D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Subject Name: Information System

Unit No:02 Unit Name: Access Control Models

Faculty:Mrs. Bhavana Alte

Mr. Prathmesh Gunjgur

Unit No: 2 Unit Name: Access Control Models

Introduction to Access Control Models, Discretionary Access Control (DAC)

What is Access Control?

- Access control is the mechanism that defines who can access a system, what actions they can perform, and what resources they can interact with.
- To ensure **security**, **confidentiality**, and **integrity** of systems and data by restricting unauthorized access.
- **Example**:
- Think about an office building where only authorized personnel can enter certain rooms, access specific files, or perform particular tasks.

Why is Access Control Important?

- **Security**: Prevent unauthorized access to sensitive data or resources.
- **Auditability**: Track who accessed what, when, and why.
- **Confidentiality**: Protect sensitive information from unauthorized disclosure.
- **Compliance**: Ensure organizations meet regulatory and legal requirements

Example:

- A bank needs to ensure that only authorized bank tellers have access to customer accounts. If an unauthorized person gains access, it could lead to data breaches or financial fraud.

Key Concepts in Access Control

- **Authentication**: Verifying the identity of the user. (e.g., username and password)
- **Authorization**: Granting or denying access to resources based on permissions and policies.
- **Accounting/ Auditing**: Tracking user activities to ensure policies are followed and to identify potential security breaches.

Introduction: Authentication vs. Authorization

- **Authentication:** It is the process of verifying who you are.
- For example, when you log in to a website with your username and password, the system checks if you are the user you claim to be.
- Example: When you use your fingerprint to unlock your phone, you are being authenticated.
- **Authorization:** After authentication, authorization determines what you are allowed to do on the system.
- For example, an administrator can install software on a computer, but a regular user may not have that permission.

•***Authentication****: "Are you who you say you are?“*

•***Authorization****: "Are you allowed to do that?"*

Authentication Methods

- Authentication can be based on three key methods, also called "somethings":

- **Something You Know**: A password.
  - **Example**: When you enter your username and password to log in to your email.

- **Something You Have**: A physical device.
  - **Example**: Using an ATM card to withdraw money from a bank.

- **Something You Are**: Physical characteristics.
  - **Example**: Using a fingerprint scanner on a phone for login.

1.Passwords

- **Weaknesses of Passwords**: Passwords are the most common method of authentication, but they are often weak. Users tend to choose easy-to-guess passwords, making it easier for attackers to crack them.

  - **Example of weak password**: “password123”
  - **Better password**: “nG$2@Mn*”

- **Cryptographic Keys vs. Passwords**: Cryptographic keys are more secure than passwords. For instance, a randomly generated 64-bit key has more possible combinations and is harder to crack compared to a typical 8-character password.

2. Password Verification

- **Hashing Passwords**: Instead of storing raw passwords, systems store a hash (a unique representation) of the password. This makes it harder for attackers to retrieve the original password if they steal the password file.

- **Example**: If your password is "mypassword", the system stores a hash like "5f4dcc3b5aa765d61d8327deb882cf99". When you log in, it hashes your input and compares it with the stored hash.

Password Issues

•**Password Reuse**: Users often reuse the same password across multiple sites. If one password is cracked, attackers might try it on other services.

•**Example**: If your password "12345" is cracked on one site, the attacker may try it on other sites where you use the same password.

•**Social Engineering**: Attackers can trick you into revealing your password by pretending to be someone you trust.

•**Example**: An attacker calls you pretending to be a tech support agent and asks for your password to "fix" an issue.

•**Keystroke Logging**: Malicious software can record your typing, including passwords, without you knowing.

•**Password Cracking Tools**: Tools like "John the Ripper" can automate the process of trying thousands of passwords.

•**Example**: An attacker can use precompiled dictionaries with common passwords to speed up the cracking process.

Biometrics

- **Biometrics** is a method of authentication based on **something you are**.
- "you are your key."
- It is seen as a more secure alternative to passwords because it uses unique physical or behavioral traits.
- **Example**: Using your fingerprint to unlock your phone or a face recognition system for authentication at a security checkpoint.

Ideal Biometrics Characteristics

•**Universal**: It should work for everyone.

•**Example**: Fingerprints are commonly used, but some people may have no fingerprints or scars that make them unreadable.

•**Distinguishing**: It should distinguish individuals with high certainty.

•**Example**: A well-designed facial recognition system can distinguish between individuals with little to no error.

•**Permanent**: It should not change over time.

•**Example**: Fingerprints are permanent, unlike your voice, which can change with age or illness.

•**Collectable**: The characteristic should be easy to collect without causing harm.

•**Example**: Scanning a fingerprint is easy and non-invasive.

•**Reliable & User-Friendly**: The system should work consistently and be easy to use.

•**Example**: A facial recognition system that works well in different lighting conditions.

Biometric Identification vs. Authentication

•**Identification** answers the question: "Who are you?"

•**Example**: A criminal’s fingerprint is compared to a database of millions to identify them.

•It is harder because it involves comparing a sample to many records (one-to-many comparison).

•**Authentication** answers: "Are you who you say you are?"

•**Example**: A person uses a thumbprint scanner to unlock their device, where the fingerprint is compared only with their stored fingerprint (one-to-one comparison).

Types of Biometric Errors

•**Fraud Rate (False Acceptance)**: When the system mistakenly accepts an unauthorized user.

•**Example**: Bob tricks the system into thinking he is Alice.

•**Insult Rate (False Rejection)**: When the system mistakenly rejects an authorized user.

•**Example**: Alice’s fingerprint is rejected even though it’s hers.

Biometric Examples

- **Fingerprint**:
- Fingerprints are widely used in authentication systems, from unlocking phones to criminal identification.
- **Example**: A fingerprint scanner at an airport security gate.

- **Hand Geometry**:
- This involves measuring the shape of a person’s hand for authentication.
- **Example**: Used in secure buildings to verify authorized personnel.

- **Iris Scan**:
- The iris (colored part of the eye) has a unique pattern for each individual and remains stable over time.
- **Example**: Some airports use iris scans for fast and secure passenger identification.

Biometrics vs. Passwords

- **Biometrics** offer greater security than passwords since they are hard to replicate or guess.
  - **Example**: A password can be cracked, but copying someone's fingerprint or iris is much harder.
- **Drawback**: Biometric data can't be changed. If someone steals your biometric data (e.g., fingerprint or iris scan), it’s difficult to revoke or change.
  - **Example**: If someone steals your password, you can change it, but if they steal your fingerprint, it's not so easy to "reset."

Something You Have

•**Smartcards**: These are credit-card-sized devices that store cryptographic keys or secrets and perform some computations. They are used with a reader to authenticate the user.

•**Example**: A smartcard reader at an office door to grant access.

.

•**Authentication with "Something You Have"**: This method requires the user to physically possess an item, such as an ATM card, laptop, or smartcard.

•**Example**: To log into a system, Alice needs to have her ATM card and know her PIN.

Authorization

- **Authorization** is the process that defines what actions an **authenticated user** is allowed to perform. After authentication (verifying who you are), **authorization** controls what you can do on the system.
- **Example**: After logging in to your work computer, the system restricts you from accessing confidential files that only managers can see.
- **Authorization in Modern Systems**
- **Authorization** is often combined with tools like **CAPTCHAs**, **firewalls**, and **intrusion detection systems** to control access to both **individual systems** and **networks**.
- **Example**: A **firewall** might block certain types of network traffic, ensuring unauthorized users can't access sensitive data.

Types of Access Control Models

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Task-Based Access Control (TBAC)
- Unified Models
- Access Control Algebra
- Temporal and Spatio-temporal Models

Access Control Models Overview

1. DAC (Discretionary Access Control):

•**Owner-based** access control model.

•Owners can decide who has access to their resources.

2. MAC (Mandatory Access Control):

•**System-enforced policies** control access to resources.

•Resources are classified, and access depends on security labels assigned to both subjects and objects.

3. RBAC (Role-Based Access Control):

- Access is determined by the **roles** users hold.
- Example: A user in the "Admin" role may have access to all resources, while a "Guest" role has restricted access.

Access Control Models Overview

4. TBAC (Task-Based Access Control):

•Access granted based on the **tasks** a user is performing.

•Example: A factory worker might be granted access to machinery control only during maintenance tasks.

5. Unified Models:

- A combination of various access control models to address different security needs.

6. Access Control Algebra:

- The use of **logical operations** to combine access control policies.
- It is a method used to express and combine access control policies using logical operations, such as **AND**, **OR**, and **NOT**
- **AND (∧)**: Both conditions must be true for access to be granted.

Access Control Models Overview

7. Temporal and Spatio-Temporal Models:

- **Time-based** and **location-based** restrictions for access control.
- Example: Access to a building may be allowed only during certain hours and from specific IP addresses.

Scenario 1: Hospital Management System

- **Situation**: A hospital management system manages patient records, treatment history, and medication information. There are multiple users: doctors, nurses, administrative staff, and lab technicians. Each user needs different levels of access to the system depending on their role and task.
- Questions?
- Which access control model would you recommend for the hospital system?

Importance of Access Control

- Protect sensitive data.
- Prevent unauthorized access.
- Audit access and track security violations.

D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You