CEN 448

SECURITY AND INTERNET PROTOCOLS

Dr. Ashraf Abdelaziz Taha

Cryptography and Network Security Principles and Practice

Fifth Edition

by

William Stallings

STANDARDS ORGANIZATIONS

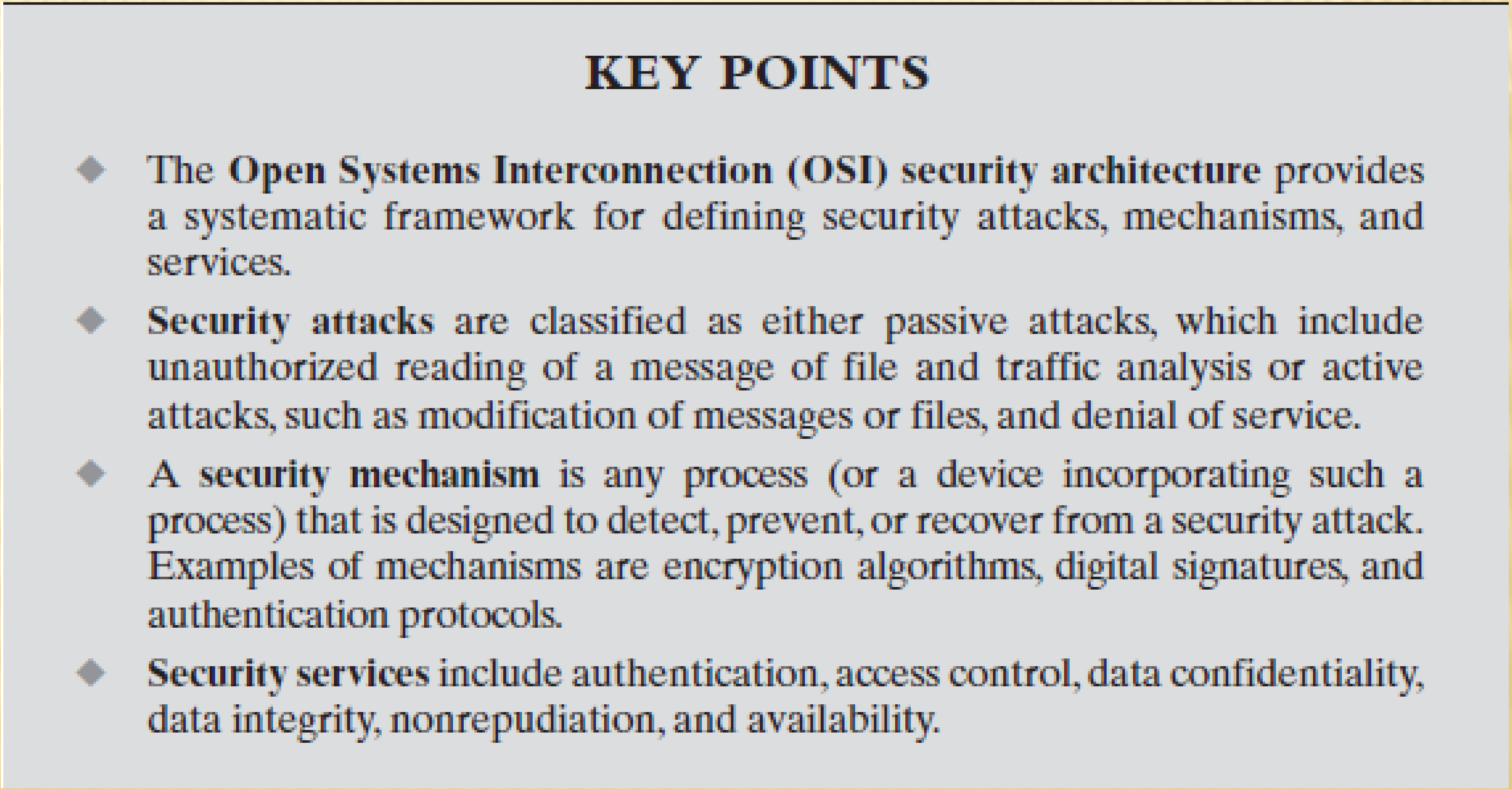
- **National Institute of Standards & Technology (NIST)**
- **Internet Society (ISOC)**
- **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)**
- **International Organization for Standardization (ISO)**

Chapter 1

Overview

CHAPTER 1 – CONTENTS

- Computer Security Concepts.
- The OSI Security Architecture.
- Security Attacks.
- Security Services.
- Security Mechanisms.
- A Model for Network Security.



KEY POINTS

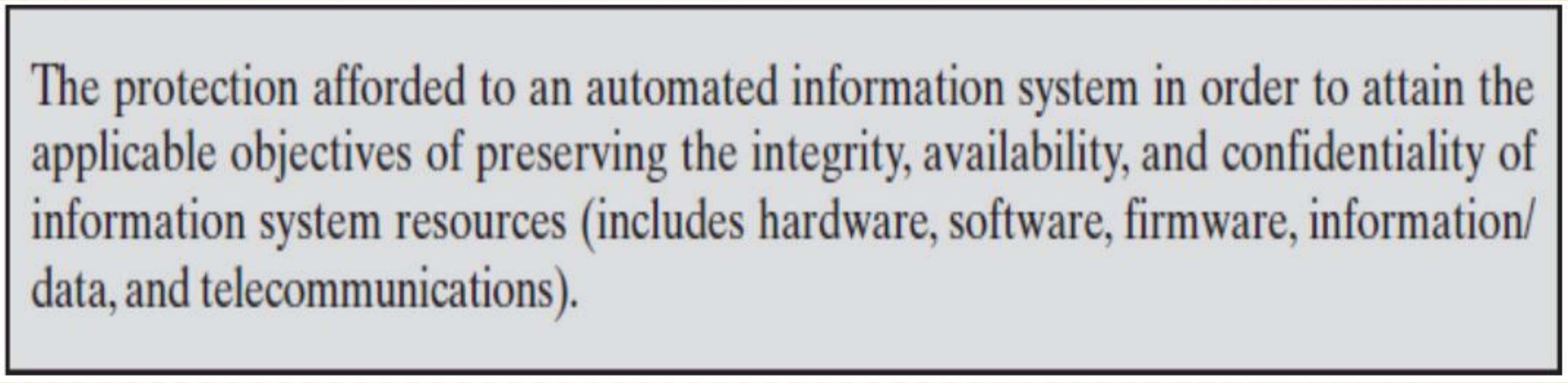
- The **Open Systems Interconnection (OSI) security architecture** provides a systematic framework for defining security attacks, mechanisms, and services.
- **Security attacks** are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service.
- A **security mechanism** is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.
- **Security services** include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability.

CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

Can be grouped into 4 main areas :

- **Symmetric encryption:** Used to hide the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords.
- **Asymmetric encryption:** Used to hide small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.
- **Data integrity algorithms:** Used to protect blocks of data, such as messages from alteration.
- **Authentication protocols:** These are schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities.

COMPUTER SECURITY



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).

DEFINITIONS

- Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

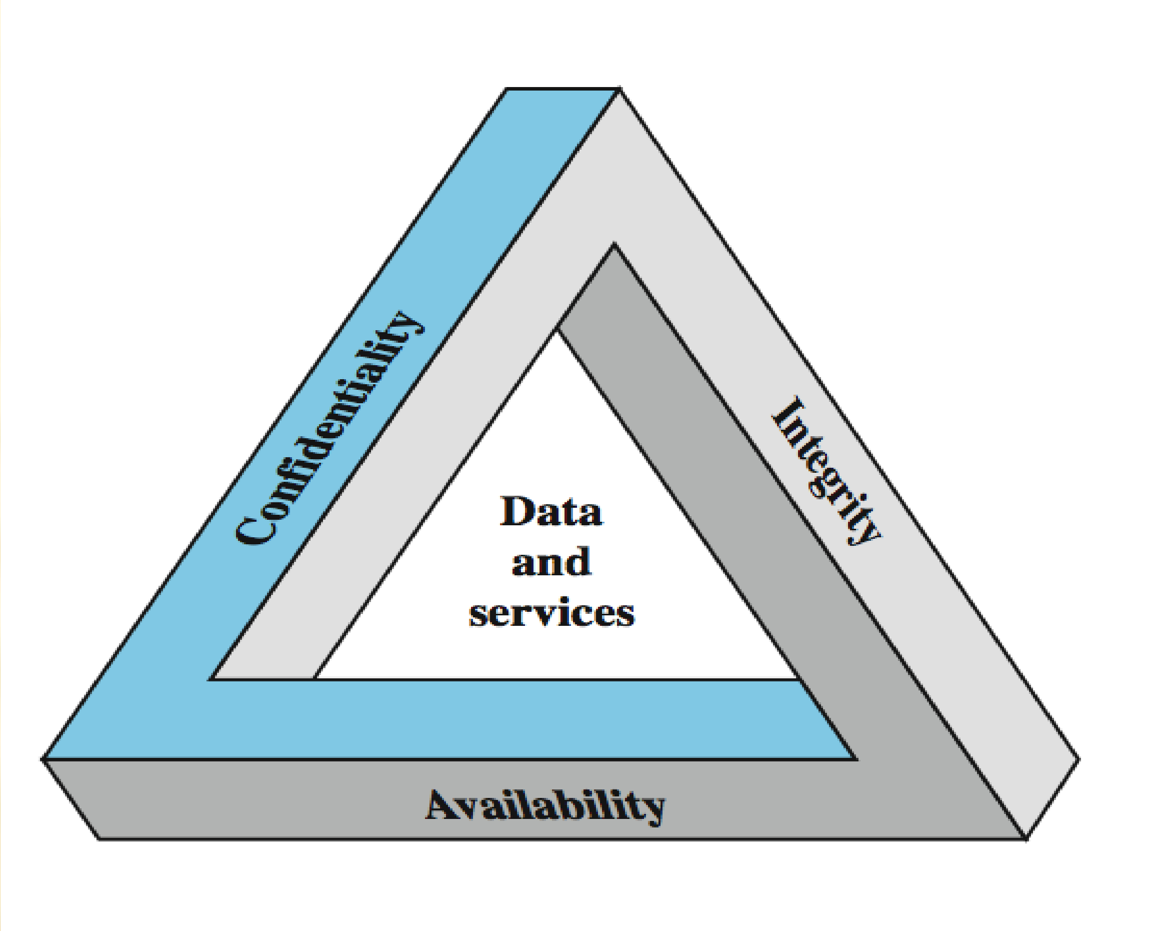
- Network Security - measures to protect data during their transmission

- Internet Security - measures to protect data during their transmission over a collection of interconnected networks

THREE KEY OBJECTIVES THAT ARE AT THE HEART OF COMPUTER SECURITY :

- **Confidentiality :** This term covers two related concepts:
  - **Data confidentiality:** Assures that private or confidential information is not made available 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 :** This term covers two related concepts:
  - **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 free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability:**
  - Assures that systems work on time and service is not denied to authorized users.

KEY SECURITY CONCEPTS



THESE THREE OBJECTIVES IN TERMS OF REQUIREMENTS AND THE DEFINITION OF A LOSS OF SECURITY IN EACH CATEGORY:

- **Confidentiality:** Keeping 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.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information non repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **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.

- **Confidentiality** (covers both data confidentiality and privacy):

- **Integrity** (covers both data and system integrity)**:**

- **Availability:** Ensuring timely and reliable access to and use of information.

- **Authenticity:** The property of being genuine and being able to be verified and trusted;

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

LEVELS OF IMPACT

- Three levels of impact from a security breach
  - Low
  - Moderate
  - High

LOW IMPACT

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

  (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

  (ii) result in minor damage to organizational assets;

  (iii) result in minor financial loss; or

  (iv) result in minor harm to individuals.

MODERATE IMPACT

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss might

  (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

  (ii) result in significant damage to organizational assets;

  (iii) result in significant financial loss; or

  (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

HIGH IMPACT

- The loss could be expected to have a severe adverse effect on organizational operations, organizational assets, or individuals. A severe adverse effect means that, for example, the loss might

  (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

  (ii) result in major damage to organizational assets;

  (iii) result in major financial loss; or

  (iv) result in severe harm to individuals involving loss of life or serious life threatening injuries.

EXAMPLES OF SECURITY REQUIREMENTS

- Confidentiality – student grades
- Integrity – patient information
- Availability – authentication service

Examples of applications that illustrate the requirements just enumerated.

- **Confidentiality**- Student grade information is an asset whose confidentiality is considered to be highly important by students. Grade information should only be available to students, their parents, and employees that require the information to do their job.

- **Integrity** – Consider a hospital patient's information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital.

- **Availability** - Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

COMPUTER SECURITY CHALLENGES

1. **Not simple :**

   The mechanisms used to meet those requirements can be quite complex and subtle.

2. **Must consider potential attacks :**

   Often unexpected on those security features

3. **Procedures used counter-intuitive**

   procedures used to provide particular services are often counter-intuitive

4. **Involve algorithms and secret info**

   it is necessary to decide where to use them.

5. **Must decide where to deploy mechanisms**

   Security mechanisms typically involve more than a particular algorithm or protocol

6. **battle of wits between attacker / admin**

   Computer 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. **Not perceived on benefit until fails**

   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. **Requires regular monitoring**

   Security requires regular monitoring, difficult in today's short-term environment.

9. **Too often an after-thought**

   Security is still too often an afterthought - incorporated after the design is complete.

10. **Regarded as impediment to using system**

    Many users / security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

OSI SECURITY ARCHITECTURE

- To satisfy the security needs of an organization and to evaluate and choose various security products and policies, This is difficult enough in a centralized data processing environment; with the use of local and wide area networks the problems are compounded.
  - ITU-T X.800, *"Security Architecture for OSI"*, defines such a systematic approach.
  - The OSI security architecture is useful to managers as a way of organizing the task of providing security.

ASPECTS OF SECURITY

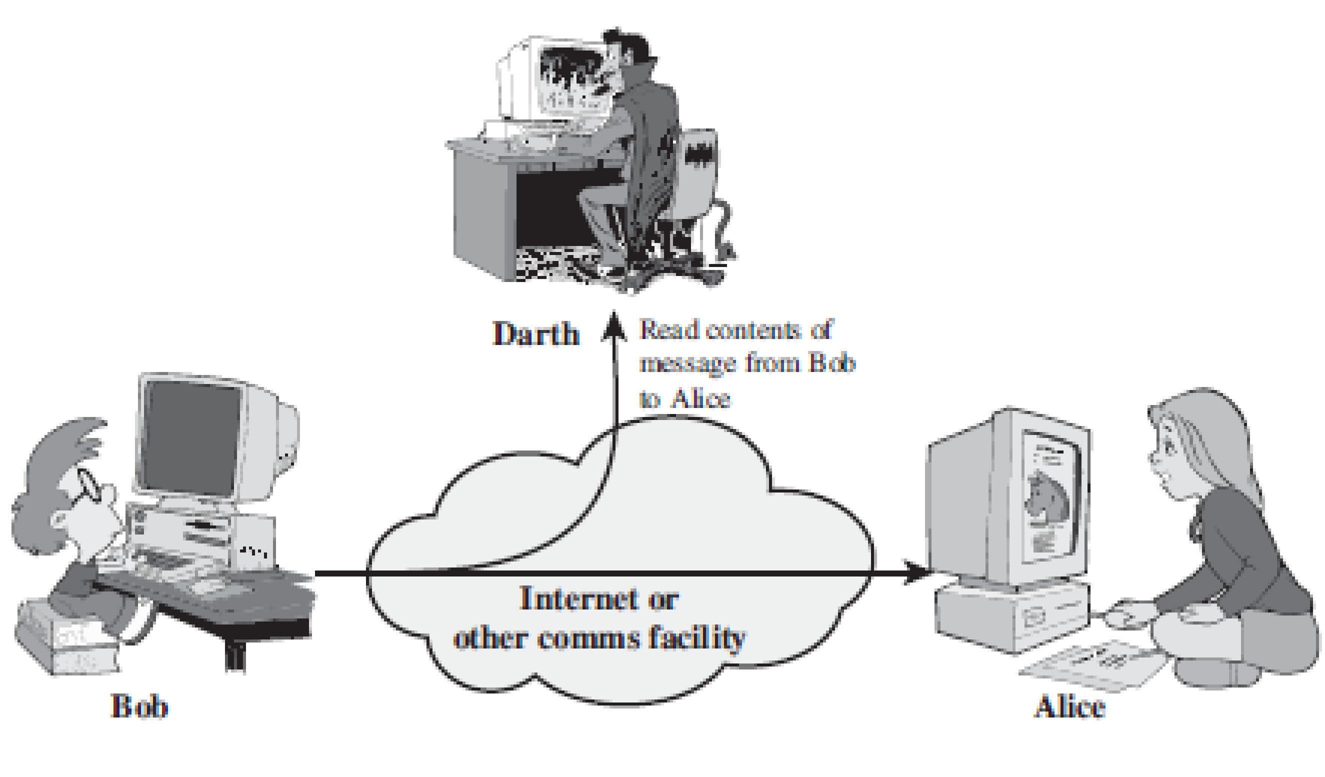
- **The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:**

- consider 3 aspects of information security:
  - **security attack:** Any action that causes dangerous on 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.

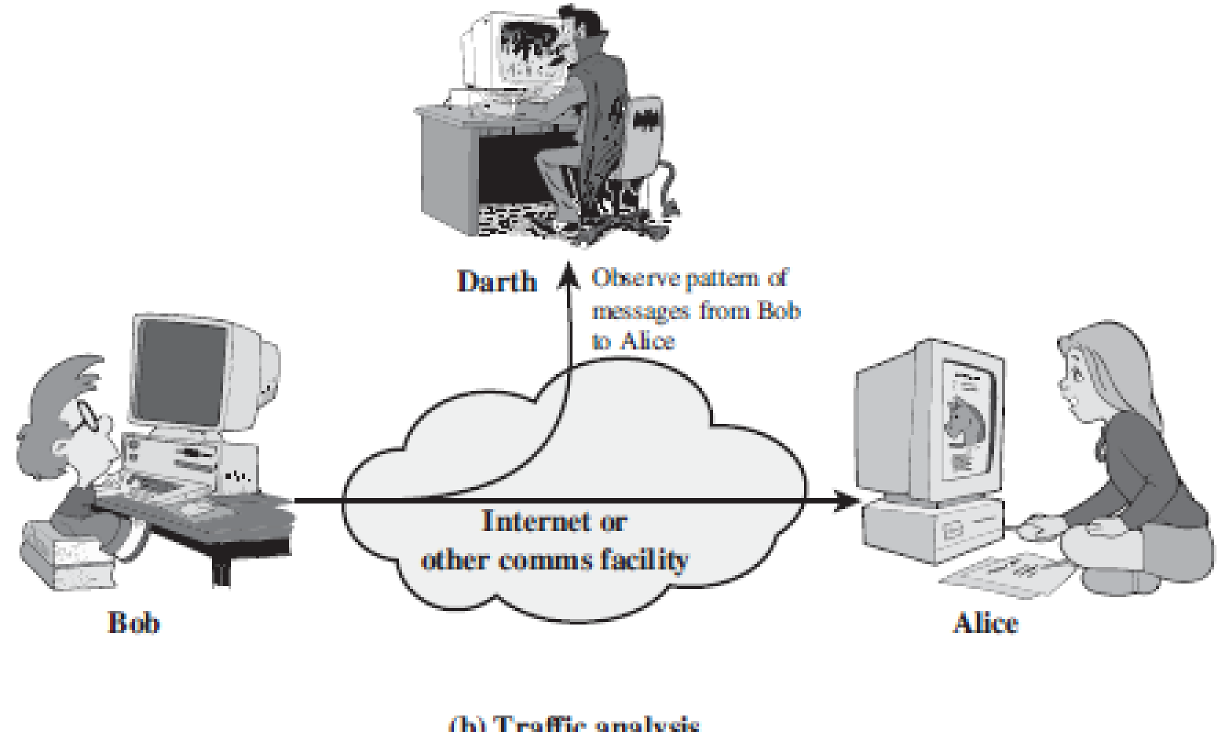
- note terms
  - *Threat* – a potential for violation of security
  - *Attack* – an assault on system security that derives from an intelligent threat.

PASSIVE ATTACKS

These attacks are difficult to detect because they do not involve any alteration of the data. Two types of passive attacks are:


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

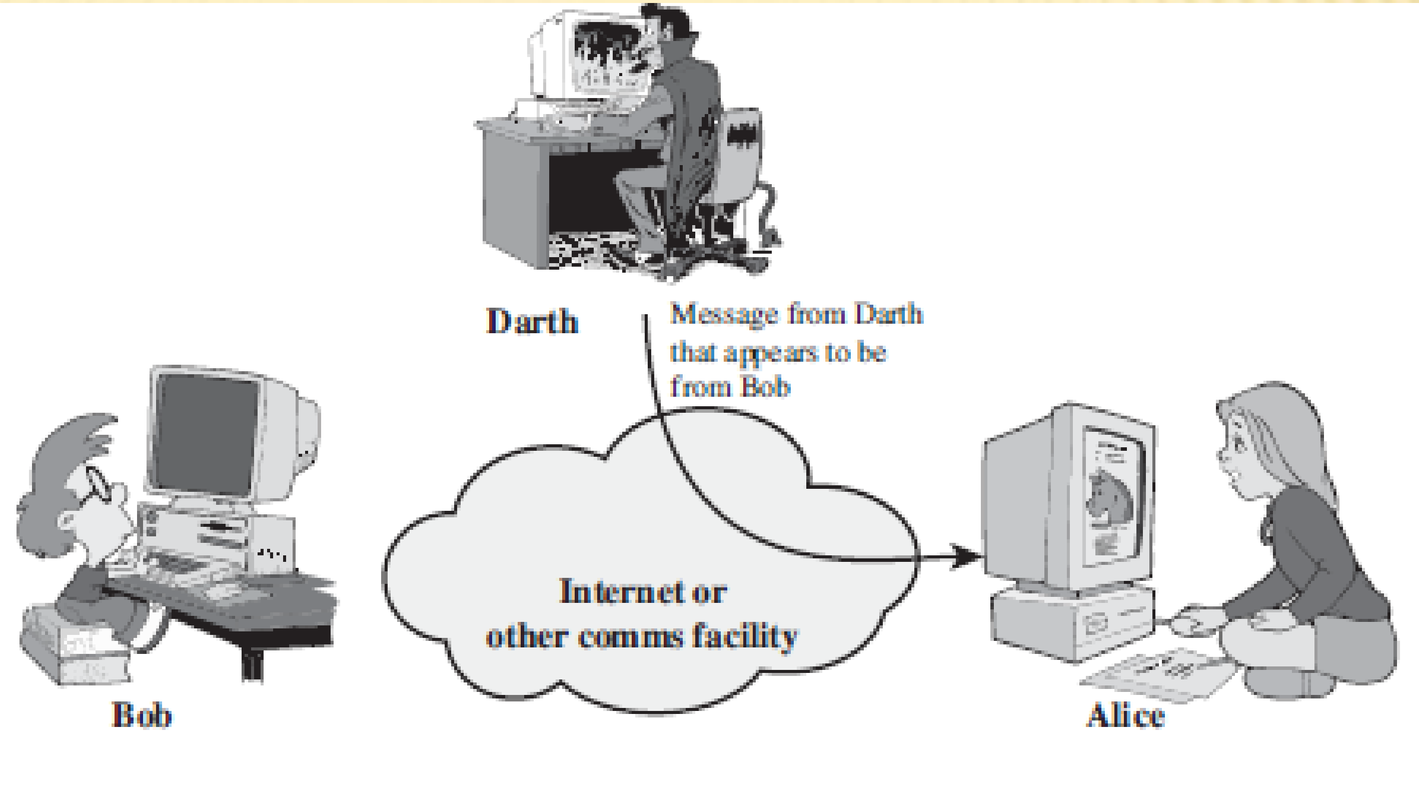
Traffic analysis - monitor traffic flow to determine location and identity of communicating hosts and could observe the frequency and length of messages being exchanged

ACTIVE ATTACKS

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service:

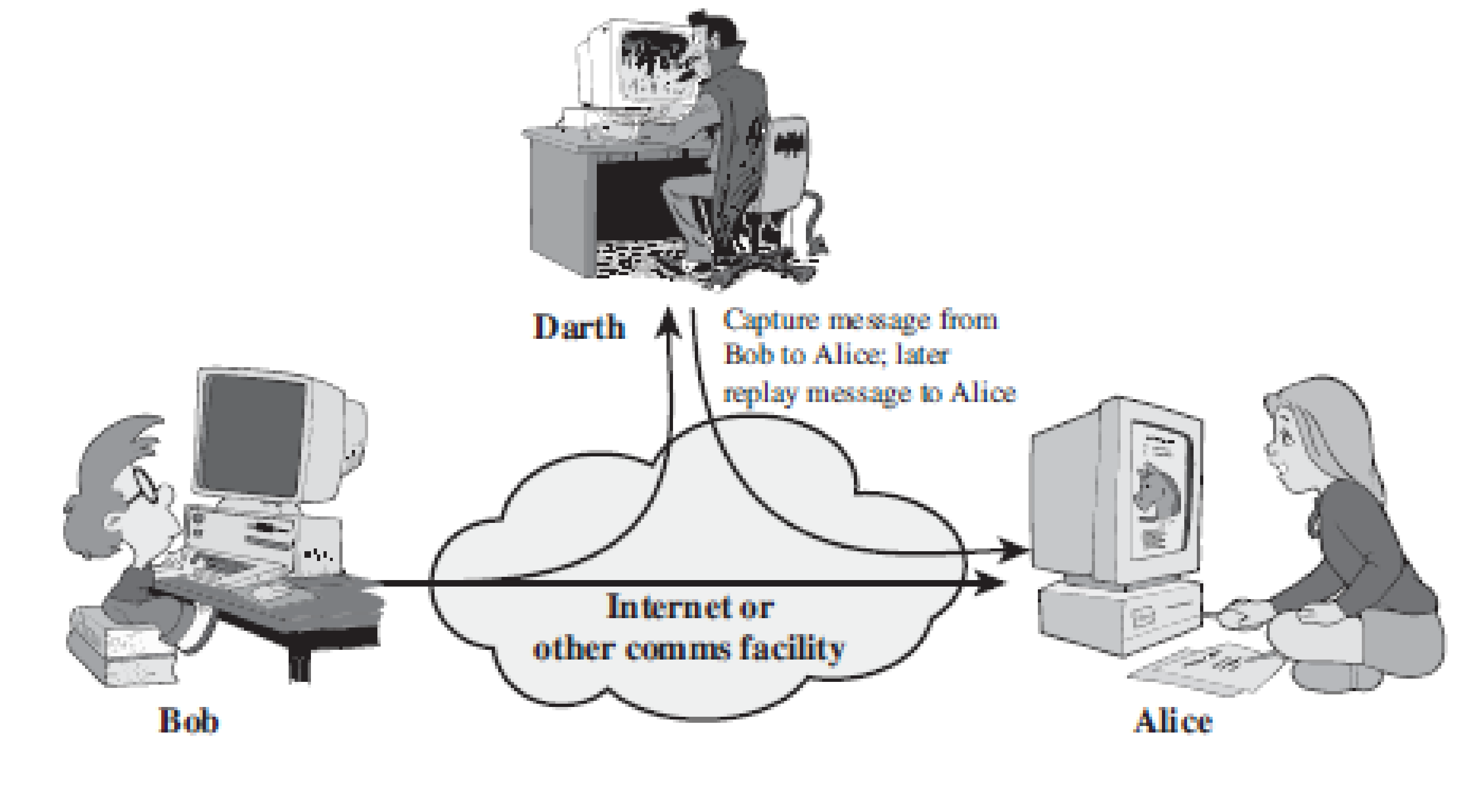
- Masquerade of one entity as some other
- Replay previous messages
- Modify/alter (part of) messages in transit to produce an unauthorized effect
- Denial of service - prevents or inhibits the normal use or management of communications facilities

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.



Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

(a) Masquerade


Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice

(b) Replay

SECURITY SERVICES

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

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** - is concerned with assuring that a communication is authentic. Two specific authentication services are defined in X.800:
  - **Peer entity authentication:** provides corroboration of the identity of a peer entity in an association; and
  - **Data origin authentication:** provides corroboration of the source of a data unit.
- **Access Control** – the ability to limit and control the access to host systems and applications via communications links.

  or prevention of the unauthorized use of a resource
- **Data Confidentiality** – the protection of transmitted data from passive attacks, and the protection of traffic flow from analysis.

  or protection of data from unauthorized disclosure
- **Data Integrity** – assures that messages are received as sent, with no duplication, insertion, modification, reordering, replay, or loss.

  or assurance that data received is as sent by an authorized entity
- **Non repudiation -** prevents either sender or receiver from denying a transmitted message.
- **Availability** – resource accessible/usable

  The property of a system / resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

SECURITY MECHANISMS

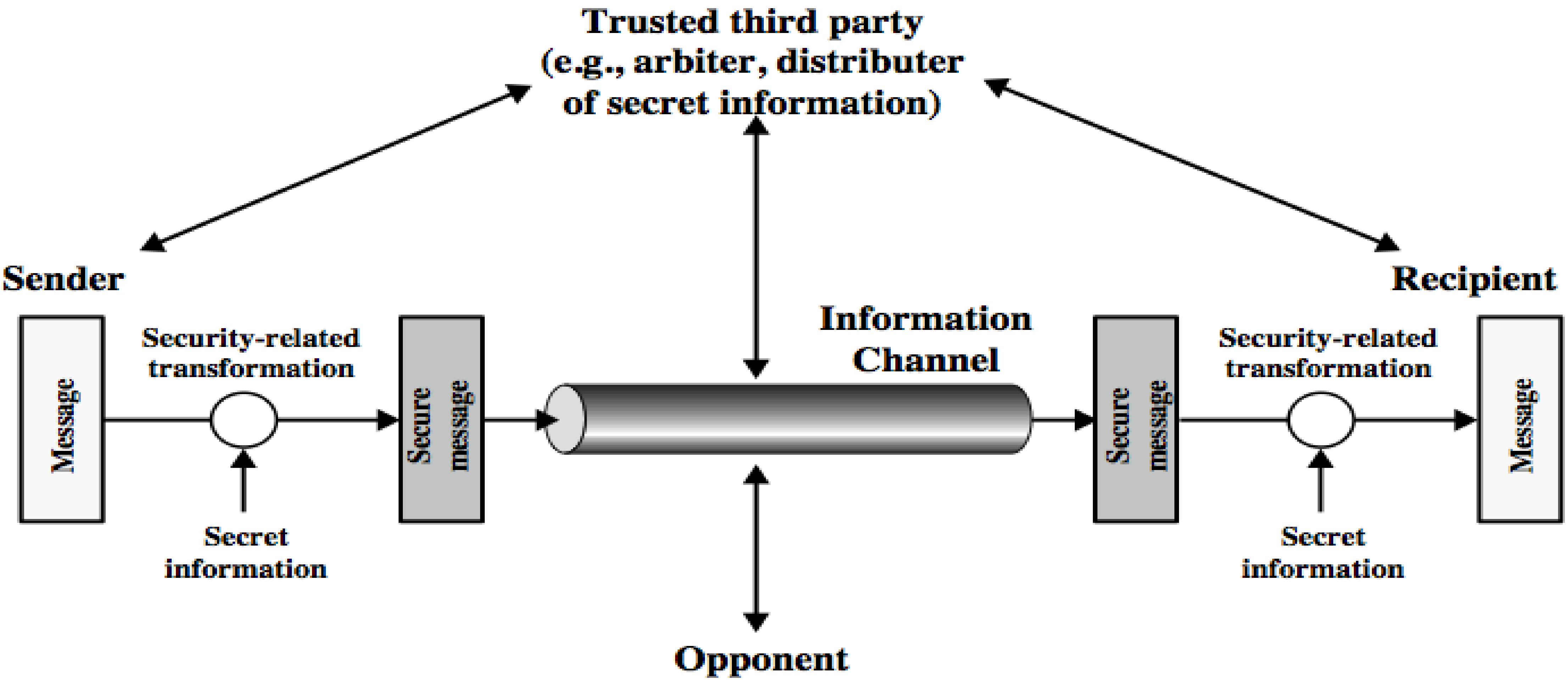
The specific means of implementing one or more security services.

- 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:
  - 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

A MODEL FOR NETWORK SECURITY

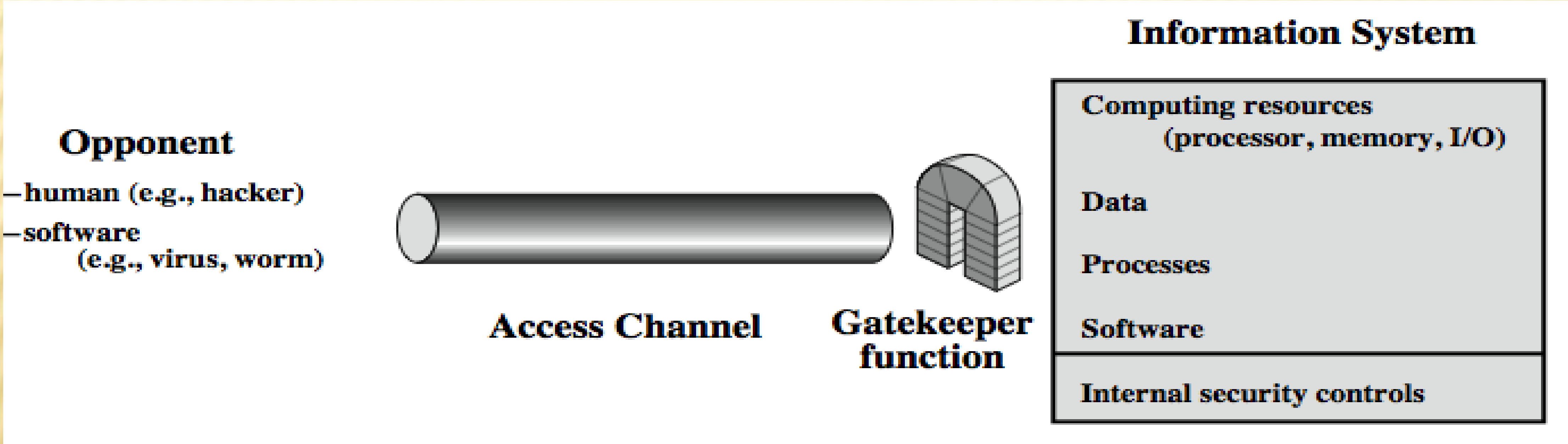


MODEL FOR NETWORK SECURITY

Using 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 principals to use the transformation and secret information for a security service

MODEL FOR NETWORK ACCESS SECURITY



MODEL FOR NETWORK ACCESS SECURITY

- appropriate controls are needed on the access to and within the system, to provide suitable security.

- using 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

- topic roadmap & standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security

REVIEW QUESTIONS

- 1.1 What is the OSI security architecture?
- 1.2 What is the difference between passive and active security threats?
- 1.3 List and briefly define categories of passive and active security attacks.
- 1.4 List and briefly define categories of security services.
- 1.5 List and briefly define categories of security mechanisms.

THANK YOU