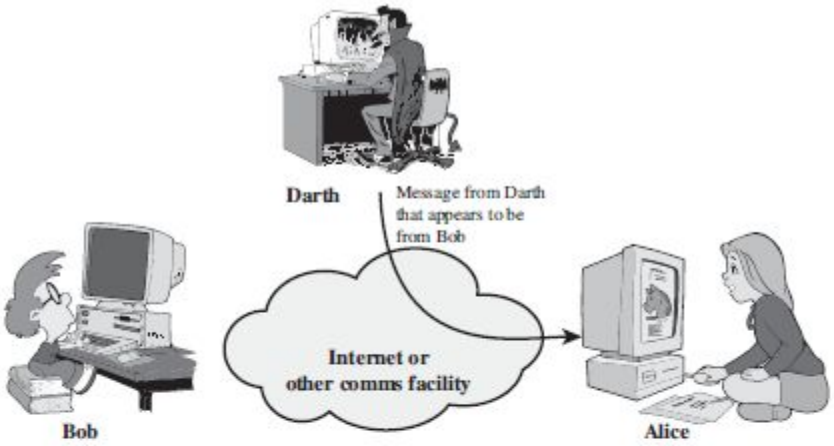


(b) Traffic analysis

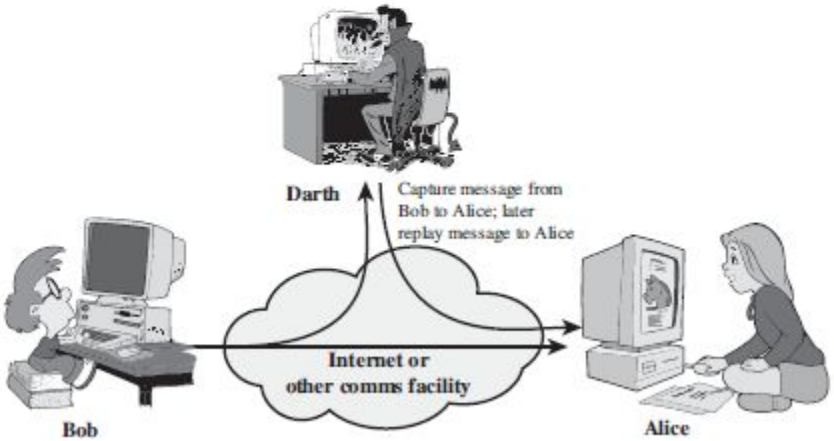
Active Attack

- Modification of data or creation of false data.
- Four types:
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of Services.

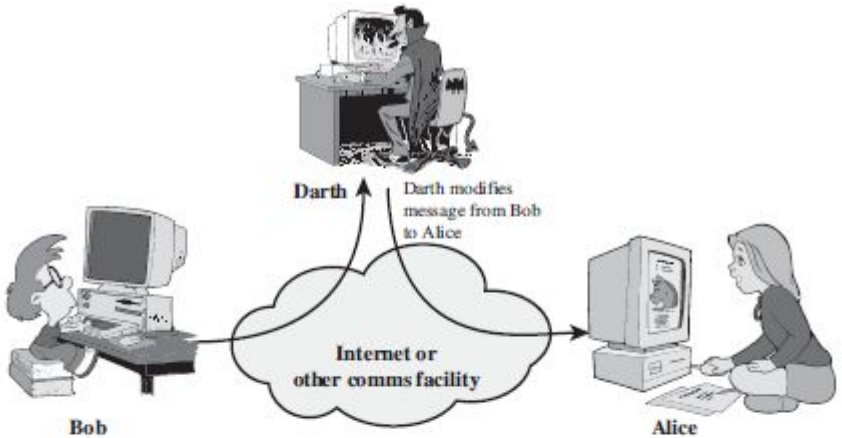
Active Attack



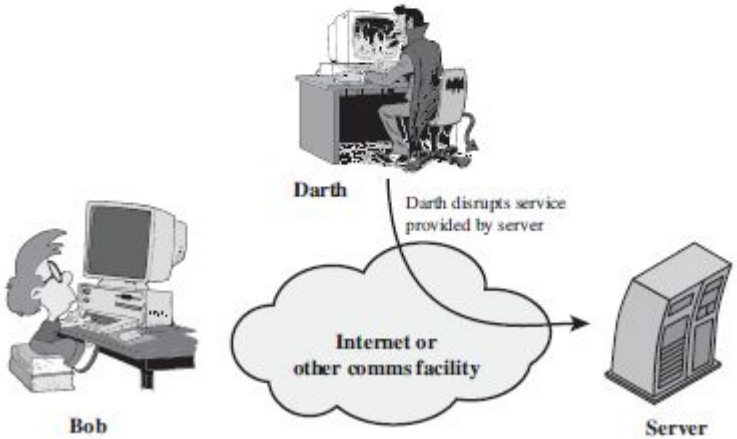
(a) Masquerade



(b) Replay



(c) Modification of messages



(d) Denial of service

Security Services

- **X.800**:

"a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- **RFC 2828**:

"a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed

– have both peer-entity & data origin authentication

- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** - protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** - resource accessible/usable

Security Services (X.800)

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.

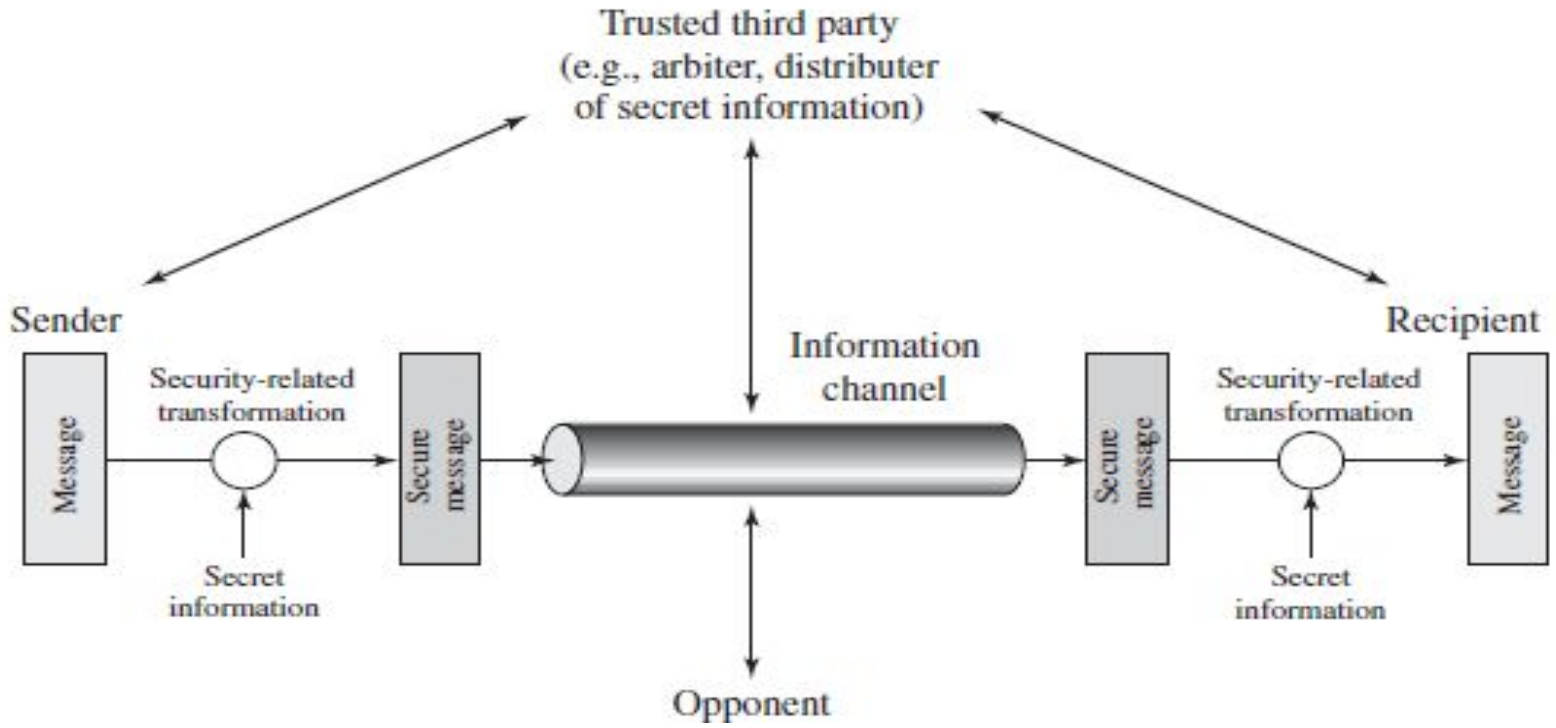
Security Mechanisms

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**

Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
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.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
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).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**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.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
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.	

Model for Network Security

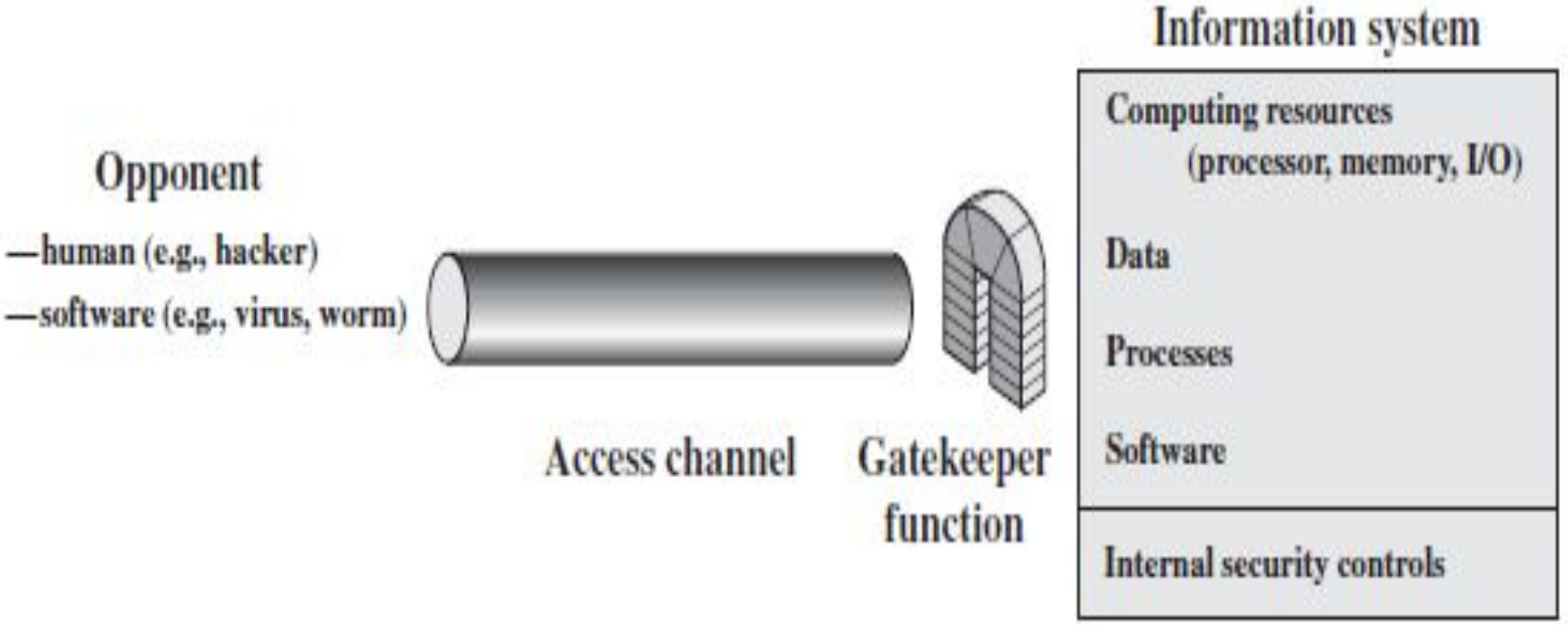


Model for Network Security

This model requires

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



Books Followed

- Chapter 1 of Cryptography and Network Security (7^{th} Edition) by William Stallings.
- Chapter 1 of Cryptography and Network Security (2^{nd} Edition) by Behrouz A. Forouzan and Debdeep Mukhopadhyay