ACCESS CONTROL CONCEPTS

Chapter Summary: In this chapter, the focus is on access control in information security, detailing the elements of access (subjects, objects, rules), the necessity of access, and its management. Access is granted based on trustworthiness, necessity, and follows the Principle of Least Privilege, which advocates for granting users only the minimum access required for their job.

The concept of defense in depth is introduced as a comprehensive strategy involving people, technology, and operational capabilities to establish multiple layers of defense against security threats. It emphasizes the importance of various types of access control (physical, logical/technical, and administrative) that professionals in information security should be familiar with.

Privileged Access Management (PAM) is discussed in relation to risk management and the CIA Triad (Confidentiality, Integrity, Availability). PAM reduces risk by limiting administrative privileges to necessary situations, thus ensuring confidentiality, integrity, and availability of data. The distinction between Regular User Accounts and Privileged User Accounts is highlighted.

Other security measures such as segregation of duties, two-person integrity, and user provisioning (from hiring to termination) are explored. The chapter delves into physical access controls, including security personnel, barriers, alarms, and surveillance systems, as well as logical access controls, which involve software and hardware configurations to manage access.

Three specific types of logical access controls are discussed in detail:

1. Discretionary Access Control (DAC): Controlled by resource owners, DAC allows users discretion over granting access to objects within the system.
2. Mandatory Access Control (MAC): Enforced uniformly across all subjects and objects within the system's boundary, MAC policies are typically set by administrators.
3. Role-Based Access Control (RBAC): User permissions are based on predefined roles within the organization, simplifying access management and enhancing security.

Overall, the chapter emphasizes the importance of implementing robust access control mechanisms to protect sensitive information and assets, mitigating risks associated with unauthorized access and ensuring the integrity and availability of organizational data.

__Chapter Takeaways:__ ***__Module 1__*** focuses on understanding the fundamental concepts of access control, which are based on three key elements:

1. **Subjects (Who):** Subjects refer to entities such as users, processes, or devices that seek access to resources within the system. These entities can be individuals, groups, or even automated systems.

2. **Objects (What):** Objects represent the resources that subjects are trying to access. These resources can include files, databases, applications, networks, or any other digital asset within the system

3. **Rules (How and When):** Rules define the conditions under which access is granted or denied. These rules specify the methods by which subjects can access objects and the timing or circumstances under which such access is permissible. Rules also dictate the actions subjects can perform on objects once access is granted, such as read, write, execute, or delete.

Understanding these elements is crucial for implementing effective access control mechanisms within an organization's information security framework. By properly defining and managing subjects, objects, and rules, organizations can ensure that only authorized entities gain access to resources, thereby mitigating the risk of unauthorized access, data breaches, and other security threats.

Defense in Depth:

Imagine your home security system. You don't just rely on one lock on your front door, right? You have multiple layers of security to protect your home. You might have a fence, a gate, a sturdy door with a deadbolt lock, an alarm system, and maybe even security cameras. Each of these layers adds another barrier that a potential intruder would have to overcome. Similarly, in an organization, Defense in Depth means using a variety of security measures like firewalls, antivirus software, access controls, and employee training to protect against cyber threats.

Privileged Access Management (PAM):

Think of your house keys. You don't give your spare keys to just anyone, right? You only give them to people you trust, and even then, you only give them access when necessary. Similarly, in an organization, PAM involves limiting administrative privileges to trusted individuals and only granting access when it's needed. This reduces the risk of unauthorized access to sensitive information or systems.

User Provisioning:

Imagine you're starting a new job at a company. On your first day, you're given an employee ID card that grants you access to certain areas of the building and a login to access the company's computer systems. This is like creating a new user account for a new employee. If you get promoted to a new position with different responsibilities, your access might need to be adjusted accordingly. Similarly, when an employee goes on temporary leave or leaves the company, their access should be either disabled or revoked to prevent unauthorized entry into systems or buildings. This process of creating, modifying, disabling, or deleting user accounts based on employees' status changes is called user provisioning.

Module 2 focuses on understanding physical access controls, which are essential for securing physical assets and facilities. Here are some key takeaways from Chapter 3:

Examples of Physical Access Controls:

1. **Security Guards:** Trained personnel stationed at entry points to monitor and control access to the premises.
2. **Fences:** Physical barriers surrounding the perimeter of a facility to prevent unauthorized entry.
3. **Motion Detectors:** Sensors that detect movement and trigger an alarm or alert security personnel.
4. **Locked Doors/Gates:** Doors or gates equipped with locks to restrict entry and exit to authorized individuals.
5. **Sealed Windows:** Windows that are securely closed and sealed to prevent unauthorized access.
6. **Lights:** Illumination to enhance visibility and deter unauthorized access, especially during nighttime.
7. **Cable Protection:** Measures to secure cables and wires to prevent tampering or unauthorized access to network infrastructure.
8. **Laptop Locks:** Physical locks or security cables used to secure laptops and prevent theft.
9. **Badges:** Identification cards issued to authorized personnel for access control purposes.
10. **Swipe Cards:** Cards containing encoded information that is swiped through a reader to grant access.
11. **Guard Dogs:** Trained dogs used for security purposes to patrol and protect the premises.
12. **Cameras:** Surveillance cameras used to monitor and record activities for security purposes.
13. **Mantraps/Turnstiles:** Enclosed areas with controlled entry and exit points to ensure only one person can pass through at a time.

14. **Alarms:** Security alarms that are triggered in response to unauthorized access attempts or security breaches.

These physical access controls play a crucial role in protecting physical assets, facilities, and personnel from unauthorized access, theft, vandalism, and other security threats. By implementing a combination of these controls, organizations can create layers of defense to enhance overall security posture and mitigate risks associated with physical breaches.

Log Anomaly: Imagine you're the manager of a retail store, and you regularly review the sales logs to track the number of transactions each day. Normally, you expect to see a consistent pattern of sales throughout the week, with perhaps a slight increase on weekends. However, one day you notice a significant spike in sales during the middle of the week when there's usually less activity. This unexpected deviation from the norm is a log anomaly. It alerts you to the possibility of unusual behavior, such as a pricing error, a promotion driving unexpected sales, or even potential fraudulent activity. In the context of cybersecurity, log anomalies could indicate abnormal network traffic, suspicious login attempts, or unauthorized access to sensitive data.

Log Consolidation: Now, imagine you're a project manager overseeing multiple construction sites for a company. Each site has its own set of daily progress reports, equipment logs, and safety incident reports. Instead of managing each site's logs separately, you implement a system where all the logs from different sites are consolidated into a single, centralized database. This allows you to easily access and analyze data from all sites in one place, identify trends, and make informed decisions more efficiently. In the realm of IT, log consolidation involves aggregating logs from various sources such as servers, network devices, applications, and security systems into a centralized repository or SIEM (Security Information and Event Management) platform. This centralized approach simplifies log management, enhances visibility, and streamlines analysis for cybersecurity and compliance purposes.

Log Retention: Continuing with the construction site example, let's say there's an incident at one of the sites where a worker is injured. As per safety regulations, you're required to maintain records of all safety incidents for a certain period. You ensure that the incident report, along with any relevant documentation, is stored securely and retained for the mandated retention period, which might be several years. This ensures compliance with legal requirements and allows for future reference if needed, such as during audits or investigations. Similarly, in cybersecurity, log retention refers to the practice of storing logs and audit trails generated by IT systems and applications for a specified duration. This retention period is typically determined by regulatory requirements, organizational policies, and best practices. Retaining logs enables organizations to investigate security incidents, conduct forensic analysis, demonstrate compliance, and track historical trends over time.

Module 3 delves into understanding logical access controls, which are essential for managing access to digital resources within an organization. Here are key points regarding logical access controls:

Logical Access Control Types:

1. **Discretionary Access Control (DAC):** DAC is a type of access control where the resource owner determines who has access to the resource and what level of access they have. In DAC, access control decisions are based on the discretion of the resource owner, allowing them to grant or revoke access permissions as needed.
2. **Mandatory Access Control (MAC):** MAC is a more rigid access control model where access decisions are determined by security labels assigned to both subjects and objects. These security labels are typically set by system administrators or security policies and are enforced uniformly across the entire system, regardless of the resource owner's discretion.
3. **Role-Based Access Control (RBAC):** RBAC is a access control model where access permissions are based on the roles that individuals hold within an organization. Users are assigned to specific roles, and access rights are granted based on those roles. This simplifies access management by grouping users with similar job functions and responsibilities.

Examples of Logical Access Controls:

1. **Configuration Settings or Parameters Stored as Data:** In this scenario, access control settings are configured within software applications or systems. These settings dictate who can access specific features or functionalities within the software. For example, an email management system might have configuration settings that control who can send or delete emails.
2. **Managed through a Software Graphical User Interface (GUI):** Access control settings can be managed through a user-friendly graphical interface provided by software applications or operating systems. System administrators can use these GUIs to assign access permissions, manage user accounts, and configure security settings.
3. **Hardware Settings Done with Switches, Jumper Plugs, or Other Means:** Some access controls are implemented at the hardware level, using physical mechanisms such as switches or jumper plugs. These hardware settings determine how devices or components interact with each other and can restrict access to certain functionalities or resources. For example, a network

switch might have physical switches that control which ports are enabled or disabled for network traffic.

By implementing logical access controls, organizations can ensure that only authorized users have access to sensitive digital resources, helping to protect against unauthorized access, data breaches, and other security threats.

Important Topics and Their Clarification of This Chapter:

1. **Audit:**
   - **Definition:** An independent review and examination of records and activities to assess the adequacy of system controls, ensuring compliance with established policies and operational procedures.
   - **Real-life Scenario:** A financial institution conducts regular audits of its accounts to ensure that transactions are recorded accurately, funds are allocated correctly, and compliance regulations are met.

2. **Crime Prevention through Environmental Design (CPTED):**
   - **Definition:** An architectural approach to designing buildings and spaces that emphasizes passive features to reduce the likelihood of criminal activity.
   - **Real-life Scenario:** A city park is designed with open sightlines, well-lit pathways, and natural surveillance features to deter vandalism and ensure the safety of park visitors.

3. **Defense in Depth:**
   - **Definition:** An information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
   - **Real-life Scenario:** A company implements multiple security measures such as firewalls, antivirus software, employee training, and physical access controls to protect its network and data from cyber threats.

4. **Discretionary Access Control (DAC):**
   - **Definition:** Access control where the resource owner determines access rights to an object.
   - **Real-life Scenario:** A document stored on a shared drive allows the creator to decide who can view, edit, or delete it, granting discretionary access control to the file

5. **Encrypt:**

- **Definition:** To protect private information by converting it into a form that can only be read by people who have permission to do so.
- **Real-life Scenario:** A healthcare organization encrypts patient medical records to ensure that only authorized healthcare providers can access sensitive patient information.

6. **Firewalls:**
    - **Definition:** Devices that enforce administrative security policies by filtering incoming network traffic based on a set of rules.
    - **Real-life Scenario:** A home network uses a firewall to block unauthorized access attempts from the internet, protecting connected devices from malware and cyber attacks.

7. **Insider Threat:**
    - **Definition:** An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
    - **Real-life Scenario:** An employee with access to sensitive company data intentionally leaks confidential information to a competitor, posing an insider threat to the organization.

8. **iOS:**
    - **Definition:** An operating system manufactured by Apple Inc. Used for mobile devices.
    - **Real-life Scenario:** iPhones and iPads run on the iOS operating system, providing users with a secure and user-friendly platform for accessing apps, browsing the internet, and communicating with others.

9. **Layered Defense:**
    - **Definition:** The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.
    - **Real-life Scenario:** A bank implements a layered defense strategy by combining physical security measures (such as security guards and surveillance cameras) with cybersecurity measures (such as firewalls and intrusion detection systems) to protect its assets and customer data.

10. **Linux:**

- **Definition:** Linux is an operating system that is open source, making its source code legally available to end users. It is widely used in software development, server environments, and embedded systems.
- **Real-life Scenario:** A company opts to use Linux-based servers to host their website and applications due to its cost-effectiveness, reliability, and robust security features. They also leverage the open-source nature of Linux to customize and optimize their server infrastructure according to their specific needs.

11. **Log Anomaly:**

- **Definition:** A log anomaly refers to a system irregularity identified when analyzing log entries, indicating events that deviate from the expected behavior and may require further investigation.
- **Real-life Scenario:** An organization's cybersecurity team notices an unusual spike in network traffic during non-business hours recorded in the system logs. This anomaly prompts them to investigate potential security breaches or unauthorized access attempts, mitigating any potential threats to the network.

12. **Logging:**

- **Definition:** Logging involves collecting and storing user activities in a log, serving as a record of events occurring within an organization's systems and networks.
- **Real-life Scenario:** A network administrator configures logging on network devices, servers, and applications to capture important events such as login attempts, file access, and system changes. These logs are then regularly reviewed for security analysis, troubleshooting, and compliance auditing purposes.

13. **Logical Access Control Systems:**

- **Definition:** Logical access control systems are automated systems that control an individual's ability to access computer system resources based on their identity and role within the organization.
- **Real-life Scenario:** An employee uses their biometric authentication credentials to access secure areas of the organization's network and systems, such as confidential databases or financial records. The logical access control system verifies their identity and grants appropriate access privileges based on their role in the company.

14. **Mandatory Access Control:**

- **Definition:** Mandatory Access Control is an access control mechanism where the system itself manages access controls according to the organization's security policies.

- **Real-life Scenario:** In a government agency handling classified information, access to sensitive data is strictly controlled using mandatory access control mechanisms. Access rights are determined by security labels assigned to subjects and objects, ensuring that only authorized personnel can access classified information.

15. **Mantrap:**

- **Definition:** A mantrap is an entrance to a building or area that requires people to pass through two doors with only one door opened at a time, enhancing physical security by controlling access.
- **Real-life Scenario:** A high-security data center employs a mantrap system at its entrance, requiring visitors to pass through a series of locked doors. This ensures that only authorized personnel can enter the facility, reducing the risk of unauthorized access or security breaches.

16. **Object:**

- **Definition:** An object is a passive information system-related entity containing or receiving information, such as devices, files, records, or processes.
- **Real-life Scenario:** In a cloud storage system, a user uploads a file containing sensitive financial data. This file becomes an object within the storage system, and access to it is controlled based on the user's permissions and security settings.

17. **Physical Access Controls:**

- **Definition:** Physical access controls are mechanisms implemented through tangible means such as walls, fences, guards, and locks to secure physical assets and facilities.
- **Real-life Scenario:** An organization installs biometric scanners and access badges at entry points to restrict access to sensitive areas within their office building. Only employees with the appropriate authorization can enter these areas, ensuring physical security of the premises.

18. **Principle of Least Privilege:**

- **Definition:** The Principle of Least Privilege states that users and programs should have only the minimum privileges necessary to complete their tasks, reducing the risk of unauthorized access and potential misuse of privileges.
- **Real-life Scenario:** A software application is designed to grant users access only to the specific features and data required for their role. By adhering to the principle of least privilege, the application minimizes the risk of data breaches or unauthorized actions by limiting users' access to only what is necessary for their tasks.

19. **Privileged Account:**
    - **Definition:** A privileged account is an information system account with approved authorizations granted to privileged users, such as system administrators or IT managers.
    - **Real-life Scenario:** A system administrator uses a privileged account to perform administrative tasks such as installing software updates, configuring network settings, and managing user accounts on servers and network devices

20. **Ransomware:**
    - **Definition:** Ransomware is a type of malicious software designed to encrypt files or lock computer screens, preventing users from accessing their system or data. The attackers demand a ransom payment, usually in cryptocurrency, in exchange for decrypting the files or restoring access.
    - **Real-life Scenario:** A user unknowingly downloads a malicious email attachment containing ransomware. The ransomware encrypts all the files on the user's computer and displays a ransom note demanding payment within a specified time frame to decrypt the files.

21. **Role-based access control (RBAC):**
    - **Definition:** RBAC is an access control system that assigns user permissions based on predefined roles within an organization. Users are granted access privileges based on their assigned roles, simplifying access management and reducing the risk of unauthorized access.
    - **Real-life Scenario:** In a corporate network, employees are assigned roles such as "HR manager," "Sales representative," or "IT administrator." RBAC is implemented to grant each role specific access permissions, ensuring that HR managers can access employee records, while sales representatives can access customer data, and IT administrators can manage network resources.

22. **Rule:**
    - **Definition:** A rule is an instruction developed to allow or deny access to a system based on the validated identity of the subject compared to an access control list (ACL). Rules define the criteria for granting or denying access to resources based on specific conditions.
    - **Real-life Scenario:** In a firewall configuration, rules are set to control incoming and outgoing network traffic. For example, a rule might allow access to a web server from specific IP addresses while blocking access from all other sources.

23. **Segregation of Duties:**
    - **Definition:** Segregation of Duties (SoD) is the practice of distributing tasks and responsibilities within an organization to prevent a single person from completing a critical process independently. SoD reduces the risk of fraud, errors, and security breaches by requiring collaboration and oversight.
    - **Real-life Scenario:** In financial institutions, SoD is implemented to separate the roles of initiating payments, approving transactions, and reconciling accounts. For example, the employee responsible for initiating payments cannot also approve them, ensuring accountability and oversight.

24. **Subject:**
    - **Definition:** A subject is generally an individual, process, or device that causes information to flow among objects or changes the system state. Subjects can include users, applications, or automated processes interacting with system resources.
    - **Real-life Scenario:** In a computer network, a user logging into an application, a software process accessing a database, or a sensor collecting environmental data are all examples of subjects interacting with system resources.

25. **Technical Controls:**
    - **Definition:** Technical controls are security controls, safeguards, or countermeasures implemented and executed by the information system through mechanisms contained in hardware, software, or firmware components. Technical controls protect against security threats and vulnerabilities.
    - **Real-life Scenario:** Examples of technical controls include firewalls, encryption protocols, antivirus software, intrusion detection systems (IDS), and biometric authentication mechanisms, all designed to safeguard against unauthorized access, data breaches, and other security risks.

26. **Turnstile:**
    - **Definition:** A turnstile is a one-way spinning door or barrier that allows only one person at a time to enter a building or pass through a specific area. Turnstiles are commonly used for access control in public transportation, stadiums, and secure facilities.
    - **Real-life Scenario:** At a subway station, passengers must pass through a turnstile to enter the platform area. The turnstile allows only one person to pass through at a time, preventing unauthorized access and fare evasion.

27. **Unix:**

- **Definition:** Unix is an operating system used in software development, server environments, and networking. Unix-based systems are known for their stability, security, and flexibility, making them popular for hosting web servers, running enterprise applications, and managing network infrastructure.
- **Real-life Scenario:** Many web servers, cloud computing platforms, and scientific research institutions use Unix-based operating systems such as Linux and macOS for their reliability, security features, and compatibility with a wide range of software applications.

28. **User Provisioning:**

- **Definition:** User provisioning is the process of creating, maintaining, and deactivating user identities on a system. It involves managing user accounts, assigning access privileges, and ensuring appropriate permissions based on roles and responsibilities.
- **Real-life Scenario:** In an organization, the IT department oversees user provisioning activities such as creating new user accounts for employees, granting access to specific applications and resources based on job roles, and deactivating accounts when employees leave the company or change roles