Cryptography

OSI Security Architecture

M S Vilkhu

06 Sep 2024 (C1/C3/C5)

OSI Security Architecture

- ITU-T3 Recommendation X.800, Security Architecture for OSI, defines a **systematic** approach

- The OSI security architecture focuses on
- **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.

Threat & Attack

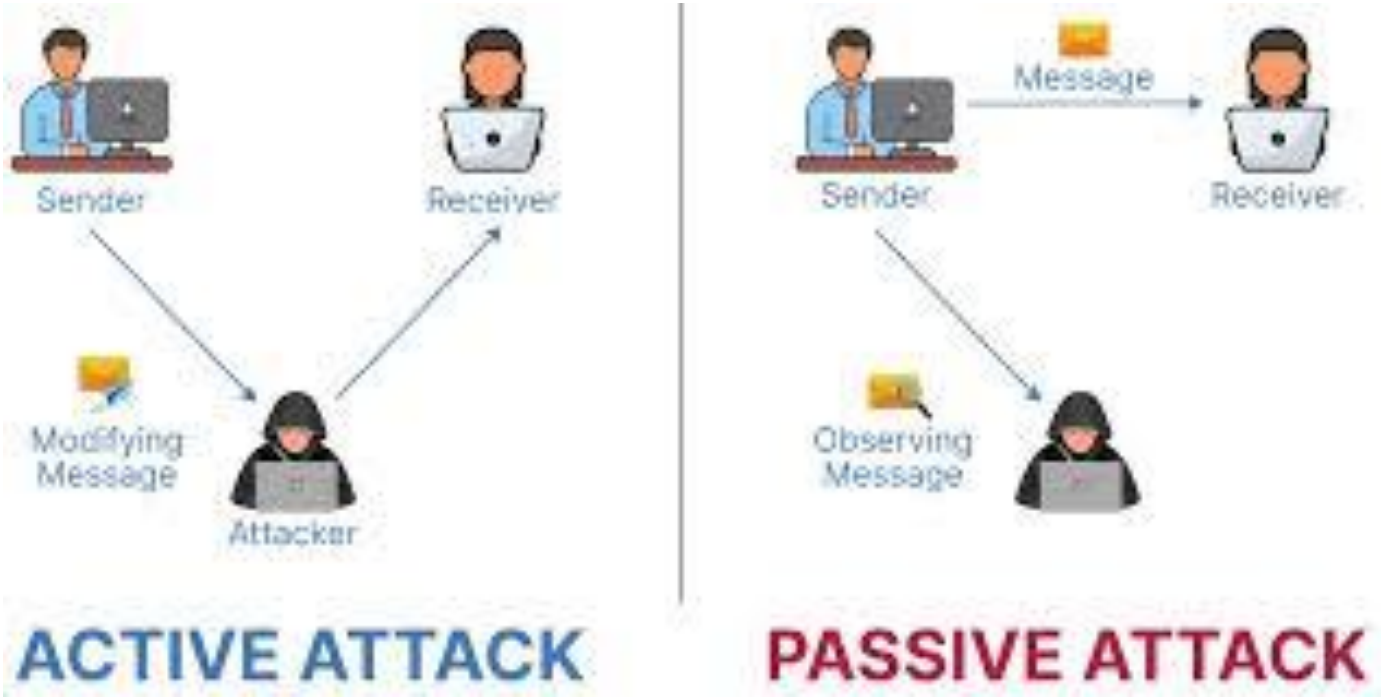
- **Threat**
- A **potential for violation of security**, **which exists** when there is a circumstance, capability, action, or event that **could breach security and cause harm**. That is, a threat is a possible danger that might exploit a vulnerability.

- **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.

Note: RFC 4949

Security Attacks

- **Passive attack**
- **Active attack**



Security Attacks

- **Passive**
- A passive attack attempts to learn or make use of information from the system but **does not affect system resources**.
- **The primary goal** of passive attacks is to **obtain information without being detected**.

- **Examples**:
- **Eavesdropping**: Listening to or intercepting communications between two parties without altering the communication.
- **Traffic Analysis**: Monitoring the flow of data to infer patterns or sensitive information.

Security Attacks

- **Active**
- An active attack attempts to
  - **alter system resources or**
  - **affect their operation**.
  - **unauthorized party makes changes to data**.
  - **modification** or **disruption** of communication.

- **Examples**:
- **Masquerade**: An attacker **pretends to be an authorized user**, often by using stolen credentials.
- **Replay**: An attacker **intercepts and retransmits a valid data transmission**, often to gain **unauthorized access** or repeat transactions.
- **Modification**: An attacker **alters data in transit or stored data to achieve unauthorized effects**.
- **Denial of Service (DoS)**: An attack that **disrupts the normal functioning** of a network or service, making it unavailable to legitimate users.

Security Services

- X.800, a recommendation by the International Telecommunication Union (ITU-T), defines a security service as:

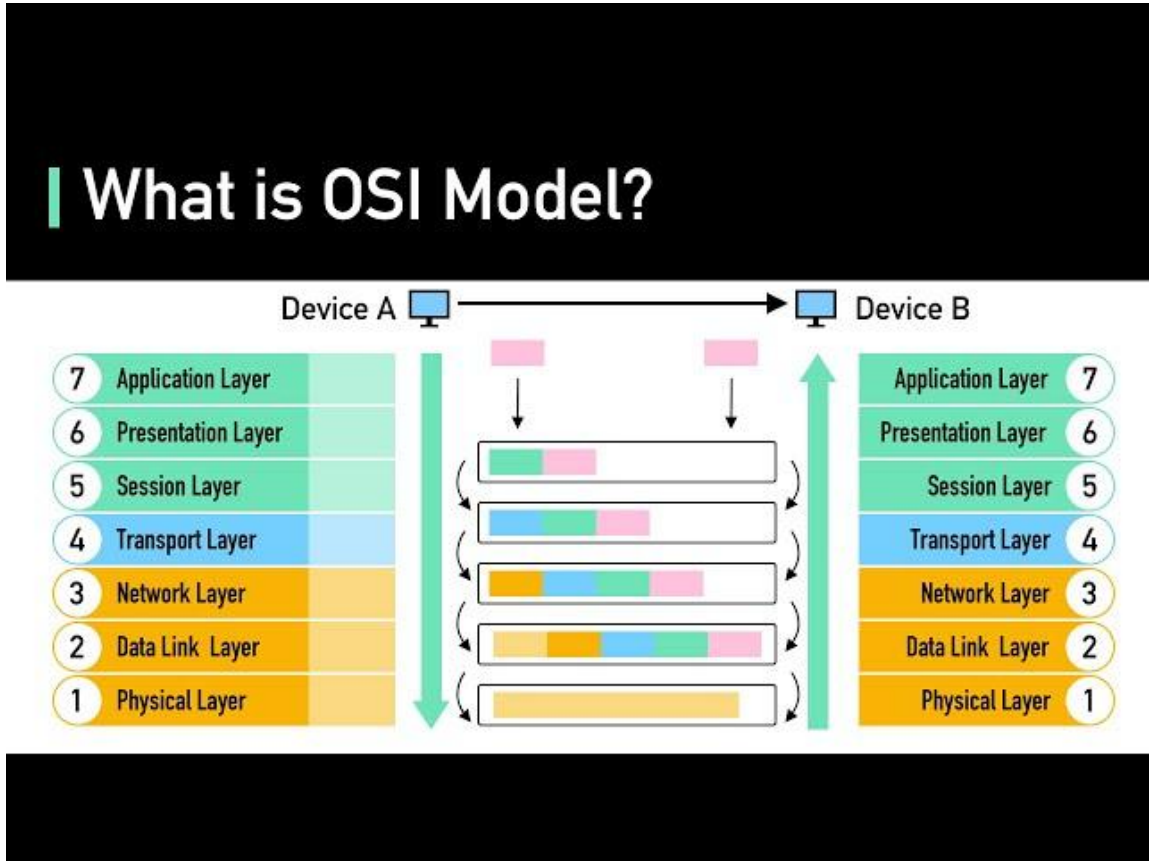
> **"A service** that is provided **by a protocol layer of communicating open systems** and that ensures **adequate security of the systems or of data transfers."**

Definitions:

1. **Service Provided by a Protocol Layer**:
2. **Communicating Open Systems**:
3. **Ensures Adequate Security**:
4. **Systems or Data Transfers**:

Security Service : definitions

1. **Service Provided by a Protocol Layer**:
    1. The security service is implemented **within a specific layer of a communication protocol**. It can be at **any level of the OSI** (Open Systems Interconnection) model, depending on the **type of security required** (e.g., **application layer**, **network layer**).



Security Services : definitions

1. **Service Provided by a Protocol Layer**:
   - The security service is implemented **within a specific layer of a communication protocol**. It can be at **any level of the OSI** (Open Systems Interconnection) model, depending on the **type of security required** (e.g., **application layer**, **network layer**).
2. **Communicating Open Systems**:
   - The term "**open systems" refers** to systems that are **designed to interoperate with others**. X.800 focuses on security in such environments, where **data is exchanged between different systems.**
3. **Ensures Adequate Security**:
   - The primary goal of the security service is to provide the **necessary level of security**, which can include **protecting data integrity, confidentiality, authentication, or availability,** depending on the specific needs of the system.
4. **Systems or Data Transfers**:
   - Security services **can protect entire systems** or **just specific data transfers between systems**. This protection can be against various threats, including unauthorized access, modification, or denial of service.

Cryptography

OSI Security Architecture

M S Vilkhu

13 Sep 2024 ((C1/C3/C5)

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

1. **Authentication**
2. **Access Control**
3. **Data Confidentiality**
4. **Data Integrity**
5. **Non-Repudiation**

- Let's define these terms

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

1. Authentication

- Authentication services are designed to verify the identity of communicating entities and the origin of data.
- **Peer Entity Authentication**:
  - Ensures that the entity at the other end of a communication is who it claims to be, typically used in connection-oriented services like a session between two systems.
- **Data-Origin Authentication**:
  - Verifies the source of the data received, ensuring that the data has originated from a legitimate entity. This is crucial for ensuring the integrity of messages.

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

2. Access Control

- Access control services prevent unauthorized use of resources and regulate who can access what within a system.
- **Access Control**:
  - Ensures that resources are used only by authorized entities. This service can involve mechanisms like access control lists, authentication mechanisms, and encryption

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

3. Data Confidentiality

- Data confidentiality services protect data from unauthorized disclosure, both during storage and transmission.
- **Connection Confidentiality**:
  - Provides confidentiality of all user data transmitted over a secured connection.
- **Connectionless Confidentiality**:
  - Protects data in a connectionless environment, typically at the level of individual data packets.
- **Selective-Field Confidentiality**:
  - Protects specific fields within a data packet or message, rather than the entire packet.
- **Traffic Flow Confidentiality**:
  - Conceals the characteristics of the data flow to prevent unauthorized users from analyzing traffic patterns.

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

4. Data Integrity

- Data integrity services ensure that data has not been altered, either accidentally or maliciously, during transmission or storage.
- **Connection Integrity with Recovery**:
  - Provides integrity of data transmitted over a connection and includes mechanisms for recovery from detected errors.
- **Connection Integrity without Recovery**:
  - Ensures data integrity but does not provide mechanisms for error recovery.
- **Selective-Field Connection Integrity**:
  - Ensures the integrity of specific fields within the data transmitted over a connection.
- **Connectionless Integrity**:
  - Provides integrity in a connectionless environment, typically on a per-packet basis, to detect and protect against data alteration.
- **Selective-Field Connectionless Integrity**:
  - Ensures the integrity of specific fields within data in a connectionless environment.

X.800

- X.800 divides security services into **five broad categories** and **specifies fourteen distinct services** within those categories. These services are designed to address different security needs and threats in open systems. Below is the breakdown:

5. Non-Repudiation

- Non-repudiation services ensure that neither the sender nor the receiver of a message can deny having processed the message.
- **Non-Repudiation with Proof of Origin**:
  - Provides proof to the recipient that the originator sent the message, preventing the sender from denying it.
- **Non-Repudiation with Proof of Delivery**:
  - Provides proof to the sender that the message was delivered to the intended recipient, preventing the recipient from denying receipt.

Types of Security Services (as per X.800)

- X.800 outlines several **types of security services** that can be applied across different layers of the OSI model:

1. Authentication:
2. Access Control:
3. Data Confidentiality:
4. Data Integrity:
5. Non-Repudiation:
6. Availability:

Types of Security Services (as per X.800)

- X.800 outlines several types of security services that can be applied across different layers of the OSI model:

1. **Authentication**:
   - **Peer Entity Authentication**: Ensures that the entities **involved in communication are authentic** (verifies the identities of the parties).
   - **Data-Origin Authentication**: Ensures that the **source of the received data is authentic.**
2. **Access Control**:
   - Prevents **unauthorized use of resources**. It regulates who can access data or services, based on identity or other credentials.
3. **Data Confidentiality**:
   - Protects data from **unauthorized disclosure**. This can involve **encryption** and other methods to ensure that only authorized parties can view the data..

Types of Security Services (as per X.800)

- X.800 outlines several types of security services that can be applied across different layers of the OSI model:

4. **Data Integrity**:
   - Ensures that **data has not been altered or tampered with**. This service can detect and prevent unauthorized data modification.
5. **Non-Repudiation**:
   - **Provides proof of the origin and delivery of data**, preventing the sender or receiver from **denying having processed** the data.
6. **Availability**:
   - Ensures that systems and data are accessible and functional when required, **protecting against attacks that would cause disruptions, such as Denial of Service (DoS) attacks.**

In summary, according to X.800, a **security service is a mechanism** provided by **communication protocols** that ensures various aspects of security—such as confidentiality, integrity, and authentication—are **maintained in open systems and during data transfers**. These services are essential for protecting data and systems from a wide range of security threats.

Security Mechanism

- lists the security mechanisms defined in X.800.
- The mechanisms are divided into
  - **implemented in a specific protocol layer**, such as **TCP or an application-layer** protocol, and
  - those that are **not specific to any particular protocol** layer or security service.

Security Mechanism

- Relationship between **Security service** and **mechanism mapping**

SERVICE \ MECHANISM	Encipherment	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			

Security Mechanism

- X.800 distinguishes between
- **reversible encipherment** mechanisms
- **irreversible encipherment** mechanisms.

- A **reversible encipherment** mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted.

- **Irreversible encipherment** mechanisms include **hash algorithms and message authentication codes**, which are used in digital signature and message authentication applications.

Fundamental Security Design Principles

- There are many design principles but would like to define following. These a concepts to be applied at all places.

- Least privileges
- Separation of duties
- Défense in depth

Fundamental Security Design Principles

- **Least privileges**
- Least Privilege is a fundamental security principle that ensures that users, programs, or processes are given the **minimum** levels of access — or permissions — necessary to perform their functions or tasks. By restricting access rights, the system reduces the risk of accidental or malicious actions that could compromise security.
- **Separation of duties**
- Separation of Duties (SoD) is a security principle that **divides responsibilities** and tasks among multiple people or systems to **prevent any one individual** or entity from having **complete control over all critical functions**. This reduces the risk of fraud, error, or abuse because no single person has enough privileges to perform malicious or harmful actions without oversight or detection.
- Défense in depth

Fundamental Security Design Principles

- **Défense in depth**
- Defense in Depth is a security strategy that employs multiple layers of defense to protect systems, networks, and data. The idea is to **create redundancy** in security measures, so that if **one layer is compromised**, additional layers are in place to slow down, detect, or mitigate an attack.
  - **Multiple Layers of Protection**: Security is not reliant on a single defense mechanism. Instead, it uses a combination of different measures (e.g., firewalls, encryption, access controls) to create overlapping defenses.
  - **Redundancy**: Each layer compensates for potential weaknesses in the others. For example, if an attacker bypasses a firewall, they might still encounter strong authentication, encryption, or intrusion detection systems.
  - **Security at Different Levels**: Defense in depth is applied across all levels of an organization's IT infrastructure:

Attack Surfaces and Attack Trees

- Already done - overview of the **spectrum of security threats** and **attacks facing** computer and network systems. about the **nature of attacks** and the **types of adversaries** that present security threats.

- **two concepts** that are useful in **evaluating and classifying threats**:
- attack surfaces
- attack trees.

Attack Surfaces and Attack Trees

Attack Surfaces

- An **attack surface** consists of the **reachable** and **exploitable vulnerabilities** in a system

- **Examples** :
- **Open ports** on outward facing Web and other servers, and code **listening on those** ports
- **Services** available on the inside of a firewall
- **Code that processes** incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- **Interfaces**, SQL, and Web forms
- An **employee** with **access to sensitive information** vulnerable to a social engineering attack

Attack Surfaces and Attack Trees

Attack Surfaces

- Can be categories as
- **Network attack surface**: This category refers to **vulnerabilities** over an enterprise network, wide-area network, or the Internet. Included in this category are **network protocol vulnerabilities**, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
- **Software attack surface**: This refers to **vulnerabilities** in application, utility, or operating system code. A particular focus in this category is **Web server software**.
- **Human attack surface**: This category refers to **vulnerabilities created by personnel** or outsiders, such as social engineering, human error, and trusted insiders.

Attack Surfaces and Attack Trees

Attack Surfaces

- An **attack surface analysis** is a useful technique for assessing the **scale and severity** of threats to a system.
- A **systematic analysis** of points of vulnerability **makes developers and security analysts** aware of where security mechanisms are required.
- Once an attack surface is defined, designers may be able to **find ways to make the surface smaller,** thus making the **task of the adversary more difficult**.
- The attack surface also provides **guidance on setting priorities** for testing, strengthening security measures, and modifying the service or application

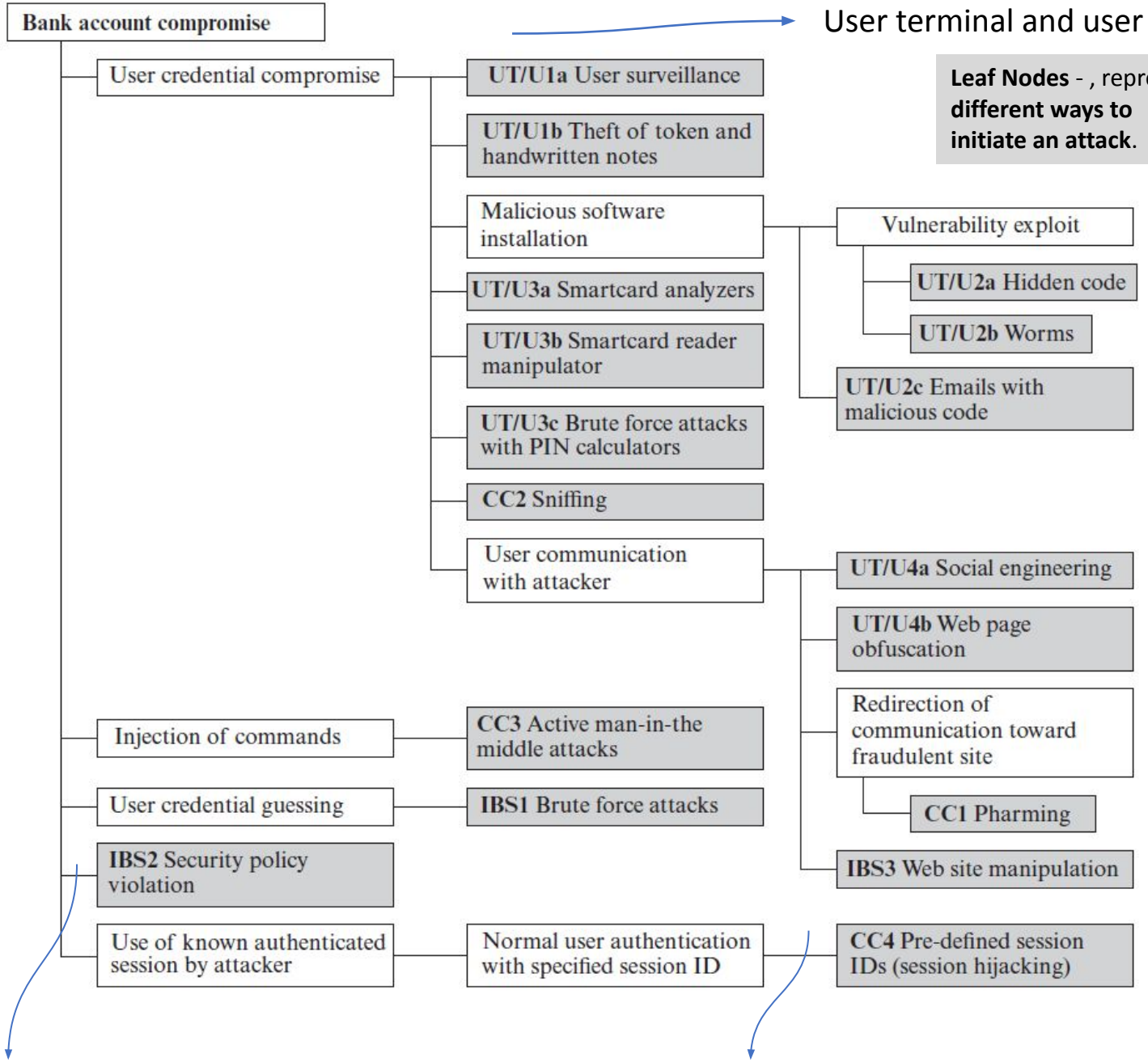
Attack Surfaces and Attack Trees

Attack Tree

- An **attack tree** is a branching, **hierarchical data structure** that represents a **set of potential techniques for exploiting security vulnerabilities**
- The **security incident – goal of attacker -** represented as the **root node of the tree**, and the ways that an attacker could reach that goal are **iteratively and incrementally** represented as branches and sub-nodes of the tree.
- Each sub-node defines a subgoal, and each subgoal may have its own set of further subgoals, and so on.
- **The final nodes** on the paths outward from the root, that is, **the leaf nodes**, represent **different ways to initiate an attack**.
- Each node other than a leaf is either an **AND-node** or an **OR-node**.
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared.

Attack Tree

Attack Surfaces and Attack Trees



Attack Surfaces and Attack Trees

- **User terminal and user (UT/U):** These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user.
- **Communications channel (CC):** This type of attack focuses on communication links.
- **Internet banking server (IBS**): These types of attacks are offline attacks against the servers that host the Internet banking application**.**

Attack Strategies

- **Five overall attack strategies** can exploits one or more of the three components.
- The five strategies are as follows

1. User credential compromise
2. Injection of commands
3. User credential guessing
4. Security policy violation
5. Use of known authenticated session

Attack Strategies

- **Five overall attack strategies**

1. **User credential compromise**

- There are procedural attacks, such as **monitoring a user's action to observe a PIN or other credential, or theft of the user's token or handwritten notes**.
- **compromise token information** using a variety of token attack tools, such as hacking the smartcard or using a **brute force approach to guess** the PIN.
- Another possible strategy is to **embed malicious software to compromise the user's login** and password.
- attempt to obtain credential information via the **communication channel (sniffing)**.

Attack Strategies

- **Five overall attack strategies**

2. Injection of commands

In this type of attack, the attacker is able to **intercept communication** between the UT and the IBS. Various schemes can be used to be **able to impersonate the valid user** and so **gain access** to the banking system.

Attack Strategies

- **Five overall attack strategies**

3. User credential guessing

- **brute force attacks** against some banking authentication schemes are feasible by sending **random usernames and passwords**.
- The attack mechanism is based on **distributed zombie personal computers**, hosting automated programs for username- or password-based calculation.

Attack Strategies

- **Five overall attack strategies**

4. Security policy violation

- **violating** the bank's **security policy** in combination with **weak access control** and **logging mechanisms**,
- an employee may cause an internal security incident and expose a customer's account.

Attack Strategies

- **Five overall attack strategies**

5. Use of known authenticated session

- This type of attack **persuades or forces** the user to connect to the IBS with a **preset session** ID.
- Once the user **authenticates to the server**, the attacker may **utilize the known session ID** to send packets to the IBS, spoofing the user's identity

Model for Network Security

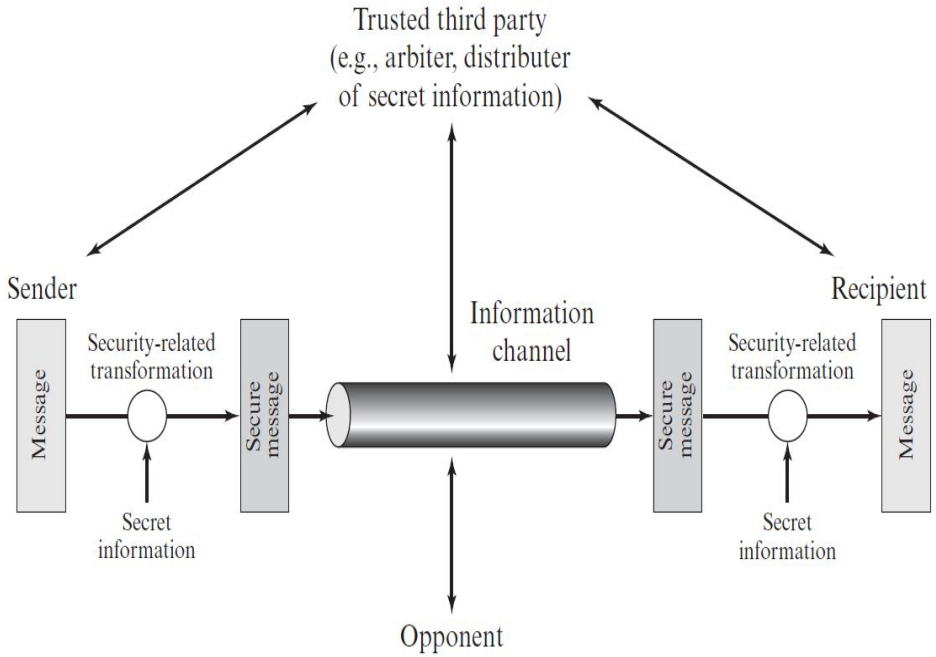
four basic tasks in designing a particular security service:

1. **Design an algorithm** for performing the **security-related transformation**. The algorithm should be such that an **opponent cannot defeat** its purpose.

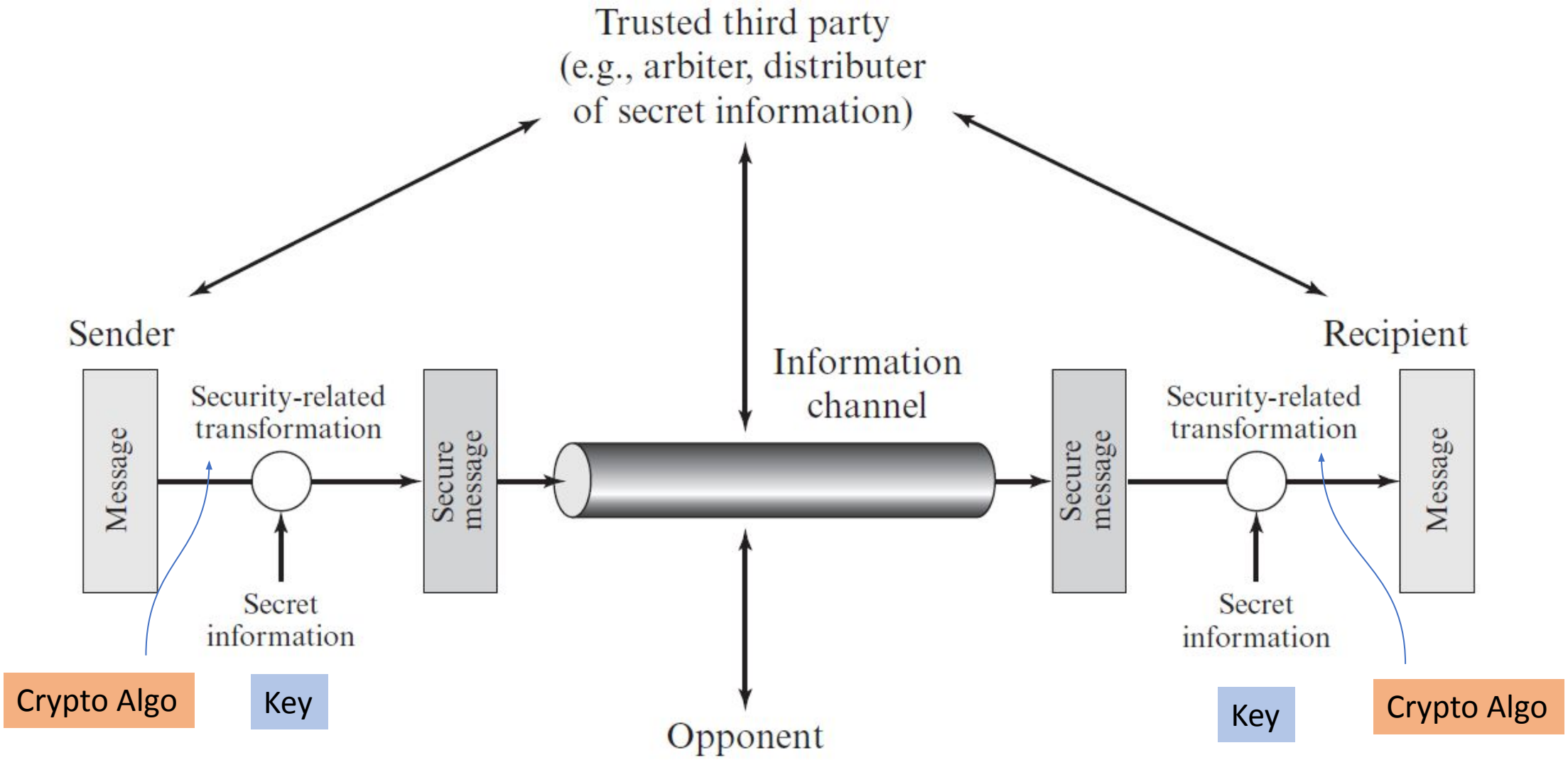
2. **Generate** the **secret information** to be **used with the algorithm**.

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.



Model for Network Security



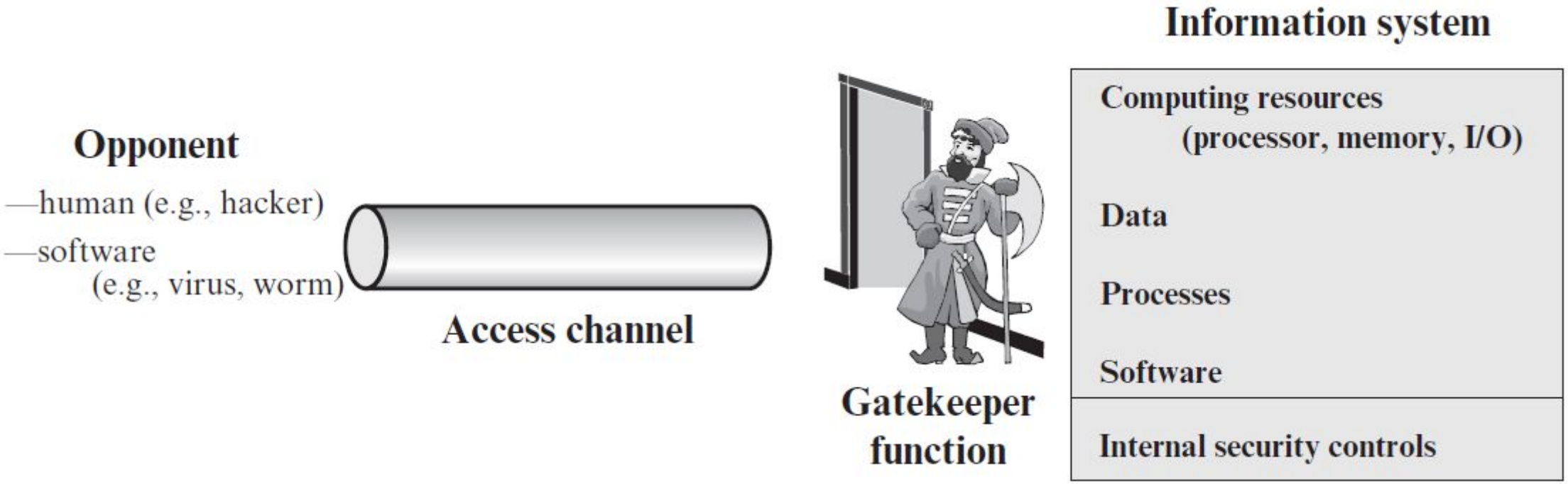
Model for Network Security

- Initial part of the study of cryptography will
- **concentrate on the types of security mechanisms** and services that fit into the model shown in Figure (previous slide).

- there are **other security-related situations** of interest that **do not neatly fit this model** will study in this course.
- A **general model of these** other situations is illustrated in Figure 1.6, which reflects a concern for protecting an information system from unwanted access.

Model for Network Security

- **Network Access Security model**



Information access threats: Intercepts or modifies data

Service threats: Exploit service flaws in computers to inhibit use by legitimate

Thank You