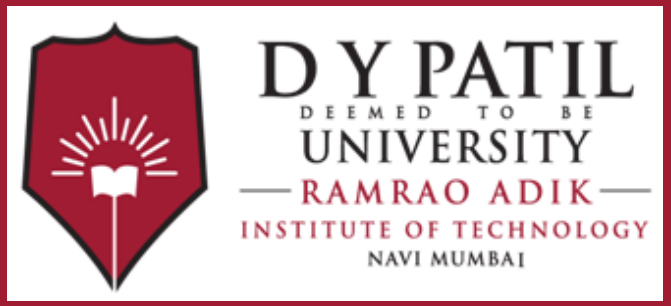


Subject Name: Information System

Unit No:01 Unit Name: Overview of Security Parameters

Faculty: Mrs. Bhavana Alte
Mr. Prathmesh Gunjgur

Security violation and threats; Security policy and procedure.

Security Violations

- Definition: Breaches of confidentiality, integrity, or availability.

- Types:
- Data breaches (confidentiality).
- Tampered records (integrity).
- Denial-of-service attacks (availability).

Definitions

- Threat: A potential violation of security.
- Attack: Actions that cause a threat to materialize.
- Attacker: The entity executing or causing an attack.

Threats

- A **threat** is a potential risk to a system's security that could harm its confidentiality, integrity, or availability.
- Even if the harm doesn't occur, the possibility of it happening means precautions must be taken.
- Threats can be categorized into four types: **disclosure**, **deception**, **disruption**, and **usurpation**.

Four Broad Classes of Threats

- Disclosure: Unauthorized access to information.
- Deception: Acceptance of false data.
- Disruption: Interruption or prevention of correct operation.
- Usurpation: Unauthorized control of a system or its components.

Types of Threats

1. Disclosure: Unauthorized access to information.

- **Example**: **Snooping** (passive wiretapping) occurs when an attacker listens to private conversations or reads sensitive files.
- **Prevention**: Encryption ensures confidentiality.

2. Deception: Accepting false or incorrect data.

- **Example**: **Spoofing** happens when an attacker pretends to be a legitimate entity, like a fake bank website tricking users into sharing credentials.
- **Prevention**: Authentication mechanisms verify identity.

3. **Disruption**: Interruption of correct operations.
   - **Example**: A **man-in-the-middle (MITM) attack** intercepts and modifies data between two communicating parties without their knowledge.
   - **Prevention**: Integrity checks (e.g., digital signatures).
4. **Usurpation**: Unauthorized control of system resources or services.
   - **Example**: **Denial of Service (DoS)** attacks flood a website with traffic, making it unavailable to legitimate users.
   - **Prevention**: Firewalls and rate-limiting mechanisms ensure availability.

Policy and Mechanism

- The concepts of **security policy** and **security mechanism** are fundamental to understanding how security is managed in any system. Let's break them down.
- **Definitions**
- **Security Policy**:
  - A **policy** is a statement that defines **what is allowed** and **what is not allowed** in a system.
  - Example: "No student is allowed to copy another student's homework files."
- **Security Mechanism**:
  - A **mechanism** is a method, tool, or procedure used to enforce the policy.
  - Example: File permissions on a computer system that allow users to restrict access to their files.

Policy and Mechanism

- The concepts of **security policy** and **security mechanism** are fundamental to understanding how security is managed in any system. Let's break them down.
- **Definitions**
- **Security Policy**:
  - A **policy** is a statement that defines **what is allowed** and **what is not allowed** in a system.
  - Example: "No student is allowed to copy another student's homework files."
- **Security Mechanism**:
  - A **mechanism** is a method, tool, or procedure used to enforce the policy.
  - Example: File permissions on a computer system that allow users to restrict access to their files.

Introduction

- When a system faces a security attack, mechanisms are used to manage it. These mechanisms focus on **prevention**, **detection**, or **recovery**, often working together.

1. Prevention

- **Goal**: Stop the attack from happening in the first place.
- **How It Works**: Preventative mechanisms are designed so that attackers cannot bypass them. These mechanisms should be trustworthy and unchangeable.
- **Examples**:
  - A computer that is not connected to the Internet cannot be attacked online.
  - Passwords prevent unauthorized access to systems.
- **Challenges**: Preventative measures can make systems less user-friendly or interfere with normal activities.

2. Detection

- **Goal**: Identify when an attack is happening or has already occurred.
- **How It Works**: Detection mechanisms monitor the system for unusual behavior or signs of an attack.
- **Examples**:
  - The system gives a warning when a user enters the wrong password three times.
  - Logs are created to record suspicious activities for further analysis.
- **Limitations**: Detection does not stop an attack but helps identify and analyze it for future prevention.

- **3. Recovery**
- Recovery focuses on addressing the damage caused by an attack and restoring normal operations. It has **two forms**:
- **(a) Repair After the Attack**
- **Goal**: Stop the attack, fix the damage, and prevent it from happening again.
- **Examples**:
  - If an attacker deletes a file, restore it from a backup.

- **(b) Maintain Operation During an Attack**
- **Goal**: Ensure the system keeps running correctly while the attack is happening.
- **Examples**:
  - Critical systems (like in airplanes or hospitals) may disable nonessential functions but continue running safely.
  - The system automatically detects incorrect behavior and fixes it in real-time.
- **Challenges**: This is hard to implement because systems are complex.

Comparison of Goals

Goal	Mechanism	Example
Prevention	Firewalls, strong passwords	Prevent unauthorized system access.
Detection	IDS, monitoring tools	Alert on multiple failed login attempts.
Recovery	Backups, fault tolerance	Restore deleted files or critical services.

Assumptions and Trust

- Security policies and mechanisms are based on assumptions about the environment and the threats they face.
- Trust plays a critical role in whether these assumptions hold true

•**Assumptions in Security Policies**:

•A policy defines what actions are secure or insecure.

•It assumes the policy itself is correct and mechanisms can enforce it.

•**Trust in Security Mechanisms**:

•Trust assumes mechanisms (like locks or digital controls) will work as intended and won't be bypassed unless authorized.

Security Mechanisms:

•**Secure Mechanism**:

Only allows safe actions and blocks all unsafe actions.

Example: A lock that prevents any unauthorized person from entering.

•**Precise Mechanism**:

Matches the security rules exactly—allows only what's safe and blocks all else.

Example: A keycard that grants access only to authorized areas.

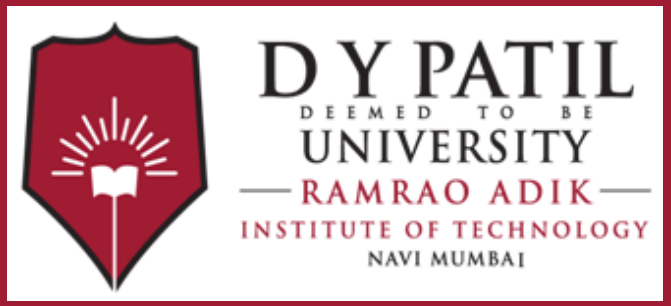
•**Broad Mechanism**:

May unintentionally allow unsafe actions.

Example: A password system that doesn't block weak passwords.

Trust Assumptions in Mechanisms:

- Mechanisms are designed to enforce the policy.
- Together, they cover all aspects of the policy.
- They are implemented correctly.
- They are installed and managed properly.
- If any assumption fails, the security system may be compromised. Security is an ongoing process of refining policies, mechanisms, and trust.


D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You