user เช่น สิทธิ์ ไม่ต้องทำ action เพื่อให้ user แต่จำกัดขอบเขตการใช้งาน user ๆ

* Privilege Escalator

Lecture 4: Access Control Ep.1

05506044 System Security

Dr. Rungrat Wiangsripanawan

privilege escalation

Additional Slide about Biometric

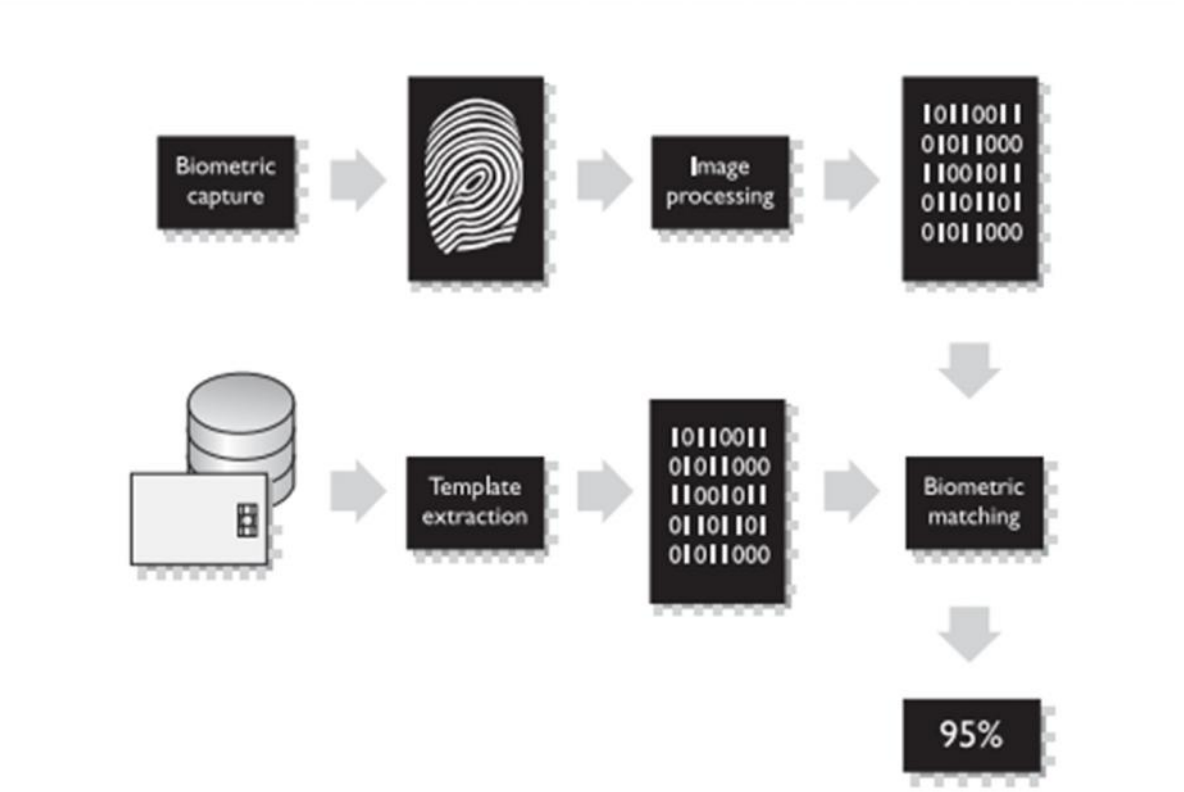
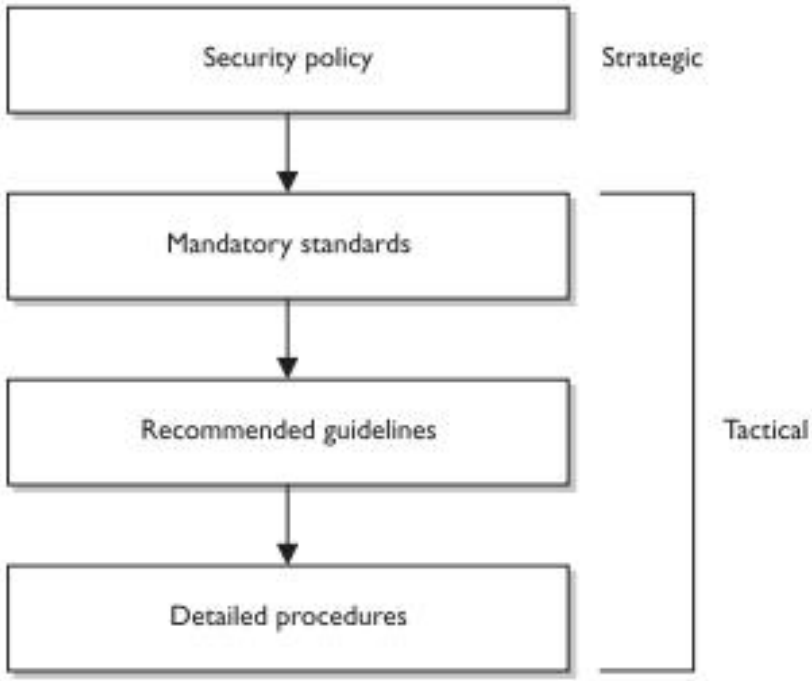


Figure 3-9 Biometric data is turned into binary data and compared for identity validation.

Additional Slice about Control: Policy

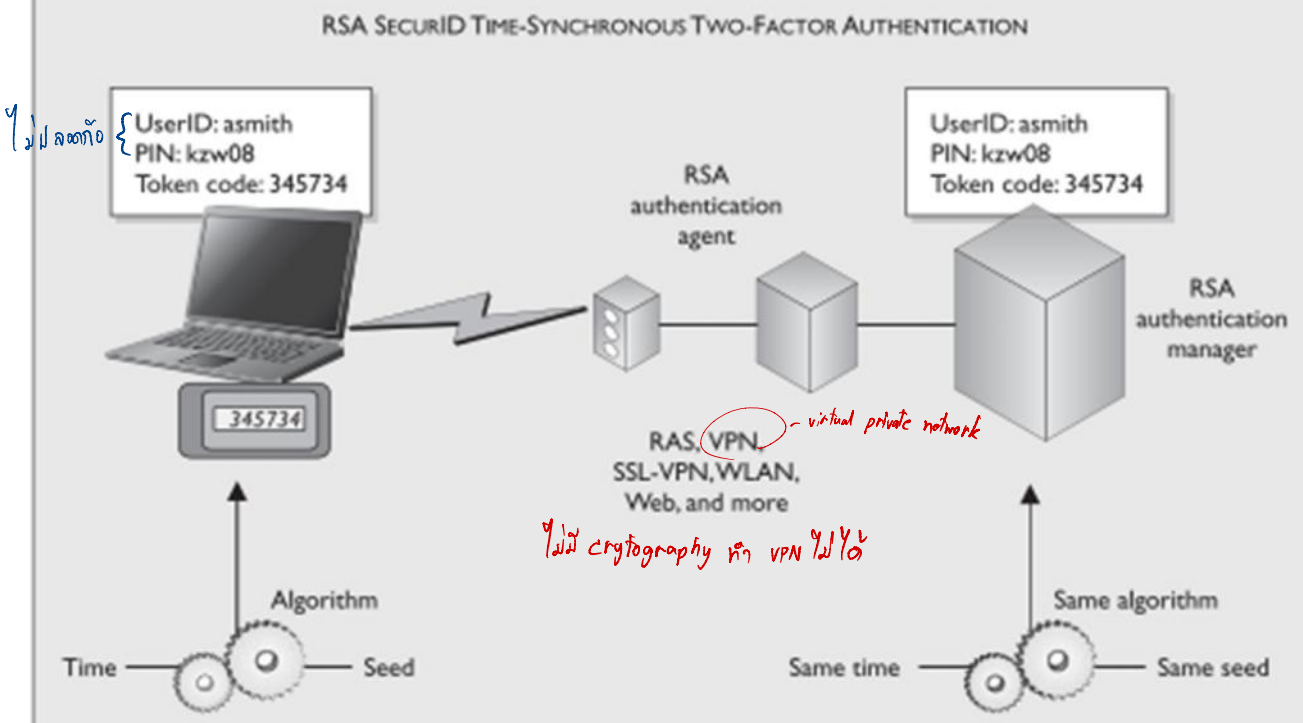
Figure 2-13
Policy establishes the strategic plans, and the lower elements provide the tactical support.



Additional Slide about Time-based Token

SecurID

SecurID, from RSA Security, Inc., is one of the most widely used time-based tokens. One version of the product generates the one-time password by using a mathematical function on the time, date, and ID of the token card. Another version of the product requires a PIN to be entered into the token device.



Objectives

Understand and being able to explain

- Differences of Identification/Authentication/Access control and Accountability
- Principle of access control
- Access Control Components
- Access Control Matrix
- Capablilities, Access Control List

Explain = Know meaning and can give Examples

ควบคุมการเข้าถึงจาก requiremet ร่วมกับการใช้ authetication

- Access control Control access to assets based on business requirements, user management, authentication methods, and monitoring
- One of the first line of defenses…

Access Control (การควบคุมการเข้าถึง) [2]

- ITU-T Recommendation X.800 defines access control as
  - prevention of unauthorized use of a resource และ ไม่ใช่ user ในระบบ
  - prevention of use of a resource in an unauthorized manner" เป็น user ในระบบ แต่ไม่มีสิทธิ์เข้าถึงข้อมูลที่กำหนด
- Recall: Computer Security principal objectives
  - prevent unauthorized users from gaining access to resources, ป้องกันผู้ใช้ที่ไม่ได้รับอนุญาติให้เข้าถึงข้อมูล
  - prevent legitimate users from accessing resources in an unauthorized manner,
    - ป้องกันผู้ใช้ของระบบจากการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาติ
  - enable legitimate users to access resources in an authorized manner.
    - เมื่อผู้ใช้ของระบบต้องการเข้าถึงข้อมูลที่ได้รับอนุญาติต้องเข้าถึงได้

Access control and authentication

- ในทุกระบบ ผู้ทำระบบ/ผู้ดูแลระบบ/เจ้าของระบบ ต้องระบุว่าใครทำอะไรได้บ้าง ได้แค่ไหน who can do what
- ซึ่งจะทำก่อนที่ระบบจะถูก implement
- Access control
  - Control access to assets based on business requirements, user management, authentication methods, and monitoring
- Authentication เป็นวิธีที่ช่วยทำให้เรามั่นใจ (confident) กฎ (rules) ถูกนำไปใช้กับ entity ที่ถูกต้อง

Here goes a question…

statement 2 statement นีแตกต่างกันอย่างไร?

Action ไหนเกิดก่อน ???

"This file can only be accessed by an authenticated user."

แต่ละสูงน์ศึกษาน่าเป็นใส

"This file can only be accessed by an authorised user."

Login → user →

Specifying access rights to resource

Authentication & Authorization: The differences: (Answer

- is a non-anonymous user
- ซึง identity ได้รับการ confirm.
- Any such user could then access this system.

An authenticated user

An authorized user is an authenticated user

- that has the required permissions to access this particular file, or is in a group/role that has the required access permissions.

While we know who you are, we won't let you access this file because you are not authorised to do so.

Hence, access control consists of two steps;

Authen then autho..

สรุป: What is access control?

Being able to restrict or allow particular actions. (การจำกัดหรือ อนุญาตในการกระทำต่างๆ)

Access Control เป็น 1 ใน mechanism ในการทำ Confidentiality

In computer security, it is only really useful if the access control is applied where there is authentication. จะเวิร์ค ต้องมีการ authen ก่อน

Access control implements a security policy that specifies

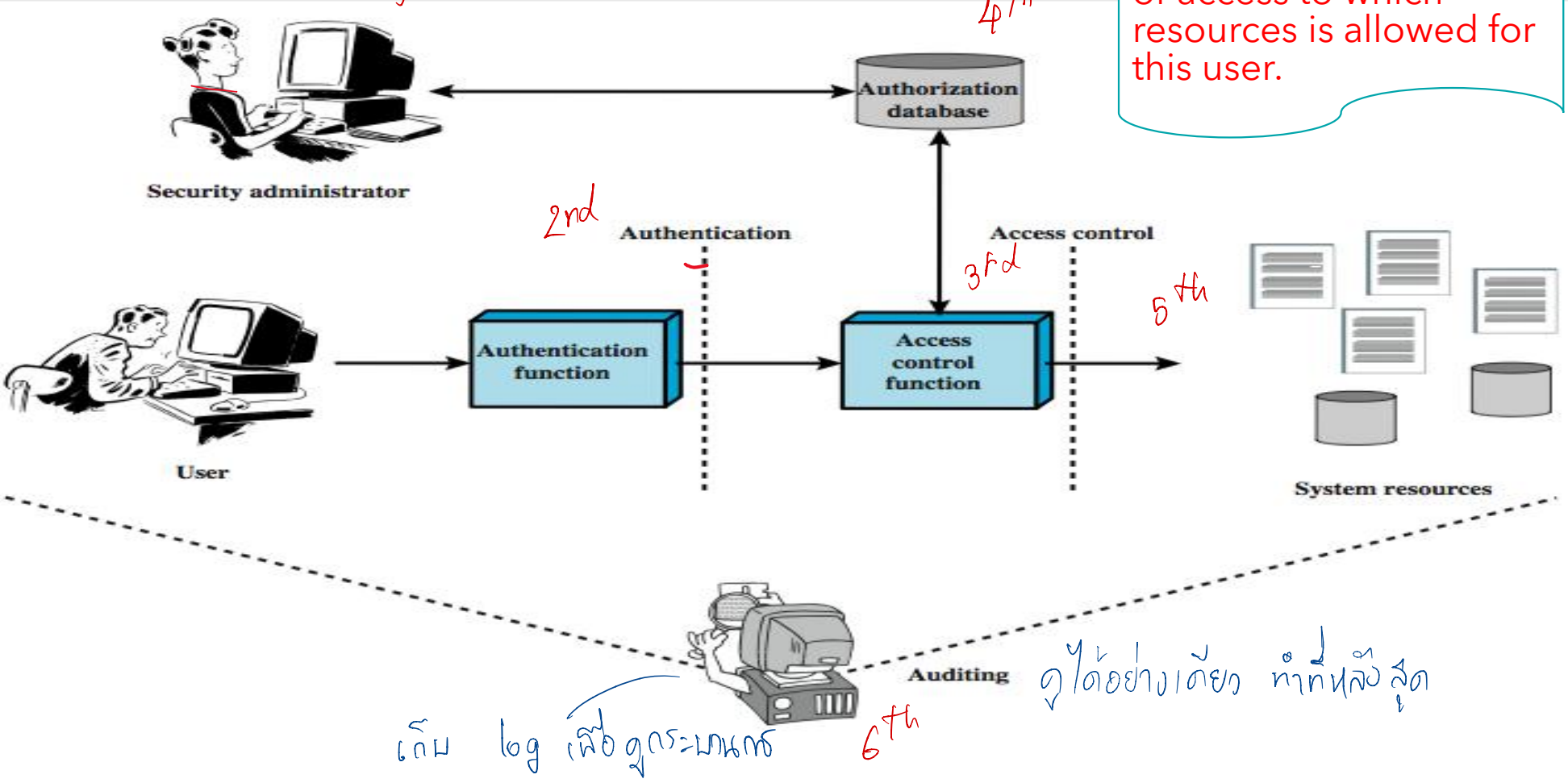
1. who or what (e.g., in the case of a process) may have access to
2. each specific system resource and
3. the type of access that is permitted in each instance.

Three Security Goals..

- The controls that enforce access control can be
  - technical, (Firewall)
  - physical, or (User can do what)
  - administrative
- These control types need to be integrated into
  - policy-based documentation,
  - software and technology,
  - network design, and
  - physical security components.

Broader view of access control:

that specifies what type of access to which resources is allowed for this user.

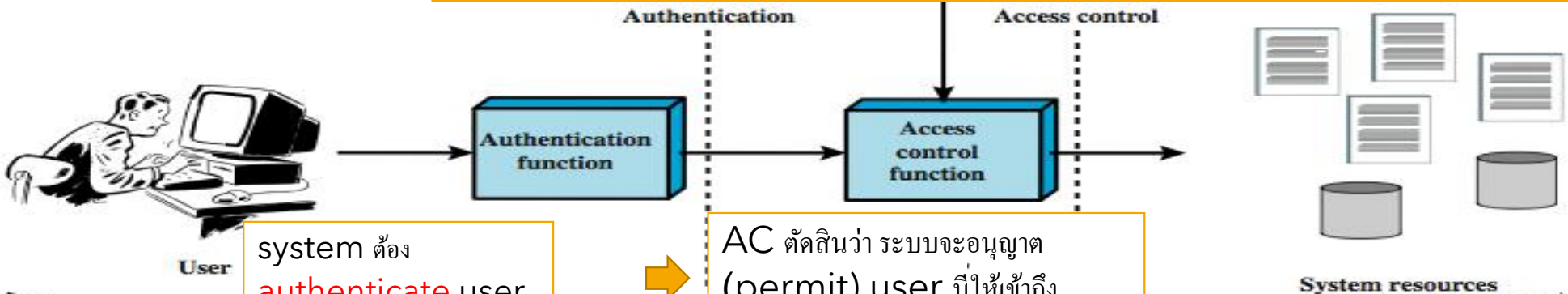


Broader view of Access Control (AC) Cont:

security admin ดูแลจัดการ authorization database

specifies what type of access to which resources is allowed for this user.

access control function เช็ค authorization db เพื่อตัดสินใจว่า จะ grant access หรือไม่



system ต้อง authenticate user ที่ต้องการ access ก่อน

AC ตัดสินว่า ระบบจะอนุญาต (permit) user นี่ให้เข้าถึง resource ที่ต้องการหรือไม่

มีการเก็บ log ของการ authen และ AC เพื่อไว้ audit

Access Control: where you can find it in Computer System?

In the previous slide access control function is shown as a single logical module.

ในทางปฏิบัติ access control function อาจประกอบไปด้วย หลายคอมโพเน้นท์ (หลายส่วน) ทำงานร่วมกัน.

AC ในส่วนของระบบปฏิบัติการ (OS)

ในส่วนของ Applications or Utilities เช่น

- Database management system

AC ที่ External devices ต่างๆ

- Firewalls..
- router

Access Control provide AC services?

Access Control Service

- Control access to information and resources.
- Model : *Initiator* and *Target* Entities.

An initiator (คน หรือ โพรเซส) requests to perform an operation on a target resource.

ACS เป็นคนกลางระหว่าง **the initiator and the target**

To grant or deny the service needs

ในระบบ

As ACS, we need

Access Control *Information*:

- Individual/Group ***identities*** of initiators and targets.
- ***Security labels*** of initiators and targets. (มีระดับขั้น - Ranking เหมือน ตำแหน่ง คุงตู่)
- ***Roles***. (ไม่มี Ranking)
- ***Actions*** or ***operations*** that can be performed.
- **Contextual information** (ข้อมูลอื่นๆที่เกียวข้อง) เช่น : routing, location, time periods.

Access Control *Policy:*

- **Rules** that define the conditions under which initiators can access targets. กฎที่กำหนดเงื่อนไขว่า initiator ใดจะเข้าถึง target ใดได้บ้าง
- Who? can Access What?, When? and How?

Access Control *Authority* (คนที่มี authority ในการจัดการ การควบคุมการเข้าถึง)

- Enforcement of access control policy. (เป็นผู้คุมกฎ ;))

Subjects and Objects

- ปกติเวลาพูดถึง entity ใน ACS,
  - Initiators จะถูกเรียกว่า subject
  - Targets จะถูกเรียกวา object

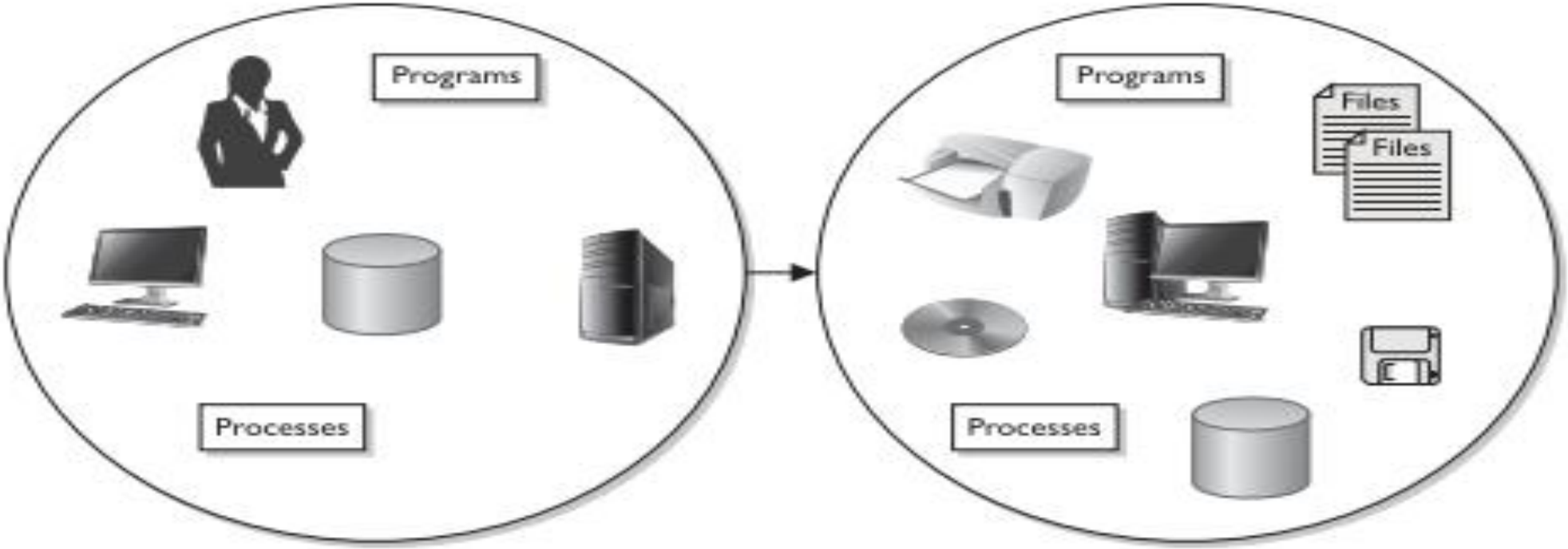
Subjects

- entities that use
- entity that can access objects
- e.g. process representing user/application

objects

- entities that are used
- access controlled resource
- e.g. files, directories, records, programs etc

no clear distinction between subjects and objects.
Depending on circumstances, an entity can be a subject in one access request and an object in another



Subjects are active entities.

ผู้ใช้หรือแอพพลิเคชันจะเข้าถึง object ผ่านทาง process ของ user หรือ app นั่นๆ (กรณีนี่ process เป็น subject)

แต่ถ้ากรณี เป็น process ทีถูกเรียกจะเป็น object

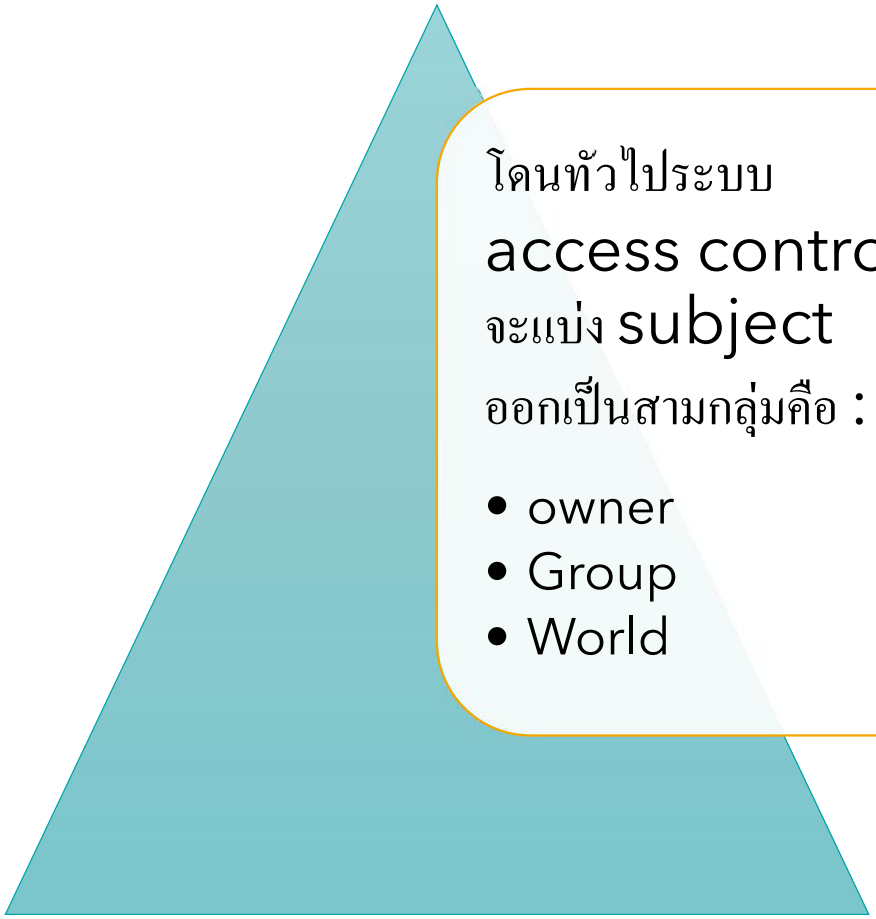
Objects are passive entities.

Examples

records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs.
bits, bytes, words, processors, communication port network nodes.

Win 10 ดูว่า user ทำอะไรได้บ้าง

More details on Subject and Objects



โดนทั่วไประบบ access control จะแบ่ง subject ออกเป็นสามกลุ่มคือ :

- owner
- Group
- World

The number and types of objects to be protected by an access control system depends on

- the environment (ของระบบ)
- และ the desired tradeoff between
  - security and complexity
  - processing burden and ease of use.

The basic elements of access control[3]

A subject

An object

An access right

An access right: what is it.

- the way in which a subject may access an object. (วิธีการที Sub ใช้เข้าถึง obj) เช่น read, write, execute, delete, create, search.
- ตัวอย่างของ access right

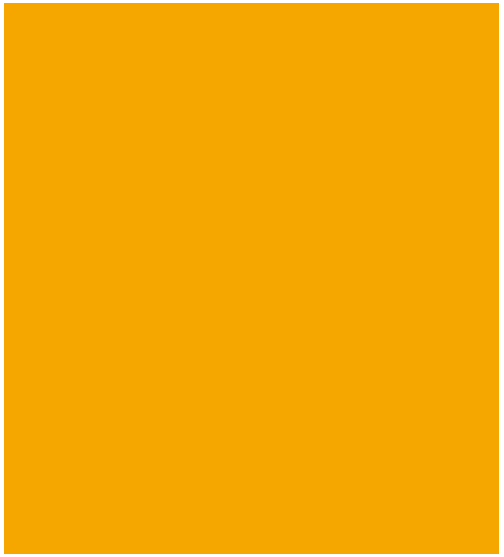
Read	User view info in system resource (files, selected records in files, selected fields within a record, or some combination).
	ดังนั่น Read access รวมไปถึง copy และ print
Write	User can add, modify, or delete data in system resource (ex. Files, records and programs)
	Write access includes read access*** (ไม่ทุกระบบ บางระบบ write ไม่รวม read เช่น สิทธิ์ append ใน Unix แต่ส่วนใหญ่แล้วจะรวม)

More examples of access right.

Execute	User may execute (run) specified programs.
Delete	User may delete certain system resources such as files or records.
Create	User may create new files, records or fields,
Search	User may list the files in a directory or otherwise search the directory.

We all know basic and broad concept of Access Control System.. Let’s see the real one.

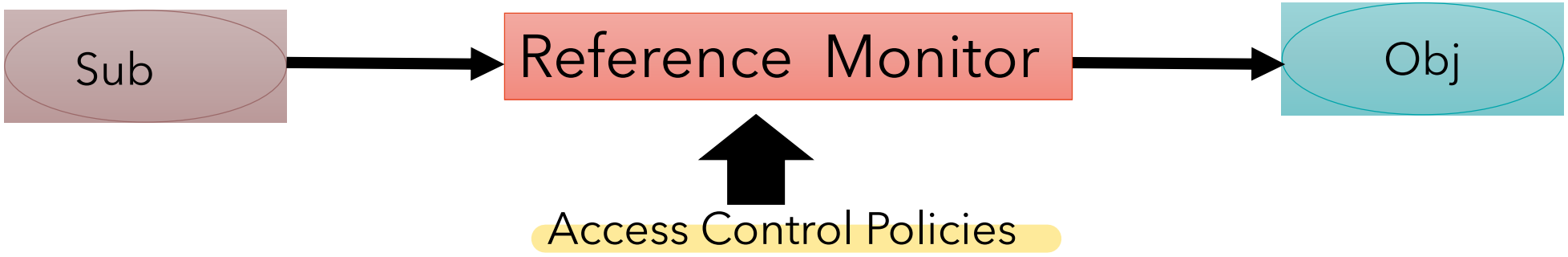
ปัญหาของ ACS ในยุคแรกคือ
ระบบจะออกแบบกันเอง
จึงมีแนวคิดในการสร้าง Model
เพื่อให้เป็น Framework กลาง



Access Control Model.

The reference monitor enforces policies for each interaction

- Subjects access objects:



- หลาย access control mechanism ในปัจจุบัน มีรากฐานมาจาก Reference Monitor.
- Reference monitor was introduced by James Anderson in 1972
  - คือ entity ที่ทำหน้าที่ในการ enforces the authorized access relationships between subjects and objects (original meaning)
  - An access control concept that refers to an abstract machines that mediates all accesses to objects by subjects [4]

Access Operations (modes): Basic access mode

- On the most elementary level, a subject may
  - observe an object, or
  - alter an object.
- With these basic access modes we can express some fundamental policies.
- For practical purposes a richer set of operations is more convenient.
- We will give a few examples for richer sets of access operations

Access Operations: Unix

Typical files: Three access operations:

- read: from a file
- write: to a file
- execute: a file

Directory: Access operations

- read: list contents
- write: create or rename files in the directory
- execute: search directory

Access Operation: Access right of the Bell-LaPadula model

- The Bell-LaPadula model has four access rights:
  - execute
  - read
  - append, also called blind write
  - write

	execute	append	read	write
observe			X	X
alter		X		X

- Mapping between access rights and access modes.

Bell-LaPadula เป็น Model ของ Access Control model หนึ่ง

Different focus of access control

What may be done with an object?

What is the subject allowed to do?

- Traditionally, multi-user operating systems manage files and resources, i.e. objects;
  - OS access control takes the first approach.
- Application oriented IT systems, like database management systems,
  - direct services to the user and often control actions of subjects.

Subjects and objects provide a different focus of control

Access Control Structure

Now, we know

- Subject
- Object
- Access operations..

The next thing is

- how to state which access operations are permitted…
- What structure should we use to capture the policy….

Access Control Structure

ถาม: จะเขียน policy อย่างไร ใช้ structure แบบไหน???

Access Control Structures

Requirements on access control structures:

- should help to express your desired access control policy (ควรช่วยในการแสดง ac policy ให้เป็นไปตามที่ต้องการได้)
- should help you to check that your policy has been used correctly. (ควรช่วยในการตรวจสอบว่า policy นั่นถูกใช้อย่างถูกต้อง)

The well known method: Access Control Matrics

The concept was developed independently by researchers in operating systems and databases.

An access control matrix (ACM) model

- สถานะของระบบจะถูกกำหนดด้วย triplet (S, O, A)
  - S: คือ set ของ subject.
  - O: คือ set of objects.
  - A: An access control matrix, A[S, O].
    - A[S, O] ลิสต์ access rights ที่ S มีต่อ O.

Access rights specify

- ชนิดของการเข้าถึงที่อนุญาตสำหรับ sub หนึ่งๆ ต่อ แต่ละ object เช่น . Read, Write, Execute, Delete, Create, Search.

Example: Access Control Matrix

- Policy in an access control matrix is expressed as follows:
  - ใช้ row แทน แต่ละ subject
  - ใช้ column for each object
- Primitive Operations ที่ต้องมีบน Access Matrix.
  - เราต้องสามารถ add/delete column ได้: (add/delete object)
    - Create Object, Delete Object.
  - เราต้องสามารถ add/delete row ได้: (add/delete subject)
    - Create Subject, Delete Subject.
- With these operations we can begin with an empty access matrix and build up an indexing of its entries.

กำหนด subject และ object ก่อน แล้วค่อยลง Access Rights

	bill.doc	edit.exe	fun.com
Alice	-	{exec}	{exec,read}
Bob	{read,write}	{exec}	{exec,read,write}

row เป็น subject

Column เป็น object

Access rights

Another example of ACM

TABLE 12.1 An Access Control Matrix

	Objects (Categorized by Type)		
Subjects	**Document File**	**Printer**	**Network Folder Share**
Bob	Read	No Access	No Access
Mary	No Access	No Access	Read
Amanda	Read, Write	Print	No Access
Mark	Read, Write	Print	Read, Write
Kathryn	Read, Write	Print, Manage Print Queue	Read, Write, Execute
Colin	Read, Write, Change Permissions	Print, Manage Print Queue, Change Permissions	Read, Write, Execute, Change Permissions

CISSP: Certified Information Systems Security Professional Study Guide
By James Michael Stewart, Ed Tittel, Mike Chapple

ตย

- กรณี มี User (subject) สามคน: เป็นต่อ พียม วอก
- มี ไฟล์อยู่ สามไฟล์ คือ
  - ไฟล์ sexygirl.doc ข้อมูลไฟล์ของเป็นต่อ
    - พียม read และ write ได้

    A[พียม, sexygirl.doc] = read, write
    - วอก อ่านได้ อย่างเดียว

    ……
  - ไฟล์ secret.exe โปรแกรม application นัดกิก ของเป็นต่อ
    - เป็นต่อrun ได้คนเดียว
    - A[เป็นต่อ,secret.exe] = execute

- ไฟล์ fun.com app เป็นต่อเขียนขึ้นให้เพือน ๆ เล่น
  - เป็นต่อ อ่าน เขียน และ รันได้
    - ……
  - พียม รันได้อย่างเดียว
    - …….
  - วอกเป็นน้องรัก เป็นต่อเลยให้นอกจากเล่น app ได้แล้ว ยังอ่านได้อีกด้วย
    - …..

ตัวอย่าง Access control matrix

	sexygirl.doc	secret.exe	fun.com
เป็นต่อ			
พียม			
วอก			

Another example

เป็นได้ทั้ง Sub และ Ob

Object & Sub Subject	O_1, (File 1)	O_2, (File 2)	S_1	
S_1,(Process)	Write	Read and Write		
S_2, (Alice)		Read	Execute	
S_3, (Bob)			Read	

Access control matrix: ข้อจำกัด

The access control matrix is

- an abstract concept,
- ไม่เหมาะสมเลย (not very suitable) สำหรับ direct implementation
  - เมือ จำนวนของ subject และ object มีมาก (large)
  - เมือ subject และ object มีการเปลียนแปลงถี (change frequently)
- จัดการ security ยาก (not very convenient for managing) security)

It is hard to represent ACM directly.

1 ต่อ 1 ไม่มี grouping

Representations of Access Control

ดึง Subject มาดูง่าย

Access Contorl Lists (ACL):

- Contain access from the viewpoint of an object.
- In other words, a column of the ACM.
- For example:
- File F : (A, Write), (B, Read).
  - Subject ไหนบ้างที่มีสิทธิ์ทำ operation ต่างๆ กับ object นี้

Capabilities:

- These correspond to the viewpoint of a subject.
- In other words, a row of the ACM.
- For example:
  - User A: ((Read, F1), (Write, F2)….)
- Subject presents a capability to an object (บอกว่า sub แต่ละ subject มีความสามารถทำ operation อะไร กับ object ทั้งหมดได้บ้าง)

Capabilities

- Focus on the subject:
  - access rights are stored with the subject
  - capabilities ≡ rows of the access control matrix

Alice	edit.exe: {exec}	fun.com: {exec,read}
พียม	sexygirl.doc {read, write}	fun.com{execute}

- Subjects may grant rights to other subjects.
  - พียมอาจให้สิทธิ์วอกในการเขียน sexygirl.doc
  - Subjects may grant the right to grant rights.
  - เป็นต่ออาจอนุญาตให้พียม อนุญาติให้วอก execute fun.com ได้

Capabilities as tickets

- We can think of a capability as a ticket that authorises the holder to access an object in a particular way.
- Each holder (user) has a number of tickets.
- Each holder (user) may be authorized to loan or give their tickets to others.
- Hence, the ticket must be unforgeable
  - => more security problem than ACL
  - การที่กำหนดสิทธิ์แบบ capabilities จะอนุญาติให้ subject มอบสิทธิ์ในการเข้าถึงข้อมูล ให้ subject คนอื่น ดังนั้นเมื่อ subject ที่ได้รับการถ่ายโอนหรือ มอบสิทธิ์ให้ เข้าไปทำการใดกับ object จะรู้ได้อย่างไร ว่า subject นี้ ได้รับ สิทธิ์อย่างถูกต้อง (จะรู้ได้อย่างไรว่าตัวที่ได้มาไม่ปลอม) (เช็นรับรอง)???
    - The Check is there for authentication
      - It could be something like a message authentication code or digital signature
    - The Check is there for authentication. Capabilities are difficult to revoke.
- Capabilities are difficult to revoke.

ที่นี้ถ้า เป็น crytography

Access Control Lists (ACLs)

- A list of subjects that are authorised to access an object.
- Focus on the object:
  - access rights are stored with the object.
  - ACLs ≡ columns of the access control matrix.

fun.com	พียม: {exec}	วอก: {read,write}

- How to check access rights of a specific subject?
- ACLs are implemented in most commercial operating systems but their actual use is limited.

fun.com

เป็นต่อ
{read, write, execute}

พียม
{execute}

วอก
{read,write}

Define users by group

Access Control Lists

- Access control lists are expensive to work with as every access to the object is checked.
  - เหมาะที่สุดกับสถานการณ์ที่ user ไม่มาก (best suited for situations where there are relatively few users (individuals, groups).)
  - Advantage
    - Giving the owner of the file a lot of control over modification of other user's access.

Identity	Type	Perm granted	Object
G. Smith	csci	r, w	report.tex
team-mem	admin	r, w, x	a.exe
alice	maths	r	intro.txt
. . .			

Access Control List: Ex. Unix

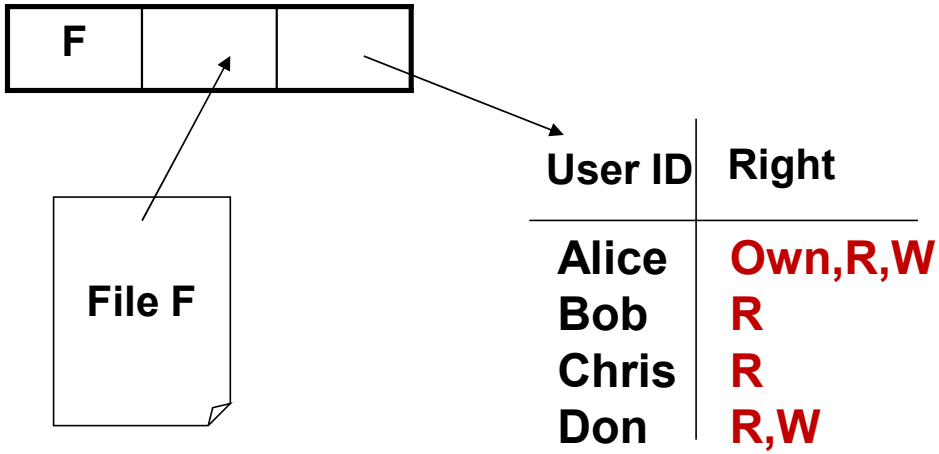
- In **Unix** a file has an access control list with **three entries**:
  - owner, group, and other users.
- The type of access can be **r, w, x.**

ดูโหดมาก

```
$ ls -al
total 120
drwx--x--x   4 kwrungra ksci    4096 Jun 26 19:14 .
drwxr-xr-x 426 root     other  32768 Nov 18 15:50 ..
-rw-------   1 kwrungra ksci     248 Jun 21  1:26 .bash_history
-r--------   1 kwrungra ksci       0 Mar 11  2009 .forward
-rw-------   1 kwrungra ksci     157 Mar 11  2009 .login
-rw-------   1 kwrungra ksci     174 Mar 11  2009 .profile
-r--------   1 kwrungra ksci       0 Mar 11  2009 .rhosts
-rw-------   1 kwrungra ksci    1108 Nov 26  1:18 .sh_history
-rw-------   1 kwrungra ksci       0 Mar 11  2009 .Xauthority
drwx------  16 kwrungra ksci    4096 Nov 25 23:34 Maildir
drwxr-xr-x   6 kwrungra ksci    4096 Jun  6 18:28 public_html
$
```

Unix: Access Control List

- Access control lists are used to protect owned objects.
- เจ้าของ (owner) object สามารถแก้ไขสิทธิ์ในการเข้าถึง object นั่น ๆ ได้
- 3 access right: R, W, X



Unix: The permission string…I

- ถ้า ตัดตัวแรกทิง permission string - --- --- --- คือ 9 ตัวหลัง แบ่งเป็น 3 ตัวแรก คือสิทธิ์สำหรับ owner, สามตัวถัดมาคือสิทธิ์สำหรับคนทีอยู่ใน group เดียวกับ owner และ สามตัวสุดท้าย สำหรับ คนอื่นๆ ทีอยู่ในระบบ

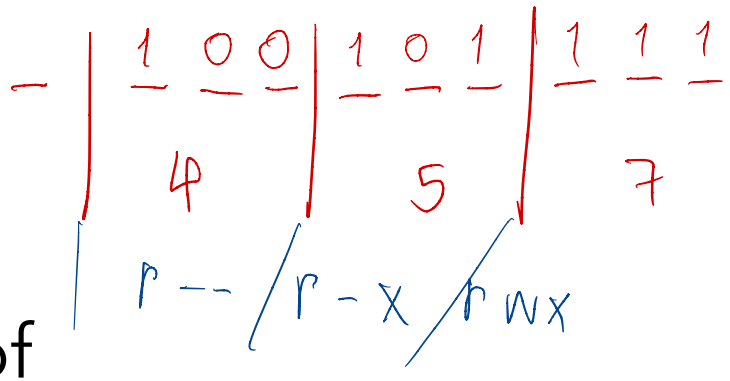
rwx | rwx | rwx

- The **'R'** permission means read.
- The **'W'** permission means write.
- The **'X'** permission means execute on a file.
  - จริงๆ ตัวแรกทีตัดทิงคือ ตัวทีบอกชนิดของไฟล์ว่าเป็น ไฟล์ธรรมดา หรือ ไฟล์ประเภทไดเรคทอรี

Unix: The permission string…II

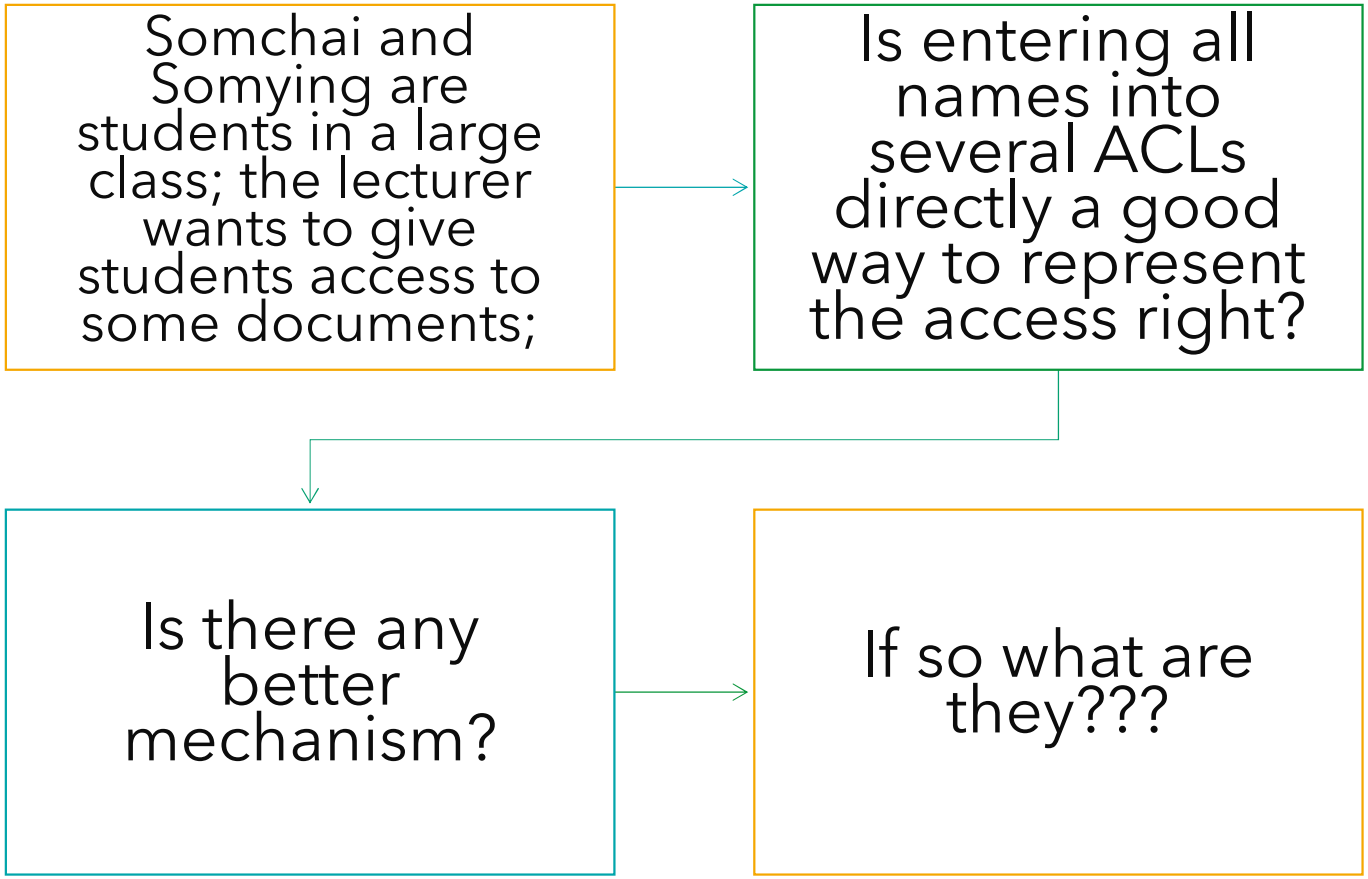
a.com = 457

- permissions สามารถแทนที่ด้วย 3 digit octal (base 8) เลขฐานแปด
  - The *read* flag contributes a 4, (100)
  - the *write* flag contributes a 2 (010)
  - the *execute* flag contributes a 1. (001)



- Exercise: Find the octal permission of
  - . -rwxr--r--
  - 4 (r) + 2 (w) + 1 (x) for owner
    4 (r) for group
    4 (r) for others/ universe

Question:


Somchai and Somying are students in a large class; the lecturer wants to give students access to some documents;
Is entering all names into several ACLs directly a good way to represent the access right?
Is there any better mechanism?
If so what are they???

row x column
3x3

ข้อตกลง

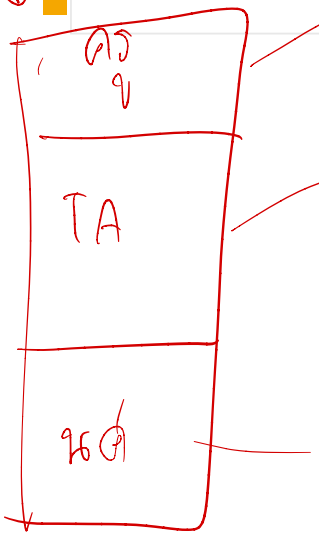
L | A | P

Lecture note

Assignment

Program

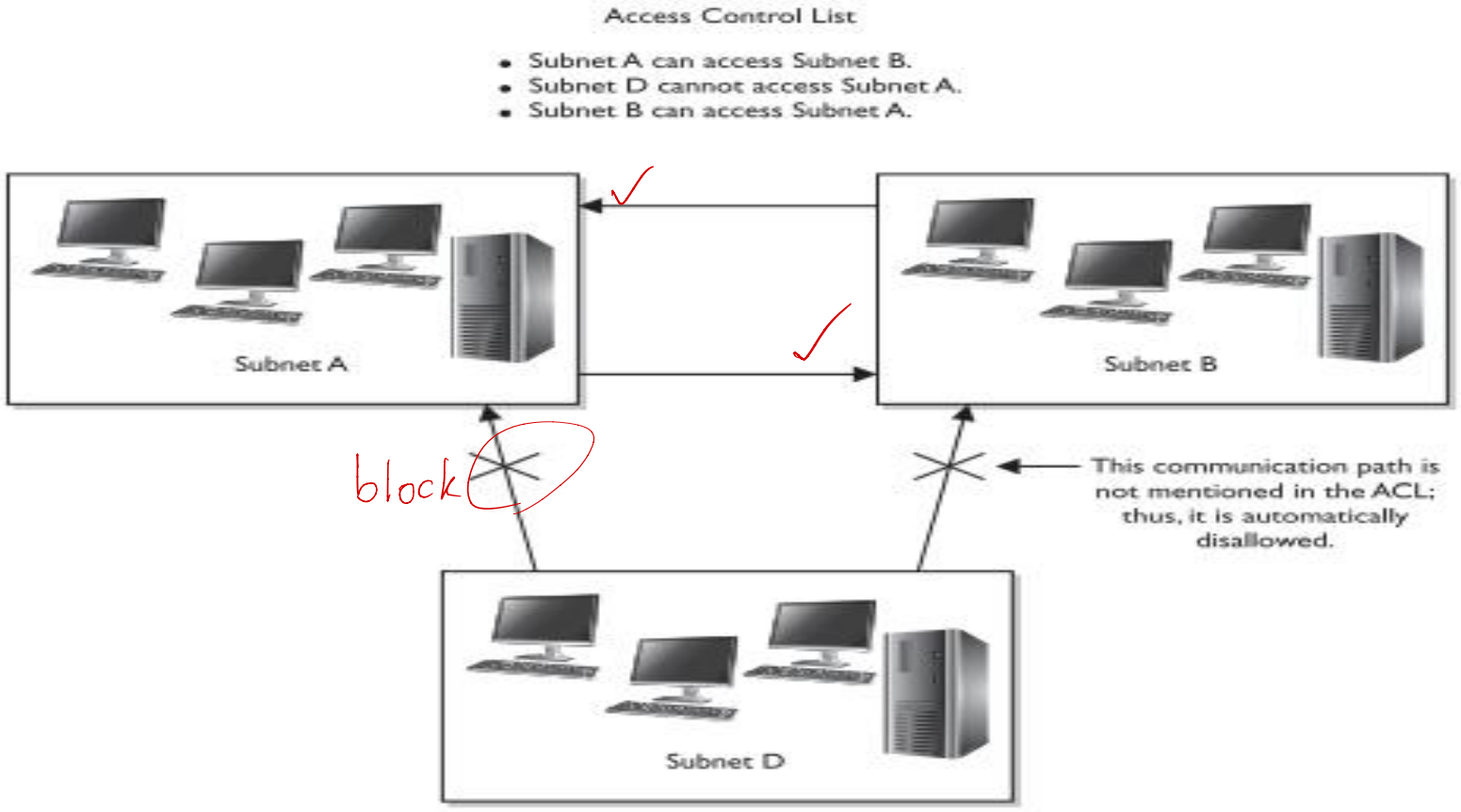
L1 access list



	L1	L2	L3	...							L15	A1	A2	A3	A4	P1	P2
อ รุ่งรัตน์	rw	rw	rw								rw	rw	rw	rw	rw	rwx	rwx
TA1	r	r	r								r	r	r	r	r	rwx	rwx
TA2	r	r	r								r	r	r	r	r	rwx	rwx
500..1	r	r	r								r	r	r	r	r	R,x	R,x
500xx	r	r	r								r	r	r	r	r	R,x	R,x
.....																	
52..xx	r	r	r								r	r	r	r	r	R,x	R,x
.....																	

subnet เดียวกัน → network address เหมือนกัน

Access Control List: Firewall [5]



Group

หรือ subject เป็น Group = Roles

- Entering all names into several ACLs is tedious.

Put them into Group !!!

  - so the lecturer defines a group,
  - declares the students to be members of the group, and
    - Ex. Subject group
  - puts the group into the ACLs
- Access rights are often defined for groups:
  - Unix: owner, group, others

Role

- Entering all names into several ACLs is tedius.

Put them in a Role/Roles!!!

- The lecturer would create a procedure for reading course material and assign this procedure to the role ‘student’.
- A role ‘course tutor’ could be assigned a procedure for updating documents.

พนักงานลาออก ลบออกด้วยนะจ๊ะ

Intermediate Controls

- ทั้ง group และ role จัดเป็น intermediate controls. (เป็นตัวกลาง)
- The intermediate control is
  - The intermediate layer between (เลเยอร์ที่อยู่ระหว่าง)
    - subjects and objects or
    - subjects and operations or
    - objects and operations.
  - ทำให้จัดการ access control policies ได้ง่ายขึ้น[2].
  - Intermediate controls facilitate better security management.
    - To deal with complexity, introduce more levels of indirection.

intermediate concepts ระหว่าง subjects และ objects มีหลายแบบ เช่น อาจแบ่งตาม

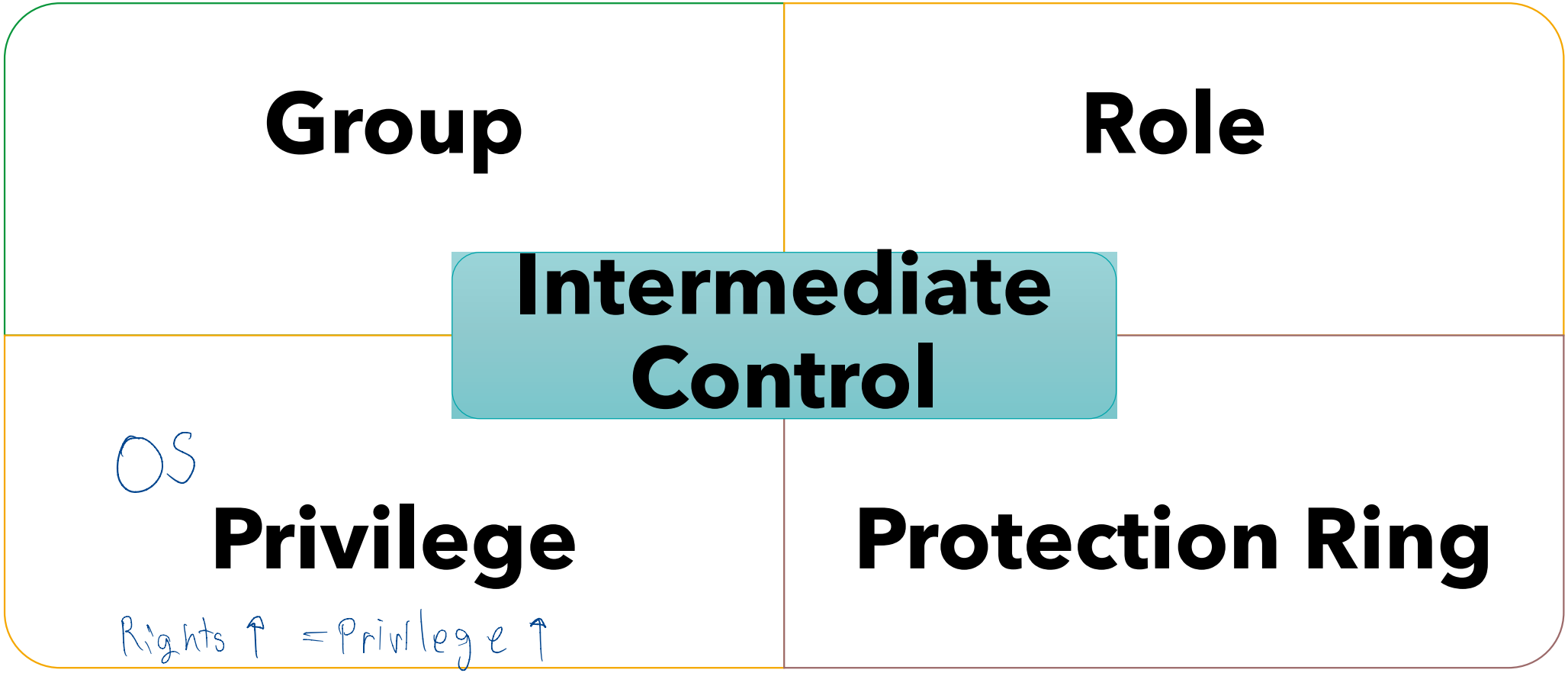
Privileges

Protection ring

We use intermediate levels of control to increase simplicity;

Principle of Privilege

Some intermediate Control mechanisms



Group concept

Users are assigned to groups.

- A user can be a member of one group or multiple groups.

Groups are given permissions to access objects.

Each user has the permissions assigned to the group or groups it is a member of.

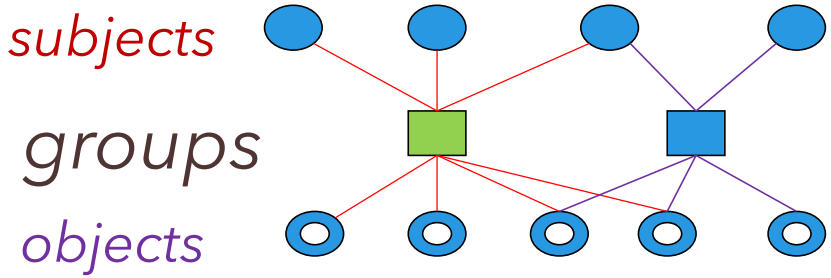
Groups are the intermediate layer between user and object.*

Objects can also be grouped.

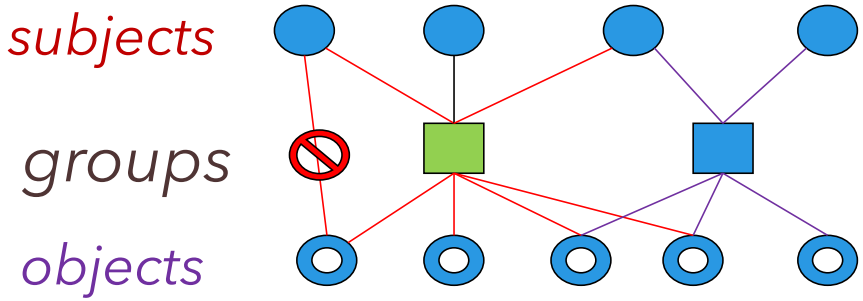
แบบฝึกหัด ให้นักศึกษาลองแบ่ง Group ของตารางใน Slide ที่ 46

Groups & Negative Permissions[3]

- Groups are an intermediate layer between users and objects.



- To deal with special cases, negative permissions withdraw rights



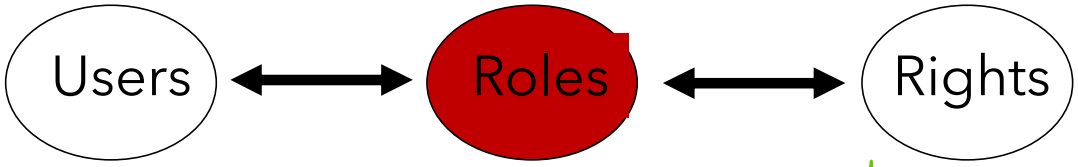
Role: What is it?

Role Base ex. Bank System

- Subject derives their access rights from their roles.
- A role is a collection of procedures assigned to users; (บทบาท คือ กลุ่มของ procedure ที่กำหนดให้ผู้ใช้)
  - a user can have more than one role and
  - more than one user can have the same role.
- Procedure:
  - 'high level' access operations with a more complex semantic than read or write
  - คือ access operation แบบ high level ที่ซับซ้อนกว่า read และ right (เช่น role ของพนักงานบัญชี)

Role based Access (Intermediate Control)

- A user is assigned a role, which comes with various permissions (rights) ผู้ใช้จะถูก assign role ซึ่งจะมี permission ที่แตกต่างกัน (Permissions คือ สิทธิ์ในการทำ operation ต่างๆ).



- For example, an accountant can issue cheques.
  - if Jane Doe is assigned the role of accountant
  - the payroll software will allow Jane to approve checks and issue them.

http://www.authenticationworld.com/Access-Control-Authentication/RoleBasedAccessControl.html

Role based access: An example

- In a banking environment there are several appropriate roles:

A Teller has permission	A Branch Manager has	A Customer is allowed	A System Administrator	An Auditor
☐ to modify a customer account with a deposit	☐ the same permissions as a teller	☐ to query the account log for his/her own account.	☐ can query all system log entries,	☐ can read any data in the system
☐ carry out withdrawal transactions up to a specified limit	☐ can also create and terminate accounts.		☐ activate/deactivate the system,	☐ but modify nothing.
☐ query all account log entries.			☐ but cannot read or modify customer account info .	

แบบฝึกหัด ให้นักศึกษาลองแบ่ง Role ของตารางใน Slide ที่ 46

More on roles

If users change roles

- their rights change in accordance with their old and new roles.
- This can simplify access control management!

As you can see, a role corresponds to a group whose

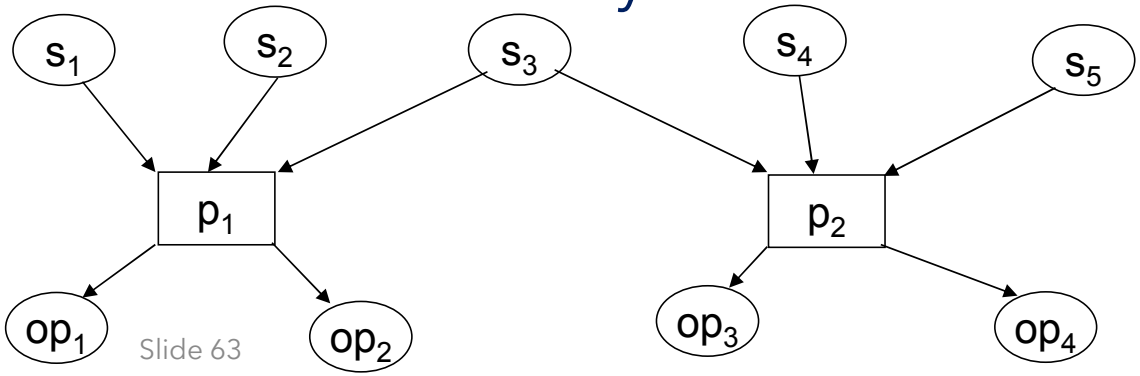
- **responsibilities,**
- **abilities or restrictions**

need to be considered when formulating access policy.

Separation of duties is an important security principle;

Privileges (Intermediate Control):

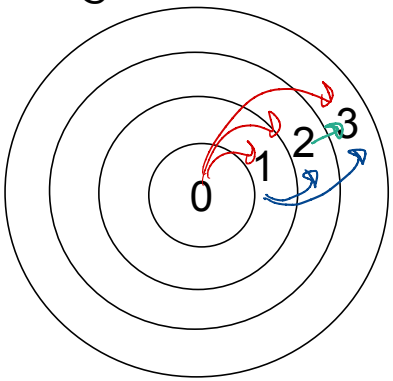
- A subject is assigned privileges that allow the subject to execute certain operations.
- Typically, privileges are associated with OS functions and relate to activities like system administration, backup, mail access, or network access.
- Privileges can be viewed as an intermediate layer between subjects and operations.



Permission

Protection Rings

- Each subject (process) and each object is assigned a number, depending on its 'importance', e.g.
  - 0 – operating system kernel
  - 1 – operating system
  - 2 – utilities
  - 3 – user processes



- These numbers correspond to concentric protection rings,
  - with ring 0 in the centre giving the highest degree of protection.
- If a process is assigned the number *i*, then we say the process
  - "runs in ring *i*".
- Access control decisions are made by comparing the subject's and object's numbers.

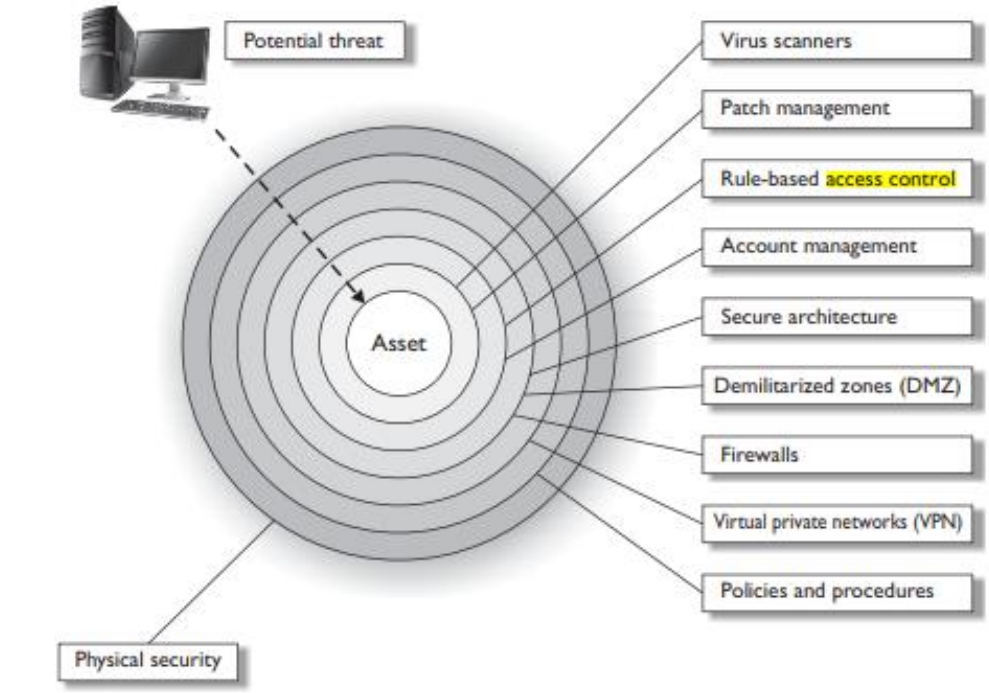


Figure 2-2 Defense-in-depth

ป้องกันเชิงลึก

Ask in class Next week:
What are the relevant subjects and objects in the context of operating systems and databases?

In operating systems:

Subject: Kenel process, User process, domains (a protection evironment in which a process executes).

Object: Files, Directories, memory segmets, processes

In databases:

Subject: Users, Application

object: row = record
column = field

API = ฟังชันของทุกสิ่ง

Exercise :

- Alice can read and write to the file x, read the file y and execute the file z.
- Bob can read x, read and write to y and has no access to z.
  - a) Write access control lists for this situation.
  - b) Write capability lists for this situation.
  - c) What is the difference between access control lists and capability lists in terms of revoking all access rights to a specific file and revoking all access rights for a specific person?
  - Add 1 record (Protect from copying)

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
- [5] All in one CISSP Exam Guide, S. Harris, 6th edition, McGrawHill, 2013.