

Introduction to Network and Information Security

week 1

Information security + Network ສັກຂອດນູດຄວບຄຸງໄປສ່ວຍເກີນ
Security → ການພໍ່ລົດ / ຂອງເບີນຍົງໄວ້ໃຫ້ການຈຳກົງຂອງຮະບັນຫຼຸດ

☞ ລຳດັບມູນການປຶກປັບປຸງ

NW security → focus ເພື່ອປຶກປັບປຸງທີ່ມີຄວາມເຕັມໃດລັບ (Physical Security)
ໃນເກມທີ່ເຮົາສິ່ງປຸກຄົນຕ່າງໆ @ server storage, pc, notebook

ຂໍ້ມູນທີ່ໂປ່ງຢູ່ໃນເນັ້ນດີ່ກໍ່ຂໍ້ມູນລົ້າສຳຄັນຂອງອົງຄົກ

• Security = major business concern

- Physical asserts: ເປັນຮະບັບທີ່ເກົ່າສາມາດຈັດກາໄດ້, ມອງເນັ້ນໄດ້
: security ທີ່ຫຼືຈະຕໍ່ພົມຄະເນັ້ນແລຍ

- Information asserts: m protected passwords, coding, certificates

• Computer and Internet → ກໍານົດລົ້າຖານຂອງການປະລິດກັບຂອງອົງຄົກໃນໆ

• Laws & enforcement in cyber crime → ex. ການກຳລັງ, ຫ້າຍຫັ້ນ, ເປົ້ນແປລ
↳ ມອບຊັບໃຊ້ : but ການປັບປຸງສາມາດໃຊ້ດັກນັກ

Example :

Shingeki no Kyojin,
Attack on Titan Wall



Wall → ກໍາເພີ້ນປະຈຸບັນທີ່ກັບກົກການ ແຕ່ທີ່ສ່ວຍເຮັດວຽກກັບຄວາມລຳດັບ
(priority)

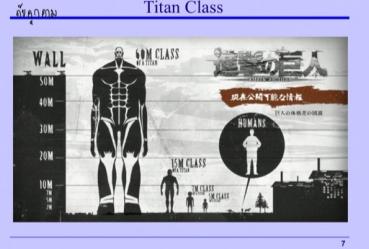
ຮັບນັດກາ wall Mariq

ຮັບກາລາງ wall Rose

ຮັບໄວ້ wall sing



Titan class → ກົມຖຸກຄົມ



ເສີ່ອງ !! →

PDPA : ພູມການກົດລົ້າໂຄນົດ, ດັບຄວນນິ້ນາ, ເປົ້ນຂອບດົກ computer
www.comtex.vip ການຄຸນໄວ້ເວັບໄວ້ PDPA

- ເກົ່າສ່ວນຄວາມເຕັມ (CBP)
- ເມື່ອມາດວິວດີວິວດີ
- ເກົ່າສ່ວນຄວາມສຳເນົາ
- ເກົ່າສ່ວນຄວາມເຕັມ, Business, ແລະ ຕົກລະຫັດ, security policy

Introduction to

Network and Information

Security → ການພໍ່ລົດ

- Ex. ມີລົງລະບົບເຊີນ → ເກົ່າສ່ວນຄວາມເຕັມເປົ້າມາ
 - Login, ພົມເຊີນ
 - ປົມເຊີນ
 - "username + password"
 - "security USB"

Business Data Communications and Networking 8th Edition

Jerry Fitzgerald and Alan Dennis
John Wiley & Sons, Inc

Primary Goals in Providing Security : เป้าหมายหลักในการรักษาความปลอดภัย . CIA

CIA : คืออะไร

Confidentiality : "C" เป็นเกี่ยวกับเรื่อง focus , protected Data (การ login + การที่ Authentication หรือไม่ได้)
↳ เป็นการ protected Data มาก ถ้า ก็ไม่มีสิทธิ์เข้าถึง , การรักษาความลับ + ป้องกันการอินไซด์ Data (Confidentiality)
UNAUTHORIZED

- Integrity : "I" แสดงถึงความน่าเชื่อถือ เชื่อมั่นว่า รายการข้อมูลนี้ ไม่ถูก tamper หรือเปลี่ยนแปลง (ข้อมูลจะต้องถูกตรวจสอบ , ข้อมูลที่เราได้รับเป็นปัจจุบัน = get ข้อมูลที่ต้องการแน่นอน)
- Availability : "A" ความพร้อมของข้อมูล



Confidentiality คือ ลักษณะและการเข้าถึงข้อมูล
บุคคลที่มีสิทธิ์เข้าถึงข้อมูลได้ ไม่ว่าจะมีสิทธิ์เข้าถึง
ข้อมูล

Integrity: ความถูกต้องของข้อมูล
ข้อมูลถูกต้อง หรือถูกเก็บ ต้องไม่ถูกแก้ไขโดยผู้
ที่ไม่มีสิทธิ์

Availability: ความพร้อมให้ใช้งาน
ไฟฟ้า หรือ ช่องทางเดินทางเข้าถึงต่อคอมพิวเตอร์ จาก
บุคคลที่มีสิทธิ์

EXAMPLE :

Confidentiality

ต้องคำนึงถึงการรักษาความลับและการเข้าถึงข้อมูลในรากฐาน



Share password: I password ให้เพื่อน หรืออาจารย์เป็นคนดูแล ล้ำเส้นขอบเขตของข้อมูลและaccount ของ
เราไม่ให้เข้าถึงข้อมูล อย่างเช่น รหัส ชื่อ นามสกุล หรืออีเมล

Post it password: หากเราโพสต์ข้อความที่มีรหัส รหัสผ่าน ไปในโซเชียลมีเดีย เช่น facebook ที่มีคนเข้ามาดูอาจทำข้อมูลนั้นพัง掉

▶ Confidentiality

Integrity

ห้ามให้คนอื่นเข้ามายั่งคานาไปได้ เนื่องจากมีข้อมูลที่สำคัญต้องห้าม

แบบนี้ เช่น software หรือไฟล์ ข้อมูล นิยามไว้ให้เป็นตัวตนอยู่ต้องห้าม ไม่ให้คนอื่นเข้ามายั่งคานาไปได้ เช่น ไฟล์ ข้อมูล internet บางอย่างไม่ได้ไว้เป็น public ก็ต้องห้าม

MDS, SHA1, SHA2 ลักษณะเดียวกันใช้ SHA2 เป็น algorithm ที่ใช้กับข้อมูลที่ต้องห้าม ไม่ให้คนอื่นเข้ามายั่งคานาไปได้ เช่นไฟล์ ข้อมูล นิยามไว้ให้เป็นตัวตนอยู่ต้องห้าม ไม่ให้คนอื่นเข้ามายั่งคานาไปได้ เช่น File

แนะนำ MDS, SHA1 หรือ SHA2 มาก

▶ Integrity

Availability

ความพร้อมใช้งาน กรณีมีลักษณะเช่นไฟล์ ก็ต้องซื้อไฟล์ได้ทุกเวลาที่ต้องการ ไม่ใช่วันนี้ซื้อ Gmail ได้ พวชั่ง
Gmail ล่ม เข้าได้บ้าง ไม่ได้บ้าง หรือบางเว็บที่เผลอเรากด F5 บอยๆ แม่จะกลับมาซึ่งกัน

▶ Availability

Types of Security Threats ➔ ภัยคุกคาม

Threats แบ่งเป็น 2 กลุ่ม

1. เกี่ยวกับ Business : ผู้เอาจริงที่ทำให้บุคคล ระบุช่องทาง

- Disruptions (รบกวน)

- ความเสียหาย ด้าน network service

- ผู้รุกราน เลี้นหาย ลarc รัชต์ชั่ง : งานเล็กน้อยหรือชั่วคราว

- Destructions of data ➔ การทำลายข้อมูล

① ② - Viruses destroying filer , crash of hard disk

- Disasters (Natural or Manmade Disasters)

ภัยพิบัติ ➔ เกิดจากผู้รุกราน

EX. Data on Hardisk NETWORK SERVICE

ผู้ Professional Hacker ลarc รัชต์ชั่ง เจ้าหน้าที่

↑

Types of Security Threats	
Business continuity planning related threats	threats relating to business
- Disruptions	ความเสียหายของระบบ service
- Loss or reduction in network service	• Loss or reduction in network service
- Could be minor or temporary (a circuit failure)	virus + ภัยคุกคาม
- Destructions of data	ข้อมูลหาย
- Viruses destroying files, crash of hard disk	• Viruses destroying files, crash of hard disk
- Disasters (Natural or manmade disasters)	ex. Data on hardisk network service
-	• May destroy host computers or sections of network
- Intrusion	การตั้งรหัสผ่านที่ไม่ถูกต้อง
- Hackers gaining access to data files and resources	• Hackers gaining access to data files and resources
- Most unauthorized access incidents involve employees	
- Results: Industrial spying; fraud by changing data, etc.	

2. Intrusion (การบุกรุก)

- Hackers gaining (Hackers แอบฝ่ายเบื้องหลัง) สามารถเข้าถึงข้อมูลและผู้ใช้งาน
ผู้ใช้งานต้องระวัง
- Most unauthorized : กรณีที่เกิดขึ้นไม่ได้รับอนุญาต ลarc รัชต์ชั่ง เจ้าหน้าที่ของรัฐกับผู้คน
- Results : Industrial spying (ภาคธุรกิจลักทรัพย์) fraud by changing data : การตั้งรหัสผ่านเปลี่ยนข้อมูล

ମୁଖ୍ୟ ପରିକାଳ
ମୁଖ୍ୟ ପରିକାଳ
ମୁଖ୍ୟ ପରିକାଳ

Network Controls

గිවිස්සානු පාඨමයි

សំណង់

- Mechanisms that reduce or eliminate the threats to network security
 - Types of controls:
 - Preventative controls ពេលការងារបានត្រូវ
▪ Mitigate or stop a person from acting or an event from occurring (e.g., locks, passwords, backup circuits)
 - Detective controls មួយក្នុងរាជ្យរាល់
▪ Reveal or discover unwanted events (e.g., auditing)
 - Documenting events for potential evidence
 - Corrective controls ដែលការពិនិត្យអនុវត្តន៍ក្នុងរាជ្យរាល់
▪ Remedy an unwanted event or a trespass (e.g., reinitiating a network circuit)

Securing the Network

- Securing the network requires personnel designated to be accountable for controls:
 - Develop network controls
 - Ensure that controls are operating effectively
 - Update or replace controls when necessary
 - Need to be reviewed periodically for usefulness, verification and testing:
 - Ensure that the control is still present (verification)
 - Determine if the control is working as specified (testing)
 - Is the control still working as it was specified?
 - Are there procedures for temporary overrides on control?

Security Threats

- **Identify threats**
 - Any potentially adverse occurrence that can
 - Harm or interrupt the systems using the network, or
 - Cause a monetary loss to an organization
 - **Rank threats according to**
 - Their probability of occurrence
 - Likely cost if the threat occurs
 - **Take the nature of business into account**
 - Example: Internet banking vs. a restaurant
 - Bank's web site: has a higher probability of attack and much bigger loss if happens
 - Restaurant web site: much less likely and small loss

Preventing Computer Viruses

- **Viruses spreads when infected files are accessed**
 - Macro viruses attach themselves to other programs (documents) and spread when the programs are executed (the files are opened)
 - **Worms**
 - Special type of virus that spread itself without human intervention (sends copies of itself from computer to computer)
 - **Anti-virus software packages check disks and files to ensure that they are virus-free**
 - **Incoming e-mail messages are most common source of viruses**
 - Check attachments to e-mails, use filtering programs to 'clean' incoming e-mail

- ▶ ເວັນຍໍອມມີການໃຫ້ Reduce ⇒ ການໃຫ້ລົງຄາມ ລດວົງ / ການໃຫ້ລົງຄາມ
ຢູ່ Network Security

Types of controls & 3 types

1. Preventative controls → การควบคุมเชิงป้องกัน → กันตัวไว้ในสิ่งที่ดี
 - เป็นการควบคุมแบบป้องกันขั้นต้น เช่น เก็บรหัสผ่านที่เข้มงวด Ex. การตั้ง password, การ backup ข้อมูล
 - ดำเนินการเพื่อให้เครื่องมือที่ดูดซึมน้ำมัน เช่น เครื่องซักผ้า
 2. Detective controls → ข้อมูลถูกหักหลัง → ไม่ได้ตั้งใจ
 - เป็นการเฝ้าระวังตัวอย่างต่อเนื่อง (เช่น การตรวจสอบ) → ตรวจสอบ log
 - บันทึกเหตุการณ์เพื่อใช้เป็นหลักฐาน
 3. corrective controls → ต้องรีบการรับมือในเมื่อทุกสิ่งที่ผิดพลาด
 - เผื่องเผื่องไว้ในชุด เครื่องคอมพิวเตอร์ / เก็บรักษาแบบมีประสิทธิภาพ

→ ກລື້ກາກຮະບວນກອງກົງໆ
ຜົບລາຍງົດ

⇒ ກ່ຽວຂ້ອງ ວິຍາຄຸກຄາມ (Threats)

កស់បានការនិងការប៉ែងក្នុង

→ กลุ่ม viruses เราก็จะรู้ว่าก็กลุ่ม viruses ก่อนแล้วก็ในรูปแบบนี้

Intrusion Prevention



- **Types of intruders**
 - **Casual intruders** กู้จูนๆ หรือตั้งการเจาะบานฯ ก็ได้ก็ตาม
 - With Limited knowledge ("trying doorknobs")
 - Script kiddies: Novice attackers using hacking tools
 - **Security experts (hackers)** เริ่มมีเป้าหมายในทางด้านต่อไปนี้
 - Motivation: the thrill of the hunt; show off
 - Crackers: hackers who cause damage
 - **Professional hackers (espionage, fraud, etc.)** - สำหรับองค์กร
 - Breaking into computers for specific purposes
 - **Organization employees** เช่นพนักงานที่แอบดูข้อมูล
 - With legitimate access to the network
 - Gain access to information not authorized to use
- หมายเหตุที่สำคัญ โน๊ตที่ ก.๒: ใช้ทักษะใดๆ

* VAT *

Preventing Intrusion

- Requires a **proactive** approach that includes routinely testing the security systems
- **Best rule for high security**
 - Do not keep extremely sensitive data online
 - Store them in computers isolated from the network
- **Security Policy**
 - Critical to controlling risk due to access
 - Should define clearly
 - Important assets to be safeguarded and Controls needed
 - What employees should do
 - Plan for routinely training employees and testing security controls in place

Securing Network Perimeter

- **Basic access points into a network**
 - LANs inside the organization
 - Dial-up access through a modem
 - Internet (most attacks come in this way)
- **Basic elements in preventing access**
 - Physical Security
 - Dial-in security
 - Firewalls
 - Network Address Translation (NAT) Proxy servers

Network Design : LAN, WLAN , VPN

Intrusion Prevention

↳ กรณีบุกดูถูก, การคุ้มครอง

- ① **Casual intruders** ก.๑ กู้จูนๆ ไม่ต้องมีฝีมือ เช่นเด็ก หัวใจดีๆ แต่ร้าย หรือคนต่างด้วยในเรื่องอาชญากรรมต่อสังคม แต่ฝีมือดีๆ ไม่ต้องมีความต้องการจะทำร้าย ผู้คน หรือสิ่งของ ที่มีค่า เช่น "Crackers" พยายามเข้ามาตั้งไฟล์ไว้ในระบบ Data ของทาง ผู้ผลิต หรือรักษาดูแล เช่น Security experts : จะใช้เก็บเครื่องไฟฟ้า เนื่องจากมีความต้องการ
- ② **Security experts** : Hacker เนื่องจากมีความรู้ทางด้านคอมพิวเตอร์ ฝีมือดีๆ ที่ต้องการจะทำร้าย ผู้ผลิต หรือรักษาดูแล เช่น "Crackers" พยายามเข้ามาตั้งไฟล์ไว้ในระบบ Data ของทาง ผู้ผลิต หรือรักษาดูแล เช่น Security experts : จะใช้เก็บเครื่องไฟฟ้า เนื่องจากมีความต้องการ
- ③ **Professional Hackers** : Hackers ที่มี Pro ทักษะเชิงอาชีพ / หลักภัยเพื่อชีวิตรักษาความปลอดภัย สำหรับองค์กร เช่น อาชญากรรมทางไซเบอร์
- ④ **Organization employees** ที่อยู่ในภายในองค์กร ที่มีอำนาจตัดสินใจในองค์กร เช่น พนักงานที่แอบดูข้อมูล

กรณีบุกดูถูก จุดย่างเอาจริงๆ ไม่สามารถป้องกันได้
ต้องยกเว้น เทคนิค level กรณีบุกดูถูกที่เล็กๆ น้อยๆ

Securing Network Perimeter

- ↑
กรณีบุกดูถูก NW หนึ่งปีแล้ว
- เป็นรูปแบบที่ใหญ่ๆ ของ NW Design
- โครงสร้างที่ต้องมีตัวกลาง เช่น (use Access Point)
use Firewall

Authenticating Users

⇒ ຖາຍຕົວຈຳສຸດສັບສົກ

- Done to ensure that only the authorized users are permitted into network
 - and into the specific resources inside the network
- Basis of user authentication
 - User profile
 - User accounts based on something you have, know or are
 - Smart card, time based token is something you have
 - Password is something you know
 - Biometric is something you are
 - Network authentication