

Computer Security: Principles and Practice

Chapter 4 - Access Control

First Edition

by William Stallings and Lawrie Brown

Lecture slides by Lawrie Brown

Access Control

- “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner”
- central element of computer security
- assume have users and groups
 - authenticate to system
 - assigned access rights to certain resources on system



Access Control: Another definition

- Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system
- It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system

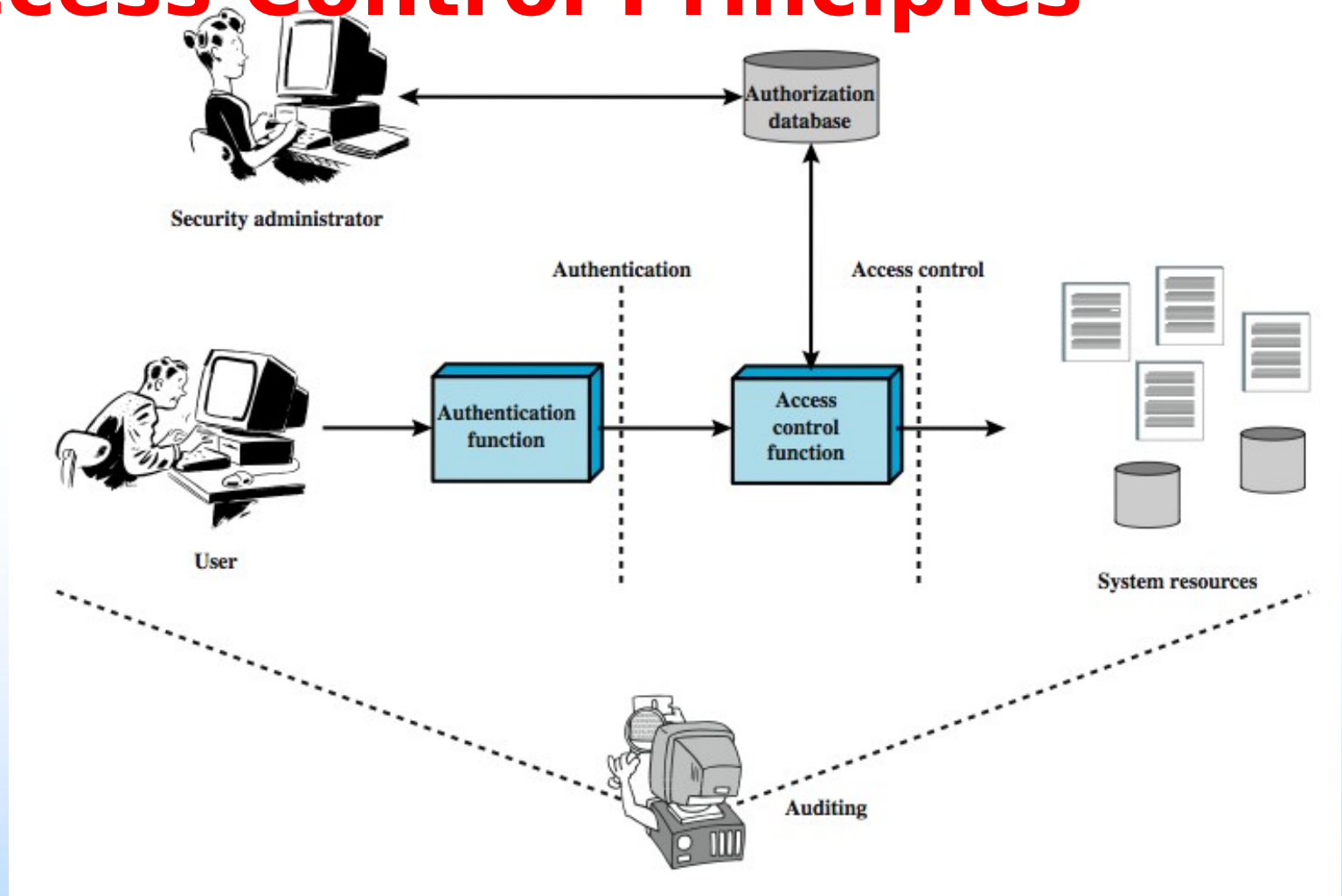


Access Control Components

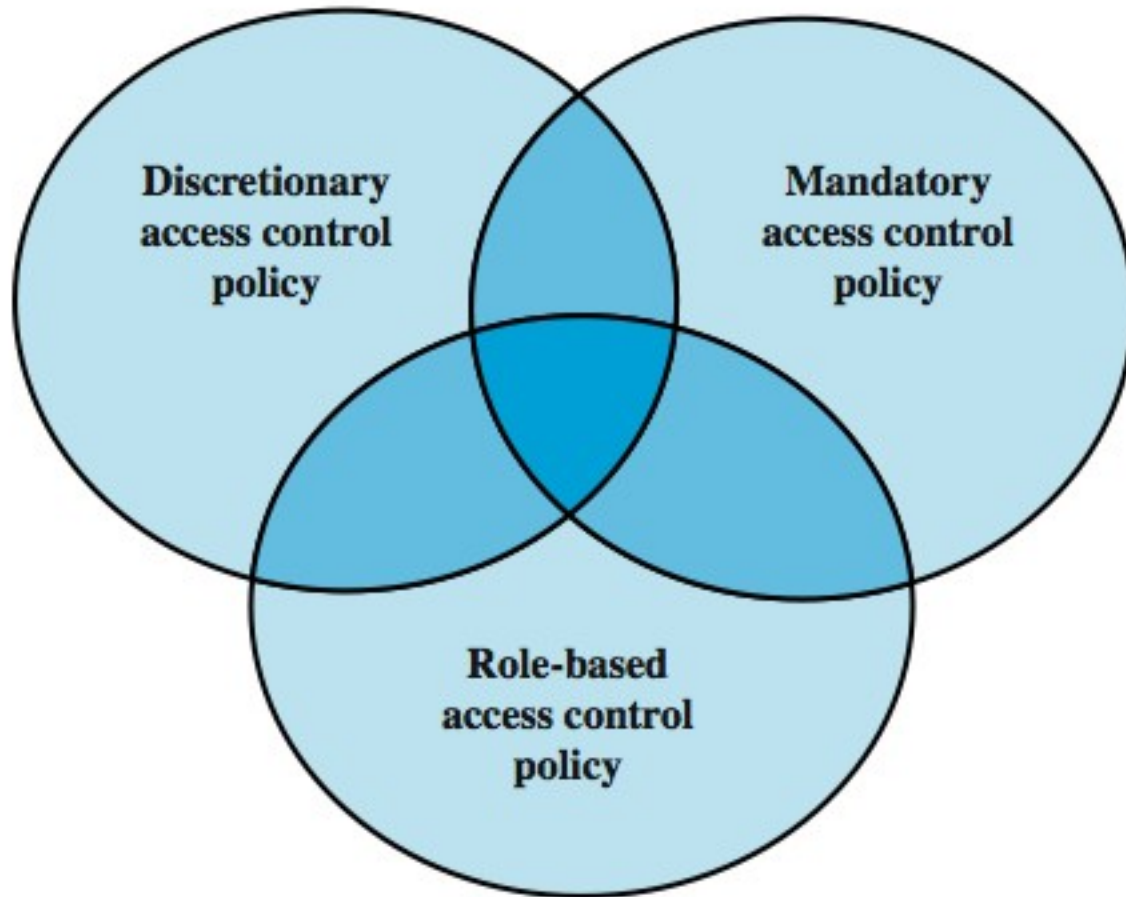
- **Access Controls:** The security features that control how users and systems communicate and interact with one another
- **Access:** The flow of information between subject and object
- **Subject:** An active entity that requests access to an object or the data in an object
- **Object:** A passive entity that contains information



Access Control Principles



Access Control Policies



Access Control Requirements

- reliable input: a mechanism to authenticate
- fine and coarse specifications: regulate access at varying levels (e.g., an attribute or entire DB)
- least privilege: min authorization to do its work
- separation of duty: divide steps among different individuals
- open and closed policies: accesses specifically authorized or all accesses except those prohibited
- administrative policies: who can add, delete, modify rules



Access Control Elements

- subject - entity that can access objects
 - a process representing user/application
 - often have 3 classes: owner, group, world
- object - access controlled resource
 - e.g. files, directories, records, programs etc
 - number/type depend on environment
- access right - way in which subject accesses an object
 - e.g. read, write, execute, delete, create, search



Discretionary Access Control

- A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources
- Access control is at the discretion of the owner



Mandatory Access Control

- Access control is based on a security labeling system
 - Users have security clearances and resources have security labels that contain data classifications
- Used in environments where information classification and confidentiality is very important (e.g., the military)



Role-Based Access Control

- Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact
- Best system for an organization that has high turnover



Access Control Implementation

- Access controls can be implemented at various layers of an organization, network, and individual systems
- Three broad categories:
 - Administrative (e.g., separation of duties, rotation of duties)
 - Physical (e.g., network segregation, physical access)
 - Technical (aka logical, e.g., auditing, network access)



DAC Matrix

- often provided using an access matrix
 - lists subjects in one dimension (rows)
 - lists objects in the other dimension (columns)
 - each entry specifies access rights of the specified subject to that object
- access matrix is often sparse
- can decompose by either row or column



Access Control Structures

- See page 117



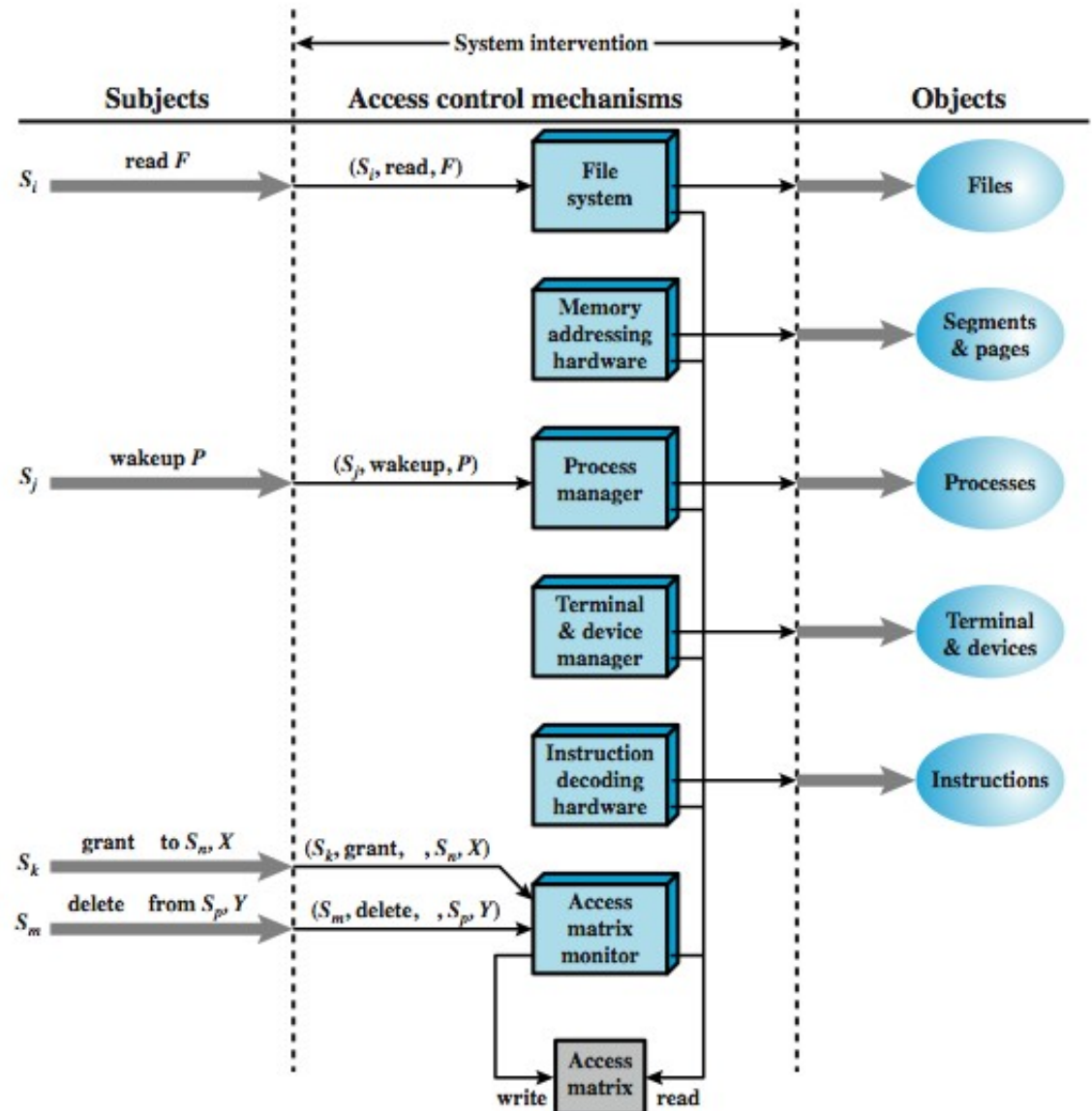
Access Control Model

		OBJECTS								
		subjects			files		processes		disk drives	
		S ₁	S ₂	S ₃	F ₁	F ₁	P ₁	P ₂	D ₁	D ₂
SUBJECTS	S ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S ₂		control		write *	execute			owner	seek *
	S ₃			control		write	stop			

* - copy flag set

A separate access control module is associated with each object type

Access Control Function



Protection Domains: More Useful

- access control matrix: associates a set of capabilities with a user (user protection domain)
- protection domains: set of objects with associated access rights to those objects
- in access matrix view each row defines a protection domain
 - but not necessarily just a user
 - may be a limited subset of user's rights
 - applied to a more restricted process

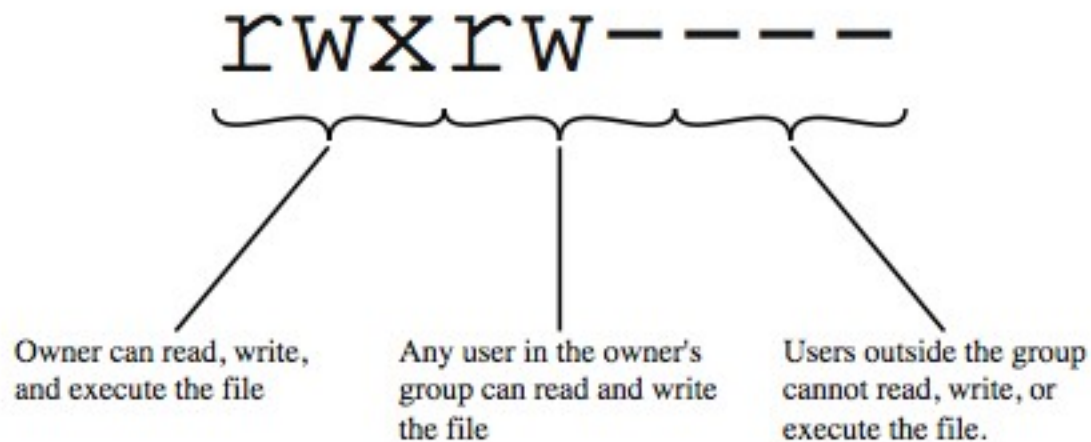


UNIX File Concepts

- UNIX files administered using inodes
 - control structure with key info on file
 - attributes, permissions of a single file
 - may have several names for same inode
 - have inode table / list for all files on a disk
 - copied to memory when disk mounted
- directories form a hierarchical tree
 - may contain files or other directories
 - are a file of names and inode numbers



UNIX File Access Control



UNIX File Access Control

- “set user ID”(SetUID) or “set group ID”(SetGID)
 - system temporarily uses rights of the file owner / group in addition to the real user’s rights when making access control decisions
 - enables privileged programs to access files / resources not generally accessible
- sticky bit
 - on directory limits rename/move/delete to owner
- superuser
 - is exempt from usual access control restrictions



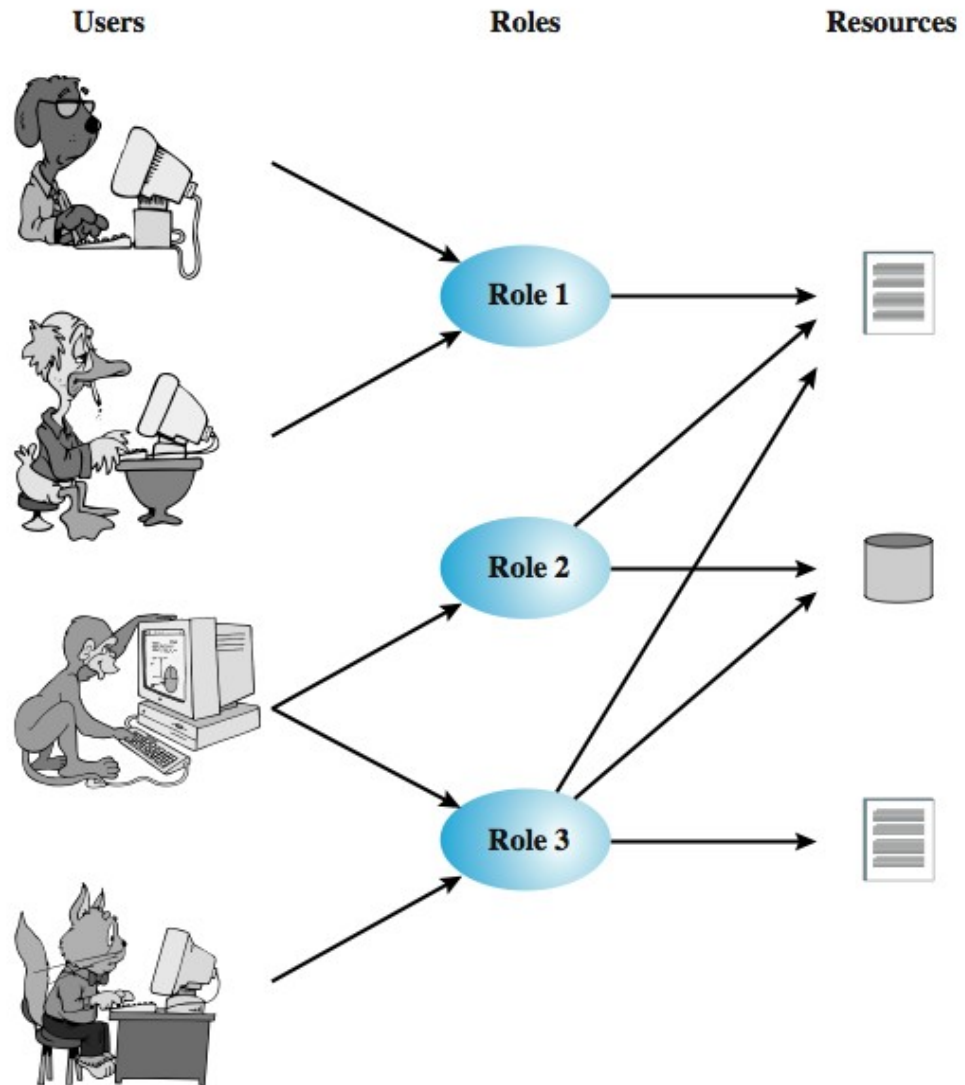
UNIX Access Control Lists

- modern UNIX systems support ACLs
- can specify any number of additional users / groups and associated rwx permissions
- group perms also set max ACL perms
- when access is required
 - select most appropriate ACL
 - owner, named users, owning / named groups, others
 - check if have sufficient permissions for access



Role-Based Access Control

Access based on 'role', not identity



Role-Based Access Control

	R ₁	R ₂	...	R _n
U ₁	×			
U ₂	×			
U ₃		×		×
U ₄				×
U ₅				×
U ₆				×
...				
U _m	×			

		OBJECTS								
		R ₁	R ₂	R _n	F ₁	F ₁	P ₁	P ₂	D ₁	D ₂
ROLES	R ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R ₂		control		write *	execute			owner	seek *
	•									
	•									
	R _n			control		write	stop			

General RBAC, Variations

- A family of RBAC with four models
 1. RBAC0: minimum functionality
 2. RBAC1: RBAC0 plus role (permission) inheritance
 3. RBAC2: RBAC0 plus constraints (restrictions)
 4. RBAC3: RBAC0 plus all of the above
- RBAC0 entities
 - User: an individual (with UID) with access to system
 - Role: a named job function (tells authority level)
 - Permission: equivalent to access right
 - Session: a mapping between a user and set of roles



Role Hierarchy

- role hierarchy: reflect hierarchical structure of roles in an organization
 - job function with higher responsibility → greater authority
 - project manager, team leader, sr programmer
 - more complex lattices
 - roles can inherit access rights from multiple subordinate roles

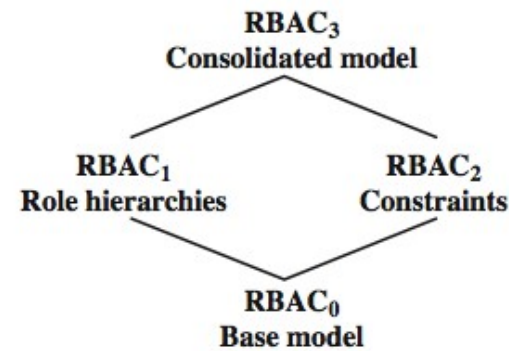


RBAC Constraints

- provides a means to adapt RBAC to the specifics of administrative policies in an organization
 - **mutually exclusive roles**: that can be assigned to only one role
 - **cardinality**: to set numbers, e.g., the maximum number of users with respect to a role
 - **prerequisite**: a user can only be assigned to a role if already assigned to some other role

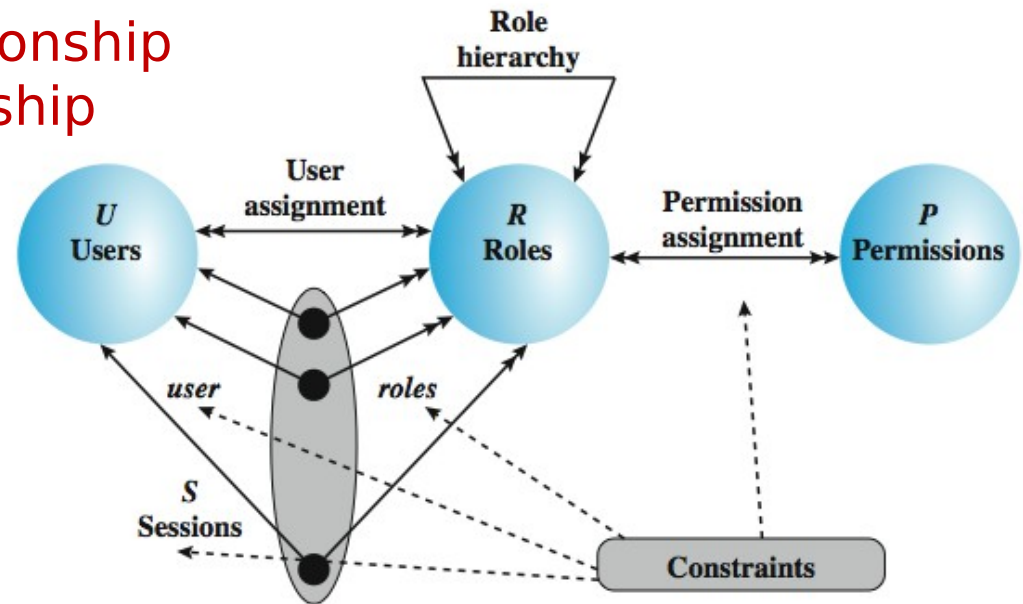


Role-Based Access Control



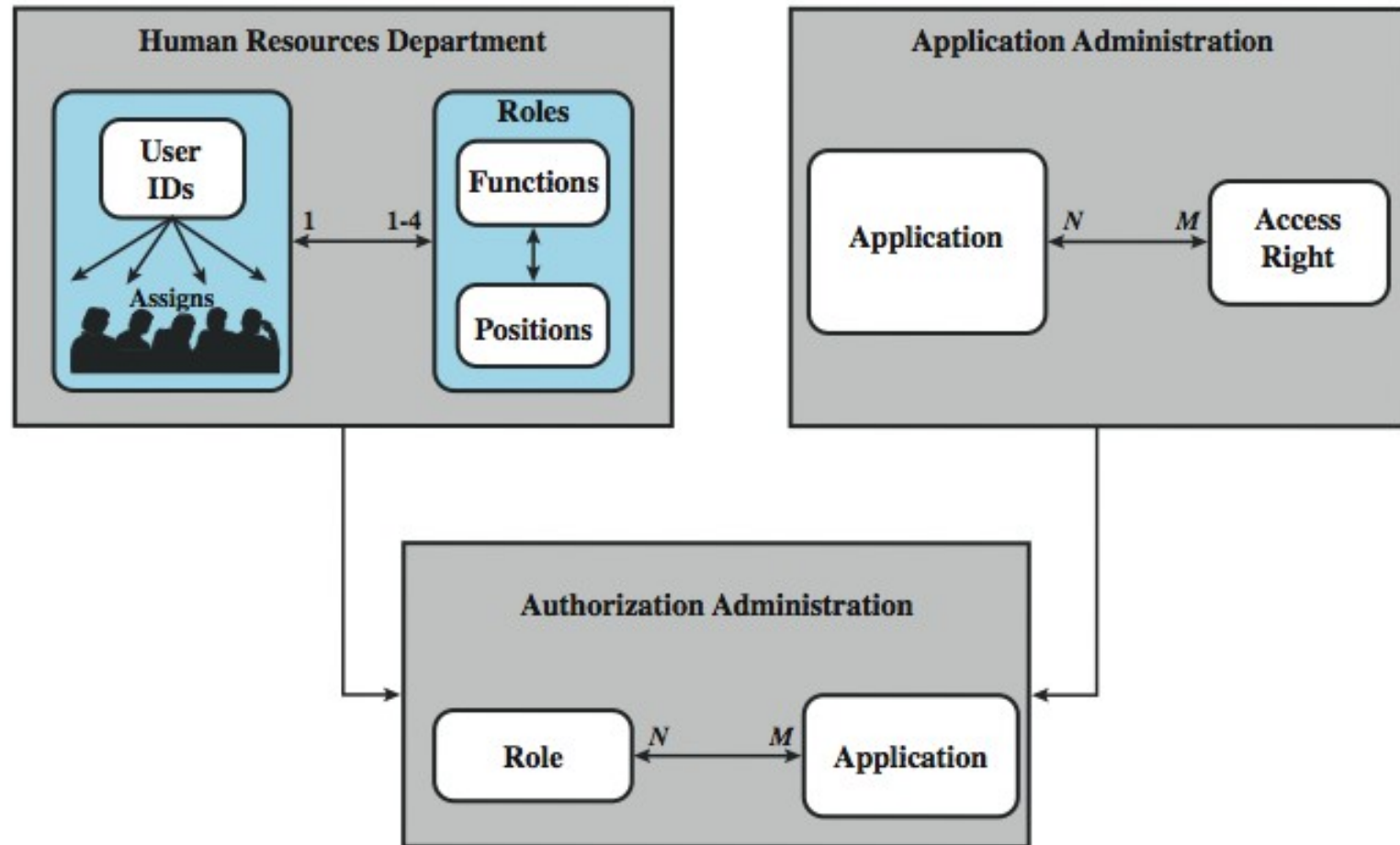
(a) Relationship among RBAC models

Double arrow: 'many' relationship
Single arrow: 'one' relationship



(b) RBAC models

RBAC For a Bank



Summary

- introduced access control principles
 - subjects, objects, access rights
- discretionary access controls
 - access matrix, access control lists (ACLs), capability tickets
 - UNIX traditional and ACL mechanisms
- role-based access control
- case study

