CS 556 – Computer Security
Fall 2012

Dr. Indrajit Ray
Email: indrajit@cs.colostate.edu

Department of Computer Science
Colorado State University
Fort Collins, CO 80523, USA
Role Based Access Control

- RBAC Model Overview
- RBAC Family of Models
- Extensions to RBAC
What?? – Another Access Control Model?

- Owner-based discretionary access control (DAC)
  - Origins: academia
- Mandatory access control (MAC)
  - Origins: military
- There is more to access control than DAC / MAC
  - Role based access control (RBAC)
  - Origins: business
Owner Based DAC

- Owner has all-or-nothing power
  - Superuser fallacy
- Spaghetti of intent
- Negative permissions make for messier spaghetti
- Trojan horses can subvert intent
Military Style MAC

- Enforce one-directional information flow in a lattice of security labels
- Rigid and simple-minded
- Can be used for
  - Confidentiality
  - Integrity
  - Aggregation (Chinese Wall)
Role Based Access Control (RBAC)

- A user’s permissions are determined by the user’s roles rather than
  - user’s identity (DAC)
  - user’s clearance (MAC)

- Facilitates
  - administration of permissions
  - articulation of policy
RBAC

- Policy neutral
- Policy oriented
  ✦ least privilege
  ✦ separation of duties
  ✦ encapsulation of primitive permissions
  ✦ separation of administration and access
- Roles are a semantic construct around which to build policy
RBAC is a framework to help in articulating policy.
The main point of RBAC is to facilitate security management.
RBAC MODEL OVERVIEW
RBAC96 Family

RBAC0
Vanilla RBAC

RBAC1
Role Hierarchies

RBAC2
Constraints

RBAC3
Role Hierarchies + Constraints
RBAC0

Role Based Access Control

RBAC Model Overview

RBAC Family of Models

Extensions to RBAC

User–Role Assignment

Permission–Role Assignment

SESSIONS
Permissions

- Primitive permissions
  - read, write, append, execute
- Abstract permissions
  - credit, debit, inquiry
- System permissions
  - auditorObject permissions
Permissions

- Permissions are positive
- No negative permissions or denials
  - handled by constraints in RBAC2
- No duties or obligations
  - outside scope of access control
Roles as Policy

- 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
Roles versus Groups

- 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
Users

- Users are
  - human beings or
  - other active agents
- Each individual should be known as exactly one user
User-Role Assignment

- A user can be a member of many roles
- Each role can have many users as members
Sessions

- A user can invoke multiple sessions
- In each session a user can invoke any subset of roles that the user is a member of
Permission-Role Assignment

- A permission can be assigned to many roles
- Each role can have many permissions
Management of RBAC

- Option 1:
  - USER-ROLE Assignment and PERMISSION-ROLE Assignment can be changed only by the chief security officer.

- Option 2:
  - Use RBAC to manage RBAC.
RBAC FAMILY OF MODELS
Role Based Access Control (RBAC)

**Overview**

- RBAC Model Overview
- RBAC Family of Models
- Extensions to RBAC

Diagram:

- **Users** connected to **Roles**
- **Roles** connected to **Permissions**
- **Roles** connected to **Sessions**

- **Role Hierarchies**
- **User-Role Assignment**
- **Permission-Role Assignment**
Hierarchical Roles

- Primary-Care Physician
- Specialist Physician
- Physician
- Health-Care Provider
Private Roles

Role Based Access Control
RBAC Model Overview
RBAC Family of Models
Extensions to RBAC

Supervising Engineer

Specialized HW Engineer

Hardware Engineer

Engineer

Software Engineer

Specialized SW Engineer
User–Role Assignment

Permission–Role Assignment

SESSIONS

CONSTRAINTS
**Constraints**

- **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
**Constraints**

- 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
Constraints

- 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
RBAC3

Role Based Access Control
RBAC Model Overview
RBAC Family of Models
Extensions to RBAC

Role Hierarchies
User–Role Assignment
Permission–Role Assignment

USERS
ROLES
PERMISSIONS
SESSIONS

Dr. Indrajit Ray, Computer Science Department
CS 556 - Computer Security - © 2012 Colorado State University – 30 / 32
EXTENSIONS TO RBAC
RBAC Limitations and Possible Extension

- No support for delegation
  - Faculty delegates to student the role of instructor
  - RBAC with delegation
- No support for access control based on contextual information
  - User can activate a role only if the user is at a certain location at certain time
  - Spatio-temporal RBAC
- Cannot provide authorization in open systems
  - User moves from one Internet site to another
  - Trust-based access control
- No support for usage control and obligation policies
  - User is obligated to not make copies of protected DVDs
  - Usage control models; RBAC with obligation policies