1. Introduction to Access Control

1.1 What is Access Control?

1.1.1 Core Concepts:

Subject:

Object:

Action:

Policy:

1.1.2 Analogy:

1. Introduction to Access Control

1.1 What is Access Control?

Access control is a security mechanism that regulates who or what can view or use resources in a computing environment. It is a fundamental component of information security, ensuring confidentiality, integrity, and availability.

1.1.1 Core Concepts:

Subject: An active entity that requests access to an object. Examples include a user, a process, a device, or a system.

Detailed Explanation:

A subject is the entity that initiates an action or request. It can be a person, a program, or a device.

In access control, it's crucial to identify and authenticate subjects accurately.

Examples:

A user typing their credentials to log in.

A program trying to read a file.

A device sending a request to a server.

Object: A passive entity that contains information or provides a service. Examples include a file, a directory, a database record, a web page, a function, an API endpoint, or a network resource.

Detailed Explanation:

An object is the resource that a subject wants to access.

Objects need to be protected from unauthorized access.

Examples:

A file containing sensitive data.

A database storing user information.

A web page displaying confidential information.

An API endpoint that performs a critical operation.

Action: An operation that a subject can perform on an object. Common actions include read, write, execute, delete, modify, access, create, update, and administer.

Detailed Explanation:

An action is the specific operation that a subject wants to perform on an object.

Access control systems define which actions are allowed for which subjects on which objects.

Examples:

A user reading a file.

A program writing to a database.

A user executing a program.

An administrator deleting a user account.

Policy: A set of rules that define the allowed actions for subjects on objects. Access control policies are the core of access control systems.

Detailed Explanation:

Access control policies are the rules that govern whether access is granted or denied.

Policies can be based on various factors, such as:

The identity of the subject.

The role of the subject.

The attributes of the subject or object.

The context of the access request.

Examples:

"Only administrators can delete user accounts."

"Users can only access their own files."

"Access is allowed only during business hours."

1.1.2 Analogy:

Imagine a building with different rooms. Access control determines who can enter the building, which rooms they can enter, and what they can do inside each room (e.g., read a book, use a computer, access a safe, or clean the room).

Detailed Explanation:

This analogy helps to visualize the different components of access control.

The building represents the system or resource.

The people represent the subjects.

The rooms represent the objects.

The keys and security guards represent the access control mechanisms.

The rules about who can enter which rooms represent the access control policies.