Access Control

Secure Application Development

Module 4

Konstantin Beznosov

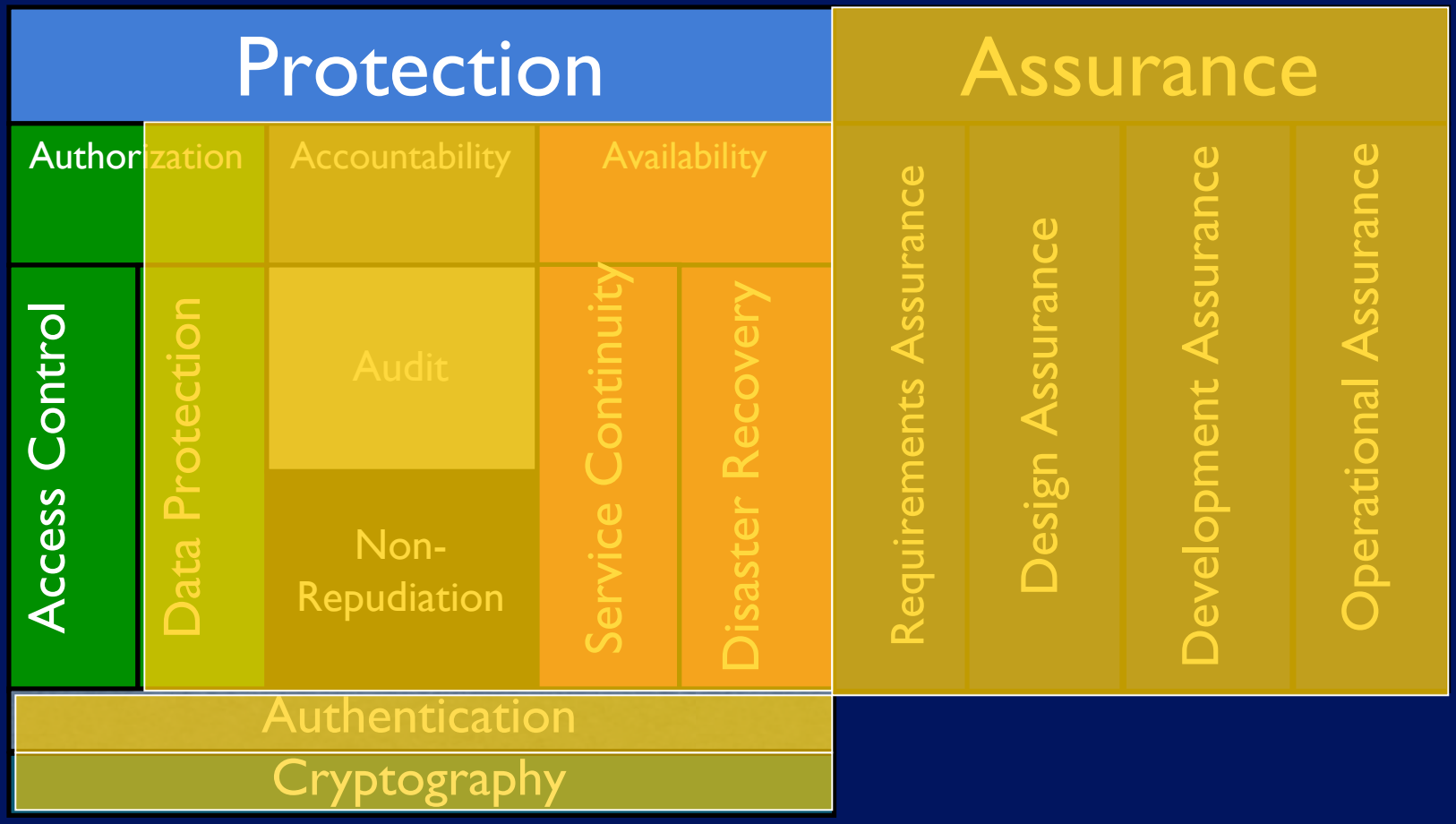
What Do You Already Know?

- What are the main elements of access control mechanisms?
- What are the three main types of security policies?
- What access control models do you know?

Outline

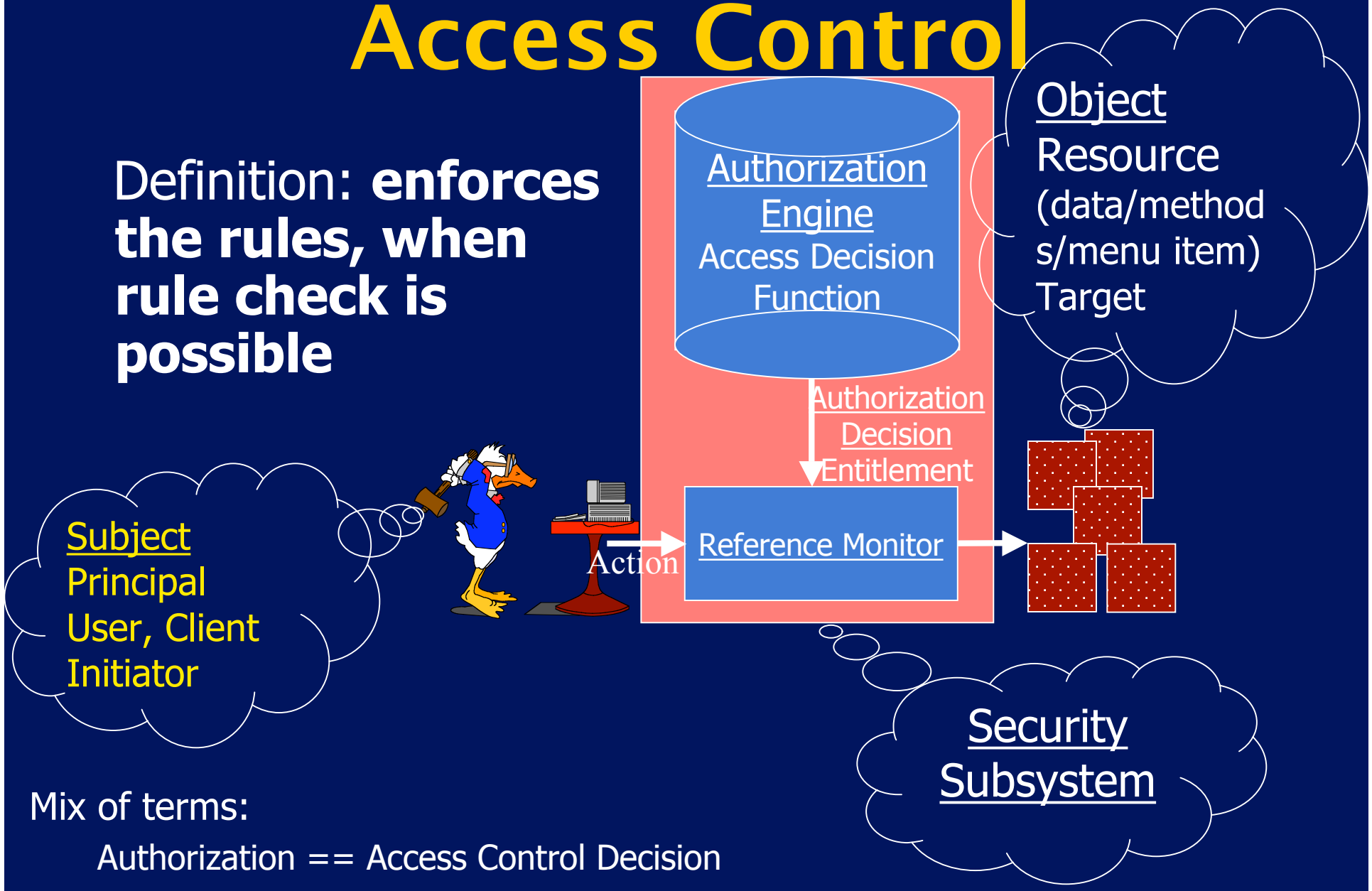
- Access control mechanisms
- Access Matrix
- Security policies
  - Confidentiality models
  - Integrity models
  - Hybrid models

Where We Are


Protection
Assurance
Authorization
Accountability
Availability
Access Control
Data Protection
Audit
Non-Repudiation
Service Continuity
Disaster Recovery
Requirements Assurance
Design Assurance
Development Assurance
Operational Assurance
Authentication
Cryptography

Authorization Mechanisms:
Access Control

Definition: **enforces the rules, when rule check is possible**



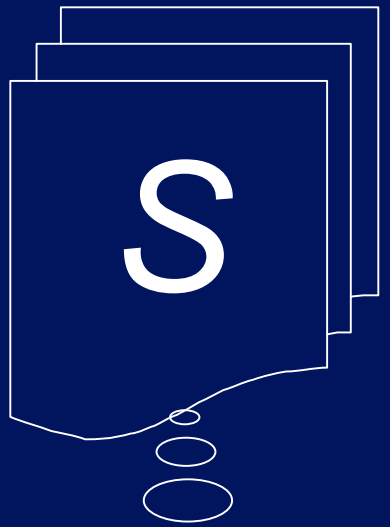
Mix of terms:

- Authorization == Access Control Decision
- Authorization Engine == Policy Engine

Access Matrix

Object System

Subjects



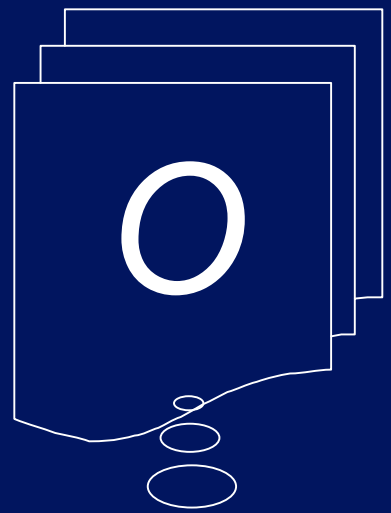
Have access to objects

Access Matrix

	Subject 1	Subject 2	Subject 3	File 1	File 2	Process 1
Subject 1	*owner control	*owner control	*call	*owner *read *write		
Subject 2			call	*read	write	wakeup
Subject 3			owner control	read	*owner	

A

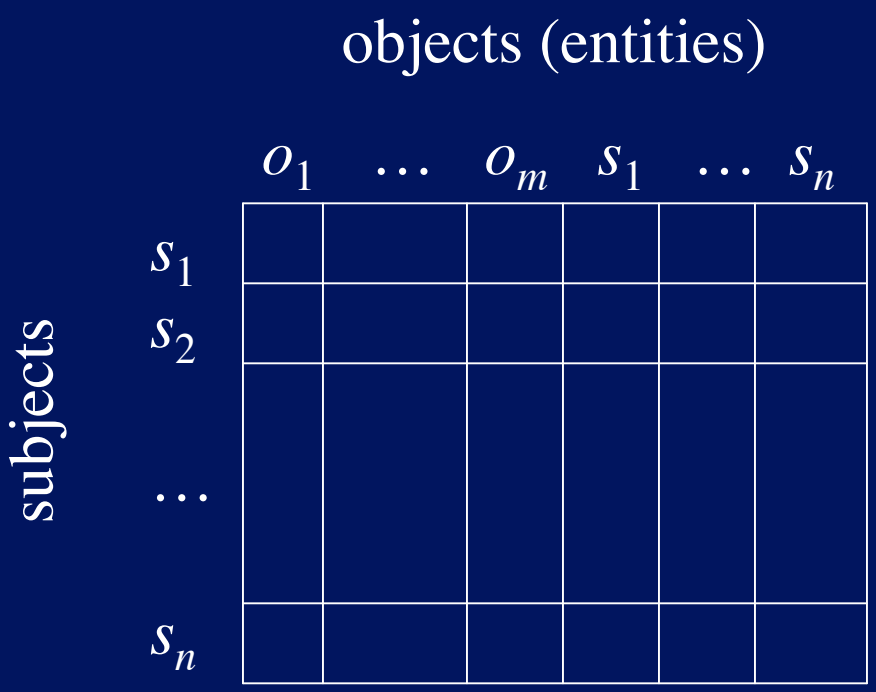
Objects



To be protected

- Subjects are objects
- Objects are not subjects

Access Matrix Structure



- Subjects $S = \{ s_1,\ldots,s_n \}$
- Objects $O = \{ o_1,\ldots,o_m \}$
- Rights $R = \{ r_1,\ldots,r_k \}$
- Entries $A[s_i, o_j] \subseteq R$
- $A[s_i, o_j] = \{ r_x, \ldots, r_y \}$ means subject s_i has rights $r_x, \ldots, r_y$ over object o_j

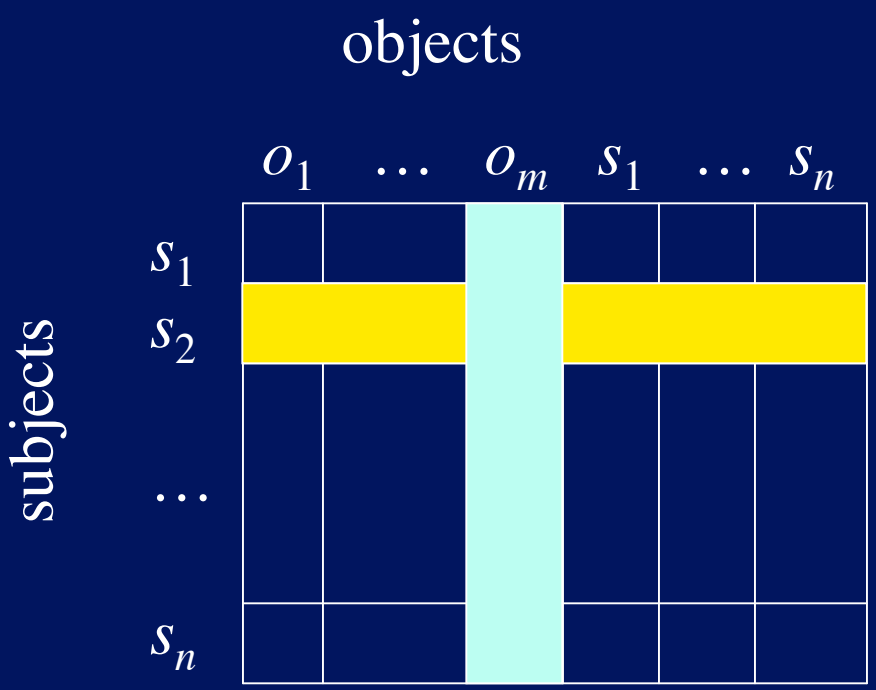
Example

- Processes *p*, *q*
- Files *f*, *g*
- Rights *r*, *w*, *x*, *a*, *o*

	f	*g*	*p*	*q*
p	*rwo*	*r*	*rwxo*	*w*
q	*a*	*ro*	*r*	*rwxo*

Owner-based Discretionary Access Control (DAC)

Matrix Implementation Techniques



- Capability list (c-list)
- Access control list (ACL)

Food for Thought

ACLs are good for revoking individual's access to a particular file.

- How hard is it to revoke a user's access to a particular set of, but not all, files if ACLs are used?
- Compare and contrast this with the problem of revocation using capabilities.

Access Matrix Summary

- Object System
  - Subjects, objects, access matrix
  - Objects are shared
  - All subjects are objects
    - not all objects are subjects
- Matrix implementation
  - Capability lists
  - Access control lists

Security Policies

What's Security Policy?

- Policy partitions system states into:
  - Authorized (secure)
    - These are states the system can enter
  - Unauthorized (nonsecure)
    - If the system enters any of these states, it's a security violation
- Secure system
  - Starts in authorized state
  - Never enters unauthorized state

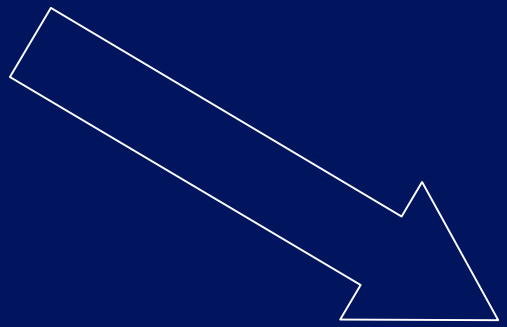
Main Types of Security Policies

- Confidentiality
  - Bell-LaPadula
- Integrity
  - Biba
  - Clark-Wilson
- Availability
  - ?
- Hybrid
  - Chinese Wall
  - ORCON
  - Role-based Access Control (RBAC)

CIA

Key Points about Policies and Mechanisms

Policies describe what's allowed



Mechanisms enforce policies

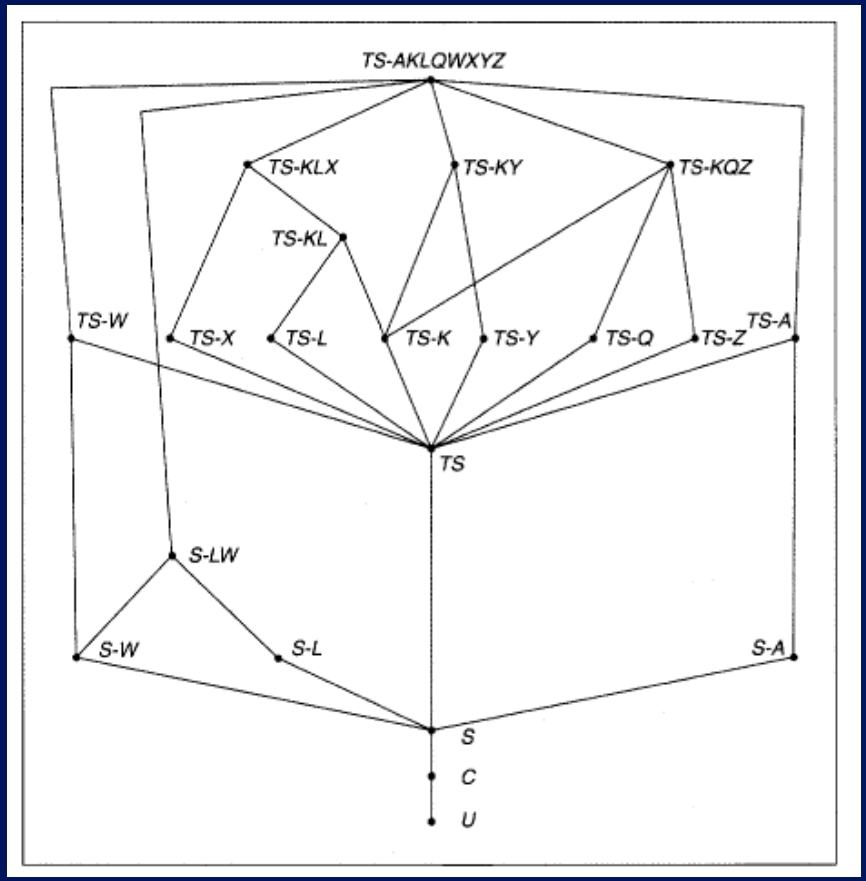
Confidentiality Policies

What's Confidentiality Policy

- Goal: prevent the unauthorized disclosure of information
  - Deals with information flow
  - Integrity incidental
- examples
  - Multi-level security (MLS) models
    - Bell-LaPadula Model basis for many

Bell–LaPadula Model

- Object and subject labels
- Categories
- "dominates" partial-order relation
- Simple security property
  - No reads up
- *-property
  - No writes down



Example for Bell-LaPadula: Controlling Access to Course Online Content

Application Description

Application:

- 10 students: s_1 … s_{10}
- 3 instructors: i_1, i_2, i_3
- 5 courses: c_1, … c_5
  - $C_1 = \{i_1, \{s_1, s_2, s_3\}\}$
  - $C_2 = \{i_2, \{s_3, s_4, s_5\}\}$
  - $C_3 = \{i_3, \{s_5, s_6, s_7\}\}$
  - $C_4 = \{i_1, \{s_7, s_8, s_9\}\}$
  - $C_5 = \{\{i_2, i_3\}, \{s_8, s_9, s_{10}\}\}$

Policy:

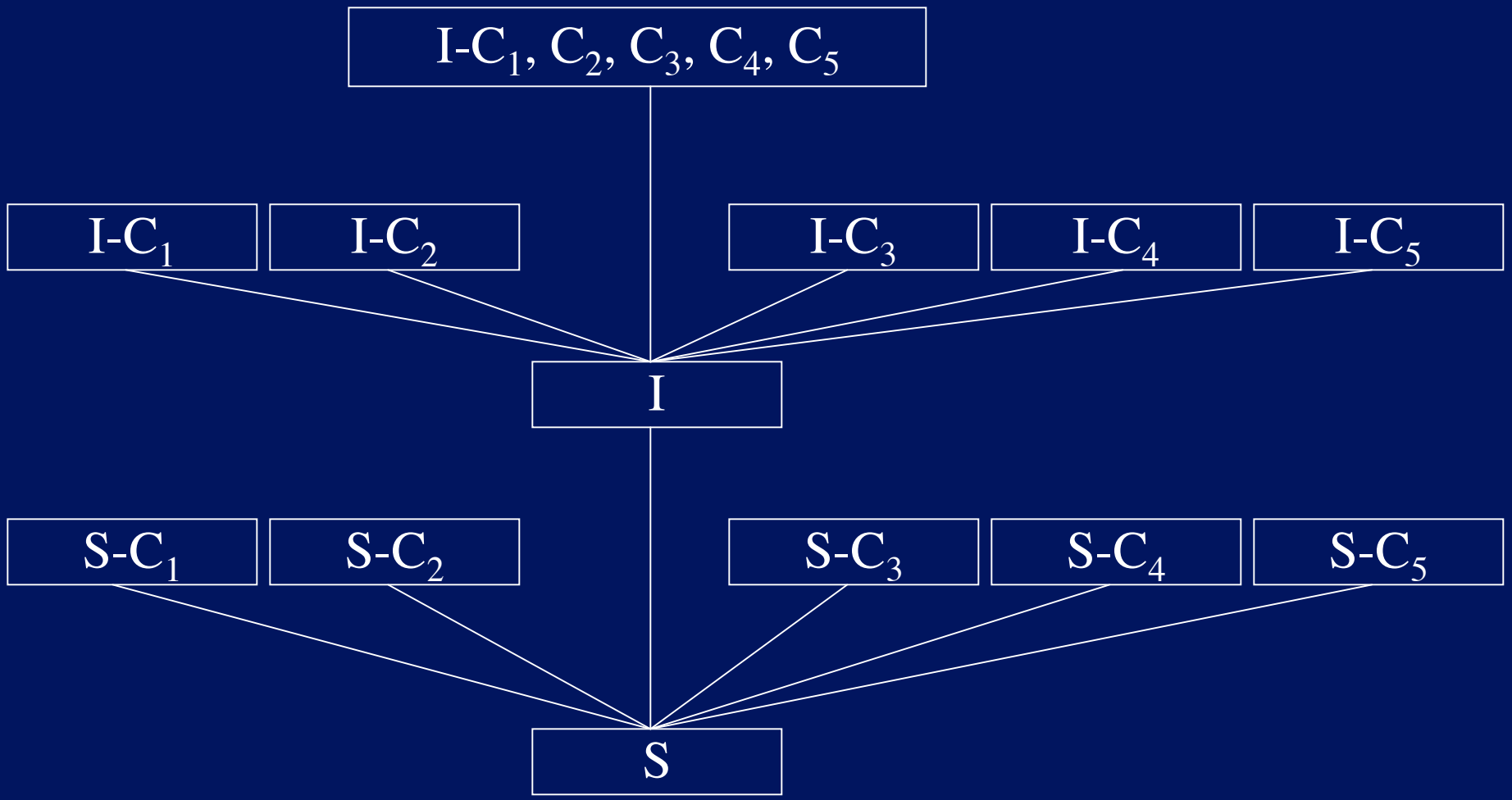
1. Students can
   1. read course material and assignment instructions for the courses they are registered
   2. submit (i.e., write) their assignments for the registered courses
2. Instructors can
   1. read student submitted assignments for the courses they teach, and
   2. post (i.e., write) course material and assignment instructions for their courses

Develop configuration (i.e., label graph, and clearance and classification assignments) for access control mechanisms based on Bell-LaPadula model

Solution

1. Security level Lattice
2. File classifications
3. User clearances
4. DAC matrix

Security level Lattice



File Classifications

Course material for course i == CM_i

Assignment Submission for course i == AS_i

	S	$S\text{-}C_1$	$S\text{-}C_2$	$S\text{-}C_3$	$S\text{-}C_4$	$S\text{-}C_5$	I	$I\text{-}C_1$	$I\text{-}C_2$	$I\text{-}C_3$	$I\text{-}C_4$	$I\text{-}C_5$	$I\text{-}C_1 \ldots C_5$
CM_1		√											
AS_1		√											
CM_2			√										
AS_2			√										
CM_3				√									
AS_3				√									
CM_4					√								
AS_4					√								
CM_5						√							
AS_5						√							

User Clearances

	S	S-C_1	S-C_2	S-C_3	S-C_4	S-C_5	I	I-C_1	I-C_2	I-C_3	I-C_4	I-C_5	I-C_1…C_5
i_1								√			√		
i2									√			√	
i3										√		√	
s1		√											
s2		√											
s_3		√	√										
s_4			√										
s_5			√	√									
s_6				√									
s_7				√	√								
s_8					√	√							
s_9					√	√							
s_{10}						√							

DAC Matrix

	CM_1	CM_2	CM_3	CM_4	CM_5	AS_1^1	AS_1^2	AS_1^3	AS_2^3	AS_2^4	AS_2^5	AS_3^5	AS_3^6	AS_3^7	AS_4^7	AS_4^8	AS_4^9
any	R	R	R	R	R												
i_1	O			O		R	R	R							R	R	R
i_2		O			O				R	R	R						
i_3			O		W							R	R	R			
s_1						O											
s_2							O										
s_3								O	O								
s_4										O							
s_5											O	O					
s_6													O				
s_7														O	O		
s_8																O	
s_9																	O
s_{10}																	

Assignment Submission for course i by student j == AS_i^j

Key Points About Confidentiality Models

- Control information flow
- Bell-LaPadula
- Often combine MAC (relationship of security levels) and DAC (the required permission)
- Don't deal with covert channels

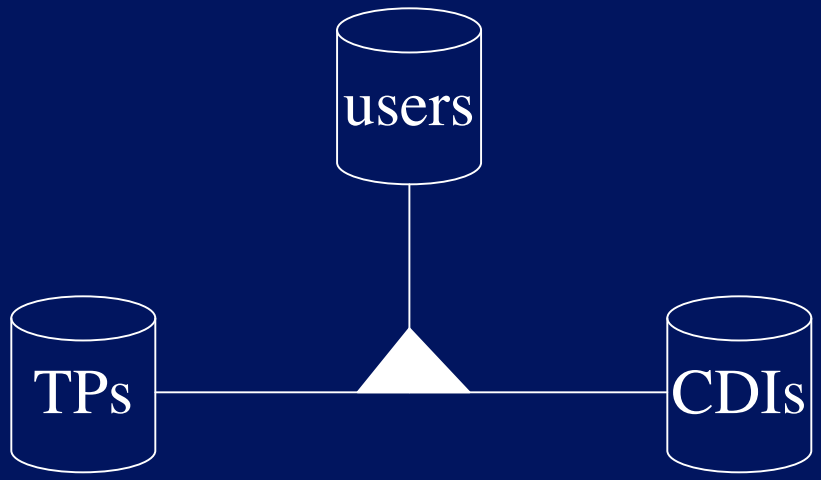
Integrity Policies

Biba Integrity Model (1977)

- Integrity levels instead of security levels in MLS
- The higher the level, the more confidence
  - That a program will execute correctly
  - That data is accurate and/or reliable

Clark–Wilson Model

- Constrains who can do what
  - authorized triples: (user, TP, {CDI})



- transaction procedures (TPs): Procedures that take the system from one valid state to another
- constrained data items (CDIs): Data subject to integrity controls

Clark-Wilson Model (cont-ed)

- Integrity defined by a set of constraints
  - Data in a *consistent* or valid state when it satisfies constraints
- Example: Bank
  - *D* today's deposits, *W* withdrawals, *YB* yesterday's balance, *TB* today's balance
  - Integrity constraint: $YB + D - W = TB$
- *Well-formed transaction* move system from one consistent state to another

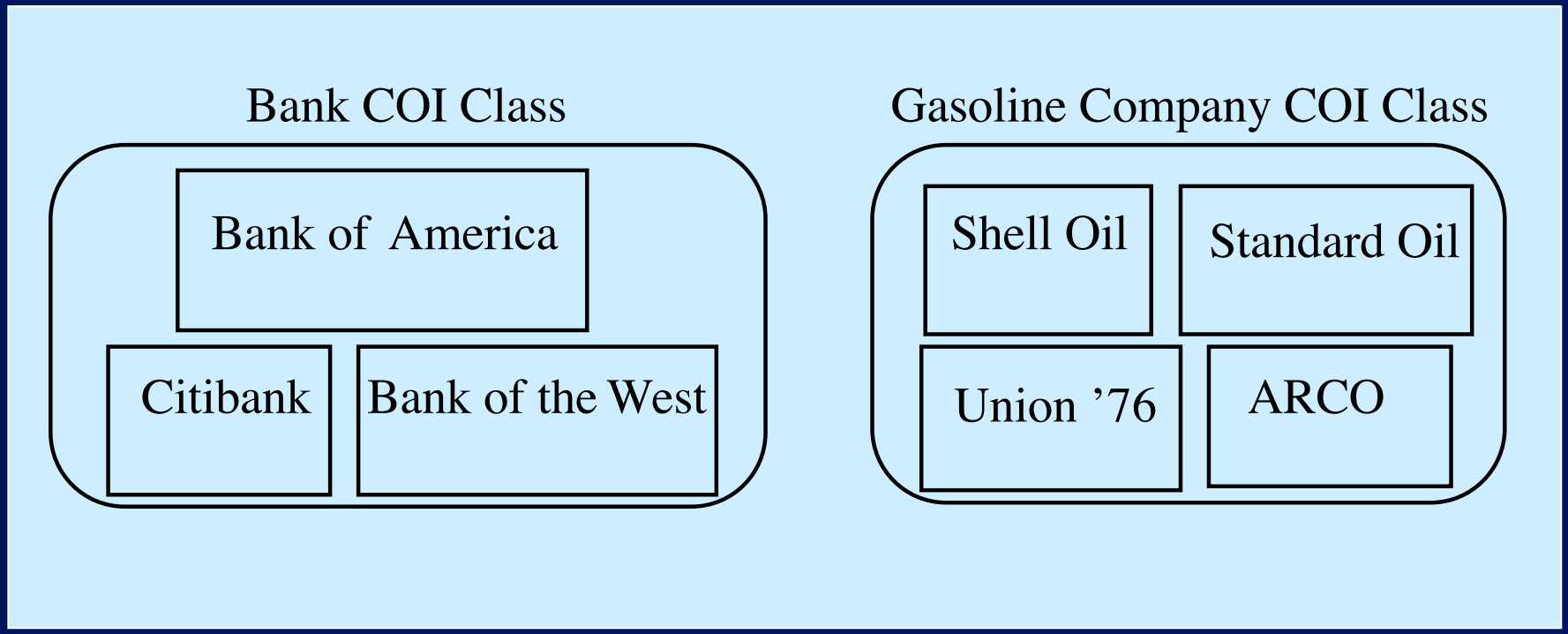
Key Points About Integrity Models

- Integrity policies deal with trust
  - As trust is hard to quantify, these policies are hard to evaluate completely
  - Look for assumptions and trusted users to find possible weak points in their implementation
- Biba's model is based on multilevel integrity
- Clark-Wilson's focuses on separation of duty and transactions

Hybrid Security Models


Chinese Wall Model

Chinese Wall Model: Illustration



- If Anthony reads any *Company dataset* (CD) in a conflict of interest (COI), he can **never** read another CD in that COI

ORCON Model

Problem: organization creating document wants to control its dissemination

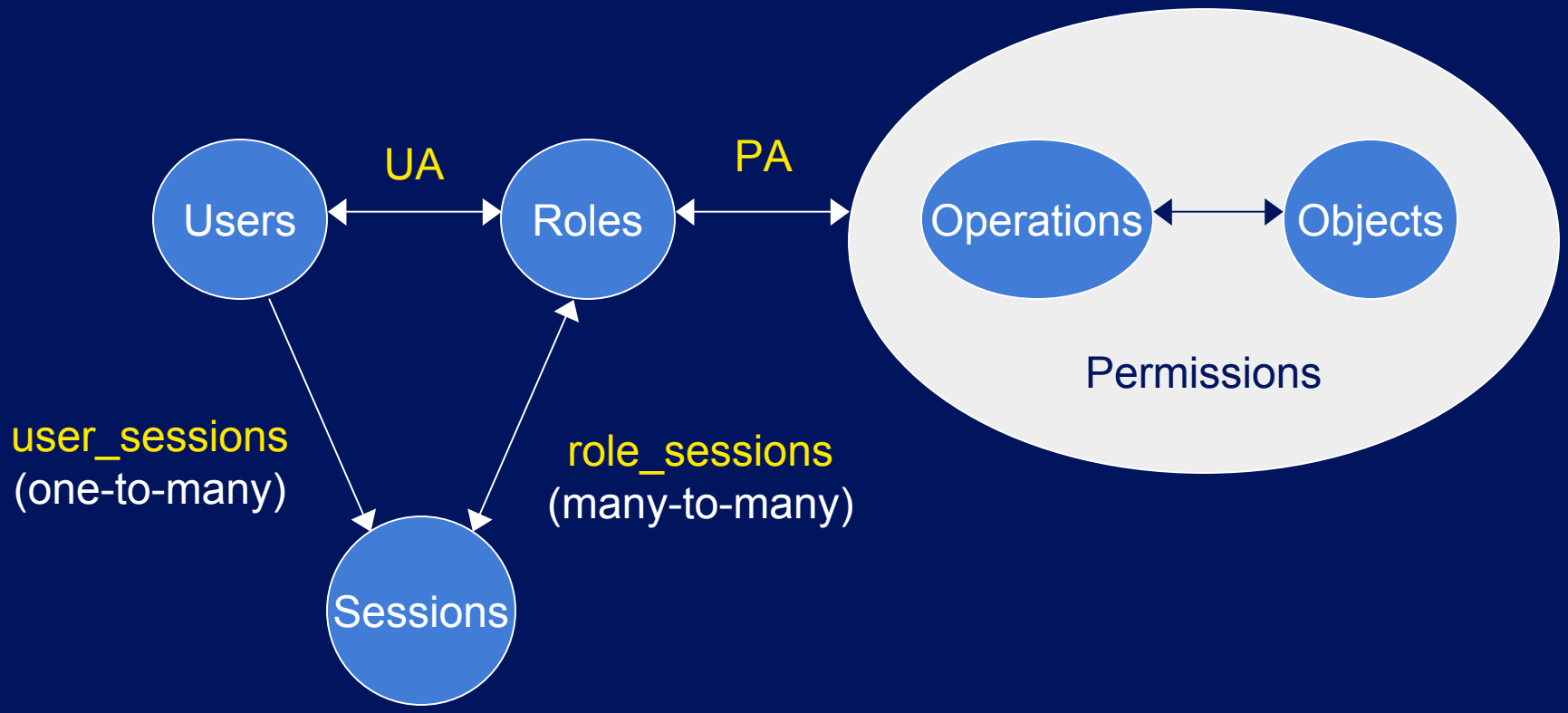
Example: Secretary of Agriculture writes a memo for distribution to her immediate subordinates, and she must give permission for it to be disseminated further. This is "originator controlled" (here, the "originator" is a person).

Role-based Access Control (RBAC)

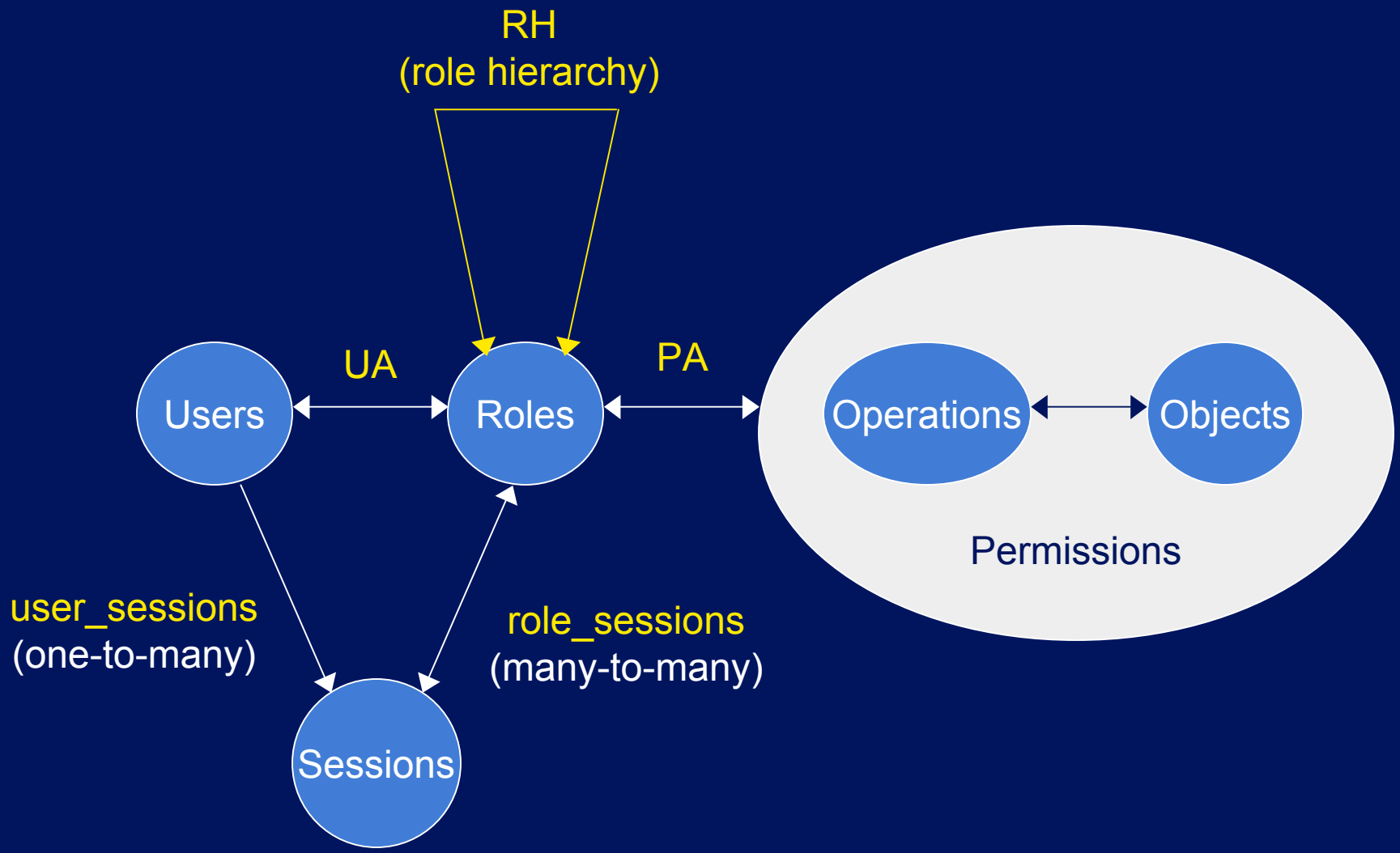
RBAC

- Access depends on role, not identity or label
  - Example:
    - Allison, administrator for a department, has access to financial records.
    - She leaves.
    - Betty hired as the new administrator, so she now has access to those records
  - The role of "administrator" dictates access, not the identity of the individual.

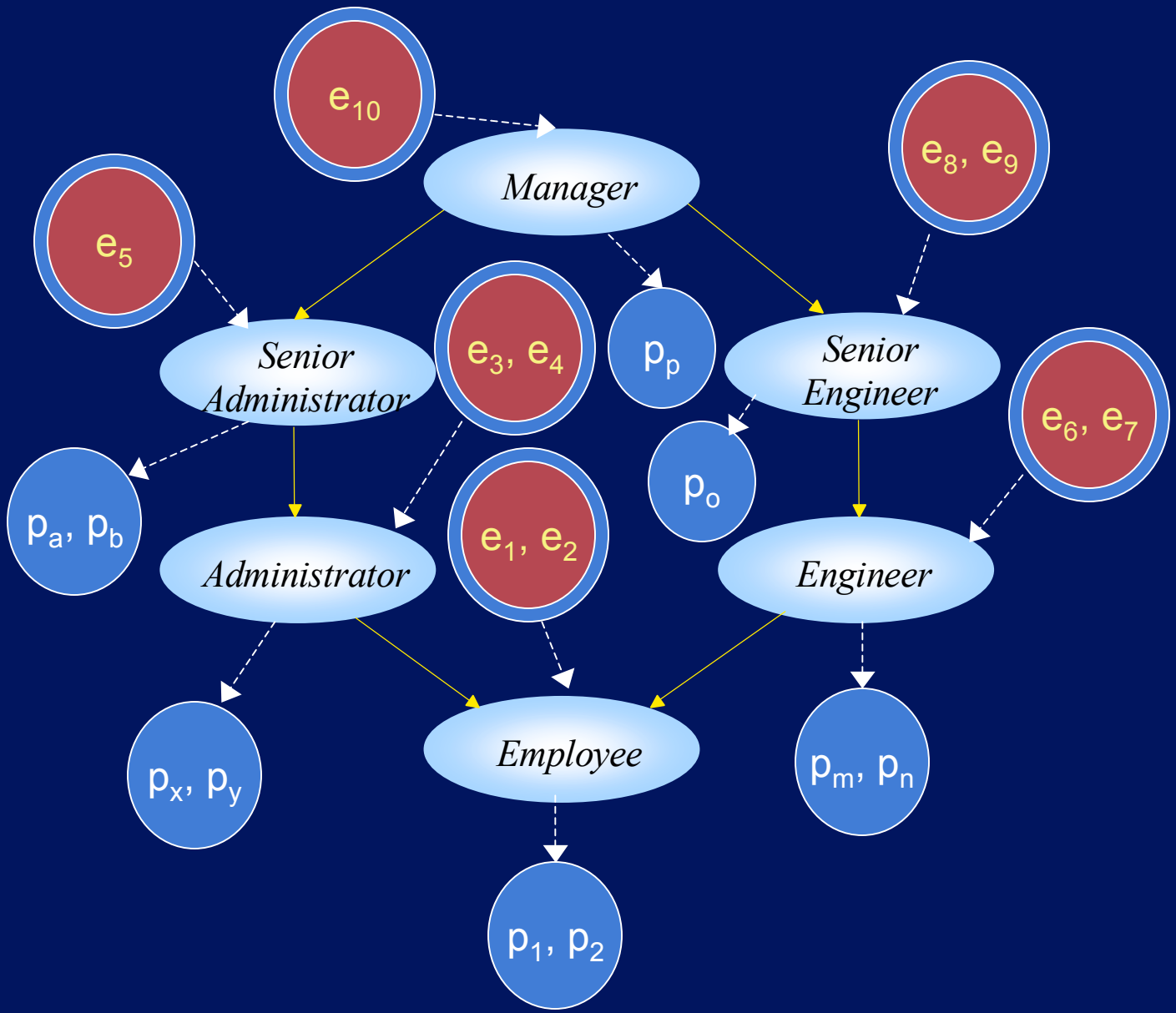
RBAC (NIST Standard)



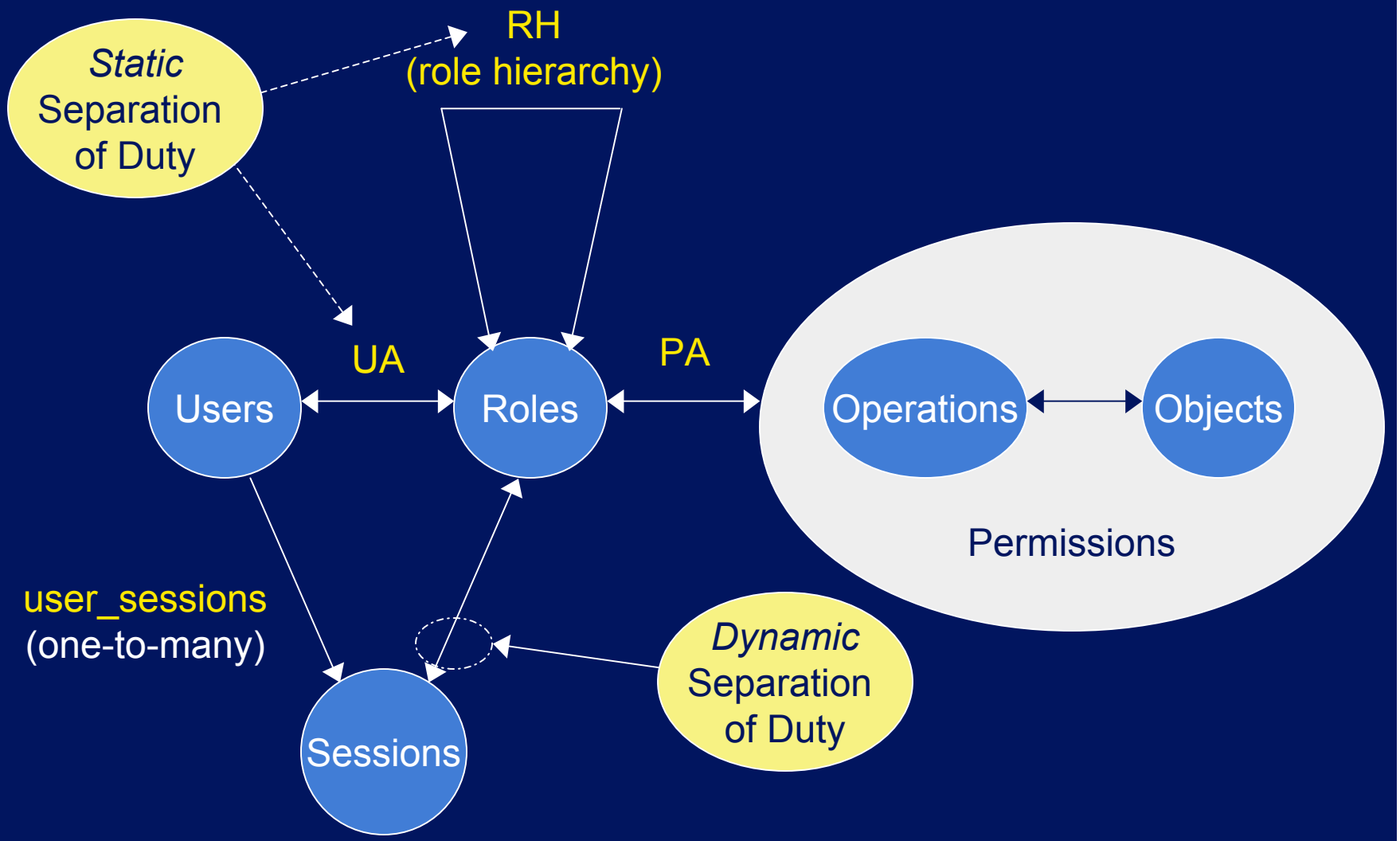
RBAC with General Role Hierarchy



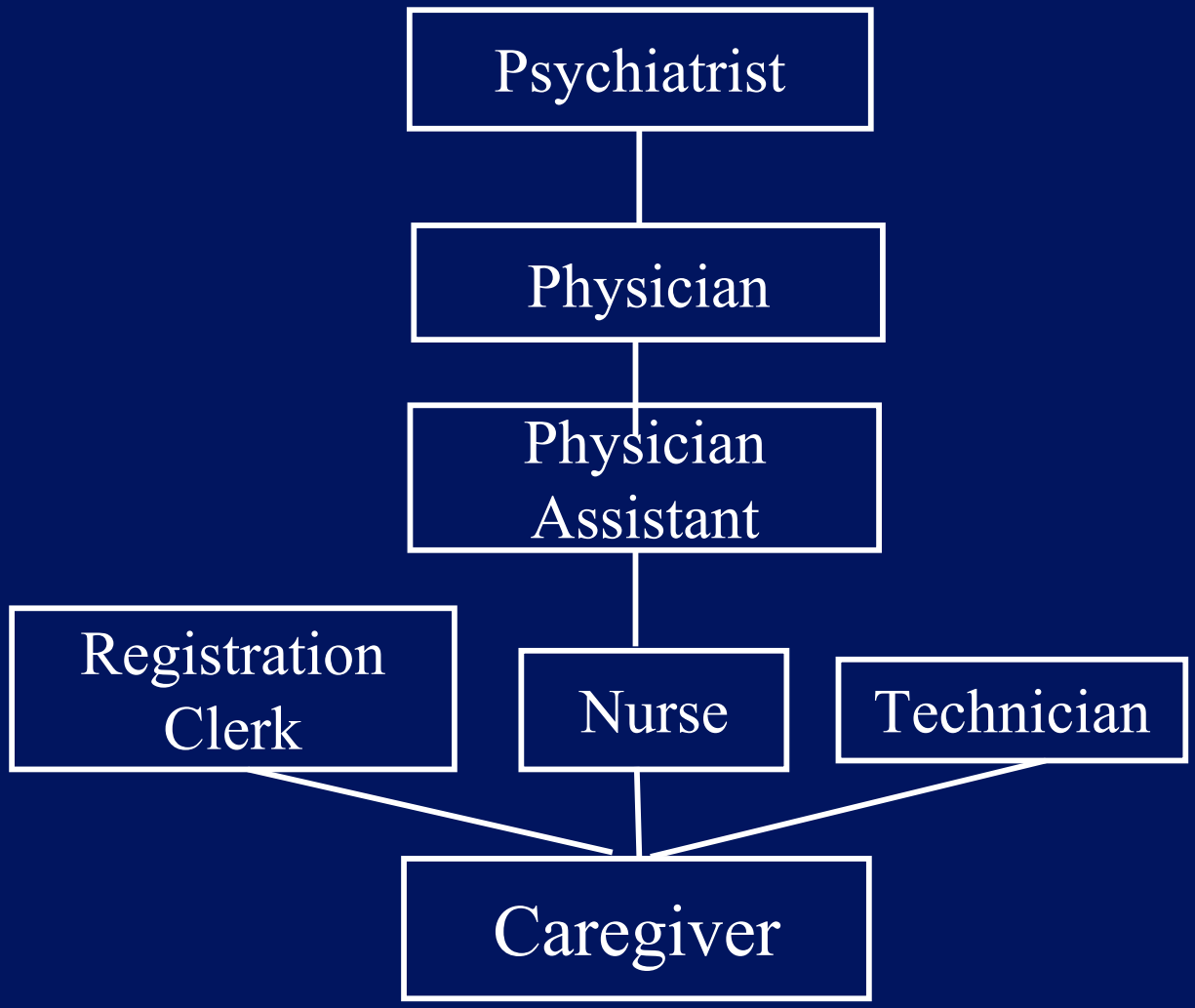
Example


e_{10}
Manager
e_8, e_9
e_5
Senior Administrator
e_3, e_4
p_p
Senior Engineer
e_6, e_7
p_o
p_a, p_b
Administrator
e_1, e_2
Engineer
p_x, p_y
Employee
p_m, p_n
p_1, p_2

Constrained RBAC



Sample System



Application Description

Application:

- 10 students: s_1 … s_{10}
- 3 instructors: i_1, i_2, i_3
- 5 courses: c_1, … c_5
  - $C_1 = \{i_1, \{s_1, s_2, s_3\}\}$
  - $C_2 = \{i_2, \{s_3, s_4, s_5\}\}$
  - $C_3 = \{i_3, \{s_5, s_6, s_7\}\}$
  - $C_4 = \{i_1, \{s_7, s_8, s_9\}\}$
  - $C_5 = \{\{i_2, i_3\}, \{s_8, s_9, s_{10}\}\}$

Policy:

1. Students can
   1. read course material and assignment instructions for the courses they are registered
   2. submit (i.e., write) their assignments for the registered courses
2. Instructors can
   1. read student submitted assignments for the courses they teach, and
   2. post (i.e., write) course material and assignment instructions for their courses

Develop configuration (i.e., UA, PA, Role hierarchy) for access control mechanisms based on RBAC model

Key Points on Hybrid Models

- deal with both confidentiality and integrity
- ORCON model neither MAC nor DAC
  - Actually, a combination
- RBAC model controls access based on subject's role(s)

Summary

- Access control mechanisms
- Access Matrix
- Security policies
  - Confidentiality models
    - Bell LaPadula confidentiality model
  - Integrity models
    - Biba integrity model
    - Clark-Wilson
  - Hybrid models
    - Chinese Wall model
    - ORCON model
    - RBAC model