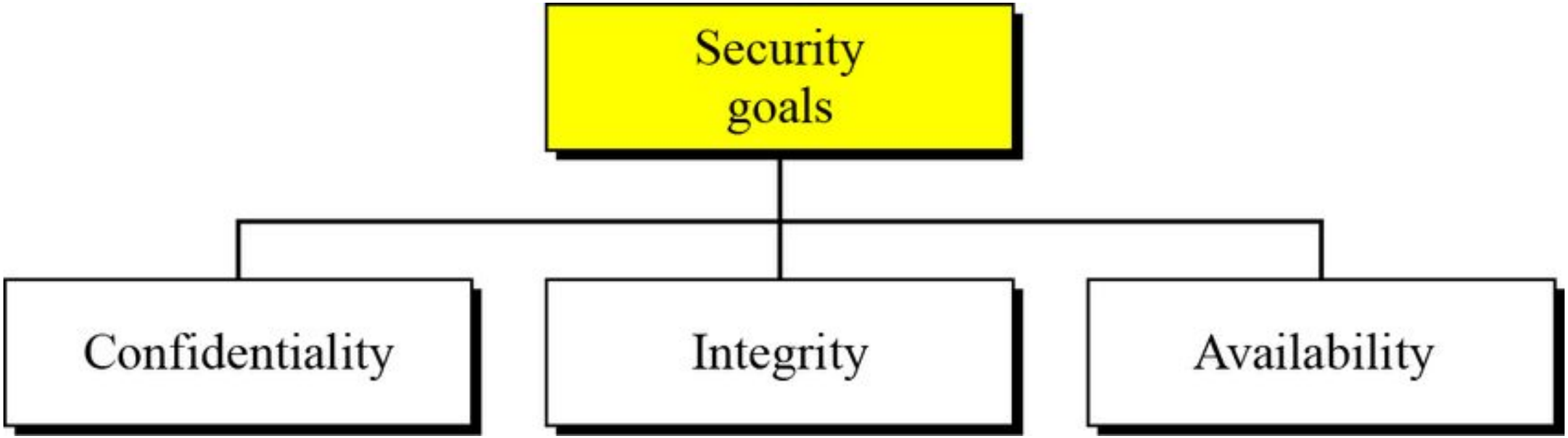
CHAPTER 9

SECURITY

Security

- Security in distributed systems introduces two specific concerns that centralized systems do not have.
- The first is the use of a network where contents may be seen by other, possibly malicious, parties.
- The second is the use of servers.
- Because clients interact with services (applications) running on a server
- Moreover, physical access to the system and the security controls configured for the operating system may be unknown to the client.

SECURITY GOALS



- Computer security is about keeping systems, programs, and data secure. It addresses three broad areas: **confidentiality**, **integrity**, and **availability**. Together, these are referred to as the **CIA Triad**.
- **Confidentiality**
- Confidentiality deals with keeping resources and data hidden from, or inaccessible to, unauthorized individuals.
- It is addressed by access control mechanisms in operating systems or application software.
- If the data may be accessed through the file system or visible over a network, confidentiality is addressed by encrypting the data.
- An application's decisions on whether data should be made accessible to a user depends on identification and authentication of the user or service.

- **Integrity**
- Integrity deals with the trustworthiness of the data or the resources. Integrity mechanisms are responsible for preventing unauthorized changes to data or detecting that changes have been made.
- Integrity mechanisms are used to validate the identity of users, systems, and services through authentication algorithms.
- **Availability**
- Availability is about having access to the data or computing services. It's the property that a system is accessible and properly functioning. Accessibility includes fault tolerance, recovery, and restoration.

SECURITY THREATS

- A threat is 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 enabling the exploitation of a vulnerability.

- There are four types of security threats to consider

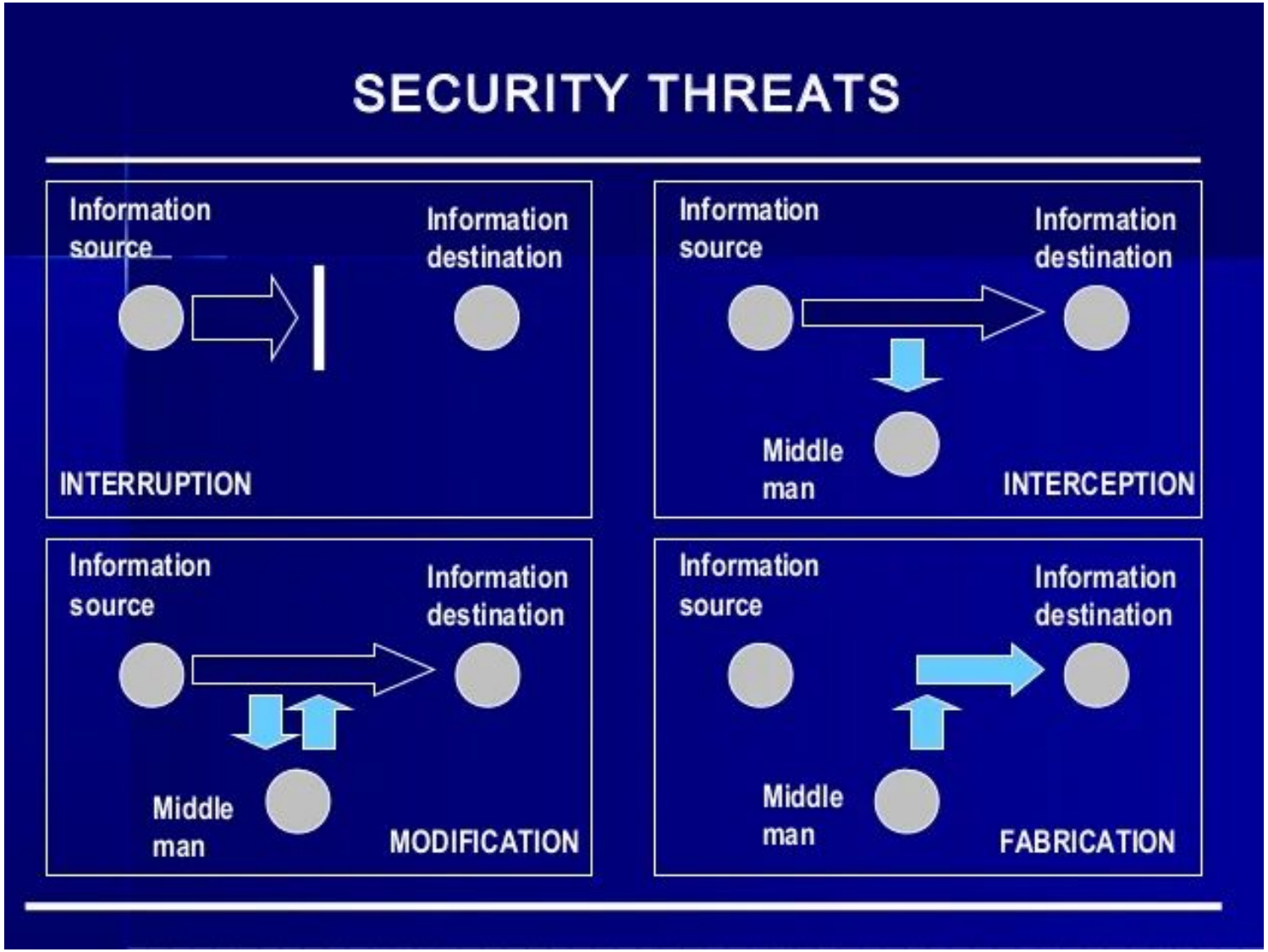
  1. Interception 2 Interruption 3. Modification 4. Fabrication

- Interception - an unauthorized party has gained access to a service or data

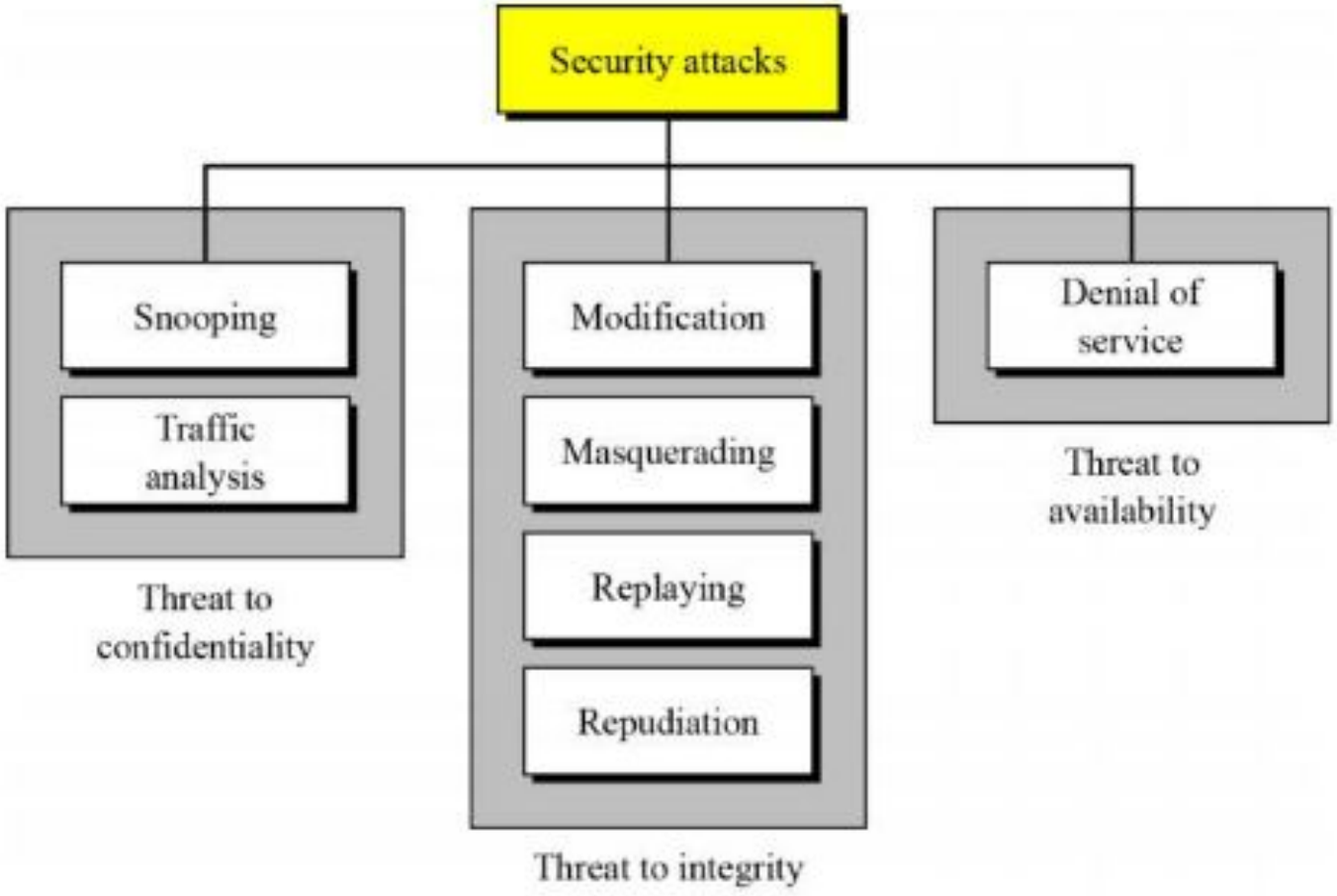
  Eg: eavesdropping , illegal copying
- Interruption - attempts to make a service inaccessible to other parties

  Eg: ddos
- Modification - unauthorized changing of data or tampering with a service

  Eg: changing values
- Fabrication - additional data or activity are generated that would normally not exist. A fabrication attack **creates illegitimate information, processes, communications or other data within** a system.


SECURITY THREATS
Information source
Information destination
INTERRUPTION
Information source
Information destination
Middle man
INTERCEPTION
Information source
Information destination
Middle man
MODIFICATION
Information source
Information destination
Middle man
FABRICATION

SECURITY ATTACKS



- **Snooping :**Snooping, the unauthorized interception of information, is a form of disclosure.
-
- It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information.

- **Traffic Analysis:** It is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- An attacker can gain important information by monitoring the frequency and timing of network packets.

- **Modification**: After intercepting or accessing information, the interceptor modifies the information to make it beneficial to itself.

- For example, a customer sends a message to a bank to do some transaction.

- The attacker intercepts the message and changes the type of transaction to benefit itself.

- **Masquerading:** Masquerading, or spoofing, happens when the attacker impersonates somebody else.
- It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.

- **Replaying :**It is an attack in which a service already authorized and completed is forged by another “duplicate request” in an attempt to repeat authorized commands.

- For example, a person sends a request to her bank to ask for payment to the attacker, which has done a job for her.

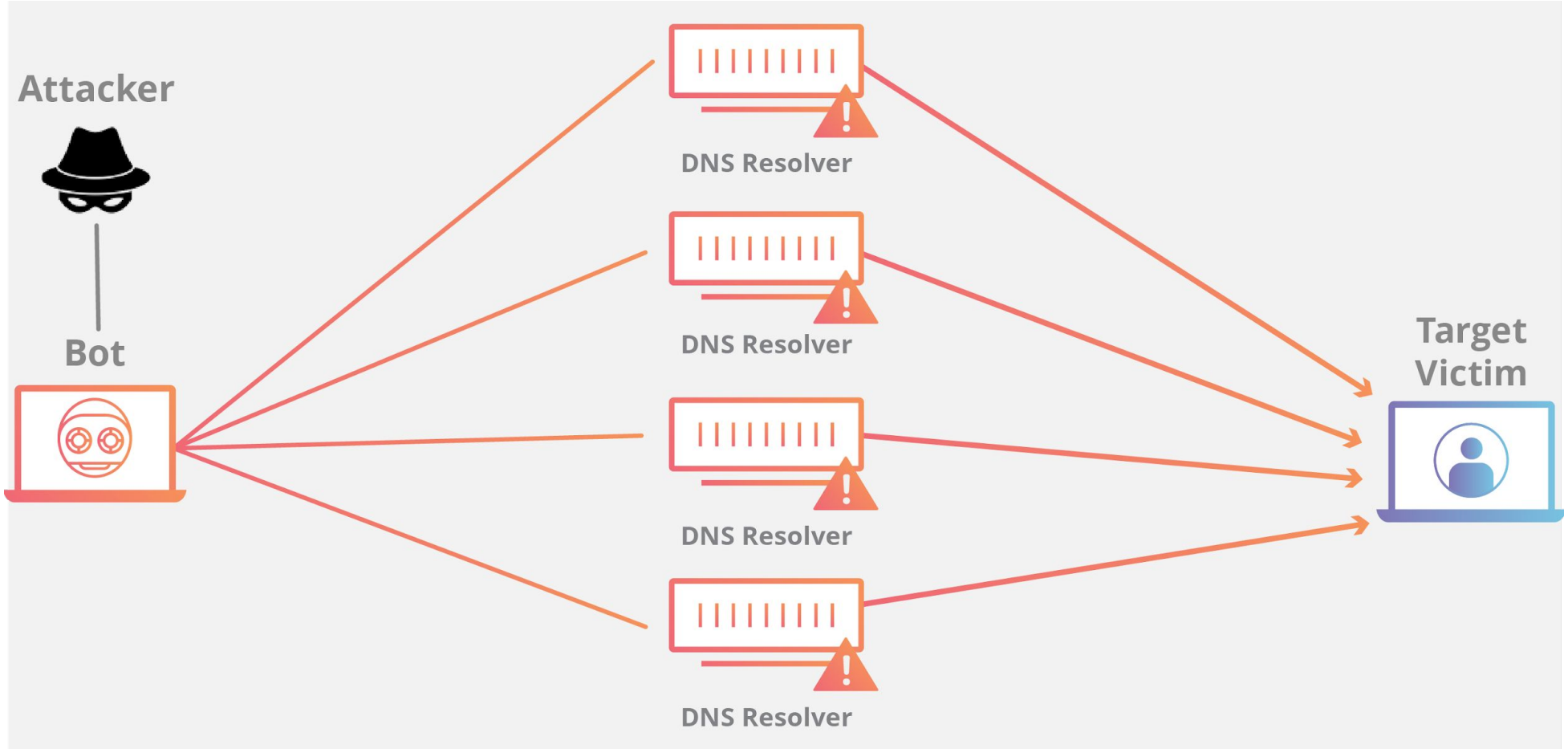
- The attacker intercepts the message and sends it again to receive another payment from bank.

- **Repudiation :**This type of attack is different from others because it is performed by one of the two parties in communication: the sender or the receiver.

- The sender of the message might later deny that he has sent the message; the receiver of the message might later deny that he has received the message .

- **Denial of Service :**It is an attempt to make a machine or network resource unavailable to its intended users.
- The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, orboth).
- The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system [1].

Ddos


Attacker
Bot
DNS Resolver
DNS Resolver
DNS Resolver
DNS Resolver
Target
Victim

PASSIVE VS ACTIVE ATTACK

- Passive Versus Active Attacks
- A. Passive Attacks In a passive attack, the attacker’s goal is just to obtain information. This means that the attack does not modify or harm the system. The system continues with its normal operation. Attacks that threaten confidentiality – snooping and traffic analysis – are passive attacks.
- B. Active Attacks An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in variety of ways.

Attacks	Passive/ Active	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of Service	Active	Availability

SECURITY POLICY and MECHANISM

- A security policy is **a statement of what is, and what is not, allowed**.
- A security mechanism is a method, tool, or procedure for enforcing a security policy.
- Security mechanisms are **technical tools and techniques that are used to implement security services**.
- A mechanism might operate by itself, or with others, to provide a particular service.
- Examples of common security mechanisms are as follows: Cryptography. Message digests and digital signatures.

Security Mechanism

- Encryption is a means **of securing digital data using one or more mathematical techniques**, along with a password or "key" used to decrypt the information.
- The encryption process translates information using an algorithm that makes the original information unreadable.
- Authentication is **the process of recognizing a user's identity**. It is the mechanism of associating an incoming request with a set of identifying credentials. The credential often takes the form of a password, which is a secret and known only to the individual and the system.

CRYPTOGRAPHY

- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.
-
- Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

- **A basic cryptosystem includes the following components:**
- Plaintext- This is the data that needs to be protected.
- Encryption algorithm- This is the mathematical algorithm that takes plaintext as the input and returns ciphertext. ...
- Ciphertext- This is the encrypted, or unreadable, version of the plaintext.

Cryptography

Techniques used For Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption.

The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

- **Confidentiality:**
  Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:**
  Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:**
  The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:**
  The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

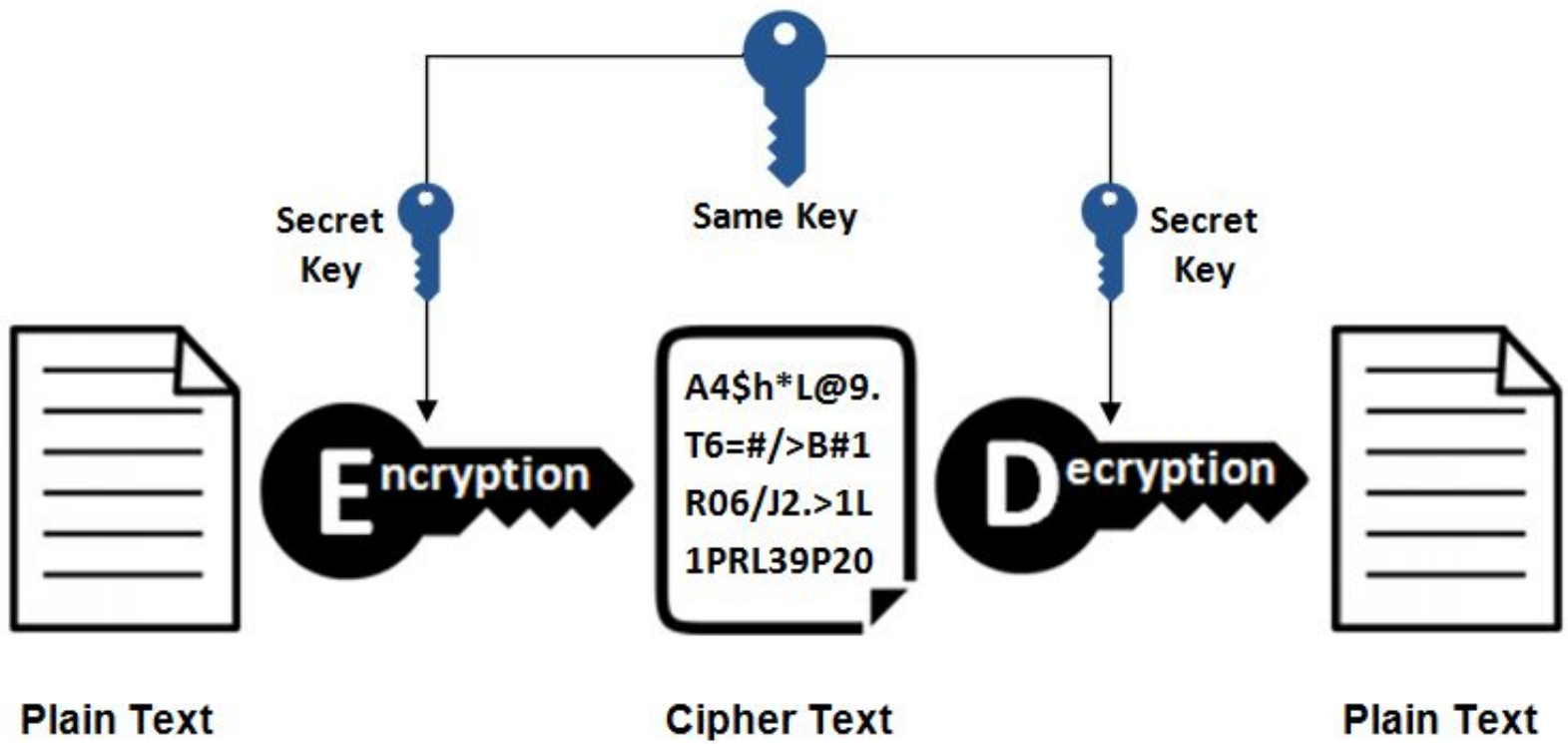
- **Symmetric Key Cryptography:**
  It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.
- **Asymmetric Key Cryptography:**
  Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption.

Symmetric Encryption

- This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.
- Symmetric encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters.
- It is a blended with the plain text of a message to change the content in a particular way.
- The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.
- Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

- The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Symmetric Encryption

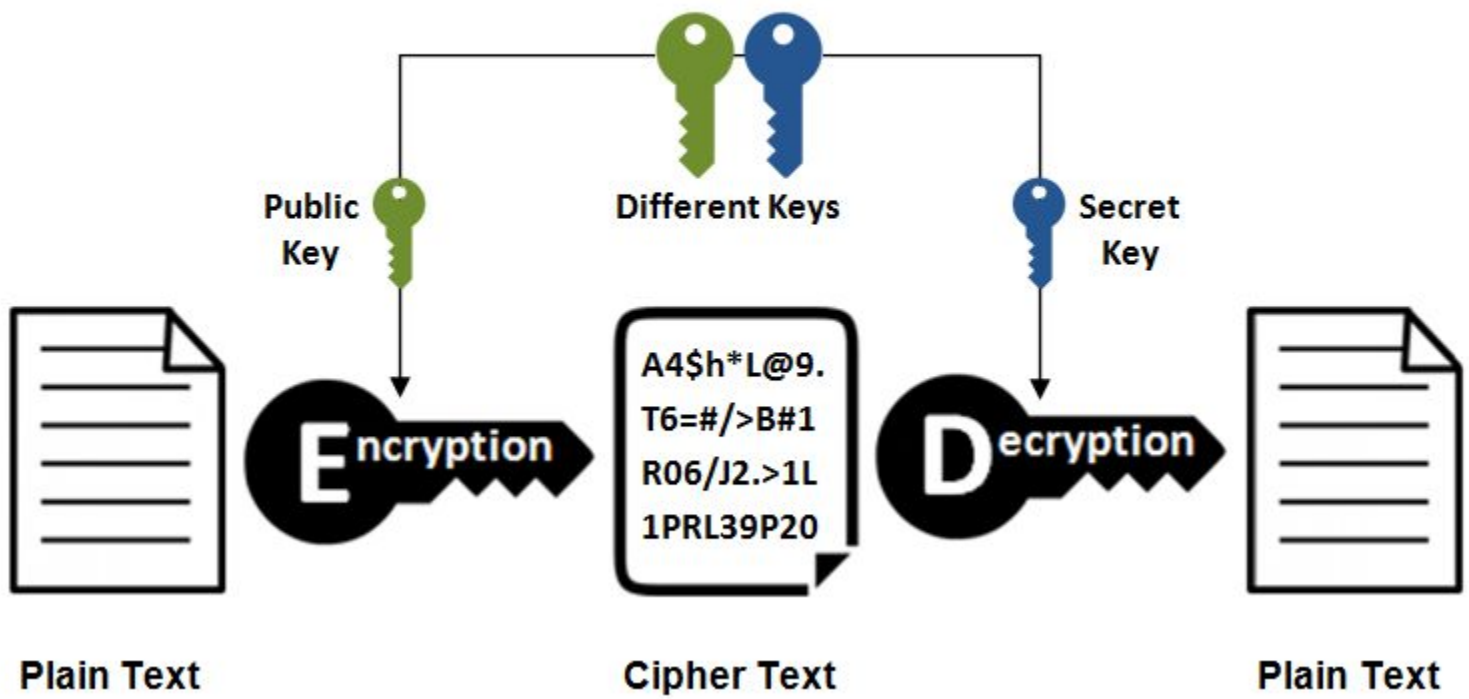


Asymmetric Encryption

- Asymmetric encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption.
- Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network.
- It ensures that malicious persons do not misuse the keys.
- It is important to note that anyone with a secret key can decrypt the message and this is why asymmetric encryption uses two related keys to boosting security.
- A public key is made freely available to anyone who might want to send you a message.
- The second private key is kept a secret so that you can only know.

- A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key.
- Security of the public key is not required because it is publicly available and can be passed over the internet.
- Asymmetric key has a far better power in ensuring the security of information transmitted during communication.
- Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet.
- Popular asymmetric key encryption algorithm includes RSA, DSA, Elliptic curve techniques, PKCS.

Asymmetric Encryption



RSA ALGORITHM

REFER SITE : ezexplanation.com (Computer Network)

HASH FUNCTION

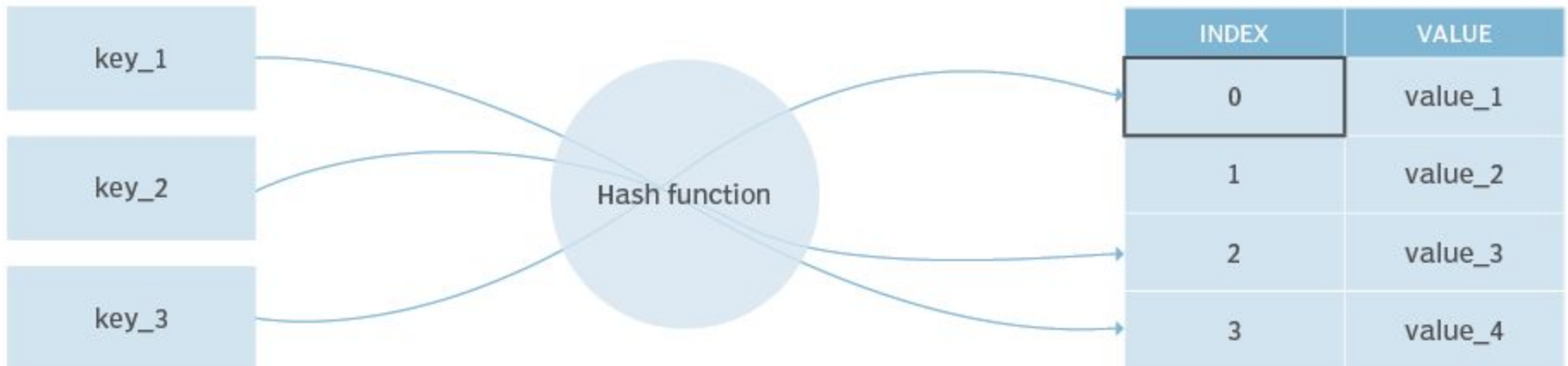
- **Hash Functions**
- Hash functions are the building blocks for modern cryptography.

- used to transform large random size data to small fixed size data.
- The data output of the hash algorithm is called hash value or digest.

- The basic uses of hash functions are:
- Generation and verification of digital signatures
- Checksum/Message integrity checks
- Derivation of sub-keys in key-establishment protocols & algorithms
- Generation of pseudorandom numbers

- Hashing is the algorithm that calculates a string value from a file, which is of a fixed size.
- It contains tons of data, transformed into a short fixed key or value.
- Usually, a summary of the information or data is in the original sent file.
- The received output is known as hash value or code.

Hash table example



Hashing


#SHA-2
f7ff9e8b7b
b2e09b709
35a5d785e
0cc5d9d0a
Plaintext
Hash Function
Hashed text

Algorithm used for hashing

-Message Digest

-Whirlpool

-RSA

-SHA(Secure hash algorithm)

Hashing is useful for validating the content's integrity by detecting all the alterations and then changes to a hash value as an output.

And, Encryption is useful for encoding data for the purpose of maintaining confidentiality and security of the data. It needs a private key for decrypting the encrypted data.

Let's study hashing in detail

assignment:

https://builtin.com/cybersecurity/what-is-hashing

STUDY AT HOME:
Example: The Globus Security Architecture

- Globus is a system supporting largescale distributed computations in which many hosts, files, and other resources are simultaneously used for doing a computation.
- Such environments are also referred to as computational grids (Foster and Kesselman, 2003).
- Resources in these grids are often located in different administrative domains that may be located in different parts of the world.

- Because users and resources are vast in number and widely spread across different administrative domains, security is essential.
- To devise and properly use security mechanisms, it is necessary to understand what exactly needs to be protected, and what the assumptions are with respect to security.
- Simplifying matters somewhat, the security policy for Globus entails the following eight statements, which we explain below (Foster et al., 1998):

- The environment consists of multiple administrative domains.
- - 2. Local operations (i.e., operations that are carried out only within a single domain) are subject to a local domain security policy only.
- 3. Global operations (i.e., operations involving several domains) require the initiator to be known in each domain where the operation is carried out.
- 4. Operations between entities in different domains require mutual authentication.
- 5. Global authentication replaces local authentication.

- 6. Controlling access to resources is subject to local security only.
- 7. A group of processes in the same domain can share credentials.

Design Issues in DISTRIBUTED SYSTEM

- A distributed system, or any computer system for that matter, must provide security services by which a wide range of security policies can be implemented.
- There are a number of important design issues that need to be taken into account when implementing general-purpose security services.
- three of these issues: **focus of control, layering of security mechanisms, and simplicity**

Focus of Control

- The first approach is to concentrate directly on the **protection of the data that is associated with the application.**
- By direct, we mean that irrespective of the various operations that can possibly be performed on a data item, **the primary concern is to ensure data integrity.**
- Typically, **this type of protection occurs in database systems in which various integrity constraints can be formulated that are aut**omatically checked each time a data item is modified.

- The **second approach** is to concentrate on protection by specifying exactly which operations may be invoked, and by whom, when certain data or resources are to be accessed.

- A **third approach** is to focus directly on users by taking measures by which -only specific people have access to the application, irrespective of the operations they want to carry out.

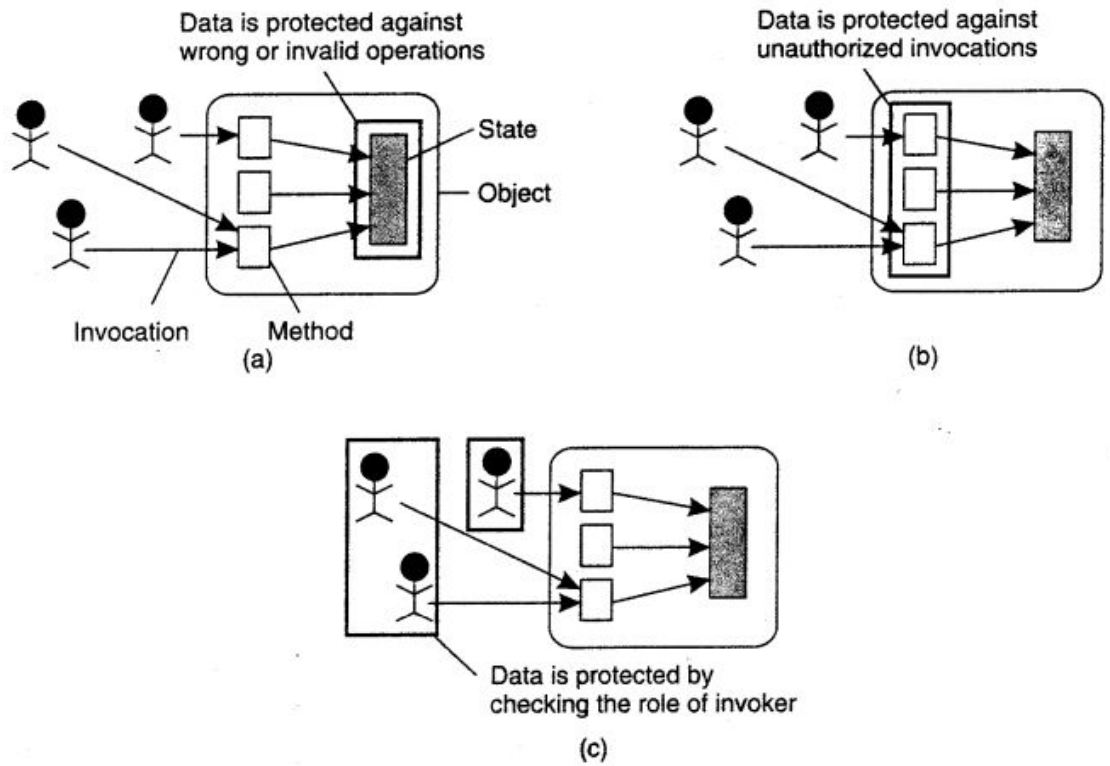


Figure 9-2. Three approaches for protection against security threats. (a) Protection against invalid operations (b) Protection against unauthorized invocations. (c) Protection against unauthorized users.

Layering of Security Mechanisms

- An important issue in designing secure systems is to decide at which level security mechanisms should be placed.
- In Chap. 1, we introduced the organization of distributed systems consisting of separate layers for applications, middleware, operating system services, and the operating system kernel.

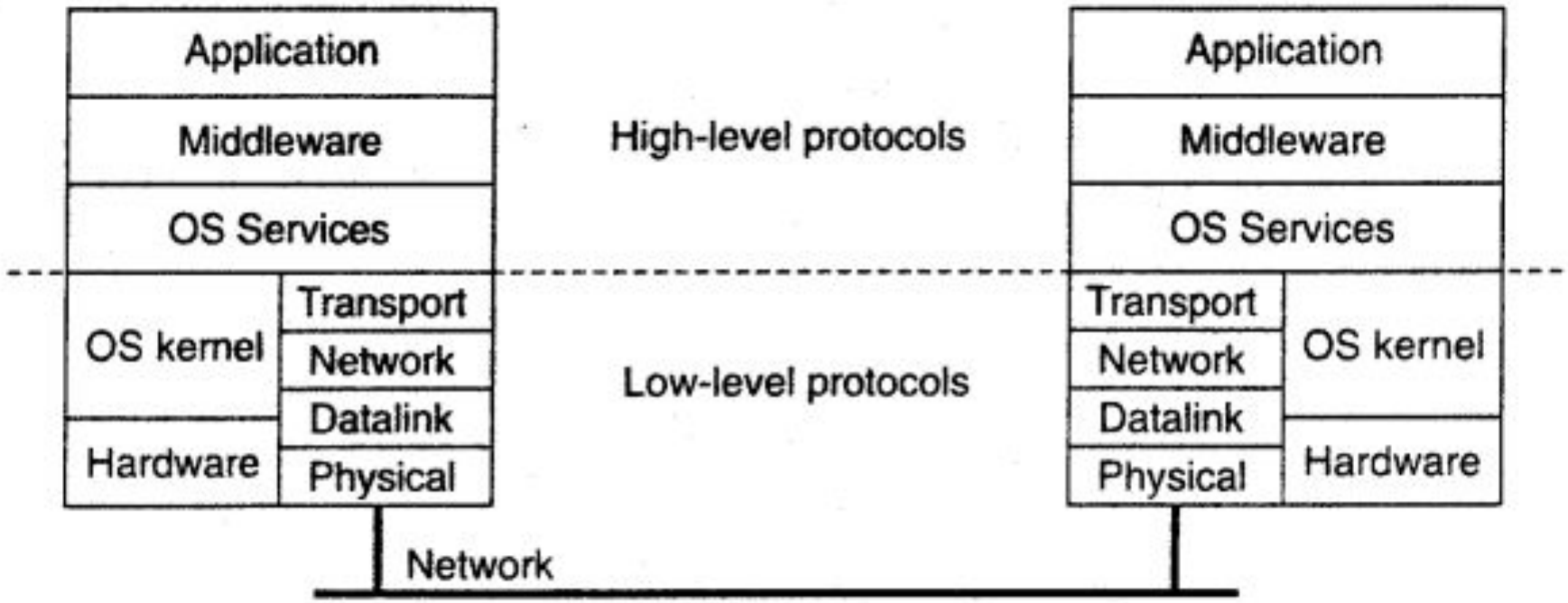


Figure 9-3. The logical organization of a distributed system into several layers.

- As an example, consider an organization located at different sites that are connected through a communication service such as Switched Multi-megabit Data Service (SMDS).
- An SMDS network can be thought of as a link-level backbone connecting various local-area networks at possibly geographically dispersed sites, as shown in Fig. 9-4

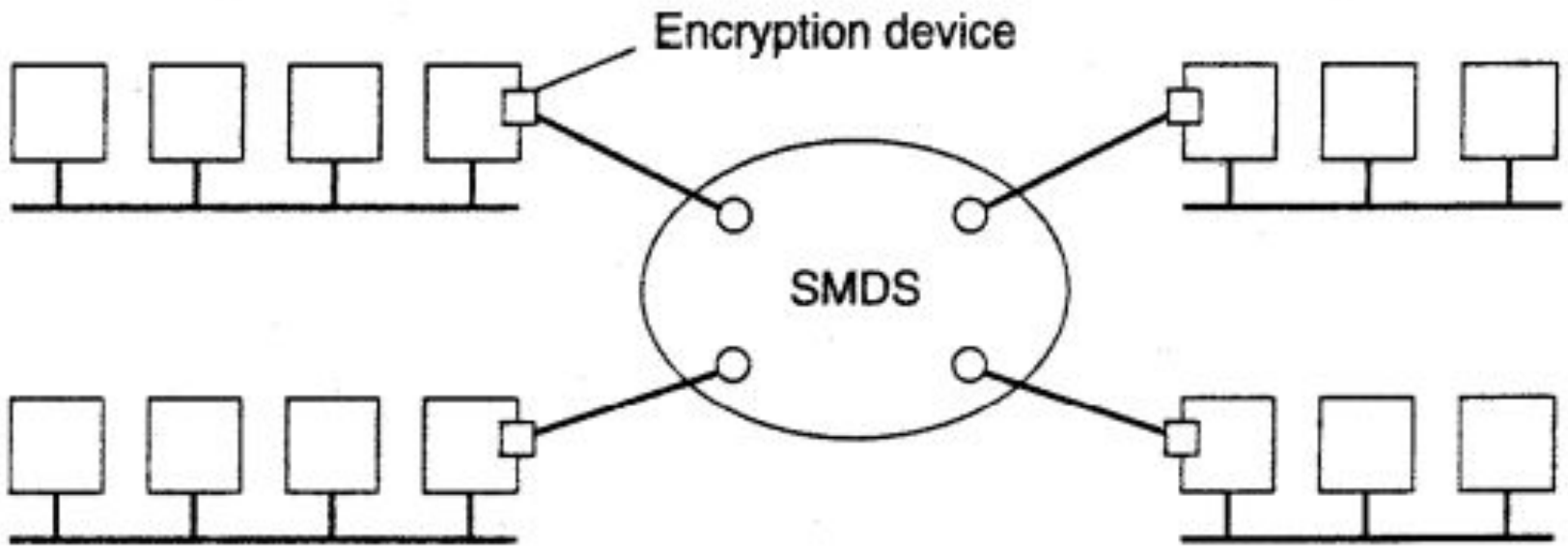


Figure 9-4. Several sites connected through a wide-area backbone service.

- Security can be provided by placing encryption devices at each SMDS router, as also shown in Fig. 9-4.
- These devices automatically encrypt and decrypt packets that are sent between sites.
- If Alice at site A sends a message to Bob at site B, and she is worried about her message being intercepted, she must at least trust the encryption of inter site traffic to work properly.
- This means, for example, that she must trust the system administrators at both sites to have taken the proper measures against tampering with the devices.

Simplicity

- Designing a secure computer system is generally considered a difficult task.
- Consequently, if a system designer can use a few, simple mechanisms that are easily understood and trusted to work, the better it is.

Secure Channel

- Secure communication requires authentication of the communicating parties, but also ensuring message integrity and possibly confidentiality as well.
- A secure channel protects senders and receivers against interception, modification, and fabrication of messages.

In a **distributed system**, a **secure channel** is a communication path between two or more nodes (e.g. computers, servers, devices) that ensures:

1. **Confidentiality** – no one can read the messages except the intended recipients.

2. **Integrity** – the message hasn't been tampered with during transit.

3. **Authentication** – both ends are sure of each other's identity.

4. **Optional: Non-repudiation** – a sender cannot deny having sent a message.

Techniques to Establish a Secure Channel

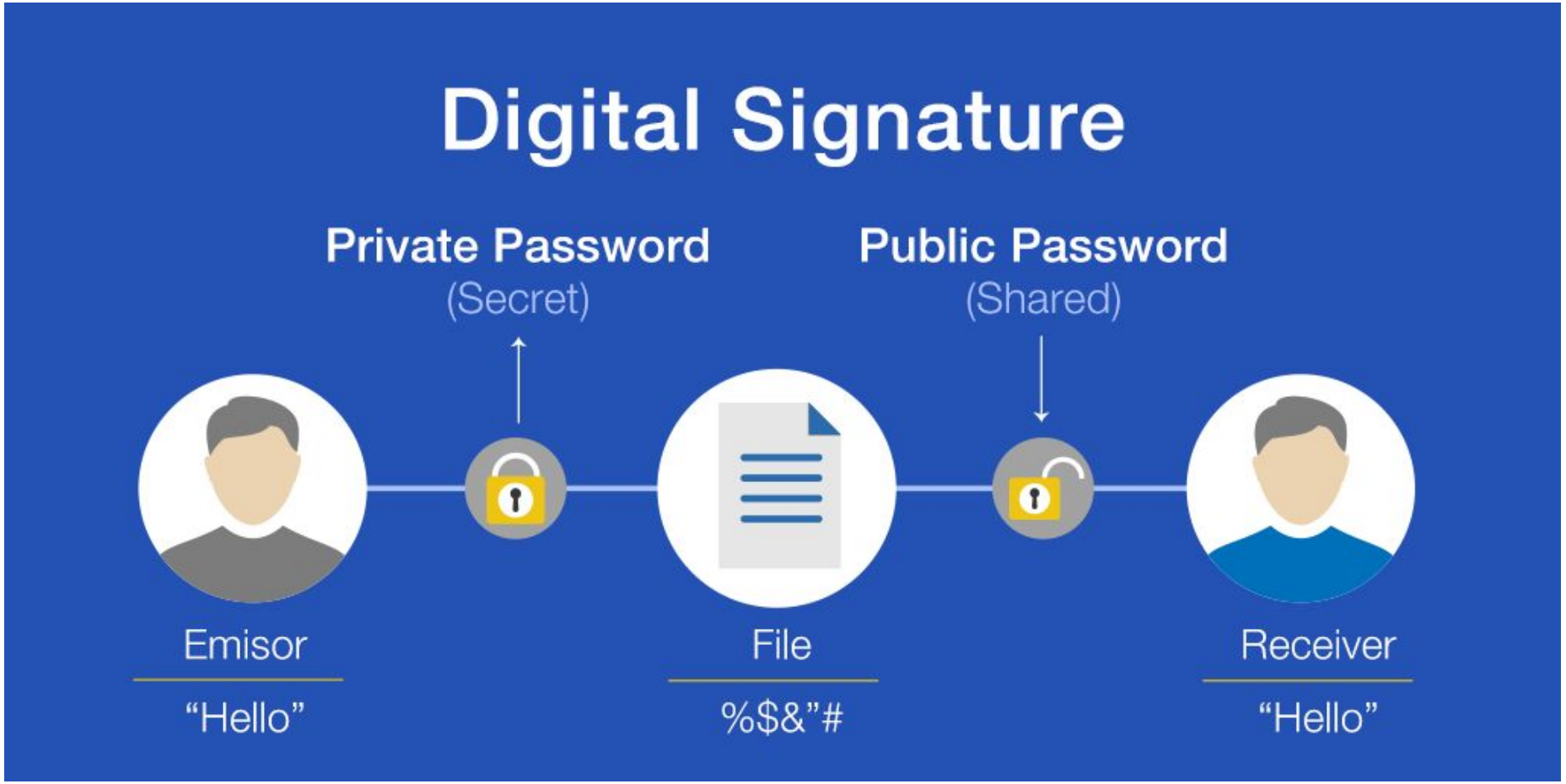
1. **TLS/SSL (Transport Layer Security)**
    - Used in HTTPS, gRPC, etc.
    - Ensures encrypted, authenticated communication.
    - Relies on public-key cryptography and digital certificates.

1. **VPNs (Virtual Private Networks)**
    - Create encrypted tunnels between systems.
    - Useful in enterprise environments for secure cross-data-center communication.
2. **End-to-End Encryption**
    - Each message is encrypted so that only the endpoints can read it.
    - Common in messaging apps (e.g., Signal, WhatsApp).

1. **Mutual Authentication**
    - Both client and server authenticate each other using certificates (e.g., mTLS).
    - Prevents impersonation or unauthorized access.
2. **Public Key Infrastructure (PKI)**
    - Used to manage keys and certificates.
    - Ensures trust between parties in a scalable way.

DIGITAL SIGNATURE-ASSIGNEMNT

- A digital signature—a type of electronic signature—is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document).
- Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents.
- In emails, the email content itself becomes part of the digital signature. Digital signatures are significantly more secure than other forms of electronic signatures.


Digital Signature
Private Password
(Secret)
Public Password
(Shared)
Emisor
"Hello"
File
%$&"#
Receiver
"Hello"

Kerberos-STUDY AT HOME

- Kerberos is a computer network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network, like the internet.
- It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities.
- Initially developed by the Massachusetts Institute of Technology (MIT) for Project Athena in the late '80s, Kerberos is now the default authorization technology used by Microsoft Windows.
- Kerberos implementations also exist for other operating systems such as Apple OS, FreeBSD, UNIX, and Linux.

- https://www.simplilearn.com/what-is-kerberos-article

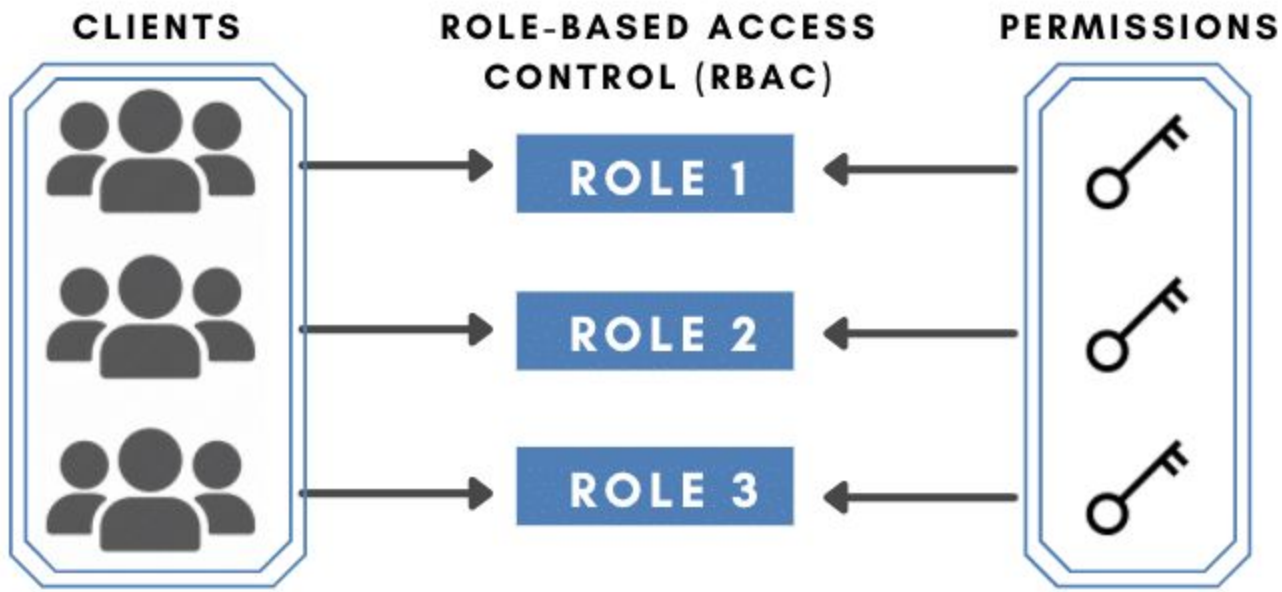
Access Control

- Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.
- Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data.
- Access control can also be applied to limit physical access to campuses, buildings, rooms, and datacenters.

- The four access control models are:

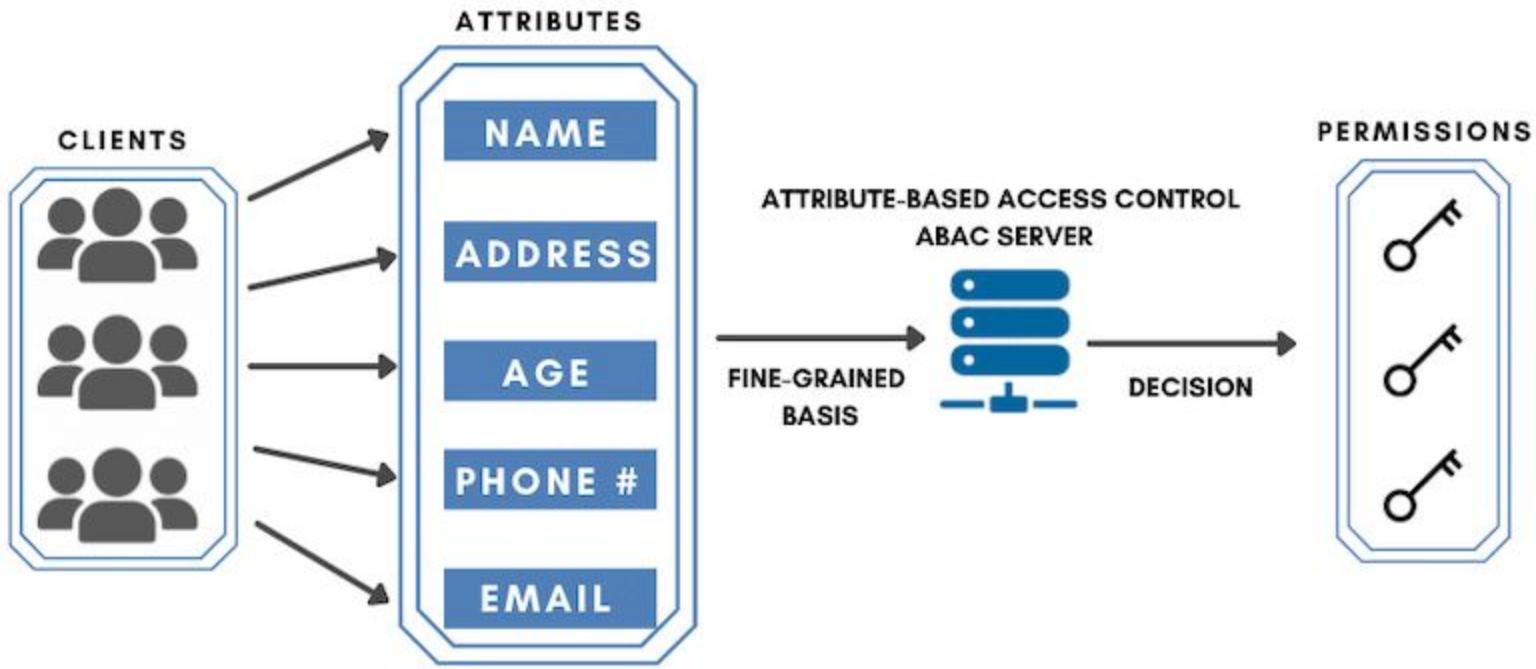
- **Discretionary access control (DAC):** In this method, the owner or administrator of the protected system, data, or resource sets the policies for who is allowed access.
- **Mandatory access control (MAC):** In this nondiscretionary model, people are granted access based on an information clearance.
- A central authority regulates access rights based on different security levels.
- This model is common in government and military environments.

- **Role-based access control (RBAC):** RBAC grants access based on defined business functions rather than the individual user's identity.
- The goal is to provide users with access only to data that's been deemed necessary for their roles within the organization.
- This widely used method is based on a complex combination of role assignments, authorizations, and permissions.

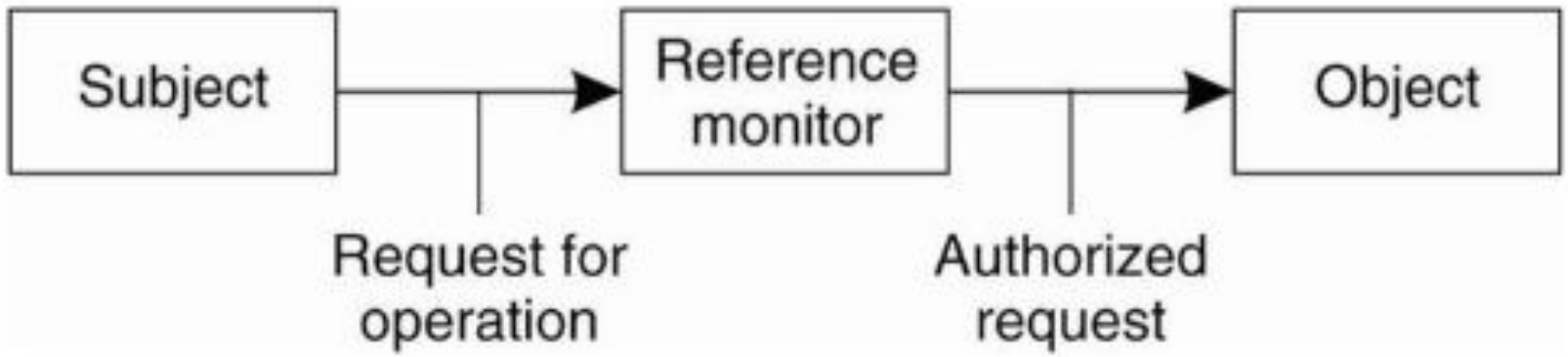

CLIENTS
ROLE-BASED ACCESS CONTROL (RBAC)
PERMISSIONS
ROLE 1
ROLE 2
ROLE 3

- **Attribute-based access control (ABAC):** In this dynamic method, access is based on a set of attributes and environmental conditions, such as time of day and location, assigned to both users and resources.

  - ***User Attributes may include the individual's name, role, or position.***
  - ***Resource Attributes can be the file type, its creation date, and its sensitivity level.***
  - ***Environmental Attributes may include access time or data location.***


ATTRIBUTES
CLIENTS
NAME
ADDRESS
AGE
PHONE #
EMAIL
ATTRIBUTE-BASED ACCESS CONTROL
ABAC SERVER
FINE-GRAINED
BASIS
DECISION
PERMISSIONS

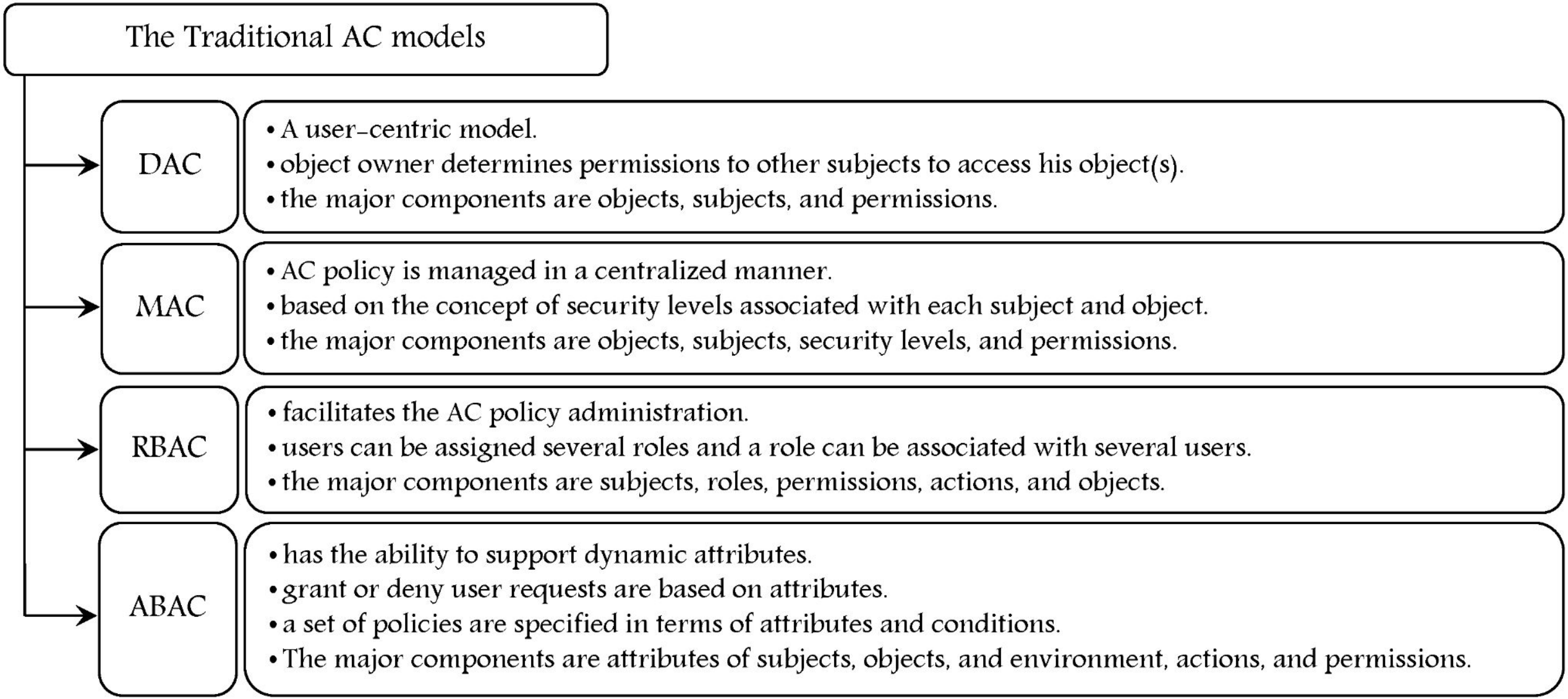
General Issues in Access Control:



Subject- Issues a request to access an object

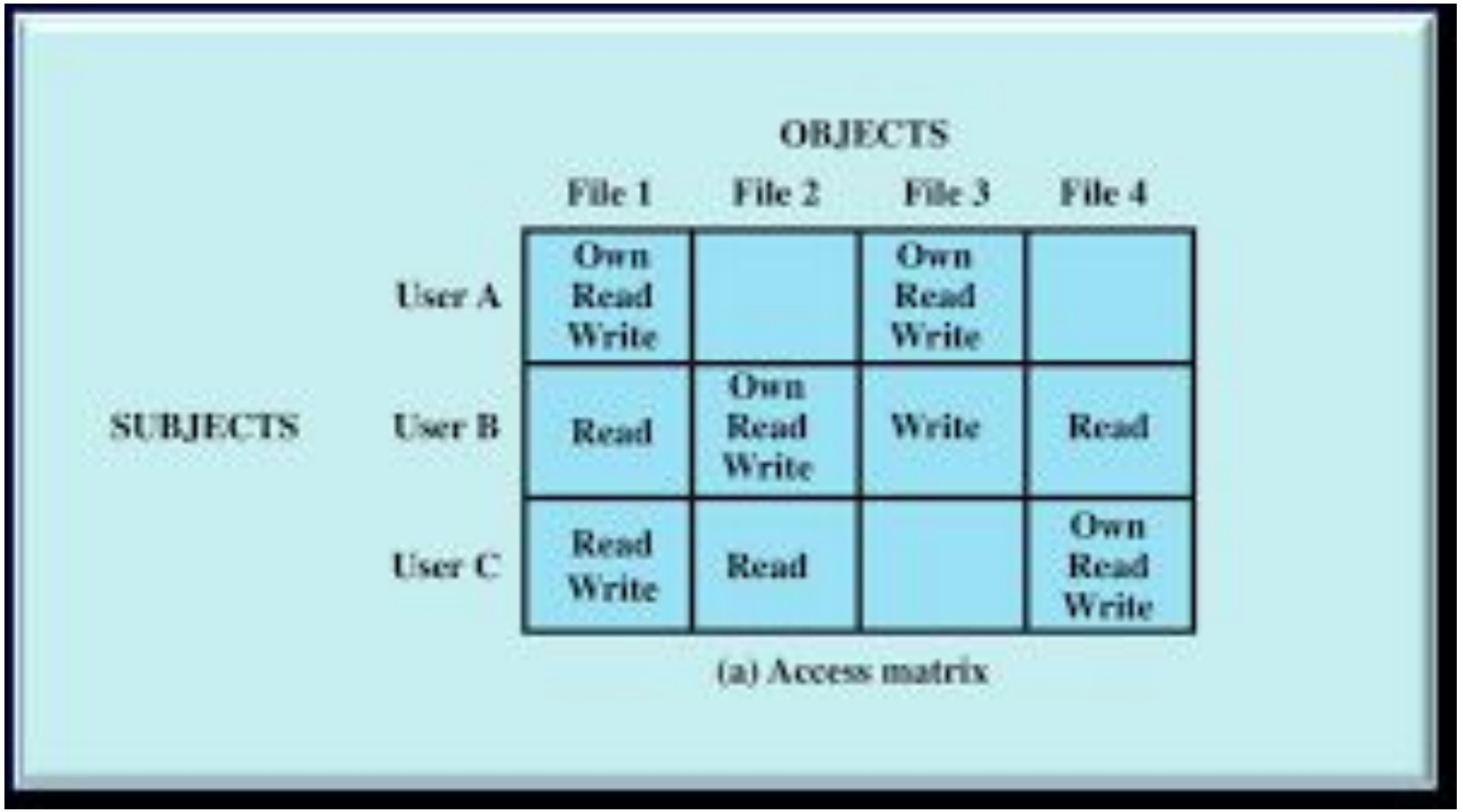
Reference monitor- Records which subject may do what, and decides whether a subject is allowed to have a specific operation carried out

Object- Encapsulates its own state and implementing the operations on that state


The Traditional AC models
DAC
• A user-centric model.
• object owner determines permissions to other subjects to access his object(s).
• the major components are objects, subjects, and permissions.
MAC
• AC policy is managed in a centralized manner.
• based on the concept of security levels associated with each subject and object.
• the major components are objects, subjects, security levels, and permissions.
RBAC
• facilitates the AC policy administration.
• users can be assigned several roles and a role can be associated with several users.
• the major components are subjects, roles, permissions, actions, and objects.
ABAC
• has the ability to support dynamic attributes.
• grant or deny user requests are based on attributes.
• a set of policies are specified in terms of attributes and conditions.
• The major components are attributes of subjects, objects, and environment, actions, and permissions.

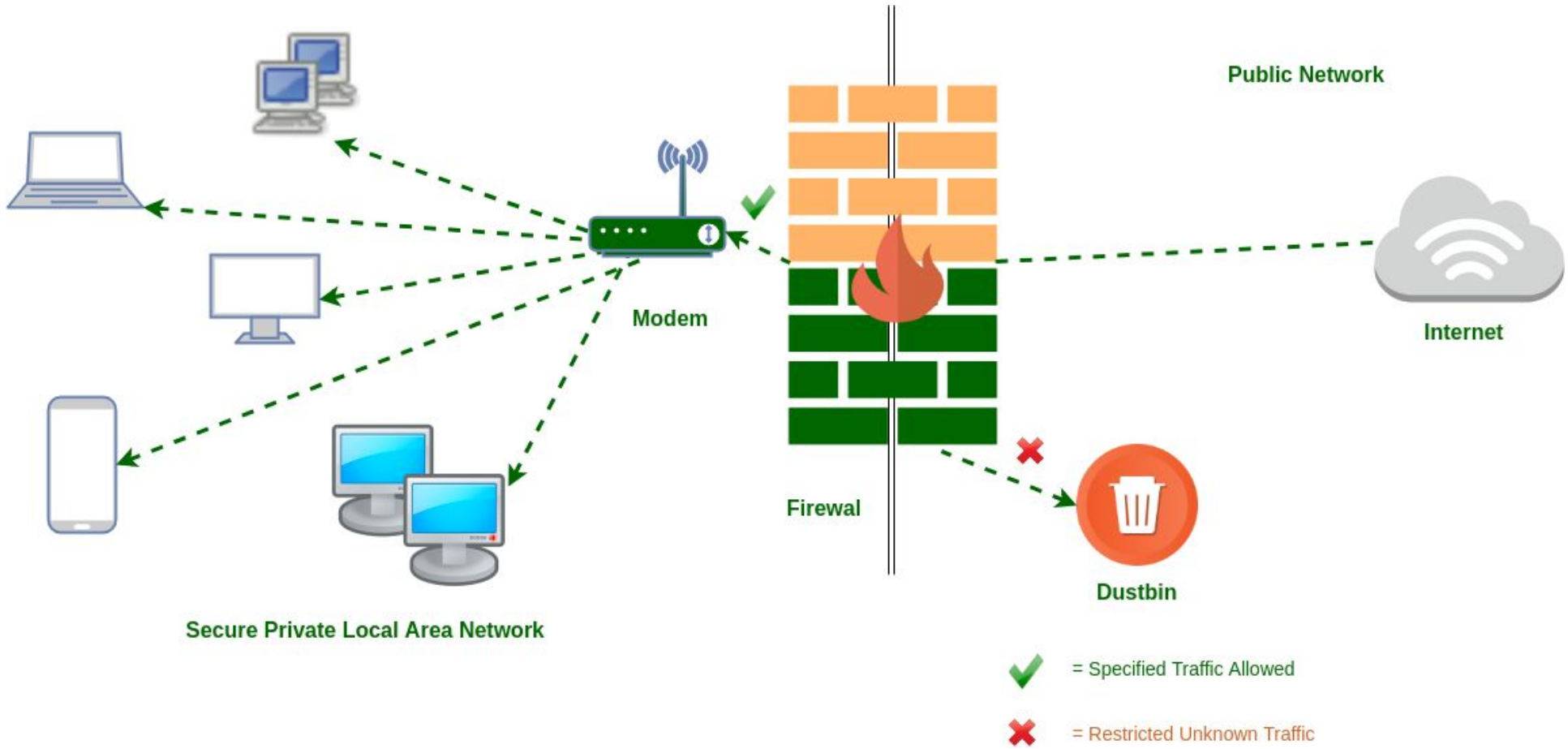
Access Matrix

- **Access Matrix** is a security model of protection state in computer system.
- It is represented as a matrix.
- Access matrix is used to define the rights of each process executing in the domain with respect to each object.
- The rows of matrix represent domains and columns represent objects. Each cell of matrix represents set of access rights which are given to the processes of domain means each entry(i, j) defines the set of operations that a process executing in domain Di can invoke on object Oj.


OBJECTS
File 1
File 2
File 3
File 4
SUBJECTS
User A
Own Read Write
Own Read Write
User B
Read
Own Read Write
Write
Read
User C
Read Write
Read
Own Read Write
(a) Access matrix

FIREWALL

- A Firewall is **a network security device that monitors and filters incoming and outgoing network traffic** based on an organization's previously established security policies.
- At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
= Specified Traffic Allowed
= Restricted Unknown Traffic

Advantages of Firewall

- 1. Monitor Traffic
- 2. Protection against Trojans
- 3. Prevent Hackers
- 4. Access Control
- 5. Better Privacy

Types of Firewalls

- **1. Packet filtering firewalls**
- Packet filtering firewalls are the oldest, most basic type of firewalls.
- Operating at the network layer, they simply check a data packet for its source IP and destination IP, the protocol, source port and destination port against predefined rules to determine whether to pass or discard the packet.
- Packet filtering firewalls are essentially stateless, monitoring each packet independently without any track of the established connection or the packets that have passed through that connection previously.
- This makes these firewalls very limited in their capacity to protect against advanced threats and attacks.

- **2. Circuit-level gateways**
- Working at the session layer, circuit-level gateways verify established Transmission Control Protocol (TCP) connections and keep track of the active sessions.
- They are quite similar to packet filtering firewalls
- However, they function at a higher layer of the Open Systems Interconnection (OSI) model.

- Primarily, they determine the security of an established connection.

- Circuit-level gateways are cost-efficient, simplistic and have barely any impact on a network’s performance.
- However, their inability to inspect the content of data packets makes them an incomplete security solution on their own.

- **3. Stateful inspection firewalls**
- A step ahead of circuit-level gateways, stateful inspection firewalls, in addition to verifying and keeping track of established connections, also perform packet inspection to provide better, more comprehensive security.
- They work by creating a state table with source IP, destination IP, source port and destination port once a connection is established.
- They create their own rules dynamically to allow expected incoming network traffic instead of relying on a hardcoded set of rules based on this information.
- They conveniently drop data packets that do not belong to a verified active connection.

- Stateful inspection firewalls check for legitimate connections as well as source and destination IPs to determine which data packets can pass through.

- **4. Application-level gateways (proxy firewalls)**
- Application-level gateways, also known as proxy firewalls, are implemented at the application layer via a proxy device.
- Instead of an outsider accessing your internal network directly, the connection is established through the proxy firewall.
- The external client sends a request to the proxy firewall.
- After verifying the authenticity of the request, the proxy firewall forwards it to one of the internal devices or servers on the client's behalf.
- Alternatively, an internal device may request access to a webpage, and the proxy device will forward the request while hiding the identity and location of the internal devices and network.

- Unlike packet filtering firewalls, proxy firewalls perform stateful and deep packet inspection to analyze the context and content of data packets against a set of user-defined rules.
- Based on the outcome, they either permit or discard a packet.

Security Management

- Security management is **the identification of an organization's assets** (including people, buildings, machines, systems and information assets), followed by the development, documentation, and implementation of policies and procedures for protecting assets.

- **Three common types of security management strategies include information, network, and cyber security management.**
- #1. Information Security Management.
- #2. Network Security Management.
- #3. Cybersecurity Management.

Information Security Management

Information Security Management involves the protection of information assets from unauthorized access, disclosure, alteration, or destruction.

This includes safeguarding the confidentiality, integrity, and availability of data.

- **Confidentiality:** Ensures that information is accessible only to those authorized to view it. Techniques to maintain confidentiality include encryption, access controls, and authentication mechanisms.
- **Integrity:** Protects information from being altered or destroyed by unauthorized individuals. Methods to ensure integrity include hashing, checksums, and digital signatures.
- **Availability:** Ensures that information is accessible to authorized users when needed. This involves measures such as redundancy, backups, and disaster recovery plans.

Network Security Management

Network Security Management focuses on protecting the integrity and functionality of network infrastructure and the data transmitted across it.

This involves safeguarding the network from unauthorized access, attacks, and disruptions.

- **Firewalls:** Hardware or software that filters incoming and outgoing network traffic based on predefined security rules.
- **Intrusion Detection and Prevention Systems (IDPS):** Tools that monitor network traffic for suspicious activity and take action to prevent or mitigate threats.
- **Virtual Private Networks (VPNs):** Secure connections over public networks to protect data transmission.

Cybersecurity Management

Cybersecurity Management encompasses strategies and practices designed to protect against cyber threats and attacks.

It focuses on safeguarding all aspects of digital operations, including hardware, software, and data.

- **Threat Management:** Identifying, assessing, and responding to various types of cyber threats such as malware, phishing, and ransomware.
- **Vulnerability Management:** Regularly scanning for and addressing vulnerabilities in systems and applications.
- **Incident Management:** Preparing for, detecting, and responding to cybersecurity incidents to minimize impact and recover quickly.
- **Security Governance:** Establishing policies, procedures, and oversight mechanisms to manage cybersecurity efforts across an organization.

Secure Mobile Code

- In distributed computing, code mobility is the ability **for running programs**, code or objects to be migrated (or moved) from one machine or application to another.
- This is the process of moving mobile code across the nodes of a network as opposed to distributed computation where the data is moved.

- An important development in modern distributed system is the ability to migrate code between host instead of just migrating passive data.
- However mobile code introduces number of serious security threats. Two major issues are:
- Securing against malicious agents
- Securing a mobile agent from a malicious environment

Secure naming

Secure Naming in the context of security in distributed systems is crucial for ensuring that entities (such as users, devices, or services) can be accurately and securely identified across a network.

Definition: Secure naming involves the processes and mechanisms used to ensure that names (identifiers) in a distributed system are both unique and securely associated with the correct entities.

Importance: Proper secure naming helps in authenticating and authorizing entities, protecting against attacks such as spoofing and impersonation.

Unique Identifiers: Each entity in a distributed system should have a unique identifier to prevent conflicts and ambiguities.

Naming Hierarchies: Hierarchical naming systems, like DNS (Domain Name System), help in organizing names in a structured way to facilitate easy resolution and management.

Techniques for Secure Naming

Public Key Infrastructure (PKI): Utilizes certificates to securely bind identities with their corresponding public keys. For example, SSL/TLS certificates in web security.

- **Certificates:** Digital certificates from trusted Certificate Authorities (CAs) establish the legitimacy of identifiers.
- **Certificate Revocation:** Mechanisms like CRLs (Certificate Revocation Lists) and OCSP (Online Certificate Status Protocol) ensure that compromised certificates are invalidated.

Secure Name Resolution: Ensures that the process of resolving a name to an address or identifier is secure.

- **DNSSEC (Domain Name System Security Extensions):** Adds security to DNS by enabling cryptographic signing of DNS data to prevent tampering and spoofing.
- **Trusted Name Resolution Services:** Use of trusted entities to resolve names securely.

Name-Based Access Control: Ensures that access to resources is controlled based on the identity of the entity.

- **Role-Based Access Control (RBAC):** Access permissions are assigned based on roles associated with names.
- **Attribute-Based Access Control (ABAC):** Access decisions are based on attributes associated with the entities and their names.

Secure Group Management

- The typical user-level group considered in a distributed group, with members located in different places.
- The group membership changes dynamically, and the group typically exists for a relatively short time.

- Users wishing to participate in shared activities are initially equipped with seed secrets (such as passwords or public-key certificates) which are registered with the group leader.

- In message 1, the member requests joining the group.
- The leader checks the validity of the request message, and if satisfied, then checks the secure group policy to see if such a user can be admitted.
- If yes, it returns message 2, which includes the group key for communication among group members. If no, the leader returns a message ``authentication failed.''

Secure Group Management

- This security systems make use of key distribution centers (KDCs) and certification authorities (CAs).
- To ensure complete trust in security services, there is a need to provide high protection against all kinds of security threats.
- To set up a secure channel for communication between two processes, at least one of them needs to contact the KDC for a shared secret key.

Questions

- Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity.

- There are a large number of cases. Most answers generalized to the following. Alice's login information to a system (e.g. online bank or email) is acquired by Bob. He can login as Alice and perform unauthorized actions (e.g. money transfer, change account info, etc.).

MCQ

1. CIA stands for ----------

2. Eavesdropping is an example of

Interception

Interruption

Modification

Fabrication

3. Which security attack is an example of threat to availability

Ddos

Snooping

Replaying

Traffic Analysis

4.Full form of DDOS ----------