CSE-4743
Computer Security
Part-1
Introduction

Presented by

Asmaul Hosna Sadika
Adjunct Faculty
Dept of CSE, IIUC

Contents

- What is computer security
- Computer Security Key Concepts
- OSI architecture of security
- Security Attacks
- Security Services
- Security Mechanism
- A Model for Network Security

What is Computer Security?

What is Computer Security?

- **Definition:** 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 (including hardware, software, firmware, information/data, and telecommunications).
- Computer security refers to safeguarding computer systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Key concept of Security

Key concept of Security

The 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

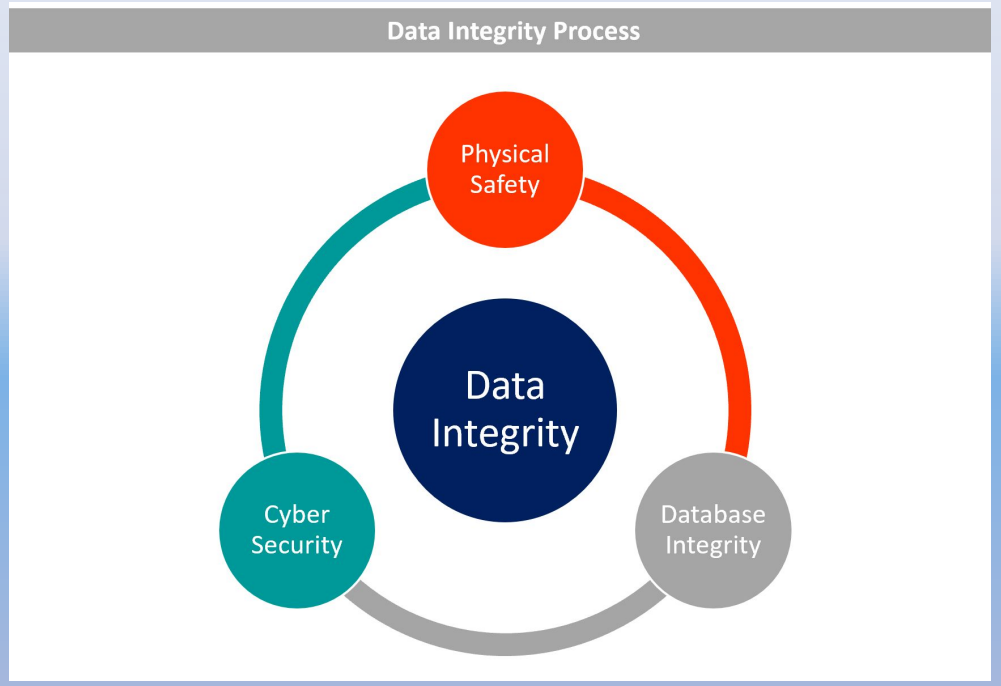
Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Key concept of Security

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 in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system



Key concept of Security

Availability: Assures that systems work promptly and service is not denied to authorized users.

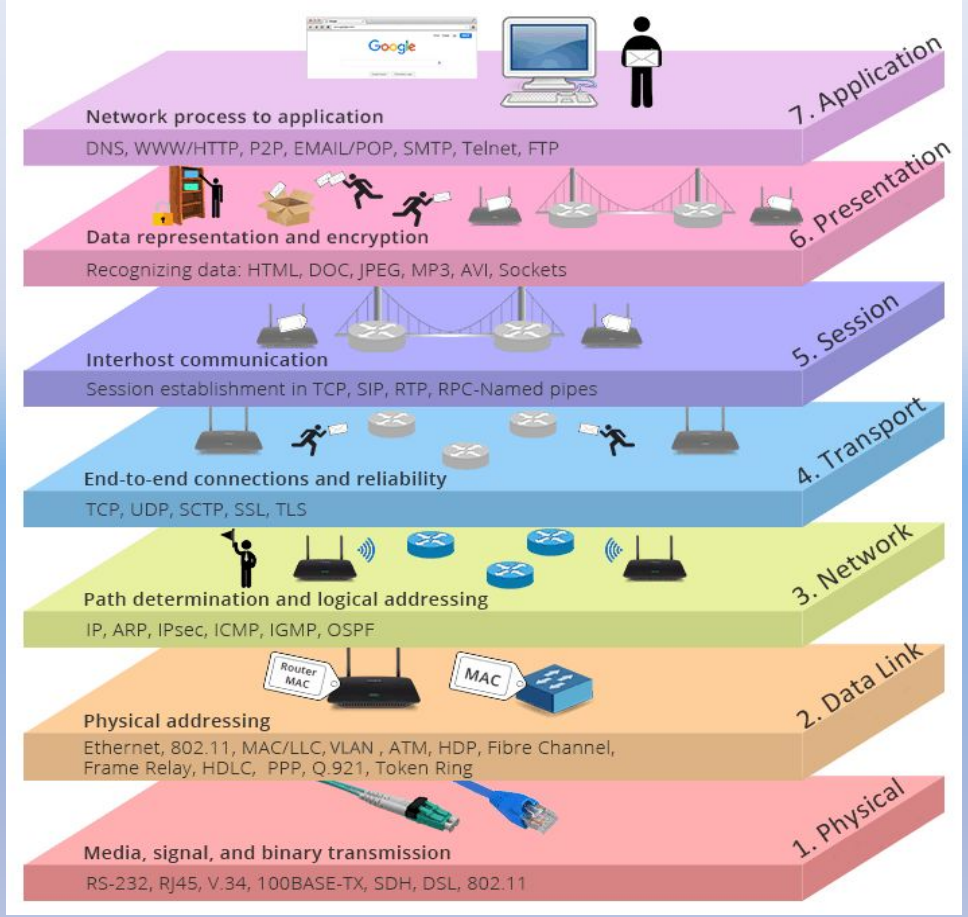
These three concepts form what is often referred to as the CIA triad. The three concepts embody the fundamental security objectives for both data and for information and computing services. For example, the NIST standard FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

The Challenges of Computer Security

1. Security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.
3. Because of point 2, the procedures used to provide particular services are often counterintuitive.
4. Having designed various security mechanisms, it is necessary to decide where to use them.
5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information
6. Computer and network 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.

OSI Security architecture

- **OSI Model Layers**:
  - **Physical Layer**: Securing cables and devices.
  - **Data Link Layer**: MAC address filtering.
  - **Network Layer**: Routers, IPsec.
  - **Transport Layer**: SSL/TLS, firewalls.
  - **Session, Presentation, and Application Layers**: Authentication, encryption, secure protocols.



OSI Security architecture

Why need an architecture?

To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security.

The OSI security architecture is useful to managers as a way of organizing the task of providing security.

Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts of security.

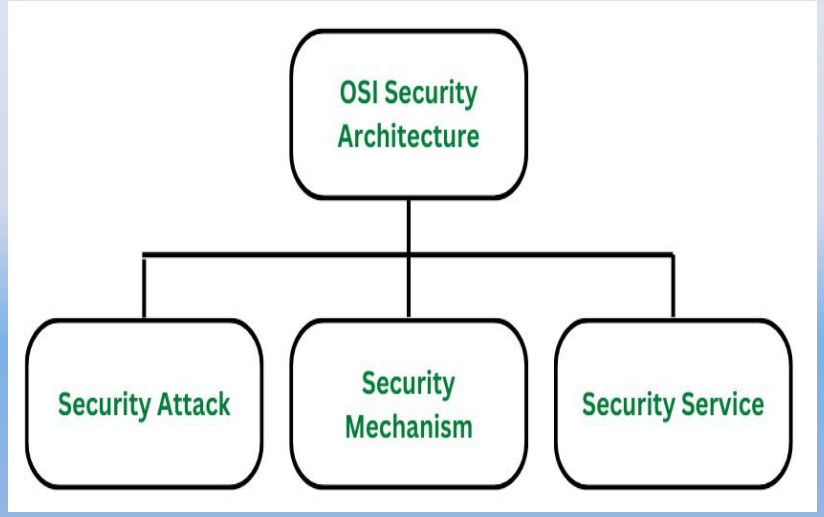
OSI Security architecture

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. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.



Terminology

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
That is, a threat is a possible danger that might exploit a vulnerability.

Example:

Disrupting normal system operation (e.g., power outage, network failure), Unauthorized alteration of data (e.g., changing account balances), and Creating false data or information (e.g., forging documents).

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Example:

An attacker intercepts network traffic to capture login credentials or confidential data.

A hacker launching a denial-of-service (DoS) attack to overwhelm a web server, rendering it inaccessible to legitimate users

Security Attacks

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

I. Active attack

II. Passive attack

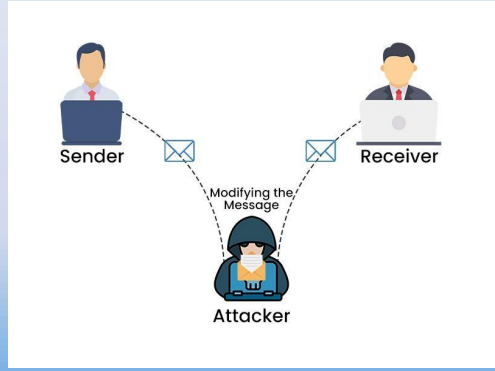
Active attack

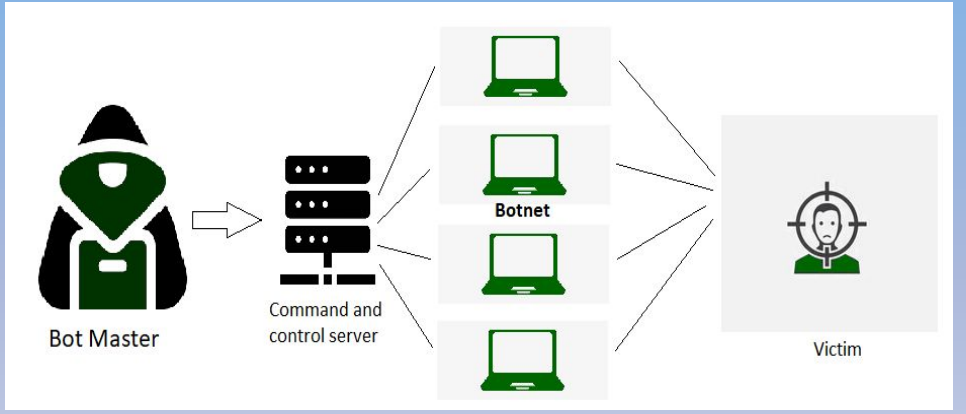
- Active attacks refer to types of attacks that involve the attacker actively disrupting or altering system, network, or device activity.
- Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence.
- Here, both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn't remain in its usual form and shows deviation from its usual behavior.
- This makes active attacks dangerous as there is no information provided of the attack happening in the communication process and the receiver is not aware that the data/ message received is not from the sender.

Active attacks

Active attacks are further divided into four parts based on their behavior:

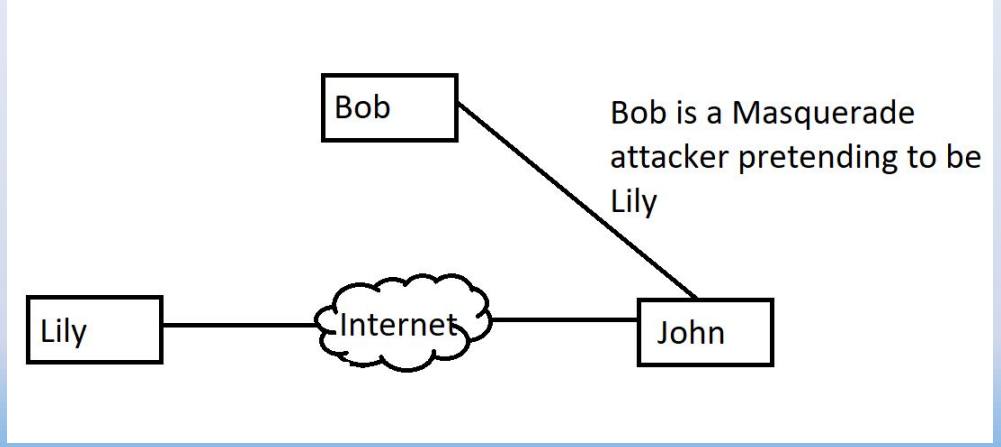
- **Modification of Message:** Modification of Message involves the attacker modifying the transmitted message and making the final message received by the receiver look like it's not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
- **Denial of service (DoS): Denial of Service** attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to users.

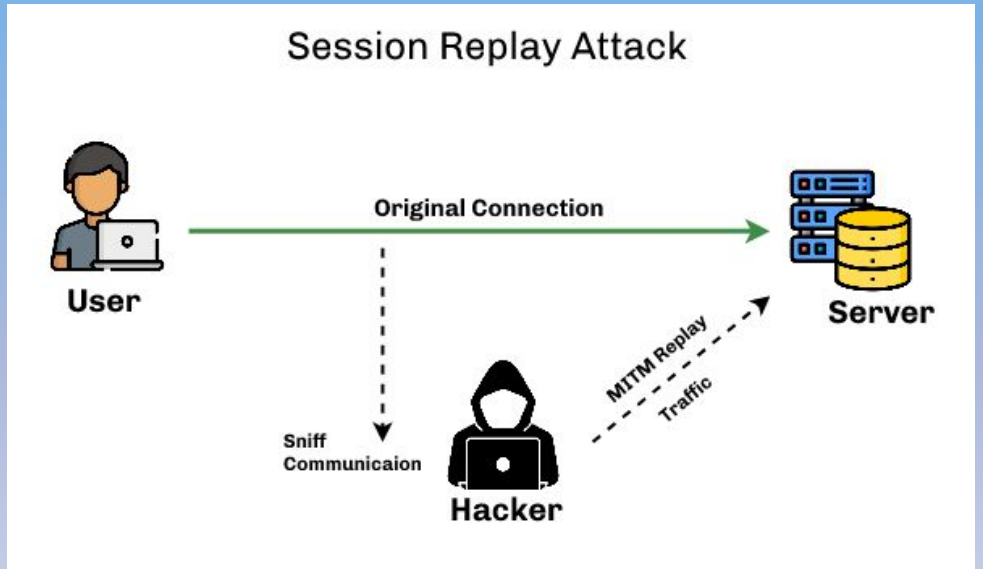




Active attack

- **Masquerade:** Masquerade is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.
- **Replay:** Replay is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.





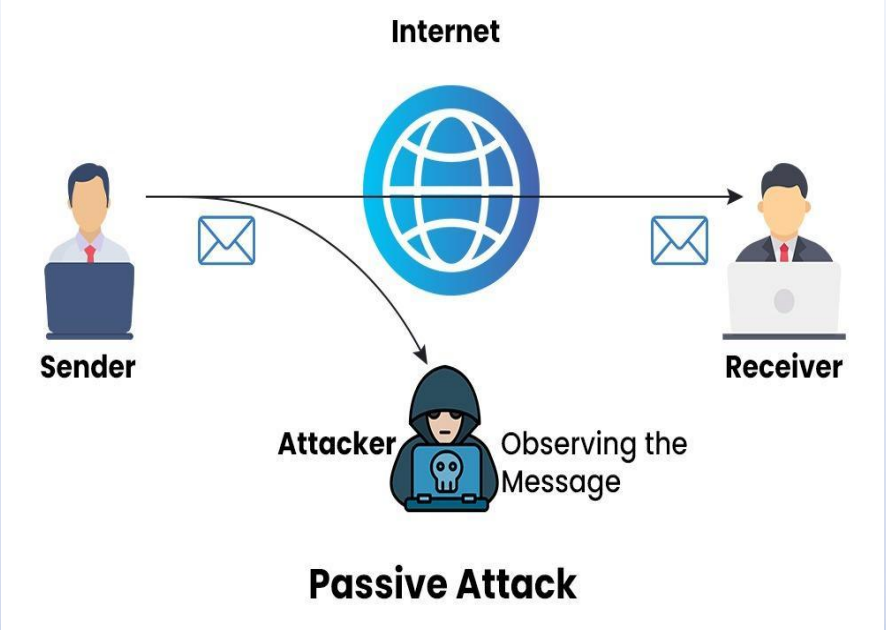
Passive Attack

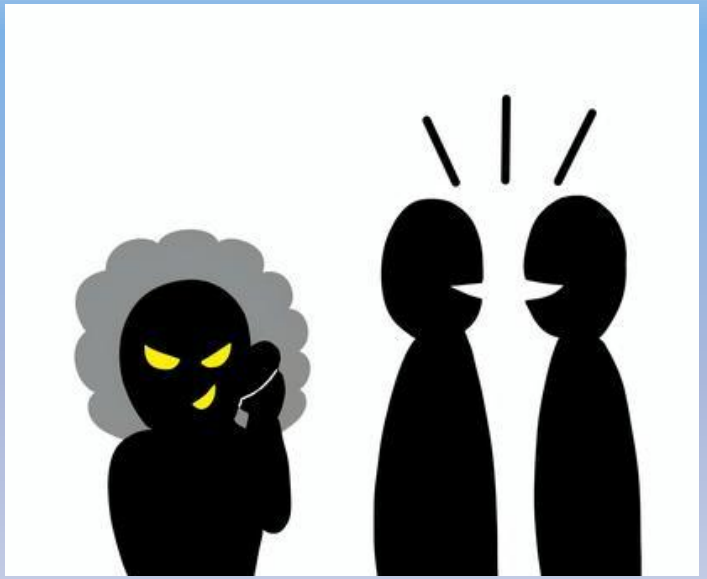
- Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks.
- These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it.
- Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.
- Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder.
- The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process.

Passive attack

Passive attacks are further divided into two parts based on their behavior:

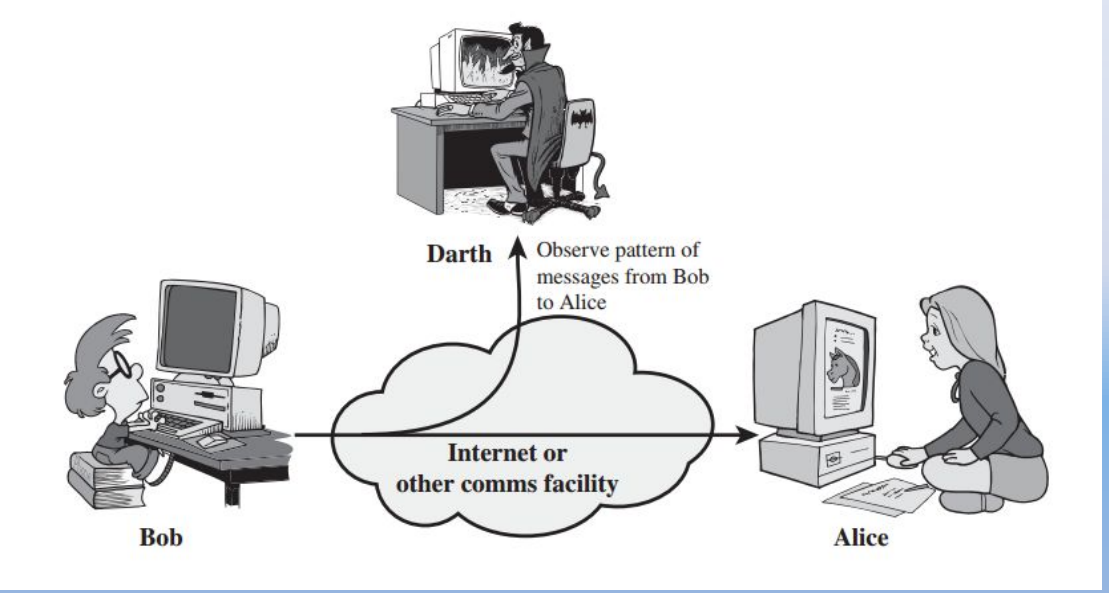
Eavesdropping: Eavesdropping involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.





Passive attack

Traffic analysis: This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.



Security Services

Definition

1. X.800 defines security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
2. Perhaps a clearer definition is found in RFC 4949, which provides the following definition: 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

X.800 divides these services into **five** categories and **fourteen** specific services. Five categories are-

1. Authentication
2. Access control
3. Data confidentiality
4. Data Integrity
5. Data nonrepudiation

Authentication

- Authentication is about **making sure that a communication is from the person or system it says it's from**. This is to prevent anyone from pretending to be someone else.
- Imagine you're receiving a phone call, and you want to be sure it's your friend calling and not a stranger pretending to be your friend. This is what authentication tries to solve in the digital world.
- There are two primary scenarios for authentication:
  - **Single message**: For example, a warning or alarm signal. The service assures the recipient that the message is from the stated source.
  - **Ongoing interaction**: For example, a terminal communicating with a host (like a client-server setup).

Authentication

Two Types of Authentication Services (Defined by X.800):

1. Peer Entity Authentication:

- **What it does**: Makes sure that both parties (like two computers or systems) involved in a conversation are who they say they are.
- **When it's used**: When two systems start talking to each other (like a client connecting to a server) or during the conversation to make sure nothing fishy is going on.
- **Why it’s important**: It prevents someone from pretending to be one of the two parties or using an old, recorded conversation to fake being part of a new one.

Example: Think of a video call. When you connect, this service checks that both people on the call are really who they say they are. Also, during the call, it keeps checking to make sure no one else jumps in pretending to be one of the speakers.

Authentication

2. Data Origin Authentication:

- **What it does**: Confirms that the message or data you received really came from the person or system that claims to have sent it.
- **When it's used**: For things like emails or files, where you're getting a message but not having an ongoing conversation.
- **Why it’s important**: It ensures that the message or data wasn't sent by someone pretending to be the real sender.

Example: When you receive an email, data origin authentication checks to ensure it was actually sent by the person whose name is on it, and not a scammer pretending to be them.

Authentication

Summary:

- **Peer entity authentication** is like checking IDs at the start of a conversation between two people to make sure they're really who they say they are.
- **Data origin authentication** is like making sure a letter you received is really from the person who signed it and not a fake letter.
- Both are about **keeping communications safe** and preventing anyone from **pretending** to be someone else.

Access control

- In simple terms, **access control** in network security is about controlling who can access certain systems or applications over a network.
- Before letting anyone in, the system first checks **who** they are by verifying their identity (this is called **authentication**). Once their identity is confirmed, the system decides **what** they are allowed to do based on their access rights.
- For example, if you try to log into your company's network, the system first checks that it's really you, and then allows you to access only the parts of the network you're authorized to use.

Data confidentiality

- **Confidentiality** means keeping data safe from eavesdroppers or hackers who are trying to secretly listen in (called **passive attacks**).
- There are different levels of confidentiality:
  - **Broad Protection**: This protects **all data** sent between two users. For example, if two computers are connected over a network (like through a TCP connection), all the data exchanged between them is kept secret.
  - **Narrower Protection**: You can also choose to protect just a **single message** or even just parts of a message. However, this approach is usually more complicated and expensive.
- Another part of confidentiality is keeping the overall **traffic flow** secret. This means preventing outsiders from seeing not just the data but also who is sending it, how often, and how much data is being sent. This stops attackers from analyzing patterns in the communication.

Data integrity

- **Data integrity** ensures that the information being sent arrives **exactly as it was sent**—without any changes, errors, or interference.
- There are two main types of data integrity services:
  - **Connection-Oriented Integrity**: This applies to a continuous flow of messages between two systems (like an ongoing conversation). It ensures:
    - No message is **duplicated, inserted, modified, reordered, or replayed**.
    - The data isn't lost or destroyed.
    - This type of integrity also helps protect against attacks like **denial of service (DoS)**.
  - **Connectionless Integrity**: This applies to **individual messages**, not a whole stream. It mainly focuses on ensuring that the message has not been **modified**.

Data integrity

- In short, data integrity ensures that what's sent is what's received, and if there's any tampering or loss, the system either reports it or fixes it.

Nonrepudiation

- **Nonrepudiation** ensures that neither the sender nor the receiver can **deny** sending or receiving a message.
  - If you **send** a message, the receiver can prove that **you** were the one who sent it.
  - If you **receive** a message, the sender can prove that **you** got it.
- This way, both parties are held accountable, and neither can claim they didn't participate in the communication. Nonrepudiation is important for trust and accountability, especially in situations like legal agreements, financial transactions, or sensitive communications.

Security mechanism

X.800 standard defines various **security mechanisms** to protect data and systems during communication. These mechanisms are divided into two categories:

1. **Specific Security Mechanisms**
2. **Pervasive Security Mechanisms**

These mechanisms work together to ensure that communication and data remain secure and protected.

Specific Security Mechanisms

These are applied to particular protocol layers (like TCP or application-layer protocols) to provide security services.

- **Encipherment**: Uses algorithms to transform data into a scrambled form that can only be understood if you have the correct key. It's like locking data in a box, and only those with the key can unlock and read it.
- **Digital Signature**: Adds extra data or transforms the original data so that the receiver can prove it came from the correct sender and hasn't been tampered with. It's like a virtual signature that ensures the message's authenticity and integrity.
- **Access Control**: These are rules that decide who can access what resources, ensuring only authorized users can interact with certain data or systems.
- **Data Integrity**: Mechanisms to ensure data remains unchanged during transmission, so the data you receive is exactly what was sent.

Specific Security Mechanisms

- **Authentication Exchange**: Verifies the identity of a user or system through information exchange.
- **Traffic Padding**: Adds extra data to obscure the real content and frustrate traffic analysis.
- **Routing Control**: Chooses secure routes for data and adjusts them if security threats are detected
- **Notarization**: Uses a trusted third party to confirm certain properties of a data exchange.

Pervasive Security Mechanisms

These mechanisms work across different protocol layers and aren’t tied to any specific security service.

- **Trusted Functionality**: Refers to parts of the system that are trusted to function securely according to predefined rules or a security policy.
- **Security Label**: A marker or tag on data that indicates its security level or attributes (e.g., "confidential" or "public").
- **Event Detection**: Monitors for security-related events, like detecting an unauthorized access attempt.
- **Security Audit Trail**: Collects data about security-related activities, which can be reviewed later for audits to ensure the system is working securely.
- **Security Recovery**: Handles recovery after a security breach or event, helping the system to return to normal operations.

Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Enchipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
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				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

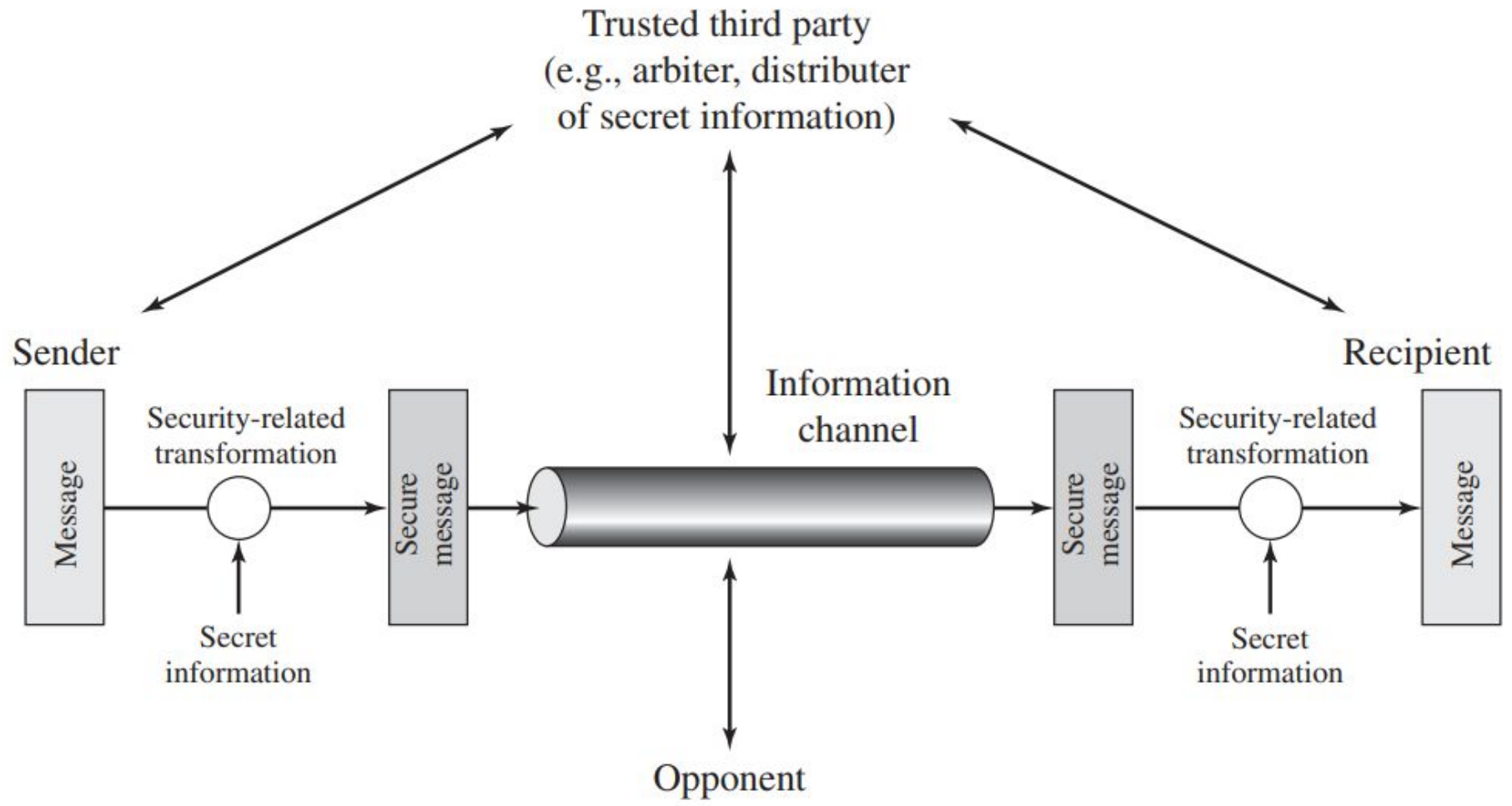


Figure 1.2 Model for Network Security

Model for Network Security

- A message is sent between two parties (the sender and the receiver) over the internet. For secure communication, the parties need to work together using protocols like TCP/IP. Security is important to protect the message from attackers who might try to steal or alter it.
- There are two key parts of securing a message:
  - **Transforming the message**: For example, using encryption to scramble the message so attackers can't read it.
  - **Sharing secret information**: Both parties share a secret, like an encryption key, which the attacker doesn’t know.
  - Sometimes, a **trusted third party** is used to help, such as managing the secret information or solving disputes about the message’s authenticity.

Model for Network Security

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. 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.

users.

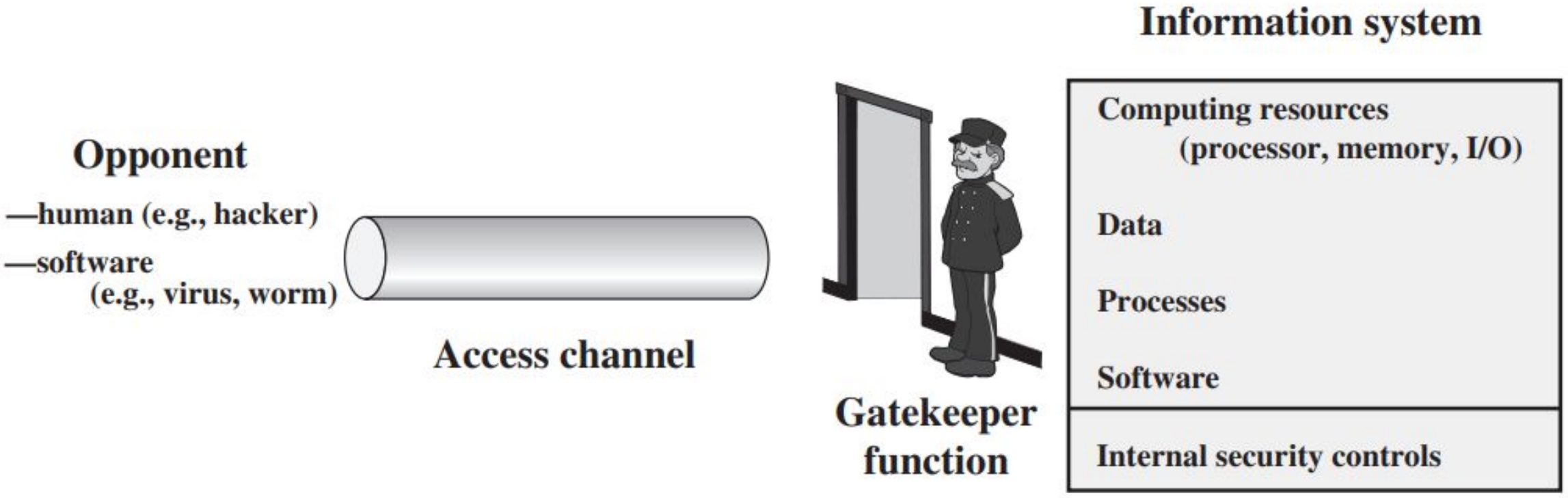


Figure 1.3 Network Access Security Model

Unwanted Access and Threats:

- **Information Access Threats**: Attacks that intercept or modify data to gain unauthorized access.
- **Service Threats**: Attacks that exploit flaws in the system to disrupt or deny services to legitimate users. Examples include viruses and worms, which can be introduced via infected disks or over a network.

Security Mechanisms:

- **Gatekeeper Functions**: Such as password logins and virus detection to block unauthorized access.
- **Internal Controls**: Monitor and detect unauthorized access or breaches within the system

THANK YOU

ANY QUESTIONS