CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

User Authentication, Access Control, and Operating System

AC Types of Access Control

Video Summary

- What is Discretionary Access Control (DAC) ✓
- What is Role-based Access Control (RBAC) ✓
- What are the limitations of RBAC
- What is Attribute-based Access Control (ABAC)
- What is Mandatory Access Control (MAC)

How does RBAC work?

- Administrators assign access permissions to roles
- Then, roles can be assigned to individual users
  - Users may have one or several roles (each with different access rights)
- Administrators can simply update roles or access permissions
  - By assigning users (or removing users from) to the appropriate roles

The Limitations of RBAC

- RBAC provides static access control configurations.
- It fails to provide a flexible mechanism by which users/entities can express their requirements.

- Limitation #1: Role Explosion
  - RBAC is limited to defining access permissions by role
  - An ever-increasing number of users requires an exponentially increasing number of roles to accommodate various permission combinations

The Limitations of RBAC

- Limitation #2: Toxic Combinations
  - Various roles assigned to a given user could contain conflicting data.
    - One user may have a role allowing him to create a purchase order, and another allowing him to approve it.

The Limitations of RBAC

- Limitation #3: Management Nightmares
  - Between growing numbers of users, and exponentially more roles
  - Administrators have to constantly be on top of changes to users and to roles, and ensure that role assignment combinations are current, accurate, and not conflicting with other roles a user might be assigned.

The Limitations of RBAC

- Limitation #4: Lack of Context
  - Due to the static nature of Role Based Access Control, RBAC is unable to model policies that depend on contextual details:
    - Time-of-day, location, relationship between users, etc.

  - RBAC has no way of determining the relationships between users and using that information to make policy decisions.

  - At its best, RBAC was originally designed to answer just one question:

What access does a user have based on their assigned role(s)?

The Limitations of RBAC

- Today, defining authorization policies based on a user’s role is not good enough.
- The context surrounding that user, their data, and the interaction between the two are also important to provide access to
  - the right user,
  - at the right time,
  - in the right location,
  - and by meeting regulatory compliance.
- That means evolving an existing Role Based Access Control model to an Attribute Based Access Control (ABAC) model

Evolving RBAC with ABAC

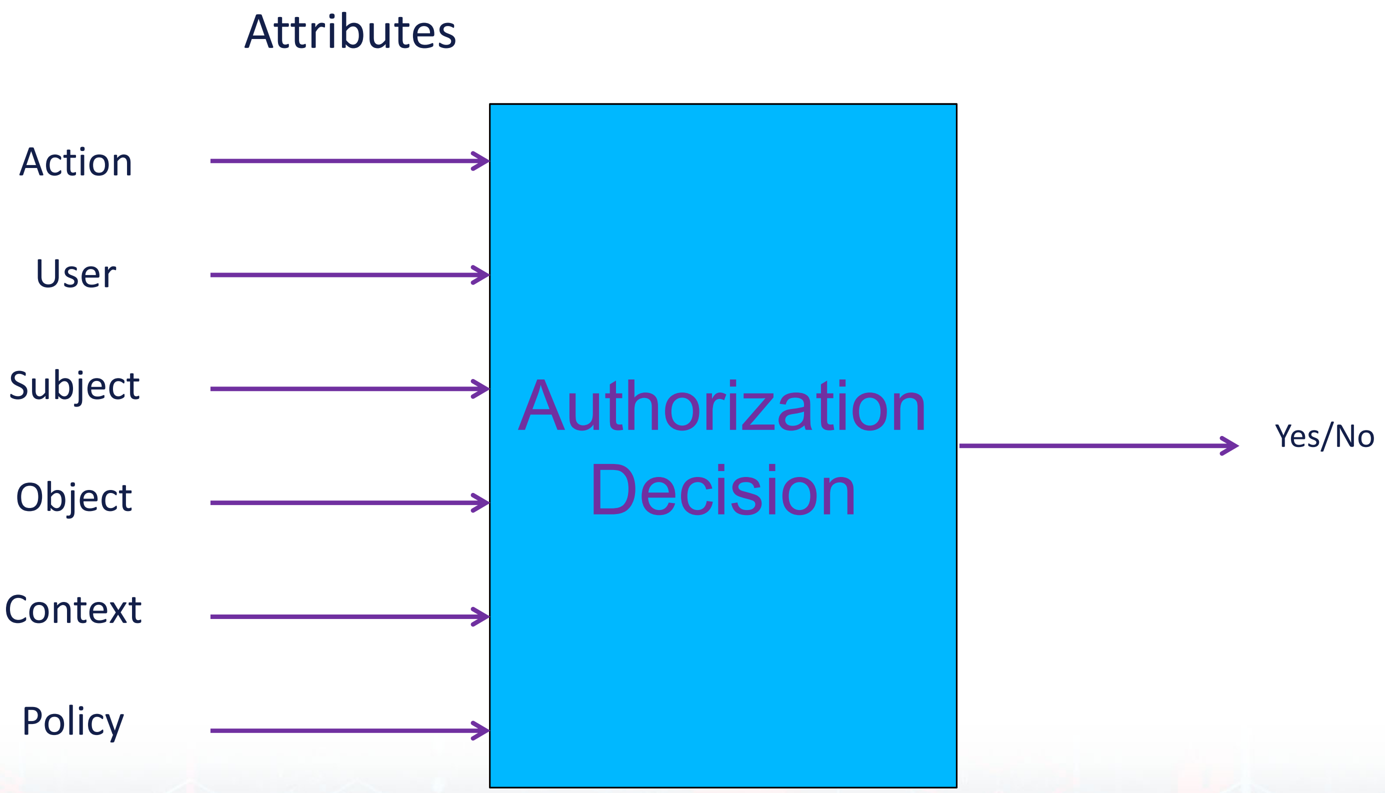
- Attribute Based Access Control allows an enterprise to extend existing roles using attributes and policies.
- By adding context, authorization decisions can be made based on:
  - Role of the user
  - Who or what that user is related to
  - What that user needs access to
  - Where that user needs access from
  - When that user needs access
  - How that user is accessing that information
- For example, a policy may be written as follows:
  - "Doctors can view medical records of any patient in their department and update any patient record that is directly assigned to them, during working hours and from an approved device."

Attribute based access control

- Similar to RBAC in the sense that it also adopts a policy driven approach.
- Uses attributes of subjects, objects, and the environment (instead of roles).

More suitable in adapting to dynamic access requirements in e-Health

Attribute based access control



Attributes

Action

User

Subject

Object

Context

Policy

Authorization Decision

Yes/No

Mandatory Access Control (MAC)

- Based on multilevel security (MLS)

  top secret > secret > confidential > restricted > unclassified

- Subject has security clearance of a given level
- Object has security classification of a given level

Mandatory Access Control (MAC)

- Based on multilevel security (MLS)

  top secret > secret > confidential > restricted > unclassified

- Subject has security clearance of a given level
- Object has security classification of a given level
- Two required properties for confidentiality:

  No read up Subject can only read an object of less or equal security level

  No write down Subject can only write into object of greater or equal security level

- Clearance and classification is determine by administrator; users cannot override security policy

Video Summary

- What is Discretionary Access Control (DAC) ✓
- What is Role-based Access Control (RBAC) ✓
- What are the limitations of RBAC ✓
- What is Attribute-based Access Control (ABAC) ✓
- What is Mandatory Access Control (MAC) ✓