

Covert vs Overt Channel



covert vs overt channel

Covert Channel vs Overt Channel

In computer security, **communication channels** are classified as **overt** (legitimate) or **covert** (hidden/unauthorized).

1. Overt Channel

An **overt channel** is a **normal, legitimate communication path** used for intended data transfer.

Characteristics:

- Designed for communication
- Authorized by system policy
- Visible and expected
- Used for regular data transmission

Examples:

- Sending email through an SMTP server
- HTTPS communication between client and server
- File transfer using FTP
- Chat messages over WhatsApp

 These are **legal and intended** communication paths.

2. Covert Channel

A **covert channel** is a **hidden communication path** that is not designed for information transfer** but is used to secretly transmit data.**

It violates the system's security policy.

Characteristics:

- Not intended for communication
- Hidden / unauthorized

- Bypasses security controls
- Often used for data leakage or spying

Examples:

- Encoding secret data in packet timing (timing channel)
- Hiding data inside image files (steganography)
- Using CPU usage patterns to transmit information
- Modifying unused TCP header bits to send secret data


Types of Covert Channels

Covert Storage Channel

Uses shared storage to communicate.

Example:

- One process writes data into a file permission bit
- Another process reads that bit

 Uses system variables, file attributes, memory, etc.

Covert Timing Channel

Uses timing differences to send information.

Example:

- Sending data by deliberately delaying responses
- Fast response = 0, Slow response = 1

 Uses system performance or timing behavior.

Comparison Table

Feature	Overt Channel	Covert Channel
Purpose	Intended communication	Hidden communication
Legality	Authorized	Unauthorized
Visibility	Visible	Hidden
Security Risk	Low	High
Example	HTTPS, Email	Timing manipulation

Simple Exam Definition (5–6 marks)

Overt channel is a legitimate communication path designed for normal data transfer according to system security policy.

Covert channel is an unauthorized communication path that is not intended for data transfer but is used secretly to bypass security restrictions.

If you want, I can also give you:

- 2-mark definition
- 8–10 mark descriptive answer
- Diagram explanation
- Real-world attack example explanation 🚀



Describes an information transmission medium over which a message is transmitted without distortion or loss of information. ?

The term described is:

Noiseless Channel (also called Ideal Channel)

Definition:

A **noiseless channel** is an information transmission medium over which a message is transmitted **without distortion, interference, or loss of information**.

♦ Explanation:

- The signal sent by the sender is received **exactly the same** at the receiver.
- There is **no noise**, no attenuation, no errors.
- Channel capacity is assumed to be perfect.
- It is a **theoretical model** used in information theory.

Example:

If a sender transmits:

101101

The receiver receives:

101101

- ✓ No errors
- ✓ No modification
- ✓ No delay distortion

📌 In Communication Theory:

In Claude Shannon's information theory, a noiseless channel is used as an **ideal reference model** to understand real-world noisy channels.

🎯 2-Mark Exam Answer:

A **noiseless channel** is an ideal communication medium in which the transmitted message reaches the receiver exactly as sent, without any distortion, loss, or noise interference.



Security concern involving whether resources are on hand when needed. ?

The correct term is:

✓ Availability

📖 Definition:

Availability is a security concern that ensures **resources, systems, and data are accessible and usable whenever authorized users need them.**

🔒 In the CIA Triad:

Availability is one of the three core principles of information security:

1. **Confidentiality** – Prevent unauthorized access
2. **Integrity** – Prevent unauthorized modification
3. **Availability** – Ensure resources are available when needed

📌 Example:

- A website should be accessible to users 24/7.
- A banking server must remain operational during transactions.
- A denial-of-service attack affects **availability**.

2-Mark Exam Answer:

Availability refers to ensuring that systems, networks, and data are accessible to authorized users whenever required, without interruption or delay.



The property that says that the levels of subjects and/or objects can vary, but only in ways that don't violate the system security properties

The correct term is:

Tranquility Principle

Definition:

The **Tranquility Principle** states that the security levels of subjects (users/processes) and objects (files/resources) may change, but **only if the changes do not violate the system's security policy**.

Explanation:

In multilevel security models (like military classification systems):

- Subjects and objects have security levels (e.g., Confidential, Secret, Top Secret).
- These levels may change.
- However, the change must **not break existing security rules**.

Related To:

The **Tranquility Principle** is associated with the Bell-LaPadula model (confidentiality-based model).

Types of Tranquility:

Strong Tranquility

Security levels never change during system operation.

Weak Tranquility

Security levels may change, but only if the change does not violate security policies.

2-Mark Exam Answer:

The **Tranquility Principle** states that the security levels of subjects and objects may change only if such changes do not violate the system's established security policies.



Security policy that says that an agent cannot access information for a client if he has previously served a client in the same "conflict" class

The correct term is:

✓ Chinese Wall Security Policy

Definition:

The **Chinese Wall Security Policy** states that a user (agent/consultant) cannot access information from one company if they have previously accessed information from another company in the same conflict-of-interest class.

Purpose:

It is designed to **prevent conflict of interest** in organizations like consulting firms, law firms, or financial institutions.

Related Model:

This policy is formally described in the Brewer-Nash model (commonly called the Chinese Wall model).

Example:

Suppose a consultant works with:

- Company A (Oil Industry)
- Company B (also Oil Industry competitor)

If the consultant accesses Company A's confidential data, they **cannot** later access Company B's confidential data, because both belong to the same conflict class (Oil Industry).

But they **can** access data from a Bank (different conflict class).

2-Mark Exam Answer:

The **Chinese Wall Security Policy** prevents a user from accessing data of a company if they have previously accessed confidential data from another company in the same conflict-of-interest class.



The aspect of security concerning who can alter or modify stored information.

The correct term is:

Integrity

Definition:

Integrity is the security property that ensures that **stored information can only be altered or modified by authorized users in an authorized manner.**

Explanation:

Integrity protects data from:

- Unauthorized modification
- Unauthorized deletion
- Unauthorized insertion of data

It ensures that information remains **accurate, complete, and trustworthy.**

Part of:

Integrity is one of the three pillars of the **CIA Triad**:

1. Confidentiality
2. Integrity
3. Availability

Example:

- Only a bank manager can update account balances.
- A student cannot modify their own grades in the database.

2-Mark Exam Answer:

Integrity is the security property that ensures only authorized users can modify or alter stored information, maintaining its accuracy and reliability.



An information transmission medium that utilizes system resources that were not designed to transmit information.

The correct term is:

✓ Covert Channel

📖 Definition:

A **covert channel** is an information transmission medium that uses **system resources not intended for communication** to transfer information secretly.

🔒 Explanation:

Unlike normal (overt) communication paths, a covert channel:

- Uses unintended system features
- Bypasses security mechanisms
- Violates system security policy
- Is usually hidden or unauthorized

🧠 Examples:

- Using CPU load changes to encode bits
- Communicating by modifying file permission bits
- Sending information through packet timing delays

🔍 Types:

1 Covert Storage Channel

Uses shared storage (files, memory, attributes).

2 Covert Timing Channel

Uses system timing behavior to transmit information.

🎯 2-Mark Exam Answer:

A **covert channel** is an information transmission medium that uses system resources not intended for communication to secretly transfer information, thereby violating security policies.



The common name for the partial order among security levels in a hierarchical access control system such as Bell and LaPadula

The correct term is:

✓ Security Lattice (or simply Lattice)

Definition:

A **security lattice** is the common name for the **partial ordering of security levels** in a hierarchical access control system.

It defines how security classifications (e.g., Confidential, Secret, Top Secret) are ordered and how information can flow between them.

Used In:

The lattice structure is fundamental to the Bell-LaPadula model, which enforces:

- **No Read Up** (Simple Security Property)
- **No Write Down** (*-Property)

Explanation:

In a lattice:

- Every pair of security levels has a **least upper bound** and **greatest lower bound**.
- Levels are partially ordered, meaning not all levels must be directly comparable.
- It supports hierarchical and multilevel security systems.

Example hierarchy:

Top Secret



Secret



Confidential



Unclassified

2-Mark Exam Answer:

A **security lattice** is the partial order structure that defines the hierarchical relationship among security levels in models like Bell-LaPadula.