정보보호 이론 및 응용 (Cryptography and Its Applications)

Chapter 1 Overview

Prof. Junbeom Hur
Department of Computer Science and Engineering
Korea University

Chapter 1 Topics

- Information security concepts
- The OSI security architecture
- Security attacks
- Security services
- Security mechanisms
- Network security model

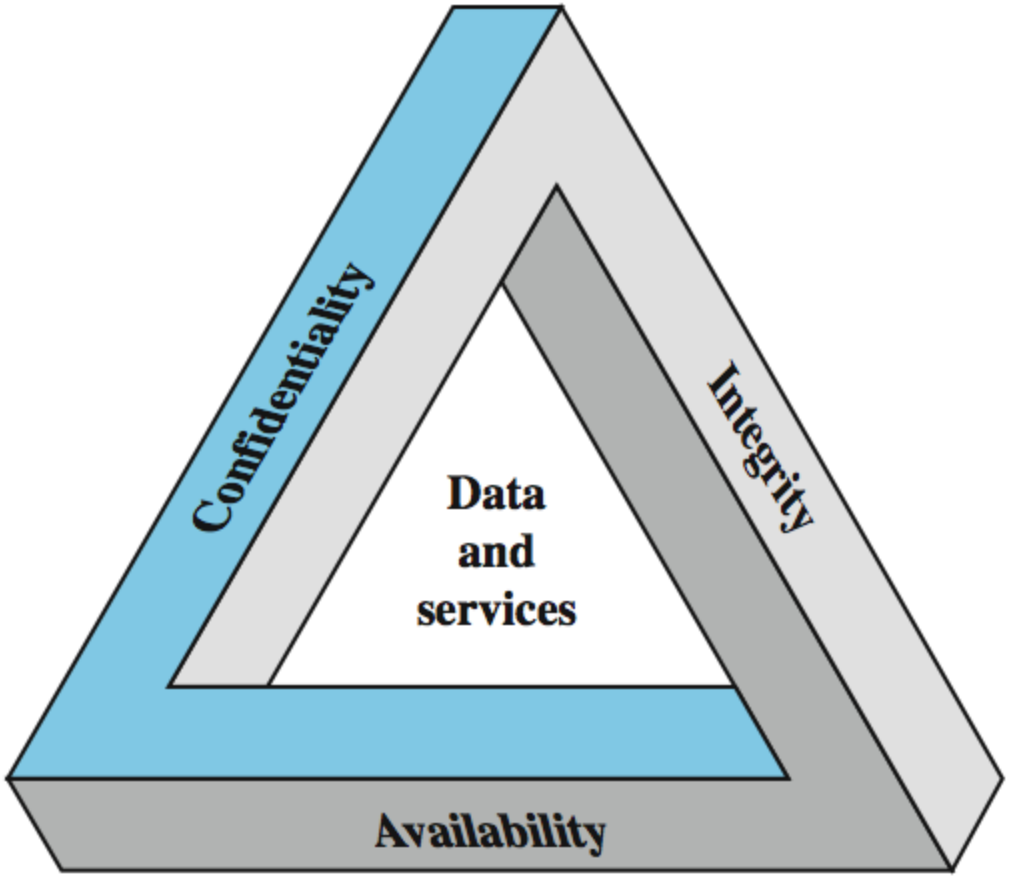
What is information security?

Definition of Computer Security

- 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)"

Information Security Objectives



Information Security Objectives

- Confidentiality
  - *Preserving authorized restrictions on information access and disclosure*
- Integrity
  - *Guarding against improper information modification or destruction*
- Availability
  - *Ensuring timely and reliable access to and use of information*

Additional Information Security Objectives

- Authenticity
  - *Verifying users are who they say they are, and that each input arriving at the system came from a trusted source*
- Accountability
  - *Actions of an entity to be traced uniquely to that entity*

Three Fundamental Questions

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

Vulnerabilities, Threats and Attacks

- Vulnerabilities (of computer or network asset)
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)

- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset

Vulnerabilities, Threats and Attacks

- Attacks (threats carried out)
  - Passive attack
    - Attempt to learn information from the system that does not affect system resources
  - Active attack
    - Attempt to alter system resources or affect their operation
  - Inside attack
    - Initiated by an entity inside the security perimeter
  - Outside attack
    - Initiated from outside the perimeter

Security Requirements Examples

- Student grades
  - Confidentiality, …
- Patient information
  - Integrity, confidentiality, …
- Server (authentication, web, cloud, …)
  - Availability, integrity, …

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 on 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
  - For us it provides a useful, if abstract, overview of concepts we will study

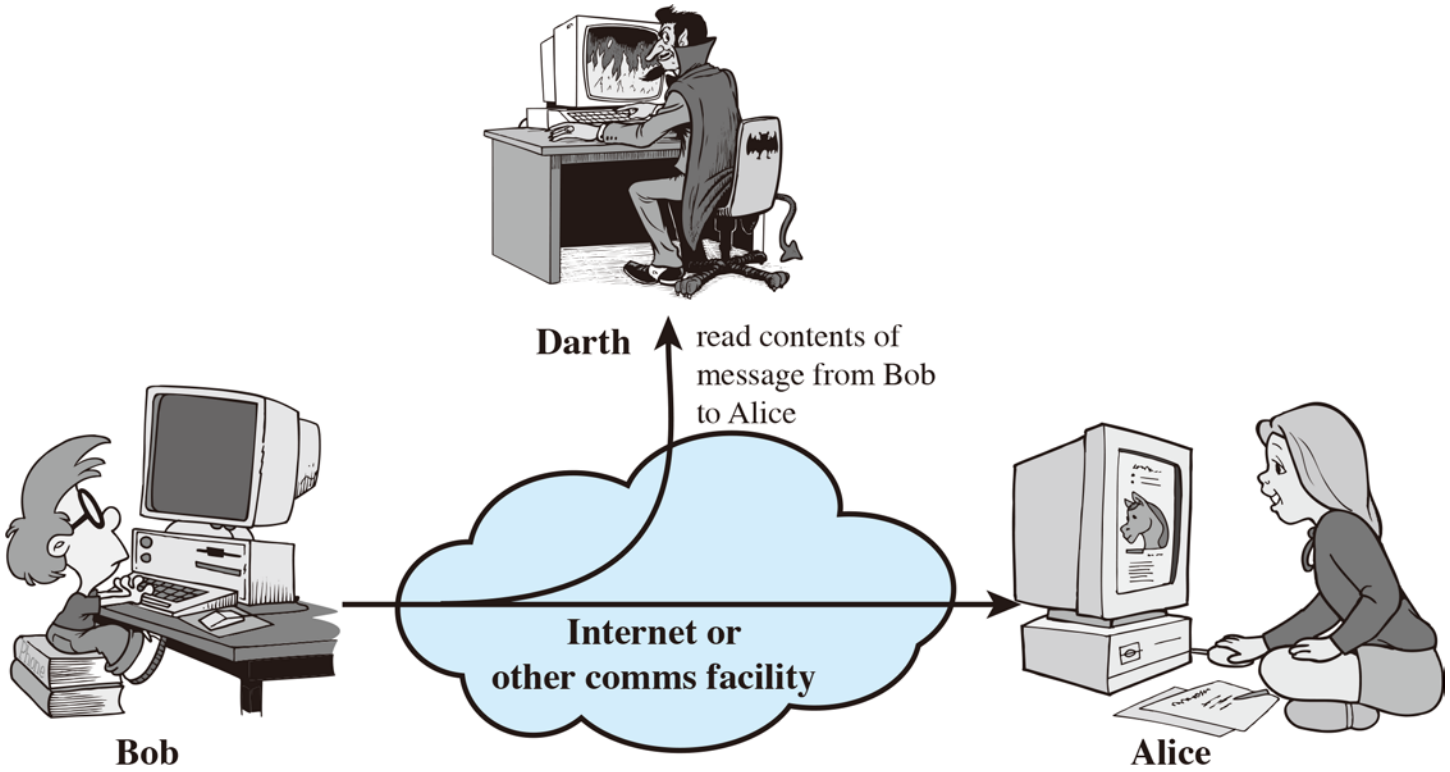
OSI Security Architecture

- 3 aspects of information security
  - Security attack
    - Action that compromise information security
  - Security mechanism
    - Process to detect/prevent/recover from security attack
  - Security service
    - Service to counter security attack
    - Make use of one or more security mechanisms

Security Attack

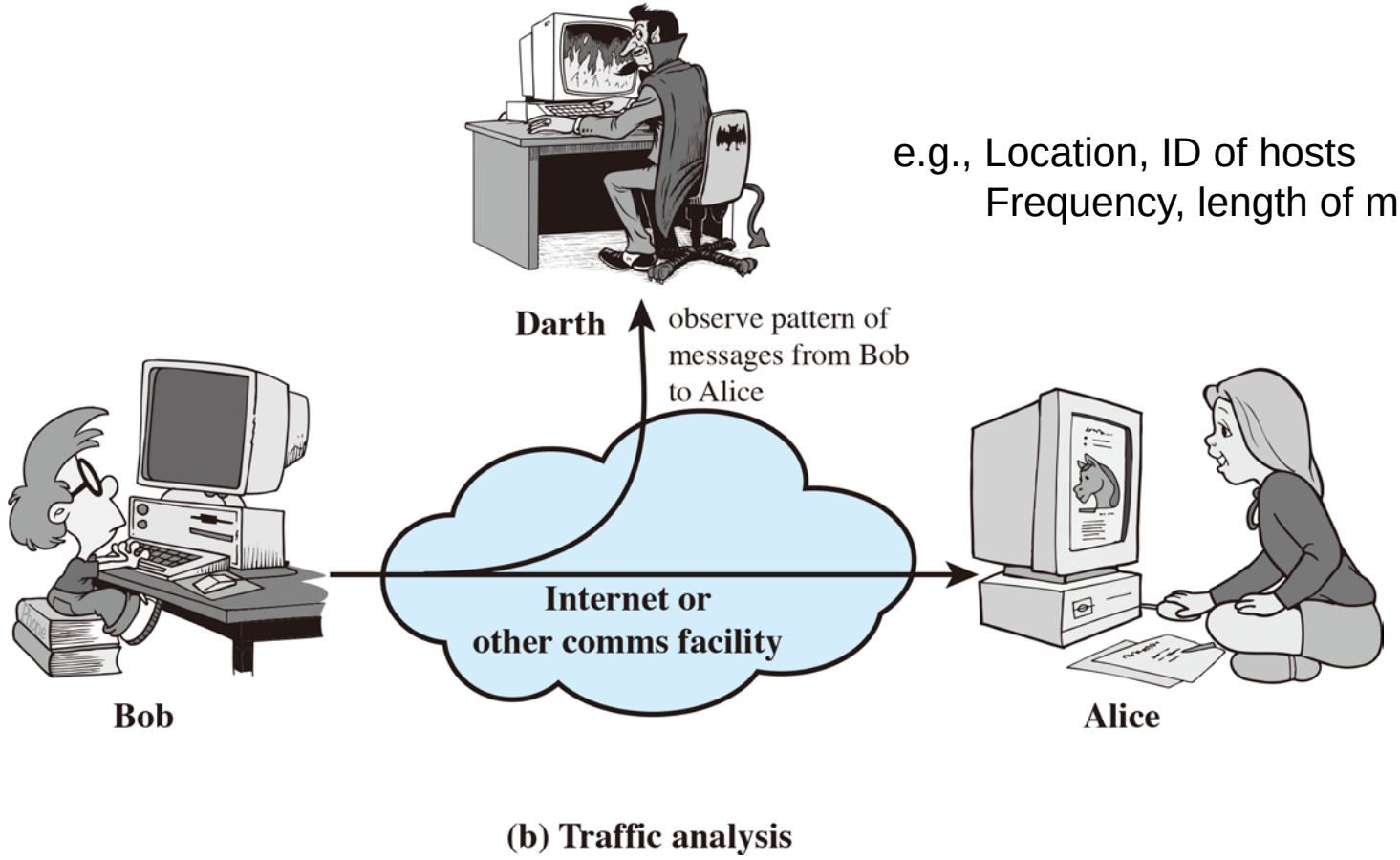
1. Passive attack
   - Learn or use information of system
   - Does not affect system resources
   - Difficult to detect (prevention rather than detection)
2. Active attack
   - Alter system resources or affect their operations
   - Difficult to prevent (detection/recover rather than prevention)

Passive Attacks



(a) Release of message contents

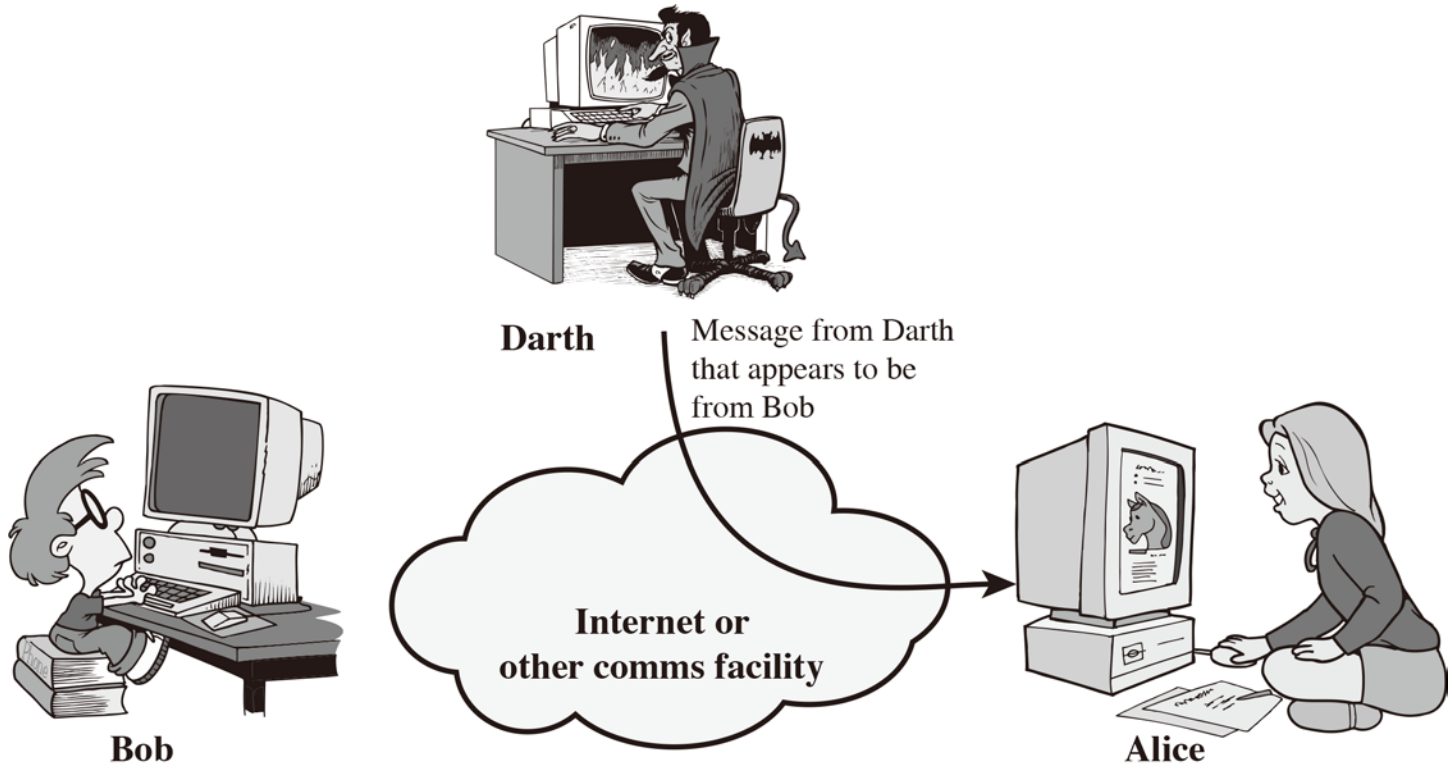
Passive Attacks



(b) Traffic analysis

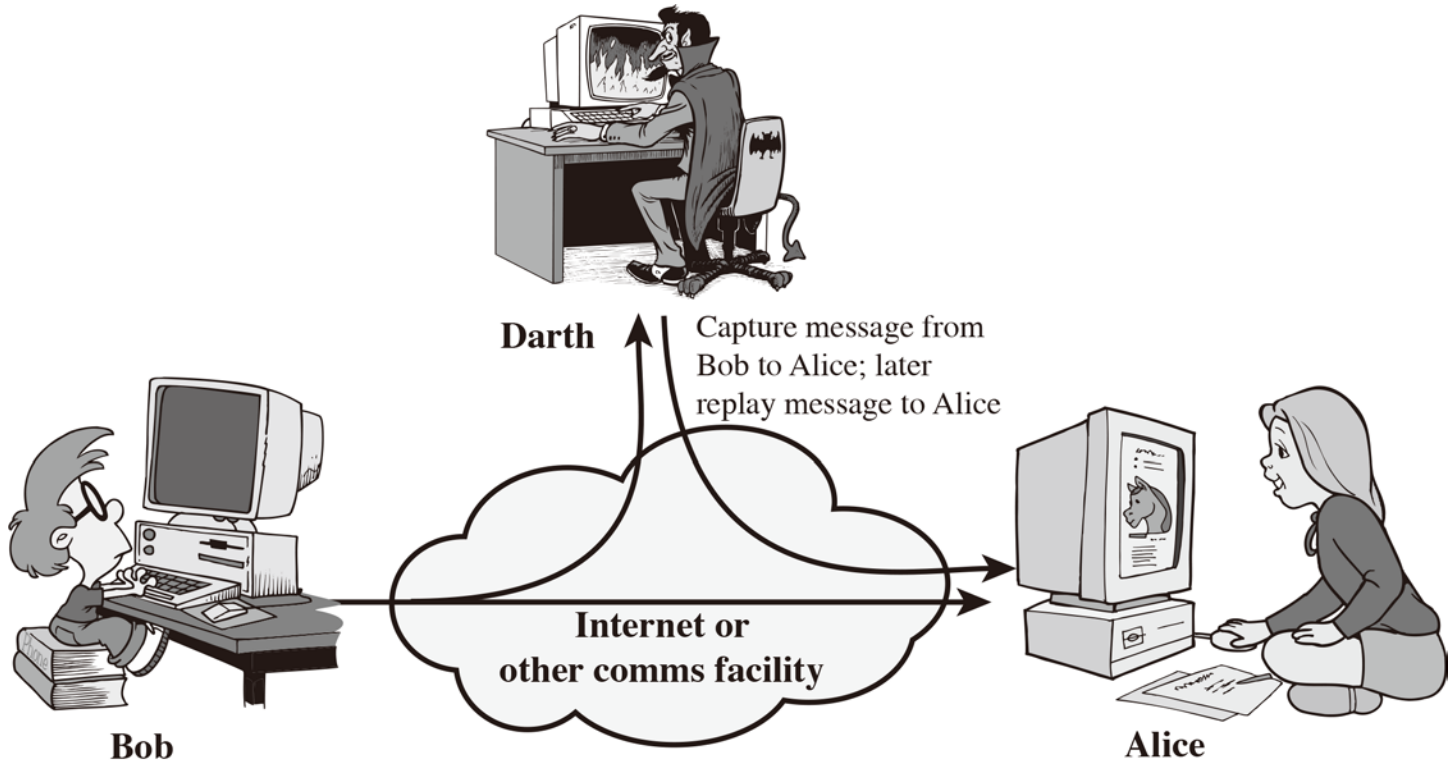
e.g., Location, ID of hosts
Frequency, length of messages

Active Attacks



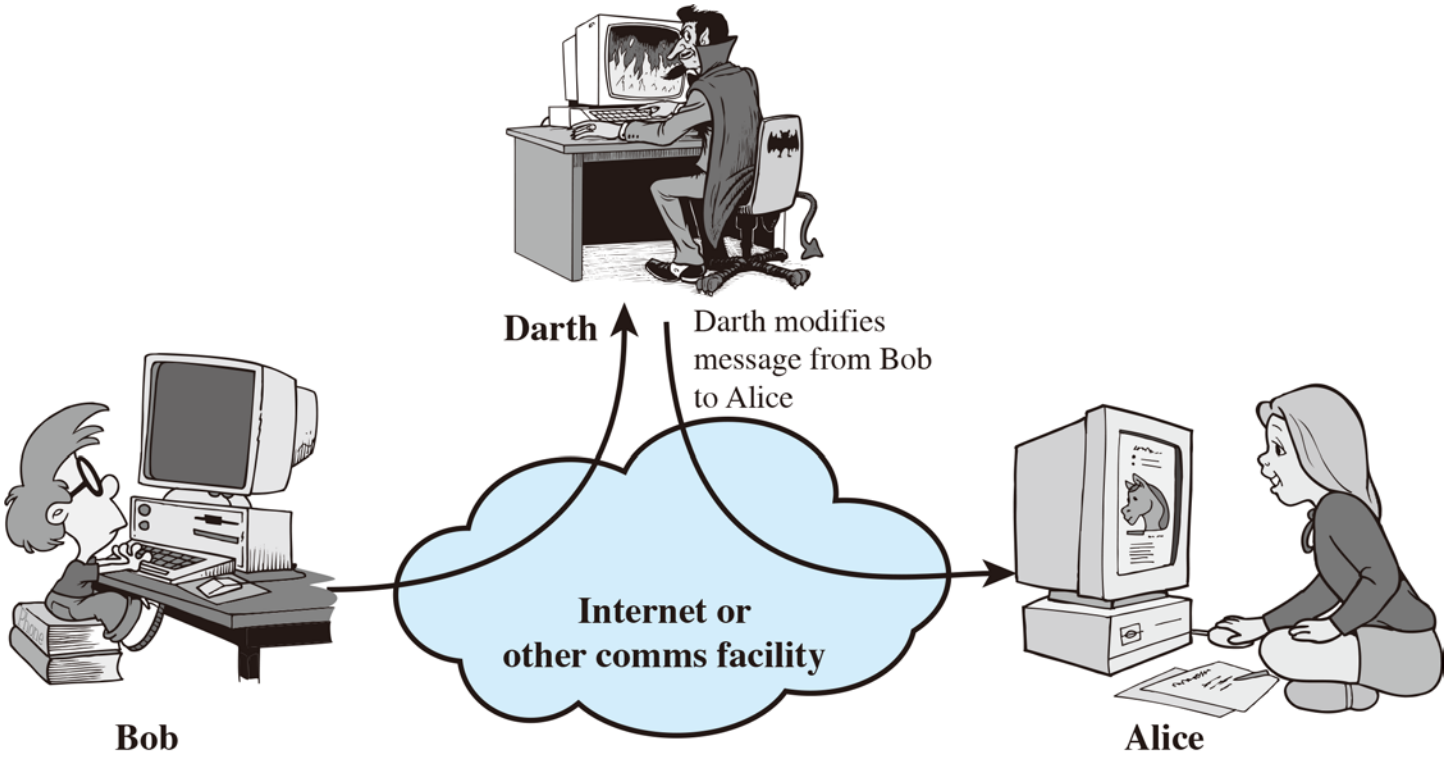
(a) Masquerade

Active Attacks



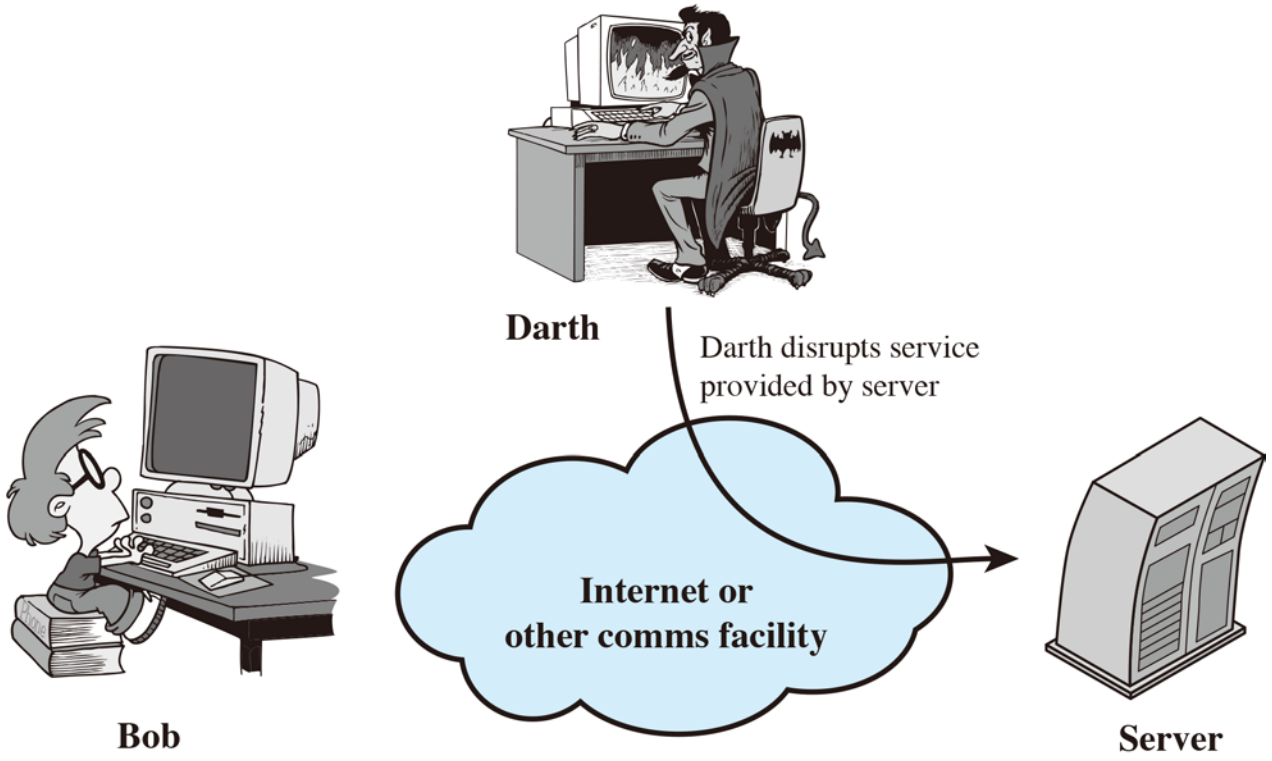
(b) Replay

Active Attacks



(c) Modification of messages

Active Attacks



(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
- **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

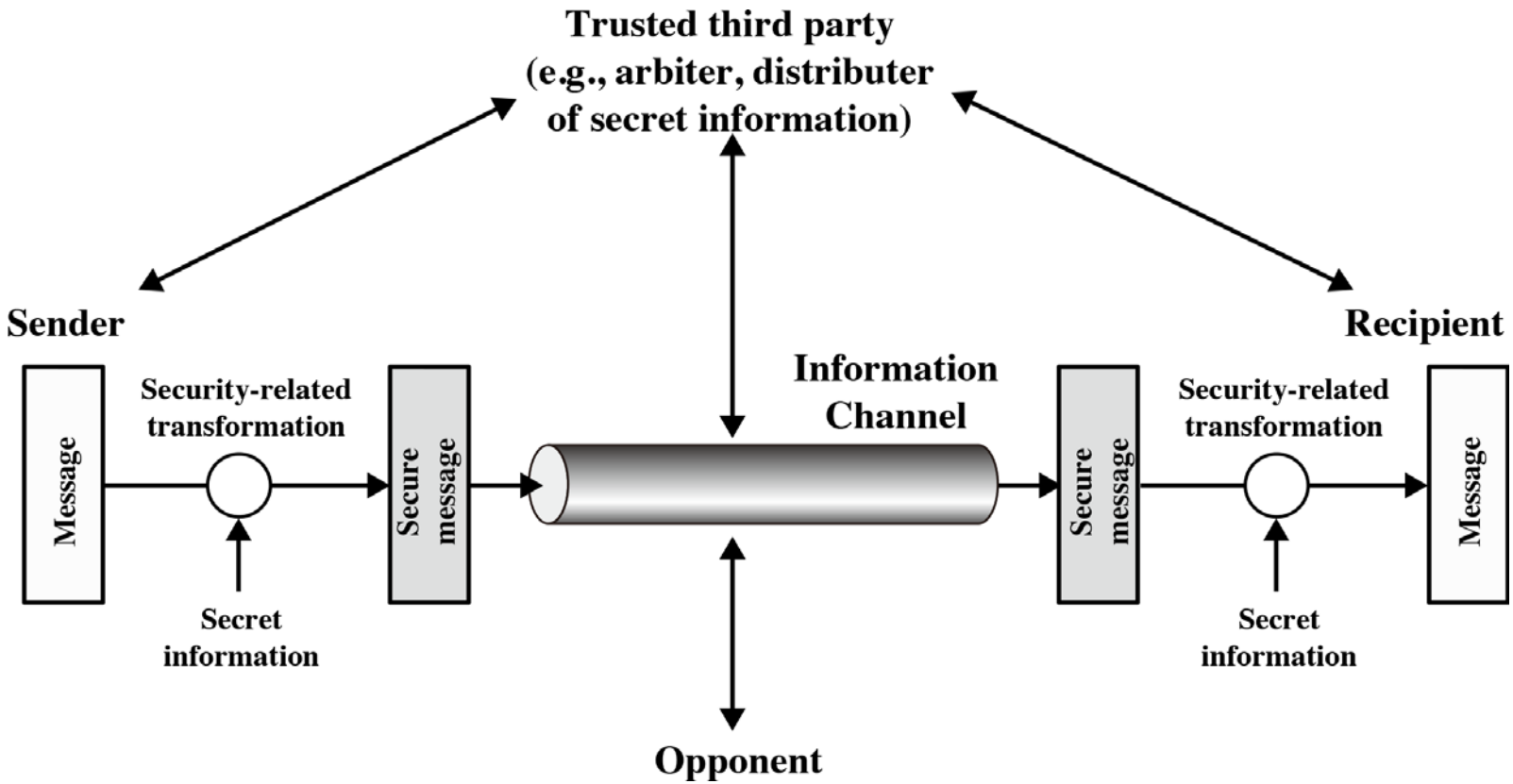
Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism supports all services required
- However one particular element underlies many of the security mechanisms in use:
  - **Cryptographic techniques**
- Hence our focus on this topic

Security Mechanisms (X.800)

- Specific security mechanisms:
  - Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms:
  - Trusted functionality, security labels, event detection, security audit trails, security recovery

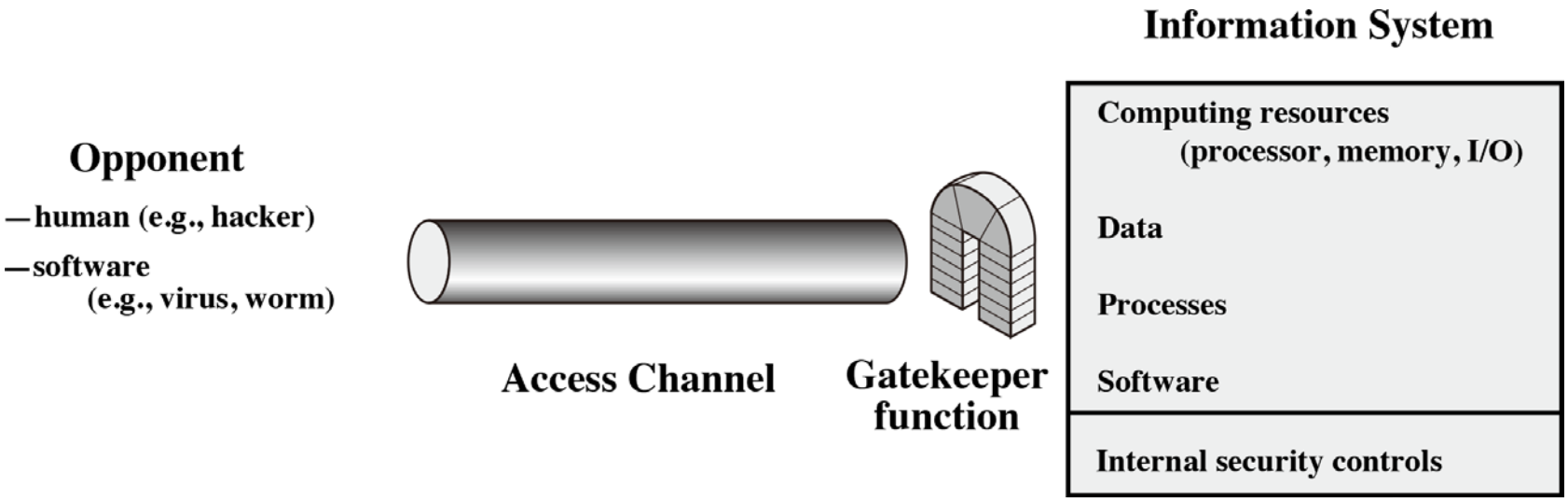
Model for Network Security



Model for Network Security

- This model requires us to:
  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 users to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- This model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorised users access designated information or resources

Summary

- Security concepts
  - Confidentiality, integrity, availability
- X.800 security architecture
- Security attacks, services, mechanisms
- Models for network (access) security