บทที่ 1
การรักษาความปลอดภัยข้อมูล

Kiadtipong Yord.
Information Technology

Physical Security

การรักษาความปลอดภัยทางกายภาพ

- ป้องกันสิ่งของที่จับต้องได้ มีคุณค่า เป็นความลับ ไม่ให้สูญหายหรือล่วงรู้
- การป้องกัน
  - กำแพง ป้อมปราการ กรงเหล็ก ตู้นิรภัย ห้องนิรภัย
  - ปกปิดเป็นความลับในคนที่ไว้ใจที่สุด
  - มีเวรยามป้องกัน สอดส่อง
  - ทำให้ความลับไม่เป็นความลับ
    - “ความลับที่รู้คนมากกว่าหนึ่งคนไม่ถือว่าเป็นความลับ” (ซุนวู)

Communication Security

การรักษาความปลอดภัยด้านการสื่อสาร

- ป้องกันการลักลอบอ่านข่าวสารระหว่างการส่งข่าวสาร
  - การซ่อนข่าวสาร
  - การเข้ารหัสข่าวสาร(Encryption)
    - Enigma -> เครื่องเข้ารหัสทางการทหารของเยอรมัน
    - ญี่ปุ่นใช้รหัสพิเศษแทนสถานที่ ในสงคราม
    - Navaho code talker -> สหรัฐใช้ภาษาชนเผ่าส่งข่าวสารผ่านวิทยุ
    - One time pad -> โซเวียตใช้ในการส่งรหัสข่าวสารของสายลับ

Emissions Security

การรักษาความปลอดภัยการแผ่รังสี

- การส่งข้อมูลด้วยไฟฟ้าผ่านสายทองแดงทำให้เกิดสนามแม่เหล็ก
- การจับสัญญาณจากคลื่นแม่เหล็ก
- Tempest -> มาตรฐานควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์ หรือลดการแผ่รังสี

Computer Security

การรักษาความปลอดภัยคอมพิวเตอร์

- ใช้ร่วมกับมาตรฐานการแผ่รังสี
- แนวคิดการจัดระดับความลับ 4 ระดับ [ไม่ลับ ลับ ลับมาก ลับที่สุด]
  - โดย เดวิด เบลล์ และ ลีโอนาร์ด ลา พาดูลา
  - ระดับสิทธิ์ในการเข้าถึงข้อมูลมี 4 ระดับเช่นกัน สิทธิ์ที่ผู้ใช้ระดับสูงกว่าเข้าถึงข่าวสารระดับต่ำลงมาได้
  - ใช้ในกระทรวงกลาโหมสหรัฐโดยชื่อว่า TCSEEC (Trusted Computing System Evaluation Criteria)

TCSEC

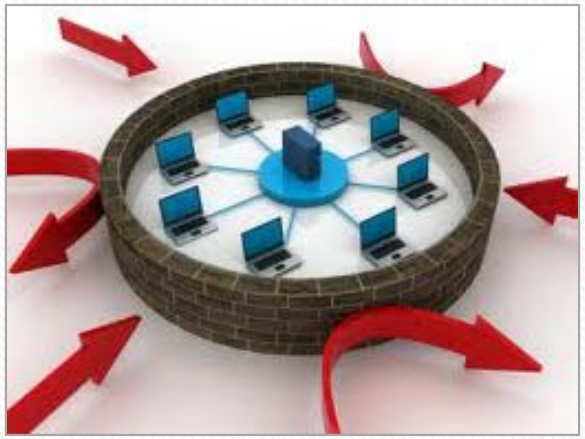
- Trusted Computing System Evaluation Criteria กำหนดระดับความปลอดภัยออกเป็นระดับต่างๆ ดังนี้ (มาตรฐานนี้เรียกอีกชื่อว่า Orange Book)
  - D : Minimal Protection or Unrated
  - C1 : Discretionary Security Protection
  - C2 : Controlled Access Protection
  - B1 : Labeled Security Protection
  - B2 : Structured Protection
  - B3 : Security Domains
  - A1 : Verified Design

การรับรองมาตรฐาน TCSEC ของผู้ผลิต

- ระดับ A1 เป็นระดับเดียวที่มีผู้ผลิตได้รับการับรองคือ Honeywell SCOMP
- Orange Book ล้าสมัยไปอย่างรวดเร็ว -> อุปกรณ์ไม่ทันใช้

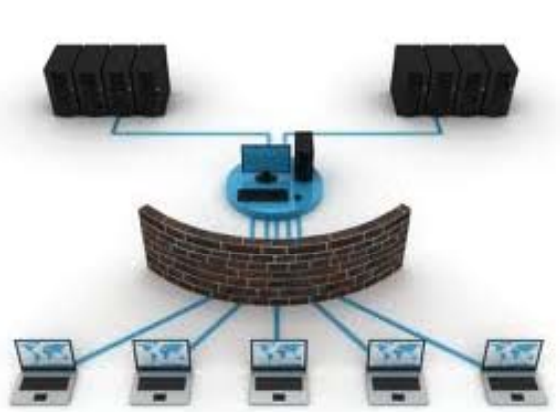
การรักษาความปลอดภัยเครือข่าย

- ใช้มาตรฐาน TNI(Trusted Network Interpretation) ของ TSEC หรือ Red Book
- เครือข่ายระดับ LAN มีการแผ่รังสีมากกว่า WAN
- เครือข่าย LAN มีมีแบนด์วิธสูงกว่า WAN การเข้ารหัสเครื่องเดียวไม่ได้ผล
- เครือข่าย LAN มีเครื่องในบริเวณเดียวกันมาก ควบคุมยากกว่า



Information Security

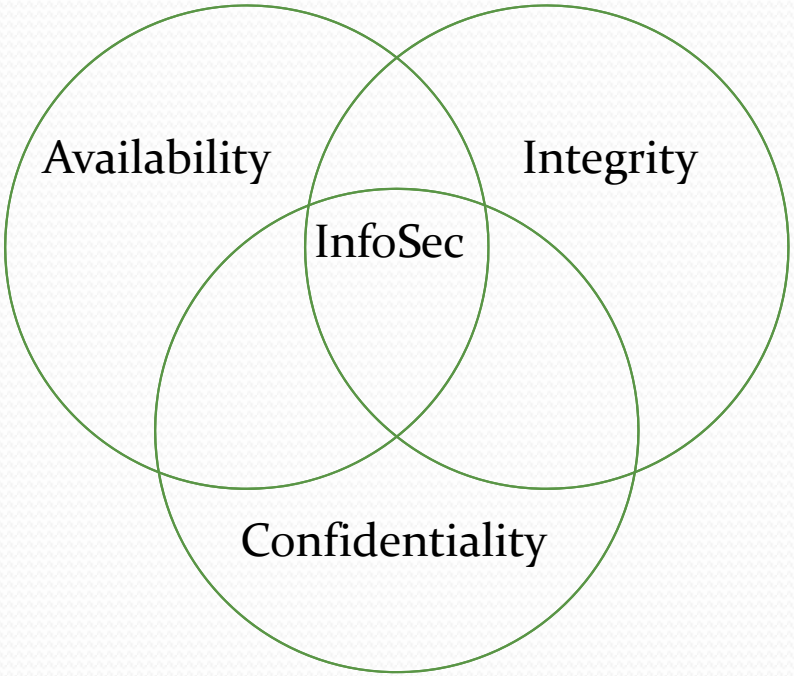
- ถ้าต้องการความปลอดภัยต้องใช้ทุกวิธี
  - การรักษาความปลอดภัยการสื่อสาร(COMSEC) สำหรับปกป้องข่าวสารระหว่างสือสาร
  - EMSEC มาตรฐานควบคุมการแผ่รังสี
  - COMPSEC การรักษาความปลอดภัยด้านคอมพิวเตอร์
  - NETSEC การรักษาความปลอดภัยด้านเครือข่าย



- ทุกวิธีนำมาใช้เป็น INFOSEC การรักษาความปลอดภัยสารสนเทศ

องค์ประกอบการรักษาความปลอดภัย

- ความลับ : Confidentiality ให้เข้าถึงข้อมูลได้เฉพาะผู้ที่ได้รับอนุญาต
- ความคงสภาพ : Integrity ทำให้ข้อมูลยังคงถูกต้อง ไม่ถูกเปลี่ยนแปลง นับจากส่ง
- ความพร้อมใช้งาน : Availability สามารถเข้าถึงได้ทันทีที่ต้องการ



ความลับของข้อมูล(Confidentiality)

- กลไกที่ใช้ในการรักษาความลับคือการเข้ารหัส
  - Cryptography / Encryption การเข้ารหัสข้อมูล ทำให้ข้อมูลอ่านไม่ได้
  - การอ่านต้องถอดรหัสด้วยรหัสคีย์(Key) หรือรหัสผ่าน(Password)
  - ต้องเพิ่มกลไกการรักษาความลับคีย์ และกลไกควบคุมการเข้าถึง(Access Control) -> การพิสูจน์ตัวตน การยืนยันตัวตน

การคงสภาพข้อมูล(Integrity)

- ความถูกต้องของข้อมูล และ ความถูกต้องของแหล่งที่มา
- กลไกการคงสภาพ
  - การป้องกัน(Prevention)
  - การตรวจสอบ(Detection)
- กลไกการคงสภาพไม่ใช่รักษาให้ข้อมูลให้คงเดิม แต่คอยตรวจสอบสภาพและป้องกัน

ความพร้อมใช้งานของข้อมูล(Availability)

- ความสามารถในการใช้งานได้ทันทีที่ต้องการ
- ระบบที่ไม่พร้อมใช้หรือใช้ไม่ได้ ไม่ต่างจากการไม่มีระบบ
- การสำรอง ทำซ้ำ หรือมีระบบคู่ขนาน
- Dos : Denial of Service การโจมตีที่จะทำให้ระบบใช้งานไม่ได้

ความเป็นส่วนบุคคล(Privacy)

- การจัดเก็บ และใช้งานข้อมูล ต้องไม่ละเมิดความเป็นส่วนตัว
- ใช้ได้ ถ้าได้รับอนุญาต ไม่ใช้ในทางที่ผิด
- การคัดลอก ส่งต่อ ต้องได้รับอนุญาตจากเจ้าของข้อมูล
- การเสาะหาข้อมูล ประติดประต่อข้อมูล ย่อมถือเป็นการละเมิด
- ผู้ให้ข้อมูลควรพิจารณาถึงผลตามมา

การระบุตัวตน(Identification)

- เป็นขั้นแรกในการเข้าถึงข้อมูลชั้นความลับ
  - การพิสูจน์ทราบตัวตน(Authentication) พิสูจน์ว่าเป็นคนที่ระบุใช้แน่หรือไม่
  - การอนุญาตใช้งาน(Authorization) เป็นการตรวจสิทธิ์ว่าทำอะไรได้บ้าง เช่น การใช้ ACL (Access Control List)

การตรวจสอบได้(Accountablility)

- กลไกสำหรับการตรวจสอบย้อนหลัง
- บันทึกทุกกิจกรรมที่เกิดขึ้นของผู้ใช้งานทุกระดับ
- กลไกที่ใช้กันมากคือ Log