แก้ไขครั้งล่าสุดเมื่อวันที่ 23 พฤศจิกายน 2567

Protection

The processes in an operating system must be protected from one another's activities.

Multi-users

ป้องกันระหว่าง user

Multi-processes

ป้องกันระหว่าง process

THE PRINCIPLE OF LEAST PRIVILEGE[*]

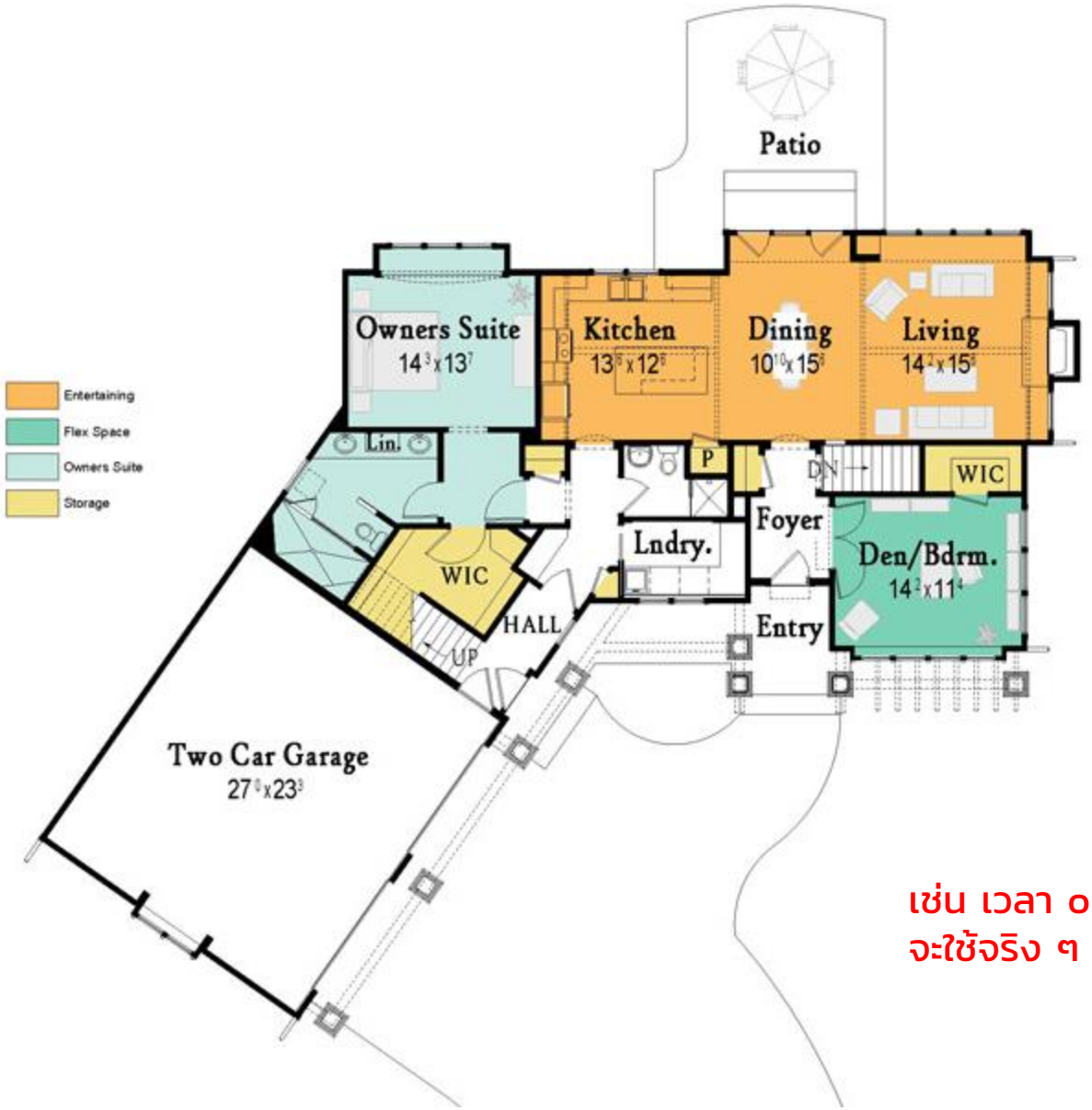
สิทธิ์

"The principle of least privilege. Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. The purpose of this principle is to reduce the number of potential interactions among privileged programs to the minimum necessary to operate correctly, so that one may develop confidence that unintentional, unwanted, or improper uses of privilege do not occur."—Jerome H. Saltzer, describing a design principle of the Multics operating system in 1974: https://pdfs.semanticscholar.org/1c8d/06510ad449ad24fbdd164f8008cc730cab47.pdf.

[*] : a right or immunity granted as a peculiar benefit, advantage, or favor : **PREROGATIVE**

especially : such a right or immunity attached specifically to a position or an office

Principle of least privilege



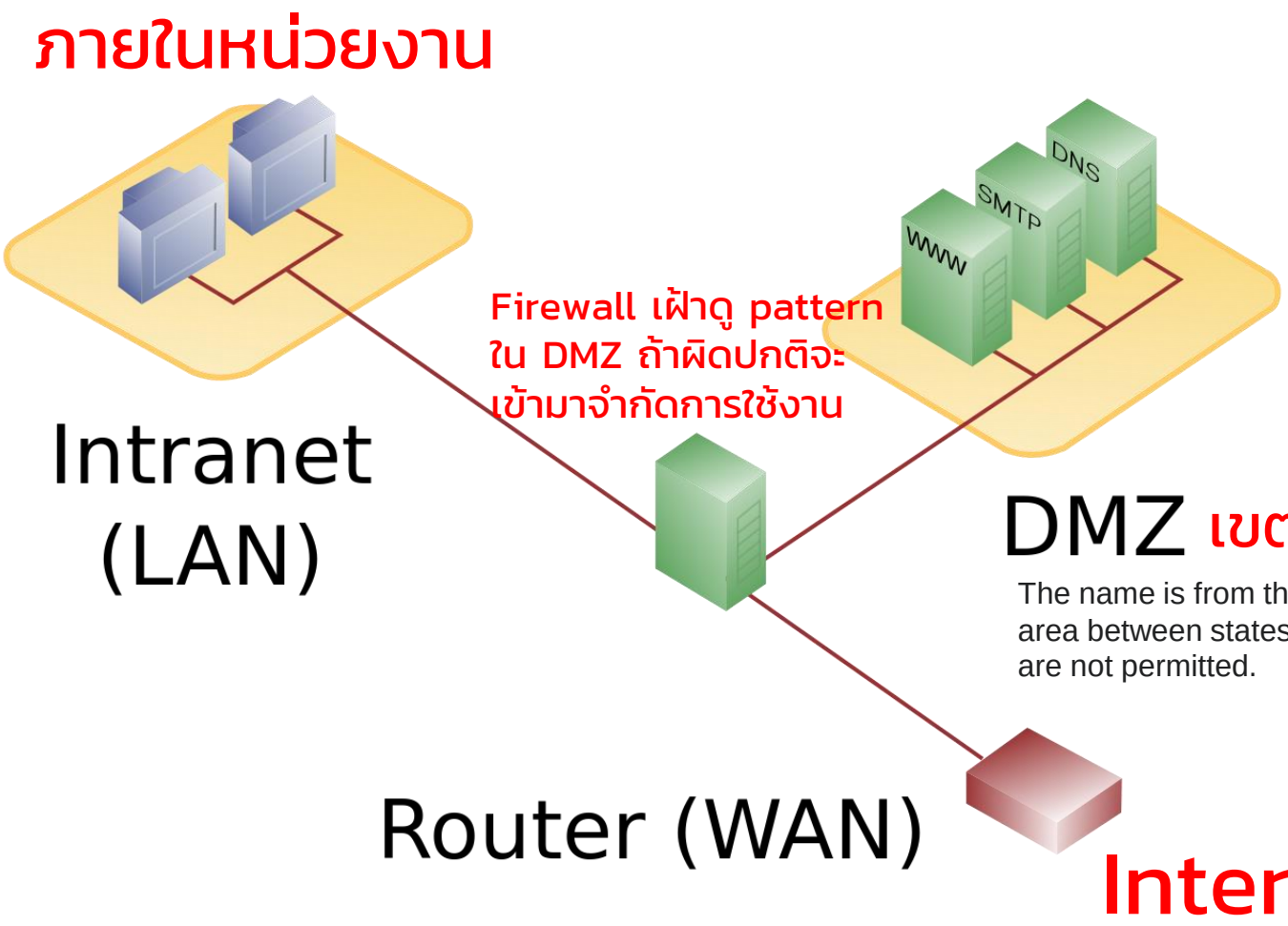
Process ล้างรถ
- Garage

Process ทำอาหารเย็น
- Kitchen
- Dining

Process ซักผ้า
- Laundry

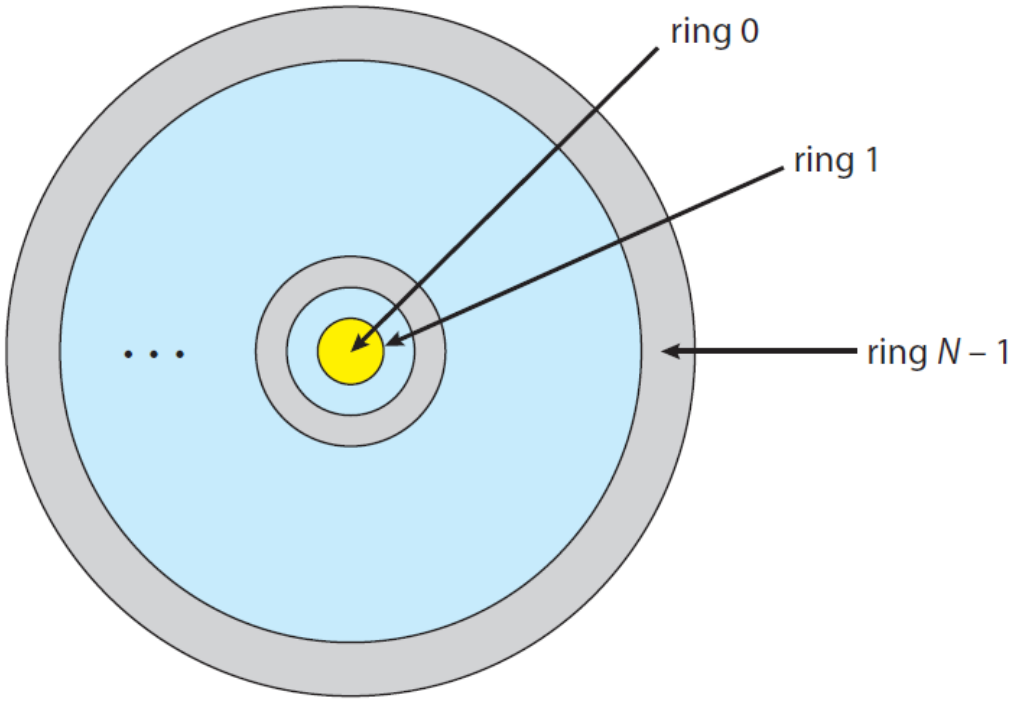
เช่น เวลา open file ก็ให้ permission เท่าที่จะใช้จริง ๆ ว่าจะ read หรือ write เป็นต้น

Compartmentalization



https://en.wikipedia.org/wiki/DMZ_(computing)

Protection Rings



- หลักการคือ outer ring ถัดไป จะได้ functionality เป็น subset ของ inner ring
- Intel processors มี ring 0, 1, 2, 3 ภายหลังเพิ่ม ring -1 ให้ hypervisor
  hypervisor คือ os ที่ถูกออกแบบมาให้รัน vm โดยเฉพาะ เช่น VMware ESXi, Proxmox
  ทำหน้าที่เป็น vm manager ใช้จัดการ vm จำนวนมาก ๆ

64-bit ARMv8 architecture

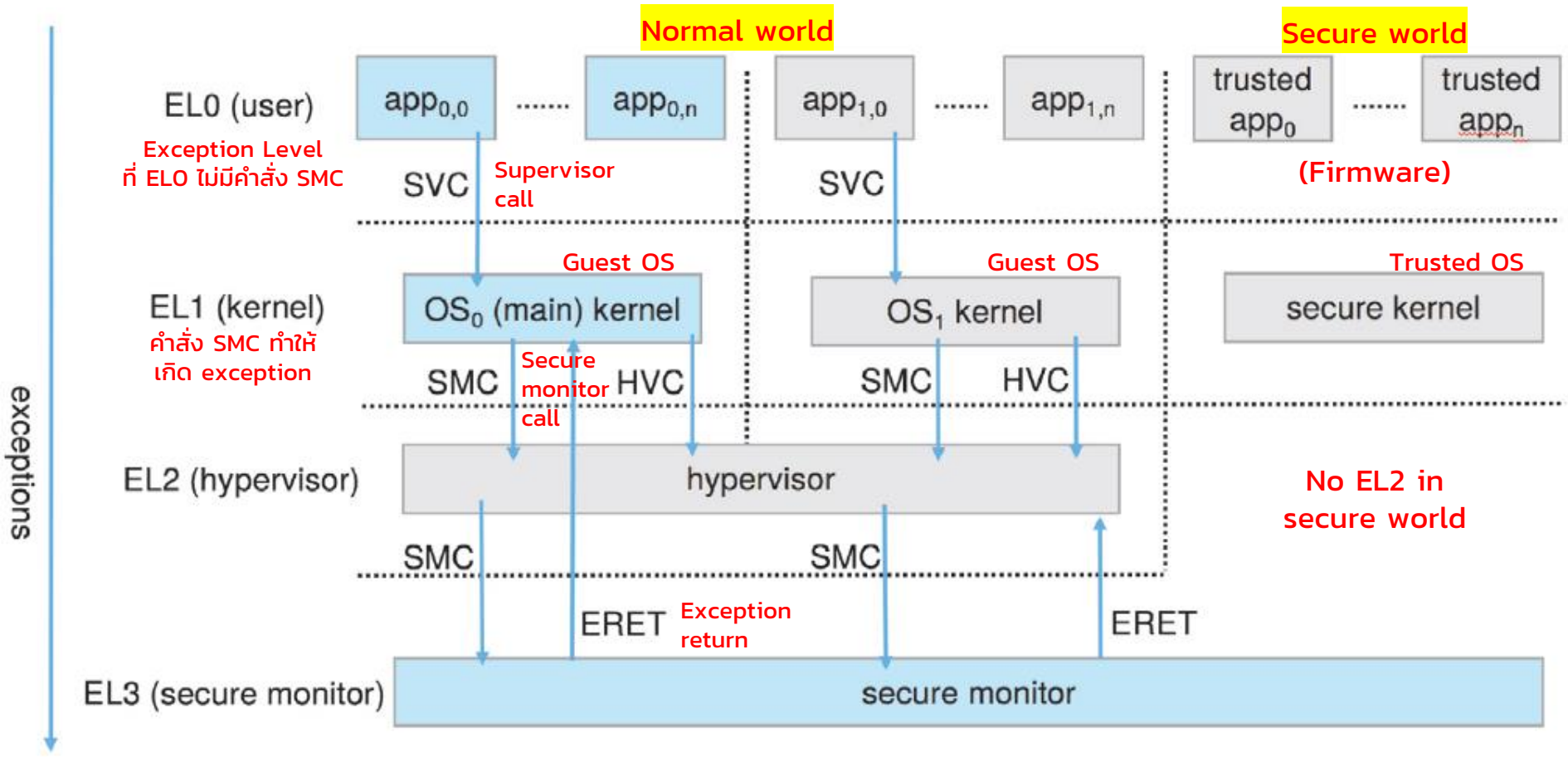


Figure 17.3 ARM architecture.

The role of the Secure monitor is to provide a gatekeeper which manages the switches between the Secure and Non-secure worlds (https://developer.arm.com/documentation/100935/0100/The-TrustZone-hardware-architecture-).

TrustZone (TZ) ใน ARMv7 processors

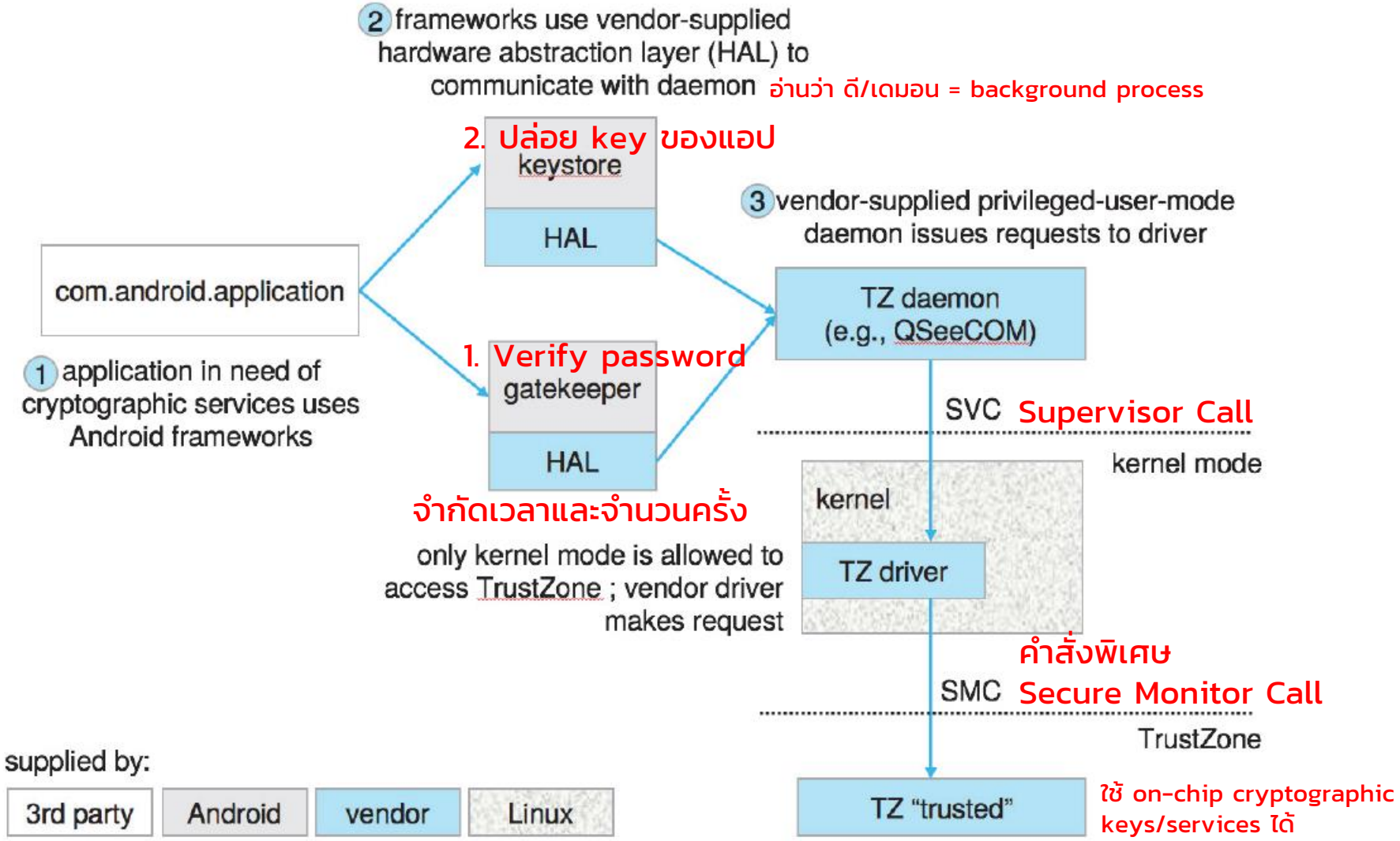
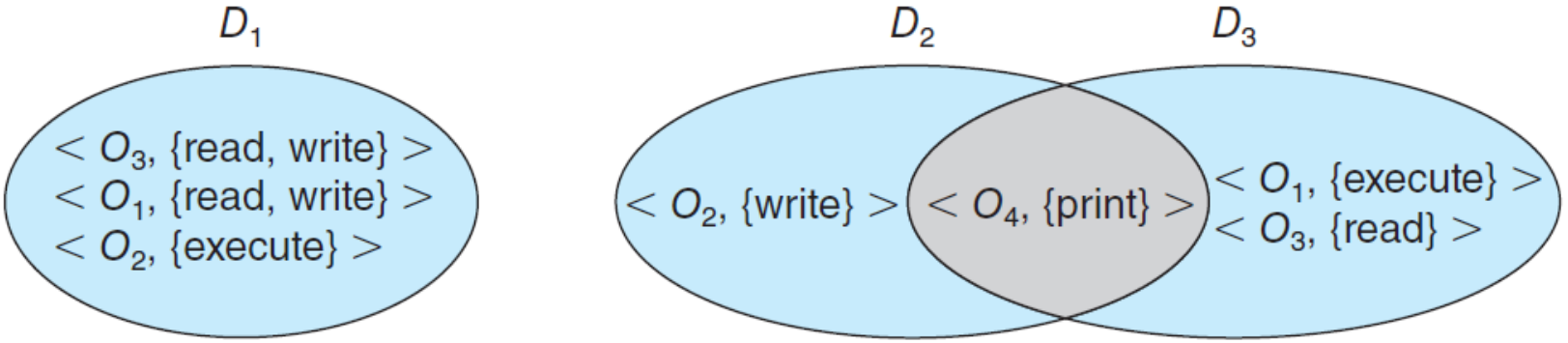


Figure 17.2 Android uses of TrustZone.

ที่ทำทั้งหมดนี้ก็เพื่อป้องกัน ไม่ให้ key ถูกขโมยไปได้

Domain Structure

ถ้า domain เป็น user, user ก็ต้องเป็นสมาชิกของ D1, D2, หรือ D3
O1, O2, O3, ... ก็คือ object ที่สมาชิกในโดเมนนั้นสามารถ {op} ได้ เช่น
object อาจจะเป็น ไฟล์ (file)



Each user, process, and procedure is in a domain.
For example,

a kernel process is in privilege domain (execute ได้ทุกคำสั่ง),
a user process is in the user domain (execute ได้แค่บางคำสั่ง).

Domain ของ kernel process

O_1, {execute}
O_2, {execute}

Domain ของ user process

O_1, { }
O_2, {execute}

O_1 คือ คำสั่งที่ execute ได้เฉพาะ kernel

Access Matrix

object / domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

object / domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

switch ระหว่าง domain ได้ คือ ย้าย object จาก domain หนึ่งไปยังอีก domain หนึ่ง

เช่น switch จาก user ธรรมดา เป็น superuser หรือ switch จาก user mode เป็น kernel mode

Access Matrix

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute		

object / domain	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute	read	

User ใน D2 สามารถให้ read access กับ user ใน domain อื่นได้

เช่น ใน DBMS ให้สิทธิ์นาย ก อ่าน db ได้ แต่นาย ก เอาสิทธิ์นี้ไปมอบให้คนอื่นต่อไม่ได้

Access Matrix

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		read* owner	read* owner write
D_3	execute		

domain \ object	F_1	F_2	F_3
D_1	owner execute		write
D_2		owner read* write*	read* owner write
D_3		write	write

User ใน D_2 เป็นเจ้าของ F_2 สามารถแก้ไข access ของ F_2 ได้ คือ แก้ได้ทั้ง column ของ F_2

- สร้าง Access Matrix สำหรับแอปพลิเคชัน
- DBMS เป็นตัวอย่างที่ดี

```
GRANT privilege_name
ON object_name
TO {user_name |PUBLIC |role_name}
[WITH GRANT OPTION];
```

- ***privilege_name*** is the access right or privilege granted to the user. Some of the access rights are ALL, EXECUTE, and SELECT.
- ***object_name*** is the name of an database object like TABLE, VIEW, STORED PROC and SEQUENCE.
- ***user_name*** is the name of the user to whom an access right is being granted.
- ***user_name*** is the name of the user to whom an access right is being granted.
- ***PUBLIC*** is used to grant access rights to all users.
- ***ROLES*** are a set of privileges grouped together.
- ***WITH GRANT OPTION*** - allows a user to grant access rights to other users.

Chapter 17 Protection