THE UNIVERSITY OF BRITISH COLUMBIA

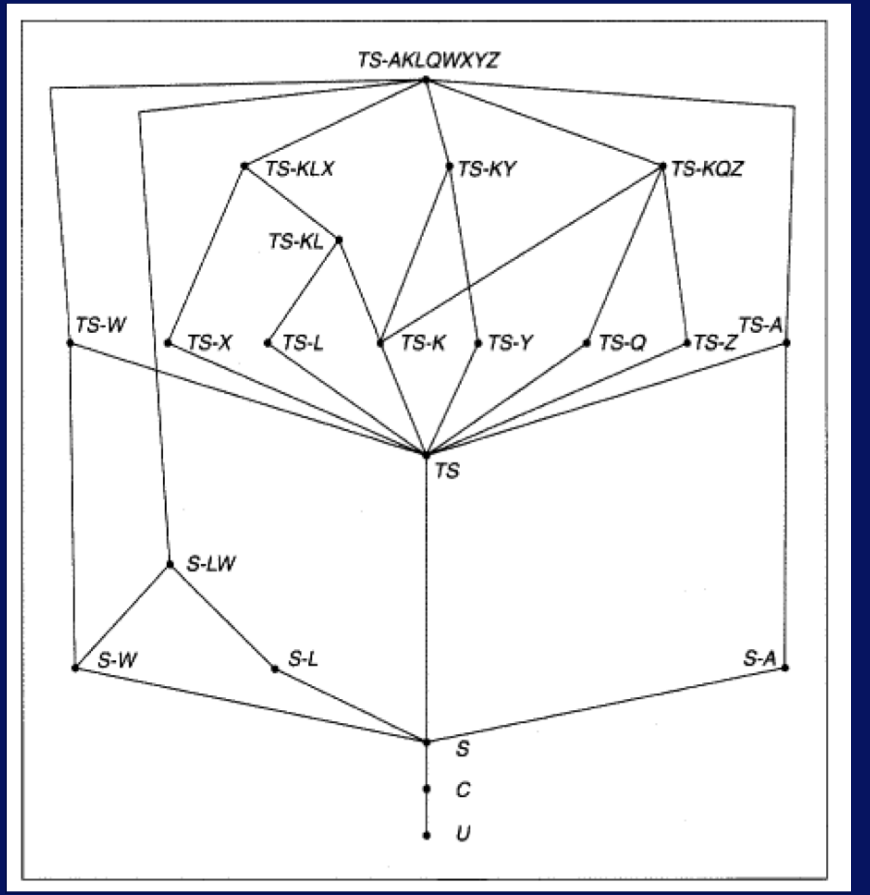
Security Policies

EECE 412

Session 14

Last Session Recap

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



Outline

Security policies

- Integrity Policies
  - Biba integrity model
  - Clark-Wilson integrity model
- Hybrid Policies
  - Chinese Wall model
  - Clinical Information Systems Security policy (self-study)
  - ORCON model
  - RBAC model

THE UNIVERSITY OF BRITISH COLUMBIA

Integrity Policies

Biba Integrity Model (1977)

- Set of subjects S, objects O, integrity levels I, relation $\leq \subseteq I \times I$ holding when second dominates first or same
- *min*: $I \times I \rightarrow I$ returns lesser of integrity levels
- *i*: $S \cup O \rightarrow I$ gives integrity level of entity
- r: $S \times O$ means $s \in S$ can read $o \in O$
- w: $S \times O$ means $s \in S$ can write $o \in O$
- x: $S \times O$ means $s \in S$ can execute $o \in O$

What does a higher integrity level of an object mean?

Intuition for Integrity Levels

- The higher the level, the more confidence
  - That a program will execute correctly
  - That data is accurate and/or reliable
- Note relationship between integrity and trustworthiness
- Important point: *integrity levels are **not** security levels*

Low-Water-Mark Policy

- Idea: when s reads o, $i'(s) = min(i(s), i(o))$; s can only write objects at lower levels
- Rules
  1. $s \in S$ can write to $o \in O$ if and only if (iff) $i(o) \leq i(s)$.
  2. If $s \in S$ reads $o \in O$, then $i'(s) = min(i(s), i(o))$, where $i'(s)$ is the subject's integrity level after the read.
  3. $s_1 \in S$ can execute $s_2 \in S$ if and only if $i(s_2) \leq i(s_1)$.
- When can s read o according to the Low-Water-Mark policy?

Problems

- Subjects' integrity levels decrease as system runs
  - Soon no subject will be able to access objects at high integrity levels
- What could be a solution?
- Alternative: change object levels rather than subject levels
  - Soon all objects will be at the lowest integrity level

Ring Policy

- Idea: subject integrity levels static
- Rules
  1. $s \in S$ can write to $o \in O$ if and only if $i(o) \leq i(s)$.
  2. Any subject can read any object.
  3. $s_1 \in S$ can execute $s_2 \in S$ if and only if $i(s_2) \leq i(s_1)$.
- Eliminates indirect modification problem

Strict Integrity Policy (a.k.a., "Biba's Model")

- Similar to Bell-LaPadula model
  1. $s \in S$ can read $o \in O$ iff $i(s) \leq i(o)$
  2. $s \in S$ can write to $o \in O$ iff $i(o) \leq i(s)$
  3. $s_1 \in S$ can execute $s_2 \in S$ iff $i(s_2) \leq i(s_1)$
- Add compartments and discretionary controls to get full dual of Bell-LaPadula model

Example: LOCUS and Biba

- Goal: prevent untrusted software from altering data or other software
- Approach: make levels of trust explicit
  - *credibility rating* based on estimate of software's trustworthiness (0 untrusted, *n* highly trusted)
  - *trusted file systems* contain software with a single credibility level
  - Process has *risk level* or highest credibility level at which process can execute
  - Must use *run-untrusted* command to run software at lower credibility level

THE UNIVERSITY OF BRITISH COLUMBIA

Clark-Wilson Integrity Model

Model

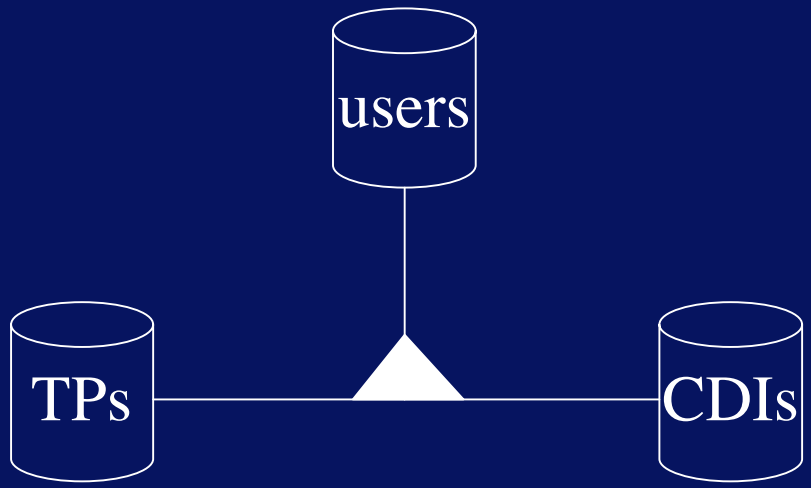
- Integrity defined by a set of constraints
  - Data in a *consistent* or valid state when it satisfies these
- Example: Bank
  - *D* today's deposits, *W* withdrawals, *YB* yesterday's balance, *TB* today's balance
  - Integrity constraint: $YB + D - W = TB$
- *Well-formed transaction* move system from one consistent state to another
- Issue: who examines, certifies transactions done correctly?
  - The principle of separation of duty

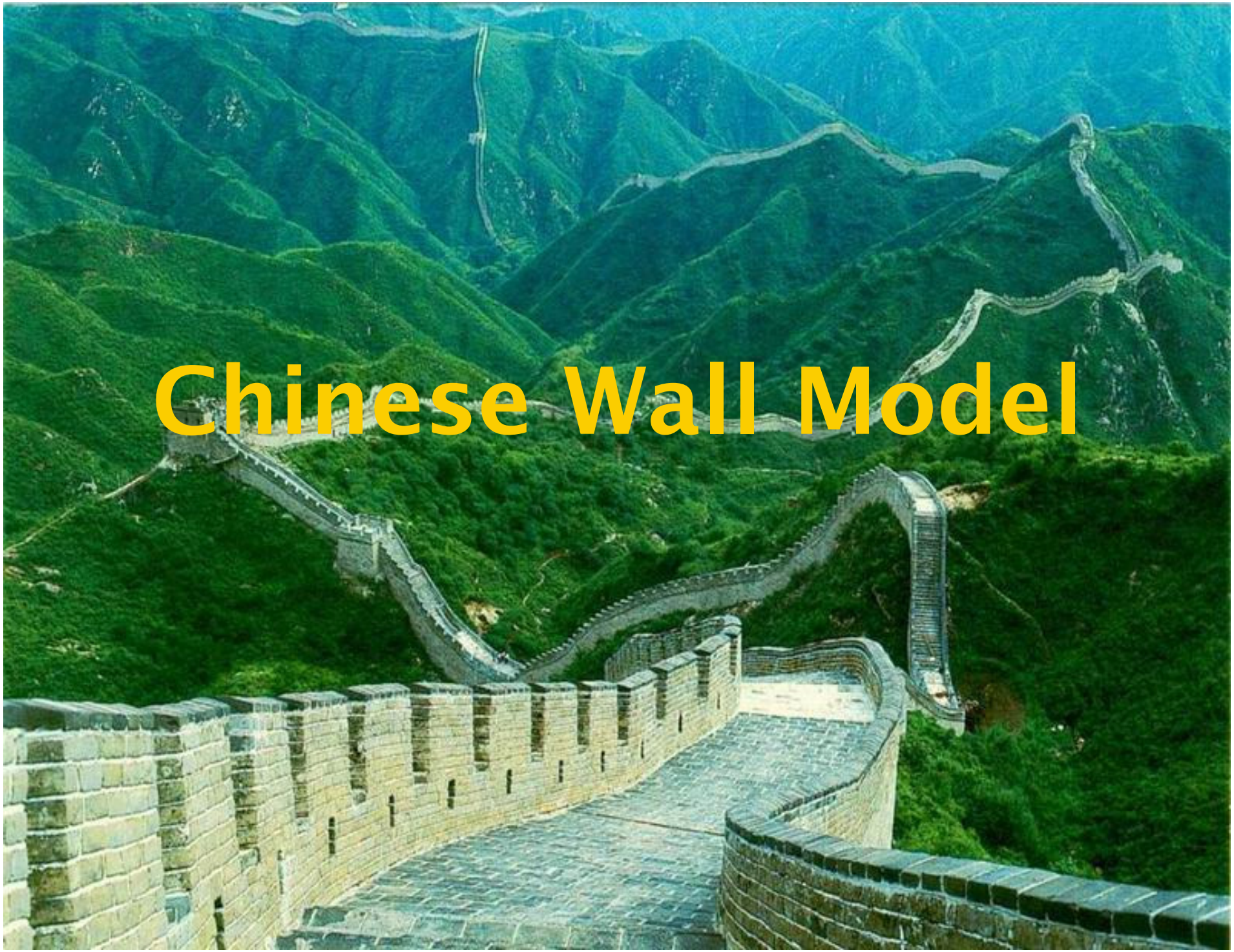
Entities in the Model

- CDIs: constrained data items
  - Data subject to integrity controls
- UDIs: unconstrained data items
  - Data not subject to integrity controls
- IVPs: integrity verification procedures
  - Procedures that test the CDIs conform to the integrity constraints
- TPs: transaction procedures
  - Procedures that take the system from one valid state to another

The Idea

Constrain who can do what by defining authorized triples: (user, TP, {CDI})




Chinese Wall Model

What's Chinese Wall Model

Problem:

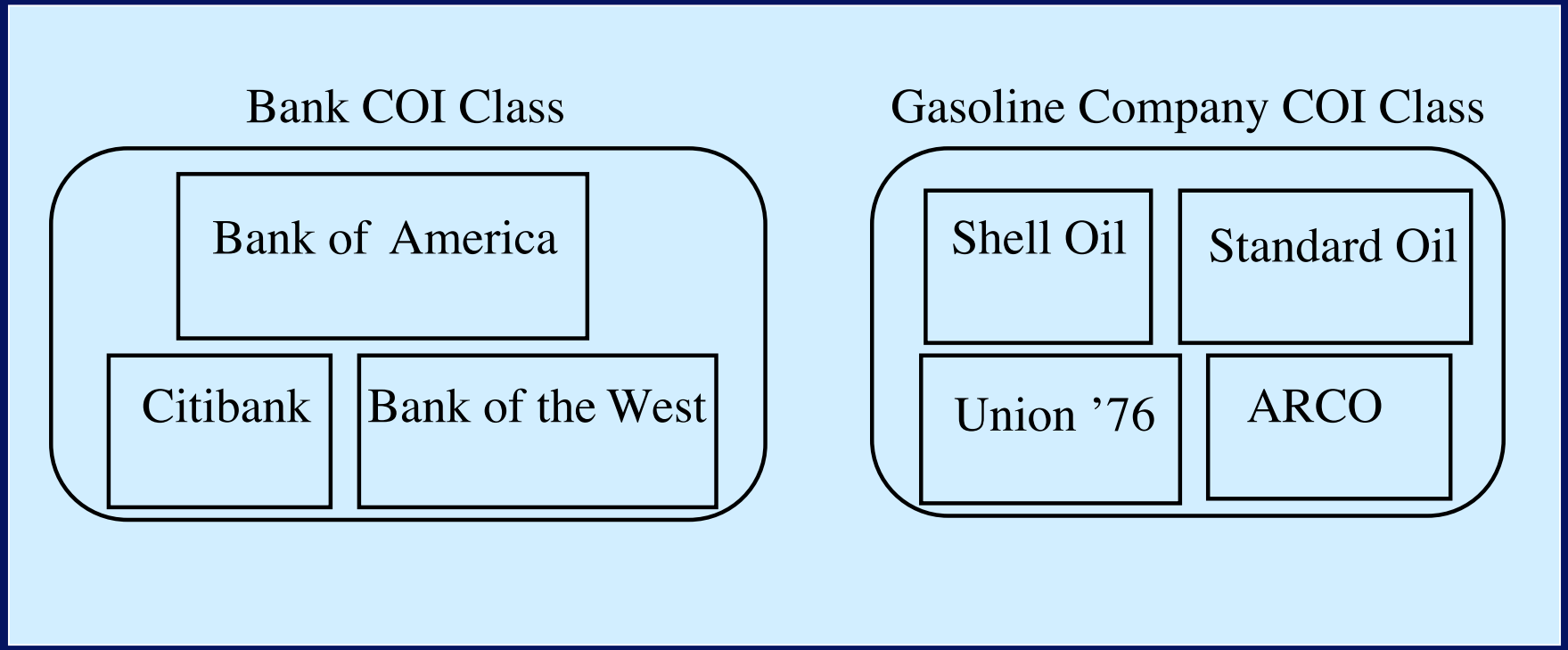
- Tony advises American Bank about investments
- He is asked to advise Toyland Bank about investments

- Conflict of interest to accept, because his advice for either bank would affect his advice to the other bank

Organization

- Organize entities into "conflict of interest" classes
- Control subject accesses to each class
- Control writing to all classes to ensure information is not passed along in violation of rules
- Allow sanitized data to be viewed by everyone

Example



- If Anthony reads any *Company dataset* (CD) in a conflict of interest (COI), he can *never* read another CD in that COI
  - Possible that information learned earlier may allow him to make decisions later

CW-Simple Security Condition

- *s* can read *o* iff either condition holds:
  1. There is an o' such that *s* has accessed o' and $CD(o') = CD(o)$
     - Meaning *s* has read something in *o*'s dataset
  2. For all $o' \in O$, $o' \in PR(s) \Rightarrow COI(o') \neq COI(o)$
     - Meaning *s* has not read any objects in *o*'s conflict of interest class
- Ignores sanitized data (see below)
- Initially, $PR(s) = \varnothing$, so initial read request granted

Writing

- Anthony, Susan work in same trading house
- Anthony can read Bank 1's CD, Gas' CD
- Susan can read Bank 2's CD, Gas' CD
- If Anthony could write to Gas' CD, Susan can read it
  - Hence, indirectly, she can read information from Bank 1's CD, a clear conflict of interest

THE UNIVERSITY OF BRITISH COLUMBIA

ORCON Model

What's the problem ORCON solves?

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).

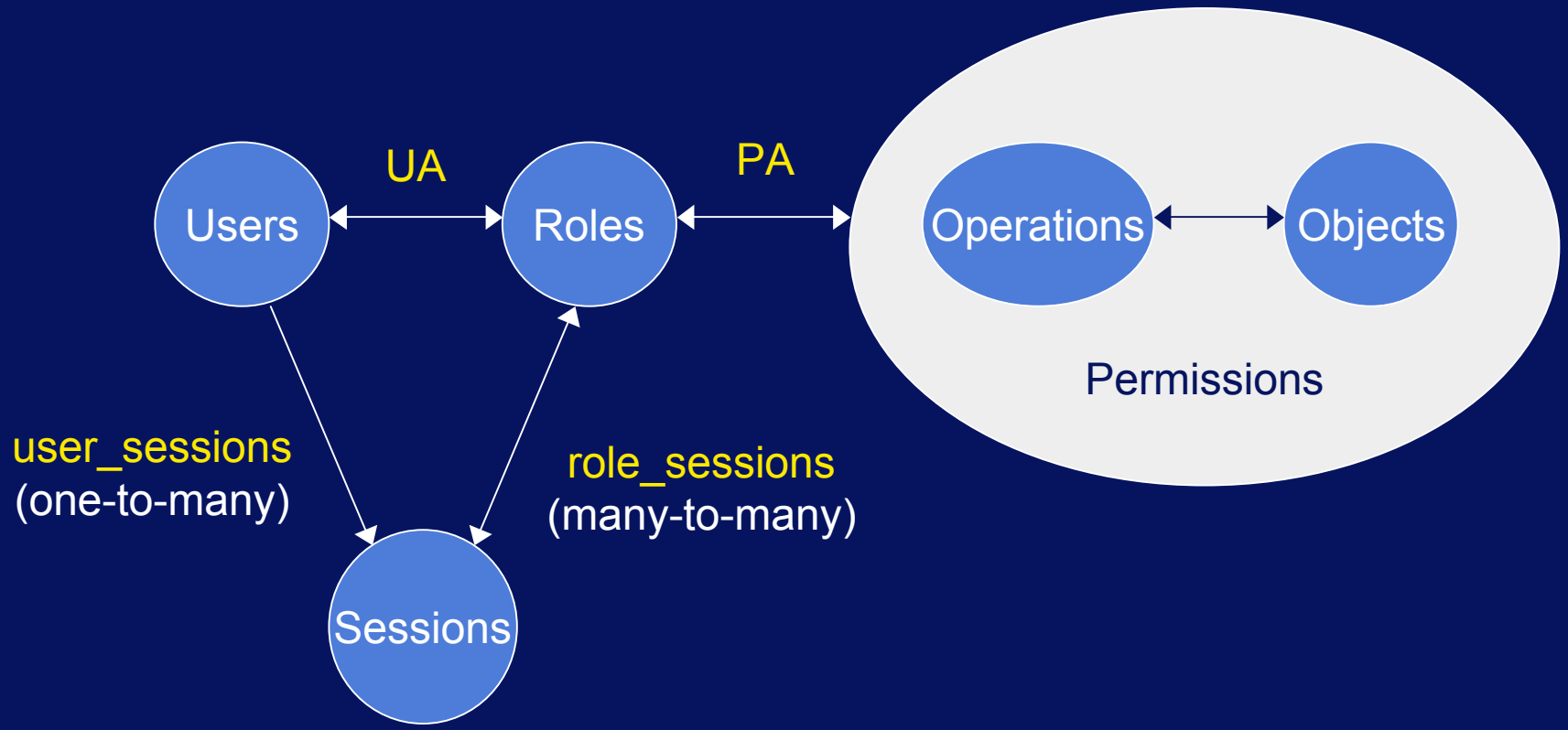
THE UNIVERSITY OF BRITISH COLUMBIA

Role-based Access Control (RBAC)

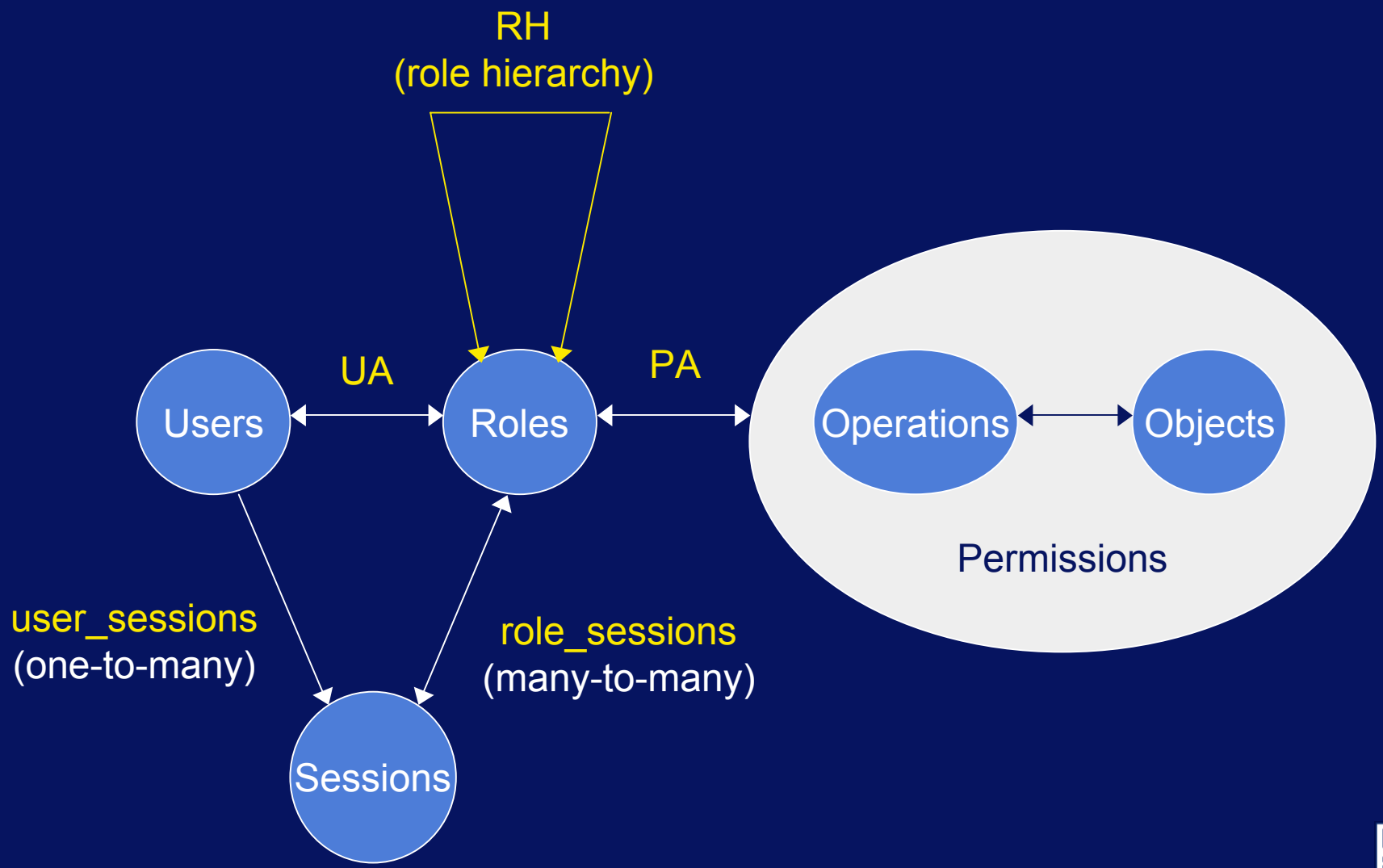
RBAC

- 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.

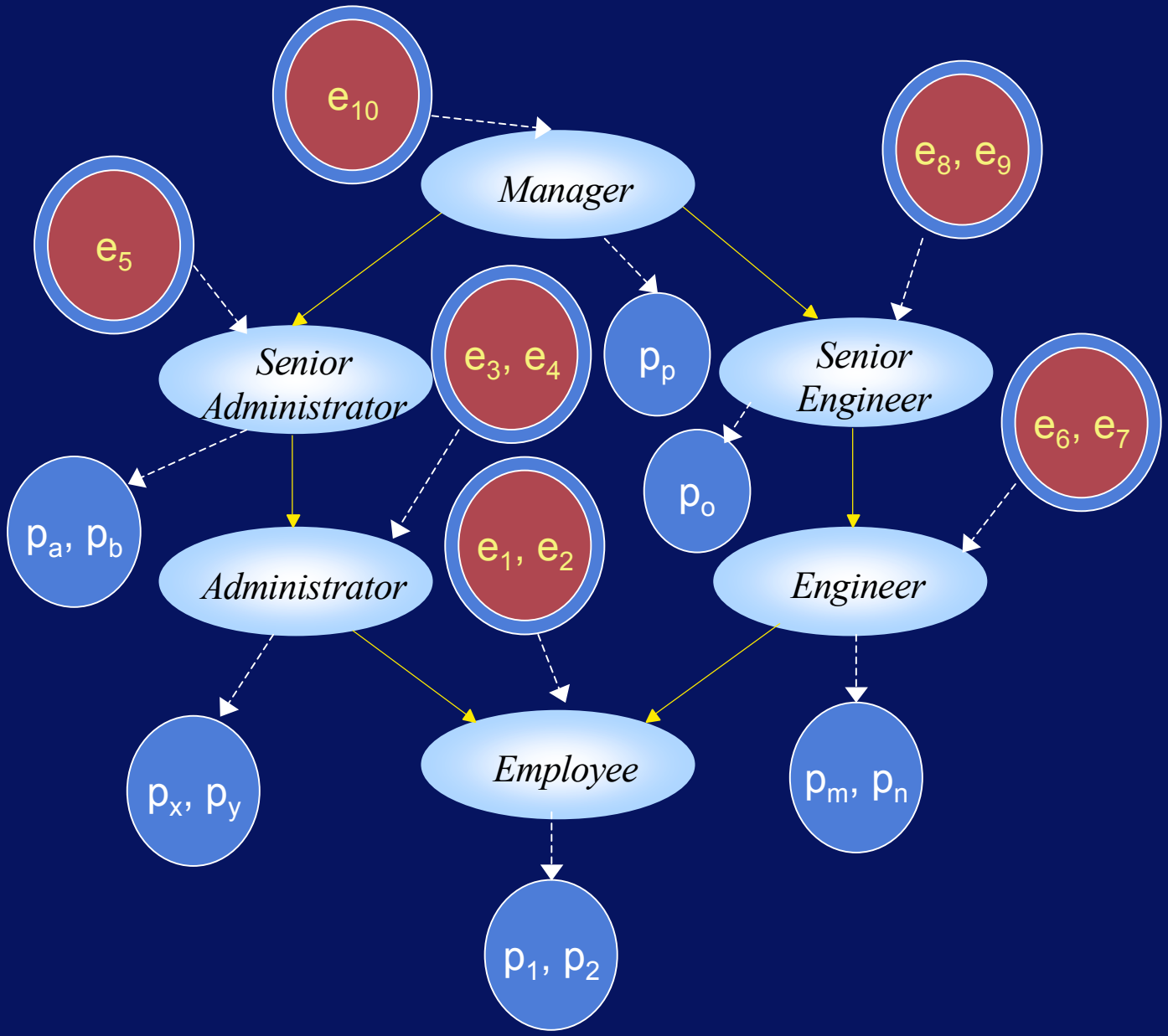
RBAC (NIST Standard)



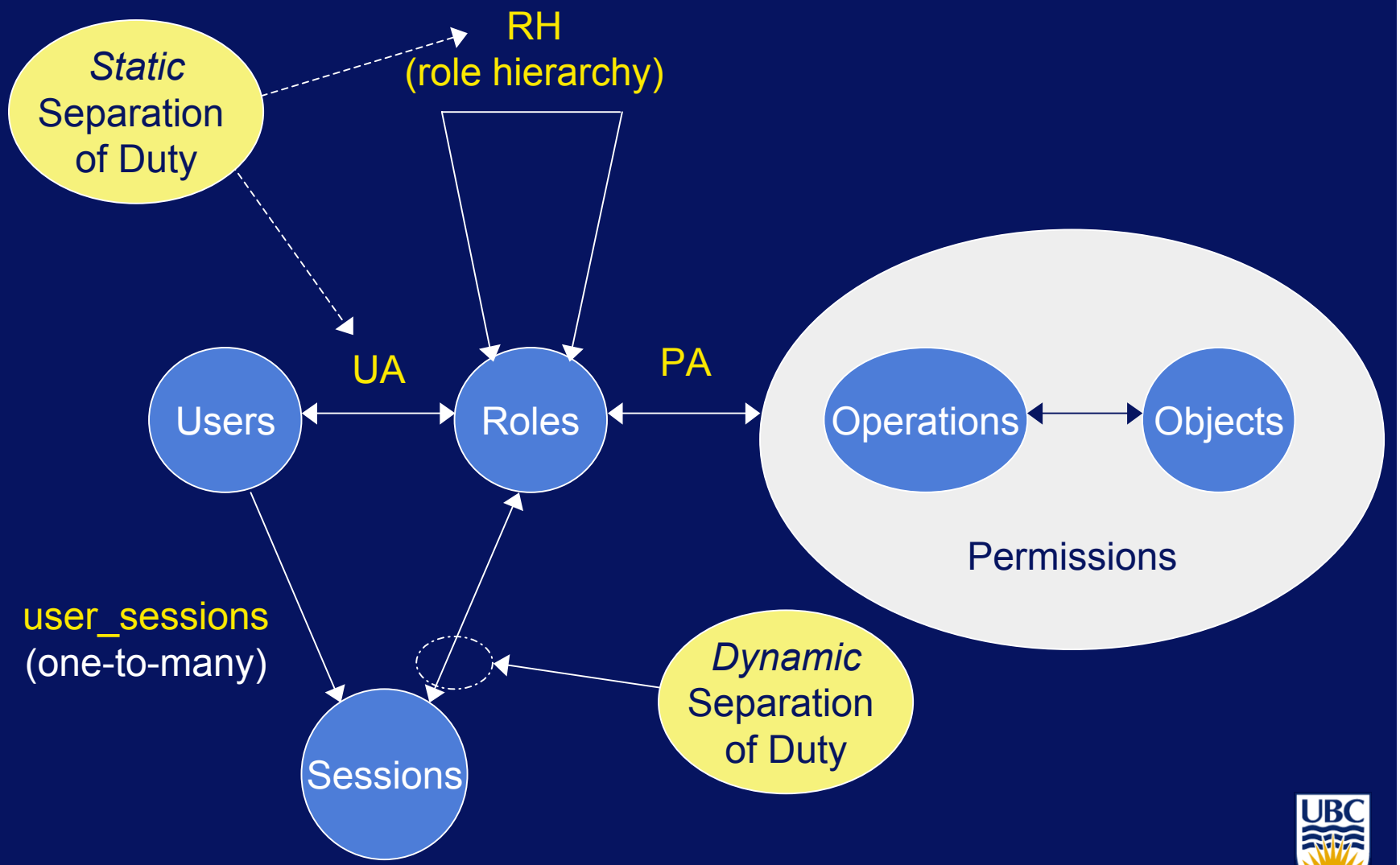
RBAC with General Role Hierarchy



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



Key Points

- 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 based on multilevel integrity
  - Clark-Wilson focuses on separation of duty and transactions
- Hybrid policies
  - deal with both confidentiality and integrity
  - Different combinations of these
  - ORCON model neither MAC nor DAC
    - Actually, a combination
  - RBAC model controls access based on subject's role(s)