Role-Based Access Control (RBAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

January 29, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com
Access Control

Discretionary Access Control (DAC), 1970

Role Based Access Control (RBAC), 1995

Mandatory Access Control (MAC), 1970

Attribute Based Access Control (ABAC), ????

Fixed policy

Flexible policy
The RBAC Story

World-Leading Research with Real-World Impact!
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

First emerged: mid 1970s
First models: mid 1990s

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 Family

ROLE HIERARCHIES

USER-ROLE ASSIGNMENT

PERMISSIONS-ROLE ASSIGNMENT

USERS

ROLES

PERMISSIONS

SESSIONS

CONSTRAINTS

© Ravi Sandhu

World-Leading Research with Real-World Impact!
RBAC96 Model Family

RBAC0
BASIC RBAC

RBAC1
ROLE HIERARCHIES

RBAC2
CONSTRAINTS

RBAC3
ROLE HIERARCHIES +
CONSTRAINTS
- 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

- 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
Supervising Engineer

Hardware Engineer

Software Engineer

Engineer
EXAMPLE ROLE HIERARCHY

Director (DIR)

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

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

Engineering Department (ED)
  - Employee (E)

PROJECT 1

PROJECT 2
EXAMPLE ROLE HIERARCHY

Director (DIR)

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

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

PROJECT 1

PROJECT 2
EXAMPLE ROLE HIERARCHY

Project Lead 1
(PL1)

Production 1
(P1)

Engineer 1
(E1)

Quality 1
(Q1)

Project Lead 2
(PL2)

Production 2
(P2)

Engineer 2
(E2)

Quality 2
(Q2)

PROJECT 1

PROJECT 2
CONTRAINTS

- 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 MODEL: CORE RBAC

USER ASSIGNMENT (UA)

PERMISSION ASSIGNMENT (PA)

SESSIONS

OPERATIONS (OPS)

OBSERVATIONS (OBS)

PRMS

user_sessions

session_roles
NIST MODEL: HIERARCHICAL RBAC

(Role Hierarchy)

 USERS

 ROLEs

 USER Assignment

 (RH)

 SESSIONs

 session_roles

 PRMS

 OPS

 OBS

 (UA)

 (PA)

 Permission Assignment
SSD IN HIERARCHICAL RBAC

SSD

(RH)
Role Hierarchy

(UA)
User Assignment

(PA)
Permission Assignment

USERS

ROLES

SESSIONS

OPS

OBS

PRMS

user_sessions

session_roles
DSD in Hierarchical RBAC

- USER ASSIGNMENT
- ROLE ASSIGNMENT
- SESSION ROLES
- USER SESSIONS
- DSD
- OPS
- OBS
- PRMS

(UA) User Assignment
(PA) Permission Assignment

World-Leading Research with Real-World Impact!
NIST MODEL FAMILY

Select Core RBAC
Option: Advanced Review

Core RBAC

Choose a or b
Option: Advanced Review

Hier. RBAC
a. Limited
b. General

Adhere to dependency

SSD Relations
a. w/hierarchies
b. wo/hierarchies

DSD Relations

Requirements
Package
OM-AM

What?

- Objectives
- Model
- Architecture
- Mechanism

How?

Assurance
PEI Models

- Security and system goals (objectives/policy)
  - Necessarily Informal
- Policy models
  - Formal/quasi-formal
- Enforcement models
  - System block diagrams, Protocol flows
- Implementation models
  - Pseudo-code
- Trusted Computing Technology (mechanisms/implementation)
  - Actual Code

Idealized
Enforceable (Approximate)
Codeable
RBAC: SERVER PULL

E model

Client -> Server

User-role
Authorization
Server
RBAC: CLIENT PULL

E model

Client

Server

User-role Authorization Server
RBAC: PROXY-BASED

Client → Proxy Server → Server

User-role Authorization Server
Discuss highlights of reference papers