ปรนัย 70 ข้อ

1. ความมั่นคงสารสนเทศเบื้องต้น (Introduction

Information System (IS) คือ กลุ่มขององค์ประกอบสารสนเทศ

ความเป็นมาของ ความมั่นคงสารสนเทศ "History of Information Security"

- การรักษาความปลอดภัยด้านกายภาพ (Physical Security)
  - ข้อมูลบันทึกบนวัตถุที่จับต้องได้ → สร้างที่เอาไว้เก็บข้อมูลให้ปลอดภัย
- การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)
  - ป้องกันข้อมูลถูกขโมยระหว่างส่ง (เข้ารหัสข้อมูล)
  - จูเลียส ซีซาร์ เป็นคนคิดค้น
  - เยอรมันเคยใช้ Enigma เข้ารหัสข้อมูลทางการทหาร
  - โซเวียดเคยใช้ One Time Pad เข้ารหัสข้อมูล
- การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)
  - อุปกรณ์เข้า/ถอดรหัส และสายโทรศัพท์ มีการแผ่รังสี ทำให้ข้อมูลที่ยังไม่เข้ารหัสถูกดักจับได้ แก้โดยการกำหนดมาตรฐาน TEMPEST
- การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)
  - ปี 1970 David d Elliott Bell และ Leonard J. La Padula จัดลำดับความปลอดภัย 4 ชั้น ได้แก่
    - ไม่จำกัดระดับ
    - ลับ
    - ลับมาก
    - ลับที่สุด
  - ระดับสิทธิ์มี 4 ระดับ (*ระดับชั้นต่ำกว่าความลับจะไม่สามารถเข้าถึงไฟล์นั้นได้)
    - ไม่จำกัดระดับ
    - ลับ
    - ลับมาก
    - ลับที่สุด
  - ถูกนำไปใช้ในกระทรวงกะลาโหมอเมริกา เรียกว่า TCSEC (52000.28) หรือ Orange Book
- การรักษาความปลอดภัยเครือข่าย (Network Security)
  - ใช้มาตรฐาน TNI ของ ITSEC เรียกว่า Red Book
  - ไม่นิยมใช้เชิงพาณิชย์ เพราะซับซ้อนและใช้เวลานาน
- การรักษาความปลอดภัยของข้อมูล (Information Security)
  - เป็นการรวมกันของหัวข้อทั้งหมดที่กล่าวมา
  - รักษาคุณสมบัติ 3 ด้าน (CIA)
    - ความลับ Confidentiality (C)
    - ความถูกต้อง Integrity (I)
    - ความพร้อมใช้งาน Availability (A)
- การรักษาความปลอดภัยไซเบอร์ (Cybersecurity)
  - วิธีการที่จะทำให้องค์กรไร่ม่เกิดความเสี่ยง หรือความเสียหาย
- สงครามไซเบอร์ (Cyber Warfare)
  - นำเทคโนโลยีมาใช้ทางการทหาร
  - ใช้เครือข่ายเป็นศูนย์กลาง
  - ป้องกันการโจมตี ตลอดจนตอบโต้กลับ

What is Seculity

สภาวะที่ปราศจากอันตราย

- ระดับการรักษาความปลอดภัยในองค์กร (6 ระดับ)
  - Physical security - Personal security
  - Operations security -Communications security
  - Network security - Information security

Information Security

มาตรการป้องกัน และรักษาระบบสารสนเทศให้รอดจากอันตราย

- เครื่องมือที่นำมาใช้ (5 ข้อ)
  - นโยบาย (Policy) - การตระหนัก (Awareness)
  - การฝึกอบรม (Training) - การศึกษา (Education)
  - Technology

note

การใช้ Security จะต้องแลกกับ Performance ลดลง และเสียตังเยอะขึ้น

- เป้าหมายของ Information Security คือ รักษาคุณสมบัติของ CIA
  - ความลับ Confidentiality (C)
  - ความถูกต้อง Integrity (I) (2 ข้อ)
    - Data Integrity ข้อมูลถูกต้อง
    - System Integrity ระบบถูกต้อง
  - ความพร้อมใช้งาน Availability (A)
    - ข้อมูลหรือบริการอยู่ในรูปแบบที่ใช้งานได้
    - มีความเพียงพอต่อความต้องการ
    - ให้บริการรวดเร็ว เหมาะสม
    - Bounded waiting time และ timely response
    - Fault tolerance
    - Controlled concurrency
  - CIA+ (เพิ่ม 4 ด้านจากของเดิม)
    - Access Control
      - Identification
      - Authentication
      - Authorization
    - Accountability ตรวจสอบได้ มีการเก็บไฟล์ประวัติ
    - Non-Repudiation ห้ามปฏิเสธความรับผิดชอบ
    - Privacy การบริหารความเสี่ยง

Element of Security Architecture (5 ข้อ)

- Identify
  - Authentication
  - Authorization
- Integrity
- Confidentiality
- Availability
- Audit

Classification of Security Threats (3 ข้อ)

- Disclosure (การเปิดเผย) / Interception การยึดครองโดยผู้ไม่มีสิทธิ์ เป็นการโจมตีคุณสมบัติข้อมูลด้านความลับ (C)
- Modification (การแก้ไข) / Fabrication การปลอมแปลง เป็นการโจมตีคุณสมบัติข้อมูลด้านความถูกต้อง (I)
- Denial of Service (การปฏิเสธการให้บริการ) Interruption การขัดจังหวะ เป็นการโจมตีคุณสมบัติข้อมูลด้านความพร้อมใช้งาน (A)

รูปแบบการโจมตี

- Passive Attacks : เป็นการโจมตี ความลับ (C) เป็นหลัก
  - การเข้าถึงข้อมูลโดยที่ไม่มีสิทธิ์
  - การใช้ Sniffer ดักจับข้อมูล
- Active Attacks : เป็นการโจมตี (A) และ (I) เป็นหลัก
  - Masqueade : การปลอมตัว (โจมตี Authenticity)
  - Replay : การทำซ้ำ (โจมตี I)
  - Modification : การแก้ไข เปลี่ยนแปลงข้อมูล (โจมตี I)
  - Denial of Service : การโจมตีให้ระบบล่ม (โจมตี A)

มาตรการควบคุมความปลอดภัย

- การเข้ารหัส (Encryption)
- การควบคุมฮาร์ดแวร์ (Hardware Controls)
- การควบคุมซอฟต์แวร์ (software Controls)
- นโยบายความปลอดภัย (Security Policies)
- การควบคุมทางกายภาพ (Physical Controls

รูปแบบการโจมตีในปัจจุบัน

- **การส่อดแนม (Sniffing)** หรือ Snooping หรือ Eavesdropping
  - เป็นการโจมตีแบบ Passive
  - เช่น Wiretapping, Packet Sniffer
- **การแก้ไขข้อมูล (Modification)**
  - เข้าไปแก้ข้อมูลแบบไม่ได้รับอนุญาติ เป็นการโจมตีแบบ Active
  - เช่น Man-in-the-middle attack
- **การปลอมตัว (Spoofing)**
  - เป็นได้ทั้ง Passive และ Active
  - เช่น Masquerading, IP Spoofing
- **การปฏิเสธการให้บริการ (DoS)**
  - ขัดขว้างไม่ให้เข้าถึงข้อมูล โดยการพยายามใช้ทรัพยากรในเครื่องแบบเกินขีดความสามารถของเครื่อง (โจมตี A)
  - โจมตีที่เครื่องเซิร์ฟเวอร์
- **การปฏิเสธแหล่งที่มา (Repudiation of Origin)**
  - การไม่ยอมรับข้อมูลที่ส่งหรือสร้างแล้วไปให้ผู้รับ
  - ป้องกันโดยรักษา I
- **การปฏิเสธการได้รับ (Repudiation of Receipt)**
  - รับข้อมูลแล้วบอกว่าไม่ได้รับ
  - ป้องกันโดยรักษา A และ I
- **การหน่วงเวลา (Delay)**
  - ยับยั้งให้ส่งข้อมูลช้ากว่าที่จะเป็น
  - ป้องกันได้โดยการรักษา A
- **วิศวกรรมสังคม (Social Engineering)**
  - ใช้จิตวิทยาหลอกถามข้อมูลที่สำคัญ หรือหลอกให้ส่งข้อมูล
  - การป้องกันทำได้โดยการใช้นโยบายควบคุม และอบรมให้ความรู้
- **การถอดรหัสข้อมูล (Cyptanalysis)**
- **การโจมตีแบบคนกลาง (Man-in-the-middle attack)**
  - บุคคลที่ 3 แอบส่อดแนมระหว่างผู้รับผู้ส่งโดยที่ไม่มีใครรู้ตัว
- **การเจาะระบบ (Hacking)** การเข้าสู่ระบบคอมฯโดยอาศัยช่องโหว่

แนวโน้มภัยคุมคาม

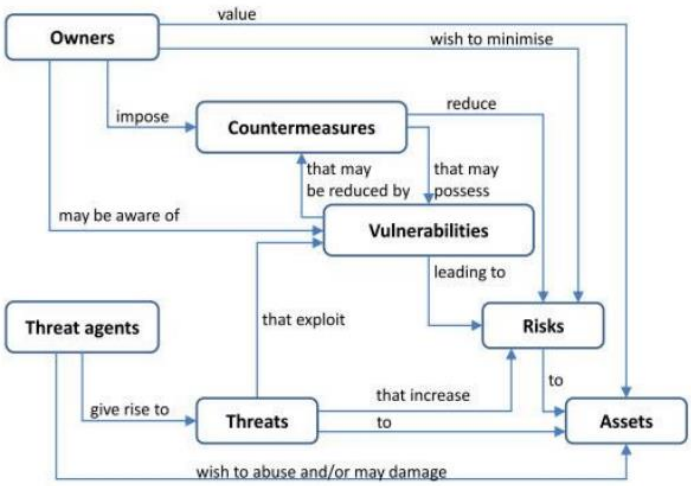
- **มัลแวร์ (Malware)** หรือ Malicious Code คือ โปรแกรมประสงค์ร้ายที่ออกแบบมาให้เจาะหรือทำลายระบบ เช่น Virus, Worm, Trojan Horse
- **บอตเน็ต (Botnet)**
  - การแฮกเข้าระบบคอมฯ
  - เครื่องที่ถูกยึดครองจะเรียกว่า Bot, Zombie หรือ Drones
  - หาถูกยึดหลายเครื่องจะเรียกว่า Botnet หรือ roBotNETwork
- **Advanced Persistent Threat (APT)** เป็นอาชญากรรมทางคอมฯ เน้นโจมตีองค์กรที่สำคัญ ถูกสนับสนุนโดยรัฐบาล
- **ฟิชชิง (Phishing)** เป็นการโจมตีแบบวิศกรรสังคม ใช้เหยื่อมาล่อ เพื่อหลอกเอาข้อมูลที่สำคัญ
- **แฮกเกอร์ (Hacker)** ผู้เชียวชาญด้านคอมฯ หาประโยชน์โดยใช้ช่องโหว่ของคอมฯ
- **อาชญากรรมคอมพิวเตอร์ (Cybercrime)** มักโจมตีผู้ใช้ที่มีบัตรเครดิต โดยใช้ SSLStrip เจาะรหัสแบบ SSL
- **สงครามไซเบอร์ (Cyberwar)**
- Cloud and BYOD (Bring Your Own Device)

2. การบริหารความเสี่ยง (Risk Management)

การวิเคราะห์ความเสี่ยง (Risk Analysis)

- **ความเสี่ยง (Risk) คือ การกระทำที่จะทำให้เกิดความเสียหาย**
- **ปัจจัยเสี่ยง (Risk Factor) คือ ต้นเหตุของความเสี่ยง** (2 ข้อ)
  - **ภัยคุกคาม (Threat)**
  - **ช่องโหว่ (Vulnerability)**
- ปัจจัยที่ใช้การประเมินความเสี่ยง (2 ข้อ)
  - **โอกาสที่จะเกิด** (Likelihood)
  - **ผลกระทบ** (Impact) หากเกิด **เหตุความเสี่ยง** (Risk Event)

ความสัมพันธ์ขององค์ประกอบความเสี่ยงตามมาตรฐาน



การบริหารความเสี่ยง

เป็นกระบวนการที่จะโอกาสที่จะเกิดความเสี่ยง และลดผลกระทบ หรือลดความเสียหายที่เกิดให้อยู่ใน ระดับที่ยอมรับได้

ขั้นตอนการบริหารความเสี่ยง

- การระบุปัจจัยความเสี่ยง (Risk Factor Identification)
- ประเมินโอกาสที่จะเกิด และผลกระทบ (Likelihood and Impact)
- จัดลำดับความเสี่ยง (Risk Ordered) ได้ผลลัพธ์ก็คือ **ระดับความเสี่ยง (Risk Level)**

การรักษาความเสี่ยง (4 แนวทาง)

- **การยอมรับความเสี่ยง** (Risk Acceptance) กรณีที่ไม่คุ้มหากควบคุมความเสี่ยง
- **การลด / การควบคุมความเสี่ยง** (Risk Mitigation) ปรับปรุงระบบการทำงาน
- **การโอนความเสี่ยง** (Risk Transfer) โยนความเสี่ยงให้คนอื่นรับผิดชอบแทน
- **การหลีกเลี่ยงความเสี่ยง** (Risk Avoidance) ไม่อนุมัติโครงการที่ดูมีความเสี่ยง

มาตรการควบคุม (Control)

แนวทางปฏิบัติเพื่อลดความเสี่ยง (4 ประเภท)

- การควบคุมเพื่อป้องกัน (Preventive Control) ควบคุมไม่ให้เกิดความเสี่ยงตั้งแต่แรก
- การควบคุมเพื่อให้ตรวจพบ (Detective Control) การวิเคราะห์ หรือตรวจสอบหาข้อผิดพลาด
- การควบคุมฌโดยชี้แนะ (Directive Control) การควบคุมเพื่อกระตุ้นให้เกิดความสำเร็จตามเป้าหมาย
- การควบคุมเพื่อแก้ไข (Collective Control) ควบคุมเพื่อแก้ไขข้อผิดพลาด เช่น การจัดเตรียมเครื่องดับเพลิง

มาตรฐานบริหารความเสี่ยง

- ISO 31000:2009 Risk Management – Principles and guidelines (การบริหารจัดการความเสี่ยงภาพรวมขององค์กร)
- ISO/IEC 27005 Information technology – Security techniques –Information security risk management (ปรับปรุงจากมาตรฐานแบบแรก เพิ่มการบริหารความเสี่ยงด้านการรักษาความปลอดภัยข้อมูล)
- NIST SP 800-30rev1 Guide for Conducting Risk Management (เน้นการบริหารจัดการความเสี่ยงด้านการรักษาความปลอดภัยข้อมูล)
- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) โดย SEI (Software Engineering Institute) (เน้นการบริหารจัดการคนและกระบวนการ)

การประเมินความเสี่ยง (Risk Assessment)

ผลลัพธ์ที่ได้จากการประเมินความเสี่ยง คือ ข้อแนะนำเกี่ยวกับวิธีการป้องกันความเสี่ยง

- ต้องปกป้องทรัพย์สินอะไรบ้าง และมูลค่าเท่าไหร่
- อะไรคือภัยคุกคามต่อองค์การณ์
- เรามีช่องโหว่อะไร
- เมื่อโดนโจมตีเราจะเสียหายมากน้อยแค่ไหน
- แก้ไขช่องโหว่ได้อย่างไร

รูปแบบการประเมินความเสี่ยง

- การประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Management) ใช้ตัวเลขกำหนด ผลกระทบและโอกาสที่จะเกิด มักใช้กับธุรกิจที่เกี่ยวข้องกับการเงิน แหล่งข้อมูล คือ ใช้ข้อมูลตัวเลขทางสถิติ
- การประเมนิความเสี่ยงเชิงคุณภาพ (Qualitative Risk Management) แบ่งระดับผลกระทบ และโอกาสที่จะเกิดเป็นระดับ สูง ปานกลาง ต่ำ อาจใช้ 5 หรือ 7 ระดับ
- การประเมินความเสี่ยงเชิงกึ่งปริมาณ (Semiquantitative Risk Management Method) เป็นวิธีที่ใช้ทั้งคำ อธิบายระดับวามเสี่ยงควบคู่กบัการใช้ค่าความเสี่ยงเป็นตัวเลข เหมาะสำ หรับกรณีที่ไม่สามารถหาระดับวามเสี่ยงเชิงปริมาณได้

ขั้นตอนการประเมินความเสี่ยง

1. การระบุทรัพย์สิน (Asset Identification)
2. การระบุภัยคุกคาม (Threat Identification)
3. การระบุช่องโหว่(Vulnerability Identification)
4. การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)
5. การประเมินผลกระทบ (Impact)
6. การประเมินความเสี่ยง (Risk) (3 ระดับ)

- System-Level Vulnerability Assessment เพื่อหาจุดอ่อนหรือช่องโหว่ของระบบคอมพิวเตอร์แต่ละเครื่องในองค์กรและตรวจสอบระบบว่ามีการควบคุมตามนโยบายความปลอดภัย หรือไม่
- Network-Level Vulnerability Assessment เป็นการประเมินระบบคอมพิวเตอร์และเครือข่ายทั้งองค์กร อาจมี การทดสอบการเจาะระบบ
- Organization-Level Vulnerability Assessment เป็นการวิเคราะห์และประเมนิความเสี่ยงของทั้งองค์กรโดยรวม เพื่อระบุภัยคุกคามข้อมูลและระบบสารสนเทศ

การระบุทรัพย์สิน (Asset Identification) (ทรัพย์สิน 5 ประเภท)

- ฮาร์ดแวร์ (Hardware)
- ซอฟต์แวร์ (Software)
- ข้อมูล (Information)
- บริการ (Service)
- บุคลากร (People)

การประเมินมูลค่าทรัพย์สิน (Asset Value Evaluation) (เกณฑ์ 5 ข้อ)

- ความลับ (Confidentiality)
- ความถูกต้อง (Integrity)
- ความพร้อมใช้งาน (Availability)

การระบุภัยคุกคาม (Threat Identification) (ประกอบด้วย 3 ส่วน)

- เป้าหมาย (Target) ได้แก่
  - ความลับ (Confidentiality)
  - ความถูกต้อง (Integrity)
  - ความพร้อมใช้งาน (Availability)
- ผู้โจมตี (Threat Agent) มีคุณสมบัติ ดังนี้
  - การเข้าถึง (Access), ความรู้ (Knowledge), แรงจูงใจ (Motivation)
  - อาจจะเป็น พนักงาน (ผู้บริหาร,เจ้าหน้าที่) , พนกังานเก่า, แฮคเกอร์, ศัตรูหรือคู่แข่ง รวมถึง ลูกค้า, ผู้มาเยี่ยม หรือภัยธรรมชาติด้วย

การระบุช่องโหว่ (Vulnerability Identification) (มี 4 ประเภท)

- ช่องโหว่ในระดับนโยบาย คือ ช่องโหว่ที่เกิดจากการบริหารจัดการ
- ช่องโหว่เกี่ยวกับคน คือ ช่องโหว่ที่เกิดจากการปฏิบัติหน้าที่ของพนักงานหรือผู้รับจ้าง
- ช่องโหว่ทางเทคนิค เป็นช่องโหว่ที่เกิดจากข้อผิดพลาดของการเขียนโปรแกรม
- ช่องโหว่ทางกายภาพ เป็นช่องโหว่ที่เกิดจากการป้องกัน และรักษาความปลอดภัยทางกายภาพ

การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)

แบ่งเป็น 2 แบบ คือ แบบเชิงปริมาณ และ แบบเชิงคุณภาพ

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก (Very High)	5	มีโอกาสเกิดเกือบจะแน่นอน
สูง (High)	4	มีโอกาสเกิดสูง
ปานกลาง (Moderate)	3	มีโอกาสที่จะเกิดปานกลาง
ต่ำ (Low)	2	มีโอกาสที่จะเกิดน้อย
ต่ำมาก (Very Low)	1	แทบจะไม่มีโอกาสที่จะเกิด

การประเมินผลกระทบ (Impact)

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก (Very High)	5	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงมากหลายด้าน หรือสร้างความหายนะต่อธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ
สูง (High)	4	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงมาก หรือสร้างความหายนะต่อธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ
ปานกลาง (Moderate)	3	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงต่อธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ
ต่ำ (Low)	2	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายบางส่วนต่อธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ
ต่ำมาก (Very Low)	1	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายน้อยมาก จนสามารถละเลยได้ต่อธุรกิจขององค์กร ทรัพย์สิน พนักงาน องค์กรอื่น หรือประเทศชาติ

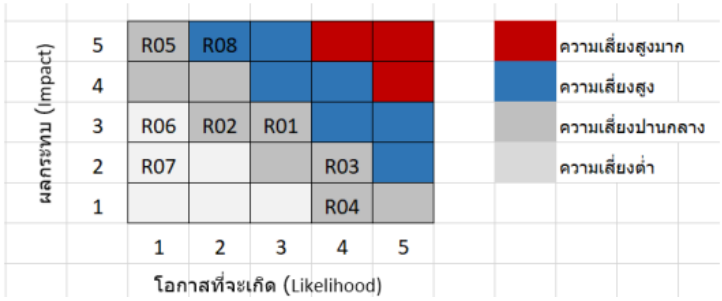
การคำนวณความเสี่ยง (Risk Determination)

ระดับความเสี่ยง = มูลค่าทรัพย์สิน x โอกาสที่จะเกิดขึ้น x ผลกระทบที่ตามมา

- ถ้าเป็นการประเมินเชิงปริมาณ จะได้ตัวเลขที่แสดงเป็นจำนวนเงินที่นะสูญเสียจากเหตุการณ์ดังกล่าว
- ถ้าเป็นการประเมินเชิงคุณภาพ ก็จะระบุถึงระดับความเสี่ยงที่มี

- ผลที่ได้จากการประเมินความเสี่ยงคือ ระดับความเสี่ยงขององค์กร

เกณฑ์การพิจารณาระดับความเสี่ยง



การรักษาความเสี่ยง (Risk Treatment)

ดูระดับความเสี่ยงขององค์กรอยู่ในระดับยอมรับได้หรือไม่ถ้าไม่ได้ต้องมีการควบคุมหรือจัดการความเสี่ยง มี 4 แนวทางคือ

- **การลดความเสี่ยง** (Risk Reduction) ตามมาตรฐานนี้มี 127 มาตรการให้เลือกใช้
- **การยอมรับความเสี่ยง** (Risk Acceptance) ใช้ในกรณีที่แก้แล้วไม่คุ้ม
- **การหลีกเลี่ยงความเสี่ยง** (Risk Avoidance) ยกเลิกกระบวนการที่ทำให้เกิดความเสี่ยง
- **การย้ายโอนความเสี่ยง** (Risk Transfer) โยนให้คนอื่นรับผิดชอบแทน เช่น การทำประกัน

มาตรการที่ใช้แก้ไขการควบคุมความเสี่ยงอาจแบ่งเป็น 3 ประเภท

- **มาตรการควบคุมทางกายภาพ** จัดสภาพแวดล้อมให้เหมาะสม
- **มาตรการควบคุมทางด้านเทคนิค** การใช้ซอฟต์แวร์ หรือฮาร์ดแวร์มาช่วยควบคุม จัดการ ด้านความปลอดภัย
- **มาตรการควบคุมด้านธุรการ** การจัดให้มีนโยบาย ระเบียบ วิธีการปฏิบัติงาน การฝึกอบรมเกี่ยวกับความปลอดภัยที่เหมาะสม สำหรับบุคลากรขององค์กร

3. การควบคุมการเข้าถึง (Access Control)

เป็นขั้นตอน การควบคุมผู้ที่ได้รับบอนุญาติในการเข้าถึง แก้ไข หรือใช้งานข้อมูล เพื่อให้ระบบมีความปลอดภัย มี 4 ขั้นตอน

- **การระบุตัวตน (Identification)** การเก็บบัญชีผู้ใช้มี 2 แนวทาง
  - เก็บไว้ในฐานข้อมูลย่อย (**ปัญหาคือการบริหารจัดการยาก)
  - เก็บไว้ในฐานข้อมูลกลาง
- **การพิสูจน์ตัวจริง (Authentication)** การตรวจสอบว่าใช้ตัวจริง หลักฐานยืนยันมี 3 ประเภท
  - **สิ่งที่คุณรู้ (What you know)** ข้อมูลหรือรหัสผ่านที่ต้องจำ
  - **สิ่งที่คุณมี (What you have)** ข้อมูลที่อ่านได้จากสิ่งของ เช่น การ์ด บัตร เป็นต้น
  - **สิ่งที่คุณเป็น (What you are) / ไบโอเมตริกส์ (iometric)** ข้อมูลหรือรหัสที่อ่านได้จากอวัยวะบางส่วนของร่างกาย
  - Password นิยมที่สุด มี 2 แบบ
    - OTP
    - PIN
  - Token หรือ Authenticator เป็นฮาร์ดแวร์พิเศษที่ใช้สร้างรหัสผ่าน ณ เวลาใช้งาน และจะมีการเปลี่ยนใหม่ทุกครั้งที่มีการเริ่มใหม่ มี 2 วิธี
    - Synchronous Authentication มี 2 แบบ
      - แบบขึ้นอยู่กับ เหตุการณ์ (Event) เมื่อต้องการเข้าสู่ระบบ ผู้ใช้กด Token เพื่อให้ Token สร้างรหัสผ่านให้แล้วนำรหัสผ่านนั้น มาใส่ฟอร์มล็อกอิน
      - แบบขึ้นอยู่กับ เวลา (Time) รหัสผ่านจะสร้างขึ้นตามช่วงเวลา (ปกติสร้างทุก ๆ 1 นาที) ผู้ใช้นำรหัส ที่ถูกสร้างมาใช้โดยระบุรหัสผ่าน และเวลาที่ถูกสร้าง เพื่อพิสูจน์ทราบ
    - Asynchronous Authentication หรือ Challenge response ผู้ใช้ต้องการเข้าสู่ระบบจะทำการร้องขอไปยังเซิร์ฟเวอร์เครื่องเซิร์ฟเวอร์จะส่ง Challenge String กลับมาเพื่อใส่ลงในโทเคนที่ผู้ใช้ถืออยู่โทเคนจะคำนวณเป็นรหัสผ่าน หลังจากนั้นผู้ใช้นำ รหัสผ่านไปใส่บนฟอร์มเพื่อเข้าสู่ระบบ
  - Biometric อาจเกิดข้อผิดพลาดได้ มี 3 แบบ
    - FRR
    - FAR
    - CER
  - Digital Signature การเข้ารหัสแบบกุญแจคู่ (Public Key) มีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบ กุญแจเดียว (Secret Key) การเข้ารหัสกุญแจคู่ต้องใช้ 2 กุญแจ ได้แก่
    - กุญแจสาธารณะ (Public Key)
    - กุญแจส่วนตัว (Private Key)
- **การอนุญาต** (Authorization) มี 3 แนวทาง
  - การอนุญาตเป็นรายๆ
  - การอนุญาตเป็นกลุ่ม
  - การอนุญาตเข้าใช้หลายๆ ระบบ หรือ SSO
- **การตรวจสอบได้** (Accountability)
  - เก็บหลักฐานเพื่อใช้ตรวจสอบ หรือ Log เมื่อเกิดปัญหา
    - ระบบ Windows **จะบันทึกไว้ที่** Event Log
    - ระบบ Linux **จะบันทึกไว้ในไฟล์** /var/log/message

กระบวนการเข้ารหัสแบบกุญแจคู่

- ผู้ใช้สร้างคู่รหัสกุญแจของตัวเอง เพื่อใช้ เข้า-ถอด รหัส
- เก็บกุญแจส่วนตัวไว้ แล้วส่งกุญแจสาธารณะออกไป
- ผู้ส่งนำกุญแจสาธารณะของผู้รับมาเข้ารหัส แล้วส่งข้อมูลออกไป
- เมื่อผู้รับได้รับข้อมูล จะใช้กุญแจส่วนตัวถอดรหัสออกมา

ระบบของลายมือชื่อดิจิทัล มี 4 ขั้นตอน

- นำข้อความส่งเข้า hash Function ได้เป็น Message Digest
- นำ Message Digest เข้ารหัสกุญแจส่วนตัว ได้ Digital Signature
- ส่ง ข้อความ กับ Signature ไปให้ผู้รับ
- ผู้รับตรวจสอบโดยการนำ ข้อความ มาคำนวณหา Message Digest และ Digital Signature ที่ส่งมาพร้อมข้อความ ถ้าได้ Message Digest เท่ากัน แสดงว่าข้อความถูกต้องเป็นอันเดียวกับของต้นฉบับ

X.509

มาตรฐานกำหนดรูปแบบการให้บริการการพิสูจน์ตัวตน มีจุดประสงค์เพื่อ

- ทำการล็อกออนครั้งเดียวหรือ SSO
- โครงสร้างสำหรับบริหารสิทธิหรือ PMI

- มาตรฐาน X.509 ประกอบด้วย
  - โครงสร้างกุญแจสาธารณะ (PKI)
  - การยกเลิกคีย์ (CRP)
  - การกำหนดคุณสมบัติใบรับรอง (AC)
  - อัลกอริทึมที่ใช้ตรวจสอบการรับรอง

ใบรับรองดิจิทัล (Certificate)

ฟิลด์	คำอธิบาย
Version	เวอร์ชันของ X.509 ซึ่งปัจจุบันคือเวอร์ชัน 3 (v3)
Serial Number	หมายเลขเฉพาะที่ CA กำหนดให้กับใบรับรองใบนี้
Algorithm ID	อัลกอริทึมที่ใช้สำหรับการลงลายมือชื่อดิจิทัลของใบรับรองนี้
Issuer	ชื่อของ CA ที่ออกใบรับรอง ซึ่งจะอยู่ในรูปแบบ DN (Distinguished Name)
Validity	ช่วงเวลาที่ใช้งานได้โดยอาจกำหนดเป็น หลังจากวันที่ หรือ ไม่เกินวันที่
Subject	ชื่อเจ้าของใบรับรองดิจิทัลนี้ ซึ่งอยู่ในรูปแบบ DN หรือ อีเมล หรือ DNS
Subject Public Key	ข้อมูลเกี่ยวกับกุญแจสาธารณะของเจ้าของใบรับรองดิจิทัล ซึ่งประกอบด้วย - อัลกอริทึมของกุญแจสาธารณะ เช่น RSA, Diffie-Hellman - กุญแจสาธารณะ
Issuer Unique Identification (Optional)	หมายเลขของผู้ออกใบรับรองดิจิทัล หรือ CA (Certificate Authority)
Subject Unique Identification (Optional)	หมายเลขประจำตัวของเจ้าของใบรับรองนี้
Extensions (Optional)	ข้อมูลอื่น ๆ เพิ่มเติม

4. วิทยาการเข้ารหัสลับ (Cryptography)

เป็นที่วิชาที่มีไว้เพื่อ

- การปกปิดบริบท (content) ของบางข้อความ
- การสอบทวน (verify) ความถูกต้องของข้อความโดยผู้รับ

จุดประสงค์ที่เอามาใช้ในคอมฯ เพื่อ?

- ความลับหรือภาวะส่วนตัว (Confidentiality)
- บูรณภาพข้อมูล (Data Integrity)
- การพิสูจน์ตัวจริง (Authentication)
- การไม่ปฏิเสธการกระทำ (Non-Repudiation)

การเข้ารหัสลับ (Encryption)

- เป็นวิธีการรักษาความลับข้อมูลที่ดีที่สุด เป็นกระบวนการที่จะแปลง Plaintext or Cleartext ไปเป็น ข้อความลับ (Ciphertext) ใช้ Decryption เป็นกระบวนการในการถอดรหัส กลับ การเข้ารหัสมี 2 แบบ
- การเขารหัสมี 2 แบบ
  - กุญแจลับ (Secret-Key Cryptography) หรือ Symmetric Encryption เช่น DES, 3DES, IDEA, Skipjack, Blowfish และ AES เป็นต้น
    - ข้อดีคือ ทำงานได้รวดเร็วและมีประสิทธิภาพสูง
    - ข้อจำกัด ขาดวิธีรักษาความปลอดภัยในการแลกเปลี่ยนกุญแจ
  - กุญแจสาธารณะ (Public-Key Cryptography)

ระบบรหัสแบบสมมาตร (Symmetric-key Cryptography)

เป็นระบบรหัสที่ใช้กุญแจชุดเดียวกันทั้งผู้ส่งและผู้รับในการเข้าและถอดรหัสลับ

ซึ่งในที่นี้ก็คือตัวกุญแจนั่นเอง กุญแจซึ่งอยู่ในรูปรหัสคอมพิวเตอร์นี้เป็นตัวแปรสำคัญสำหรับการเข้าและถอดรหัสลับข้อมูล ซึ่งขนาดของกุญแจ (มีหน่วยเป็นบิต : bit) จะแสดงถึงระดับความปลอดภัยของข้อมูลที่ได้รับการเข้ารหัสลับ โดยการใช้กุญแจที่มีความยาวหรือจำนวนบิตสูง จะทำให้การเข้ารหัสลับข้อมูลนั้นมีความปลอดภัยมากยิ่งขึ้น

ระบบรหัสแบบอสมมาตร (Asymmetric-key Cryptography)

เป็นระบบรหัสที่ใช้ กุญแจคู่ (Key Pair) ซึ่งประกอบด้วย

- กุญแจส่วนตัว (Private Key)
- กุญแจสาธารณะ (Public Key)

- กุญแจส่วนตัวจะต้องเก็บรักษาไว้กับเจ้าของกุญแจ ส่วนกุญแจสาธารณะต้องมีการประกาศให้ผู้อื่นรับรู้หรือเก็บไว้ในที่ซึ่งบุคคลอื่นสามารถเข้ามาสืบค้นได้
- ในการเข้ารหัสลับข้อมูลจะต้องใช้กุญแจดอกหนึ่งในการเข้ารหัสลับและใช้กุญแจอีกดอกหนึ่งที่เป็นคู่กันในการถอดรหัสลับ

กรรมวิธีเปลี่ยนแปลงข้อความปกติ

ไซเฟอร์ (ciphers) คือ อัลกอริทึมที่ใช้ในการเปลี่ยนรูปแบบข้อความไปเป็นรหัสลับ โดยใช้วิธี การโยกย้ายตำแหน่ง (Transposition) และวิธีการแทนที่ (Substitution)

Stream Cipher

จะแปลงสัญลักษณ์ตัวหนึ่ง (หนึ่งบิตหรือหนึ่งไบต์) ของข้อความปกติในทันทีให้เป็นสัญลักษณ์ตัวหนึ่งของข้อความเข้ารหัส และมีกลไกสำหรับฟีดแบ็ค เพื่อให้คีย์เปลี่ยนไปเรื่อย ๆ

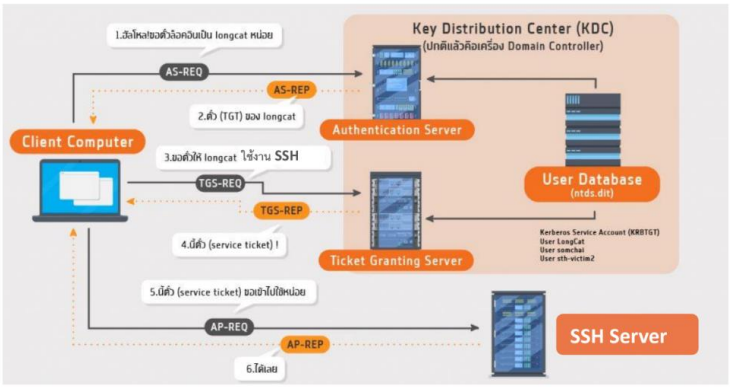
Block Cipher

ข้อความจะถูกแบ่งเป็นบล็อกขนาด n บิต (ปกติขนาดของบล็อกประมาณ 64-128 บิต), แต่ละบล็อกจะถูกเข้ารหัสและเปลี่ยนเป็น Ciphertext Block ที่มีขนาด n บิต

6. LAB Kerberos

- Kerberos เป็น โปโตคอล ตรวจสอบความถูกต้องของเครือข่ายที่ใช้การเข้ารหัสคีย์แบบสมมาตร
- ต้องมีการอนุญาตจากบุคคลที่ 3 เพื่อตรวจสอบความถูกต้องของ Server/Client
- พัฒนาโดย MIT จากโครงการ Athena

ขั้นตอนกระบวนการ



อัตนัย 1 ข้อ

5. DES

กำหนดอัลกอริทึมที่ใช้ในการแปลงข้อความปกติให้เป็นข้อความลับทีละบล็อกๆ บล็อกละ 64 บิต และใช้กุญแจขนาด 56 บิต เรียกว่า **การเข้ารหัส** สามารถแปลงข้อความกลับได้ด้วย เรียกว่า **การถอดรหัสลับ (ปัจจุบันเลิกใช้ไปแล้วจร้า)** แบ่งขั้นตอนออกเป็น 3 ส่วน

- นำข้อมูลมาแบ่งบล็อกข้อมูล แล้วนำเอาบล็อกข้อมูลมาผ่านการสลับบิตขั้นต้น (Initail Permutation)
- นำเข้าการทำฟังก์ชัน Round จำนวน 16 รอบ
  - แบ่งข้อมูลรอบรอบก่อนหน้าออกเป็น 32 บิต 2 ชุด เขียนแทนด้วย L และ R
  - ดึงค่าที่ได้เข้าสู่ฟังก์ชัน f และ xor โดยดึงคีย์ย่อยเข้ามา แทนด้วย K_i เขียนเป็นสมการได้ ดังนี้ (ให้ i แทน รอบที่)

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \text{ xor } f(R_{i-1}, K_1)$$

- นำค่า R_{16} และ L_{16} มาผ่านการสลับบิตย้อนกลับ (Reverse Initial Permutaion)