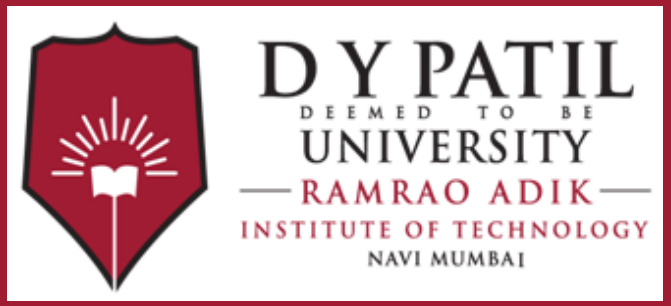


Subject Name: Information System

Unit No:01 Unit Name: Overview of Security Parameters

Faculty: Mrs. Bhavana Alte
Mr. Prathmesh Gunjgur

Confidentiality, Integrity and Availability

Confidentiality

- Confidentiality is a fundamental aspect of information security, ensuring that sensitive information is accessible only to authorized individuals or processes.
- It arises from the need to protect data in fields such as government, military, industry, and personal domains.

Key Aspects of Confidentiality

- **1. "Need to Know" Principle**

The principle restricts access to information only to those who need it to perform their duties.

Example:
In the military, details of a covert operation are shared only with relevant officers directly involved in the mission. Other personnel, even within the same organization, are not privy to this information unless necessary.

2. **Cryptography for Confidentiality**

Cryptography is a powerful access control mechanism used to protect sensitive information by scrambling (encrypting) it. Only individuals with the correct cryptographic key can decrypt and read the data.

- **Example**:
  Suppose an individual's income tax return is encrypted using AES (Advanced Encryption Standard).The encrypted file appears as random data to anyone without the key.
- To view the return, the owner enters their decryption key into a program.

Key Aspects of Confidentiality

- **3. Mechanisms to Prevent Unauthorized Access**
- Other mechanisms, such as role-based access control, restrict access to data. These controls protect against unauthorized access but depend on system integrity.
- **Example**:
  - A company may configure a database such that only the HR department can access employee records.
  - However, if someone bypasses the controls (e.g., exploiting a vulnerability), the data is exposed.
- **4. Protecting the Existence of Data**
- Sometimes, the mere existence of certain data is confidential. For example:
- Knowing that a survey was conducted can reveal sensitive information, even if the survey results are not disclosed.
- **Example**:
  A government poll on citizens' opinions about a controversial policy is classified. While the results are sensitive, the fact that the poll exists might suggest the government is concerned about public dissent.

Key Aspects of Confidentiality

- **5. Resource Hiding**
- Concealing the existence or configuration of resources protects organizations from attacks or misuse.
- **Example**:
  - A company uses specific high-performance servers for critical applications. If attackers know about these servers, they might target them directly.
  - Access control mechanisms hide server configurations and usage details, protecting the infrastructure.

Assumptions and Trust in Confidentiality Mechanisms

- Confidentiality mechanisms rely on the underlying system (e.g., operating system kernel) and supporting services to function correctly. If these services are compromised, confidentiality mechanisms can fail.
- **Example**:
  - An encrypted file is secure, but if the decryption program contains a vulnerability (e.g., exposing the key during the decryption process), the confidentiality of the file is at risk.
  - Trust is placed in the system kernel to ensure proper access enforcement and prevent bypassing security measures.

Integrity in Information Security

- **Integrity** ensures the trustworthiness, accuracy, and correctness of data and resources by preventing unauthorized or improper modifications. It has two key components:
- **Data Integrity**: Ensures the content of information is accurate and remains unchanged without proper authorization.
- **Origin Integrity (Authentication)**: Ensures that the source of the information is genuine and credible.

- **KEY POINTS**
- **1. Data Integrity and Origin Integrity**:
- Data integrity focuses on the correctness of the data itself. For example, ensuring that an accounting record hasn't been tampered with.
- Origin integrity focuses on ensuring that the source of the information is genuine and trustworthy.

Integrity in Information Security

2. Prevention vs. Detection Mechanisms:

- **Prevention Mechanisms**: Block unauthorized changes to data.
  - Example: Access controls and authentication mechanisms prevent an unauthorized user from modifying an accounting database.
- **Detection Mechanisms**: Identify violations after they occur by analyzing system events or the data itself.
  - Example: A system may detect that a file's checksum no longer matches, indicating that the file has been altered.

3. Two Types of Unauthorized Changes:

- **Unauthorized Access**: When someone without permission tries to modify data.
  - Example: A hacker tries to alter accounting records.
- **Authorized but Improper Use**: When someone with legitimate access misuses their authority to make unauthorized changes.
  - Example: An accountant embezzles money by altering financial records to hide transactions.

Integrity in Information Security

- **Difference Between Confidentiality and Integrity**:
- **Confidentiality** ensures that unauthorized users cannot access data.
- **Integrity** ensures that the data is correct, credible, and trustworthy.
- Integrity also considers the history of data: its source, how it was handled before reaching the current system, and how well it is protected now.

- **Challenges in Evaluating Integrity**:
- Integrity is difficult to evaluate because it depends on assumptions about:
  - The trustworthiness of the data source.
  - The protection measures applied before and during the data's storage.
- For example, even if data appears unaltered, it may have originated from an untrusted source, affecting its credibility.

Availability

- **Availability** in security refers to ensuring that information and system resources are accessible to authorized users whenever needed.
- It plays a critical role in system reliability and usability.
- A failure in availability can make a system effectively useless, as users cannot access the required data or services.
- When availability is compromised deliberately, it often results in **Denial of Service (DoS)** attacks.
- These attacks aim to make a system, network, or resource unavailable by overwhelming it with excessive requests or by exploiting its vulnerabilities.

Key Points

1. Statistical Models and Availability:

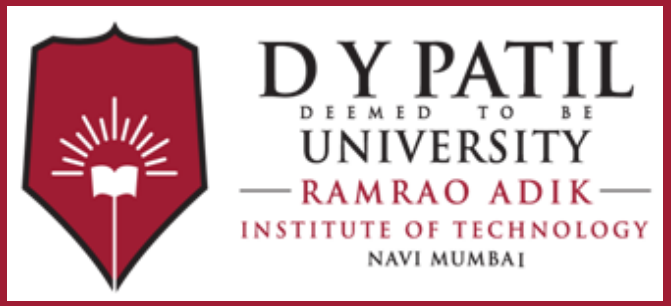
- Systems are designed with statistical models that predict usage patterns (e.g., expected traffic volume on a server).
- Mechanisms are implemented to ensure availability under normal conditions as per these models.
- However, attackers may manipulate resource usage or parameters (e.g., network traffic) to exceed the limits of these statistical models. When this happens, availability mechanisms often fail because the environment becomes one for which they were not designed.

2. **Denial of Service Attacks (DoS)**:

- In DoS attacks, the goal is to intentionally disrupt the availability of services.
- Attackers may flood a system with excessive traffic or exploit vulnerabilities to make resources or data inaccessible to legitimate users.

3. Difficulty in Detection:

- It is challenging to determine whether a service unavailability is due to a deliberate attack or natural atypical usage patterns.
- Even in statistical models, outlier events may be normal, making it hard to differentiate between malicious intent and legitimate spikes in usage.


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

Thank You