ACCESS CONTROL

Contents

1. What is Access Control ?

- **Access control** are methods used to restrict and allow access to certain items, such as automobiles, homes, computers, and even your smartphone.
- **Access control** is the process of protecting a resource so that it is used only by those allowed to use it.

2. Four-Part Access Control

- **Identification**: Who is asking to access the asset?
- **Authentication**: Can the requestor’s identity be verified?
- **Authorization**: What, exactly, can the requestor access? And what can they do?
- **Accountability**: How can actions be traced to an individual? We need to ensure that a person who accesses or makes changes to data or systems can be identified

Authorization Policies

- The first step to controlling access is to create a policy that defines authorization rules.
- **Authorization** is the process of deciding who has access to which computer and network resources:
  - Authorization policy is based on job roles
  - Authorization policy is based on each individual user

Methods and Guidelines for Identification

- **Identification Methods:** username, smart card, Biometric (fingerprints, face, voice, …)
- **Identification Guidelines:** To ensure that all actions carried out in a computer system can be associated with a specific user, each user must have a unique identifier

Processes and Requirements for Authentication

- Authentication Types: There are five types of authentication
  - **Knowledge**: Something you know, such as a password, passphrase, or personal identification number (PIN).
  - **Ownership**: Something you have, such as a smart card, key, badge, or token.
  - **Characteristics**: Some attribute that is unique to you, such as your fingerprints, retina, or signature.

Processes and Requirements for Authentication

- Authentication Types:
  - **Location**: Somewhere you are, such as your physical location when you attempt to access a resource
  - **Action**: Something you do or how you do it, such as the way you type on a keyboard

Policies and Procedures for Accountability

- Accountability is tracing an action to a person or process to know who made the changes to the system or data.
  - Log Files
  - Monitoring and Reviews

2. Four-Part Access Control

These four parts are divided into two phases:

- **The policy definition phase**: This phase determines who has access and what systems or resources they can use. The authorization definition process operates in this phase.
- **The policy enforcement phase**: This phase grants or rejects requests for access based on the authorizations defined in the first phase. The identification, authentication, authorization execution, and accountability processes operate in this phase

3. Types of Access Controls

- **Physical access controls:** These control access to physical resources. They could include buildings, parking lots, and protected areas.
- **Logical access controls:** These control access to a computer system or network. Your company probably requires that you enter a unique username and password to log on to your company computer

4. Formal Models of Access Control

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-Based Access Control
- Rule-based access control

a. Discretionary Access Control (DAC)

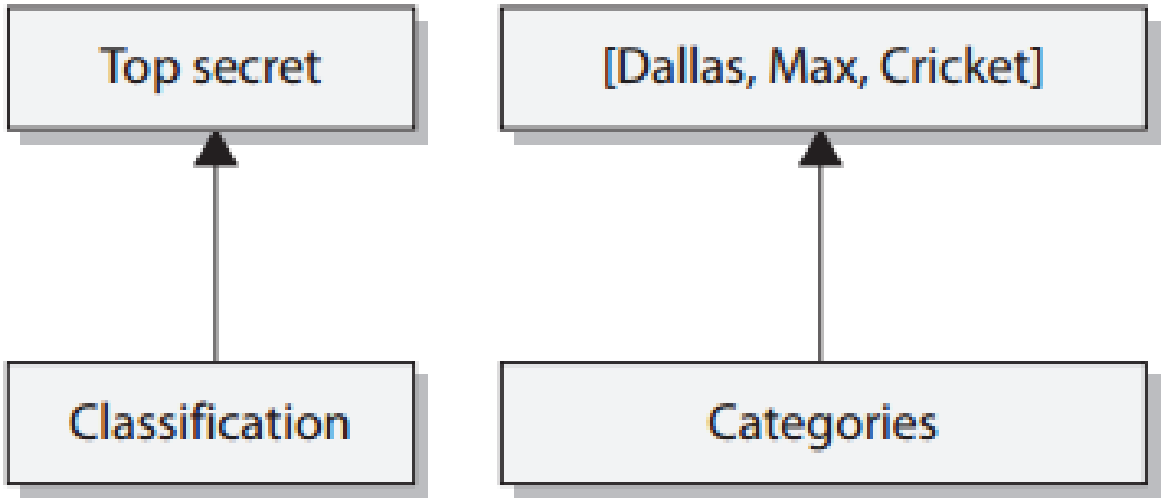
- Means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
- In a DAC model, access is restricted based on the authorization granted to the users

a. Discretionary Access Control (DAC)

- In a DAC environment, the authorization system uses permission levels to determine what objects any subject can access. Permission levels can be any of the following:
  - User-based
  - Job-based, group-based, or role-based access control (RBAC)
  - Project-based
  - Task-based

b. Mandatory Access Control

- In a mandatory access control (MAC) model, users do not have the discretion of determining who can access objects as in a DAC model.
- **Security labels** are attached to all objects; thus, every file, directory, and device has its own security label with its classification information



c. Role-Based Access Control

- A role-based access control (RBAC) model uses a centrally administrated set of controls to determine how subjects and objects interact.
- This type of model lets access to resources be based on the role the user holds within the company.
- An RBAC model is the best system for a company that has high employee turnover

d. Rule-Based Access Control

- Rule-based access control uses specific rules that indicate what can and cannot happen between a subject and an object.
- *"If the user's ID matches the unique user ID value in the provided digital certificate, then the user can gain access."*

Thanks