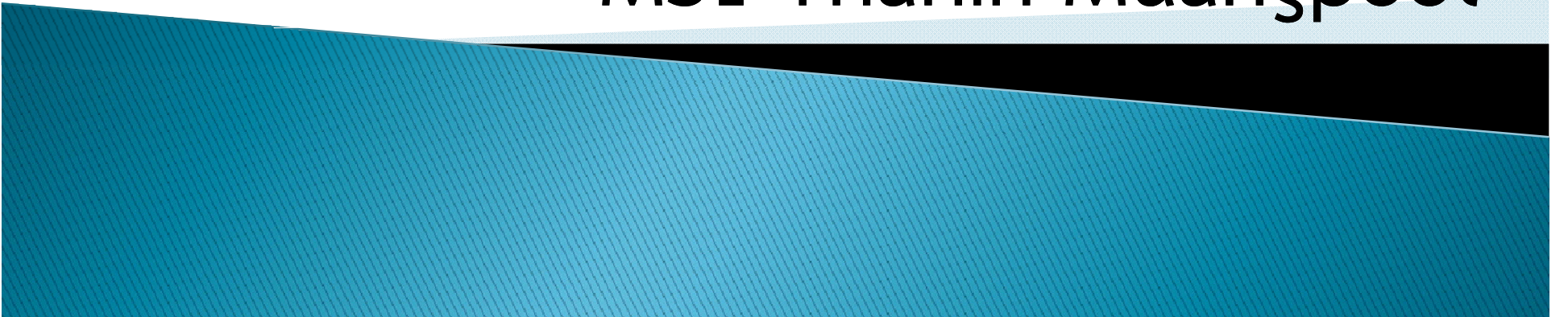


Access Control

MS1 Thanin Muangpool



What is a Access Control ?

Access Control หมายถึง การทำให้มั่นใจว่าทรัพยากรต่างๆ ของระบบจะได้รับอนุญาตให้ถูกใช้โดย User ที่มีสิทธิ์เท่านั้น ประกอบด้วย

1. **Identification** เป็นกลไกการพิสูจน์ตัวตนบุคคลที่เข้าใช้ระบบโดยแต่ละคนจะไม่ซ้ำกัน และใช้ร่วมกับ Authentication

2. **Authentication** เป็นกลไกการตรวจสอบสิทธิ์ในการใช้งานระบบ

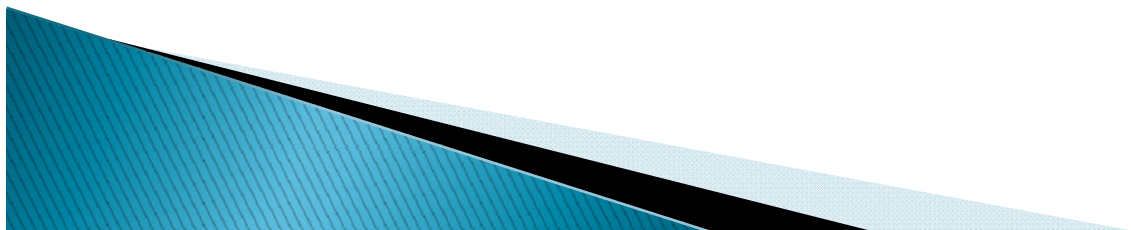
3. **Authorization** เป็นกลไกการอนุญาตหรือให้สิทธิการเข้าถึงระบบในแต่ละระดับ

4. **Accountability** เป็นส่วนที่ใช้บันทึกในการเข้าใช้ระบบของ User (System Logs) เพื่อจัดทำเป็นหลักฐานในการตรวจสอบ (Audit Trail)

Identification

หมายถึง กระบวนการพิสูจน์ความถูกต้องของตัวบุคคล อาจอาศัย Identifier ของบุคคล ในการพิสูจน์ตัวบุคคลต้องอาศัยข้อมูล 3 ประการ ดังนี้

1. **Something you know** เช่น Password
2. **Something you have** เช่น Identity card, ATM Card
3. **Something you are** ได้แก่ Biometric เช่น Fingerprint, Face Recognition, Blood Vein Pattern, Iris Scan, Retina Scan

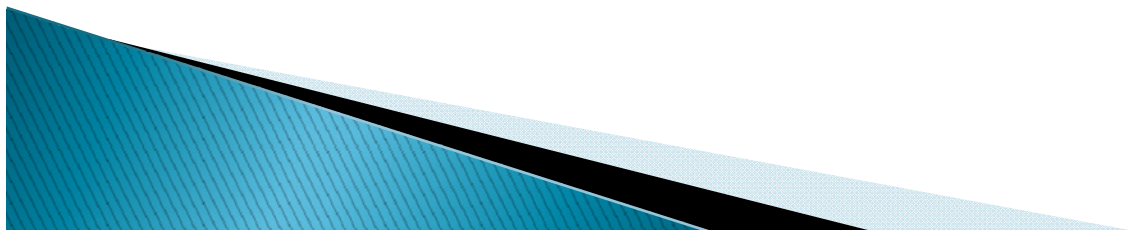


Identification → Something you know

- **Password** คือ คำ หรือกลุ่มคำที่ผู้ใช้กำหนดขึ้น ซึ่ง Password ที่ดีสามารถสรุปได้ 3 มุมมอง ดังนี้

1. ความยาวของ Password
2. ชุดของตัวอักษร
3. การสุ่ม

- **Passphrase** คือชุดตัวอักษร คล้าย Password แต่มีความยาวกว่า คาดเดาได้ยากกว่า



Identification → Something you have

- Magnetic Strip Card เช่น ATM Card, Credit Card, Debit Card
- Smart Card
- Radio Frequency Identification : RFID
- Token

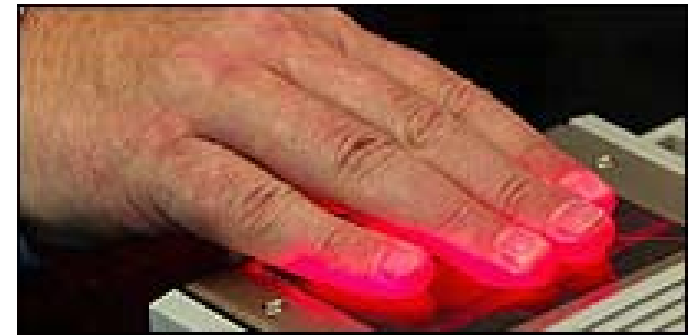


<https://www.mypw.com/press/>

Identification → Something you are

- Biometric technology uses computerised methods to identify a person by their unique physical or behavioural characteristics.
- Developments and uses have increased with demand to match concerns over international, business and personal security.
- Biometrics is more personal than a passport photo or Pin, using traits such as fingerprints, face or eye "maps" as key identifying features.

Identification → Something you are



<http://news.bbc.co.uk/2/3/health/spl/hi/guides/456900/456993/html/nn5page1.stm>

Identification → Something you are

การประเมินประสิทธิภาพของ Biometric

- **Identification/One-to-many** : Sample is compared to all biometric data saved in a system. It seeks to find an identity, rather than verify a claimed one.
- **Verification/One-to-one** : Comparison of sample with previously enrolled template to determine if from same person.
- **Slaps** : Fingerprints taken by simultaneously pressing four fingers of one hand onto a scanner.

Identification → Something you are

การประเมินประสิทธิภาพของ Biometric

- **False Acceptance Rate** : Probability that a system will incorrectly identify an individual or fail to reject an impostor.
- **False Rejection Rate** : Probability that a system will fail to identify a registered user.
- **Enrolment** : Process of collecting a biometric, converting it into a biometric reference and storing it for later comparison.

Identification → Something you are

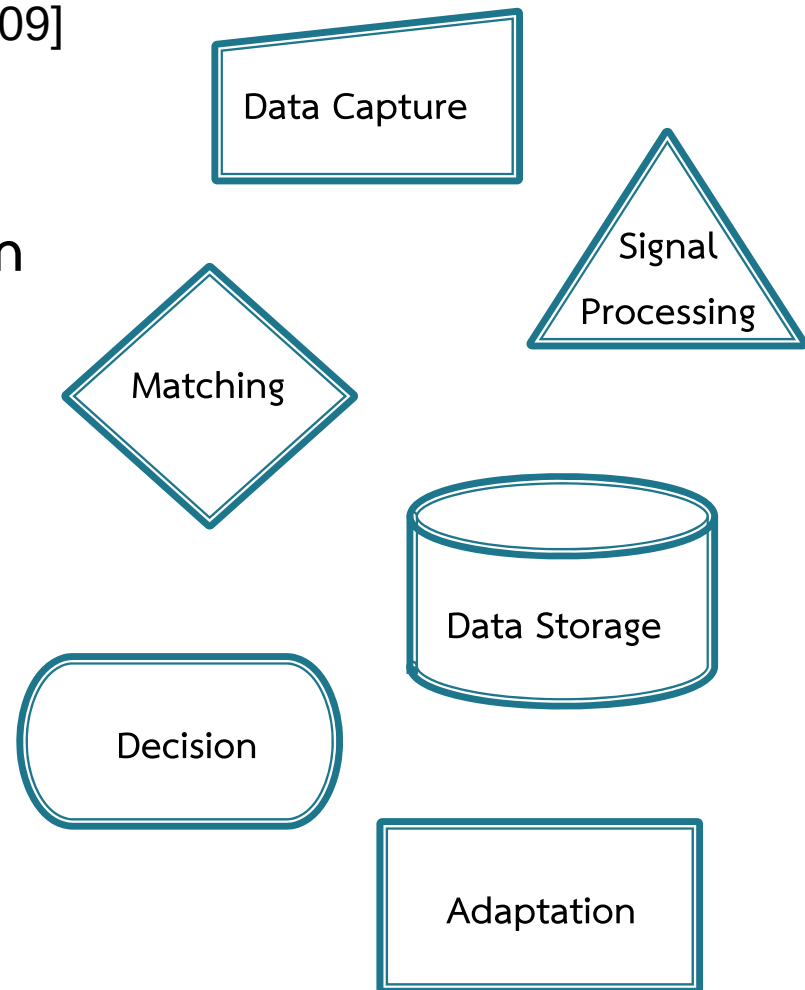
การประเมินประสิทธิภาพของ Biometric

- **Liveness detection** : Ensures only characteristics from a living person can be stored, read or used.
- **Multimodal Biometric System** : A system that uses two or more biometric characteristics or sensor types.

Identification → Something you are

Architecture of Biometric [R. Vacca,2009]

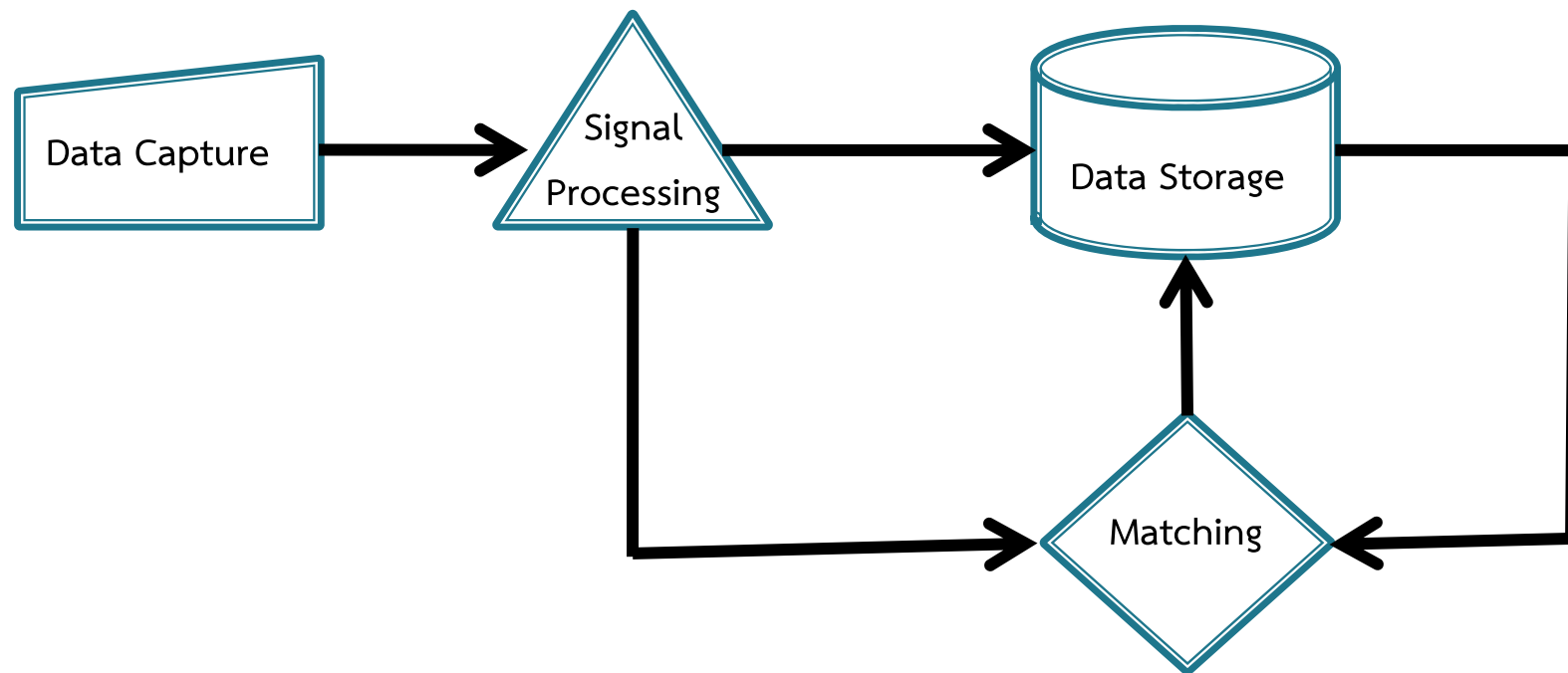
- Data Capture Subsystem
- Signal Processing Subsystem
- Matching Subsystem
- Data Storage Subsystem
- Decision Subsystem
- Adaptation Subsystem



Identification → Something you are

การใช้ระบบ Biometric

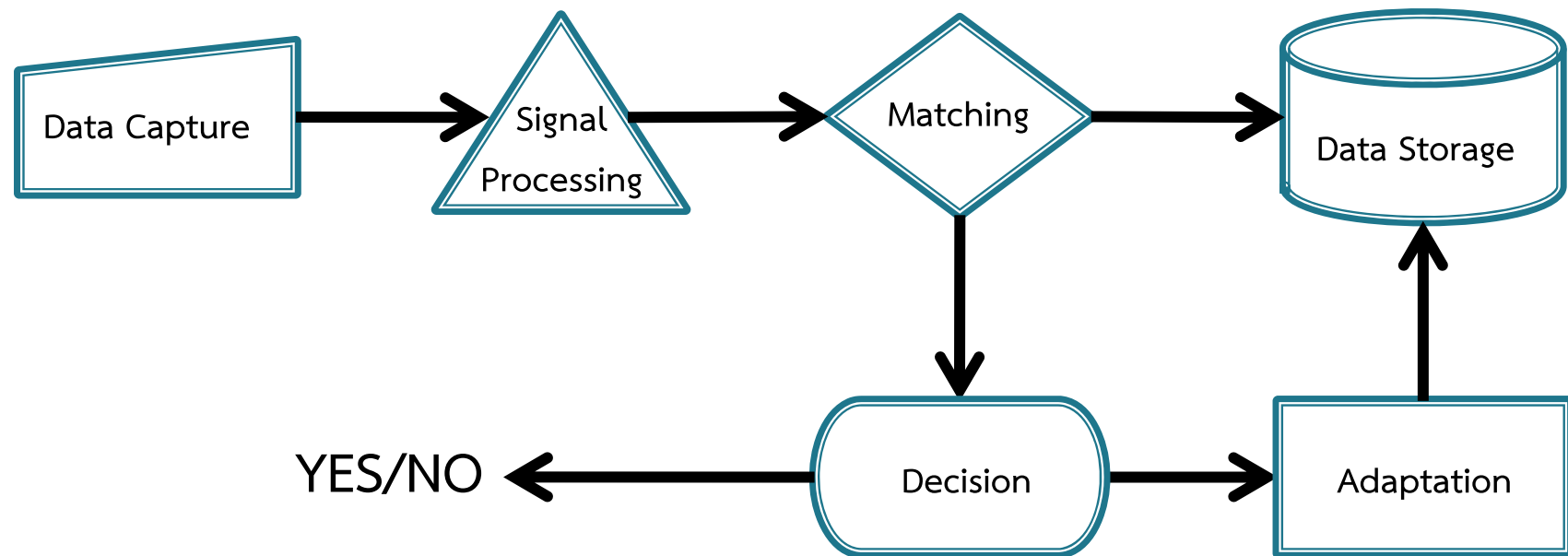
- Enrollment



Identification → Something you are

การใช้ระบบ Biometric

- Authentication



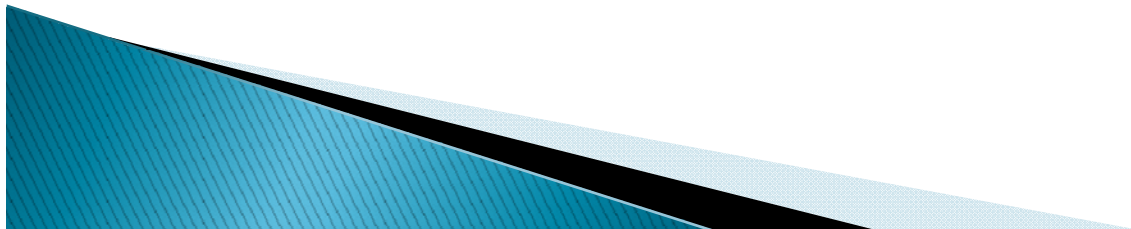
Authorization

คือ การจำกัดสิทธิ์ในการกระทำใด ๆ ต่อระบบและข้อมูลในระบบของ User มี 3 ลักษณะ ดังนี้

1. เป็นรายบุคคล
2. เป็นกลุ่ม
3. ใช้งานข้ามระบบ

ตัวอย่างเช่น

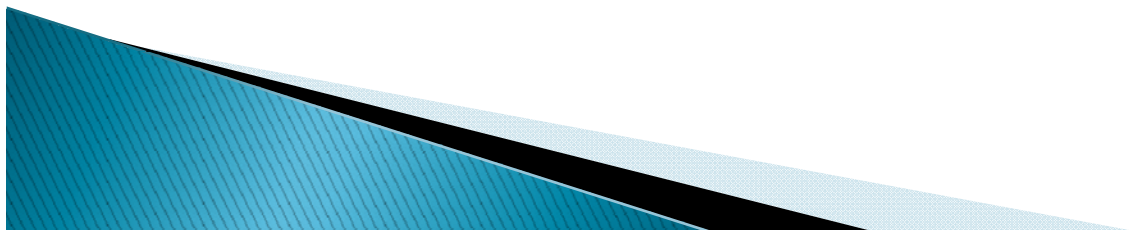
- Bell LaPadula Model
- Access Control List Matrix : ACL



Authorization → Bell LaPadula Model

เป็นแบบจำลองที่ใช้กำหนดการควบคุมการเข้าถึงแบบ Mandatory Access Control ซึ่งเป็นการกำหนด Multi-Level Security โดยแบ่งระดับสิทธิ์ในการเข้าถึงและดำเนินการในระดับที่ถูกกำหนดให้เท่านั้น ไม่สามารถส่งสิทธิ์ต่อให้กับผู้อื่นได้ มีองค์ประกอบ ดังนี้

1. **Object** ประกอบด้วย Table, View, Row, Column, and Operation
2. **Subject** ประกอบด้วย User, Program and Module Access Data
3. **Class** คือ Level Security of Object มี 4 Level ดังนี้ Top Secret : TC, Secret : S, Confidential : C and Unclassified : U
4. **Clearance** คือ สิทธิ์ Subject ในการเข้าถึง Object มี 4 ระดับ



Authorization → Bell LaPadula Model

เช่น กำหนดให้ S = Subject and O = Object

กำหนดให้ความมั่นคงของ Object (O) = Class (O)

สิทธิ์ในการเข้าถึง Object ของ Subject = Class (S)

User can Read and Write จะต้องตรงเงื่อนไข Mandatory Access Control ดังนี้

1. **Simple Security Property or Read Up Policy** หมายถึง S จะอ่าน O ได้ต้อง $\text{Class}(S) \geq \text{Class}(O)$ เป็นกฎการของ **ความพร้อมใช้งาน (Availability)**

2. **Star Property (*-Property) or Write Down Policy** หมายถึง S จะเขียนข้อมูล O ได้ต้อง $\text{Class}(S) \leq \text{Class}(O)$ เป็นกฎของ **การรักษาความลับ (Confidentiality)** ซึ่งการป้องกันการเขียนข้อมูลในระดับความมั่นคงที่ต่ำกว่า เรียกว่า Flow Down Information



Authorization → Bell LaPadula Model

ตัวอย่าง Jimmy อยู่ฝ่ายบุคคล มีหน้าที่ในการสร้างและแก้ไขข้อมูล Table **EMPLOYEE** ซึ่งได้รับสิทธิ์ดังกล่าวจาก Admin ส่วน Somsri อยู่ฝ่ายขาย ไม่มีสิทธิ์เรียกใช้ข้อมูลใน Table **EMPLOYEE** แต่มีสิทธิ์สร้าง Table ที่เกี่ยวข้องกับการขายได้ทั้งหมด Somsri ต้องการข้อมูล **เงินเดือน** ของพนักงาน จึงวางแผนสร้าง Table **MYTABLE** แล้วให้สิทธิ์การเพิ่มข้อมูลกับ Jimmy เพื่อนำข้อมูล **เงินเดือน** พนักงานมาใส่ไว้ใน Table **MYTABLE** เพื่อป้องกันการส่งต่อสิทธิ์ในสถานการณ์ดังกล่าว **DBA** จึงได้กำหนดมาตรการการควบคุมการเข้าถึงข้อมูลแบบ **Mandatory** โดยกำหนดระดับความมั่นคงของ **Object and Subject** ต่าง ๆ ดังนี้

- Table **EMPLOYEE** Level Security = S
- Jimmy Level Access Data = S
- Somsri Level Access Data = C
- Table **MYTABLE** Level Security = C

Class (Jimmy) > Class (MYTABLE)
นั่นคือ Jimmy อ่านข้อมูลจากจาก **MYTABLE** ได้ แต่เขียนไม่ได้ ซึ่งเป็นไปตามกฎ ***-Property**

Authorization → Access Control List Matrix : ACL

คือ กลไกการควบคุมการเข้าถึงทรัพยากรของระบบ โดยการแสดงรายชื่อ User System และการกระทำที่ User ได้รับอนุญาตให้กระทำต่อทรัพยากรใดๆ ของระบบ ตาราง ACL ประกอบด้วย

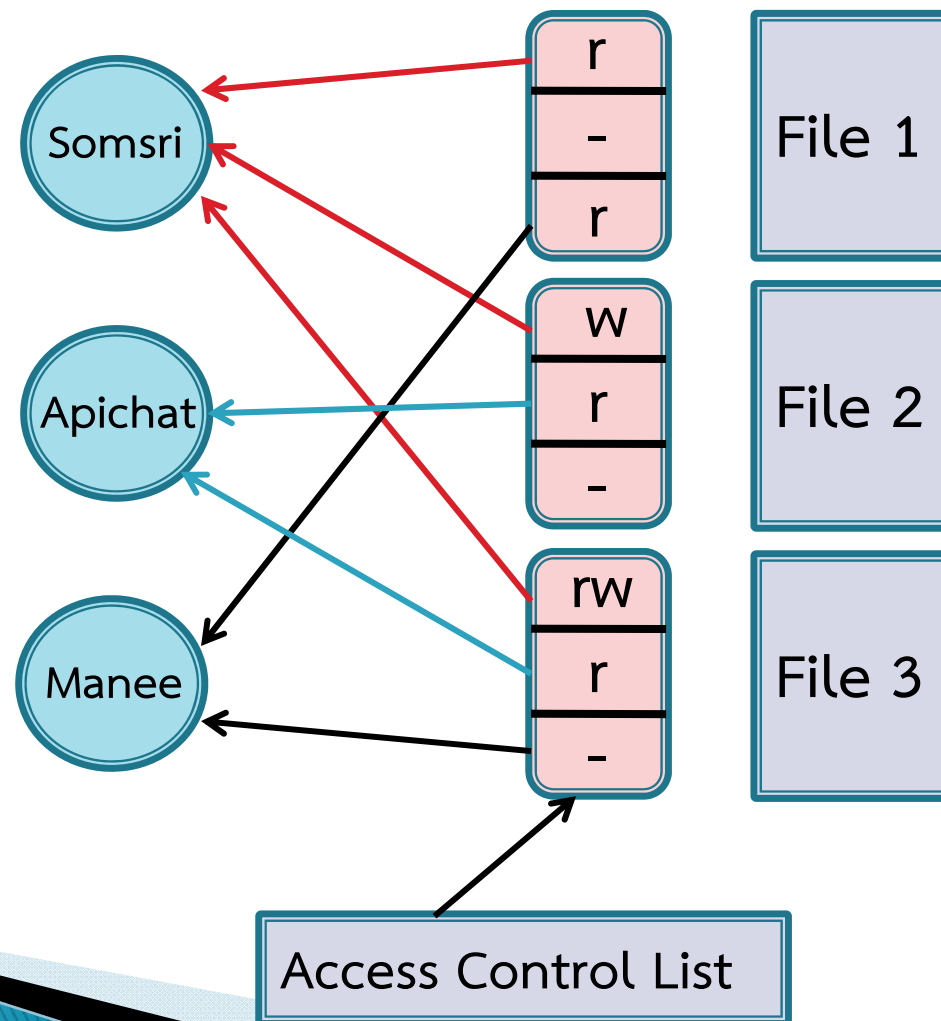
1. **Subject User** : Users have access to the system.
2. **Object** : Resources of the system that will be used by the user.
3. **Access Operation** : Read, Write, Execute.

ACL จะถูกนำมาสร้างเป็นตาราง โดย **Row = Subject and Column = Object**

	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Somsri	rx	rx	r	–	–
Apichat	rx	rx	r	rw	rw
Manee	rwX	rwX	r	rw	rw
Udom	rx	rx	rw	rw	r

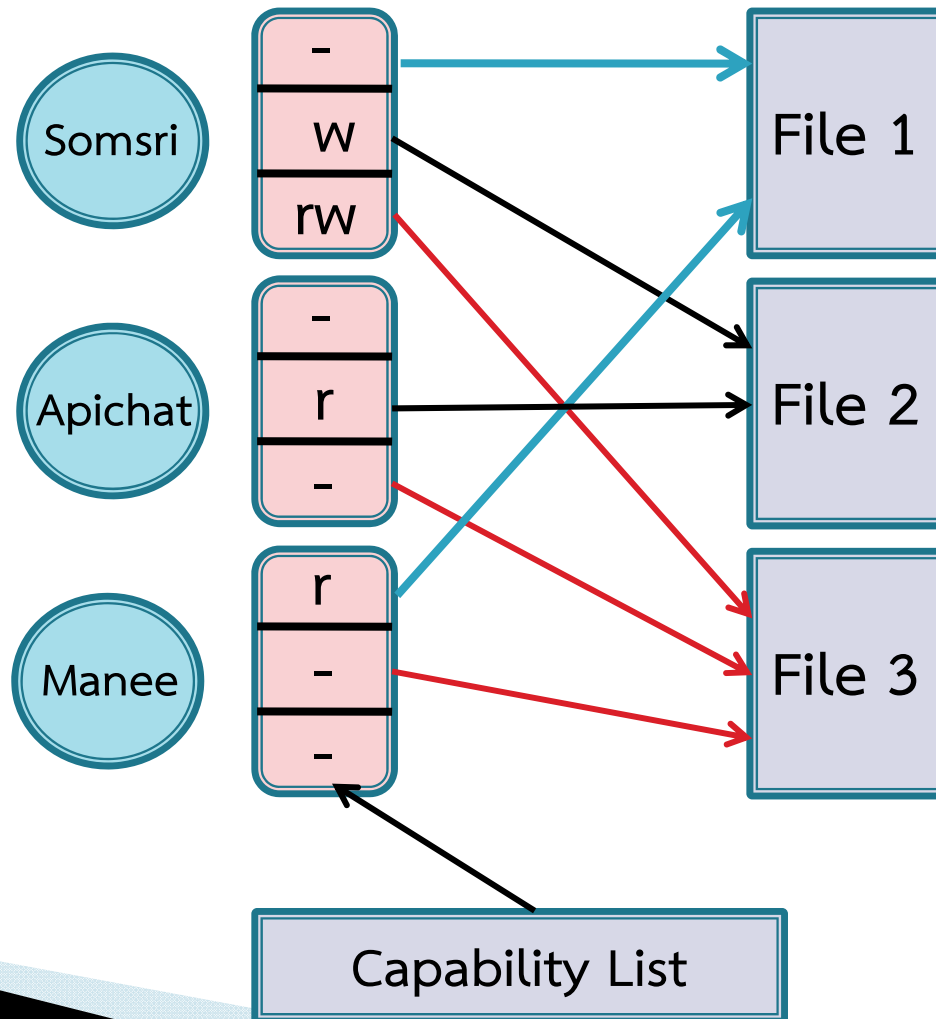
Authorization → Access Control List Matrix : ACL

ถ้าเขียน Column จะเรียกว่าตาราง ACL เวลาเขียนจะยึด Object เป็นหลัก



Authorization → Access Control List Matrix : ACL

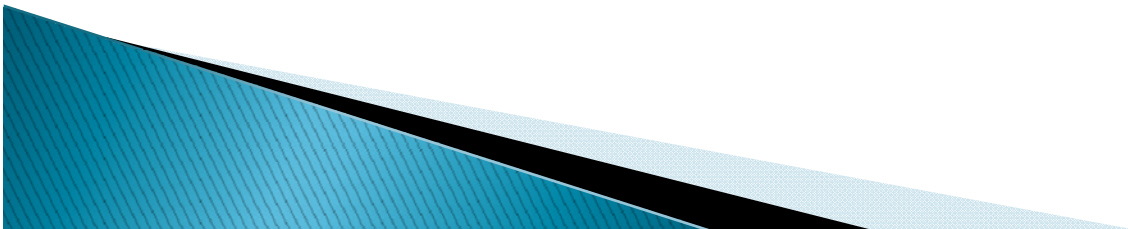
ถ้าเขียน Row จะเรียกว่าตาราง C- List or Capability List เวลาเขียนจะยึด Subject เป็นหลัก



Physical Access Control

เป็นการรักษาความปลอดภัยทางด้านกายภาพ ไม่ว่าจะเป็นสิ่งของ อุปกรณ์ สถานที่ หรือพื้นที่ใดพื้นที่หนึ่งขององค์กร จากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ในทางที่ผิด ในการควบคุมเพื่อป้องกันการเข้าถึงอาคารหรือสถานที่ที่ต้องการความปลอดภัย ได้แก่

1. กำแพง รั้ว และประตู
2. เจ้าหน้าที่รักษาความปลอดภัย
3. สุนัข
4. บัตรประจำตัว
5. กล้อง/โทรทัศน์วงจรปิด
6. ระบบสัญญาณเตือนภัย
7. ผนังและประตูด้านใน



Physical Access Control

8. ชุดกุญแจ แบ่งตามการทำงานได้ 2 แบบ คือ

- Mechanical Lock
- Electromechanical Lock ได้แก่ Manual Lock, Programmable Lock, Electronic Lock, Biometric Lock



Programmable Lock



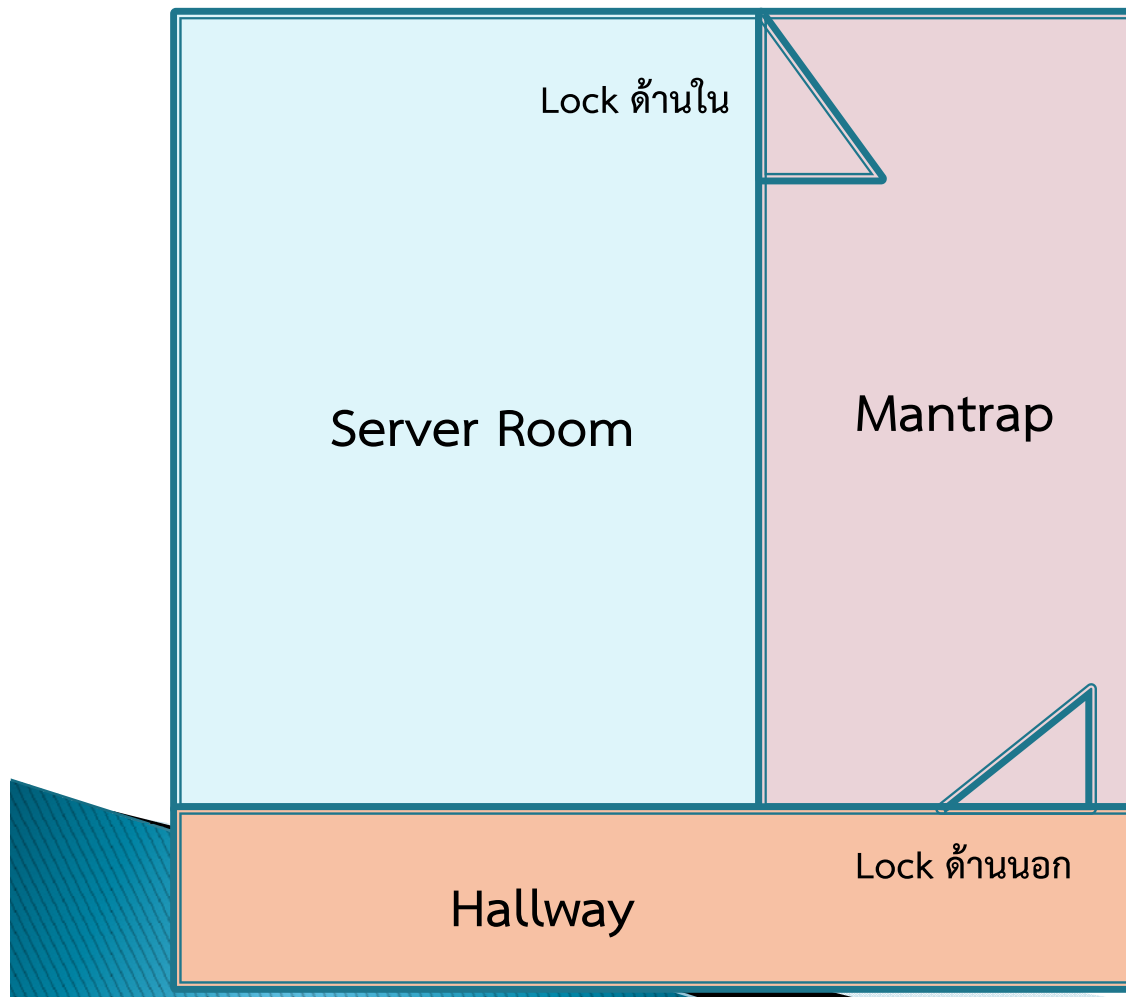
Biometric Lock



Electronic Lock

Physical Access Control

9. ห้องล๊อบดักจับผู้บุกรุก (Mantrap)



1. ผู้บุกรุกเข้าทางประตูด้านหน้าที่ Lock จากด้านนอกห้อง
2. ต้องเปิดประตูนี้จึงจะเข้าห้อง Server ได้ แต่ประตูนี้ Lock จากด้านใน ผู้บุกรุก จึงไม่สามารถเข้าไปได้
3. ต้องออกประตูเดิมที่เข้ามา แต่ไม่สามารถเปิดประตูออกได้เนื่องจากประตู Lock จึงติดอยู่ด้านใน

Fire System

- เป็นระบบที่ติดตั้งสัญญาณเตือนภัย
- อุปกรณ์ดับเพลิงชนิดต่าง ๆ เช่น ถังและสายยางฉีดน้ำ แก๊สดับเพลิง
Sprinkler
- อุปกรณ์สารเคมี เช่น CO₂ กรดโซดา แก๊ส
- อุปกรณ์ที่ใช้ในการตรวจจับเหตุที่ทำให้เกิดเพลิงไหม้ เช่น จากอุณหภูมิ
จากควันไฟ
- มีองค์ประกอบที่สำคัญ 2 ส่วน คือ
 1. Fire Detection
 2. Fire Suppression



Fire System → Fire Detection

จำแนกได้ 3 ประเภท ดังนี้

1. **Thermal Detection** มี Sensor วัดระดับอุณหภูมิ มี 2 ลักษณะ

- Fixed Temperature
- Rate-of-Rise

2. **Smoke Detection** นิยมใช้ในอาคารสำนักงาน มี 3 วิธี

- Photoelectric Sensor : ยิงลำแสงผ่านควัน
- Ionization Sensor : ตรวจจากอนุภาคของไอออน
- Air-aspirating Detector : ตัวอย่งอากาศ

3. **Flame Detection** มี Sensor ตรวจจับคุณลักษณะของแสงอินฟราเรด

หรือแสงอัลตราไวโอเล็ต มาเปรียบเทียบกับ Database



Fire System → Fire Suppression

จำแนกได้ 2 กลุ่ม ดังนี้

1. แบบ Portable Extinguisher จำแนกได้ 4 ชนิด

- ประเภท A :เพลิงเกิดจาก ไม้ กระดาษ ผ้า ยาง หรือขยะ
อุปกรณ์ดับเพลิง ได้แก่ น้ำ ผงเคมีแห้ง
 - ประเภท B :เพลิงเกิดจาก น้ำมัน สี แลคเกอร์ น้ำมันเชื้อเพลิง
อุปกรณ์ดับเพลิง ได้แก่ CO₂ ผงเคมีแห้งบางชนิด สารฮาโลน
 - ประเภท C :เพลิงเกิดจาก อุปกรณ์ไฟฟ้าและอิเล็กทรอนิกส์
อุปกรณ์ดับเพลิง ได้แก่ CO₂ ผงเคมีแห้ง สารฮาโลน
 - ประเภท D :เพลิงเกิดจาก แมกนีเซียม ลิเทียม โซเดียม
อุปกรณ์ดับเพลิง ได้แก่ ชนิดพิเศษ
- 

Fire System → Fire Suppression

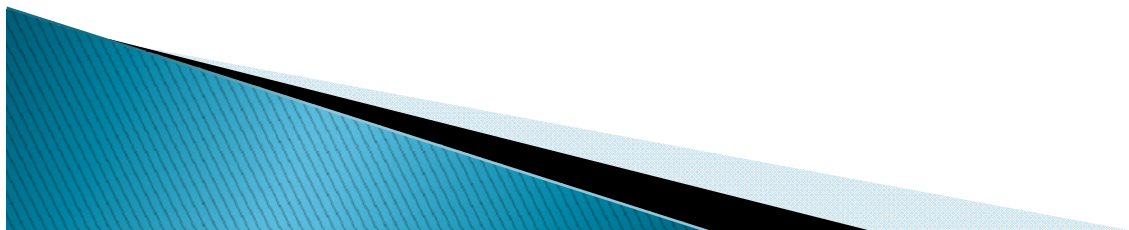
2. แบบ Manual and Automation Extinguisher จำแนกได้ ดังนี้

- Sprinkler System : แบ่งเป็น 3 ชนิด

1. Wet-Pipe System
2. Dry-Pipe System
3. Water Mist System

- Gaseous Fire Suppression System : แบ่งเป็น 2 ชนิด

1. CO₂
2. Halon



Questions and Answers

MS1 Thanin Muangpool

Thank you