Lecture 5: Access Control Ep.2

05506044 System Security

Dr. Rungrat Wiangsripanawan

Recap

- Access Control Concepts
- Subject/object/Access Write
- ACM/Access Control List

- Security m
- Access Control Models
  - DAC
  - MAC
  - RBAC
- Bell-lapadula Models

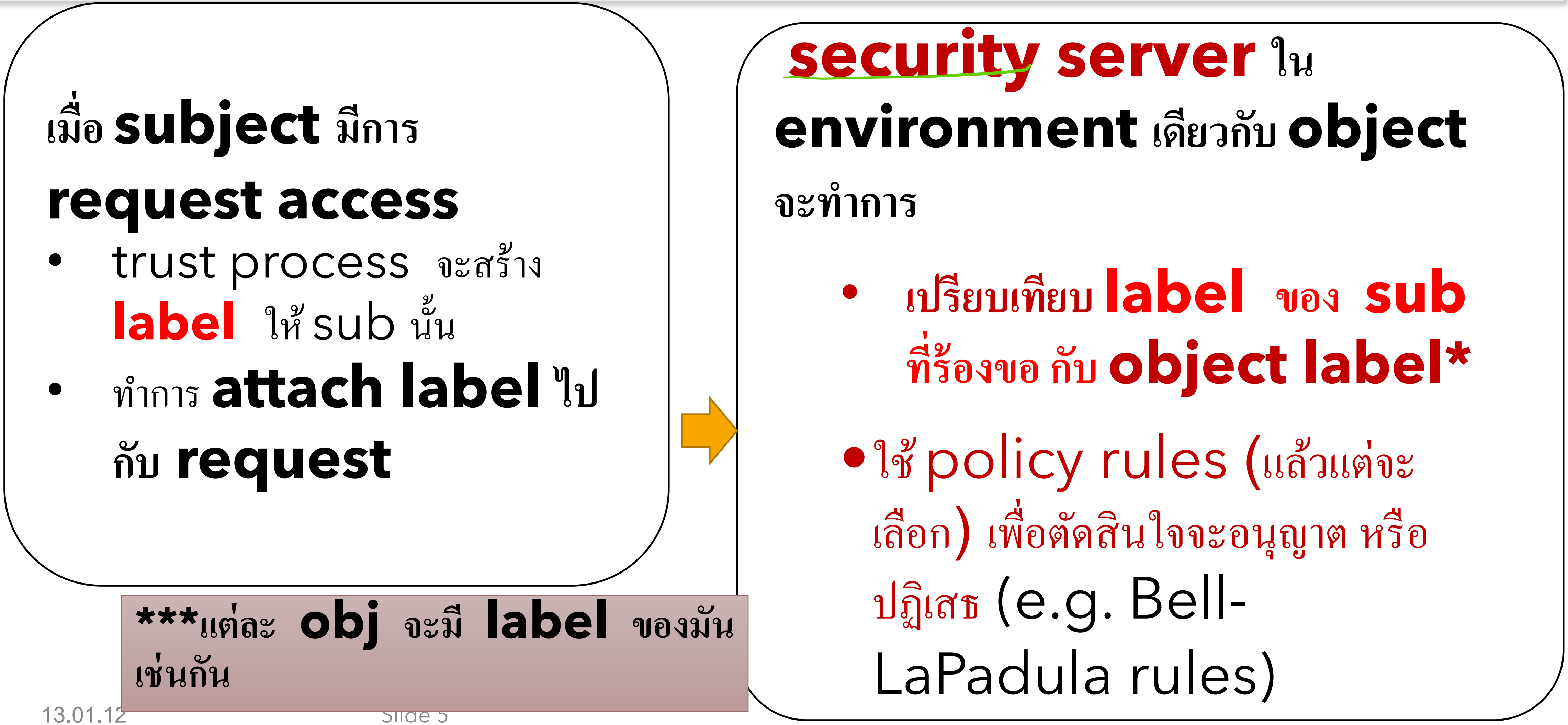
Security label

With protection rings,

- **เปรียบเทียบระหว่าง**
  - **the subject (number) and**
  - **the object (number)**
- **numbers**
  - **examples of Security label**

- มักจะถูกใช้ใน access control policy แบบ multi-level access control policies.

Security label คืออะไร



เมื่อ **subject** มีการ **request access**

- trust process จะสร้าง **label** ให้ sub นั้น
- ทำการ **attach label** ไป กับ **request**

security server ใน **environment** เดียวกับ **object** จะทำการ

- เปรียบเทียบ **label** ของ **sub** ที่ร้องขอ กับ **object label***
- ใช้ policy rules (แล้วแต่จะเลือก) เพื่อตัดสินใจจะอนุญาต หรือ ปฏิเสธ (e.g. Bell-LaPadula rules)

***แต่ละ **obj** จะมี **label** ของมัน เช่นกัน

Multilevel security

- *ทั้ง sub และ obj จะต้องมีค่า security label* ซึ่ง label ของ sub และ obj จะเป็นคนละชนิด
- subjects labels => clearances,
- objects labels => classifications or sensitivity
  - every action/operation has a sensitivity rating (like top secret).
- Multilevel Security label เหมาะกับ องค์กรหรือระบบที่แบ่งการเข้าถึงข้อมูลเป็นลำดับชั้น เช่น
  - Military organizations.
  - Banks.
- We will look at an example in military organisations but the same approach can be used in other cases.

Access Control Policies

- คำถาม
  - Who might set the security policies? (ใครเป็นคนกำหนดว่า ใครทำอะไรได้บ้าง)

เจ้าของ object หรือ ระบบ ???

Access Control Models

An access control model is a **framework** that dictates how subjects access objects.

It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.

There are three main types of access control models:

Access Control Policies/Models:

Discretionary Access:

ผู้ใช้ที่เป็นเจ้าของ obj เป็นคนกำหนดว่าใครจะเข้าถึงอะไรได้บ้าง

Non-Discretionary Access:

- Subjects and Objects have fixed security attributes that are used by the System to determine access.
- Users cannot modify security attributes.
- System (Sec. Admin) → decides.

ประเภทของ Access Control Policies/Models

Discretionary Access Control (DAC)

- Users decide how they want to protect their asset files

Mandatory Access Control (MAC)

- The system decides.

Role-based Access Control (RBAC)

- The system decides.

Access Control Model

- Each model type uses different methods to control how subjects access objects, and each has its own benefits and limitations.
- These models are built into the core or the kernel of the different operating systems and possibly their supporting applications.
- Every operating system has a security kernel that enforces a reference monitor concept, which differs depending upon the type of access control model embedded into the system.
- For every access attempt, before a subject can communicate with an object, the security kernel reviews the rules of the access control model to determine whether the request is allow

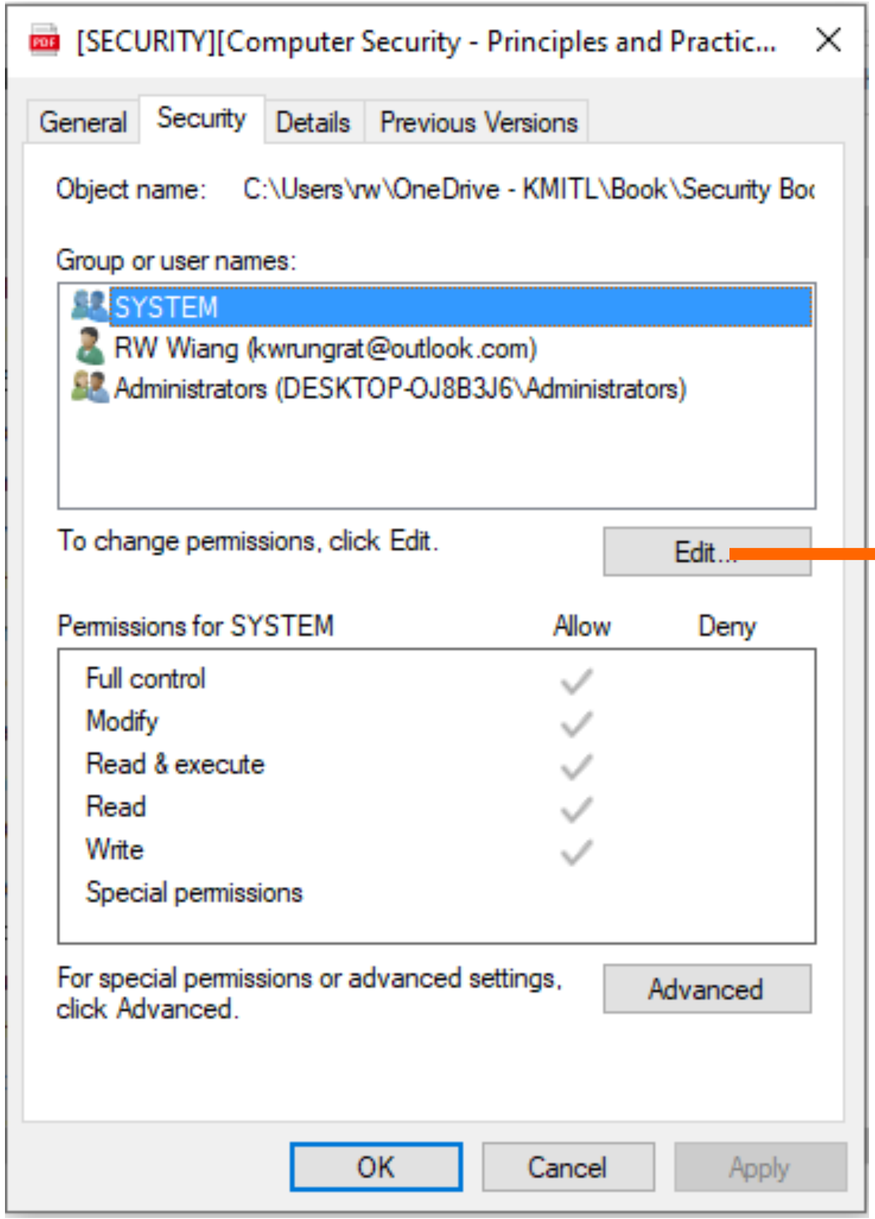
How to know which model to use?

- The **business and security goals** of an organization will help prescribe what access control model it should use, along with **the culture of the company** and the **habits of conducting business.**
- Some companies use one model exclusively, whereas others combine them to be able to provide the necessary level of protection.

Discretion access control (DAC)

- A *discretionary access control* (DAC) policy is a means of assigning access rights based on rules specified by users *(owner of the file) .*
- This model is called discretionary because the control of access is based on the discretion of the owner.
- Ex. capabilities, access control list
- Also, the file permissions model implemented by nearly all operating systems.
  - Ex. permission string in unix   are in this category.
  - the users (owner of the file) CAN change the permissions on files they own, making this a discretionary policy.

http://www.cs.cornell.edu/Courses/CS513/2007fa/NL.accessControl.html



[SECURITY][Computer Security - Principles and Practic...

Object name: C:\Users\rw\OneDrive - KMITL\Book\Security Boo

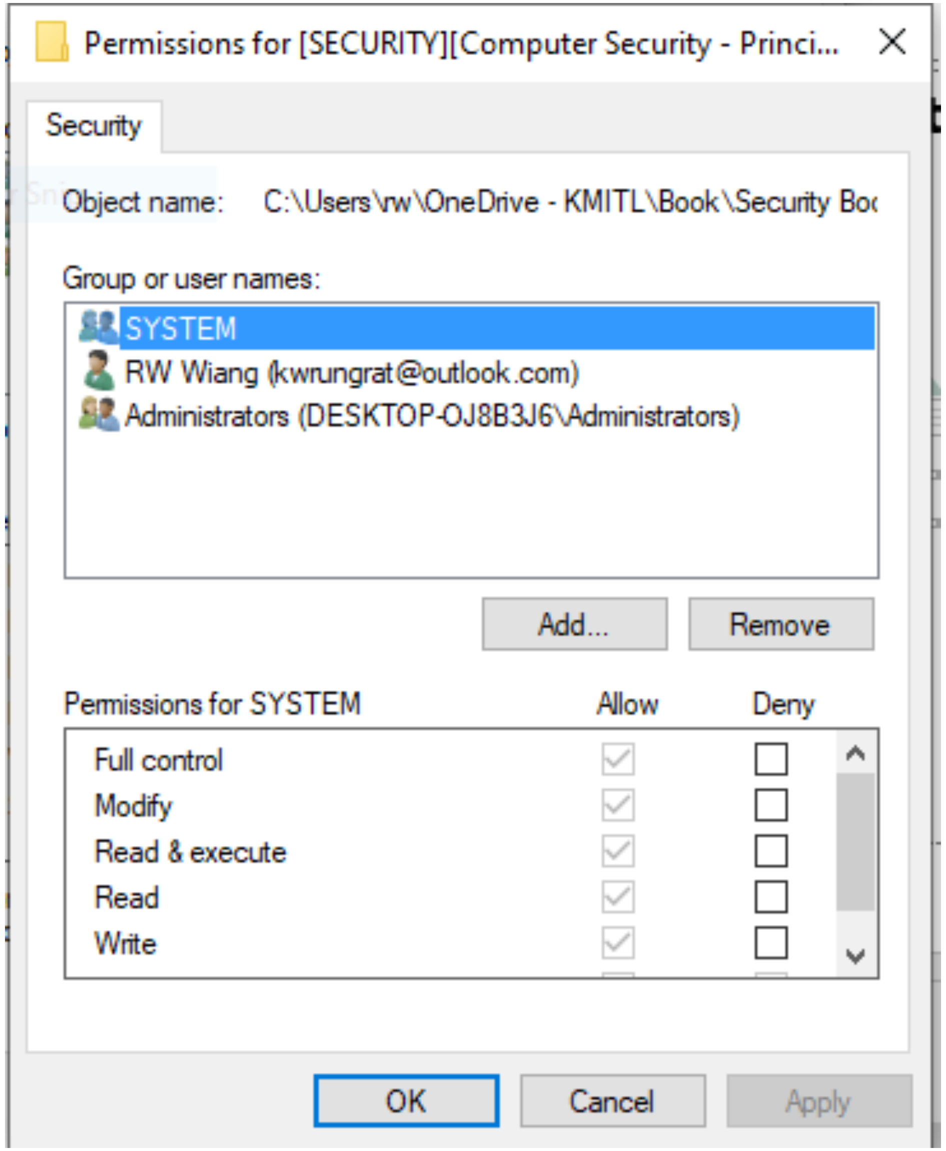
Group or user names:

- SYSTEM
- RW Wiang (kwrungrat@outlook.com)
- Administrators (DESKTOP-OJ8B3J6\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.



Permissions for [SECURITY][Computer Security - Princi...

Object name: C:\Users\rw\OneDrive - KMITL\Book\Security Boo

Group or user names:

- SYSTEM
- RW Wiang (kwrungrat@outlook.com)
- Administrators (DESKTOP-OJ8B3J6\Administrators)

Permissions for SYSTEM	Allow	Deny
Full control	☑	☐
Modify	☑	☐
Read & execute	☑	☐
Read	☑	☐
Write	☑	☐

Mandatory Access Control Policies

Access Control Policy :	• The system decides. • Object owners cannot change the policy
Enforces the control mandated by	• a central authority
Everything has a label,	• security label • Subject - clearance label • Object – sensitivity label
The most common form	• is the multi-level security policy

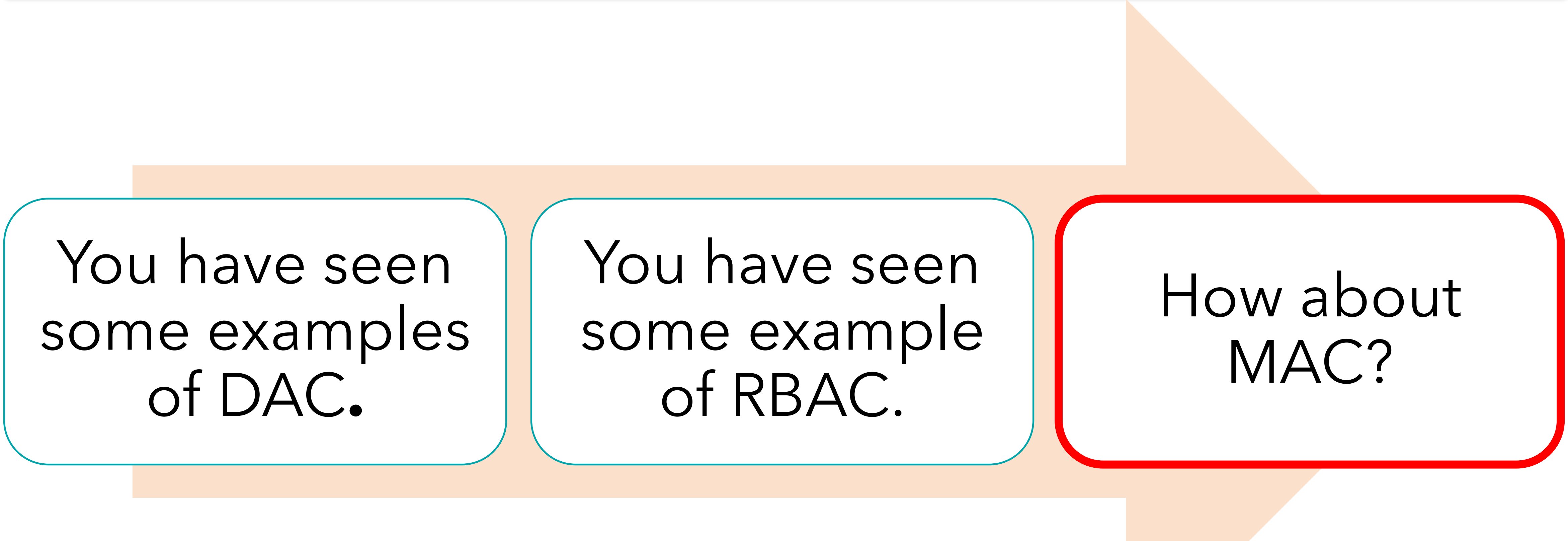
http://www.cs.cornell.edu/Courses/cs513/2005fa/L11.html

Role based access control Policy

The system decides

Based on the roles that users are assigned in the system rather than the user identity.

- Example - Teller, customer manager in the bank.



You have seen some examples of DAC.

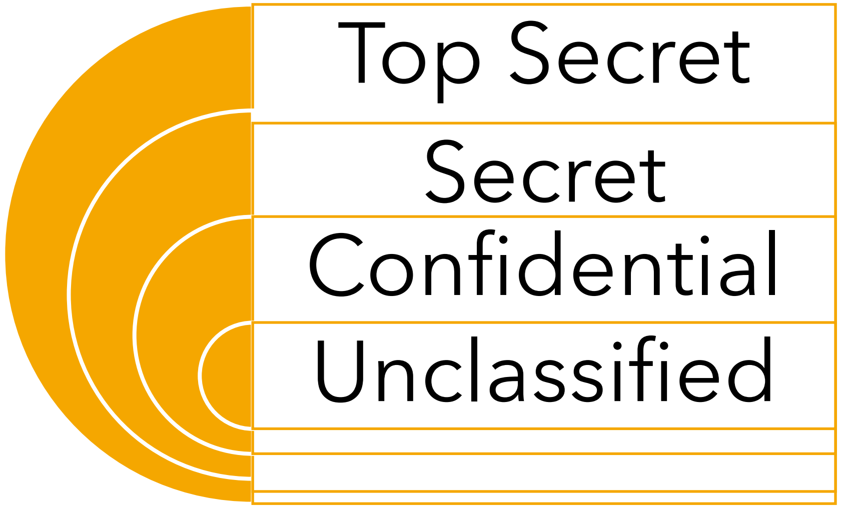
You have seen some example of RBAC.

How about MAC?

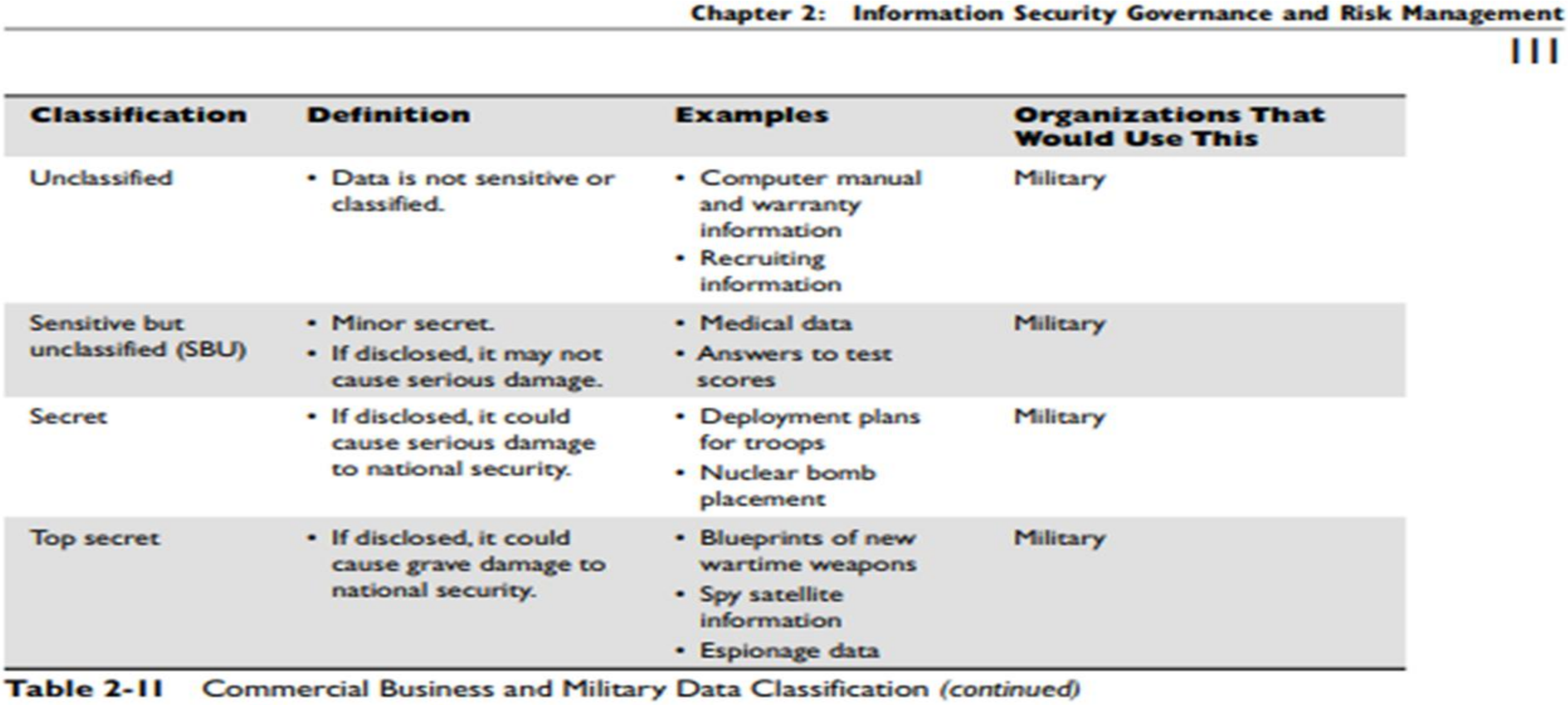
- **Mostly, when talk about MAC, the multilevel security (MLS) policy is given as the example of this type of policy.**

MAC: Multilevel Security Policy

- The policy specifies whether a subject with a given clearance can read or write an object that has a given sensitivity.
- Example: the US Department of Defense multilevel security model classifies the security of their documents into four levels



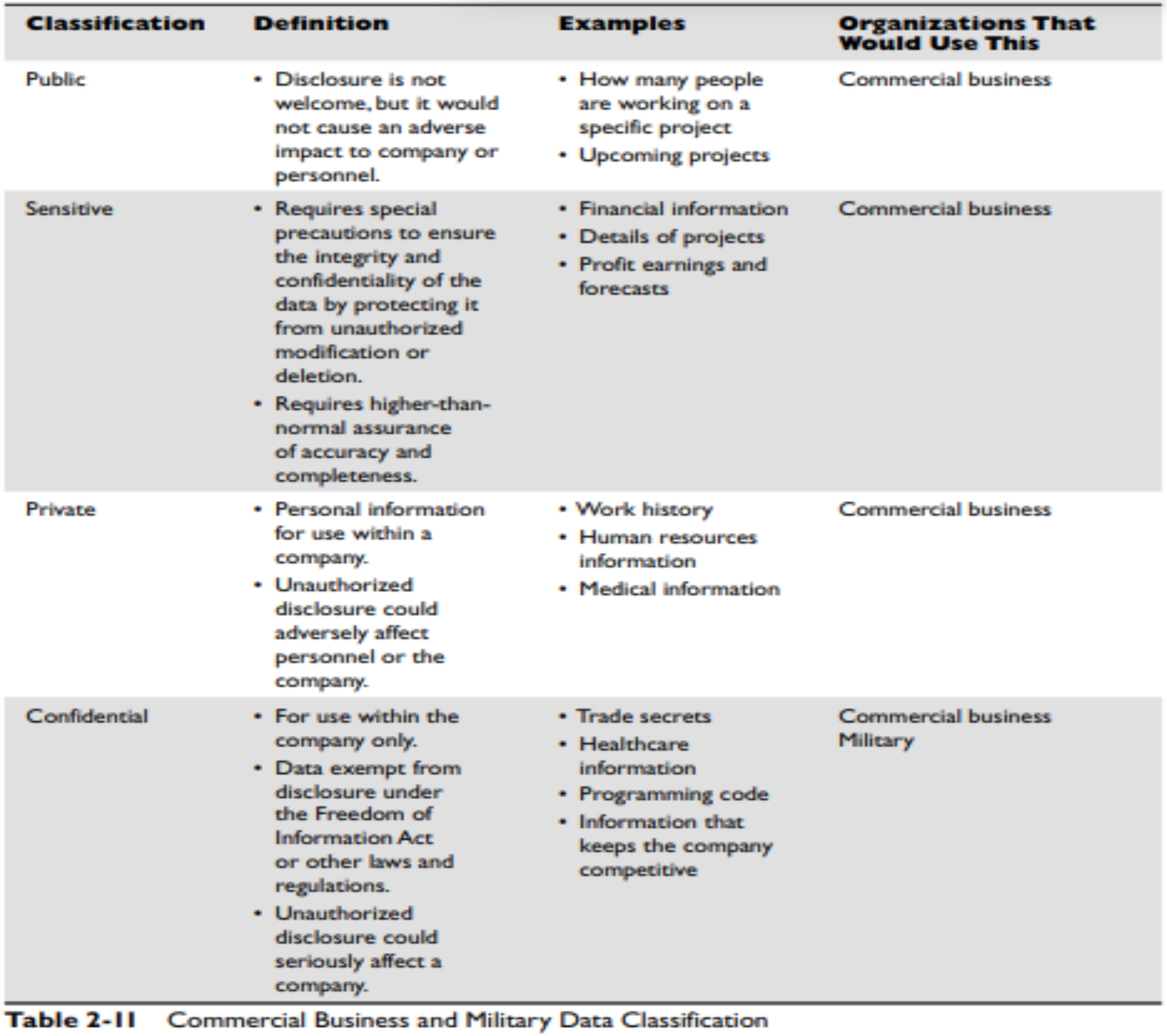
- Users are given various levels of clearance.
- Objects have different levels of sensitivity.
- The access rights of a subject to an object is determined based on these two parameters.
  - (clearance, sensitivity)



Classification	Definition	Examples	Organizations That Would Use This
Unclassified	• Data is not sensitive or classified.	• Computer manual and warranty information • Recruiting information	Military
Sensitive but unclassified (SBU)	• Minor secret. • If disclosed, it may not cause serious damage.	• Medical data • Answers to test scores	Military
Secret	• If disclosed, it could cause serious damage to national security.	• Deployment plans for troops • Nuclear bomb placement	Military
Top secret	• If disclosed, it could cause grave damage to national security.	• Blueprints of new wartime weapons • Spy satellite information • Espionage data	Military

Table 2-11 Commercial Business and Military Data Classification *(continued)*

- Confidential
- Private
- Sensitive
- Public



Classification	Definition	Examples	Organizations That Would Use This
Public	• Disclosure is not welcome, but it would not cause an adverse impact to company or personnel.	• How many people are working on a specific project • Upcoming projects	Commercial business
Sensitive	• Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion. • Requires higher-than-normal assurance of accuracy and completeness.	• Financial information • Details of projects • Profit earnings and forecasts	Commercial business
Private	• Personal information for use within a company. • Unauthorized disclosure could adversely affect personnel or the company.	• Work history • Human resources information • Medical information	Commercial business
Confidential	• For use within the company only. • Data exempt from disclosure under the Freedom of Information Act or other laws and regulations. • Unauthorized disclosure could seriously affect a company.	• Trade secrets • Healthcare information • Programming code • Information that keeps the company competitive	Commercial business Military

Table 2-11 Commercial Business and Military Data Classification

Lattice

- Lattice ซึ่งเป็นคุณสมบัติหนึ่งทางคณิตศาสตร์
- A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.
- **Definition**: A lattice $(L, \leq)$ consists of
  - a set L
  - and a partial order $\leq$
  - so that for every two elements $a, b \in L$ there exists:
    - A least upper bound $u \in L$.
    - A greatest lower bound $l \in L$.
- Formally:
  - $a \leq u$, $b \leq u$, and for all $v \in L : (a \leq v \wedge b \leq v) \rightarrow (u \leq v)$
  - $l \leq a$, $l \leq b$, and for all $k \in L : (k \leq a \wedge k \leq b) \rightarrow (k \leq l)$

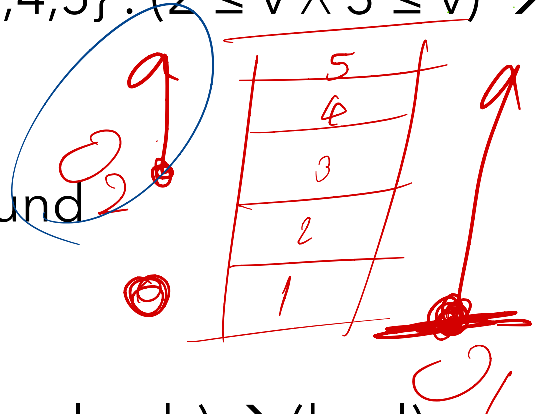
Properties of a lattice

- If a ≤ b, b dominates a.
    - Domination can be interpreted as meaning requiring a higher security level.
- If a ≤ b and b ≤ c then a ≤ c.
- If a ≤ b and b ≤ a then a = b.

Example of a lattice

- Let L={0,1,2,3,4,5}.
- a = 2, b = 3
- Find u (least upper bound)
  - a ≤ u, b ≤ u, and for all v ∈ L : (a ≤ v ∧ b ≤ v) → (u ≤ v)
  - 2 ≤ u,3 ≤ u and for all v ∈ {0,1,2,3,4,5} : (2 ≤ v ∧ 3 ≤ v) → (u ≤ v)
    - v ∈ {3,4,5}
    - u ≤ {3,4,5}, 2 ≤ u,3 ≤ u
    - u => u is the least upper bound
    - u = 3
- Find l (greatest lower bound)
  - l ≤ a, l ≤ b, and for all k ∈ L : (k ≤ a ∧ k ≤ b) → (k ≤ l)
  - l ≤ 2, l ≤ 3, and for all k ∈ {0,1,2,3,4,5} : (k ≤ 2 ∧ k ≤ 3)→ (k ≤ l)
    - k∈ {0,1,2}
    - {0,1,2} ≤ l
    - so l is the greatest lower bound.
    - l = 2

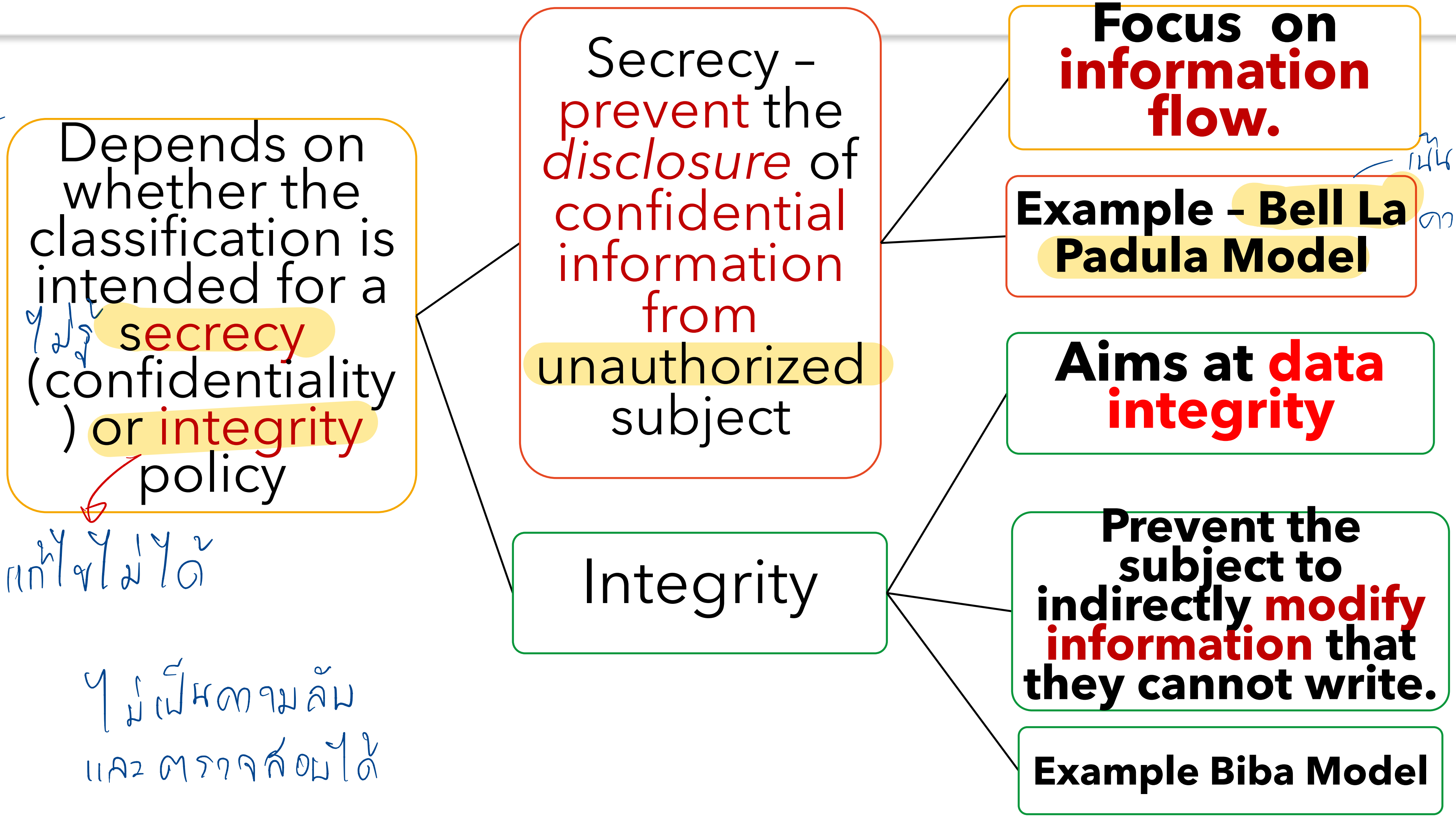
Least upper bound ตอบปัญหาของการมี object 2 objects subjects level ไหนขึ้นไป ถึงจะอ่าน object นี้ได้



Greatest lower bound ตอบปัญหาของการมี subject 2 subject object สูงสุด level ไหนที่เกินกว่านี้ไป แล้ว subject อ่านไม่ได้

0

Categories of multilevel security policies



Depends on whether the classification is intended for a secrecy (confidentiality) or integrity policy

Secrecy – prevent the *disclosure* of confidential information from unauthorized subject

Focus on information flow.

Example – Bell La Padula Model

Integrity

Aims at data integrity

Prevent the subject to indirectly modify information that they cannot write.

Example Biba Model

ความลับ คือ

ไม่รู้

รู้แต่ แก้ไขไม่ได้

ไม่เป็นความลับ
และตรวจสอบได้

เป็นเรื่อง
ความลับ

Confidential based policies' principles

- มีกฎพื้นฐานที่สำคัญอยู่ สอง กฎ คือ
  - No-read -up policy ไม่ให้ read object ที่อยู่สูงกว่า
    - A subject is allowed a read access to an object only if the access class of the subject dominates the access class of the object
  - No-write-down policy ไม่ให้ write ข้อมูลลง obj ที่ต่ำกว่า
    - A subject is allowed a write access to an object only if the access class of the subject is dominated by the access class of the object.

Confidential based policies' principles: no read up policy

- the read ability is only possible for subjects with a level higher or equal to that of the object level.
- เน้นที่ security level ของ sub (clearance)
- อนุญาตให้ read access ถ้า sub-clearance สูงกว่า หรือ อยู่ในระดับเดียวกับ obj-sensitivity
  - เช่น top secret sub อ่าน obj ของระดับต่ำกว่า ได้ทั้งหมด
  - Unclassified sub อ่าน obj ได้แค่ระดับ unclassified เท่านั้น
  - secret clearance subj อ่าน obj ได้ ระดับ
    - unclassified sensitivity, confidential sensitivity and unclassified sensitivity but not top secret sensitivity.
- SS property -> simple security property.
  - For subject S, object O, and authorization or ability A, with A = read, the subject S dominates the classification of the object O.

Confidential based policies' principles: no write down policy

- Sub อนุญาติให้เข้าถึง obj โดยการ write ได้ ถ้า access class ของ obj dominate access class ของ sub
  - เน้นที่ security level ของ obj
  - อนุญาตให้ write เฉพาะ sensitivity ของ obj สูงกว่า หรือ อยู่ในระดับเดียว กับ clearance ของ obj
    - Sub ระดับ top secret clearance write ได้เฉพาะ obj ระดับ top secret sensitivity เท่านั้น
    - Sub ในระดับ unclassified clearance สามารถ write ได้ทั้งหมด
    - Sub ในระดับ confidentiality clearance write ได้ obj แต่ confidentiality sensitivity ขึ้นไป
  - * property -> star property

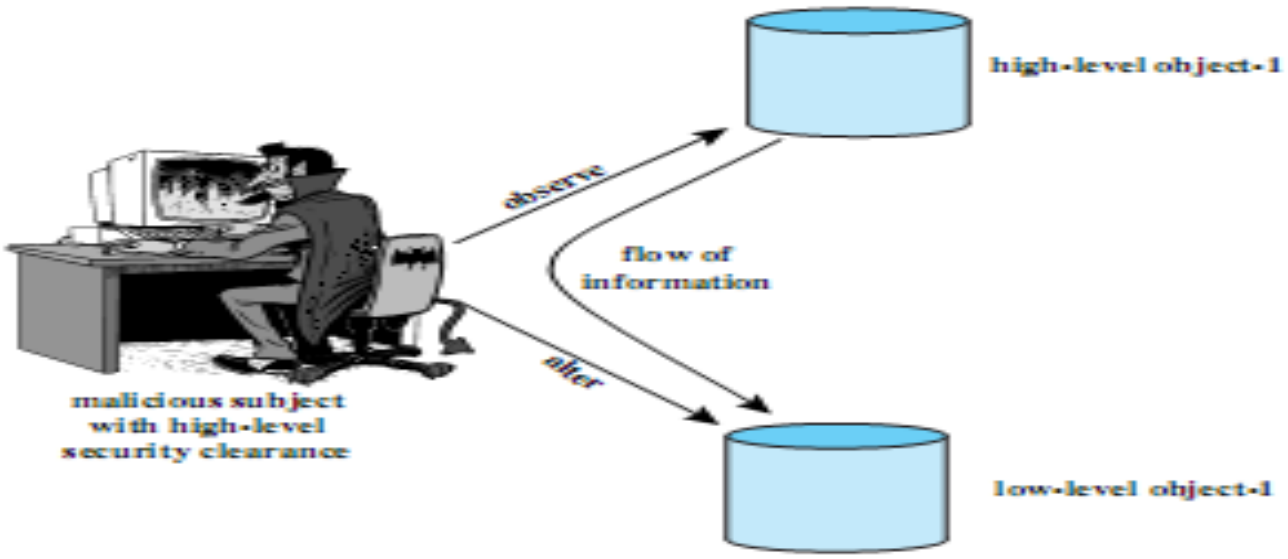
เซ็นเอกสารส่งให้สิทธิที่สูงกว่า

star property (*)

Hacker นำ data ไปใส่ใน สิทธิ์ที่ต่ำกว่า
เพื่อลบร่องรอยการแฮก

No Write Down

- For subject S, object O, and authorization or ability A, where A = writing, the subject S is *dominated by* the object O.



http://www.computing.dcu.ie/~dobrien/ca647/lectures/pdf/lecture17/lecture17_4.pdf

Problems with the * – property

- เมื่อ ห้าม write down แล้วถ้า
- How can high ranking subjects pass any information to lower level subjects?
  - One way is to allow subjects to operate at lower ranks.
  - Another is to identify trusted subjects which are allowed to violate the * – property.

Integrity based policies principle

- The mandatory policy that we have discussed above protects only the confidentiality of the information
  - No control is enforced on its integrity.
  - Low classified subjects could still be able to enforce improper indirect modification to objects they cannot write. Sub สามารถทำการ modify obj ที่ไม่สามารถ write ได้
- Like for secrecy, each subject and object is assigned an integrity classification.
- detail see in Biba Model.

The real model: Multilevel security policy

Confidentiality based security policy

- Bell La Padula Model

Integrity based security policy

- Biba model

Other models

Bell-LaPadula Model (BLP)

- The Bell-LaPadula Model (1973, 1975) is a multilevel security model which works by specifying allowable paths of information flow in a secure system.
- This is an important model when a system/machine has to concurrently handle data at different sensitivity levels.
  - For example, a machine processing confidential and top-secret files at the same time.
- Focuses on Data Confidentiality and access to classified information

3 properties

ss property

* property

ds property

BLP properties

- As a whole the properties are designed to protect against unauthorized disclosure of information.
    - 2 mandatory properties
        - No read up – ss property
            - A subject can only read an object of less or equal security level
        - No write down - * property
            - A subject can only write into an object of greater or equal security level
- 1 discretionary property
    - ds property
        - This is designed to capture the idea that permission may be passed from an authorised subject to another subject.

Biba Integrity Model

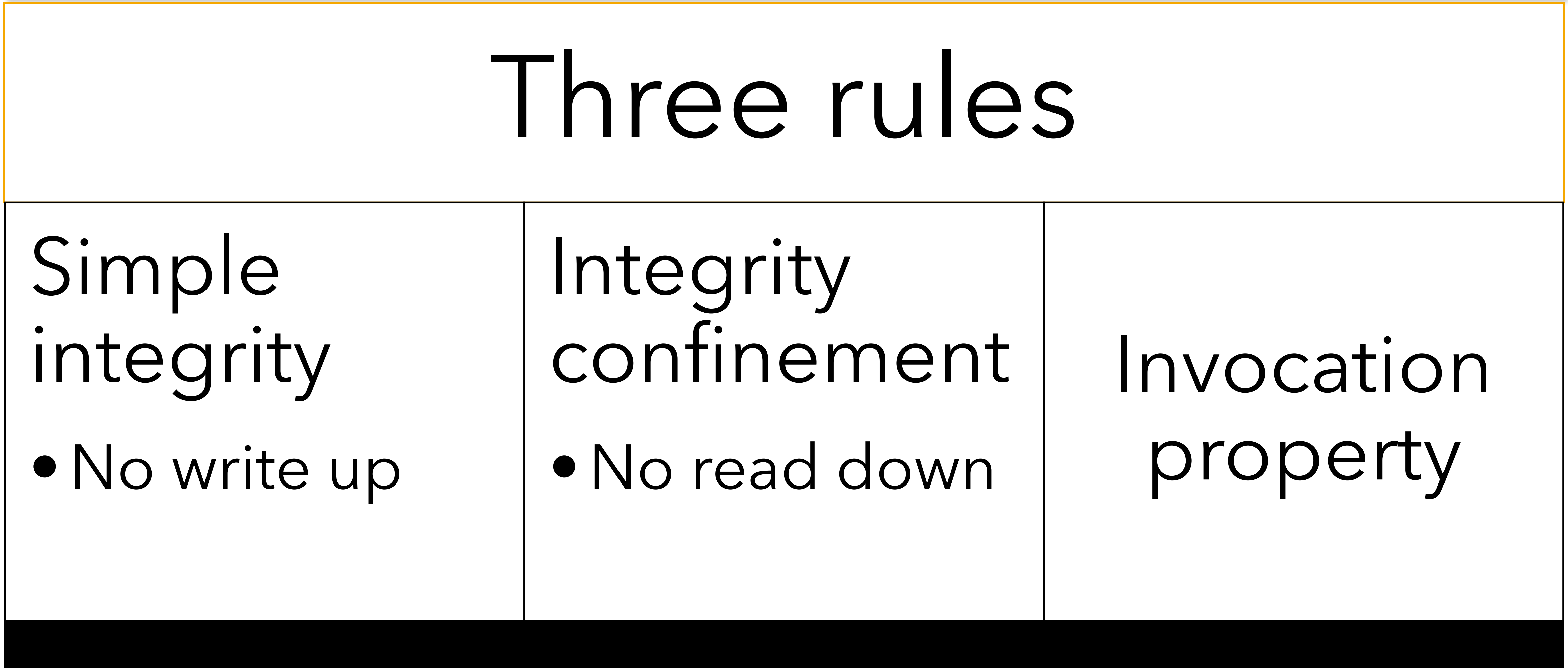
- Concerned with **unauthorized modification of data**.
- Deal with the case in which
  - there is data that must be visible to users at multiple or all security levels
  - but should only be modified in controlled ways by authorized agents.
  - เนื่องจากในบางระบบ ข้อมูลไม่ได้เป็นความลับ ต่อ ผู้ใช้ในระดับต่างๆ
  - แต่สิ่งที่ต้องการ คือ ผู้ที่จะทำการ แก้ไขข้อมูลเหล่านั้นได้จะต้องเป็น ผู้ที่ได้รับอนุญาติในการแก้ไข
- Has the same structure (component) as BLP model.
  - S,O, A, (L, $\leq$)

Different access mode

- The access modes can be extended to include an Invoke instruction:
- {Modify (Write), Observe (Read), Execute, Invoke (subject to subject communication/use)}
- The rules to provide the appropriate policies are, in some sense, the reverse (or dual) of those for BLP.
  - "No write up, no read down!"
- This policy is used in the static version of the Biba model, but not in the dynamic version which we won't consider in detail.
- Biba is important now because of it's use in Vista.

หน้า 84-89_ไม่ออกข้อสอบค่ะ แต่สอน
;)

The policy is based on these three rules



Three rules

Simple integrity

- No write up

Integrity confinement

- No read down

Invocation property

Simple integrity

- A subject can modify an object only if
  - the integrity level of the subject dominates the integrity level of the object
- This is the no write up policy.
- Integrity is to do with how much you can rely on something.
  - If A, as a process say, is trusted less then B as a resource, then B should not be modified on the basis of A.
  - We shouldn't contaminate B.

Integrity confinement

- A subject can read an object only if
  - the integrity level of the subject is dominated by the integrity level of the object.
- This is the **no read down** policy.
- Effectively this means a subject doesn’t trust information with a lower integrity level, so it shouldn’t even be influenced by it.
  - Juries in court cases are sometimes told to disregard something that has been said, or to ignore some evidence.
    - Humans tend to take information into account whether they have been told to disregard it or not.
    - The **no read down** means the jury would never see the untrustworthy evidence.

Invocation property

- A subject S_1 can invoke/execute/use another subject S_2 only if
  - the integrity level of S_1 dominates the integrity level of S_2.
  - In other words, a process cannot use a process or entity that has higher integrity than it does.

Other Models

No read Up
No read Down } ลำบากจัด

Confidential Model

Ex. The Harrison-Ruzzo-Ullman Model

- addresses some of the shortcomings of BLP, in particular,
  - how to create and delete files, and how to change access rights.

Integrity Model

Ex. Clark Wilson Model

- Clark-Wilson is another integrity based access model.
- Aims for commercial applications.
- many of the earlier access control models were driven by the military.
- Appeared as the paper : "A Comparison of Commercial and Military Computer Security Policies."

Mix Model

- Ex. Chinese Wall Model

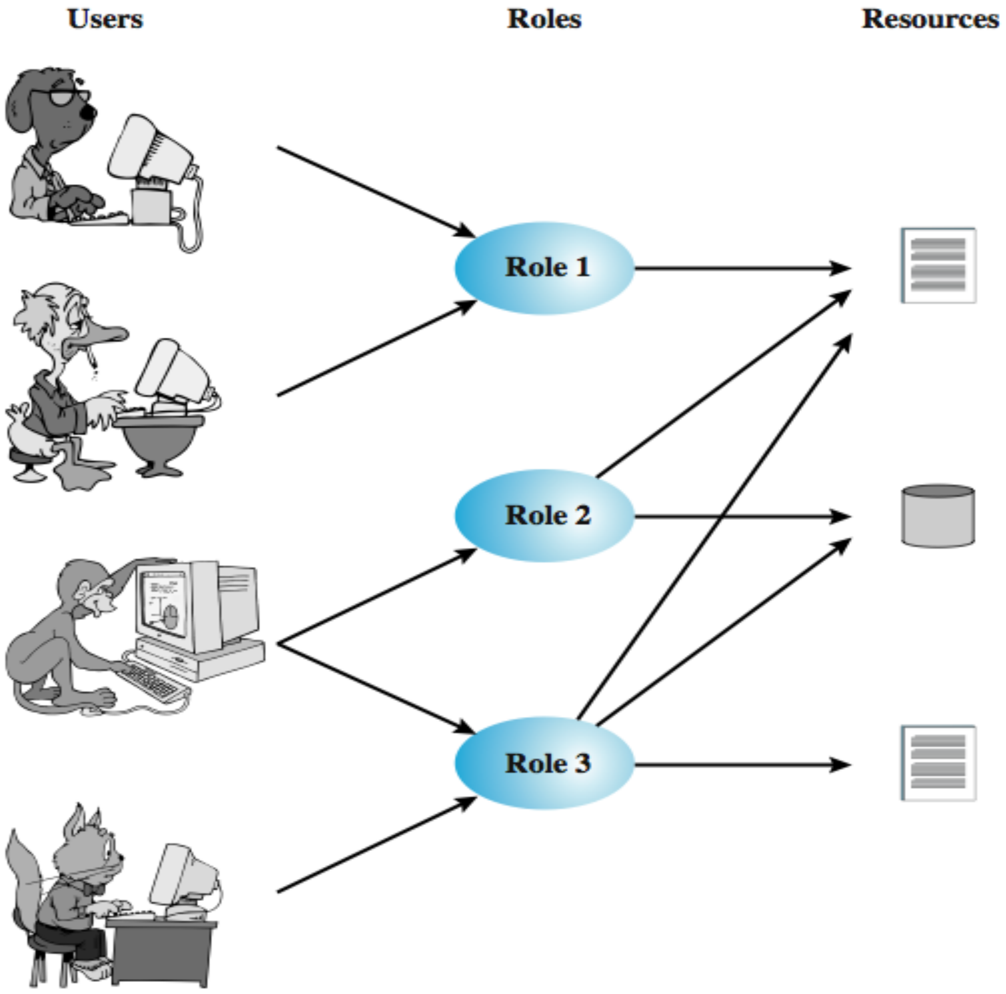
Role-Based Access Control

RBAC based on roles ของผู้ใช้ในระบบไม่ใช่ the user's identity.

Access right จะถูกกำหนดตาม role

ความสัมพันธ์ระหว่าง ผู้ใช้ กับ role

- Many to many



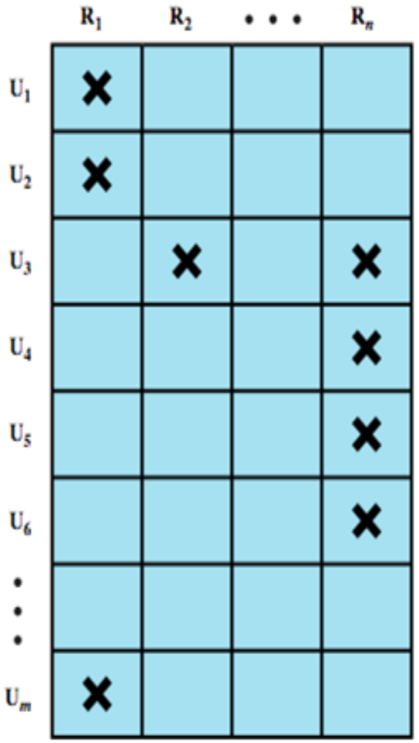
Role-Based Access Control

เราสามารถใช้ access matrix ในการช่วยกำหนด key elements ของแต่ละ Role

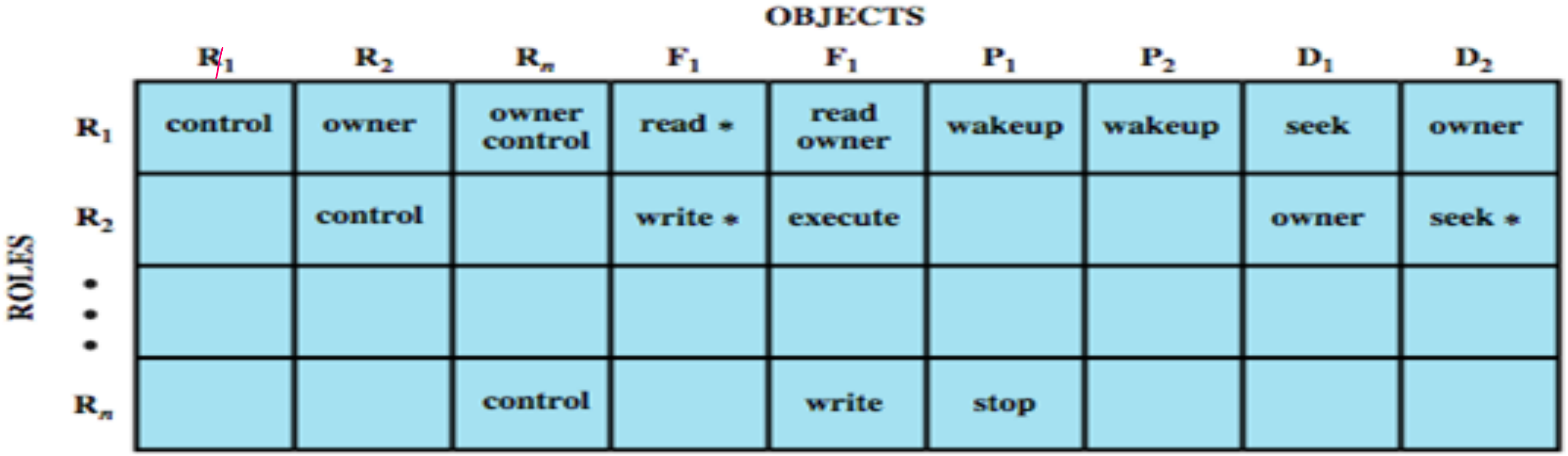
RBAC lends itself to an effective implementation of the principle of least privilege.

Each role should contain

- the minimum set of access rights needed for that role.
- A user is assigned to a role that enables him or her to perform only what is required for that role. Multiple users assigned to the same role, enjoy the same minimal set of access rights.



	R_1	R_2	• • •	R_n
U_1	✗			
U_2	✗			
U_3		✗		✗
U_4				✗
U_5				✗
U_6				✗
⋮				
U_m	✗			



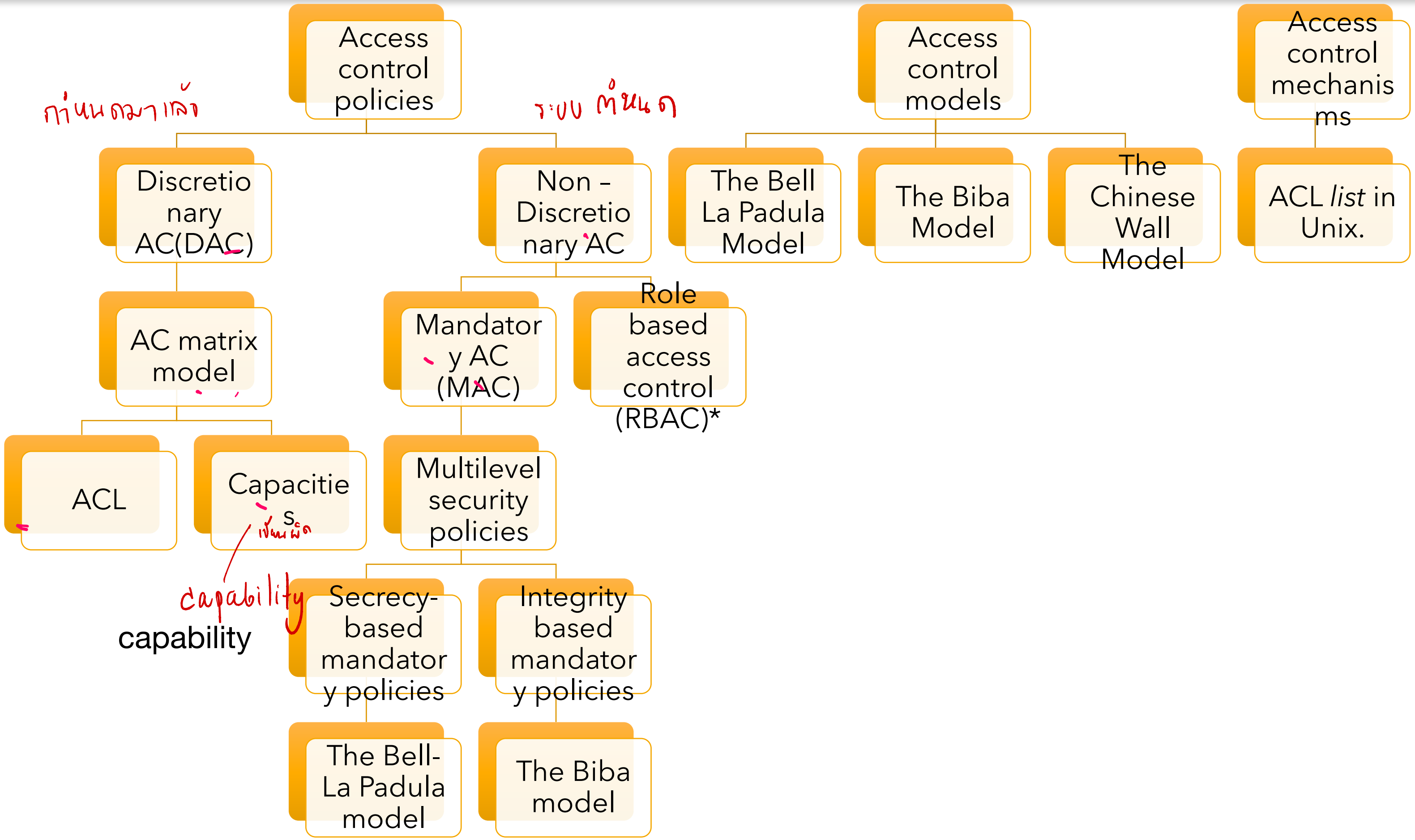
OBJECTS

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			

Summary: AC policies Vs AC mechanisms Vs AC models

- High level requirement that specifies
  - How access is managed
  - Who, under what circumstances may access what inforation.
- Can be application-specific
  - Thus taken into consideration by the application vendor.
- Pertain the user actions within the context of an organizational unit or across organizational boundaries.
- Enforced through a *mechanism.*
  - *Implementation level.*
- Access control model bridges the gab between the policy and mechanism.

Summary of AC system



Access control policies

กำหนดมาแล้ว

Discretionary AC(DAC)

AC matrix model

ACL

Capacities

เขียนผิด

capability

capability

ระบบ กำหนด

Non - Discretionary AC

Mandatory AC (MAC)

Multilevel security policies

Secrecy-based mandatory policies

The Bell-La Padula model

Integrity based mandatory policies

The Biba model

Role based access control (RBAC)*

Access control models

The Bell La Padula Model

The Biba Model

The Chinese Wall Model

Access control mechanisms

ACL *list* in Unix.

References:

- [1] CSCI262 Lecture Notes by Dr. Luke McEvan, University of Wollongong Australia.
- [2] Computer Security: Principles and Practice, W. Stalling and L. Brown, 1st edition, Pearson Education, 2008.
- [3] Computer Security, D. Gollman. 2nd edition, John Wiley & Sons, 2006.
- [4] Wikipedia.org

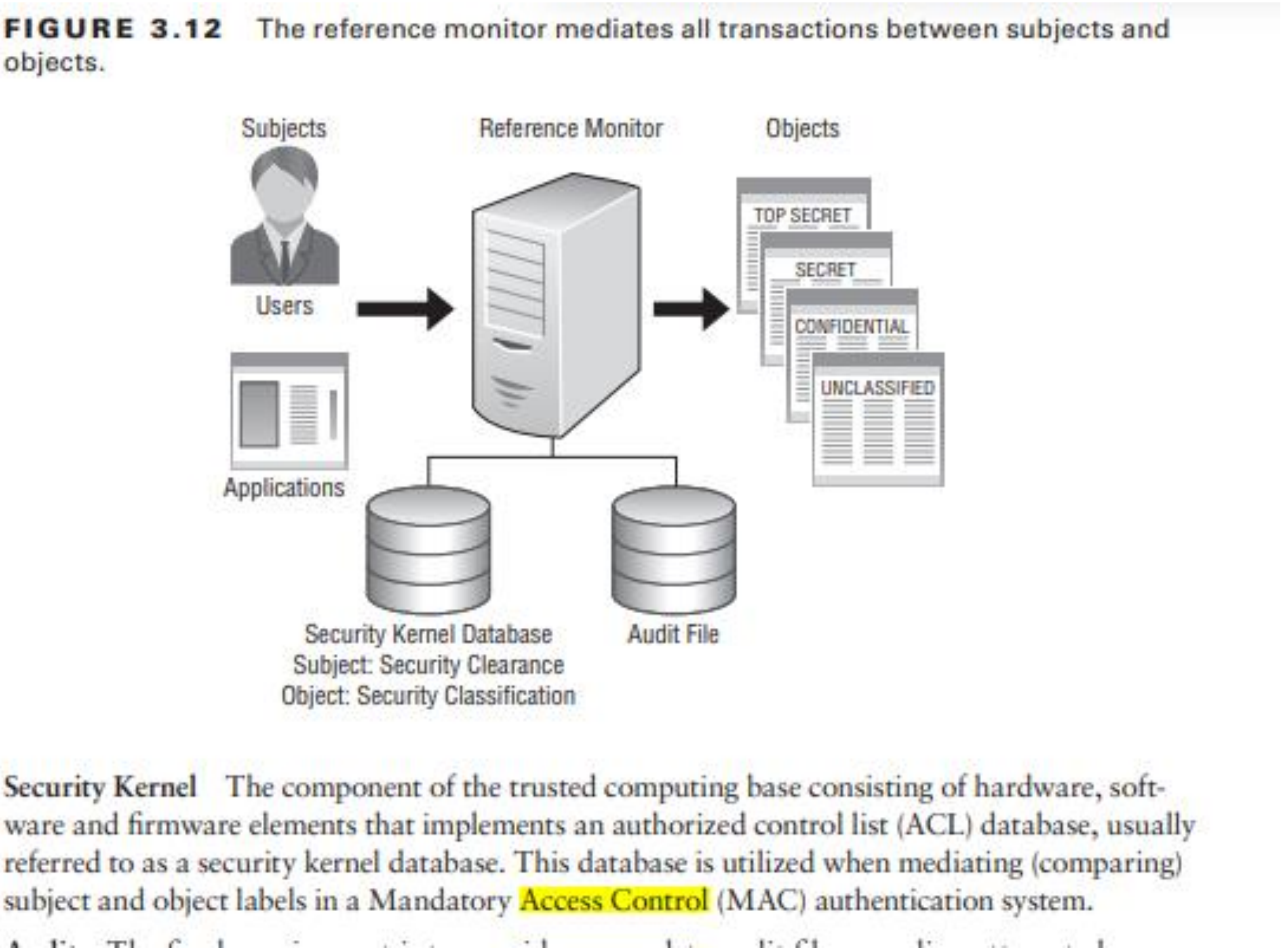


FIGURE 3.12 The reference monitor mediates all transactions between subjects and objects.

Subjects
Reference Monitor
Objects
Users
Applications
TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED
Security Kernel Database
Subject: Security Clearance
Object: Security Classification
Audit File

Security Kernel The component of the trusted computing base consisting of hardware, software and firmware elements that implements an authorized control list (ACL) database, usually referred to as a security kernel database. This database is utilized when mediating (comparing) subject and object labels in a Mandatory Access Control (MAC) authentication system.