Google IT Support Certificate

IT Security: Defense Against the Digital Dark Arts

Course 5

Samart Skills
A Grow with Google PROGRAM

Skooldio

Overview:

01

Understanding Security Threats

02

Pelcgbybtl (Cryptology)

03

AAA Security (Not Roadside Assistance)

04

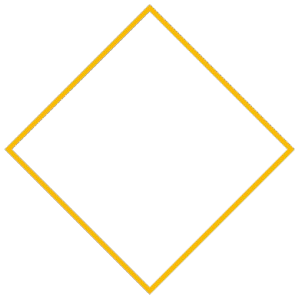
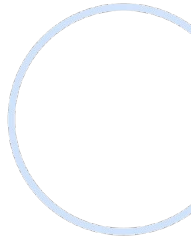
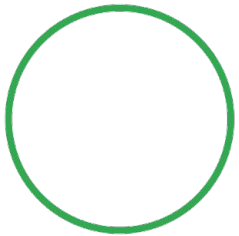
Securing Your Networks

05

Defense in Depth

06

Creating a Company Culture for Security


Introduction to IT Security

การรักษาความถูกต้องของข้อมูล

- ไม่ถูกแก้ไขโดยผู้ที่ไม่มีสิทธิ์
- Hash, MAC, ESP

การรักษาความลับของข้อมูล

- ป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึงได้
- Encryption, Authentication

ความพร้อมใช้ของข้อมูล

- เข้าถึงได้ ใช้งานได้ ตามเวลาที่ตกลงกันไว้
- DoS Protection, Backup

CIA Triad

Introduction to IT Security

- **Threat** คือ ภัยคุกคามที่อาจเข้ามาโจมตีระบบได้
- **Vulnerability** คือ ช่องโหว่หรือจุดอ่อนของระบบที่อาจจะถูกโจมตีเข้ามาได้
- **Risk** คือ โอกาสที่ภัยคุกคามจะเข้ามาโจมตีช่องโหว่ของระบบจนเกิดผลเสียหายได้
- **Exploit** คือ Software ที่ใช้ในการโจมตีช่องโหว่
- **Attack** คือ การโจมตีที่เกิดขึ้นและมีผลเสียหายจริงกับระบบ
- **Zero-day Vulnerability** คือ ช่องโหว่ที่ไม่เคยถูกเปิดเผยโดยผู้พัฒนาหรือผู้ผลิตมาก่อน แต่อาจถูกค้นพบและนำมาโจมตีโดยผู้ไม่ประสงค์ดี

Introduction to IT Security

Hacker คือ ผู้ที่พยายามโจมตีระบบ

- Black Hat Hacker คือ Hacker ที่ประสงค์ร้ายต่อระบบ โดยโจมตีเพื่อให้เกิดผลเสียหายหรือผลประโยชน์ส่วนตน
- White Hat Hacker คือ Hacker ที่ประสงค์ดีต่อระบบ โดยโจมตีเพื่อให้เจ้าของระบบรู้ช่องโหว่และนำไปปรับปรุงระบบให้มีความปลอดภัยมากขึ้น

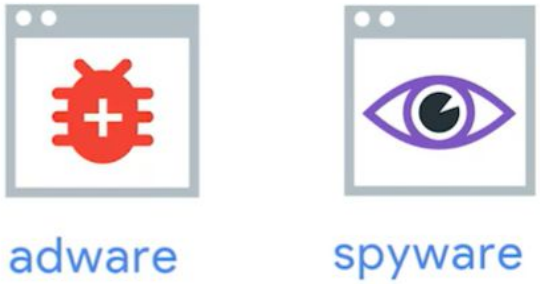
Malicious Software

Malicious Software (Malware) คือ โปรแกรมประเภทหนึ่งที่สามารถใช้ในการสร้างผลเสียหายกับเครื่องคอมพิวเตอร์ได้ เช่น ดักจับ แก้ไข หรือทำลายข้อมูล เป็นต้น

Malicious Software

- **Virus** คือ Malware ที่ต้องแทรกตัวไปกับไฟล์อื่น ซึ่งเมื่อไฟล์นั้นทำงาน จะทำให้ Virus สามารถแพร่กระจายไปยังไฟล์หรือคอมพิวเตอร์อื่น ๆ ได้
- **Worm** คือ Malware ที่มีชีวิตอยู่ด้วยตัวเองได้ ไม่ต้องอาศัยการแทรกตัวไปกับไฟล์อื่น และสามารถแพร่กระจายตัวเองไปยังไฟล์หรือคอมพิวเตอร์อื่น ๆ ได้

Malicious Software

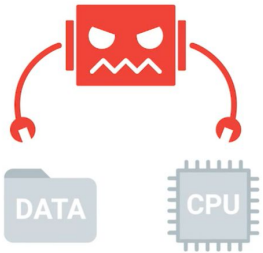


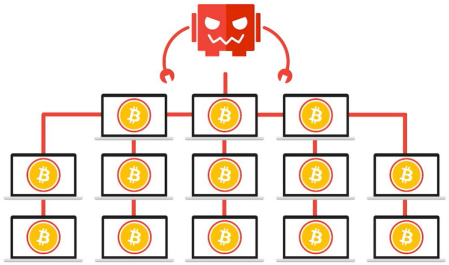
- **Adware** คือ Malware ที่แสดงโฆษณาและเก็บรวบรวมข้อมูลการใช้งานโปรแกรม
- **Spyware** คือ Malware ที่สอดแนมข้อมูลต่าง ๆ บนเครื่องคอมพิวเตอร์และส่งข้อมูลกลับไปยังผู้ไม่ประสงค์ดี เช่น ข้อมูลหน้าจอ การกดคีย์บอร์ด (Key Logger)
- **Ransomware** คือ Malware ที่เข้ารหัสข้อมูลและเรียกค่าไถ่ในการถอดรหัสข้อมูล

Malicious Software

- **Trojan** คือ Malware ที่แฝงตัวเองไปในโปรแกรมที่น่าเชื่อถือ และแอบทำงานที่ไม่ประสงค์ดีซ่อนอยู่ภายใน
  - ต้องถูก Download และ Install โดยผู้ใช้งานเอง

Malicious Software



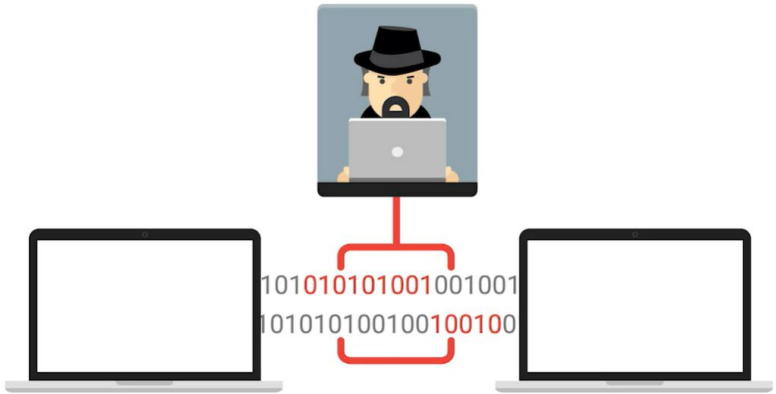


- **Bot** คือ เครื่องคอมพิวเตอร์ที่ถูกควบคุมโดยผู้ไม่ประสงค์ดี โดยมีเครื่องคอมพิวเตอร์เครื่องนั้นสามารถถูกนำไปใช้ในการหาผลประโยชน์หรือใช้ทำงานในทางที่ไม่ดีได้ เช่น ขุดบิตคอยน์
- **Botnets** คือ Bot จำนวนมากที่ถูกควบคุมผ่านอินเตอร์เน็ต

Malicious Software

- **Backdoor** คือ Malware ที่ใช้ในการเข้าถึงเครื่องคอมพิวเตอร์ในภายหลัง หลังจากที่ผู้ไม่ประสงค์ดีสามารถยึดเครื่องคอมพิวเตอร์นั้นได้แล้ว
- **Rootkit** คือ Malware ที่มีสิทธิ์ระดับ Administrator ที่สามารถแก้ไขค่าต่าง ๆ บนระบบปฏิบัติการได้
    - สามารถซ่อนตัวในระบบได้ ทำให้ยากในการตรวจสอบ
- **Logic Bomb** คือ Malware ที่จะทำงานเมื่อตรงเงื่อนไขที่ถูกตั้งไว้ เช่น ตามเวลาที่กำหนด หรือ เมื่อบางไฟล์ถูกเปิด เป็นต้น

Network Attacks

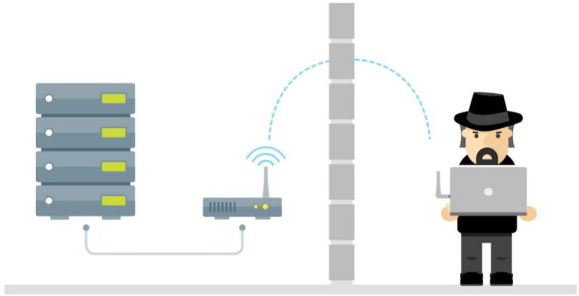


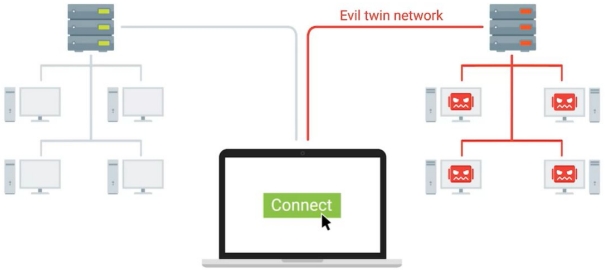
DNS Cache Poisoning คือ การปลอมแปลงแก้ไข DNS Record ให้ชี้ไปยัง IP Address ของผู้ไม่ประสงค์ดี

Man-in-the-middle Attack คือ การโจมตีที่ผู้ไม่ประสงค์ดีสามารถทำตัวอยู่ระหว่างกลางของเครื่องคอมพิวเตอร์สองเครื่องเพื่อดักจับหรือแก้ไขข้อมูลได้

- Session/Cookie Hijacking

Network Attacks

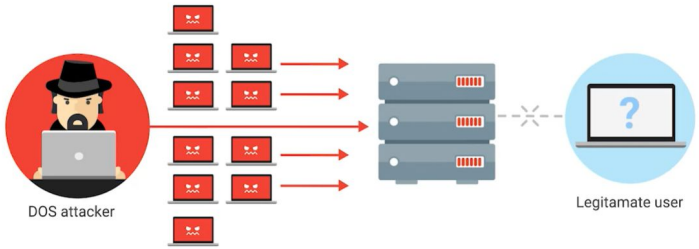




Rogue AP คือ เทคนิคหนึ่งในการทำ Man-in-the-middle Attack โดยการนำ Access Point ที่ไม่ได้รับอนุญาตเข้าไปติดตั้งในองค์กร

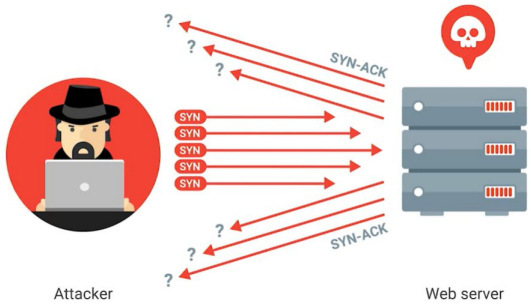
Evil Twin คือ เทคนิคหนึ่งในการทำ Man-in-the-middle Attack โดยการสร้าง Wireless Network ที่ชื่อเหมือนกับชื่อ Wireless Network ที่ใช้ในองค์กร เพื่อหลอกให้ผู้ใช้งานหลงเข้ามาเชื่อมต่อ

Network Attacks



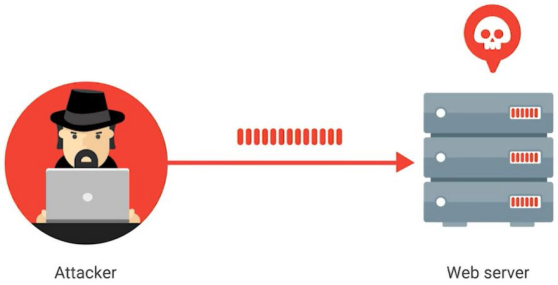
Denial-of-Service (DoS) Attack คือ การโจมตีที่พยายามทำให้ Network หรือ Server ทำงานหนักเกินขีดความสามารถจนไม่สามารถให้บริการกับผู้ใช้งานได้

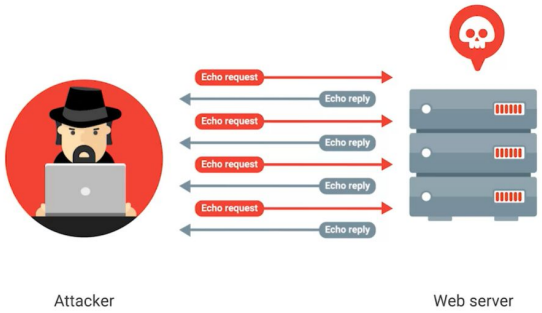
- การโจมตีเกิดมาจากแหล่งเดียว



- **SYN Flood (Half-open Attack)** คือ DoS Attack ประเภทหนึ่ง ซึ่งโจมตีโดยการส่ง SYN Packet จำนวนมากไปที่ระบบจนทำให้ระบบไม่สามารถให้บริการงานอื่นได้

Network Attacks

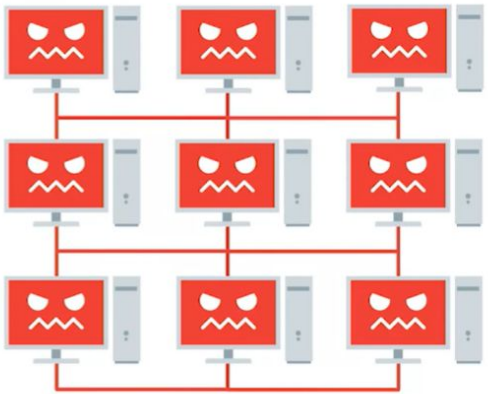




- **Ping of Death** คือ DoS Attack ประเภทหนึ่ง ซึ่งโจมตีโดยการส่ง Ping Packet ขนาดใหญ่เกินกว่าที่ Protocol ออกแบบไว้ ส่งผลทำให้เกิด buffer overflow ทำให้เครื่องคอมพิวเตอร์หยุดการทำงานและอาจถูกส่งคำสั่งจากระยะไกล (Remote Code Execution) ได้

- **Ping Flood** คือ DoS Attack ประเภทหนึ่ง ซึ่งโจมตีโดยการส่ง Ping Packet (Echo Request) จำนวนมากไปที่ระบบจนทำให้ระบบไม่สามารถให้บริการงานอื่นได้

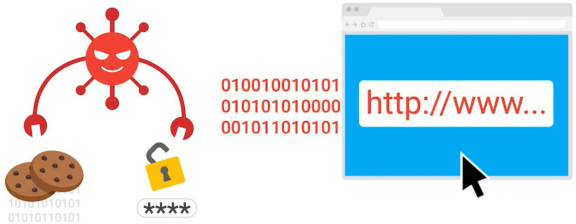
Network Attacks



Distributed Denial-of-Service (DDoS) Attack คือ การใช้เครื่องคอมพิวเตอร์ที่ถูกควบคุมจำนวนมาก (Botnets) ในการทำ DoS Attack

- การโจมตีเกิดมาจากหลายแหล่งพร้อม ๆ กัน

Other Attacks



Injection Attack คือ การโจมตีโดยการแทรกคำสั่งไปกับ Input เพื่อให้ระบบทำงานตามที่ต้องการได้

- **Cross-Site Scripting (XSS) Attack** คือ Injection Attack ประเภทหนึ่ง ซึ่งโจมตีโดยการแทรก Malicious Script เช่น JavaScript ไปยังช่อง Input ของ Web Application เพื่อให้ Script นี้ถูก Run บนเครื่องผู้ใช้งาน (Client)
    - สามารถนำไปใช้ขโมย Session Cookie ของผู้ใช้งานได้
- **SQL Injection (SQLI) Attack** คือ Injection Attack ประเภทหนึ่ง ซึ่งโจมตีโดยการแทรก SQL Command ไปยังช่อง Input ของ Web Application เพื่อ Query ข้อมูลบน Database

การป้องกัน Injection Attack

- Input Validation
- Data Sanitization

Other Attacks

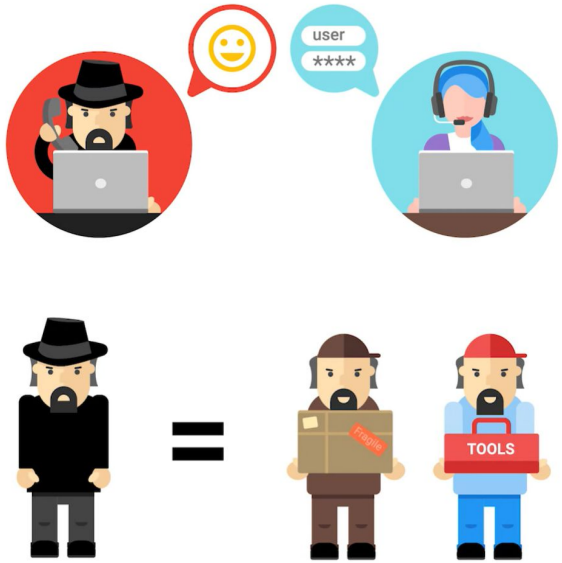
Password Attack คือ การโจมตีโดยการใช้ Software ในการพยายามเดารหัสผ่าน

- **Brute-force Attack** คือ การพยายามเดารหัสผ่านโดยการใช้ทุกความเป็นไปได้ของการผสมกันของตัวอักษร ตัวเลข และอักขระพิเศษ
- **Dictionary Attack** คือ การพยายามเดารหัสผ่านโดยใช้คำที่มีใน Dictionary หรือ Wordlist

การป้องกัน Password Attack

- การใช้รหัสผ่านที่มีความแข็งแรง (Strong Password) คือ มีความยาวอย่างน้อย 8 ตัว โดยมีการผสมกันของอักษรตัวใหญ่ อักษรตัวเล็ก ตัวเลข และอักขระพิเศษ รวมไปถึงไม่ใช้คำที่มีอยู่ใน Dictionary เช่น s@nDwh1ch
- Captcha

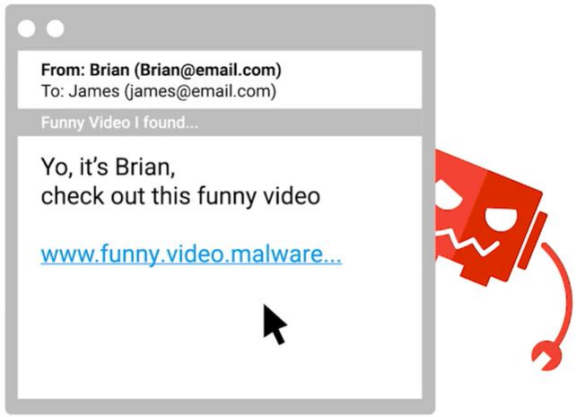
Other Attacks



Deceptive Attack คือการโจมตีโดยการหลอกลวงหรือปลอมแปลง

- **Social Engineering** คือ การหลอกลวงให้ผู้ใช้งานหลงเชื่อทำตามในสิ่งที่ผู้ไม่ประสงค์ดีต้องการ
  - **Phishing** คือ การส่งอีเมลหลอกลวงไปหาผู้ใช้งานเพื่อหลอกให้กรอกข้อมูลสำคัญ เช่น Username และ Password หรือหลอกให้กด Link เพื่อ Download Malware
  - **Baiting** คือการแกล้งทำสิ่งของหล่น เช่น Malicious USB Drive เพื่อให้คนเก็บและนำไปเชื่อมต่อกับคอมพิวเตอร์
  - **Tailgating** คือ การเดินตามผู้ใช้งานเข้าไปในตึกสำนักงานหรือพื้นที่ต้องห้าม

Other Attacks

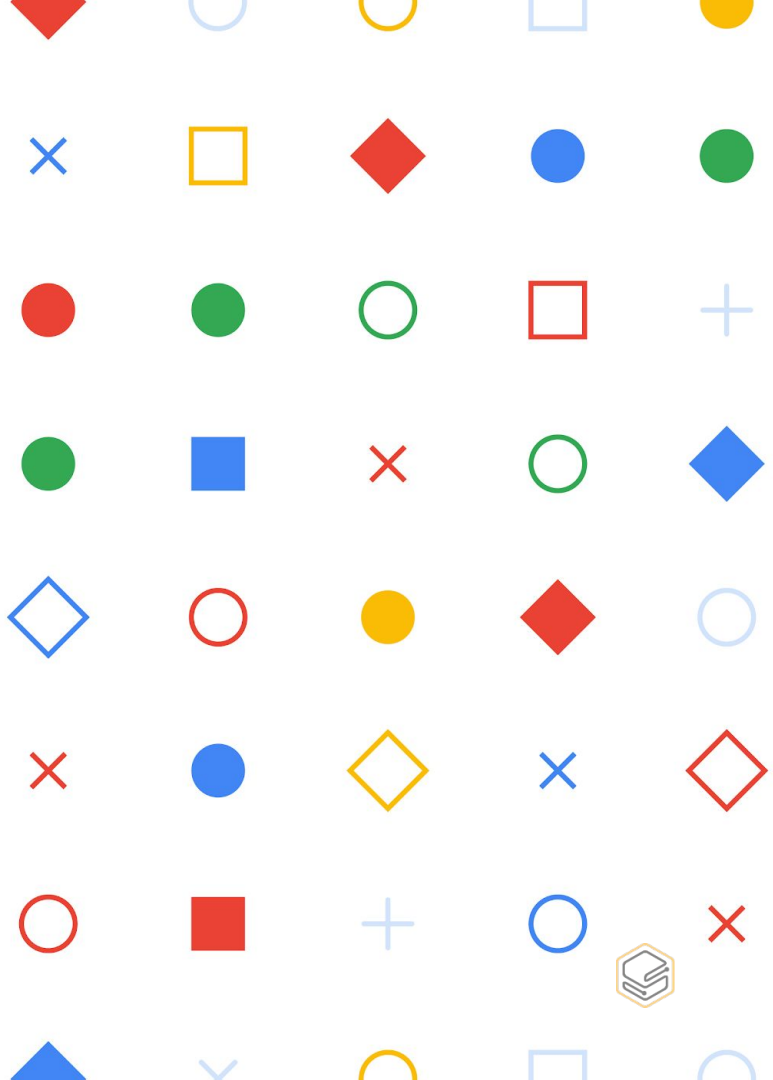


Deceptive Attack

- Email Spoofing คือการปลอมแปลง Email Address ของผู้ส่ง ซึ่งมักใช้ร่วมกับ Phishing
- การป้องกัน Phishing:
  - Spam Filtering
  - ให้ความรู้ด้าน Security กับผู้ใช้งาน
  - 2FA

Week 2

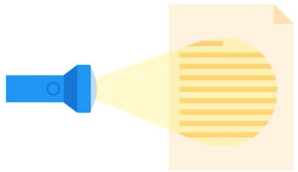
Pelcgbybtl (Cryptology)

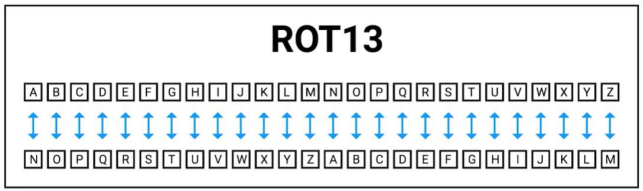


Samart Skills
A Grow with Google PROGRAM

Skooldio

Symmetric Encryption





URYYB JBEYQ
=
HELLO WORLD

- **Cryptography** คือ วิทยาการเข้ารหัสลับ
- **Cryptology** คือ การศึกษา Cryptography
- **Steganography** คือ วิธีการในการซ่อนข้อความไปในสื่อต่าง ๆ เช่น ภาพ เสียง วีดีโอ โดยไม่มีการเข้ารหัสข้อความ
- **Encryption** คือ การเข้ารหัส ซึ่งเป็นการนำข้อความ (Plaintext) มาเข้าสู่ Cipher เพื่อให้ได้ข้อความที่ไม่สามารถอ่านออก (Ciphertext)
- **Decryption** คือ การถอดรหัสจาก Ciphertext กลับมาเป็น Plaintext
- **Cryptanalysis** คือ ผู้ที่วิเคราะห์หาจุดอ่อนของการเข้ารหัส

Symmetric Encryption

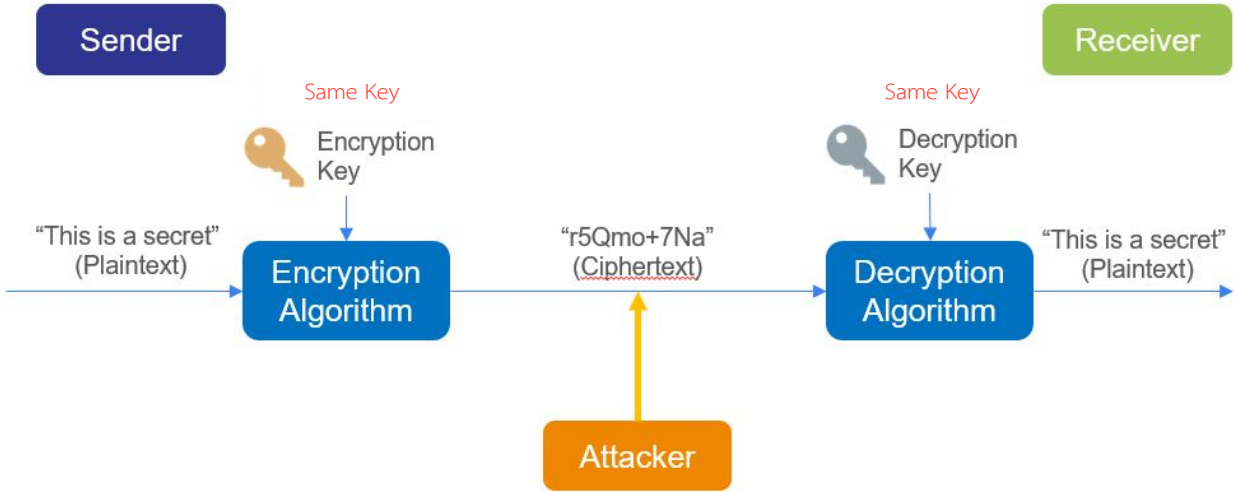
Cipher ประกอบด้วย 2 ส่วน

- **Encryption Algorithm** คือ กระบวนการที่ใช้เปลี่ยนจาก Plaintext ไปเป็น Ciphertext
- **Key** คือ กุญแจที่ใช้ในการเข้ารหัส ซึ่งต้องเก็บเป็นความลับ
    - **Key Length** คือ ความยาวของ Key ซึ่งยิ่งมีความยาวมากขึ้นก็จะทำให้โจมตีการเข้ารหัสได้ยากขึ้น

Symmetric Encryption

Symmetric-Key Encryption คือ การเข้ารหัสแบบกุญแจสมมาตร

- ผู้ส่งและผู้รับมีกุญแจเหมือนกัน



Symmetric Encryption

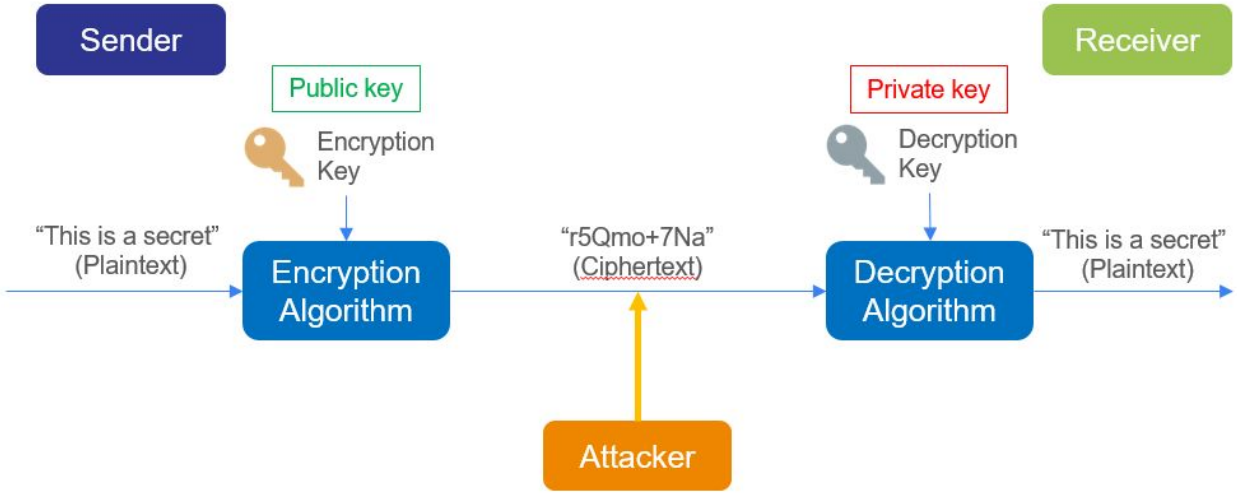
ประเภทของ Symmetric Cipher

- **Stream Cipher** คือ การนำ Plaintext มาเข้ารหัสทีละ Bit
  - RC4 (Rivest Cipher 4)
- **Block Cipher** คือ การนำ Plaintext มาแบ่งเป็น Block แล้วนำมาเข้ารหัสทีละ Block เช่น
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

Public Key or Asymmetric Encryption

Asymmetric Key Encryption คือ การเข้ารหัสแบบกุญแจไม่สมมาตร

- ผู้ส่งและผู้รับมีกุญแจต่างกัน
- ประยุกต์ใช้กับ Digital Signature



Public Key or Asymmetric Encryption

- **Asymmetric Encryption Algorithm**
  - RSA
  - DSA (Digital Signature Algorithm)
  - DH (Diffie-Hellman)
  - ECC (Elliptic Curve Cryptography)

Hashing

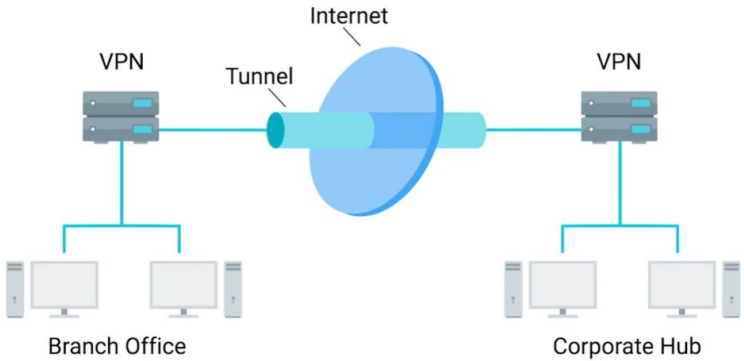
"Hello World" | [hash function] | E49AOOFF

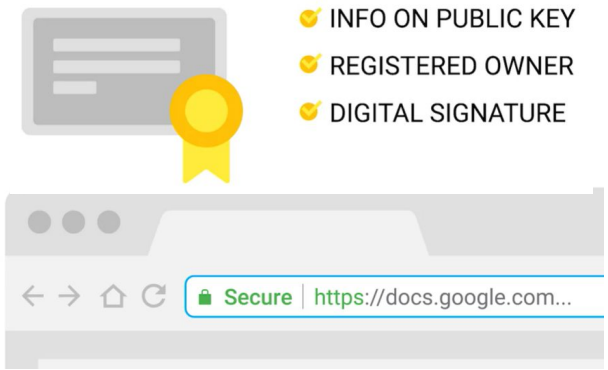
"hello world" | [hash function] | FF1832AE

- **Hashing** คือ Function ที่สามารถรับ Input ความยาวเท่าไหร่ก็ได้ และคำนวณ Output ออกมามีความยาวคงที่ โดย Output นี้จะเรียกว่า Hash หรือ Digest หรือ Message Integrity Check (MIC)
  - Output จะต้องเหมือนเดิมสำหรับ Input เดิม
  - Output จะต้องแตกต่างไปอย่างสิ้นเชิงสำหรับ Input ที่แตกต่างกัน
  - ถ้ารู้ Output จะไม่สามารถย้อนกลับไปหา Input ได้
  - Hash Collision คือ การที่ 2 inputs สามารถถูกคำนวณไปเป็น Output เดียวกัน
- **Hash Algorithms**
  - MD5, SHA1, SHA2, SHA3

Cryptography Applications

- Public Key Infrastructure (PKI)
  - X.509 Certificate
- HTTPS, VPN, SSH, etc.



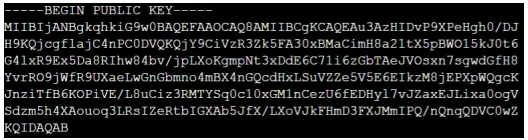


OpenSSL

OpenSSL เป็น Software ที่จัดการเกี่ยวกับ Public Key Encryption ได้ เช่น

- สร้าง Keypair (Private Key และ Public Key)
- Encryption/Decryption
- Sign/Verify Digital Signature

OpenSSL



Command ที่ใช้ในการจัดการ Keypair

- สร้าง 2048-Bit RSA Private Key:
  - openssl genrsa -out [PRIVATE_KEY_NAME] 2048
- อ่าน Private Key:
  - cat [PRIVATE_KEY]
- สร้าง Public Key ที่คู่กับ Private Key ที่เราสร้างขึ้นมา
  - openssl rsa -in [PRIVATE_KEY] -outform PEM -pubout -out [PUBLIC_KEY_NAME]
- อ่าน Public Key:
  - cat [PUBLIC_KEY]

OpenSSL

Command ที่ใช้ในการทำ Encryption/Decryption

- Encrypting File (ใช้ Public Key)
  - openssl rsautl -encrypt -pubin -inkey [PUBLIC_KEY] -in [FILE] -out [ENCRYPTED_FILE_NAME]
- Decrypting File (ใช้ Private Key)
  - openssl rsautl -decrypt -inkey [PRIVATE_KEY] -in [ENCRYPTED_FILE]

Creating and Verify Hash

- **md5sum** เป็น Software ที่ใช้ในการสร้าง (Create) และตรวจสอบ (Verify) MD5 Hash

- **Command ที่ใช้ในการสร้างและตรวจสอบ MD5 Hash**
  - การสร้าง MD5 Hash สำหรับไฟล์
    - md5sum [FILE] > [MD5_HASH_NAME]
  - อ่าน MD5 Hash
    - cat [MD5_HASH]
  - ตรวจสอบ MD5 Hash
    - md5sum -c [MD5_HASH]

Creating and Verify Hash

shasum เป็น Software ที่ใช้ในการสร้าง (Create) และตรวจสอบ (Verify) SHA1, SHA256 Hash

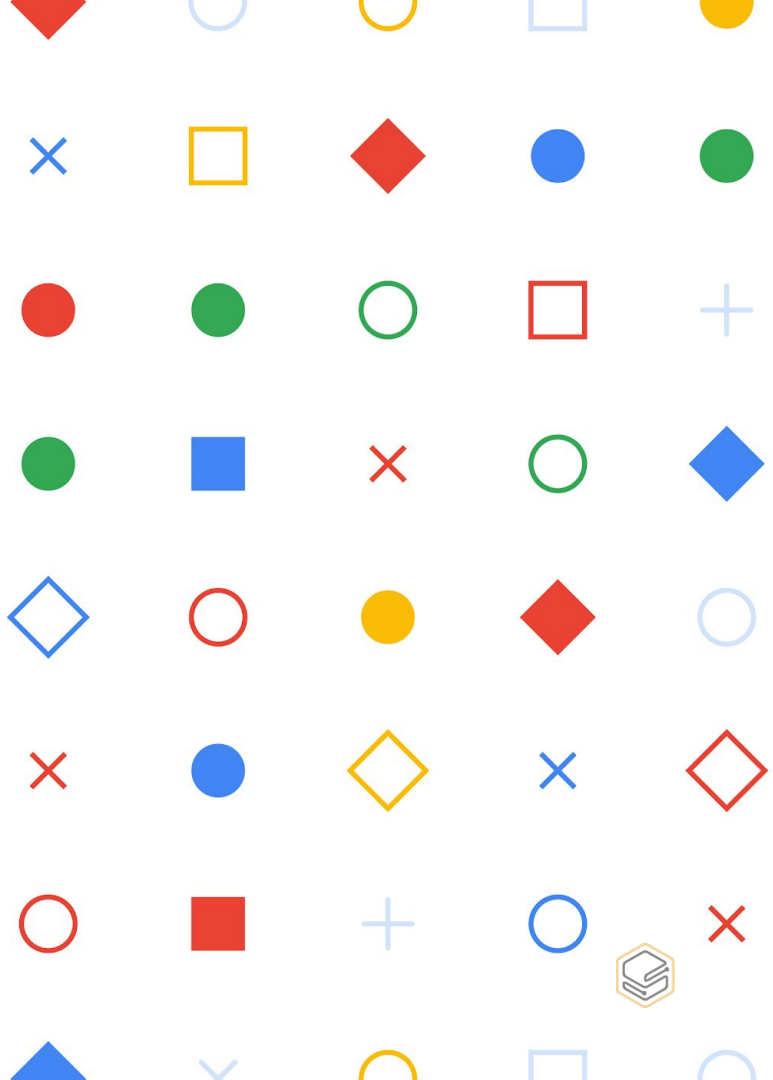
- **Command ที่ใช้ในการสร้างและตรวจสอบ SHA1 Hash**
  - การสร้าง SHA1 Hash สำหรับไฟล์
    - shasum [FILE] > [SHA1_HASH_NAME]
  - อ่าน SHA1 Hash
    - cat [SHA1_HASH]
  - ตรวจสอบ SHA1 Hash
    - shasum -c [SHA1_HASH]

Creating and Verify Hash

- **Command ที่ใช้ในการสร้างและตรวจสอบ SHA256 Hash**
  - การสร้าง SHA256 Hash สำหรับไฟล์
    - shasum -a SHA256 [FILE] > [SHA256_HASH_NAME]
  - อ่าน SHA256 Hash
    - cat [SHA256_HASH]
  - ตรวจสอบ SHA256 Hash
    - shasum -c [SHA256_HASH]

Week 3

AAA Security (Not Roadside Assistance)



Samart Skills
A Grow with Google PROGRAM

Skooldio

Authentication

AAA = Authentication, Authorization and Accounting

Authentication (Authn) มี 2 ขั้นตอน คือ

- Identification คือ การแสดงตัวตน (Identity) เช่น Email Address, Username
- Authentication คือ การพิสูจน์ตัวตนที่ได้แสดงมา เช่น Password ของ Username นั้น
    - เป็นการพิจารณาว่า Identity ที่แสดงมานั้นเป็นตัวจริง

Authentication

Authentication Factor คือ ปัจจัยที่จะนำมาใช้พิสูจน์ตัวตน มี 3 อย่าง

- **Something You KNOW** คือ สิ่งที่คุณรู้ เช่น Password, PIN
- **Something You HAVE** คือ สิ่งที่คุณมี เช่น Smart Card, Security Token
- **Something You ARE** คือ สิ่งที่คุณเป็น เช่น ลายนิ้วมือ ใบหน้า

Single-Factor Authentication คือ การใช้ปัจจัยเดียวในการพิสูจน์ตัวตน

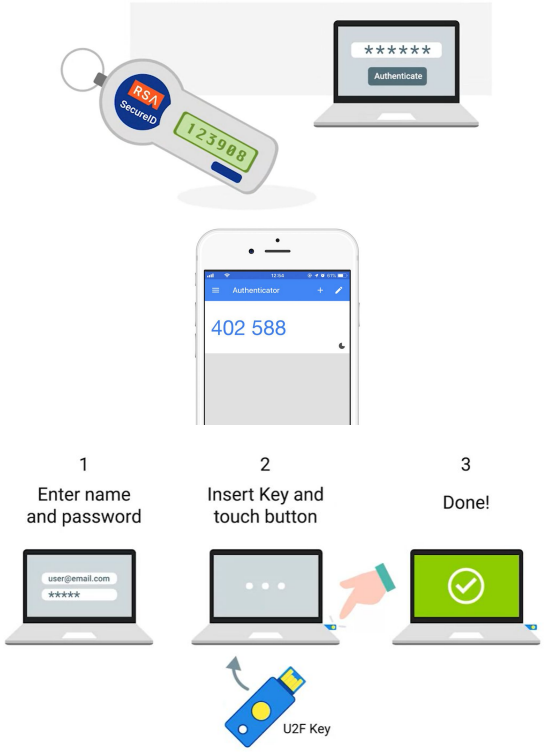
Multifactor Authentication คือ การใช้ปัจจัยที่แตกต่างกันอย่างน้อยสองปัจจัยในการพิสูจน์ตัวตน เช่น การใช้ Password และ Security Token

Authentication

Something You Know

- **Password** คือ รหัสผ่าน
  - ควรตั้งให้มีความยาวอย่างน้อย 8 ตัว ประกอบด้วยตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ เช่น s@nDwh1ch
  - ไม่ใช้คำที่อยู่ใน Dictionary และข้อมูลส่วนตัว
- เทคนิคการตั้ง Password
  - ให้ใช้ Passphrase เช่น Ilik3ponies@hom3
- **PIN** คือ รหัสผ่านที่ใช้เพียงตัวเลข

Authentication



Samart Skills
A Grow with Google PROGRAM

Skooldio

Something You Have

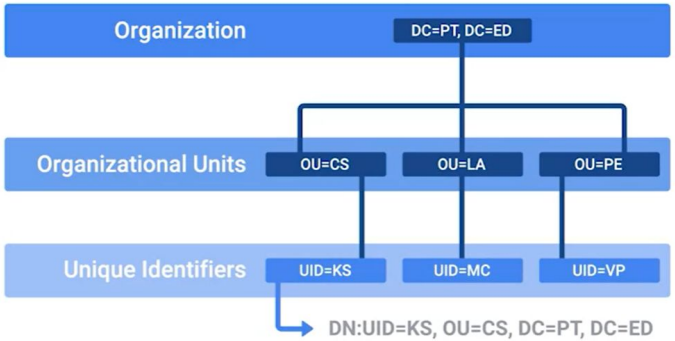
- **Physical Token** คือ USB Device ที่มีรหัสผ่านแบบใช้ครั้งเดียว (One-Time-Password:OTP) แสดงอยู่
- **Software Token** คือ Software ที่ทำหน้าที่คล้าย Physical Token ซึ่งสามารถติดตั้งได้บน Smartphone
- **Security Token (U2F Token)** คือ Physical Token ที่พัฒนาตามมาตรฐานของ FIDO Alliance
    - ใช้เทคนิค Challenge-response ร่วมกับ Public Key Cryptography ในการพิสูจน์ตัวตน
    - ป้องกัน Phishing ได้ดีกว่า OTP
    - Tempering and Clone Resistance

Authentication

Something You Have

- **Client Certificate** คือ การใช้ Certificate ในการพิสูจน์ตัวตนผู้ใช้งาน (Client)
  - ใช้เทคนิค Challenge-response เพื่อพิสูจน์ว่า Client เป็นเจ้าของ Private Key
  - ต้องมี Certificate Authority (CA) Infrastructure ในการ Issue และ Sign Client Certificate

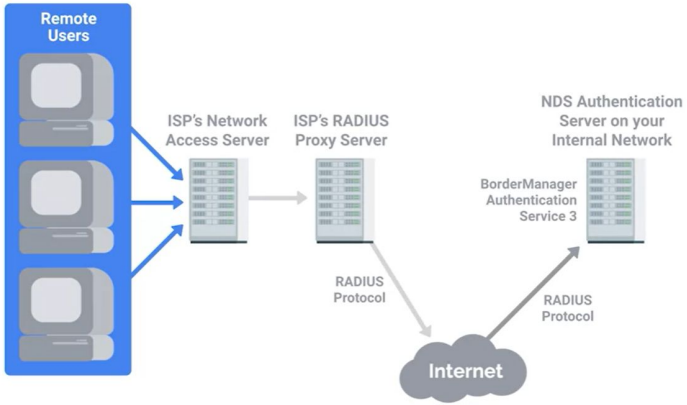
Authentication



LDAP (Lightweight Directory Access Protocol) คือ Open Standard Protocol ที่ใช้ในการเข้าถึง Directory Services ซึ่งใช้เป็นฐานข้อมูลในการทำ Authentication

- ใช้ Data Information Tree ในการเก็บข้อมูล Object
- Common Operations:
  - **Bind**: ใช้ Authenticate Clients
  - **StartTLS**: ติดต่อ LDAP ผ่าน TLS ทำให้การติดต่อนั้นปลอดภัย
  - **Search**: ค้นและแสดงข้อมูลบน Directory
  - **Add/Delete/Modify**: เพิ่ม/ลบ/แก้ไข ข้อมูลบน Directory
  - **Unbind**: ปิดการติดต่อ LDAP Server

Authentication



RADIUS (Remote Authentication Dial-In User Service) คือ Protocol ที่ใช้ในการทำ AAA Services สำหรับผู้ใช้งานบน Network เช่น WiFi Network หรือ VPN เป็นต้น

- NAS (Network Access Server): รับการ Authentication จาก Client และส่งต่อไปให้ RADIUS Server
- RADIUS Server: พิสูจน์ตัวตน Client ให้สิทธิการใช้งาน และเก็บ Log การใช้งาน

Authentication

TACACS+ (Terminal Access Controller Access Control System Plus) คือ AAA Protocol ที่ถูกพัฒนาโดย Cisco ซึ่งปัจจุบันกลายเป็น Open Standard แล้ว

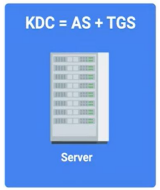
- พัฒนามาทดแทน TACACS และ XTACACS
- มักถูกใช้ในการทำ Device Administration และ AAA ของอุปกรณ์เครือข่าย
- มีการเก็บ Log ข้อมูล เช่น Command ที่ถูกรันโดยผู้ใช้งาน, User Authentication และ Device/System ที่ User เข้าถึง เป็นต้น

Authentication

Kerberos เป็น Network Authentication Protocol ที่ใช้ Ticket ในการพิสูจน์ตัวตน

- เป็น Default Authentication สำหรับเครื่อง Windows ที่ Join Domain
- ใช้ Symmetric Encryption (AES) และ Checksums ทำให้มี Confidentiality และ Integrity
- พิสูจน์ตัวตนแบบ Mutual Authentication คือ การที่ Server พิสูจน์ตัวตน Client และในทางกลับกัน Client ก็พิสูจน์ตัวตน Server ด้วยเช่นเดียวกัน
- เวลาของ Client และ Server จะต้องใกล้เคียงกัน โดย Default แล้วจะต้องห่างกันไม่เกิน 5 นาที หากเกินกว่านี้จะทำให้ Authentication ไม่สำเร็จ

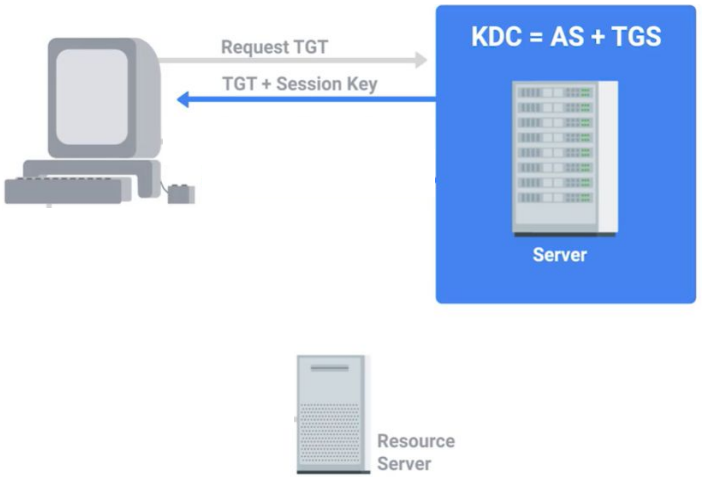
Authentication



Kerberos Authentication Flow

- **KDC** (Key Distribution Center) = AS (Authentication Server) + TGS (Ticket Granting Server)
- **AS** ทำหน้าที่ Authentication ผู้ใช้งาน
- **TGS** ทำหน้าที่ Authorization สำหรับ Service
- **Resource Server** คือ เครื่องที่ให้บริการ Service เช่น File Service, Web Service
- **Client** คือ เครื่องที่ต้องการใช้ Service

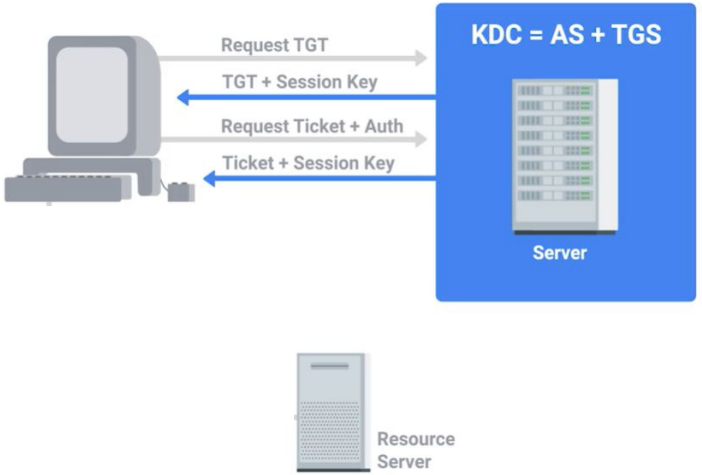
Authentication



Kerberos Authentication Flow

- 1. Client กรอก Username และ Password และส่ง Request ขอ Ticket Granting Ticket (TGT) ไปที่ AS
- 2. AS จะพิสูจน์ตัวตน Client ซึ่งหากถูกต้อง AS จะส่ง TGT พร้อมกับ Session Key ที่ใช้คุยกับ TGS กลับไปให้ Client
    - TGT สามารถนำไปใช้คุยกับ TGS เพื่อขอเข้าถึง Service บน Resource Server ได้ในขั้นตอนถัดไป

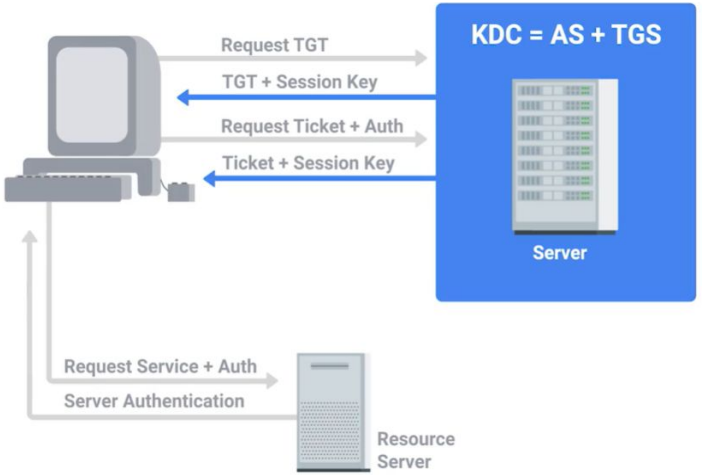
Authentication



Kerberos Authentication Flow

- 3. เมื่อ Client ต้องการเข้าถึง Resource Server ก็จะส่ง TGT และ Authenticator ไปหา TGS เพื่อ Request Ticket
    - Authenticator คือ Message ที่ประกอบไปด้วย Client ID และ Timestamp ซึ่งถูกเข้ารหัสด้วย Session Key ที่ได้รับมาจาก AS ก่อนหน้านี้
- 4. TGS จะพิสูจน์ตัวตน Client จาก TGT และ Authenticator ซึ่งหากถูกต้อง TGS จะส่ง Service Ticket พร้อมกับ Session Key ที่ใช้คุยกับ Resource Server กลับไปให้ Client
    - Service Ticket จะถูกนำไปใช้พิสูจน์ตัวตนได้ในขั้นตอนถัดไป

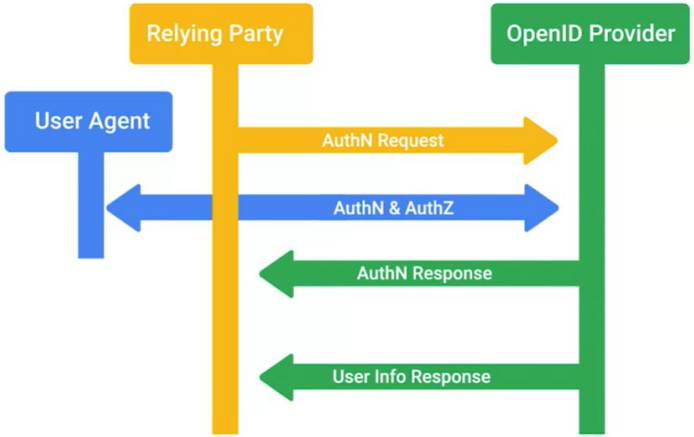
Authentication



Kerberos Authentication Flow

- 5. Client ส่ง Service Ticket และ Authenticator ไปหา Resource Server เพื่อ Request การเข้าถึง Service
    - Authenticator คือ Message ที่ประกอบไปด้วย Client ID และ Timestamp ซึ่งถูกเข้ารหัสด้วย Session Key ที่ได้รับมาจาก TGS ก่อนหน้านี้
- 6. Resource Server จะพิสูจน์ตัวตน Client จาก Service Ticket และ Authenticator ซึ่งหากถูกต้อง Resource Server จะส่ง Server Authentication กลับไปให้ Client
- 7. Client จะพิสูจน์ตัวตน Server ซึ่งหากถูกต้อง Client ก็จะสามารถเข้าถึง Service บน Resource Server ได้

Authentication



Single Sign-On (SSO) คือ การอนุญาตให้ผู้ใช้งานทำการพิสูจน์ตัวตนเพียงครั้งเดียว เพื่อที่จะเข้าถึง Service หรือ Application ต่าง ๆ ได้จำนวนมาก

- มักใช้งานร่วมกับ MFA เพื่อความปลอดภัยที่มากขึ้น

Example of SSO

- Kerberos
- OpenID คือ Open Standard ที่ทำให้ Web Application หนึ่ง (Relying Parties) สามารถใช้บริการ Authentication จาก Third-party ได้

Authentication

ข้อดีของ SSO

- ผู้ใช้งานใช้ Credential เดียวในการเข้าถึงระบบต่าง ๆ ทำให้มีความสะดวกมากขึ้น
- ลดเวลาในการทำ Authn
- ลดความเสี่ยงในการจดรหัสผ่านลงกระดาษ
- ลดปริมาณงานของ IT Helpdesk ในการช่วยเหลือการ Reset Password

ข้อเสียของ SSO

- Single Point of Failure
- หาก Account ถูกขโมย จะทำให้สามารถเข้าถึงระบบต่าง ๆ ได้จำนวนมาก

Authorization

Authorization (Authz) คือ การกำหนดสิทธิ์ในการเข้าถึง Resource ให้ผู้ใช้งาน

- กำหนดว่า Resource ใดที่ผู้ใช้งานสามารถเข้าถึงได้ และ Resource ใดที่ผู้ใช้งานไม่มีมีสิทธิ์เข้าถึง
- บางครั้งจะเรียกว่า Access Control System

Authorization

Example of Authz

- **RADIUS** สามารถกำหนดให้บาง User มีสิทธิ์เข้าถึง VPN ในขณะที่บาง User ไม่มีสิทธิ์เข้าถึง
- **TACACS+** สามารถกำหนดให้ Support Team มีสิทธิ์อ่าน Configuration บนอุปกรณ์ Switch ได้เท่านั้น แต่กำหนดให้ Admin Team มีสิทธิ์แก้ไข Configuration บนอุปกรณ์ Switch ได้
- **TGS** ใน Kerberos Protocol ทำหน้าที่กำหนดสิทธิ์ว่าผู้ใช้งานมีสิทธิ์เข้าถึง Service ที่ Request เข้ามาได้หรือไม่

Authorization

OAuth เป็น Open Standard สำหรับการทำ Authorization ที่สามารถอนุญาตให้ผู้ใช้งานให้สิทธิ์ Third-party Website หรือ Application ในการเข้าถึงข้อมูลของผู้ใช้งาน เช่น Mailing List ได้ โดยไม่ต้องบอก Credential ให้กับ Third-party

- Third-party App จะแสดงรายการข้อมูลที่ต้องการเข้าถึงให้ผู้ใช้งานเพื่อกดอนุญาตการเข้าถึงข้อมูลนั้น
- Third-party App จะได้รับ Access Token เพื่อใช้ในการเข้าถึง โดยใน Access Token จะมี Scope ที่บอกว่าข้อมูลใดที่สามารถเข้าถึงได้บ้าง

Authorization

Access Control List (ACL) คือ รายการของการกำหนดสิทธิ์ให้กับ Objects เช่น Files, Folders และ Programs เป็นต้น

- แต่ละบรรทัดของรายการจะเรียกว่า Access Control Entry (ACE)
- แต่ละ ACE จะกำหนดสิทธิ์ว่า User หรือ Group ใดสามารถ Read/Write/Execute กับ Object ได้

Accounting

Accounting คือ การบันทึกกิจกรรมต่าง ๆ ที่เกิดขึ้น (Logging)

- ใคร ทำอะไร ที่ไหน เมื่อไหร่ อย่างไร

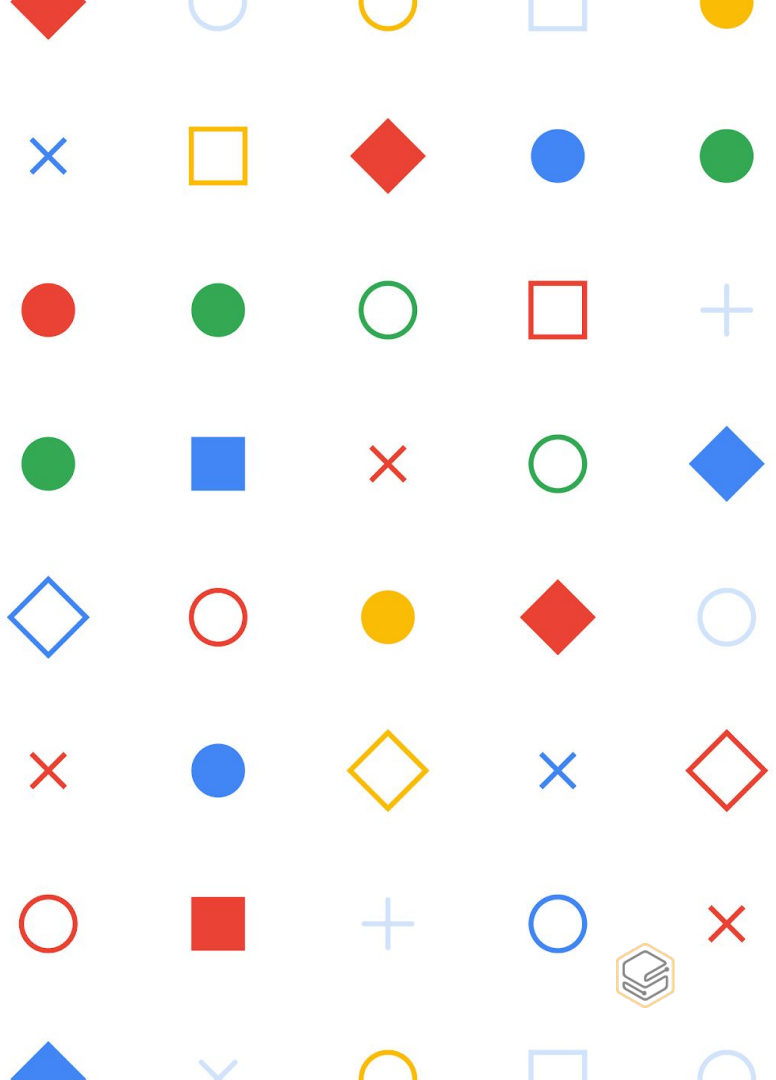
Auditing คือ การ Review กิจกรรมต่าง ๆ เพื่อตรวจสอบว่า มีเหตุการณ์ผิดปกติเกิดขึ้นหรือไม่

Example of Accounting

- TACACS+ มีการบันทึกว่า User ใดที่ Authn เข้ามา, เข้าถึงระบบใด, รัน Command อะไรบ้าง
- RADIUS มีการบันทึกว่า User ใดใช้งานเป็นระยะเวลาเท่าไหร่, ใช้ Bandwidth ไปเท่าไหร่

Week 4

Securing Your Networks



Samart Skills
A Grow with Google PROGRAM

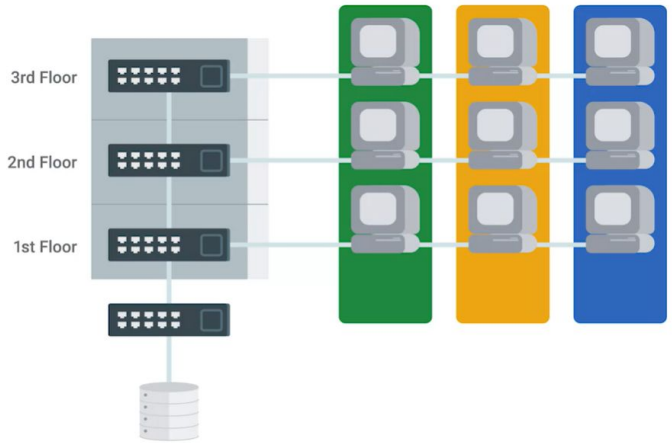
Skooldio

Secure Network Architecture

Least Privilege คือ การให้สิทธิ์ให้น้อยที่สุดเท่าที่จะสามารถทำงานได้

Implicit Deny คือ สิ่งใดที่ไม่ระบุชัดเจนว่าอนุญาต ให้ปฏิเสธไว้ก่อนเสมอ (Whitelisting)

Secure Network Architecture



Flood Guards คือ อุปกรณ์ที่ใช้ในการป้องกัน DoS Attack

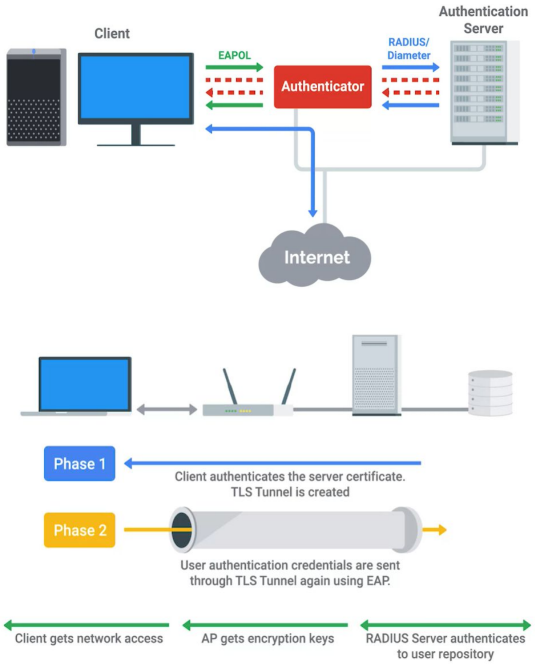
Network Separation หรือ Network Segmentation คือ การแบ่ง Network ออกเป็น Network ย่อย ๆ เพื่อให้ง่ายต่อการบริหารจัดการ และง่ายในการตรวจสอบและป้องกัน เช่น การแบ่ง VLAN

Secure Network Architecture

Switch Security Features:

- DHCP Snooping ช่วยป้องกัน Rogue DHCP Server Attack
- Dynamic ARP Inspection (DAI) ช่วยป้องกัน ARP Poisoning และ Man-in-the-middle Attack
- IP Source Guard (IPSG) ช่วยป้องกัน IP Spoofing

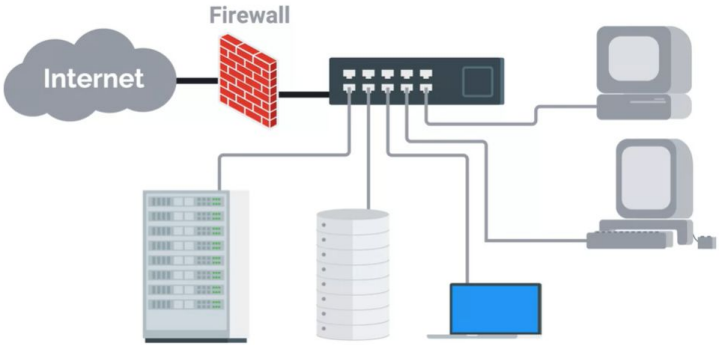
Secure Network Architecture



802.1X คือ มาตรฐานความปลอดภัยของเครือข่าย Ethernet, Wi-Fi และ Fiber

- ใช้ Extensible Authentication Protocol (EAP) ในการพิสูจน์ตัวตนเพื่อเข้าใช้เครือข่าย
  - บางครั้งจึงถูกเรียกว่า EAP over LAN (EAPOL)
- EAP-TLS เป็นประเภทของการทำ Network Authentication ที่นำ Certificate เข้ามาช่วย ทำให้การพิสูจน์ตัวตนมีความปลอดภัยมากยิ่งขึ้น
  - จำเป็นต้องมี PKI Infrastructure

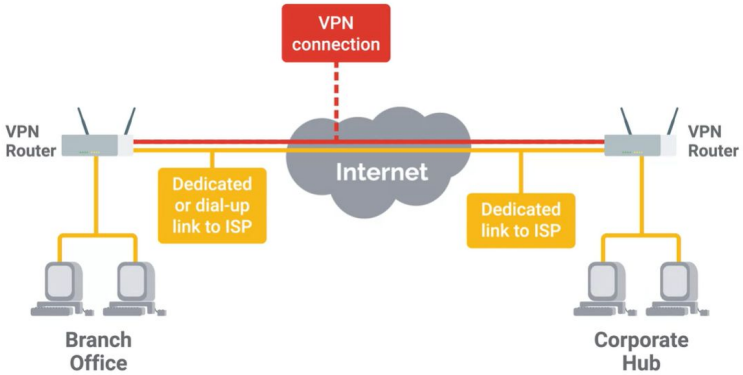
Secure Network Architecture



Firewall คือ อุปกรณ์หรือ Software ที่ทำหน้าที่อนุญาตหรือปฏิเสธ Traffic ตามกฎที่ตั้งไว้

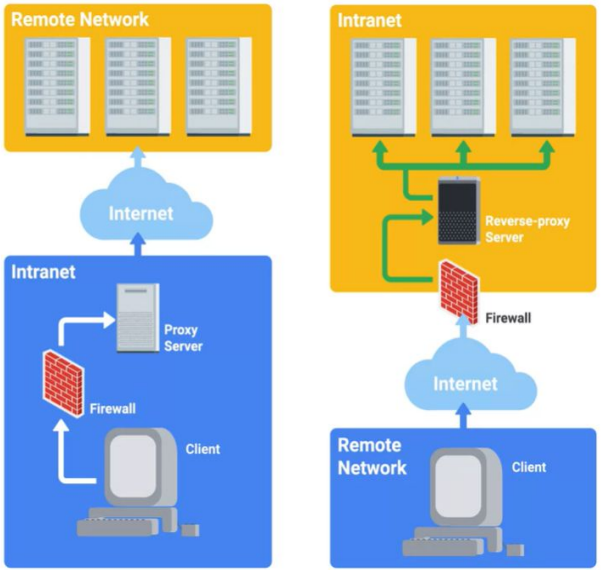
- Network-based Firewall เป็น Firewall ที่ถูกติดตั้งอยู่ในระบบ Network
- Host-based Firewall เป็น Firewall ที่ถูกติดตั้งอยู่บนเครื่องคอมพิวเตอร์
  - ช่วยป้องกันการโจมตีเมื่ออยู่ใน Untrusted Network
  - ช่วยป้องกันการโจมตีจากเครื่องคอมพิวเตอร์ที่ถูก Compromised ใน Trusted Network เดียวกัน

Secure Network Architecture



VPN ทำให้ Remote Access เข้าสู่เครือข่ายขององค์กรปลอดภัย รวมถึงยังสามารถทำให้ Link ระหว่าง Network มีความปลอดภัยได้ด้วย

Secure Network Architecture

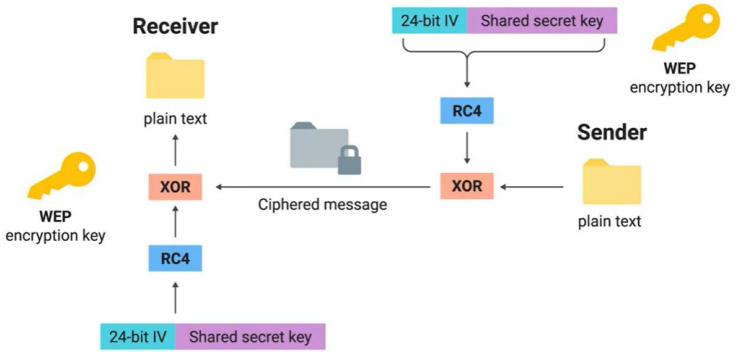


Proxy คือ อุปกรณ์ที่เป็นตัวแทนผู้ใช้งานในการติดต่อออกไปสู่อินเทอร์เน็ต

- Logging การใช้งาน Website ของผู้ใช้งานได้
- Block Website หรือ Content ที่อาจเป็นอันตรายหรือขัดกับนโยบายองค์กรได้

Reverse Proxy คือ อุปกรณ์ที่ช่วยให้ Remote Access ไปหา Web-Based Service ได้อย่างปลอดภัย โดยไม่ต้องใช้ VPN

Wireless Security



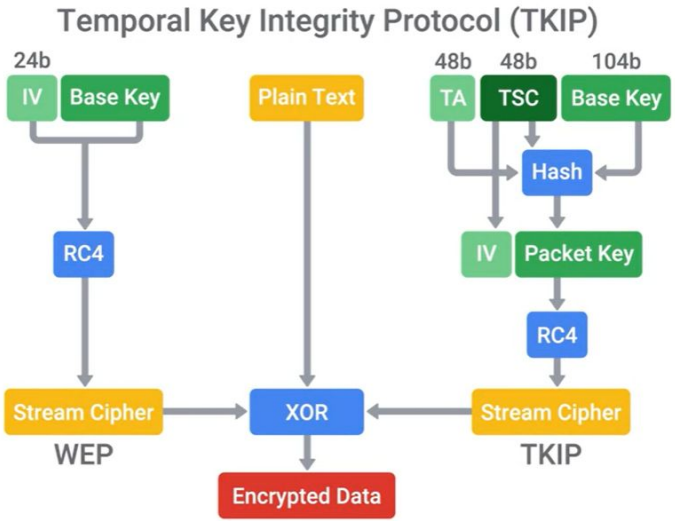
Wired Equivalent Privacy (WEP)

- เพื่อป้องกันการดักจับข้อมูล (Eavesdropping)
- RC4 Symmetric Stream Cipher
- Shared Secret Key Length: 40-Bit
- Concat with Initialization Vector (IV) 24-Bit

WEP ไม่ปลอดภัยเนื่องจาก:

- RC4 Stream Cipher มีช่องโหว่หลายจุด
- วิธีการในการ Generate Encryption Key ไม่ปลอดภัย
- จำนวน Bit ของ IV สั้นเกินไป ทำให้เกิดการ Reuse ได้ง่าย

Wireless Security



WPA (Wi-Fi Protected Access) ถูกออกแบบมาใช้แทน WEP ชั่วคราว

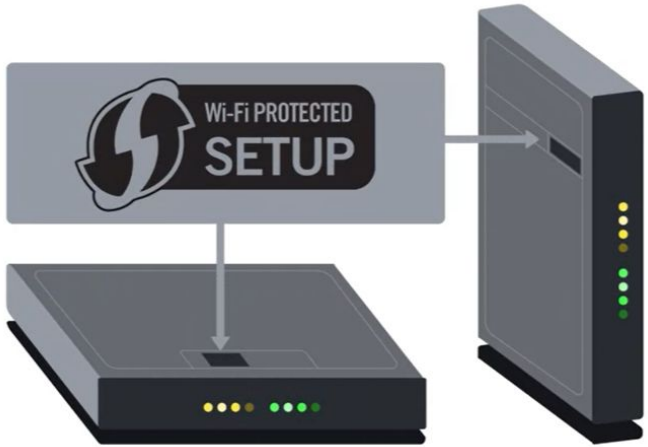
- TKIP (Temporary Key Integrity Protocol)
  - ยังคงใช้ RC4 Stream Cipher แต่มีกระบวนการทำให้การ Generate Encryption Key ปลอดภัยขึ้น
  - ใช้ Sequence Counter ในการป้องกัน Replay Attack
  - ใช้ Message Integrity Check (MIC) ในการตรวจสอบ Integrity ของ Packet
- Pre-Shared Key 256 Bits

Wireless Security

WPA2 ถือว่าปลอดภัยในปัจจุบัน

- AES Cipher
- CCMP (Counter Mode CBC-MAC Protocol) เป็น Operation Mode หนึ่งของ Block Cipher ซึ่งมีการทำ Authenticated Encryption
- สามารถใช้ร่วมกับ 802.1X ได้ ซึ่งจะเรียกว่า WPA2-Enterprise
- หากไม่ได้ใช้ร่วมกับ 802.1X จะเรียกว่า WPA2-Personal หรือ WPA2-PSK ซึ่งใช้ Pre-Shared Key ในการพิสูจน์ตัวตน
- สามารถถูกโจมตีด้วย Dictionary Attack และ Rainbow Tables Attack ได้ ซึ่งป้องกันโดย
    - ตั้ง Password ให้มีความแข็งแรง
    - เปลี่ยนชื่อ SSID ให้ไม่ใช้ชื่อที่เป็น Common

Wireless Security

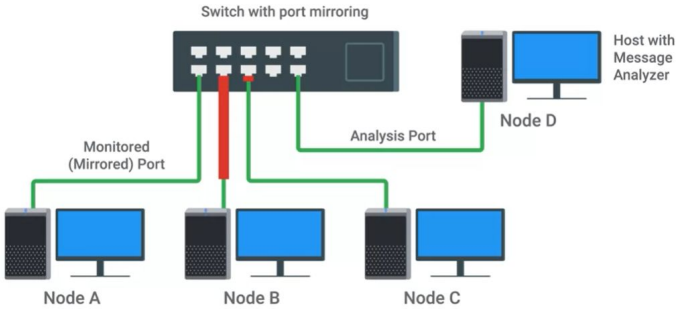


WPS (Wi-Fi Protected Setup) ถูกออกแบบมาเพื่อให้ง่ายต่อผู้ใช้งานในการเชื่อมต่อ

WPA-PSK

- โดยส่วนมากจะใช้วิธีกดปุ่มเฉพาะที่อยู่บนอุปกรณ์ Access Point และบนอุปกรณ์ Client ในการพิสูจน์ตัวตน
- อีกวิธีหนึ่งที่นิยมคือการใช้ PIN ความยาว 8 หลักในการพิสูจน์ตัวตน
    - สามารถถูกโจมตีด้วย Brute Force Attack ได้
- การป้องกัน:
    - ตั้ง Lockout Policy เช่น หากใส่ PIN เกิน 5 ครั้งให้ Lock การพิสูจน์ตัวตน
    - Disable WPS

Network Monitoring



Packet Sniffing or Packet Capture คือ การดักจับ Packet จาก Network Traffic เพื่อนำมาใช้วิเคราะห์

- ต้องเปิด Promiscuous Mode บน Network Interface
- ต้องใช้สิทธิ์ Admin หรือ Root

Capture Packets บน Wireless Network

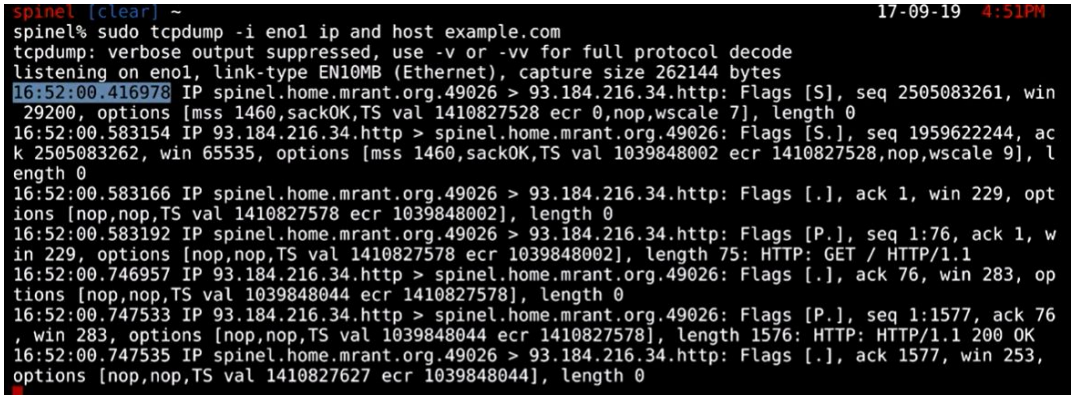
- Monitor Mode จะทำให้สามารถ Capture Wireless Traffic ที่ถูกส่งไปมาระหว่าง AP และ Client ในบริเวณนั้นได้

Port Mirroring คือ ความสามารถของอุปกรณ์ Switch ในการ Mirror Packets จาก Port หรือ VLAN ไปยัง Port ที่ระบุ

Network Monitoring

Tcpdump คือ Command-Line Based Program ที่ใช้ในการ Capture และ Analyze Packets

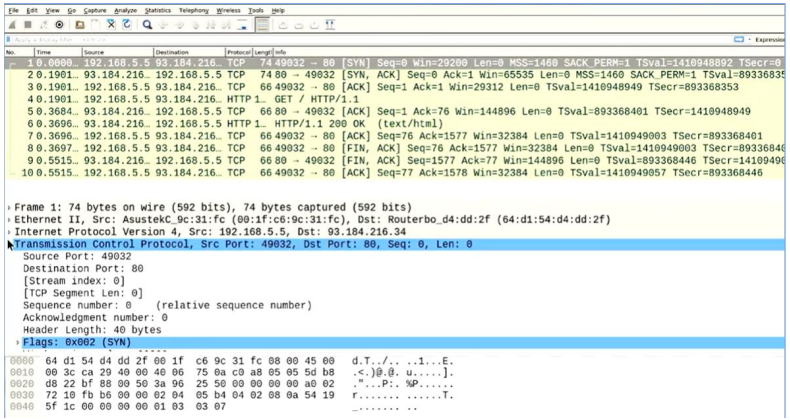
- ต้องใช้สิทธิ์ระดับ Root ในการ Capture



Network Monitoring

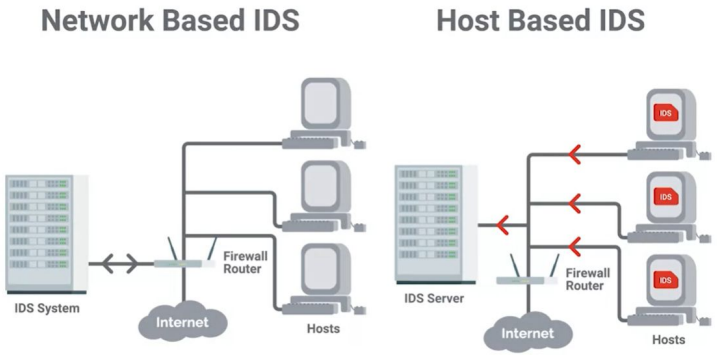
- **Basic Commands for Tcpdump**
  - เริ่มการ Capture Packets บน Interface ที่ต้องการ
    - sudo tcpdump -i [INTERFACE]
  - หยุดการ Capture ด้วยการกด Ctrl+C
  - เริ่มการ Capture Packet แบบละเอียด โดย Filter เฉพาะ IP Address และ Port ที่สนใจ
    - sudo tcpdump -i [INTERFACE] -vn host [IP_ADDRESS] and port [PORT]
  - Save Packet ที่ถูก Captured ลงใน File
    - sudo tcpdump -i [INTERFACE] -w [FILENAME]
  - อ่าน File ที่ Capture ไว้
    - tcpdump -r [FILE]

Network Monitoring



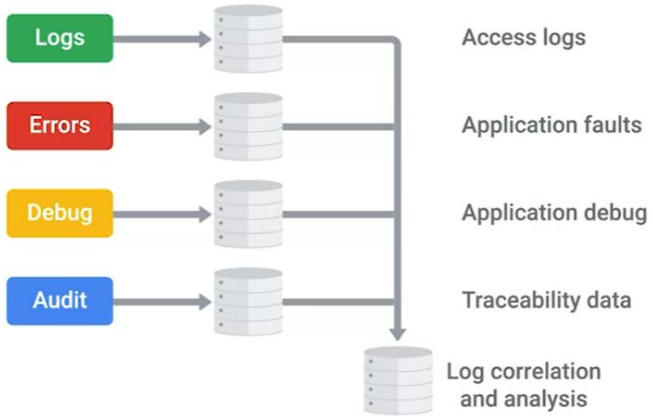
- **Wireshark** คือ Graphical Program ที่ใช้ในการ Capture และ Analyze Packets
    - มีความสามารถในการวิเคราะห์ Protocol และ Application

Network Monitoring



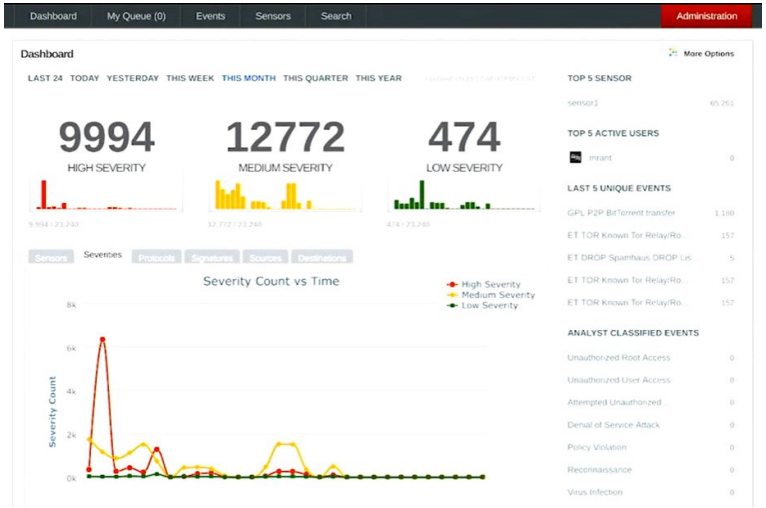
- **Intrusion Detection/Prevention Systems (IDS/IPS)** คือ อุปกรณ์รักษาความปลอดภัยซึ่งทำหน้าที่คอยตรวจจับและวิเคราะห์ Traffic เพื่อหา Malicious Traffic
  - IDS: Detect, Log, and Alert
  - IPS: Block Attack ได้หลังจาก Detect
  - Network-Based IDS/IPS (NIDS)
  - Host-Based IDS/IPS (HIDS)

Network Monitoring



- **Centralized Logging** คือ การเก็บรวมรวม Log จากแหล่งต่าง ๆ เช่น Firewall Logs, Authentication Server Logs เพื่อนำข้อมูลมาเก็บรักษาและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Log Analysis)
  - **Normalizing Logged Data** คือ การนำ Log ที่อยู่ในรูปแบบแตกต่างกัน มาจัดให้อยู่ในรูปแบบเดียวกัน เพื่อให้ง่ายต่อการนำไปใช้งานและการวิเคราะห์
  - **Correlation Analysis** คือ การวิเคราะห์ความสัมพันธ์ของ Logs ต่าง ๆ
  - สร้าง Rule ในการแจ้งเตือน (Alert)
  - Investigating and Event Reconstruction
  - Auditing

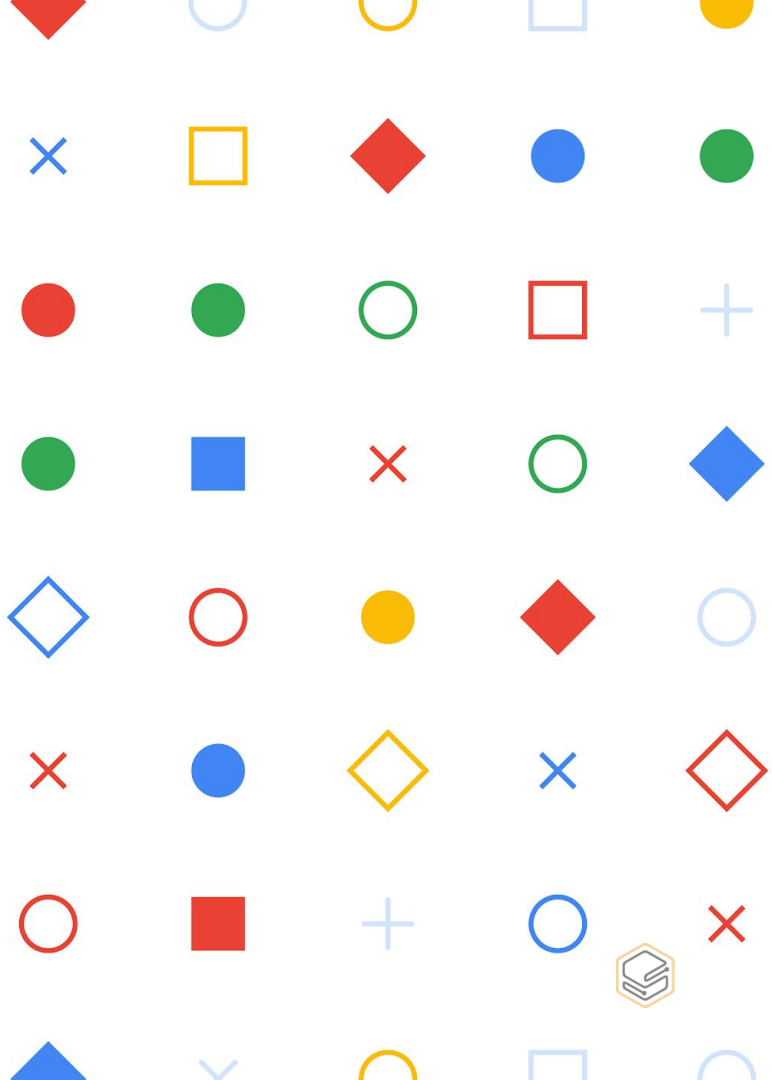
Network Monitoring



- **SIEM (Security Information and Event Management)** คือ ระบบที่ทำหน้าที่เป็น Central Log Server และนำมาวิเคราะห์เพื่อตรวจหาเหตุการณ์ภัยคุกคามทางไซเบอร์ และแจ้งเตือนเมื่อเกิดเหตุการณ์ได้

Week 5

Defense in Depth



Samart Skills
A Grow with Google PROGRAM

Skooldio

System Hardening

- **Defense in Depth** คือ แนวความคิดที่ใช้การป้องกันหลาย ๆ ชั้น โดยมีจุดประสงค์หลักเพื่อลดความเสี่ยงในการถูกโจมตี
- **Attack Vector** คือ วิธีการที่ผู้ไม่ประสงค์ดีหรือ Malware ใช้ในการเข้าถึงระบบหรือ Network เช่น Email Attachments, Network Protocols และ User Input เป็นต้น
- **Attack Surface** คือ ผลรวมของหลาย ๆ Attack Vectors ที่แตกต่างกันต่อระบบหนึ่ง

System Hardening

- **Disable Components, Services และ Software ที่ไม่จำเป็นต้องใช้แล้ว**
  - ช่วยลด Attack Surface
- **ไม่ให้ผู้ใช้งานใช้สิทธิ์ Administrator**
  - เพื่อป้องกันไม่ให้ผู้ใช้งาน Disable Security Features
- **Logging and Auditing**

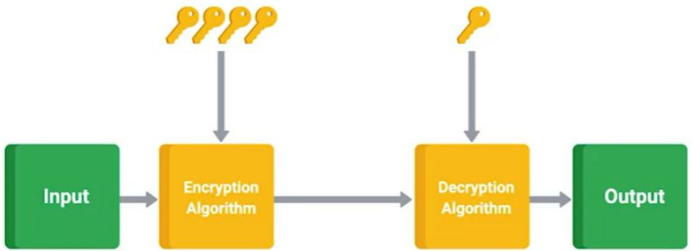
System Hardening

- **Antimalware Protection**
  - Antivirus Software เป็นโปรแกรมสำหรับป้องกัน Malware โดยจะตรวจสอบและวิเคราะห์ไฟล์ต่าง ๆ บนเครื่องคอมพิวเตอร์ที่ตรงกับ Malware Signatures
  - Malware Signature คือ ฐานข้อมูลของ Malware ที่ถูกจัดเก็บในรูปแบบของ Hash
  - ช่วยป้องกัน Common Attacks ส่วนใหญ่ที่อยู่บนอินเทอร์เน็ต

System Hardening

- **Full-Disk Encryption (FDE)** คือ การเข้ารหัสข้อมูลทั้งหมดบน Disk
  - ช่วยป้องกันการขโมยข้อมูลที่อยู่ใน Disk ในกรณีที่เครื่องหายหรือถูกขโมย (Confidentiality)
  - ช่วยป้องกันการแก้ไขข้อมูลบน Disk ได้ (Integrity)
  - ยังคงมีบางส่วนที่ไม่สามารถเข้ารหัสได้คือ ส่วนที่ใช้ในการ Boot OS ทำให้เป็นช่องทางที่ผู้ไม่ประสงค์ดีอาจจะเข้าไปแก้ไขไฟล์ให้เป็น Malicious ไฟล์ได้

System Hardening



- **Full-Disk Encryption (FDE)**
  - จำเป็นต้องใช้ Key ในการ Encrypt และ Decrypt ข้อมูลบน Disk
  - โดยปกติการเข้าถึง Key นั้นจะต้องใส่ Password ซึ่งอาจจะทำให้เกิดปัญหาการลืม Password ของผู้ใช้งานอยู่บ่อยครั้งสำหรับองค์กรใหญ่ ทำให้ไม่สามารถกู้คืนข้อมูลใน Disk ได้
  - **Key Escrow** คือ การเก็บ Encryption Key อย่างปลอดภัยไว้กับ Authorized Party ซึ่งสามารถนำมาใช้ในภายหลังได้
    - หากผู้ใช้งานลืม Password ในการถอดรหัส Disk ก็สามารถไปใช้ Key ที่ Authorized Party เก็บไว้ได้

Application Hardening

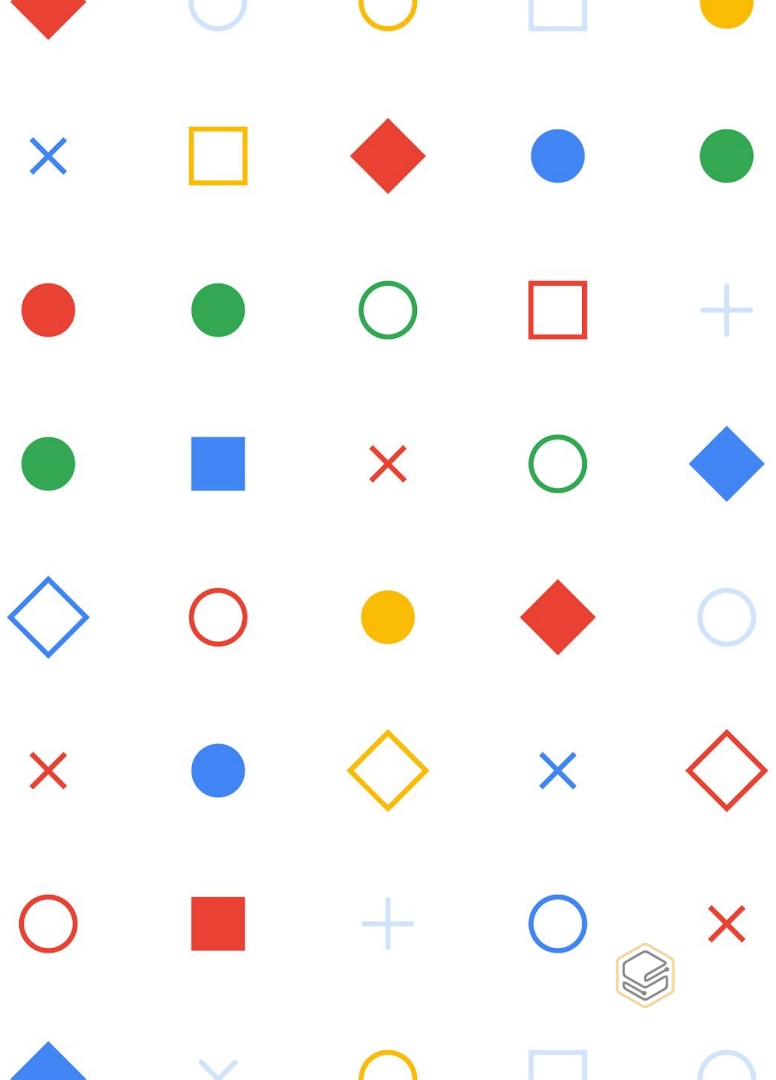
- **ติดตั้ง Security Patch และ Update ของ Software อย่างสม่ำเสมอ**
  - Software จะรวมไปถึง OS และ Firmware ของ Hardware ด้วย
  - Software Update ไม่เพียงแต่ปรับปรุงประสิทธิภาพการทำงาน เพิ่มความเสถียร หรือเพิ่ม Features ใหม่ ๆ ให้ Software แต่ยังทำการปิดช่องโหว่ต่าง ๆ ที่พบด้วย
  - Software Patch Management ใช้ในการบริหารจัดการ Software และตรวจสอบ Software Update บนเครื่องคอมพิวเตอร์ขององค์กร

Application Hardening

- **Application Policy** เป็นนโยบายที่กำหนดว่า Application ใดที่อนุญาตและไม่อนุญาตให้ใช้ในองค์กร
    - รวมถึงกำหนดว่าควรจะต้องใช้ Software ที่เป็น Version ล่าสุด

Week 6

Creating a Company Culture for Security



Samart Skills
A Grow with Google PROGRAM

Skooldio

Risk in the Workplace

กฎหมายหรือข้อบังคับที่เกี่ยวกับ Security

- **PCI-DSS** (Payment Card Industry Data Security Standard) เป็นมาตรฐานที่บังคับใช้กับองค์กรที่ต้องจัดการกับการใช้จ่ายด้วยบัตร

Risk in the Workplace

6 Main Objectives of PCI-DSS

- 1. to Build and Maintain a Secure Network and Systems
  - ติดตั้งและตั้งค่า Firewall
  - ไม่ใช้ Default Password ที่มากับระบบ
- 2. to Protect Cardholder Data
  - Encrypt Cardholder Data ที่ถูกส่งไปมาใน Open Network
- 3. to Maintain a Vulnerability Management Program
  - ติดตั้งและ Update Antivirus Software
  - Vulnerability Scanning

Risk in the Workplace

6 Main Objectives of PCI-DSS

- 4. to Implement Strong Access Control Measures
  - ให้เข้าถึง Cardholder Data กับผู้ที่มีสิทธิ์เท่านั้น
  - 2FA
- 5. to Regularly Monitor and Test Networks
  - ติดตั้ง IDS
  - Vulnerability Scan for Network
- 6. to Maintain an Information Security Policy

Risk in the Workplace

- **Balance Between Security and User Productivity**
  - Security เป็นเรื่องเกี่ยวกับการพิจารณา Risk และการจัดการกับ Risk นั้น เพื่อให้ Risk อยู่ในระดับที่รับได้
- **Risk** ก็คือ โอกาสที่จะเกิด Attack และมีผลเสียหายกับระบบ
- **High-Value Data** หมายถึงข้อมูลที่มีความสำคัญกับองค์กร เช่น Usernames, Passwords, Customer Data
- **Threat Modeling** คือ การหาว่ามีภัยคุกคามใดบ้างที่สามารถเข้ามาโจมตีระบบได้

Risk in the Workplace

Vulnerability Scanner คือ Software ที่ทำการตรวจสอบช่องโหว่ของและ Misconfiguration ของระบบและ Network เช่น Nessus, Qualys, OpenVAS

Penetration Testing คือ การทดสอบความแข็งแกร่งของระบบ โดยการพยายามเจาะระบบและ Network เพื่อตรวจสอบว่าระบบมีช่องโหว่ที่สามารถโจมตีได้หรือไม่

- In-house หรือ Third-party
- อาจพบช่องโหว่ที่ Vulnerability Scanner ตรวจไม่พบ

Risk in the Workplace

Privacy Policy คือ นโยบายที่ใช้ในการกำกับดูแลการเข้าถึงและใช้งานข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลส่วนบุคคลของลูกค้า

- ต้องมีการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึงและใช้ข้อมูลได้

Data Handling Policy คือ นโยบายที่ใช้ในการกำกับดูแลการนำข้อมูลไปใช้งาน โดยแบ่งตามลำดับชั้นความลับ (Data Classification)

- แต่ละลำดับชั้นจะมีความเข้มข้นในการป้องกันไม่เท่ากัน
- เช่น การส่ง Sensitive Data จะต้องส่งแบบเข้ารหัส และห้ามเก็บ Sensitive Data บน Removable Media หรือ Public Cloud Storage

Users

Bad User Habits

- ปล่อยคอมพิวเตอร์ที่ Login แล้วทิ้งเอาไว้ โดยไม่ Lock Screen
- จด Password และแปะไว้บนโต๊ะหรือคอมพิวเตอร์
- Upload Sensitive Data ไปเก็บไว้บน Public Cloud

Users

Security Training จะช่วยให้ผู้ใช้งานมีความตระหนักใน Security เพิ่มมากขึ้น รวมถึงสามารถเปลี่ยนพฤติกรรมผู้ใช้งานและปลูกฝัง Security Culture ให้กับองค์กรได้

- คอร์สอบรม Offline/Online, Short Video พร้อมทั้งมี Quiz เพื่อทดสอบความเข้าใจ
- กำหนดให้ผู้ใช้งานเข้าอบรม Security Training อย่างน้อยปีละครั้ง
- มีช่องทางให้ผู้ใช้งานถามคำถามหรือแจ้งเหตุการณ์เกี่ยวกับ Security เช่น Mailing List, Website เป็นต้น
- Poster หรือใบปลิวเกี่ยวกับ Security

Users

- **ตัวอย่างเนื้อหาของ Security Training**
  - Security Policy ขององค์กร
  - ภัยคุกคามทางไซเบอร์ที่พบเป็นประจำและวิธีการป้องกัน เช่น Phishing เป็นต้น
  - Good User Habits
    - Lock Screen ทุกครั้งที่ไม่อยู่หน้าคอมพิวเตอร์
    - ตั้ง Password ที่มีความแข็งแรง
    - ใช้ 2FA
    - ตรวจสอบ Website URL ก่อนใส่ข้อมูล Credential เสมอ
    - ถามคำถามเกี่ยวกับ Security ผ่านช่องทางที่กำหนด เมื่อมีความไม่แน่ใจเรื่อง Security

Users

Third-party Security หมายถึง การประเมินความปลอดภัยของ Vendor หรือ Third-party

- Vendor Security Assessment Questionnaires จะช่วยให้รู้ถึง Security Policies, Procedures และอุปกรณ์รักษาความปลอดภัยที่ถูกติดตั้งไว้
    - Google มีให้ Download ฟรี https://vsaq-demo.withgoogle.com/
- ทดสอบ Vendor's Hardware or Software เพื่อตรวจสอบดูว่ามีช่องโหว่หรือไม่
- Security Audit Report

Incident Handling

Incident Handling Process

- **Detection** เช่น มี Alert จากอุปกรณ์ IDS หรือมีผู้ใช้งานแจ้งพฤติกรรมที่น่าสงสัยเข้ามา
- **Analysis** คือ การวิเคราะห์ Incident ว่ามีผลกระทบรุนแรงระดับใด (Severity) และกระทบเป็นวงกว้างแค่ไหน (Scope)
    - Severity สามารถประเมินมาจาก
        - Effect to Business Functions: มีผลกระทบกับการดำเนินธุรกิจหรือไม่?
        - Chance of Exploitation: โอกาสที่จะถูกโจมตี
        - Type of Access Gained: เข้าถึงสิทธิ์ระดับใด
        - Remotely Exploitable or Not: สามารถโจมตีจากระยะไกลได้หรือไม่?

Incident Handling

Incident Handling Process

- **Containment** คือ การป้องกันไม่ให้เสียหายไปมากกว่าเดิม เช่น Disconnect Network หรือ เปลี่ยน Password เป็นต้น
- **Remediation** คือ การแก้ไข Incident และการกู้คืนระบบให้กลับมาทำงานเป็นปกติ รวมถึงการทำ Root Cause Analysis เพื่อการป้องกันไม่ให้ Incident เกิดซ้ำ
    - ต้อง Test ก่อนที่จะนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบที่ Restore ขึ้นมาจะสามารถทำงานได้

Incident Handling

Incident Handling Process

- **Lesson Learn** คือ การเรียนรู้จาก Incident
  - สามารถเรียนรู้เหตุการณ์ที่เกิดขึ้นโดยการ Review และ Analyze Log ได้
  - เหตการณ์ที่เกิดขึ้นคืออะไร? สาเหตุการเกิดคืออะไร? ตอบสนองต่อเหตุการณ์อย่างไร? ป้องกันไม่ให้เกิดซ้ำได้อย่างไร?