

# Lecture 1: Introduction to Computer Security

**05506044 System Security**

**Dr. Rungrat Wiangsripanawan**

# Objective ( อุบาย )

On top of security

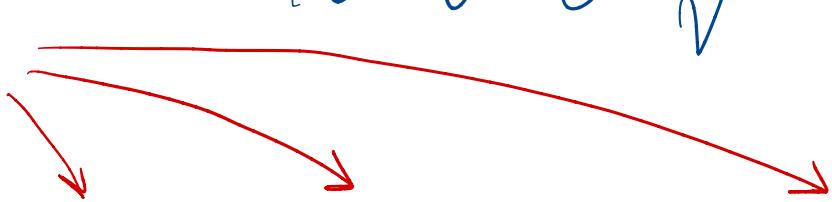
- Explain what is meant by **Computer Security**
- Explain what is meant by **Security Goals**
  - Confidentiality, Integrity, and Availability. ต้องมี CIA
  - Others ex. Authentication accountability and non-repudiation  
ที่พอยู่ในส่วนนี้ เราต้องมาฟัง asset
- Explain what is meant by **asset, threat and attacks.**
- Explain attacks/threat categories
  - Interception/Interruption/Modification/Fabrication

Explain = Know meaning and can give Examples

# *Yokaw 9/12*

## Asset, Threat, Attack, Vulnerability and Control

0:10



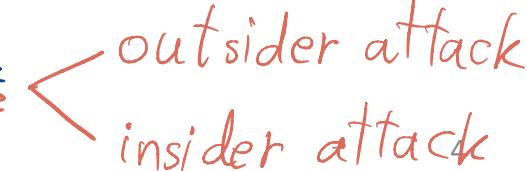
:

# What is Computer Security

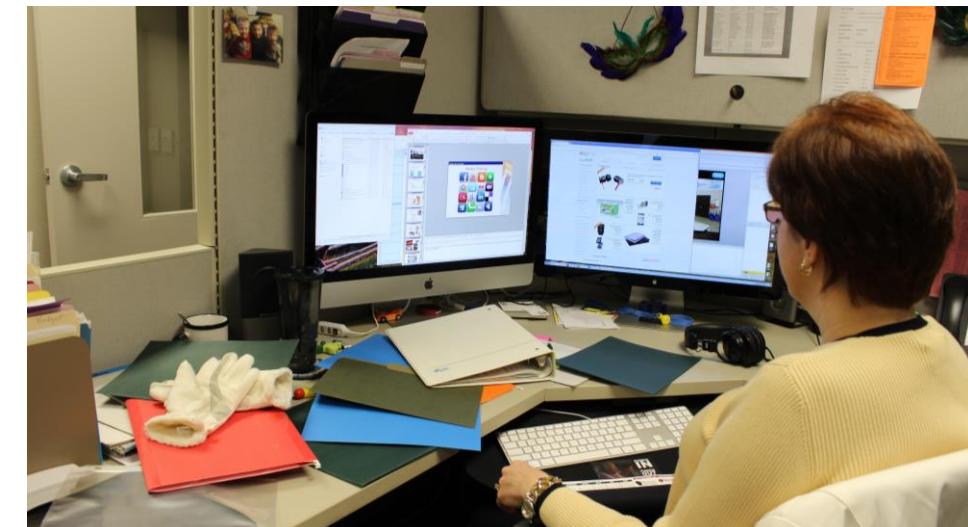
Computer security is about protecting computer\_based assets\_against possible threats.

Computer Security คือการป้องกัน ที่มีค่าหักอย่างของระบบคอมพิวเตอร์ จากภัยคุกคาม

ป้อง data , hardware , people และ software

threats มีโอกาสเกิดแต่ถ้าเกิดแล้ว ก็อ attack  outsider attack  
insider attack

ระบบคอมพิวเตอร์ ประกอบไปด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้ ระบบการเข้ามายื่นต่อ ซึ่งสิ่งเหล่านี้คือ asset ทางคอมพิวเตอร์



This Photo by Unknown Author is licensed under CC BY-NC

# Security in General

When talking about security

1. we need to be able to identify
  - Assets.
  - Threats. / Attacks
    - Vulnerabilities
    - Possible controls. *ชุดของโหนด*
2. estimate the cost and resulting benefits of implementing the **controls** (risk analysis)  
*ประเมินความเสี่ยง*

Damage to assets can be intentional or accidental.

In this course, *ฯพ.ร.บ.ตั้งมิ. บป*

mainly concerned with intentional damages, i.e. where people undertake attacks.



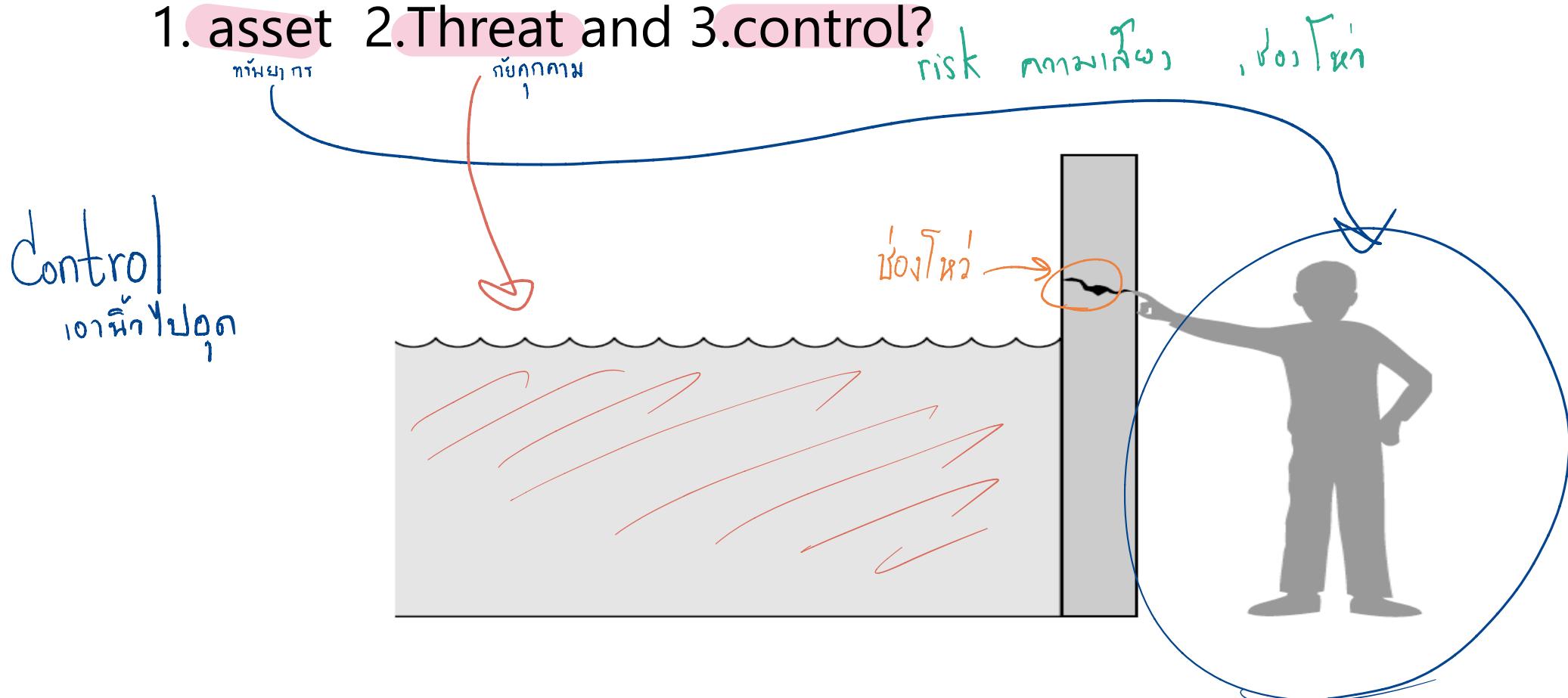
[This Photo](#) by Unknown Author is licensed under [CC BY](#)



# Example1: อะไรคือ threat, asset and control?

จากรูป ให้นักศึกษาอภิปรายว่า สถานการณ์ในรูปคืออะไร และ อะไรคือ

1. asset
- 2.Threat and 3.control?



# Pre-content: เด็กๆ ช่วยครูคิดว่า อะไรคือ

**Computer asset**

**Computer threat**

**Computer vulnerability**

# Asset

- Computer asset or computer system resource
- Hardware
  - Computer systems and other data processing, data storage and data communication devices.
- Software
  - Operating system, system utilities and applications
- Data
  - Files, databases
- People

# Threat (ภัยคุกคาม)

- A **threat** is something which potentially **violates** security. (อะไรก็ตามที่สามารถละเมิดความปลอดภัยของระบบ)
- not necessary that the violation needs to occur to be a threat. (ซึ่งไม่จำเป็นว่าเกิดขึ้นหรือยัง)
- exists when there is a **circumstance, capability , action or event** that could **breach security and cause harm.**
- In other words, a threat is a **possible danger** that might **exploit** a **vulnerability**.

ปัจจัยจากภัยคุกคาม

ภัยคุกคาม , ภัยทาง

# Threat Definitions

[ISO27001]

- potential cause of an unwanted incident,
- which may result in **harm** to a system or organization

**A threat is a possible danger that might exploit a vulnerability. !!!!**

**NIST**

Any circumstance or event with

- the potential to adversely impact
  - organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via
    - unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- Also, the potential for a threat-source to successfully **exploit** a particular **information system vulnerability**.

# Vulnerability

អ្នកដែលមានពេលវេលាដែលបានរាយពី phishing នៅក្នុងទូរសព្ទ

## Several NIST Documents

សារព័ត៌មានយោង នគរបាល USA

### Weakness in

- an information system,
- system security procedures,
- internal controls, or
- implementation

that could be exploited or triggered by  
a threat source.

=> To cause lost or harm

### NIST SP 800-47 Definition

A **flaw** or **weakness** in

- system security procedures,
  - design,
  - implementation, or
  - internal controls
- that could be exercised (accidentally triggered or intentionally exploited) and
- result in a **security breach** or a violation of the system's security policy.

# Attack (การโจมตี)

- An action (of the threat) that could cause the violation to occur.
  - การกระทำที่ทำให้การละเมิดความปลอดภัยของระบบเกิดขึ้น
- We use the term attack to mean **a deliberate attempt**
  - to evade security services and
  - to violate the security policy of a system.
- ในที่นี้เวลาเราพูดถึง attack เราจะหมายถึง ความพยายามที่**เจตนา**ที่จะ
  - ละเมิด และ รุกร้าว เซอร์วิสต่างๆ ที่ทางระบบมีไว้ เพื่อป้องกัน ความปลอดภัย (security services)
  - ละเมิดนโยบายทางความปลอดภัยของระบบ

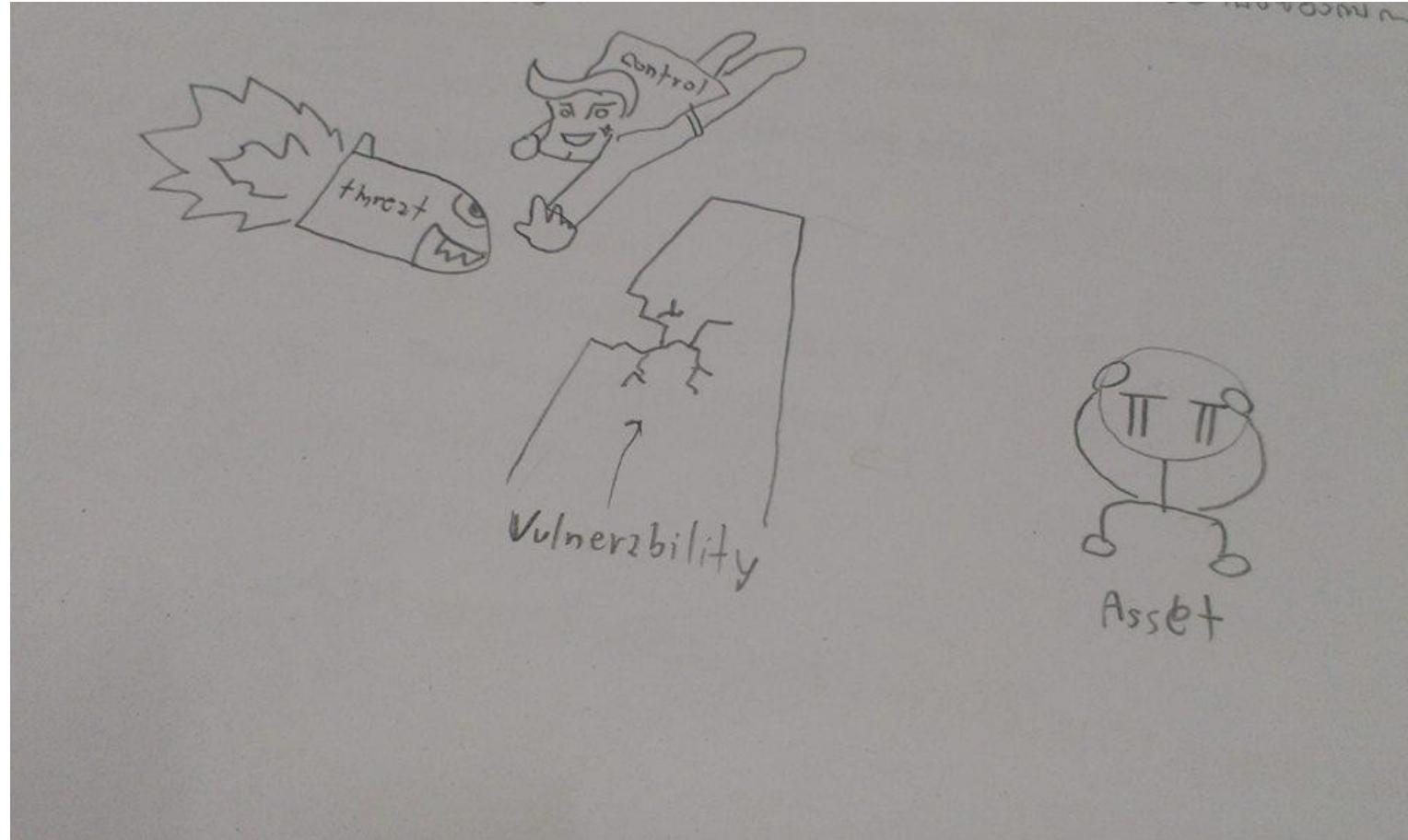
# Control/Countermeasure

- is used as a **protective measure**.
- A control is an action, a procedure, a device or a technique
  - that removes or reduces a vulnerability
- A threat is blocked by the **control of vulnerability**.

- การควบคุมภัยใช้เป็นมาตรการในการป้องกัน เพื่อที่ กำจัด หรือ ลด ช่องโหว่ต่างๆ ที่เกิดขึ้นในระบบ
- วิธีการที่ใช้ในการควบคุมเป็นได้ทั้งการกระทำ การใช้ขั้นตอนต่างๆ การใช้อุปกรณ์และเทคนิคต่างๆ หรือทั้งหมดรวมกัน
- การที่เราสามารถควบคุมช่องโหว่ต่างๆ ของระบบได้ จะทำให้สามารถ ป้องกันภัยคุกคามไม่ให้เกิดขึ้นได้

## Example2:

### What are threat, asset and control?



# L1Q1: ให้นักศึกษายกตัวอย่าง Threat, Vulnerability และ Assets ในเชิงของ Computer Security



## 4

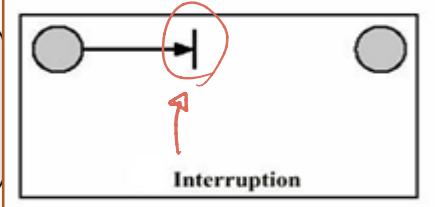
# The four basic attack (threat) types

จุดจังหวะ

## Interruption

ความพร้อมใช้งาน

- an attack on **availability** of an asset.



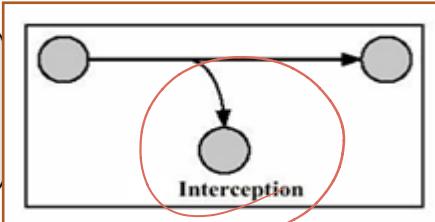
สายเดือด (อยากรู้อยากรึ)

## Interception

ข้อมูล ภัยคุกคามที่รักษาไว้

ความลับ

- an attack on **confidentiality**.



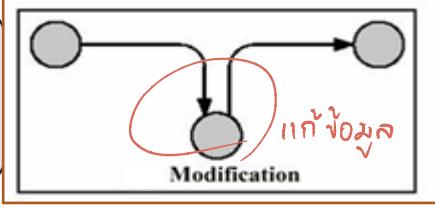
แก้ไข

## Modification

การซ่อนเร้น

ความถูกต้อง

- an attack on **integrity**.



偽合意

## Fabrication

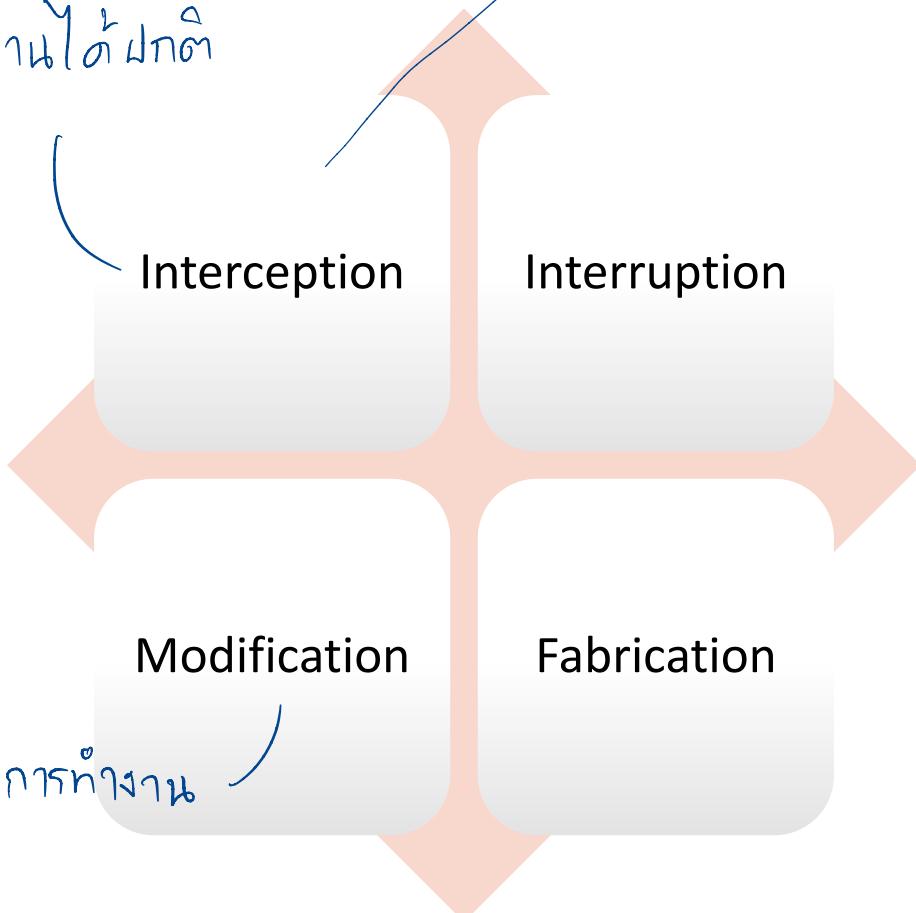
- an attack on **authenticity**.



Let's talk about attacks..more

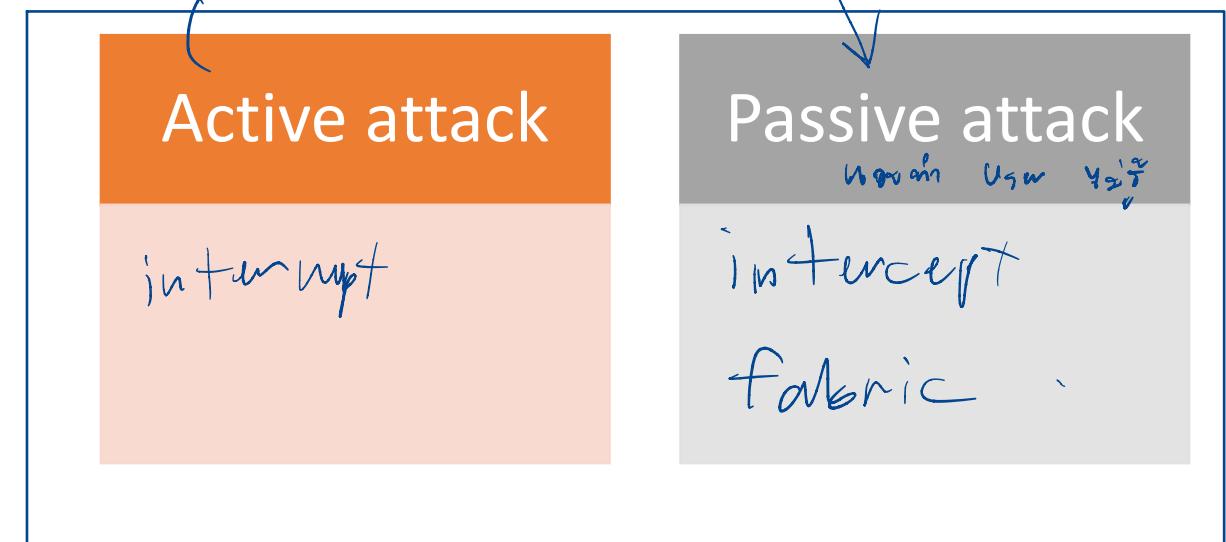
# Types of attack

ສະເປົກການຢ່າງດີ



ກົງນີ້ສະເປົກກາຍ້າຍໍາວາກາກົງນີ້

ຕະຫຼາມ

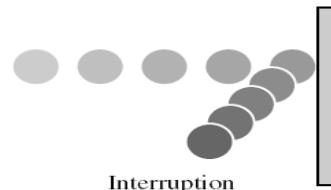


# Interruption

ซอฟต์แวร์ เก็บ

- An asset of the system becomes
  - lost, unavailable or unusable
  - จัดเป็น Active attack
  - Ex. Hardware destruction, software erasure. OS malfunction.
  - Some call this attack as Disruption. interrupt
  - Counter Availability....

ความน่าจะ

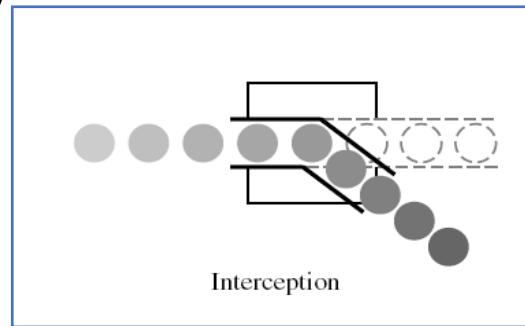


อีกชุด

การโจมตีประเภทนี้  
มีจุดมุ่งหมายใน  
การทำให้ asset  
ของระบบ  
ไม่ได้  
• ใช้งานไม่ได้  
(สูญหาย ใช้  
ไม่ได้ ทำงาน  
ไม่ได้)

# Interception

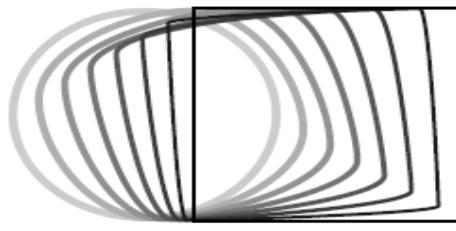
- Some unauthorized party has gained access to an asset => (unauthorized interception of information)
- Passive attack
- Ex. *Wiretapping network, illegal copying of files.*
- Some call it '*disclosure*' รั่วไหล
- *Confidentiality* .... counters this attack.



การโจมตีประเภทนี้  
ระบบยังทำงานได้  
เหมือนเดิม ไม่มีการ  
เปลี่ยนแปลง  
แต่มีจุดมุ่งหมาย  
ในการเข้าถึงข้อมูล  
หรือ asset ของระบบ  
โดยไม่ได้รับอนุญาติ

# Modification

- An unauthorized party
  - not only accesses the asset but also tampers with (modify) it
- Active attack
- Ex.
  - เปลี่ยนข้อมูลใน Database
  - แก้ไขข้อมูลที่ส่งระหว่างกัน (man-in-the middle attack)
- Some call alteration.
- Counter Integrity....(...inconsistency of actions or values)



Modification

การโจมตีประเภท  
นี้นักจากจะ<sup>เข้าถึง asset โดย</sup>  
<sup>ไม่ได้รับอนุญาต</sup>  
แล้ว ยังเข้าไป<sup>เปลี่ยนแปลง</sup>  
<sup>เนื้อหา หรือ การ</sup>  
<sup>ทำงาน asset</sup>  
<sup>นั้นๆ</sup>

# Fabrication

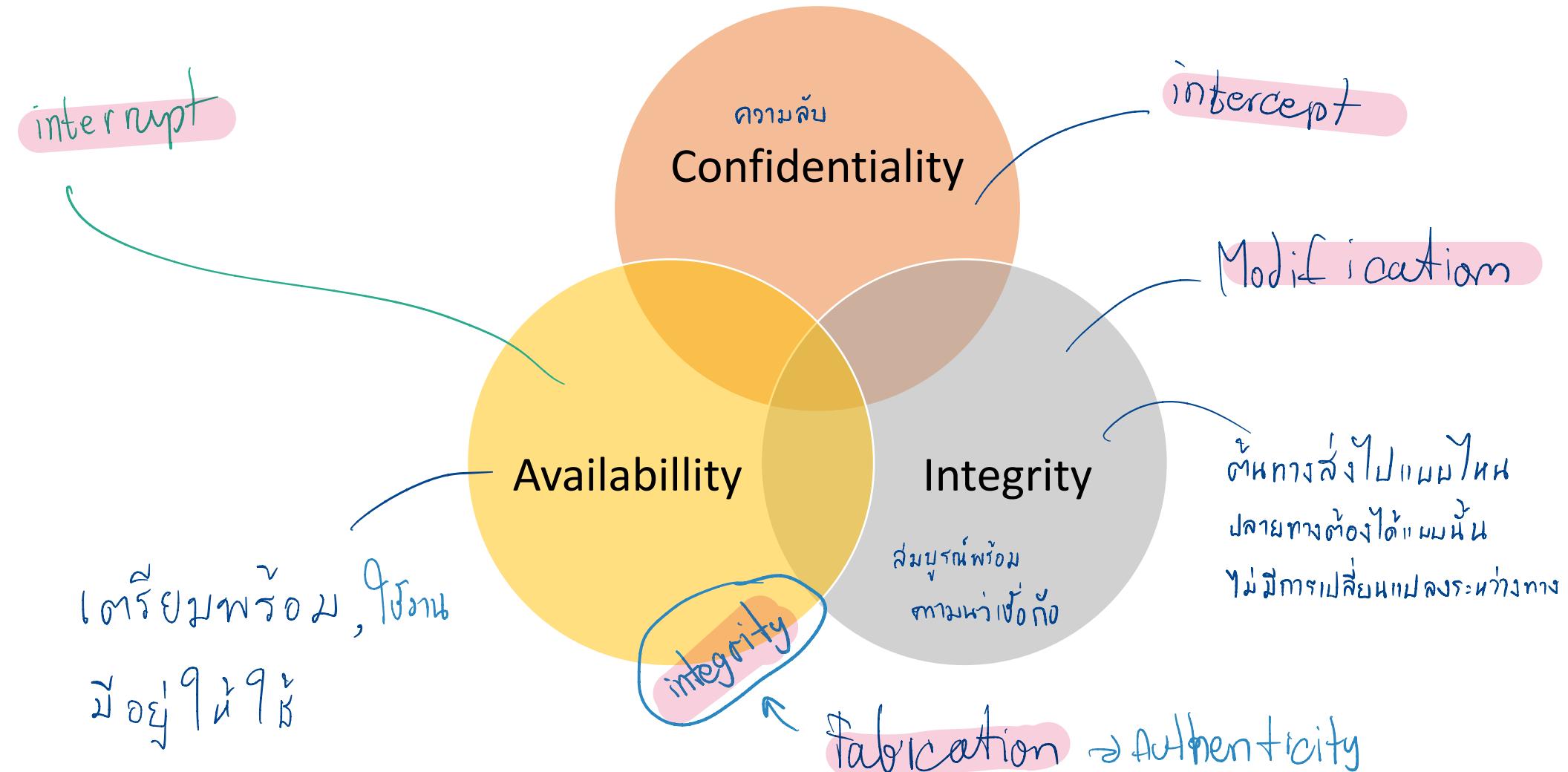
- An **impersonation** of one entity by another.  
(pretend to be someone that they are not)
  - IP Spoofing, MAC Spoofing, DNS Spoofing
  - Ex. a user log into a computer across the Internet but instead reaches another computer that claims to be the desired one
- Some calls **spoofing / impersonate**
- Counter Integrity or authenticity

๑๐๗๒ ๒๕ ๘๘๔

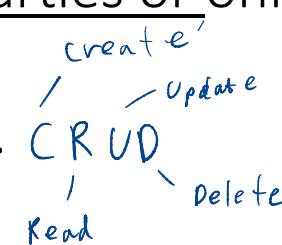
การโจมตี  
ประเภทนี้มี  
จุดมุ่งหมายใน  
การ  
**ปลอมแปลงเป็น**  
**คนอื่น** เพื่อจะใช้  
สิทธิ์ของคนๆ  
นั้น

# Goals of Security:CIA

In security world, no one don't know this CIA. So do you, you must know this CIA otherwise failed the exam ;)



# Goals of security

- We need to know what we mean when we say the system is ‘secure’
- There are three important aspects (CIA)
  - Confidentiality
    - Ensure that computer-related assets are accessed only by authorised parties.
    - Sometimes is called secrecy or privacy
  - Integrity
    - Assets should be modified only by authorised parties or only in authorised ways.
    - Include writing, changing, deleting and creating.  


The diagram illustrates the four operations of CRUD (Create, Read, Update, Delete) as follows:  
- Create: Represented by a blue arrow pointing upwards from the bottom left towards the top left.  
- Read: Represented by a blue arrow pointing downwards from the top left towards the bottom left.  
- Update: Represented by a blue arrow pointing diagonally up and to the right from the bottom left towards the top right.  
- Delete: Represented by a blue arrow pointing diagonally down and to the right from the top left towards the bottom right.
  - Availability
    - Assets are accessible to authorised parties at appropriate times.

# Integrity ความสมบูรณ์พร้อม

- Precise/unmodified/ modified only in acceptable ways/modified only by authorised processes/ consistent etc.
- Assets **ไม่ควรที่จะถูกแก้ไข** หรือ **ปลอมแปลง** จากผู้ที่ไม่มีสิทธิในการแก้ไข หรือ **ปลอมแปลงนั้น**
- Covered two related concepts
  - **Data integrity**
    - Assures that information and programs are changed only in a specified and authorised manner
      - ความสมบูรณ์ของข้อมูล
        - รับรองว่าข้อมูลและโปรแกรมมีการเปลี่ยนแปลงเฉพาะในลักษณะที่กำหนดและได้รับอนุญาตเท่านั้น
        - ความสมบูรณ์ของระบบ
          - มั่นใจได้ว่าระบบ
          - ดำเนินการตามวัตถุประสงค์ในลักษณะที่ไม่บกพร่อง ปราศจาก การจัดการโดยไม่ได้รับอนุญาตโดยเจตนาหรือ โดยไม่ได้ตั้งใจของระบบ
  - **System integrity**
    - Assures that a system
      - performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system.

# Availability

លទ្ធផលរៀង, សេវានៃ

ផែវកុវត្ថិ

នគរណ៍លើមុខងារនៃសេវានៃការបញ្ចូលការងារ

- Sometimes known by its opposite -> Denial of Service
- Applied both to **data** and to **services**
- A *data item, service or system* is available if
  - There is a **timely response** to our request
  - Resources are **allocated fairly** (no requester is favored over others)
  - The service or system involved follows a philosophy of **fault tolerance**.
    - HW or SW fault
  - The service or system can **be used easily** and in the way it was intended to be used.
  - Concurrency is controlled
    - Simultaneous access deadlock management are supported as required.

# Other goals

- นอกจากรากฐานแล้ว ยังมี วัตถุประสงค์อื่นๆ

- Authentication \*\*\* *พิสูจน์ user*

- Accountability (logging auditing) *พิสูจน์ว่าได้เป็นคนทำ*

- \* Non-repudiation (only possible with Public key cryptography in Digital Signature)  
*ผู้รับไม่ได้รับเจ้าของข้อมูล*

*ผู้รับไม่ได้รับเจ้าของข้อมูล*

*คนส่งจะปฏิเสธไม่ได้ถ้าไม่เป็นคนส่งข้อมูล*

*เกิดขึ้น ทราบ Digital signature*

# Recalled Asset

สิ่งของค้างชั่วคราว

Computer asset or computer system resource

Hardware

- Computer systems and other data processing, data storage and data communication devices.

Software

- Operating system, system utilities and applications

Data

- Files, databases

People



# Hardware Vulnerabilities

can be **occurred accidentally or intentionally.**

- Accidental damage such as coffee, dust or power surges
- deliberate damage usually involved theft or destruction.

ทางการภาพและการบริหาร  
มีการใช้มาตรการรักษาความปลอดภัยเพื่อจัดการกับช่องโหว่ประเภทนี้

## Physical and administrative security

measures are used to deal with this type of vulnerabilities.

เกิดขึ้นได้โดยบังเอิญหรือใจ

- ความเสียหายจากอุบัติเหตุ เช่น กาแฟ ฝุ่น หรือไฟกระชาก
- ความเสียหาย โดยเจตนามักจะเกี่ยวข้องกับการโจรมกรรมหรือการทำลาย

A major threat to computer hardware is the threat to 'A'-availability.

ภัยคุกคามที่สำคัญต่อฮาร์ดแวร์คอมพิวเตอร์คือภัยคุกคามต่อความพร้อมใช้งาน 'A'-availability

物理安全 Physical Security

# Software Modification → ໂກງວ່າ

# Software vulnerabilities

## ภัยคุกคามต่อความพร้อมใช้งาน

- สามารถใช้การจัดการการกำหนดค่าซอฟต์แวร์อย่างระมัดระวัง เพื่อรักษาความพร้อมใช้งานสูง

# Software deletion

- threat to availability
  - Careful software configuration management can be used to maintain high availability

## ภัยคุกคามต่อความพร้อมใช้งาน

- ทำให้ซอฟต์แวร์ล้มเหลว
  - ภัยคุกคามต่อความสมบูรณ์และความถูกต้อง
  - โปรแกรมที่ยังคงทำงานแต่มีพฤติกรรมแตกต่างจากก่อนอดีต มลแวร์

# Software modification

- threat to **availability**
    - Cause the software to fail
  - threat to **integrity** and **authenticity.**
    - A program that still functions but behaves differently than before Ex. Malware
  - ทำ เหชอพตแวรลเมหลวง
  - ภัยคุกคามต่อความสมบูรณ์และความถูกต้อง
  - โปรแกรมที่ยังคงทำงานแต่มีพฤติกรรมแก่ก่อนอดีต มัลแวร์

สำเนาซอฟต์แวร์ที่ไม่ได้รับอนุญาต

# Software theft (software piracy)

- Threat to confidentiality สำเนาซอฟต์แวร์ที่ไม่ได้รับอนุญาต
  - Ex. Unauthorised copy of the software

# Data Vulnerabilities

ថែរបស់

ការអនុវត្តន៍  
ការគ្រប់គ្រងទិន្នន័យ

## Data Confidentiality

- An unauthorised read of data is performed.
- Ex.
  - Wiretapping
  - Data Breach ដែលសំណងចូរបាយកំពង់

ទេរងទេរង ខ្លួនខ្លួន

## Data Integrity

- Ex. Existing file are modified or new files are fabricates.
- Salami attacks.
- Replaying messages to cause a bank to credit the same account again.

សំណោចអឺប៊ីវេរីទៀតឱ្យទៅទិន្នន័យ

# More Examples: Damaged to software/data \*

វិនិយោគនៃការប្លង់ទិន្នន័យ



Deletion (interruption):	<ul style="list-style-type: none"><li>Erasing a file, or copying it.</li></ul>
Software Modification:	<ul style="list-style-type: none"><li>cause a program to <b>crash</b> immediately, or at a certain time (<b>logic bomb</b>),</li><li>can make program do what it is not supposed to do.<ul style="list-style-type: none"><li>Ex. <b>modifying access rights</b> while copying.</li></ul></li></ul>
Data modification	<ul style="list-style-type: none"><li><b>Replaying</b> used data,</li><li>fabrications of messages etc.</li></ul>
Software interception:	<ul style="list-style-type: none"><li>Stealing software (including piracy).</li></ul>
Data interception:	<ul style="list-style-type: none"><li>Breaching confidentiality of data Ex. by<ul style="list-style-type: none"><li>Wiretapping</li><li>Packet sniffing</li></ul></li></ul>

# Other exposed assets - Network

- Networks.
  - Specialised collections of hardware, software and data
  - Additional **problems** that involve the **interaction of system components** and outside resources **arise.**
- Ex.
  - Lack of physical protection
  - Use of insecure shared media.
  - Inability of a network to identify remote users

# Other exposed assets - Access

- Access leads to **three types** of vulnerability
  - An **intruder** may **steal** computer time to do general-purpose computing that **does not attack the integrity** of the system.
    - Cryptomining
  - **Malicious access** to a computer system where an intruder eventually destroys software or data.
  - **Unauthorised access** may deny service to a legitimate user.

# Computer Criminal

- Amateurs (script kiddies)
- Hacker  
602
- Crackers or **malicious** hackers
- **Career Criminals** มิจฉาชีวัน
  - Mike Danseglio, a security project manager with microsoft.
    - *In 2006, the attackers want to pay the rent, They don't want to write a worm that destroys your hardware.*
- Terrorists จุติหิ
- Shut down the national power resource.

# Method of defense: Ways to do it.



- Prevent it ป้องกัน
- Deter it กีดขวางไม่ให้เข้า
- Deflect it (change target) ลบชื่อ
- Detect it ตรวจส่อง
- Recover it from its affects. ฟื้นฟูระบบ
  - ตย. การ Recovery จากการโดน ransomware
  - <https://www.thaicert.or.th/papers/general/2017/pa2017ge002.html>

ดึงข้อมูลจากที่ฟื้นมาอีกที่หนึ่ง

# Method of defense: Control

ការពិន្ទុការណ៍

- Encryption
- Software controls
  - Internal program controls.
    - Access limitation in a database management program
    - Operating system and network controls.
      - Access right by O.S.
    - Independent control programs
      - Password checking.
    - Development controls
      - Quality standards under which a program is designed, coded, tested, and maintained to prevent software faults.

Access Control ឧប្បរភ័យការដោះស្រាយទូទៅ ចំណាំការងារក្នុងវិវាទ  
ឱ្យកើន Interception ឬ = Modifine

# Method of defense: Control Cont.

- Hardware controls.
  - Use of smart cards, locks, firewall, intrusion detection systems
  - Hardware **implementation of encryption**.
  - **Chip sets** with embedded security functionality,
- \*\*\*Policies and procedures
  - Frequently **changes of passwords**
  - Legal and ethical controls (codes of ethics for computer professional)
- **Physical controls** ฝารកษา

# Effectiveness of Controls

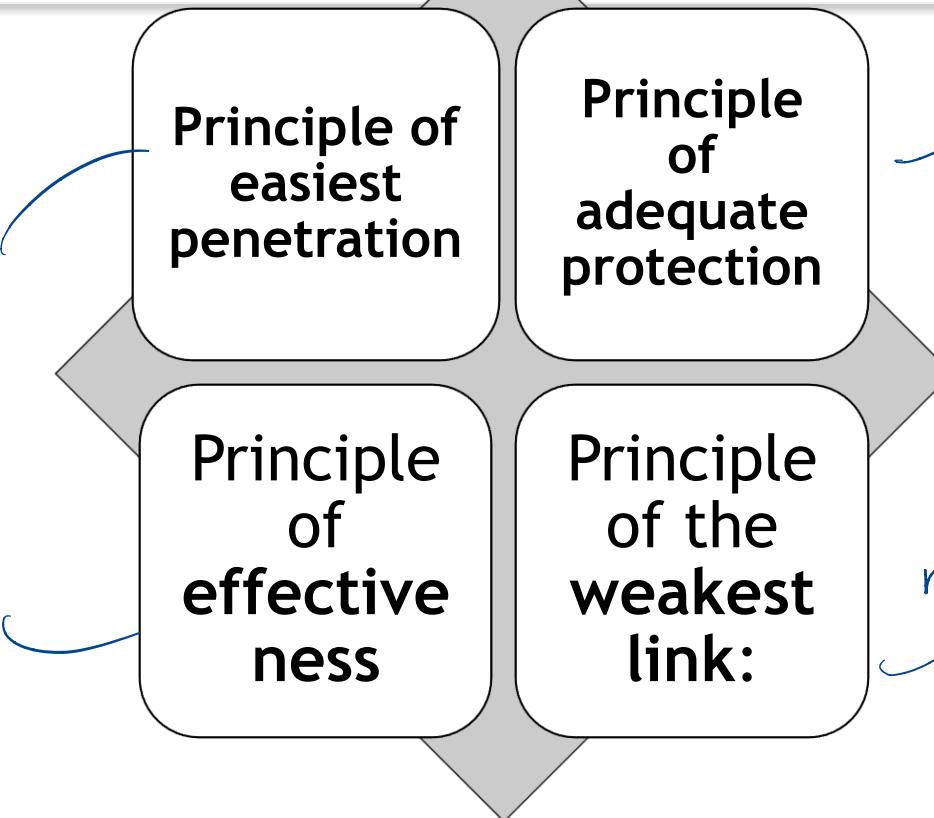
- Awareness of Problem
  - People will willingly cooperate.
- Likelihood of Use *જો નાની વિધાની પ્રક્રિયા કરી શકતી નથી*
  - No control is effective unless it is used.
- Overlapping Controls
  - Several different controls may apply to address a single vulnerability
  - Ex. Security for a microcomputer application
    - Controls of program access to the data
    - Controls on physical access to the microcomputer and storage media
    - File locking to control access to processing programs.
- Periodic Reviews.

# Security Principles: Construction and analysis I

ออกส่อน

เจา=ธ=ผมง่ายสุด

นี่ดูดี



หลักการในการสร้างและวิเคราะห์ระบบความปลอดภัย

# Principle of easiest penetration

នេរតាហ័រ កំពង់ ចុះហាន ការវិភាគ  
bomkhanh

- លក្ខារណី ចាំបាច់គ្រប់គ្រងការប្លើប្លាញទូទៅ
- Intruders will use **any available means of penetration**.
- (ដូចជាប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ ឬការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ)
- This makes **security assessment** of security a **very difficult** problem because **all possible ways** of breaching security must be **examined**.  
(ការស្នើសុំវិធាននៃការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ និងការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ)
- Moreover, the penetration analysis must be done repeatedly especially, whenever the system and its security change.  
(នៅពេលការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ និងការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ)
- Strengthening one aspect of a system may simply make another means of penetration more appealing to intruders. (ការពិនិត្យការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ និងការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធដែលមានការប្លើប្លាញដោយប្រើប្រាស់ប្រព័ន្ធ)

# Principle of adequate protection\*\*\*

เพียงพอ

- หลักการนี้ จะเน้นที่การป้องกันแบบพอเพียง prudent protection principle
- Also known as the **timeliness principle**. ex คงอุดติดตาม
- This means items should only be **protected while** they are **valuable**, and that the **level of protection** should be consistent **with their value**.  
( ป้องกันในขณะที่ข้อมูลยังมีค่าอยู่ )
- **practical principle** which **underlies** a large proportion of modern computer security.

# Principle of effectiveness

## Principle of weakest link.

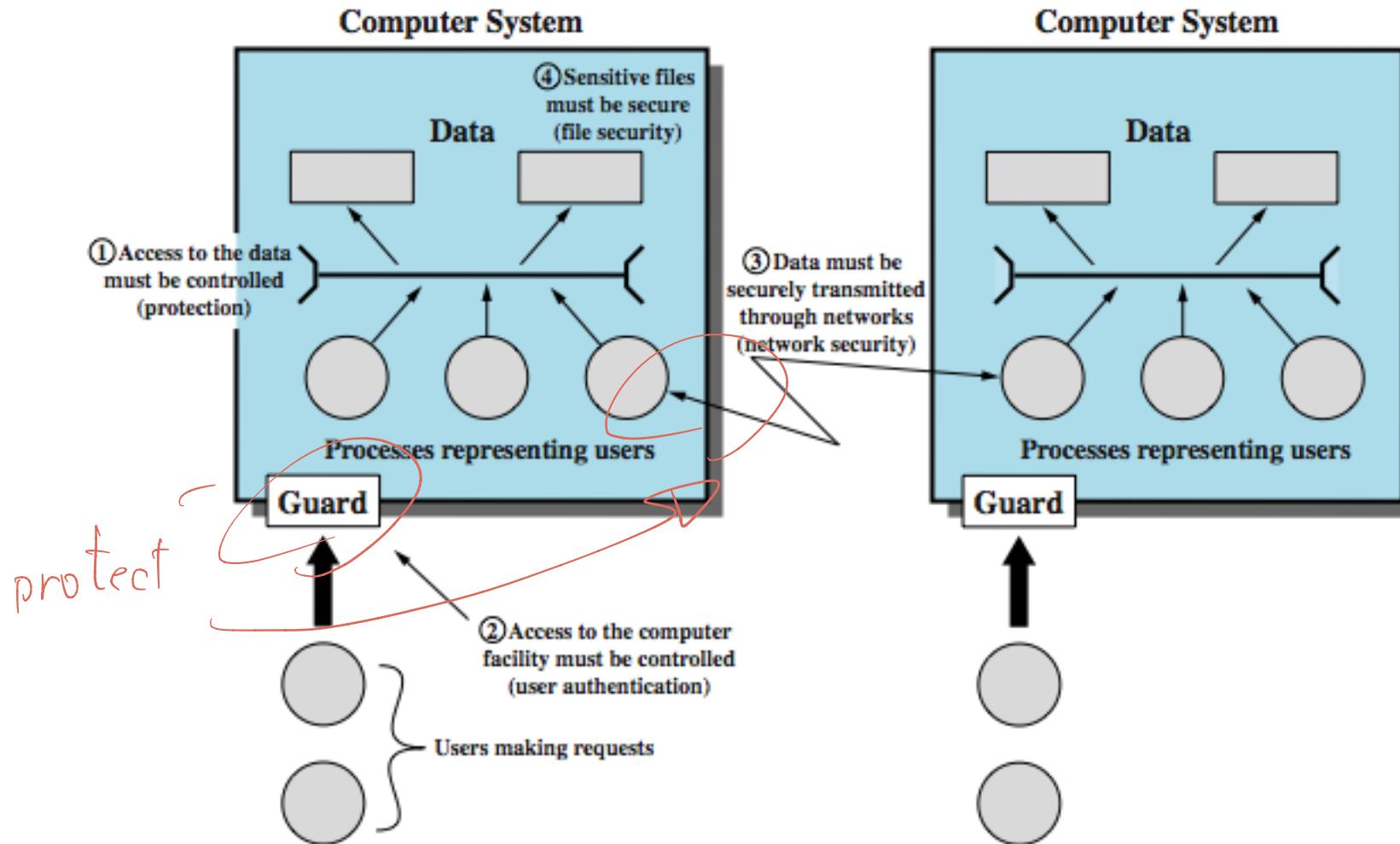
### Principle of effectiveness

- Controls must be used properly to be effective.
- Controls should be efficient, easy to use and appropriate.
- หลักการนี้จะ คำนึงถึงประสิทธิภาพของ Control ที่นำมาใช้ ว่า เมื่อใช้แล้วใช้ได้มีประสิทธิภาพ ใช้ง่าย และ เหมาะสมหรือไม่

### Principle of the weakest link

- Security is only as strong as the weakest link in the system.
- หลักการนี้ ความปลอดภัย ของระบบจะเท่ากับ ความปลอดภัยของ weakest link

# Scope of Computer Security \*[1]



# References:

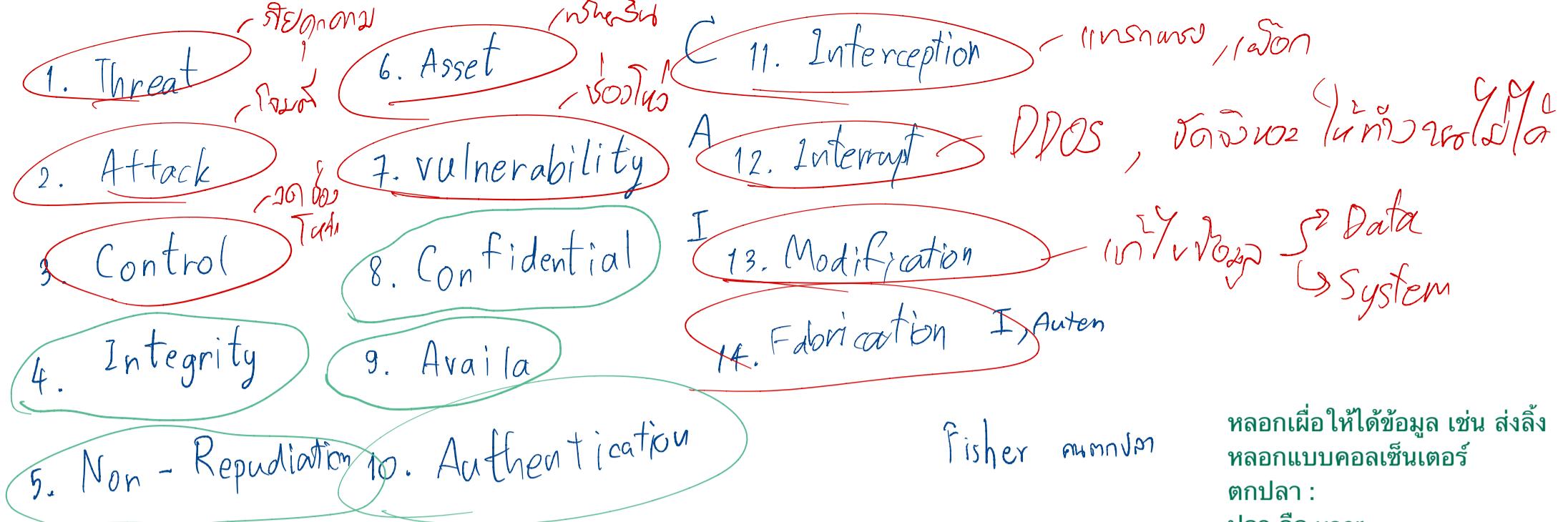
- [1] Lecture slides prepared by Dr Lawrie Brown (UNSW@ADFA) for “Computer Security: Principles and Practice”, 1/e, by William Stallings and Lawrie Brown, Chapter 1 “Overview”.
- [2] Computer Security: Principles and Practice, W. Stalling and L. Brown, 2nd edition, Pearson Education, 2012.
- [3] **Security in Computing**, Charles Pfleeger, Shari , and Jonathan Margulies, 5<sup>th</sup> edition, Pearson Education, 2015.

ឧបករណ៍សម្រាប់លោកស្រី

Can you answer these questions? If not... you have to.

- Explain what is meant by **Computer Security**
- Explain what is meant by **Security Goals**
  - Confidentiality, Integrity, and Availability.
  - Others ex. Authentication accountability and non-repudiation
- Explain what is meant by **asset, threat** and **attacks**.
- Explain **attacks/threat categories**
  - Interception/Interruption/Modification/Fabrication

Explain = Know meaning and can give Examples



หลอกเพื่อให้ได้ข้อมูล เช่น ส่งลิงค์  
หลอกแบบคอลเซ็นเตอร์  
ตกลา :  
ปลา คือ user  
ทะเล internet  
เหยื่อที่ใช้ล่อ link

phishing = Fishing

Factor # sth = something

1. sth you know = Password Security

Two step Vean

2. sth you posses (you have) = Debit card

⇒ OTP

3. sth you /are do = share biome

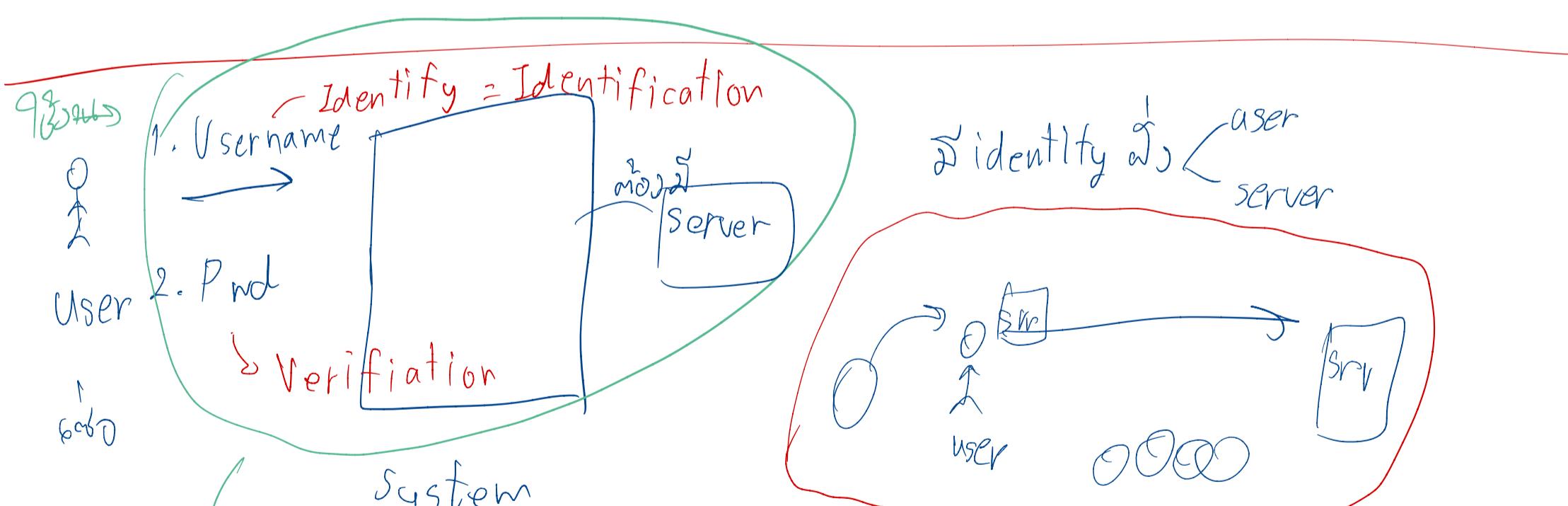
⇒ Google Authorization

Biometric

⇒ Email

2SV | MFA 2FA

Two Factor Auten



→ identification

↳ verify → pwd

Password Threat

- Trojan
- Phishing
- รบดิบดี
- หัก

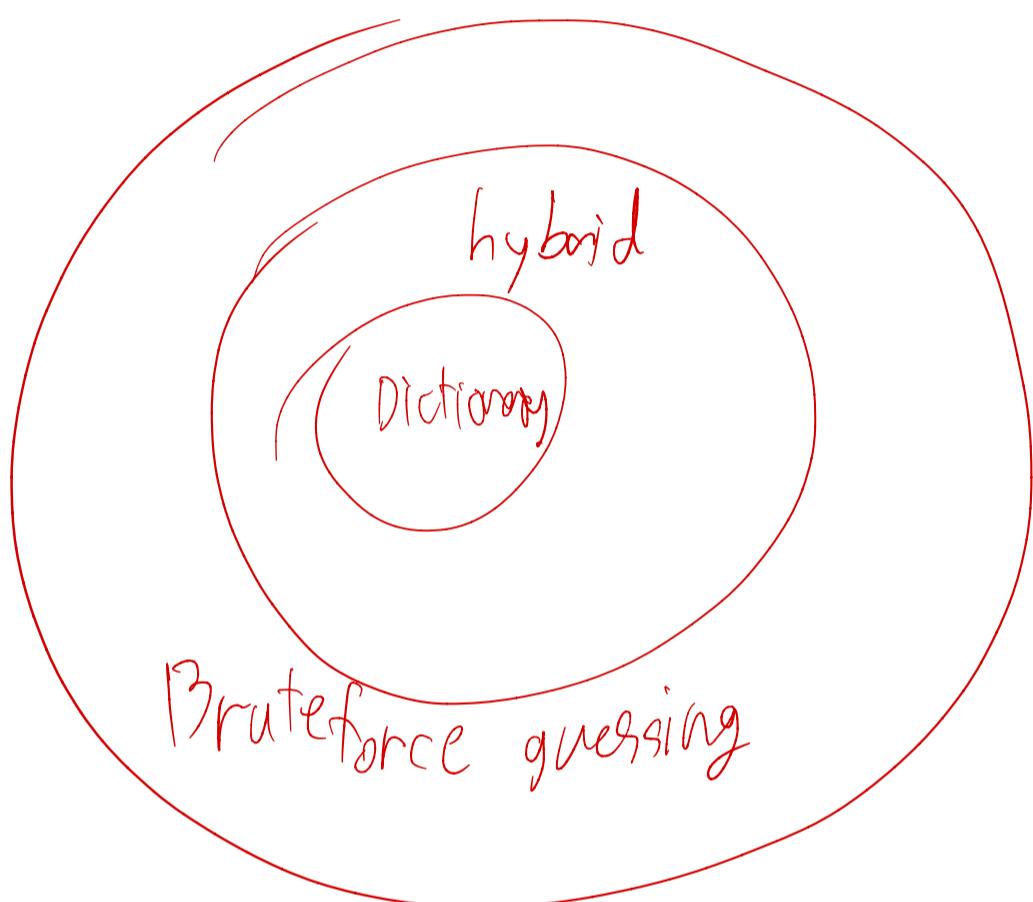
Password guessing

Password Exposer

Bruteforce attack

Dictionary Password Attack

Social Engineer



Can you answer these questions? If not... you have to.

- Explain what is meant by **Computer Security**
- Explain what is meant by **Security Goals**
  - Confidentiality, Integrity, and Availability.
  - Others ex. Authentication accountability and non-repudiation
- Explain what is meant by **asset, threat** and **attacks**.
- Explain **attacks/threat categories**
  - Interception/Interruption/Modification/Fabrication

Explain = Know meaning and can give Examples