DATA PROTECTION, PRIVACY AND ANONYMITY

Another one.

Fabio Lorenzato

Contents

Chapter 1

Definitions

A fundamental requirement of any information management system is the protection of data and resources from unauthorized access, modification, or service denial. To achieve this, access control mechanisms ensure that only authorized accesses occur within a system.

1.1 Definitions from Standards

The concept of access control is formally defined in several standards:

- **NISTIR 7298**: Access control is "the process of granting or denying specific requests to obtain and use information and related information processing services, or to enter specific physical facilities."
- **RFC 4949**: Access control is "a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems)."

1.2 Access Control Security Requirements

Access control mechanisms should allow specification of:

1. Authorized users and their permissions.
2. The resources they can access.
3. The duration and conditions of access.
4. The specific operations they are permitted to perform.

A comprehensive set of security requirements is outlined in NIST SP 800-171, including:

1.2.1 Basic Security Requirements

1. Restrict system access to authorized users, processes, and devices.
2. Limit user access to only authorized transactions and functions.

1.2.2 Derived Security Requirements

Additional controls include:

1. Enforcement of information flow restrictions.
2. Separation of duties to prevent collusion.
3. Implementation of the principle of least privilege.
4. Prevention of non-privileged users from executing privileged functions.
5. Use of cryptographic mechanisms for securing remote access.
6. Authorization and encryption for wireless access.
7. Control over external system connections and mobile devices.

1.3 Access Control Principles

Access control is a core aspect of computer security. RFC 4949 defines computer security as "measures that implement and assure security services in a computer system, particularly those that assure access control service."

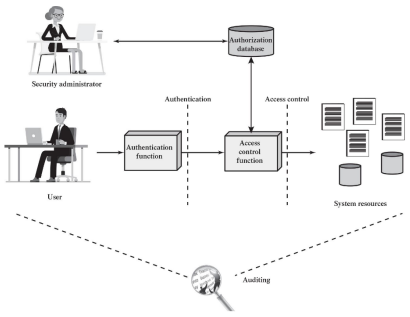

Figure 1.1: Access Control Principles

1.4 Relationship with Other Security Functions

Access control interacts with several other security functions:

- **Authentication**: Verifies user credentials before granting access.
- **Authorization**: Determines permissions based on policies and trust levels.
- **Audit**: Ensures compliance by reviewing system activities and identifying security breaches.

Administrators manage an authorization database, while authentication functions verify users before granting access. Auditing provides an independent review to maintain security compliance.

1.5 Authentication and Audit

Authentication ensures that a user or process is verified before accessing system resources. Auditing plays a crucial role in maintaining security by monitoring activities.

1.5.1 Internal and External Audit

IT enterprises conduct two types of audits:

Internal Audit is performed within the organization to identify risks related to performance, security, and compliance. Internal auditors monitor mitigation efforts to improve the organization's security posture.

External Audit is conducted by independent professionals, often Certified Public Accountants (CPAs), who assess an organization's security and compliance. External audit reports are vital for stakeholders and clients.

1.6 Access Control Mechanisms

An access control mechanism regulates interactions between users and system resources such as applications, operating systems, firewalls, routers, files, and databases.

The process involves:

1. Authentication of the entity seeking access. 2. Authorization checks against an access control database. 3. Enforcement of access control policies.

Operating systems incorporate built-in access control functions, supplemented by security add-ons and application-specific controls.

1.7 Security Mechanisms and Policies

Security mechanisms enforce policies through software and hardware functions. The separation of policies from mechanisms allows flexibility in implementation.

A security mechanism should:

- Independently define protection requirements. - Compare different policies and enforcement mechanisms. - Support multiple policies within the same system.

1.7.1 Access Control Policies

Access control policies define rules for regulating user access. They specify what types of access are permitted, under what conditions, and by whom. These policies can be formalized into authorization databases.

1.8 Subjects, Objects, and Access Rights

A well-defined access control system must identify:

- **Objects**: The resources requiring protection. - **Subjects**: Entities requesting access. - **Actions**: Operations performed on objects.

Objects include files, databases, messages, and programs. The number and type of protected objects depend on system complexity and security requirements.

Subjects represent active entities such as users, applications, and processes. Subjects are accountable for their actions, with audit trails recording relevant activities.

Actions refer to access operations such as Read, Write, Execute, Delete, Create, and Search.

1.9 Access Control Policy Models

Access control policies are categorized into:

Discretionary Access Control (DAC): Grants access based on user identity and explicit authorization rules. Users can delegate their access privileges to others.

Mandatory Access Control (MAC): Enforces access restrictions based on security labels and clearance levels. Users cannot override these restrictions.

Role-Based Access Control (RBAC): Grants access based on organizational roles rather than individual identities. Users inherit permissions from their assigned roles.

Attribute-Based Access Control (ABAC): Grants access based on attributes of users, objects, and environmental conditions, offering a flexible and dynamic approach.

1.10 Implementation of Access Control

Access control mechanisms are implemented using:

- **Access Control Lists (ACLs)**: Define permissions for each user-object pair. - **Capability Lists**: Assign access rights to subjects rather than objects. - **Authorization Tables**: Store access rules as a set of conditions.

1.11 Advanced Access Control Concepts

1.11.1 Least Privilege and Separation of Privilege

The principle of least privilege ensures that subjects are granted the minimum access necessary to perform their tasks, reducing the risk of unauthorized actions.

Separation of privilege divides access across multiple entities, requiring more than one authorization to perform critical actions, thereby mitigating insider threats.

1.11.2 Role Hierarchies and Constraints in RBAC

Role hierarchies allow roles to inherit permissions from superior roles. Constraints define conditions such as:

- Mutually exclusive roles (a user can hold only one role in a set). - Cardinality limits (restricting the number of users per role). - Prerequisite roles (requiring users to hold a specific role before obtaining another).

1.11.3 ABAC and its Flexibility

ABAC offers a powerful and flexible access control model by evaluating attributes of subjects, objects, and environmental conditions. However, it requires high computational effort, making it more complex than DAC and RBAC.