Identity

Identity management is critical to securing access to resources in any organization. It **defines who can access what and under which conditions**, ensuring that only authorized users and services interact with sensitive data. Key concepts include **Access Control Lists (ACLs), service accounts vs. user accounts, impersonation, and federated identity**.

1. Access Control Lists (ACLs)

- Definition: An ACL is **a set of rules that defines which authenticated users or services have permission to access specific resources and what actions they can perform**.
- Purpose: ACLs are used to **enforce access control policies**, allowing organizations to restrict access based on user identity and predefined permissions.
- How It Works
  - Each entry in an ACL **specifies a subject (user, group, or service) and their permitted actions (read, write, execute, etc.) on a resource**.
  - ACLs can be implemented at various levels, such as file systems, databases, and network resources.
- Example: A file system ACL may allow a user to read a file but deny write access, ensuring data integrity by limiting modification rights to specific users.

2. Service Accounts vs. User Accounts

- **User Accounts**
  - Definition: User accounts are created for individuals who need access to systems, applications, or resources for their job functions.
  - Privileges: User accounts are typically **assigned privileges based on the user's role** and are subject to regular review and adjustments.
  - Authentication: User accounts use personal credentials for access, often combined with **multi-factor authentication**.
- **Service Accounts**
  - Definition: Service accounts, also known as robot accounts, are non-human accounts **created to support automation and application-to-application communication.
  - Purpose: Used by applications, scripts, or automation processes to access resources without human intervention.
  - Privileges: Service accounts **should be restricted to the minimum permissions required for their tasks**, as these accounts can be highly targeted by attackers.
  - Security Implications
    - Privileges: Over-permissioned service accounts are a common security risk, especially in cloud environments.
    - Attack Vector: Attackers may **target service accounts to gain access to resources or escalate privileges**, making it critical to enforce the principle of least privilege.
  - Example: A service account used by a backup service might need read access to databases and storage but shouldn't have administrative privileges.

3. Impersonation

- Definition: Impersonation is when an entity (user or service) **assumes the identity and privileges of another entity**. In cloud environments, this often involves **obtaining tokens or keys to act on behalf of a legitimate account**.
- How It Works
    - Exported Account Keys: Attackers may acquire access keys or credentials associated with an account, allowing them to operate with the same privileges.
    - ActAs and Impersonation Tokens
        - Some cloud providers allow specific roles or services to “ActAs” another user or service, temporarily assuming their identity to perform specific actions.
        - This is commonly done **using tokens, such as JWT (JSON Web Tokens)**, which include identity claims and can be used to authenticate and authorize actions on behalf of another identity.
- Security Implications
    - **Token Compromise**: If JWTs or other tokens are stolen, attackers can perform actions as the impersonated identity.
    - **Privilege Escalation**: Improper use or configuration of ActAs permissions can allow attackers to gain higher privileges by impersonating more privileged accounts.

4. Federated Identity

- Definition: Federated identity **allows users to authenticate with multiple systems or organizations using a single identity from an external identity provider (IdP)**, rather than creating separate accounts for each system.
- How It Works
    - **Single Sign-On (SSO)**: Federated identity is often implemented as part of SSO systems, where **users authenticate with a central IdP**, and the IdP vouches for their identity across different applications and services.
    - **Identity Providers**: Examples include Google, Microsoft, Okta, and other services that allow users to log in with their corporate or personal credentials across multiple applications.
    - **Security Protocols**: Federated identity commonly uses protocols like **SAML (Security Assertion Markup Language)** and **OAuth** to enable secure identity federation across organizations.
- Benefits
    - **Reduced Complexity**: Users can access multiple applications with one identity, reducing password fatigue.
    - **Improved Security**: Centralized authentication with the IdP simplifies account management and enables consistent security policies.
- Security Considerations
    - **Trust in the IdP**: Organizations must trust the security of the IdP since a compromise at the IdP level affects all federated services.
    - **Access Control Consistency**: Proper configuration of permissions across federated systems is essential to prevent over-permissioned access.

Comparison Table

Aspect	User Accounts	Service Accounts	Federated Identity

Aspect	User Accounts	Service Accounts	Federated Identity
Purpose	Individual access	Automation, service-to-service access	Cross-application identity sharing
Privileges	Role-based	Minimal, task-specific	Defined by federated systems
Security Requirements	MFA, role-based permissions	Limited privileges, monitoring	Trust in IdP, access control alignment
Common Security Concerns	Account compromise, password reuse	Privilege escalation, token misuse	IdP compromise, misconfigured access

Summary

- **ACLs**: Define permissions for users or services on resources, controlling access based on identity.
- **Service Accounts vs. User Accounts**: Service accounts facilitate automation and should have limited permissions, while user accounts are for individuals with role-based privileges.
- **Impersonation**: Allows entities to act on behalf of others, often using tokens or keys; it can be abused by attackers if tokens or impersonation permissions are improperly secured.
- **Federated Identity**: Enables users to access multiple systems with a single set of credentials via an external IdP, improving usability but requiring robust trust and access control.

Each of these identity management mechanisms plays a unique role in access control and security. Understanding their differences and best practices helps organizations protect resources by controlling access, reducing over-permissioned accounts, and ensuring secure authentication across services and platforms.