Role-Based Access Control (RBAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 3-1

ravi.utsa@gmail.com
www.profsandhu.com
Access Control

Fixed policy

Ownership gives discretion
Discretionary Access Control (DAC), 1970

One-directional information flow
Mandatory Access Control (MAC), 1970

Policy neutral
Role Based Access Control (RBAC), 1995

Flexible policy

Attribute Based Access Control (ABAC), ????
The RBAC Story

RBAC: Role-Based Access Control

- Access is determined by roles
- A user’s roles are assigned by security administrators
- A role’s permissions are assigned by security administrators

Is RBAC MAC or DAC or neither?

- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

RBAC is neither MAC nor DAC!
RBAC96 Model
ROLE HIERARCHIES

USER-ROLE ASSIGNMENT

SESSIONS

PERMISSIONS-ROLE ASSIGNMENT

CONSTRAINTS

USERS

ROLES

PERMISSIONS
RBAC96 Model Family

RBAC3
ROLE HIERARCHIES + CONSTRAINTS

RBAC1
ROLE HIERARCHIES

RBAC2
CONSTRAINTS

RBAC0
BASIC RBAC
Abstraction of Privileges
- Credit is different from Debit even though both require read and write

Separation of Administrative Functions
- Separation of user-role assignment from role-permission assignment

Least Privilege
- Right-size the roles
- Don’t activate all roles all the time
- Limit roles of a user
- Limit users in a role

Separation of Duty
- Static separation: purchasing manager versus accounts payable manager
- Dynamic separation: cash-register clerk versus cash-register manager
A role brings together
- a collection of users and
- a collection of permissions

These collections will vary over time
- A role has significance and meaning beyond the particular users and permissions brought together at any moment
Groups are often defined as
- a collection of users

A role is
- a collection of users and
- a collection of permissions

Some authors define role as
- a collection of permissions

Most Operating Systems support groups
- BUT do not support selective activation of groups

Selective activation conflicts with negative groups (or roles)
HIERARCHICAL ROLES

Primary-Care Physician

Physician

Specialist Physician

Health-Care Provider
EXAMPLE ROLE HIERARCHY

Director (DIR)

Project Lead 1 (PL1)
  Production 1 (P1)
  Quality 1 (Q1)
  Engineer 1 (E1)

Project Lead 2 (PL2)
  Production 2 (P2)
  Quality 2 (Q2)
  Engineer 2 (E2)

Engineering Department (ED)

Employee (E)

PROJECT 1  PROJECT 2
EXAMPLE ROLE HIERARCHY

- Project Lead 1 (PL1)
  - Production 1 (P1)
  - Quality 1 (Q1)
  - Engineer 1 (E1)

- Project Lead 2 (PL2)
  - Production 2 (P2)
  - Quality 2 (Q2)
  - Engineer 2 (E2)

- Engineering Department (ED)

- Employee (E)

PROJECT 1

PROJECT 2
EXAMPLE ROLE HIERARCHY

Director (DIR)

Project Lead 1 (PL1)
- Production 1 (P1)
- Quality 1 (Q1)
- Engineer 1 (E1)

Project Lead 2 (PL2)
- Production 2 (P2)
- Quality 2 (Q2)
- Engineer 2 (E2)

PROJECT 1

PROJECT 2
EXAMPLE ROLE HIERARCHY

PROJECT 1

Project Lead 1 (PL1)

Production 1 (P1)

Quality 1 (Q1)

Engineer 1 (E1)

PROJECT 2

Project Lead 2 (PL2)

Production 2 (P2)

Quality 2 (Q2)

Engineer 2 (E2)
CONSTRANTS

- Mutually Exclusive Roles
  - Static Exclusion: The same individual can never hold both roles
  - Dynamic Exclusion: The same individual can never hold both roles in the same context

- Mutually Exclusive Permissions
  - Static Exclusion: The same role should never be assigned both permissions
  - Dynamic Exclusion: The same role can never hold both permissions in the same context

- Cardinality Constraints on User-Role Assignment
  - At most k users can belong to the role
  - At least k users must belong to the role
  - Exactly k users must belong to the role

- Cardinality Constraints on Permissions-Role Assignment
  - At most k roles can get the permission
  - At least k roles must get the permission
  - Exactly k roles must get the permission
NIST RBAC Model
NIST MODEL: CORE RBAC

USER ASSIGNMENT

(UA) User Assignment

ROLE ASSIGNMENT

(PA) Permission Assignment

SESSIONS

user_sessions

SESSIONRoles

session_roles

OPS

OBS

PRMS
NIST MODEL: HIERARCHICAL RBAC

(RH) Role Hierarchy

(UA) User Assignment

(PA) Permission Assignment

© Ravi Sandhu
World-Leading Research with Real-World Impact!
SSD IN HIERARCHICAL RBAC

- **SSD**
- **Role Hierarchy (RH)**
- **User Assignment (UA)**
- **Permission Assignment (PA)**
- **Users (USERS)**
- **Roles (ROLES)**
- **Sessions (SESSIONS)**
- **OPS**
- **OBS**
- **PRMS**

**Keywords**: user_sessions, session_roles

© Ravi Sandhu

World-Leading Research with Real-World Impact!
DSD IN HIERARCHICAL RBAC

- USERS
- ROLES
- SESSIONS
- DSD
- OPS
- OBS
- PRMS

(UA) User Assignment
(PA) Permission Assignment

session_roles

user_sessions
Compare RBAC96 Model Family

RBAC3
ROLE HIERARCHIES +
CONSTRAINTS

RBAC1
ROLE
HIERARCHIES

RBAC2
CONSTRAINTS

RBAC0
BASIC RBAC
RBAC Administration
RBAC96 Model Family

ROLE HIERARCHIES

USER-ROLE ASSIGNMENT

PERMISSIONS-ROLE ASSIGNMENT

USERS

ROLES

PERMISSIONS

SESSIONS

CONSTRAINTS