

# COMPUTER SECURITY

## SEGMENT-1

INSTRUCTOR: SAZID ZAMAN  
KHAN

ASSISTANT PROFESSOR , CSE,  
IIUC



# Textbooks and Syllabus

- **Textbooks:**
- 1. Cryptography and Network Security, Principles and Practice (7<sup>th</sup> Edition)
- -William Stallings.
- 2. Lecture sheets from Prof. Avinash Kaak.
- 3. Understanding Cryptography
- -Christoph Paar
- Some other textbooks hopefully :)
- **Syllabus:**
- I will provide you the syllabus.

# Definition of Computer Security

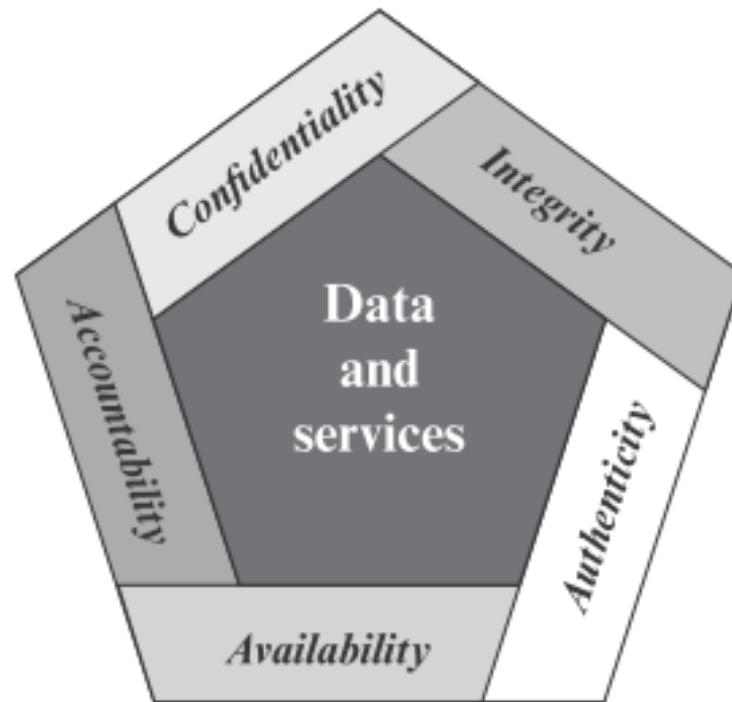
- The NIST Computer Security Handbook [NIST95] defines the term computer security as follows:
- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

- This definition introduces 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 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: This term covers two related concepts:
- Data integrity: Assures that information (both stored and in transmitted packets) 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.
- These three concepts form what is often referred to as the CIA triad.

# Two other significant security concepts

- 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.




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

# Use cases of the security concepts

- **CONFIDENTIALITY:** Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA).
- **INTEGRITY:** Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current.



- 
- AVAILABILITY The more critical a component or service, the higher is the level of availability required. 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

# Some Challenges

- Security mechanisms typically involve more than a particular algorithm or protocol.
- The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.


# OSI Security Architecture

- The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as
  - ■ Security attack: Any action that compromises the security of information owned by 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.
  - ■ Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

- 
- **Threat**
  - A potential for violation of security, That is, a threat is a possible danger that might exploit a vulnerability.


# Security Attacks

- Passive attacks (Figure 1.2a) are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attacks are the release of message contents and traffic analysis.
- The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

- 
- A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

# Active attacks

- Active attacks (Figure 1.2b) 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.
- A masquerade takes place when one entity pretends to be a different entity.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

- 
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
  - The denial of service prevents or inhibits the normal use or management of communications facilities.



# Security services



- A security service is a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

# Security services



- The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

# Security services

## 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.

## 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

## **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.

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


**Table 1.3** Security Mechanisms (X.800)

| <b>SPECIFIC SECURITY MECHANISMS</b>   | <b>PERVASIVE SECURITY MECHANISMS</b>  |
|---|---|
| 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.  |
| <b>Encipherment</b><br>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.         | <b>Trusted Functionality</b><br>That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).                                    |
| <b>Digital Signature</b><br>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). | <b>Security Label</b><br>The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.                              |
| <b>Access Control</b><br>A variety of mechanisms that enforce access rights to resources.   | <b>Event Detection</b><br>Detection of security-relevant events.  |
| <b>Data Integrity</b><br>A variety of mechanisms used to assure the integrity of a data unit or stream of data units.   | <b>Security Audit Trail</b><br>Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. |
|   | <b>Security Recovery</b><br>Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.                                       |

# A model for network security

- In Figure 1.5. A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.
- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.

- All the techniques for providing security have two components:
  - A security-related transformation on the information to be sent. Examples include the encryption of the message. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission.

- 
- A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information.



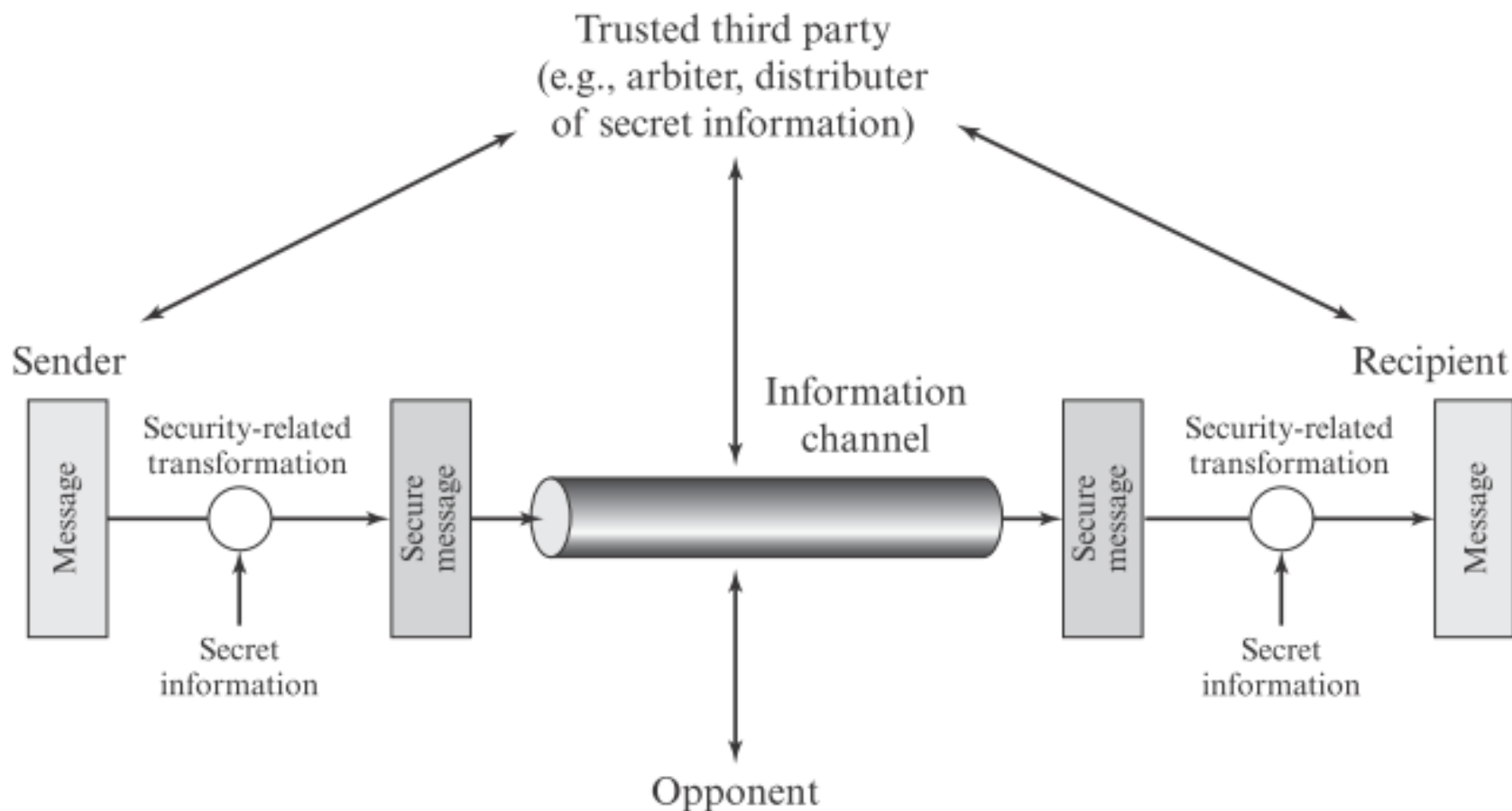


Figure 1.5 Model for Network Security

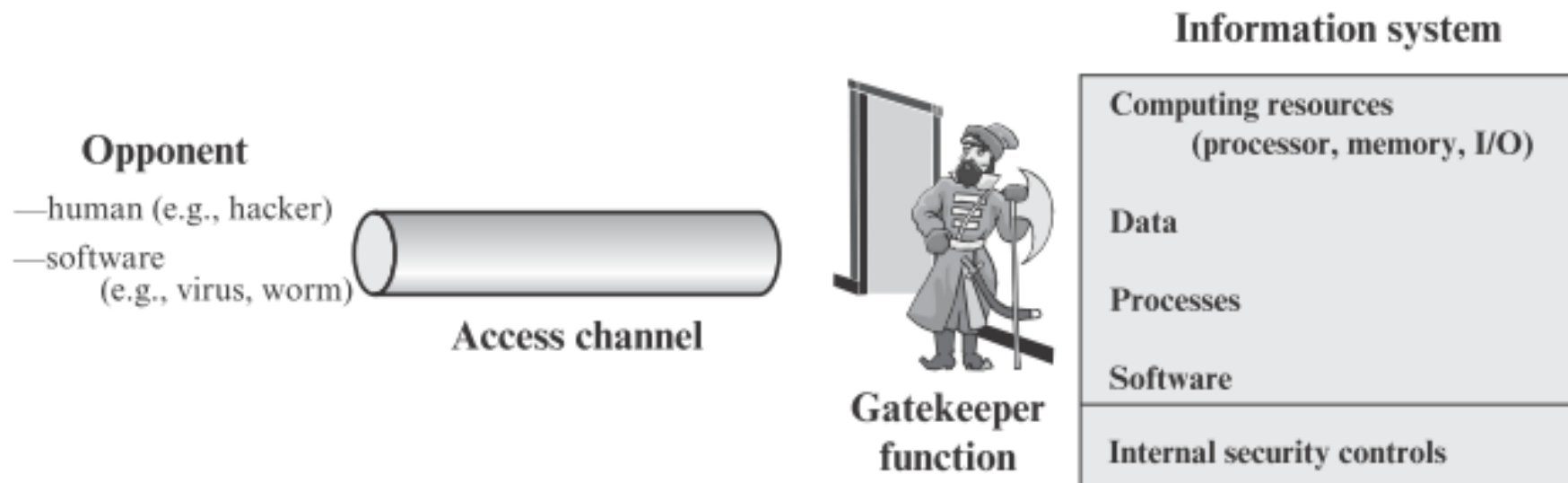


Figure 1.6 Network Access Security Model

# References and disclaimer

- All resources used here are properties of the respective owners. Those are used here for educational purpose.
- **References:**
- 1. Cryptography and Network Security, Principles and Practice (7<sup>th</sup> Edition)
- -William Stallings.