week 6 Revision notes

IFB240 Week 6 - Access Control

Overview

Access control is a fundamental aspect of information security, helping ensure that only **authorized users** access **critical resources**. This involves defining, enforcing, and monitoring who can access what and how they can interact with those resources. We explore various control types, major access control approaches, and how these policies can be effectively implemented in an organizational context.

1. Introduction to Access Control

What is Access Control?

- **Access Control** involves restricting the use of information assets to:
  - **Authorized Users**: Allowing access to necessary information or resources.
  - **Prevent Misuse**: Ensuring authorized users do not misuse resources.
  - **Deny Unauthorized Users**: Preventing unauthorized access to resources.
- **Resources Examples**:
  - **Hardware**: Routers, laptops.
  - **Software**: Applications, system software.
  - **Information Assets**: Data files, documentation.
  - **Services**: Computing resources, communication, power.

Why is Access Control Important?

- **Prevents Breaches**: Unauthorized access or misuse can lead to breaches compromising **Confidentiality**, **Integrity**, or **Availability** (CIA).
- **Real-World Examples**:
  - **Hospital Database Breach (MongoDB)**: Patient data was exposed due to inadequate access controls.
  - **Victoria Police Misuse (2022)**: Officers misused the LEAP database to pursue and harass individuals, demonstrating misuse risks even by authorized users 75.

Types of Controls

- **Preventive Controls**: Aim to **stop security incidents** before they occur.

    - **Example**: Firewalls, encryption.
- **Detective Controls**: **Monitor and detect** attempts or signs of incidents.
    - **Example**: IDS (Intrusion Detection System).
- **Corrective Controls**: Aim to **repair** or mitigate damage after detection.
    - **Example**: Backups, restoring corrupted data.

2. Major Access Control Approaches

Discretionary Access Control (DAC)

- **Description**: Access rights are **granted at the discretion of the resource owner**. Typically implemented through **Access Control Lists (ACLs)**.
- **Examples**:
    - **Windows 10**: Sharing files through properties where the file creator can define access permissions (e.g., read, write).
    - **Unix/Linux**: Permissions for **owner, group, and others**, managed with commands like `chmod`.
- **Advantages**: Flexible; individual owners have direct control.
- **Disadvantages**: Vulnerable to privilege escalation since users can grant permissions to others 76.

Mandatory Access Control (MAC)

- **Description**: **Central authority** assigns attributes to both subjects and objects, applying **system-wide rules** to control access.
- **Examples**:
    - **BLP Model Security Level Hierarchy**:
        - **Top Secret > Secret > Confidential > Classified > Unclassified**.
        - A subject with "Secret" clearance can only access objects at "Secret" or lower levels.
- **Advantages**: Highly secure; prevents users from granting permissions beyond their level.
- **Disadvantages**: Rigid; difficult to implement in dynamic environments where access needs change frequently 76.

Role-Based Access Control (RBAC)

- **Description**: **Access permissions are based on roles**, rather than individual identities.
    - **Roles** define what access a user has based on their **job function** (e.g., student, administrator).
- **Example**: In a university system like **Canvas**, roles could include "Lecturer," "Student," or "Admin," and each role has different access rights.
- **Advantages**: Simplifies permission management in large organizations.
- **Disadvantages**: Roles must be well defined, and users can only act in **one role at a time** 76.

Combining Access Control Approaches

- **Mixed Approaches**: For added security, organizations can **combine MAC and DAC**.
  - **Process**:
    - **MAC** rules are applied first.
    - If access is granted, **DAC** is applied next.
    - **Access is only granted** if both sets of rules permit it, ensuring no sensitive information is accessed improperly 76.

3. Implementing Access Control

Phases of Implementation

1. **Policy Definition Phase**:
   - **Privileges are allocated** and administered by defining access control policies.
   - **User Accounts**:
     - Create accounts and associate **privileges** with users or user groups.
     - For accountability, each user must be **uniquely identifiable**.
2. **Policy Enforcement Phase**:
   - **Authentication**: Verifies the claimed identity (e.g., user provides ID and password).
   - **Authorization**: Determines whether the authenticated user has the necessary permissions.
   - **Access Granting and Monitoring**: Enforces the policy to either permit or deny access based on the authorization check 77.

Example of Access Control Phases

- **Conceptual Diagram**:
  - **Policy Administration Point (PAP)**: Handles **policy definition**.
  - **Policy Enforcement Point (PEP)**: Handles **enforcement** when access is requested, using **authentication** and **authorization** to make a decision.

Challenges in Implementation

- **Handover of Privileges**:
  - Ensure that handover of access means (e.g., ID cards, passwords) is secure and to the correct recipient.
  - There must be processes to **withdraw privileges** when no longer needed, e.g., after employment termination.
- **Security of Records**:

- Maintain records of user privileges securely, ensuring that they cannot be tampered with and are legally admissible.
- Records should clearly state which **privileges** a user has for each **resource** 77.

Example: Withdrawal of Privileges

- In cases like **termination of employment**, privileges should be **automatically revoked**.
- Users must also **hand back** physical access methods, such as ID badges, to prevent unauthorized access after departure 77.

4. Monitoring and Reviewing Access Control

Importance of Monitoring

- **Monitor Access**: Essential for:
  - **Detecting unauthorized activities**.
  - **Identifying loopholes** or access control bypass incidents.
  - **Providing evidence** in case of a breach.
  - **Maintaining a model of normal system behavior** (used for detecting anomalies).
- **Examples of Loopholes**:
  - **Tapplock Smart Lock**: A vulnerability allowed hackers to bypass access control within **two seconds**.
  - **Shopify Access Token Exposure**: Revealed weaknesses in improper access control configuration 77.

Using Monitoring Tools

- **Intrusion Detection Systems (IDS)**: Can help identify abnormal access patterns that could indicate a security breach.
- Monitoring should be part of **continuous security improvement**, identifying flaws and ensuring access control measures remain effective.

5. Principles for Effective Access Control

Principle of Least Privilege

- **Definition**: Users should only have the **minimum level of access** required to perform their job.
  - **Example**: A lecturer should only have access to students' grades, not their personal details like home address or financial information.

Separation of Duties (SoD)

- **Definition**: Divide responsibilities and access permissions to prevent any single individual from having control over critical tasks.
  - **Example**: In financial transactions, one person should handle data entry, while another handles approval.
  - **Purpose**: Reduces the risk of **fraud** or **security bypass** 75.

Whitelist vs. Blacklist

- **Whitelist**: Only explicitly permitted users or processes are allowed access.
  - **Example**: Applications that users are allowed to install.
- **Blacklist**: All users or processes are allowed unless explicitly denied.
  - **Example**: Websites that are forbidden for access within an organization.

6. Summary

Key Takeaways

- **Access Control** is vital for protecting information assets, ensuring only authorized individuals can access or modify resources.
- **Three Major Approaches**:
  - **Discretionary Access Control (DAC)**: Owner-driven and flexible.
  - **Mandatory Access Control (MAC)**: Centralized rules for strict access control.
  - **Role-Based Access Control (RBAC)**: Access is based on job roles, simplifying management.
- **Implementation** involves two phases:
  - **Policy Definition**: Assigning and managing privileges.
  - **Policy Enforcement**: Authenticating and authorizing each access request.
- **Effective Monitoring** and **regular review** are necessary to identify vulnerabilities and ensure compliance.

These detailed notes cover the core concepts of **Access Control**, including practical approaches, implementation phases, and common principles, to help you understand and effectively apply these concepts in any cybersecurity context.