Access Control Fundamentals in Operating System Security

Access control is a fundamental security mechanism that determines who can access what resources within an operating system. It aims to protect sensitive data, prevent unauthorized access, and maintain system integrity.

Key Concepts:

1. **Subject:** An entity that requests access to a resource (e.g., user, process).
2. **Object:** A resource that can be accessed (e.g., file, directory, network device).
3. **Access Right:** The type of access permitted to a subject on an object (e.g., read, write, execute, delete).

Types of Access Control:

- **Discretionary Access Control (DAC):**
  - The owner of a resource determines who can access it and with what privileges.
  - Example: File system permissions (read, write, execute) for owner, group, and others.
- **Mandatory Access Control (MAC):**
  - Enforces access control based on security labels assigned to subjects and objects.
  - Access is granted or denied based on the relationship between the subject's security label and the object's security label.
  - Example: Security-Enhanced Linux (SELinux).
- **Role-Based Access Control (RBAC):**
  - Assigns users to roles, and roles are associated with specific permissions.
  - Simplifies access control management for large organizations.
- **Attribute-Based Access Control (ABAC):**
  - Access decisions are based on attributes of the subject, object, and environment.
  - Provides fine-grained control and flexibility.

Access Control Mechanisms:

Access Control Lists (ACLs): Explicitly list the users or groups that have specific permissions

- **Capabilities:** Tokens that grant a subject the right to access a specific object.
- **Security Labels:** Labels assigned to subjects and objects to enforce access control policies in MAC systems.

Importance of Access Control:

- **Confidentiality:** Prevents unauthorized disclosure of sensitive information.
- **Integrity:** Ensures that data is not modified or deleted without proper authorization.
- **Availability:** Ensures that authorized users can access resources when needed. By implementing effective access control mechanisms, operating systems can protect critical resources, prevent unauthorized access, and maintain a secure computing environment.