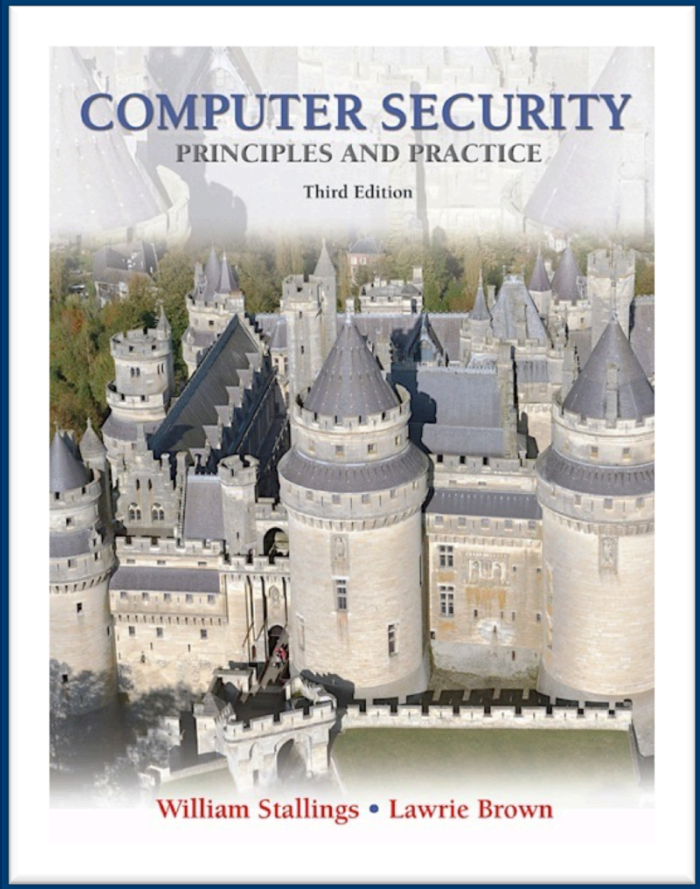
Lecture 14
Access Control



modified from slides of Lawrie Brown

Access Control

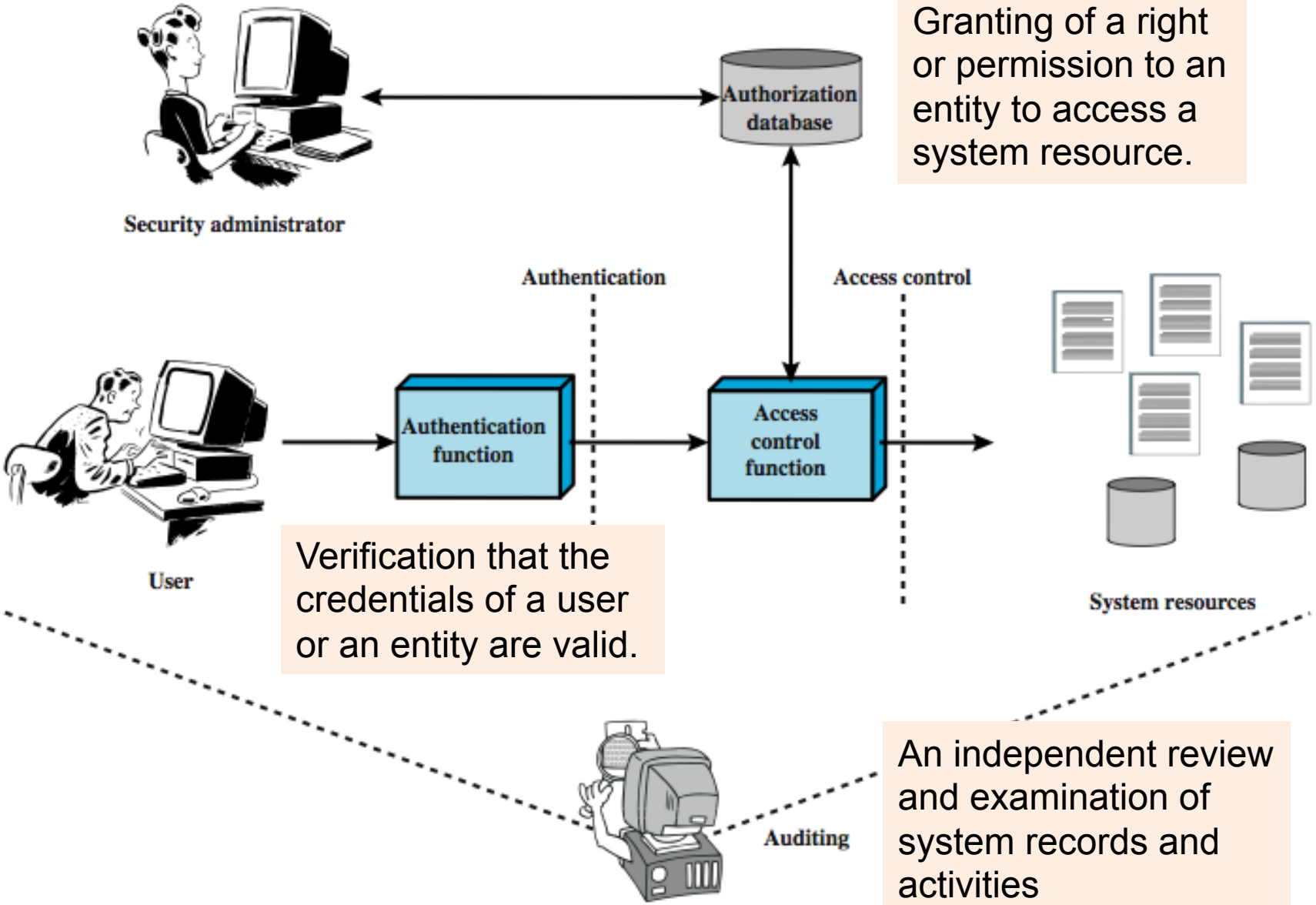
- ITU-T Recommendation X.800 definition:
  - "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner."

- RFC 2828 defines computer security as:
  - "Measures that implement and assure security services in a computer system, particularly those that assure access control service".

Access Control

- **For short**--The restriction of access to the resources
- Comparing **user authentication** and **access control**
  - prevent unauthorized users from gaining access to resources
  - prevent legitimate users from accessing resources in an unauthorized manner

Access Control Principles



Granting of a right or permission to an entity to access a system resource.

Verification that the credentials of a user or an entity are valid.

An independent review and examination of system records and activities

Access Control Policies

- Core of AC: AC policies
  - Embodied in the authorization database
- Dictates
  - what types of access are permitted,
  - under what circumstances,
  - by whom.
- Four classes
  - Discretionary access control; Mandatory access control; Role-based AC; Attribute-based AC

Access Control Basic Elements

subject entity capable of accessing objects

- Users/Applications
- often have three classes: owner, group, world

object resource to which access is controlled

- Resources
- entity used to contain and/or receive information

access right: the way in which a subject may access an object

- e.g. read, write, execute, delete, create, search

Access Control Basic Elements

- Subject: users and applications
  - Owner: creator of a resource
  - Group: a group of users who may also be granted access right
  - World: all the other user, with the minimum access right

Access Control Basic Elements

- Object: the resource to which access is controlled
  - Records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs (hardware and software)

Access Control Basic Elements

- Access right : describes the way in which a subject may access an object (how can a user operates over the resources)
  - Read: User may view information in a system resource
  - Write: User may add, modify, or delete data in system resource
  - Execute, delete, create, search

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Mandatory Access Control (MAC)

- When a system/security admin configures security rules that apply to users
- Users cannot change the rules set by admins, and are not usually considered to “own” files

Mandatory Access Control (MAC)

- MAC is well suited when an organization own the data, and wants to have control over what happens to data
  - Military, government
- Can prevent users from misconfiguring permisions

Mandatory Access Control (MAC)

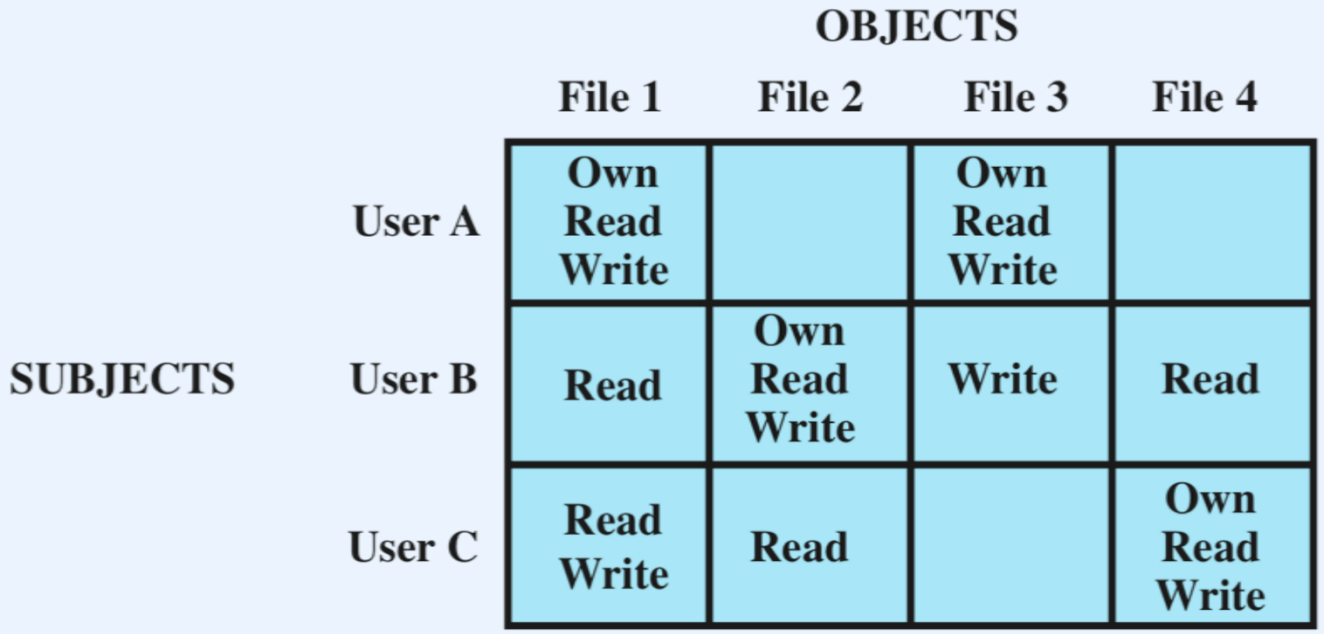
- MAC models typically work by attaching security context labels (such as clearance) to objects (files)
- A separate label (such as classification or domain) is attached to a subject (process)
- Rules define what interactions are allowed

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Discretionary Access Control

- Scheme in which an entity may enable another entity to access some resource
  - often provided using an access matrix
    - one dimension consists of identified subjects that may attempt data access to the resources
    - the other dimension lists the objects that may be accessed
  - each entry in the matrix indicates the access rights of a particular subject for a particular object

Access Matrix



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

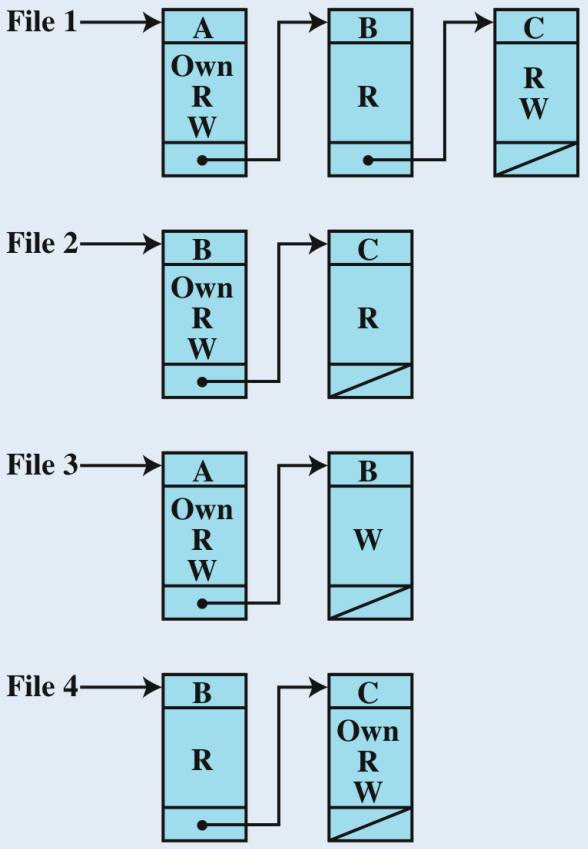
(a) Access matrix

Example of Access Control Structures

- An access matrix is usually sparse—it is implemented by decomposition in one of two ways
  - By columns: yielding access control list (ACL)
  - By rows: yielding capability tickets

Example of Access Control Structures

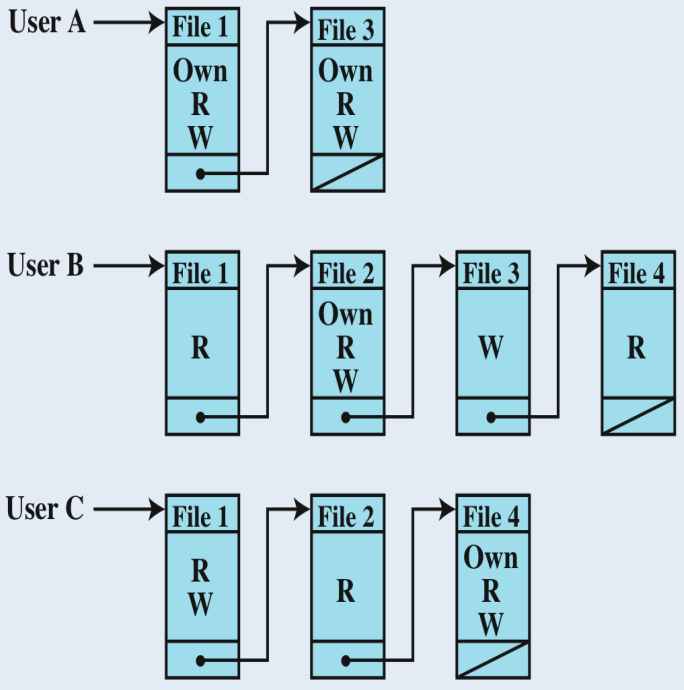
- By columns: yielding access control list (ACL)
- For each object, an ACL lists users and their permitted access rights



(b) Access control lists for files of part (a)

Example of Access Control Structures

- By rows: yielding capability tickets
- A capability ticket (A row) specifies authorized objects and operations for a particular user



(c) Capability lists for files of part (a)

- Summary for access control lists and capability tickets
  - When it is desire to determine which subjects have which access rights to particular resources, ACLs are convenient
  - When is is desire to determine the set of access rights that a given user has, capability tickets are more convenient

- They are actually different data structures for an access matrix stored in the system

Authorization Table

Another data structure for access matrix. A combination of ACLs and capability lists

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

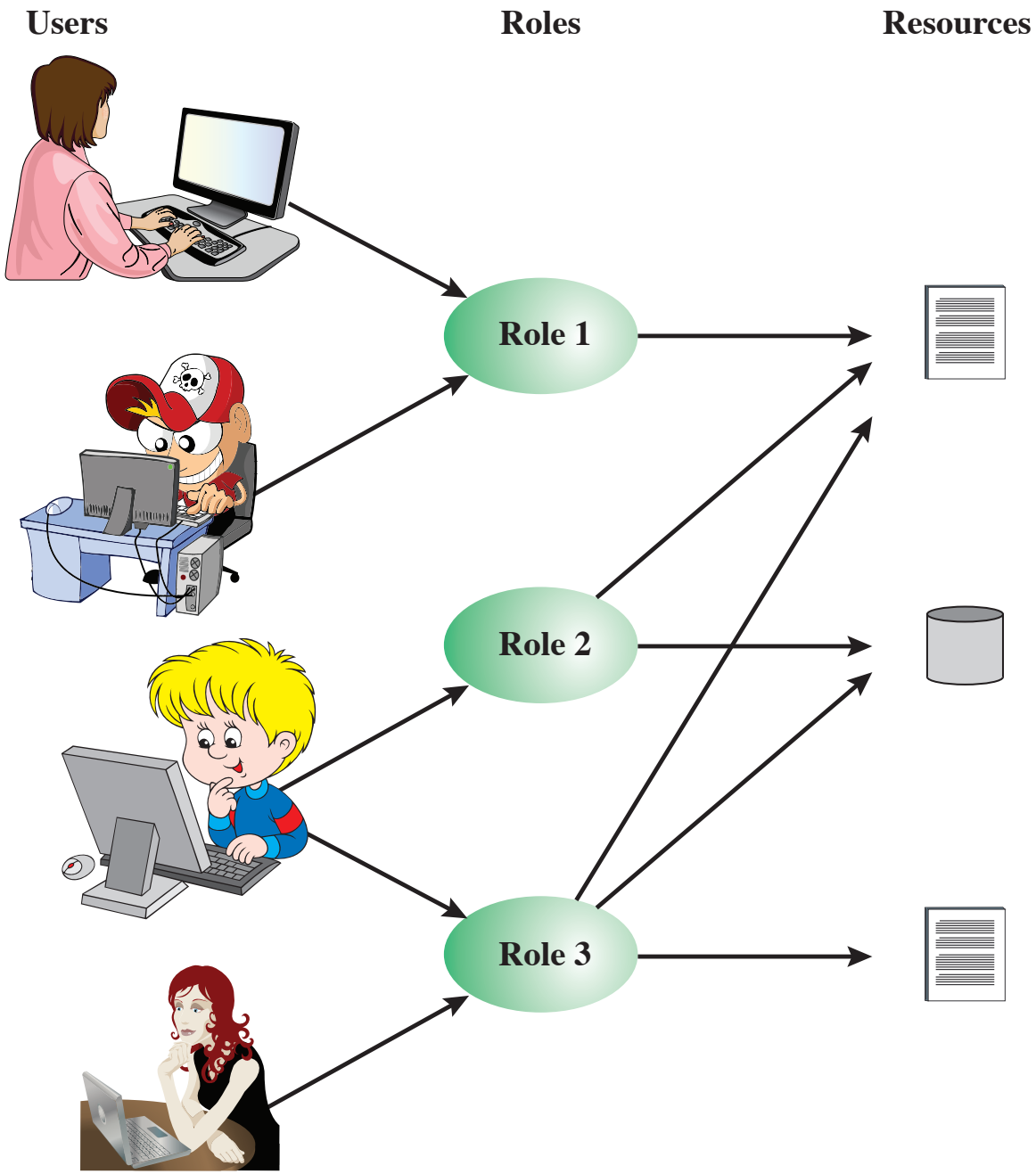
Role-Based Access Control

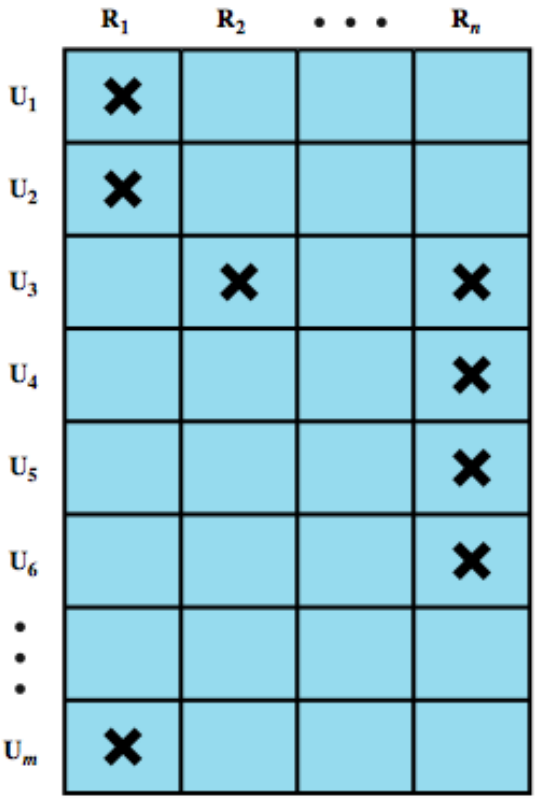
- Traditional DAC systems define the access rights of individual users
- RBAC is based on the roles that users assume in a system rather than the user's identity
  - WebCampus: faculties, students

Role-Based Access Control (RBAC)

Many to many

good aspects of RBAC?-consider a new user joins



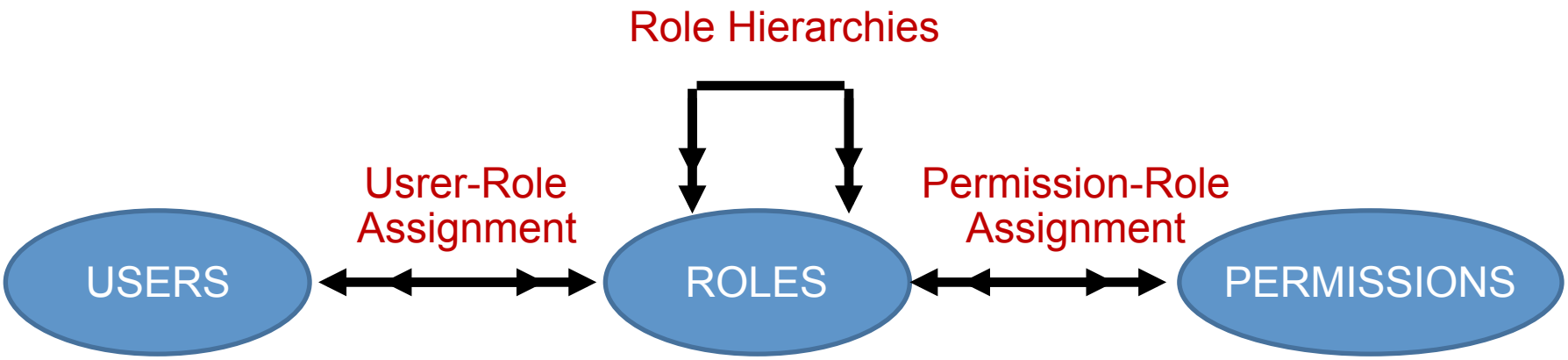


Access Control Matrix

OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
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			

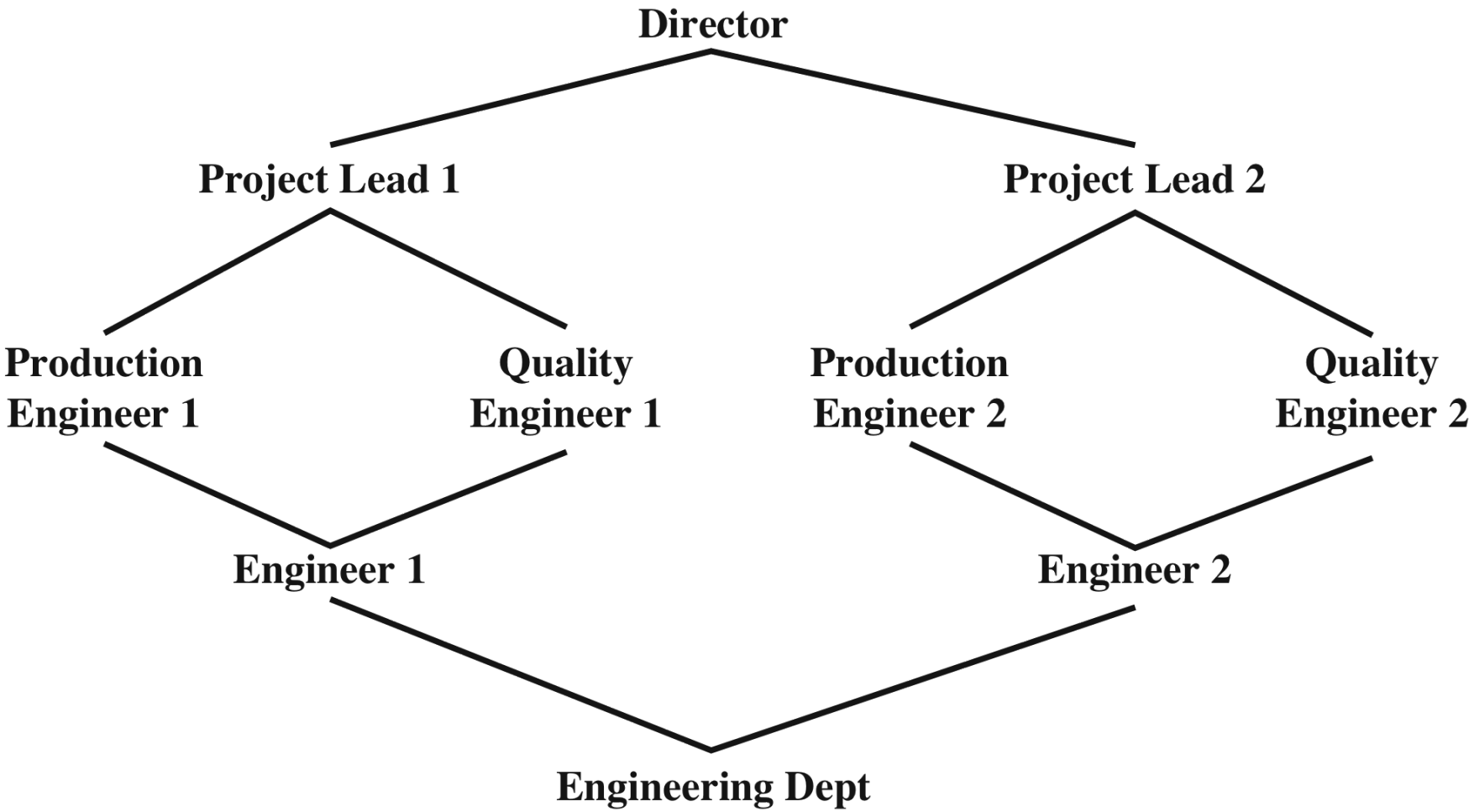
Role-Based Access Control



- Users are human beings or other active agents
- Business function the user perform is role
- A user can be a member of many roles
- Each role can have many users as members

- A permission can be assigned to many roles
- Each role can have many permissions
  - read, write, append, execute

Example of Role Hierarchy

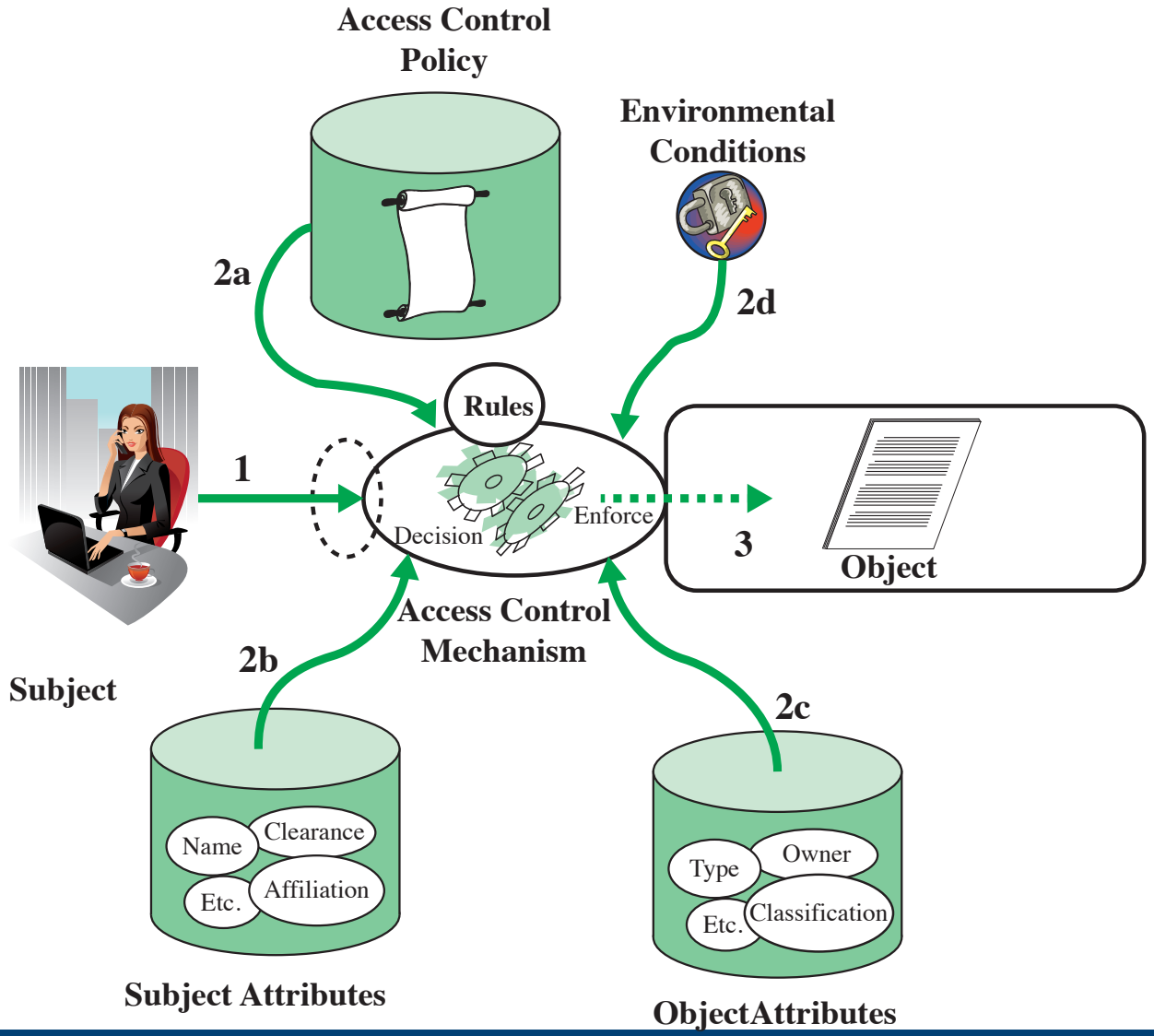


- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**

Attribute Based Access Control

- **Subject attributes**
  - Attributes define the identity and characteristics of the subject
- Object attributes
  - Objects have attributes that can be leverages to make access control decisions
- Environment attributes
  - Describe the operational, technical, and even situational environment or context in which the information access occurs

ABAC Scenario

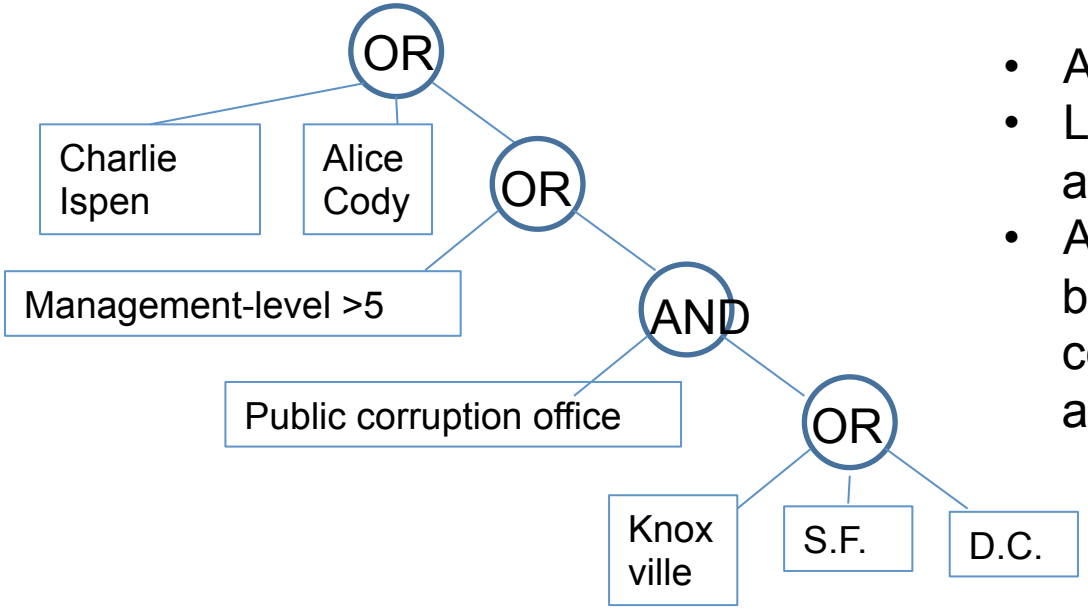


Attribute Based Access Control

- Example: the FBI public corruption offices in Knoxville, San Francisco and D.C. are investigating a corruption case. The head FBI agent may want to encrypt a sensitive memo so that only personnel that have certain credentials or **attributes** can access it.

Attribute Based Access Control

- The head agent may specify the following access structure for accessing this information: ((“Public Corruption Office” AND (“Knoxville” OR “San Francisco” OR “D.C.”)) OR (management-level > 5) OR “Name: Charlie Ipsen” OR “Name: Alice Cody”).



- Access control tree
- Leaves represent the attributes
- Any attribute sets can be expressed as the combinations of “or” and “and” relations

Summary

- **Discretionary access control**
- Mandatory access control
- **Role-based access control**
- **Attribute-based access control**