

See this video while <https://www.youtube.com/watch?v=kd33UVZhnAA>

# Lecture <sup>5</sup>~~4~~: Access Control Ep.1

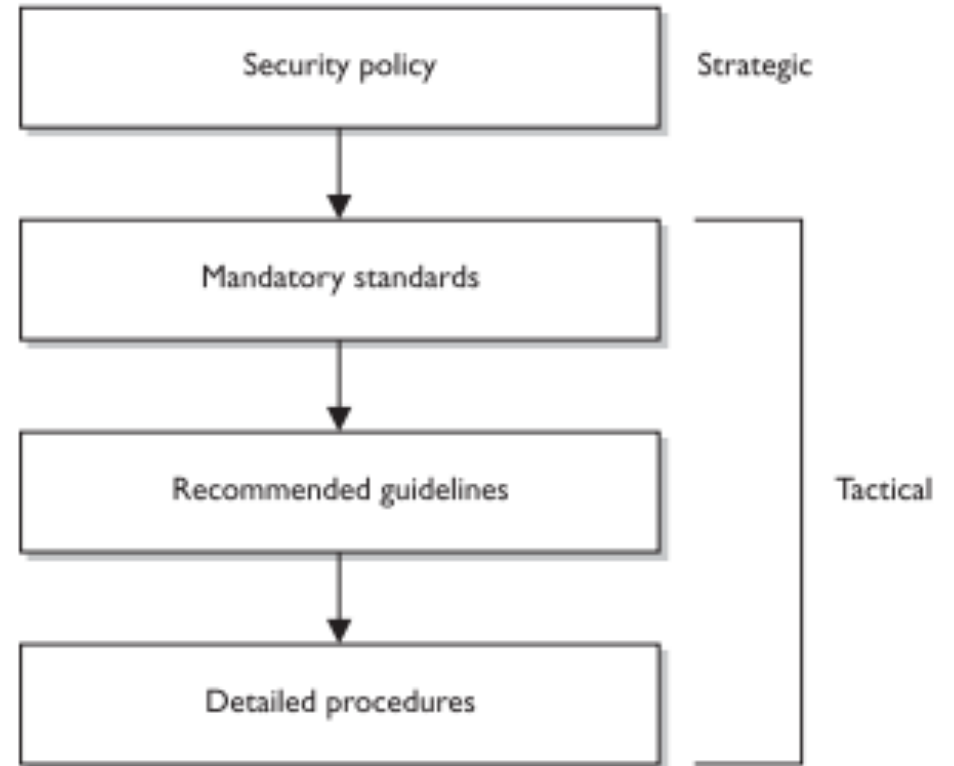
05506044 System Security

Dr. Rungrat Wiangsripanawan

# Additional Slice about Control: Policy

**Figure 2-13**

Policy establishes the strategic plans, and the lower elements provide the tactical support.



กรรมสิทธิ์ คือ ~

# 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.



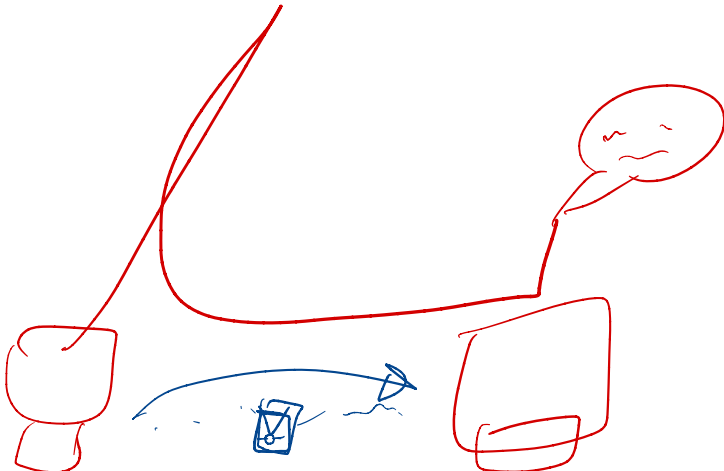
SYSTEM

User

Administrators

} User ใช้งานผ่าน 11 ตัวที่ต่าง 11 แอปพลิเคชัน

เพราะ ใช้งานผ่าน User 1 ชื่อ 4 คน ใช้งานผ่าน 11 ตัว



# Security label คืออะไร

เมื่อ subject มีการ  
request access

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



**security server** ใน  
environment เดียวกับ  
object จะทำการ

- เปรียบเทียบ **label** ของ  
**sub** ที่ร้องขอ กับ  
**object label\***

- ใช้ policy rules (แล้วแต่  
จะเลือก) เพื่อตัดสินใจจะ

อนุญาต หรือ ปฏิเสธ

\*\*\*แต่ละ obj จะมี label ของ  
มันเช่นกัน

# Multilevel security

Sensitive Info - Biometric, ๑๙๗๓, ๒๐๑๘

- ทั้ง *sub* และ *obj* จะต้องมียุทธศาสตร์ *security label* ซึ่ง label ของ *sub* และ *obj* จะเป็นคนละชนิด
- subjects labels => clearances, ใข้รหัสนี้ ๑๐ ๑๙๗๓
- objects labels => classifications or sensitivity
  - every action/operation has a sensitivity rating (like top secret).
- Multilevel Security label เหมาะกับ องค์การหรือระบบที่แบ่งการเข้าถึงข้อมูลเป็นลำดับชั้น เช่น
  - Military organizations. ๑๙๗๓ ๑๙๗๓ ๑๙๗๓
  - Banks. — เป็นห้องสอง
- 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? (ใครเป็นคนกำหนดว่าใครทำอะไรได้)
- เจ้าของ object หรือ ระบบ ???



# Access Control Policies:

## Discretionary Access:

ผู้ใช้ที่เป็นเจ้าของ obj เป็นคนกำหนดว่าใครจะเข้าถึงอะไรได้บ้าง *ex. Facebook*

## 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.** *เป็นต้งกำหนด*

# ประเภทของ Access Control Policies

(DAC) Discretionary Access Control

- **Users** decide how they want to protect their asset files

(MAC)

- **The system decides.**

(RBAC)

- **The system decides.**

# Discretion access control (DAC)

- *A discretionary access control (DAC) policy is a means of assigning access rights based on rules specified by users.*
- 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.

# 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

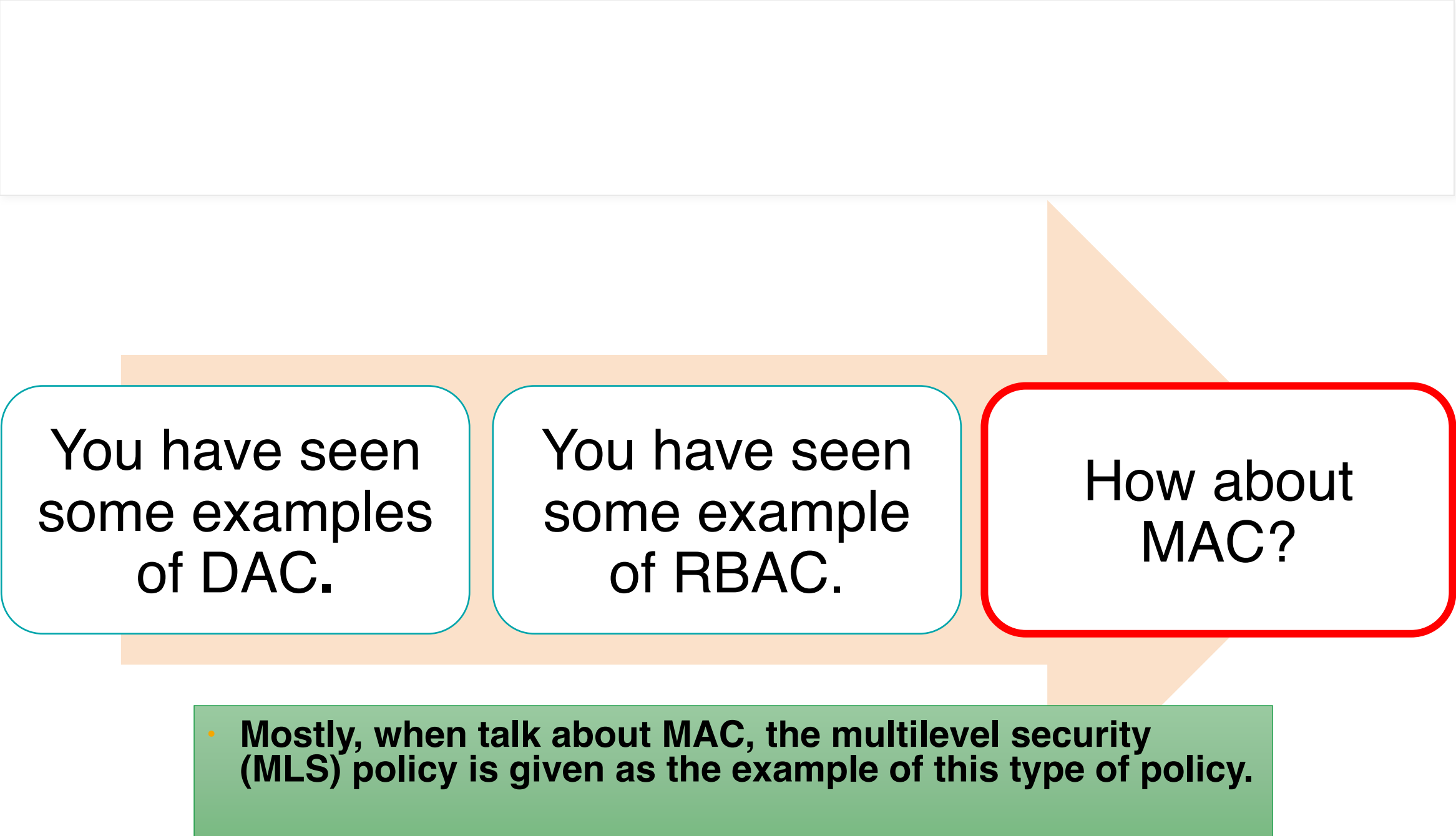
- is the **multi-level security policy**

# Role based access control Policy

system decides

roles are  
assigned  
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

• ขอบบน  
Upper Bound      • ขอบล่าง  
Lower Bound

- 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)

# Lattice

$S_1 \Rightarrow \text{Confidential}$   
 $S_2 \Rightarrow \text{Secret}$

$\left. \begin{array}{l} \text{Confidential} \\ \text{Secret} \end{array} \right\} \begin{array}{l} \text{Confidential} \\ \text{Unclassified} \end{array}$

$O_1 = \text{top Secret}$   
 $O_2 = \text{Confidential}$

- 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  $k \in L : (k \leq a \wedge k \leq b) \rightarrow (k \leq l)$

Cryptography  $\left[ \begin{array}{l} \text{Hard Problem} \\ \text{Hard to Hack} \end{array} \right.$

ทยไป 10 นาทีก็แก้ไม่ได้



# Properties of a lattice

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

# Example of a lattice

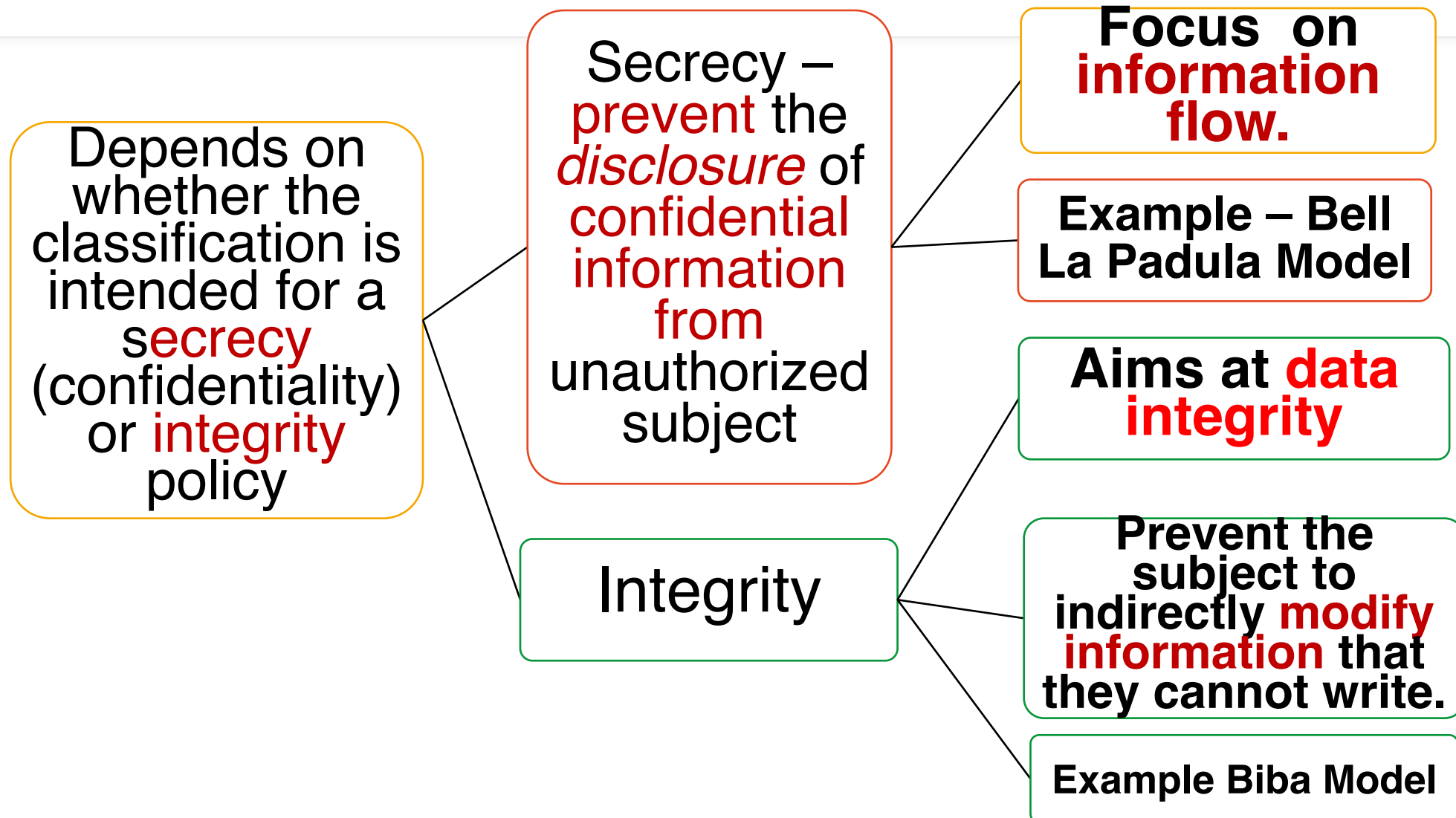
อาจารย์เขียนถูกไหม

- Let  $L = \{0, 1, 2, 3, 4, 5\}$ .
- $a = 2, b = 3$
- Find  $u$  (least upper bound)
  - $a \leq u, b \leq u$ , and for all  $v \in L : (a \leq v \wedge b \leq v) \rightarrow (u \leq v)$
  - $2 \leq u, 3 \leq u$  and for all  $v \in \{0, 1, 2, 3, 4, 5\} : (2 \leq v \wedge 3 \leq v) \rightarrow (u \leq v)$ 
    - $v \in \{3, 4, 5\}$
    - $u \leq \{3, 4, 5\}, 2 \leq u, 3 \leq u$
    - $u \Rightarrow u$  is the least upper bound
    - $u = 3$
- Find  $l$  (greatest lower bound)
  - $l \leq a, l \leq b$ , and for all  $k \in L : (k \leq a \wedge k \leq b) \rightarrow (k \leq l)$
  - $l \leq 2, l \leq 3$ , and for all  $k \in \{0, 1, 2, 3, 4, 5\} : (k \leq 2 \wedge k \leq 3) \rightarrow (k \leq l)$ 
    - $k \in \{0, 1, 2\}$
    - $\{0, 1, 2\} \leq l$
    - so  $l$  is the greatest lower bound.
    - $l = 2$

**Least upper bound** ตอบปัญหา  
ของการมี object 2 objects subjects  
level ไหนขึ้นไป ถึงจะอ่าน object นี้  
ได้

**Greatest lower bound** ตอบปัญหา  
ของการมี subject 2 subject object  
สูงสุด level ไหนที่เกินกว่านี้ไป แล้ว  
subject อ่านไม่ได้

# Categories of multilevel security policies



# 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

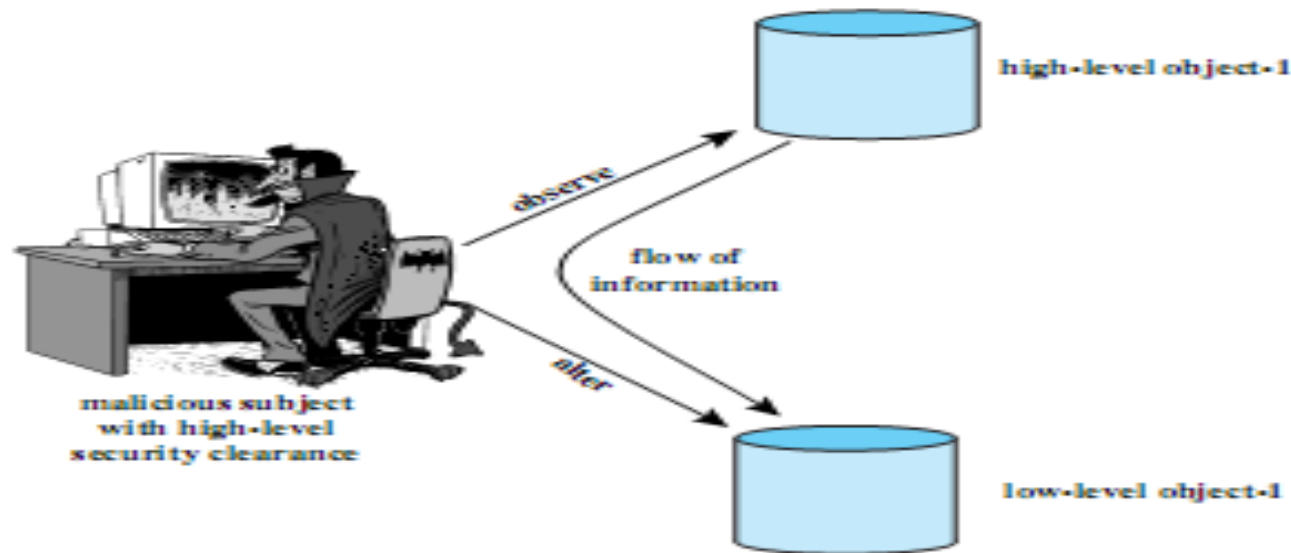
- the **read ability** is only possible for **subjects** with a level **higher or equal** to that of the **object level**.
- เน้นที่ security level ของ sub (clearance)
- อนุญาตให้ read access ถ้า sub-clearance สูงกว่า หรือ อยู่ในระดับเดียวกับ obj-sensitivity
  - เช่น top secret sub อ่าน obj ของระดับต่ำกว่า ได้ทั้งหมด
  - Unclassified sub อ่าน obj ได้ แค่ระดับ 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 อนุญาตให้เข้าถึง 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

# star property (\*)

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



## 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

- **Bell La Padula Model**

- **Biba model**

# 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



# 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 ผู้ที่ได้รับอนุญาตในการแก้ไข
- 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 its use in Vista.

หน้า 84-89\_ไม่ออกข้อสอบค่ะ  
แต่สอน ;)

The policy is based on these three rules

## Three rules

--	--	--

# 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 than 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

**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**

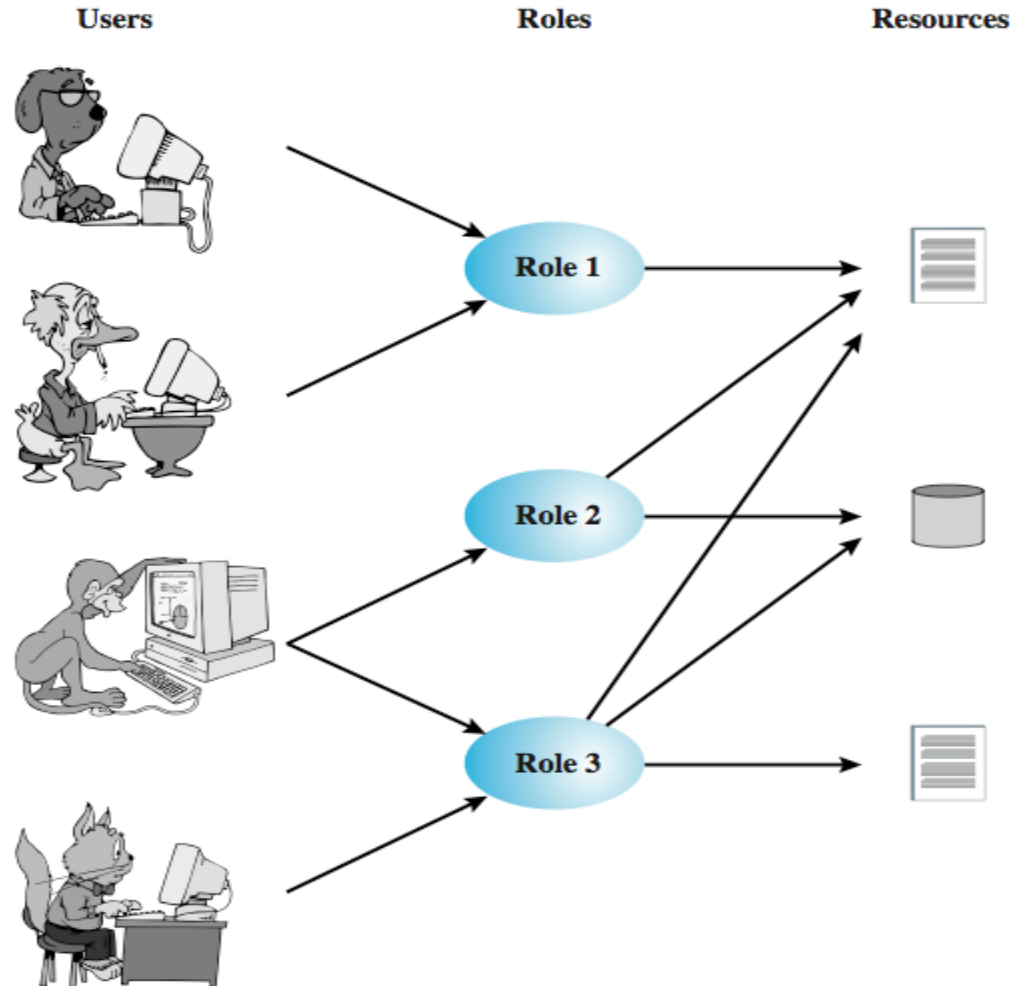
- Clark-Wilson is another integrity based access model.
- Aims for **commercial applications**.
- many of the earlier access control models were driven by the military.
- Appeared as the paper : “A Comparison of Commercial and Military Computer Security Policies.”

**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

	R <sub>1</sub>	R <sub>2</sub>	...	R <sub>n</sub>
U <sub>1</sub>	×			
U <sub>2</sub>	×			
U <sub>3</sub>		×		×
U <sub>4</sub>				×
U <sub>5</sub>				×
U <sub>6</sub>				×
⋮				
U <sub>m</sub>	×			

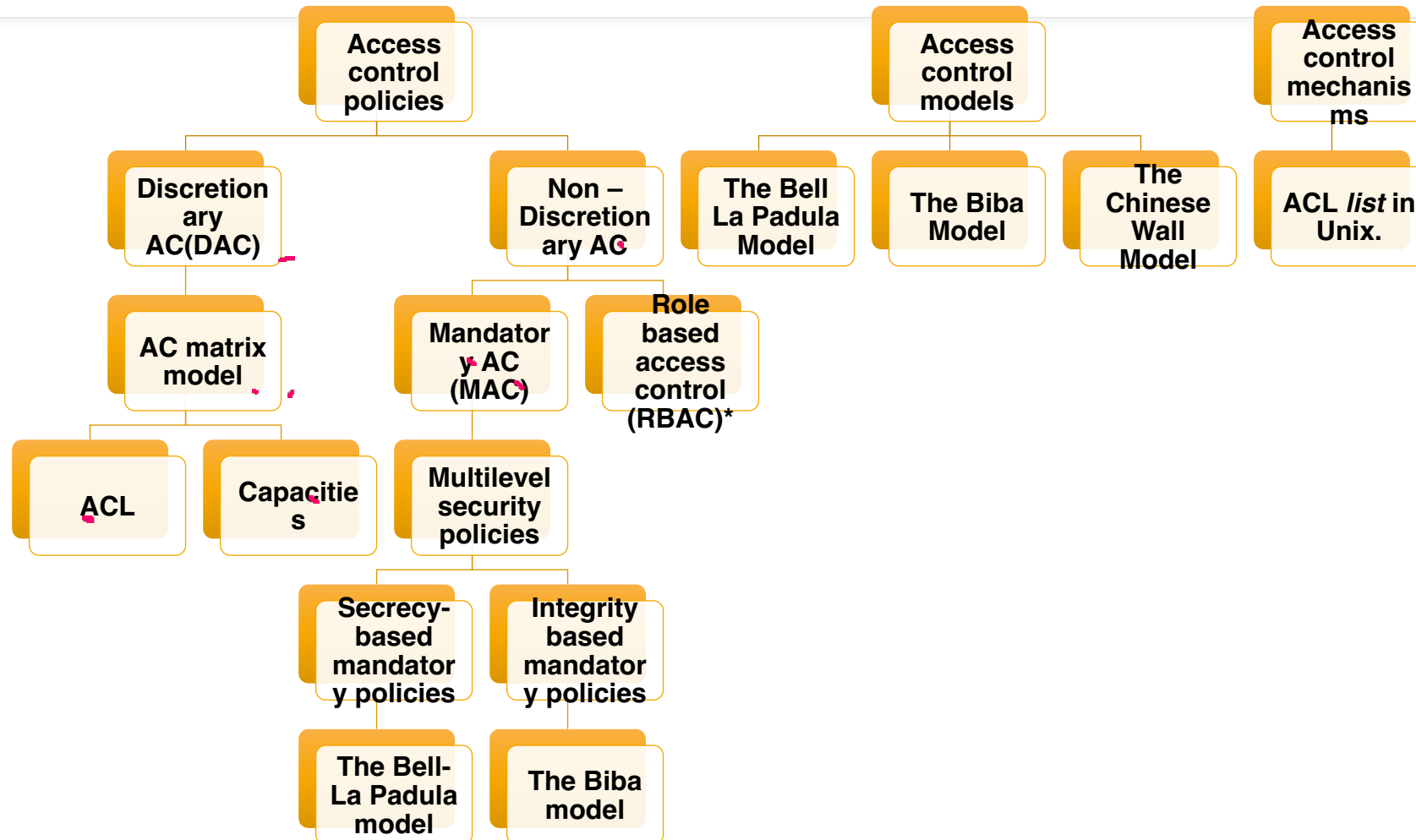
- เราสามารถใช้ access matrix ในการช่วยกำหนด key elements ของแต่ละ Role
- RBAC lends itself to an effective implementation of the **principle of least privilege**. Each role should contain the minimum set of access rights needed for that role. A user is assigned to a role that enables him or her to perform only what is required for that role. Multiple users assigned to the same role, enjoy the same minimal set of **access rights**.

		OBJECTS								
		R <sub>1</sub>	R <sub>2</sub>	R <sub>n</sub>	F <sub>1</sub>	F <sub>1</sub>	P <sub>1</sub>	P <sub>2</sub>	D <sub>1</sub>	D <sub>2</sub>
ROLES	R <sub>1</sub>	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R <sub>2</sub>		control		write *	execute			owner	seek *
	⋮									
	R <sub>n</sub>			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 information.
- 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 gap between the *policy* and *mechanism*.

# Summary of AC system



# 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



- Confidential
- Private
- Sensitive
- Public

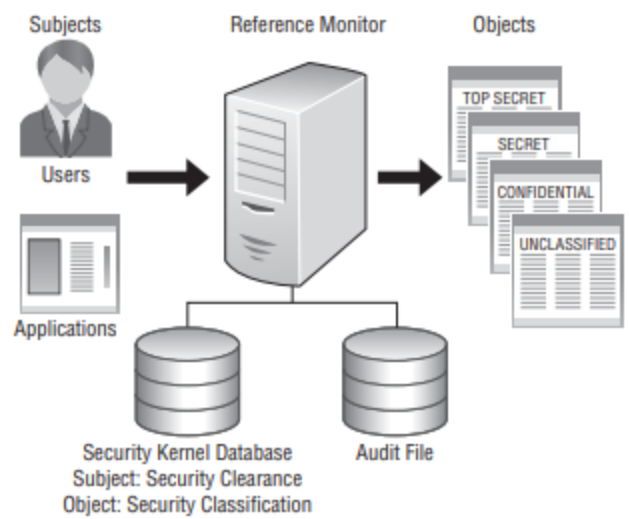
Classification	Definition	Examples	Organizations That Would Use This
Public	<ul style="list-style-type: none"> <li>Disclosure is not welcome, but it would not cause an adverse impact to company or personnel.</li> </ul>	<ul style="list-style-type: none"> <li>How many people are working on a specific project</li> <li>Upcoming projects</li> </ul>	Commercial business
Sensitive	<ul style="list-style-type: none"> <li>Requires special precautions to ensure the integrity and confidentiality of the data by protecting it from unauthorized modification or deletion.</li> <li>Requires higher-than-normal assurance of accuracy and completeness.</li> </ul>	<ul style="list-style-type: none"> <li>Financial information</li> <li>Details of projects</li> <li>Profit earnings and forecasts</li> </ul>	Commercial business
Private	<ul style="list-style-type: none"> <li>Personal information for use within a company.</li> <li>Unauthorized disclosure could adversely affect personnel or the company.</li> </ul>	<ul style="list-style-type: none"> <li>Work history</li> <li>Human resources information</li> <li>Medical information</li> </ul>	Commercial business
Confidential	<ul style="list-style-type: none"> <li>For use within the company only.</li> <li>Data exempt from disclosure under the Freedom of Information Act or other laws and regulations.</li> <li>Unauthorized disclosure could seriously affect a company.</li> </ul>	<ul style="list-style-type: none"> <li>Trade secrets</li> <li>Healthcare information</li> <li>Programming code</li> <li>Information that keeps the company competitive</li> </ul>	Commercial business Military

**Table 2-II** Commercial Business and Military Data Classification

# 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.



Organizations That Would Use This
Military
Military
Military
Military
• Espionage data

**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.

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