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

Unified Access Control Models

Unified Access Control Models:

- **Unified Access Control Models** combine elements of different access control models to provide a **comprehensive and flexible approach** to access control.
- In the real world, different organizations may have varied needs, and no single access control model (such as **Role-Based Access Control (RBAC)** or **Task-Based Access Control (TBAC)**) may meet all their security requirements.
- **Unified models** aim to blend the strengths of multiple models, addressing the **varied security needs** of an organization while **simplifying management** and ensuring **consistent enforcement** of policies across different levels of access.

Key Concepts of Unified Models

- A **Unified Access Control Model** typically:
- **Combines** multiple models, such as **RBAC**, **ABAC (Attribute-Based Access Control)**, and **MAC (Mandatory Access Control)**, to cover a wide range of use cases.
- **Supports complex and flexible policies**, combining the static nature of **roles** with the **dynamic nature of attributes** (like time, location, and environment).
- **Centralizes the management** of access policies while still considering the various permissions required at different organizational levels.

Types of Unified Access Control Models

- **Role-Based and Attribute-Based (RBAC + ABAC)**
- **Role-Based and Task-Based (RBAC + TBAC)**
- **Discretionary and Mandatory Access Control (DAC + MAC)**
- **Combining RBAC, ABAC, and MAC**

1. Role-Based and Attribute-Based Access Control (RBAC + ABAC)

- **ABAC** (Attribute-Based Access Control) assigns permissions based on **attributes** (e.g., department, time of day, location) of the **user**, **resource**, and **environment**. For example, a user may be granted access to a resource if their role is “Manager” and the current time is within working hours.

- In a **Unified RBAC + ABAC Model**, access control is determined based on both:
- The **user’s role** (e.g., Admin, Employee).
- **Attributes** such as time of day, location, or other environmental factors.

- **How it Works:**
- **Role**: A user is assigned a role (Admin, Manager, Employee).
- **Attributes**: Additional attributes (such as time or location) determine the **context** of access.

Example:

- Consider a company where:
- **Admin** has the role to **create**, **read**, **update**, and **delete** files.
- **Manager** has the role to **read** and **update** files but cannot delete them.
- **Employee** has the role to **read** files but cannot modify them.

- In this **RBAC + ABAC** model, an additional **attribute** might be added:
- **Time of Day Attribute**: Access to certain resources (e.g., sensitive financial reports) may only be allowed during working hours (9 AM to 5 PM).
- **Location Attribute**: Employees accessing resources from **outside the company network** may be restricted to read-only access, while those on the company network may have full access.

Benefits of this Unified Model:

- **Flexibility**: Combines **role-based security** with the flexibility of **contextual attributes**, such as time, location, or even device type.
- **Granularity**: Provides fine-grained access control based on dynamic factors, making it suitable for modern, dynamic environments.

2. Role-Based and Task-Based Access Control (RBAC + TBAC)

- In a **Unified RBAC + TBAC Model**, access control is granted based on both:
- The **role** of the user (e.g., Admin, Manager).
- The **specific task** they are performing (e.g., reviewing a report, approving a request).

- **How it Works:**
- **Role**: A user is assigned a role (Admin, Employee, etc.), which determines the **general permissions** they have.
- **Task**: For each specific task the user performs (e.g., reviewing a report, approving a request), they are granted additional permissions.

Example:

- Consider a **Document Management System** where employees have different roles and need to perform specific tasks:
- **Admin Role**:
  - Permissions: Full access to **all tasks** (create, read, update, delete documents).
- **Manager Role**:
  - Permissions: Can only **review** and **approve** reports.
- **Employee Role**:
  - Permissions: Can **create** and **read** reports but cannot approve them.
- In this **RBAC + TBAC** model, access permissions depend on:
- **Role**: The **Admin** has full control over the document system, while the **Employee** has limited access.
- **Task**: The **Manager** can review and approve reports, but cannot create new ones.

Benefits of this Unified Model:

- **Fine-Grained Control**: Combines the **role-based structure** with **task-specific access**, providing more flexible and precise control over what users can do.
- **Task-Oriented Security**: Access is determined not just by the role but by **what the user is trying to do**, adding an extra layer of security.

3. Discretionary and Mandatory Access Control (DAC + MAC)

- **Example:**
- **DAC**: A file owner grants access to specific users (e.g., “Employee A” can access file X).
- **ABAC**: The access might depend on the **time of day.** For example, "Employee A" might only be able to access file X **during office hours** but not outside of those hours.

Scenario 1: Healthcare System (RBAC + ABAC)

- In a **healthcare system**, a unified model combining **RBAC** and **ABAC** might be used:
- **Roles**: Doctors, Nurses, Administrative Staff.
- **Attributes**: Patient's condition (critical, non-critical), Time of Day (emergency hours, regular hours), Department (Cardiology, Neurology).

- **Example Access Decision**:
- A **Doctor** in the **Neurology Department** can access **patient records** based on their role, but access might be restricted during **non-emergency hours** unless the patient's condition is **critical**.

Scenario 2: Government Agency (RBAC + MAC)

- A **government agency** might implement a unified model using **RBAC** and **MAC**:
- **Roles**: Admin, Analyst, Employee.
- **Security Levels**: Top Secret, Secret, Confidential, Public.

- **Example Access Decision**:
- An **Admin** role might have the clearance to modify resources, but their access to **Top Secret** data is restricted by **MAC policies** unless they have the appropriate **security clearance**.

Scenario 3: Financial System (DAC + ABAC)

- A **financial system** might combine **DAC** and **ABAC** for access control:
- **Resource Owners**: Finance department members (who own financial reports).
- **Attributes**: User department, location (office or remote), time of day.
- **Example Access Decision**:
- **DAC**: A finance department employee might grant access to a financial report to a colleague.
- **ABAC**: However, access might be restricted based on attributes like time of day (e.g., reports can only be accessed during office hours), location (e.g., employees working remotely may have restricted access), and departmental roles (e.g., only those in the finance department).

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

Thank You