① Introduction to computer security

10 security principles

1) Least Privilege ต้องมี access + grant
2) Defense in Depth ผถาม password หลายครั้ง
3) Secure failure
4) Secure the weakest link
5) Compartmentalization แบ่งส่วน จะได้พังแค่บางส่วนได้
6) Simplicity
7) It's hard to hide secret ถ้าลับก็ไม่ต้องพูด
8) Promote Privacy
9) Don't extend trust easily
10) Trust the community

Security vs Privacy

security = Free from risk of lost = บอกได้ว่าใคร มีสิทธิ์ทำอะไร เมื่อไหร่
= The protection of resources from being accessed by an unauthorized person at a particular time

Privacy = The freedom to control access to our personal information, depending on intent
→ make an agreement

* No privacy without security

② Security Component

The AAA of security ต้องมี ถ้าขาดจะไม่มี security
- Authentication เป็นใคร
- Authorization role นี้ทำอะไรได้บ้าง
- Accounting (Auditing)

Supporting Concept
- Integrity (Authenticity)
- Software engineering & Threat modeling
- Validation of Input

③ Authentication พิสูจน์ได้ว่าเป็นของแท้ ของจริง ของเดิม

Validate คุณสมบัติบางอย่าง

สิ่งที่รู้ Prearrange questions, Password, OTP, Challenge and Response
สิ่งที่มี การ์ด กุญแจ
สิ่งที่เป็น Biometric

การโจมตี Hash / Password Hacking เพราะทำ f(x) → x ไม่ได้
1) Dictionary Attack เดา x ตาม dictionary จนกว่า f(x) จะตรง
2) Bruteforce generate strings every possibility
3) Rainbow table generate strings แล้วสร้างตาราง hash

④ Authorization อนุญาต หรือ ไม่อนุญาต

ใช้ Policy (นโยบาย), App-based, to guide and determine present and future decisions
มี Type enforcement คล้ายกับตำรวจ บังคับใช้กฎ
Secure system - starts in auth state and cannot enter unauth state

Security Policy = ประโยคใดๆ ที่แบ่งการกระทำเป็น 2 กลุ่ม คือ Secure / Insecure (Auth/Unauth)
- Confidentiality who can read : หน้าที่ในการปกปิดความลับ
- Integrity who can write / alter
- Availability when to access

Access Control Model - ใครเป็นคนสร้าง Policy

Mandatory Access Control (MAC) จำเป็นต้องทำ ไม่ทำแล้วระบบพัง	Discretionary Access Control (DAC) เจ้าของข้อมูลจัดการเองทั้งหมด	Role-based Access Control (RBAC) คนเข้าใจ Role เป็นคนสร้าง
• Admins control users • Multilevel systems • Sensitivity labels	• Access rights and permissions • ownership • ใช้ร่วมกับ MAC	• Least privilege • Access ขึ้นกับ Action • จำกัดสิทธิ์เพื่อให้ทำงานได้ • How to define Role - Combination of MAC and DAC Admin แบ่งกลุ่ม = MAC แต่ละกลุ่มตั้ง Policy เอง = DAC

Access Control Matrix - Product of Policy
- Subject on rows, Resource on Columns, Specify the Rules
  - Access Control List - Who can do what with this object
  - Capability - What I can access

Security Models

1) Multilevel security (within organization) usage: Bell-Lapadula for Auth, Biba for Unauth

1.1 Bell-Lapadula ไม่เชื่อถือข้างบน
- simple property No read up
- *-Property No write down
- Tranquility property มี simple, * ในระหว่างทำงานเท่านั้น

1.2 Biba ไม่เชื่อถือข้างล่าง
- Never read down or write up
- Confidentiality
- Windows security warning when installations

2) Multilateral security (Between departments)
- China Walls model : มีช่องเล็กๆ คัดของที่ผ่านได้
- Reverse engineering

⑤ Log Analysis (Part of Auditing) ข้อมูลที่เก็บไว้เพื่อตรวจสอบย้อนหลัง

1) Log Collection
- Syslog
- Event log
- App logs
- Firewall logs
- Network logs
- Infrastructure logs

2) Event Management
- What (All / Filtered)
- How (Centralized / Backup / Format / Raw / Parsed)
- Preprocess (Index / Summaries)
- Who (Direct / Program / Dashboard / Data sensitivity)

3) Analysis
- How (Manual / Automate)
- Technique (Stat / Anomaly / Association / AI/ML)
- Time (Real-Time / Post-Mortem)

4) Response
- Reporting
- Incident response
- Evidence preservation
- Lesson learned

⑥ Physical security (Defense against the dark)

- การจับ computer เพื่อโจมตีโดยตรง, ทำได้ถ้ามีเวลานานพอและมีเครื่องมือที่เหมาะสม
1) Keylogger
2) HTTP request ที่ฝัง script ใน parameter
3) โจมตีเชื่อมต่อ network
4) คลิกลิงก์ที่ฝัง script

⑦ Integrity and Basic Encryption

Integrity - ข้อมูลเหมือนเดิม ไม่ถูกเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต/ไม่จงใจ
- require hardware support → Ring by Multics
  - memory compartment (page and segmentation)
  - inner ring (kernel) can access outer ring
  - interprocess communication through kernel
  - ต้องมีอย่างน้อย 2 rings (kernel/user)

Trust (เชื่อใจ)
- processor เชื่อว่า chip จะทำงานถูก
- user/dev เชื่อว่า user จะทำงานตามที่คาดหวัง
- SW/process เชื่อว่า code จะทำงานถูก

เช่น memory segmentation
บอกว่า memory ส่วนนี้เป็นของใคร แล้วคาดหวังว่าผู้อื่นจะไม่เข้าถึง * ไม่ดี → minimize trust

Sandbox by Java Applet
- If trust → run anywhere
- else → run in sandbox (Cannot access local files)
- trust - ขึ้นกับคนเขียนโค้ด

Domain
- กำหนดขอบเขตการทำงานของโปรแกรม
- Isolation

Encryption when no hardware support (network)
- Monoalphabetic Substitution Cipher (Julius Caesar) ข้อเสีย บางตัวอักษรถูกใช้บ่อยกว่าตัวอื่น

1) Hash Digest - Message Digest (MD5, SHA1)
- oneway function
- vary input to fixed size output
- collision-free
- integrity check
- sometimes not considered as encryption (no decryption)

2) Symmetric encryption

2.1 Stream Cipher ยืดความยาว key ให้เท่า input แล้วเทียบ output ใน matrix

2.2 Block Cipher n×n cipher block, block size = k ตัวกรอบเทียบกับตัวรอบๆ
- need hardware support vector operation

Mode of operation
1. Electronic CodeBlock (ECB) เอา input ไปให้ encryption - ยังเห็น pattern ของรูปเดิม
2. Cipher Block Chaining (CBC) มี Initial Vector (IV) xor input แล้ว next IV = output
3. Cipher feedback (CFB) เอา IV ไป encrypt แล้ว xor กับ input
4. Counter คล้าย IV

3) Asymmetric encryption - Public key
key pair : keep private, distributed public
Q : Bob เขียน Alice อ่านได้คนเดียว
A : (message Bob's private) Alice's public concern Alice อ่านได้คนเดียว

Performance, security Tradeoff			
fast / low	Hash,	Symmetric,	Asymmetric slow / high security

Security Protocol

speed | scale

1) Digital signature ส่ง plain text และ signature (hashed + encrypted) ไปด้วยกัน ตรวจสอบ integrity ได้
2) HTTPS/SSL/TLS Client สร้าง key เข้ารหัสด้วย pub key ของ server แล้วส่งกลับไป
แล้ว server จะเข้ารหัส content ด้วย key นั้นแล้วส่งกลับมา key = symmetric encryption

⑧ Public Key Infrastructure

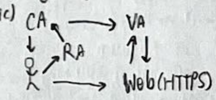
Digital Certificate - a trusted document issued and signed by a trusted third party with digital signature - ถ้าไม่น่าเชื่อถือ ก็ทำให้เป็นคนจริงๆ ยาก

Main Components : Issuer (CA), Subject, Subject Public Key, Issuer digital signature

self-signed Certificate = ออกหนังสือรับรองตัวเอง

Public Key Infrastructure - set of roles, policies, procedures for the registration, management, validation of public key

PKI parties
1. Certificate Authority (CA) Gen key, Revoke, Back-up, Cross-Certificate amongs CAs
2. Verification Authority (VA) Registration (Face-to-Face, Remote, Automatic)
3. Registration Authority (RA) and local RA
4. Certificate Distribution System : LDAP (Special Purpose Database)



⑨ Practical Network security

How system are Hacked
- Remotely : Remote login service, Malware, Trojan
- Locally : social engineering

Hacking Procedure

1) สืบว่าระบบเป็นอย่างไร (Sniff the environment)
server อะไร (Nginx, Apache) version อะไร, OS information, วิธีเรียก API
Tools : Wireshark ป้องกันโดยการปลอมตัว
1.1 Social side ตามดูกับเจ้าของระบบ, ดู domain name registration
1.2 Network side map target-target network Tools: nmap ดู OS fingerprint, Service fingerprint

2) Identify possible vulnerabilities in network service

Defense firewall (network and transport layer), encryption, IDS/IPS (App layer)
ปิดทั้งหมด เปิดเท่าที่ใช้, honeypots, network segmentation

Attacker : Spoof IP address, Spoof MAC address
Distributed Denial of Services (DDOS) : ใช้ bots

ช่องโหว่ของ Network

1) DoS in DNS, TCP, ICMP
2) TCP SYN flood attack
Spoof fake IP, server ต้องเปิด connection รอ ACK จนไม่พอ
แก้ : set timeout, วิธีรอ ACK
3) TLS/SSL Heartbleed
use SSL Heartbeat เปลี่ยนขนาดของข้อความที่ขอคืนให้ยาวกว่าข้อความจริงที่ส่งไป จะได้ของใน buffer ของ server คืนมา

(10) Buffer Overflow – การอ่าน เขียน ทับที่หน่วยความจำอื่น

- อาจเขียนทับ return address เพื่อข้ามไปรันโค้ดอะไรก็ได้ (Remote code execution) → stack smashing
- เขียนทับ shared library ของภาษา เช่น printf

Observation Injecting Malicious code/data, Redirect Program

Similar vulnerabilities Integer overflow (ทดเกิน), "printf" vulnerability

Protection

1) Static Analysis กันไม่ได้ ทำได้แค่ detect และแก้เอง
   1. Lexical Analysis Tokenization
   2. Semantic Analysis Parser

   ปัญหาพบอยู่เนื่องจากแอพส่วนใหญ่เขียนบน C/C++ ซึ่งไม่มีการตรวจสอบ buffer overflow
2) Dynamic Solutions
   1. Address Protection → Canary words (เอาค่ามาวางบน return), Address encode, Copy of address, Tags (บอกว่าเป็น input หรือไม่)
   2. Input protection
   3. Bounds checking
   4. Obfuscation สุ่มวางตัวแปรให้เดาที่เก็บยากขึ้น
3) Isolation (Non-executable, Sandboxing)

(11) Digital Forensics (การตามรอยหลักฐาน)

= Law + Computer Science

Collect and analyze data from computer systems, networks, storage devices

- Networks, Small scale Digital Devices, Storage media, Code analysis

วิธีทำลายหลักฐาน
- ฝังหลักฐานไว้
- หาวิธีทำลาย
- สนามหลักฐาน
- เขียนทับ 7 รอบ

Forensics Process (Process การกู้ข้อมูล)

1) Acquisition or imaging of exhibits : อ่านข้อมูลบน disk โดยทำ write-blocked
2) Analysis : Visible, Encrypted, Hidden, Deleted files
3) Reporting

- Image Tampering การเปลี่ยนสภาพของรูป
- อ่าน Metadata ของไฟล์ ทำได้ทั้ง visible และ deleted file

วิธี anti-forensics
- Hidden files
- เปลี่ยนชื่อ folder ให้คล้ายกับชื่อ files
- Wiping Disk
- Change files extension (ไม่ตรงกับ MIME)

(12) Cyber Security & Penetration Testing Training

Introduction to cyber security

Cyber security Track

1) Security Management – แม่บ้านคุมบ้าน
   1. Legislative Track
   2. Global standard Track ป้องกัน ดูแล ลดความเสี่ยง ตามมาตรฐานในแต่ละมาตรฐาน
2) Penetration Test – offensive
   - ทำได้บน web – Red Teaming
3) Monitoring and Detection – defensive
   - Blue Team – SOC/SIEM – Security Architecture
4) Incident Response & Threat Hunting – เมื่อเกิดภัยคุกคาม จะรับมืออย่างไร
   - Digital forensic – Malware Analysis – Threat Intelligence

Security Management ดูมาตรฐานเรื่องความปลอดภัย
- Gap Assessment ดูระหว่าง current state – desired state รู้ว่ามีอะไร ทำก่อน Implement
- Risk Assessment ดูความเสี่ยงของแต่ละ Component (สาเหตุ ผลกระทบ ความเสี่ยง วิธีแก้) รู้ priority ของ risk
- IT Audit ตรวจสอบย้อนกลับ

Security Assessment

1) Vulnerability Assessment (VA) : ใช้ automated tool, known vulnerabilities e.g. antivirus (knowledge-based)
2) Penetration Test : hacker aspect ทำอย่างไรจึงจะได้ข้อมูลโดยไม่ต้อง login
3) Red Teaming : ไม่เจาะจง target และวิธีการ ตามหา critical core/sensitive files

- PenTest Level : Black Box, Grey Box, White Box (e.g. hard code user credential)
- PenTest Process
  1. Scope Definition
  2. Information Gathering
  3. Enumeration (Port Scanning, System-OS fingerprint)
  4. Vulnerabilities Identification (automate + manual)
  5. Result Analysis
  6. Research
  7. Exploitation
  8. Analysis & Reporting

Monitoring and Detection + Incident Response
- SIEM centralized system to define threat
- SOC team

} ทำงานร่วมกัน

OWASP & Penetration Test

OWASP Web Security Testing Guide (WSTG)

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing
7. Input Validation Testing
8. Testing for Error Handling
9. Testing for Weak Crypto
10. Business Logic Testing เช่น โอนเงิน -100 บาท
11. Client Side testing
12. API Testing

PenTesting Tools

Enumeration : Nmap, DirBuster (DirB), TheHarvester ค้นข้อมูล server ต่างๆ

Vulnerabilities Identification : BurpSuite, OWASP Zed Attack Proxy, W3af

Exploitation : SQLmap, Metasploit Framework, Kali Linux อื่นๆน่าของที่นำมาใช้ได้จริง

(13) Biometric การวัดของสิ่งมีชีวิต, make each person unique

Identity Issues : fake documents, identity thefts (เช่น เอาหนังสือเดินทาง)

ข้อดีของ Biometric : คัดลอก โอนไม่ได้, ทำหายไม่ได้, detects multiple enrollments (1 account/person) ปฏิเสธการกระทำของตัวเองไม่ได้

Application : Forensics, Government, Commercial

ประเภท (ควรจะ unique, permanent)

ลายนิ้วมือ ลายฝ่ามือ รอยข้อนิ้ว ความยาวนิ้ว ลายเส้น รูปใบหน้า Heatmap ใบหน้า ใบหู ม่านตา, เสียง จังหวะการพิมพ์ → พฤติกรรม : soft biometric เลียนแบบได้

Good Biometric – เก็บง่าย เหมาะสมกับการใช้งาน

Large inter-class similarity ต่างคนกัน ต้องวัดแล้วต่างกันมาก

Small intra-class similarity คนเดียวกัน ต้องวัดแล้วได้ค่าใกล้เคียงเดิม

Quality of biometric

Property – สิ่งที่ใช้ระบุความ unique

Image Quality – รูปดี → วัดได้ดี, อาจเกิด false match

Fake biometric – ลายนิ้วมือปลอม

(14) Secure by Design Plan more than just functionality (Plan for security)

Attack Surface Reduction

Attack surface = The collection of targets exposed to an attacker (vulnerability, control, network)

(จุดที่การโจมตีได้) เช่น endpoint
- จุดเริ่มต้นของการทำ PenTest

ลดได้โดย
- Defense in Depth – ป้องกันทุกวิถีทาง
- Least Privilege
- Secure Defaults – Less code running → Less stuff to attack
  – ปิดทั้งหมดแล้วเปิดเท่าที่จะใช้

Assume zero trust
Create strong user access protocols
Use string authentication policies
Protect your backups
Segment your network
Eliminate complexity
Visualize vulnerabilities
Control endpoints
Prioritize analytics

ปิด port ที่ไม่ใช้ → ปิด UDP → กำหนด IP ที่สามารถเข้าได้ → ใช้ password → share เฉพาะที่จำเป็น → ปรับ Access Control Lists

Threat Modeling คิดในมุมมองของผู้ที่จะโจมตีระบบ

Threat Analysis

Threat ≠ vulnerability
(ภัยคุกคาม) (ช่องโหว่)

Threat lives forever → Mitigation (บรรเทา)

Vulnerability can be Fixed

Process
1) Gather background info (Dependency)
2) Model the system (Data flow diagram)
3) Identify threats (Type, Threat tree)
4) Resolve threats (Fix/Work-around)

* Try to prune threat tree
  cut

Threat type (STRIDE) → แก้ได้ด้วย Secure Design Principle

Spoofing	ปลอมตัวเข้ามาในระบบ	Authen
Tampering	เข้าไปแก้ไขข้อมูล	Integrity
Repudiation	ปฏิเสธความรับผิดชอบ	Auditing
Information Disclosure	เปิดเผยข้อมูล	Confidentiality
Denial of Service	ทำให้ระบบใช้การไม่ได้	Availability
Elevation of Privilege	เพิ่มสิทธิ์	Author

Input validation
- Validate all inputs
- Type, Length, Range [A-Z], Format

Activity (บางส่วน)

- Netcat สามารถใช้เป็น trojan horse ได้, ป้องกันได้โดยไม่ใช้ admin user ในการใช้เครื่อง
- ป้องกัน Nmap ไม่ได้ เพราะมี option เปลี่ยน string User-agent และ decoy เพื่อเปลี่ยน ip และ server มองว่าการเข้าถึง port 80 เป็น client ทั่วไป
- SYN Cookie is an IP spoofing attack mitigation technique whereby a server replies to TCP SYN requests with crafted SYN-ACKs, without creating a new TCB for the TCP connection

Study questions (บางส่วน)

- **Trusted Computing Platform Alliance (TCPA)** สร้างนิยามของ trusted computing

  Memory Curtaining : full isolation of sensitive areas of memories → ensure cryptographic keys are isolated

  Secure I/O : prevent keylogger

  Sealed Storage : protects private information

  Remote Attestation (การรับรอง) : อนุญาตให้ 3rd parties ตรวจสอบเครื่องเราได้

  - Non-malleable trusted root for trusted storage
  - Inability to disable all of the functionality of the TPM
  - Inability to provide a reasonable degree of privacy

  ปัญหา privacy trusted third parties สามารถจับคู่ anonymous to real → ซ่อนไม่จริง

- **XSS** ป้องกันได้ด้วย input validation

  เนื่องจาก XSS เกิดจาก user input หากนำ input มาใช้เลยโดยตรง จะเป็นอันตรายต่อระบบ ต้องทำการตรวจสอบ user input ก่อนนำมาใช้งานทุกครั้ง ว่าตรงกับ input ที่เราคาดหวังหรือไม่ ในฝั่งผู้ใช้อาจป้องกันได้โดยตรวจสอบ แต่ทุกสิ่งก่อนเข้าถึง แต่ความรับผิดชอบหลักควรอยู่ที่ฝั่ง server

- **Canonicalization**

  Canonicalization is the process of mapping inputs to their canonical equivalent. It is often used for cryptographic algorithms and data that are intended to be secured from tampering, usually by hashing. A canonicalization attack is a cyberattack method in which the attacker substitudes various inputs for the canonical name of a path or file. Typically exploited by entering the file path in an input field or webpage or path of a URL, canonical attacks enable attackers to access unauthorized files and directories on a web server

- **Phishing** is a fraudulent activity that is done to steal confidential user information such as credit card numbers, login credentials, and passwords. It is usually done by using email or fake reliable business webpage. ถือเป็น social eng เพราะมีการหลอกถามจาก user ที่รู้ข้อมูลโดยตรง

- **Pharming** คือ การโจมตีเครื่อง server เพื่อให้ผู้ที่เข้าถึง ถูก redirect ไปยัง attacker-controlled website. หรือการแก้ไข hosts ฝั่ง client ก็ได้ ไม่ถือเป็น social eng เนื่องจากไม่ต้องการ user interaction, เป็นการทำ malware อย่างหนึ่ง

- **PKI and e-commerce** – help customers and businesses to verify the source of information and files and to determine the authenticity of software applications and other products

- **Bitcoin Mining** คือกระบวนการสร้างเหรียญ Bitcoin ใหม่ด้วยการถอดรหัสสมการทางคณิตศาสตร์เพื่อตรวจสอบ transaction หากทำการแก้สมการสำเร็จคนแรก จะได้รับ Bitcoin เป็นรางวัลตอบแทน

  The problem that miners solve to earn Bitcoin is to partially invert the SHA-256 hash function.

  ประโยชน์ : ตรวจสอบธุรกรรมที่สร้างขึ้นใหม่ เพื่อป้องกันไม่ให้มีการทุจริตบนเครือข่ายบล็อกเชน