**Access Control Concepts**

1. **Access Control**
   * **Explanation**: Mechanisms or policies that restrict who or what can view, modify, or use resources in a computing environment. It ensures that only authorized entities can access specific systems or data.
2. **Authentication**
   * **Explanation**: The process of verifying the identity of a user, system, or device before allowing access to resources. Common methods include passwords, biometrics, and multi-factor authentication (MFA).
3. **Authorization**
   * **Explanation**: Determines what an authenticated user is allowed to do on a system or network. It defines permissions to access specific resources, typically using role-based access control (RBAC) or other models.
4. **Multi-factor Authentication (MFA)**
   * **Explanation**: A security method that requires users to provide multiple forms of verification (e.g., something they know, have, or are) to gain access. MFA strengthens security by combining different types of credentials, like a password and a fingerprint.
5. **Role-Based Access Control (RBAC)**
   * **Explanation**: Access is granted based on the roles a user holds within an organization. Permissions are associated with specific roles rather than individual users, making access easier to manage.
6. **Discretionary Access Control (DAC)**
   * **Explanation**: An access control model where the owner of the resource determines who has access to it. The owner can grant or revoke permissions as needed.
7. **Mandatory Access Control (MAC)**
   * **Explanation**: A strict access control model where access to resources is based on predefined security labels. Users and resources are classified, and only those with the appropriate level of clearance can access specific data.
8. **Attribute-Based Access Control (ABAC)**
   * **Explanation**: A model that grants access based on user attributes (e.g., department, job title, or location) and environmental conditions (e.g., time of day). It allows for more fine-grained access control.
9. **Least Privilege**
   * **Explanation**: A security principle that ensures users or systems are only granted the minimum level of access necessary to perform their job functions. Reducing permissions minimizes the attack surface.
10. **Separation of Duties (SoD)**
    * **Explanation**: A principle that divides tasks and responsibilities among multiple individuals to prevent fraud, errors, or abuse. For example, the person who authorizes a transaction should not be the one executing it.
11. **Access Control List (ACL)**
    * **Explanation**: A list that defines which users or systems are granted or denied access to resources, such as files, directories, or network segments. ACLs specify which permissions apply to each user or group.
12. **Identity and Access Management (IAM)**
    * **Explanation**: A framework that manages digital identities and controls who has access to what within an organization. IAM systems include authentication, authorization, and user lifecycle management.
13. **Single Sign-On (SSO)**
    * **Explanation**: A system that allows users to authenticate once and gain access to multiple resources without re-entering credentials. SSO improves user convenience while maintaining security.
14. **Federated Identity Management (FIM)**
    * **Explanation**: A system that enables users to authenticate across multiple systems or organizations using a common identity. This is often used for cross-organizational or cloud-based services.
15. **Access Token**
    * **Explanation**: A digital credential used to access specific resources or systems. Tokens are often issued after authentication and contain specific permissions for accessing resources.
16. **Session Management**
    * **Explanation**: The process of managing user sessions once access is granted. This includes tracking active sessions, setting timeouts, and revoking access when necessary.
17. **Principle of Need to Know**
    * **Explanation**: A principle where access to information is restricted to individuals who need it to perform their job duties. It limits the dissemination of sensitive data.
18. **Access Control Policy**
    * **Explanation**: A formal document that outlines an organization’s rules for granting and managing access to its systems and resources. This includes guidelines on roles, permissions, and monitoring.
19. **Zero Trust**
    * **Explanation**: A security model that assumes no user or system is trusted by default, even if inside the network. Access is continuously verified, and only minimal privileges are granted based on strict policies.
20. **Password Policy**
    * **Explanation**: A set of rules governing the creation and management of user passwords, typically enforcing complexity, length, and expiration periods to enhance security.
21. **Biometrics**
    * **Explanation**: A method of authentication based on physical characteristics of users, such as fingerprints, facial recognition, or iris scans. Biometrics provide strong security as they are unique to each individual.
22. **Context-Aware Access Control**
    * **Explanation**: An access control method that takes into account context factors like the user’s location, device, or time of access when determining whether to grant access.
23. **Privilege Creep**
    * **Explanation**: A situation where a user accumulates excessive privileges over time, often due to job role changes or insufficient privilege management. It increases the risk of unauthorized access.
24. **Privileged Access Management (PAM)**
    * **Explanation**: A security strategy focused on controlling and auditing access to critical systems by privileged users (e.g., administrators), ensuring that sensitive systems are protected from misuse.
25. **User Provisioning and De-provisioning**
    * **Explanation**: The process of granting (provisioning) and removing (de-provisioning) access to resources based on an individual’s role or employment status. Proper user lifecycle management helps prevent unauthorized access.
26. **Access Review**
    * **Explanation**: The process of periodically reviewing access permissions to ensure they are up to date and in line with current job roles. Access reviews are a key part of maintaining proper security controls.
27. **Role Engineering**
    * **Explanation**: The process of designing and defining roles within an organization to ensure appropriate access control and simplify the assignment of permissions.
28. **Security Assertion Markup Language (SAML)**
    * **Explanation**: A standard used for exchanging authentication and authorization data between parties, often used in SSO and federated identity management systems.
29. **OAuth**
    * **Explanation**: An open standard for token-based authorization, often used to grant third-party applications limited access to a user's resources without exposing their credentials.
30. **Time-Based Access Control**
    * **Explanation**: A method where access to resources is limited to specific time periods. This is often used to restrict access during non-working hours to enhance security.