บทที่ 1 : การรักษาความปลอดภัยข้อมูล Part1

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Agenda

- หลักการรักษาความปลอดภัย
- การรักษาความปลอดภัยข้อมูล
- การรักษาความปลอดภัยสารสนเทศ
- ประวัติการรักษาความปลอดภัย

หลักการรักษาความปลอดภัย

การรักษาคุณลักษณะ 3 ประการเอาไว้ ได้แก่ **ความลับ** (Confidentiality), **ความถูกต้อง** (Integrity) และ**ความพร้อมใช้งาน** (Availability) **[CIA]**

โดยต้องทำทั้ง 3 ส่วนควบคู่กัน ได้แก่ **คน** (People), **กระบวนการ** (Process) และ**เทคโนโลยี** (Technology)

การรักษาความปลอดภัยข้อมูล

- สิ่งหนึ่งที่มีค่ามากที่สุดขององค์กรคือ **ข้อมูล หรือ สารสนเทศ**
- การปกป้องรักษาข้อมูลเป็นสิ่งสำคัญในยุคแห่งข้อมูลข่าวสาร
- ***“ยุคที่ผู้ครอบครองสารสนเทศมากกว่าย่อมเป็นผู้ได้เปรียบ”***
- ข้อมูลมีความเสี่ยงที่จะถูกโจมตีจากหลายทาง
- จำเป็นต้องมีระบบรักษาความปลอดภัยที่แข็งแกร่ง

การรักษาความปลอดภัยข้อมูล [ต่อ]

- เกือบทุกองค์กรจำเป็นต้องเชื่อมต่อกับอินเทอร์เน็ต
- **“อินเทอร์เน็ตเป็นดาบสองคม”**
- ข้อมูลและเครื่องมือที่ใช้สำหรับเจาะระบบ หาได้อย่างง่ายดายจากอินเทอร์เน็ต
- คนที่ไม่มีความรู้ทางคอมพิวเตอร์มากนักก็สามารถใช้เครื่องมือโจมตีเครือข่ายได้

การรักษาความปลอดภัยข้อมูล [ต่อ]

- *“ไม่มีระบบใดที่ปลอดภัยอย่างสมบูรณ์” = “ไม่มีระบบใดที่ไม่มีช่องโหว่”*
- การมีระบบรักษาความปลอดภัยที่ดีที่สุดไม่ได้หมายความว่าข้อมูลจะปลอดภัย
- การรักษาความปลอดภัยเป็นการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

การรักษาความปลอดภัยข้อมูล [ต่อ]

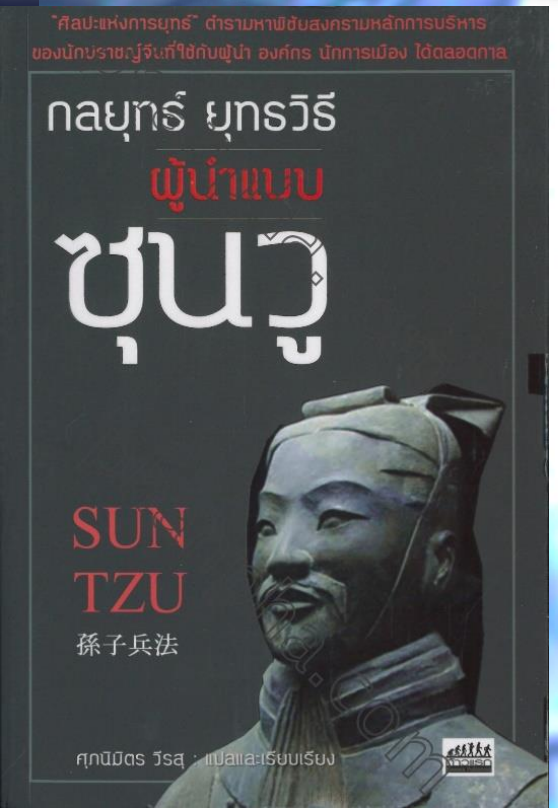
- ไม่ใช่เพียงแค่การติดตั้งระบบรักษาความปลอดภัย แต่รวมถึง
  - *การวิเคราะห์และบริหารความเสี่ยง (Risk)*
  - *ภัยคุกคาม (Threat)*
  - *ช่องโหว่หรือจุดอ่อน (Vulnerability)*
  - *การกำหนดและบังคับใช้นโยบาย (Policy)*
  - *การเฝ้าระวังเหตุการณ์อยู่ตลอดเวลา (Monitoring)*

การรักษาความปลอดภัยสารสนเทศ (Information Security)

- สารสนเทศ (Information) หมายถึง ความรู้ ความคิด ข่าวสาร ข้อเท็จจริง
- การรักษาความปลอดภัย (Security) หมายถึง การทำให้รอดพ้นจากอันตราย ความกลัว ความทุกข์ใจ หรือความกังวล
- การรักษาความปลอดภัยสารสนเทศ ในความหมายด้านไอที หมายถึง *มาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งานความรู้ ความคิด ข่าวสาร และข้อเท็จจริง*

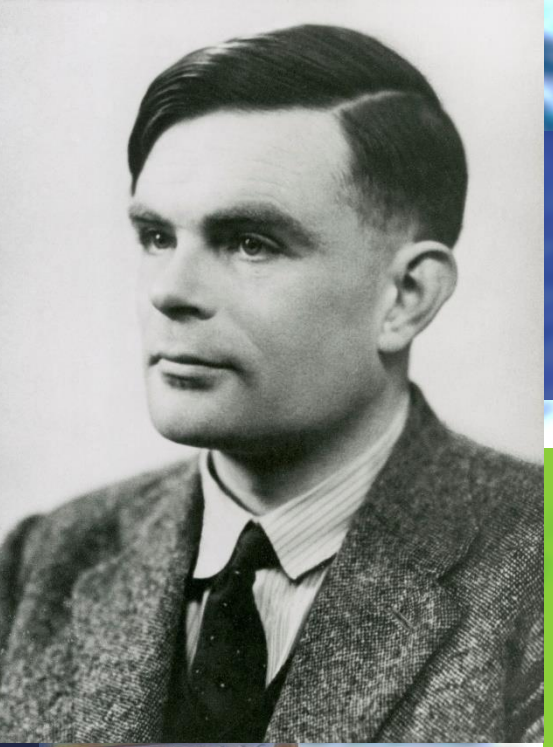
ประวัติของการรักษาความปลอดภัย

- ด้านกายภาพ (Physical Security)
- ด้านการสื่อสาร (Communication Security)
- คอมพิวเตอร์ (Computer Security)
- เครือข่าย (Network Security)
- สารสนเทศ (Information Security)

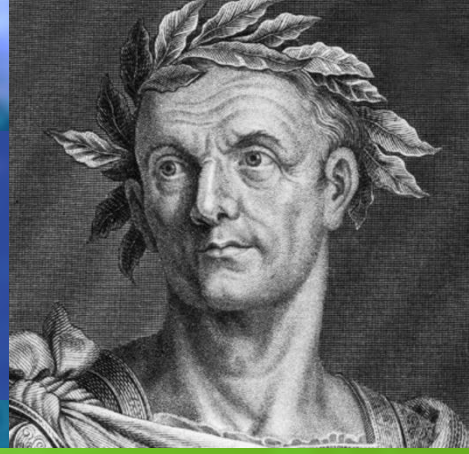


ความปลอดภัยด้านกายภาพ (Physical Security)

- ในอดีตข้อมูลสำคัญจะอยู่ในรูปวัตถุที่จับต้องได้ เช่น แผ่นหิน แผ่นหนัง กระดาษ
- ใช้การป้องกันทางกายภาพ เช่น กำแพง ปราสาท ยาม ผู้คุ้มกันคน นำสาส์น
- แต่บุคคลสำคัญในอดีตส่วนใหญ่จะไม่นิยมบันทึกข้อมูลสำคัญลงบนสื่อถาวร และจะสนทนาข้อมูลสำคัญกับบุคคลที่ไว้ใจได้เท่านั้น
- ซุนวู กล่าวว่า ***“ความลับที่รู้โดยคนมากกว่าหนึ่งคน ย่อมไม่ถือว่าเป็นความลับอีกต่อไป”***

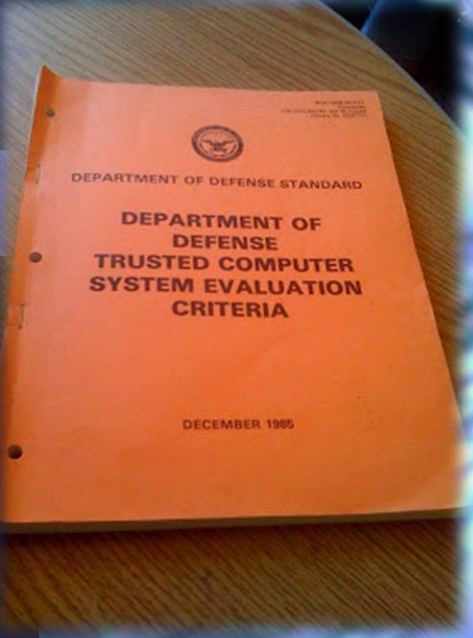


การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

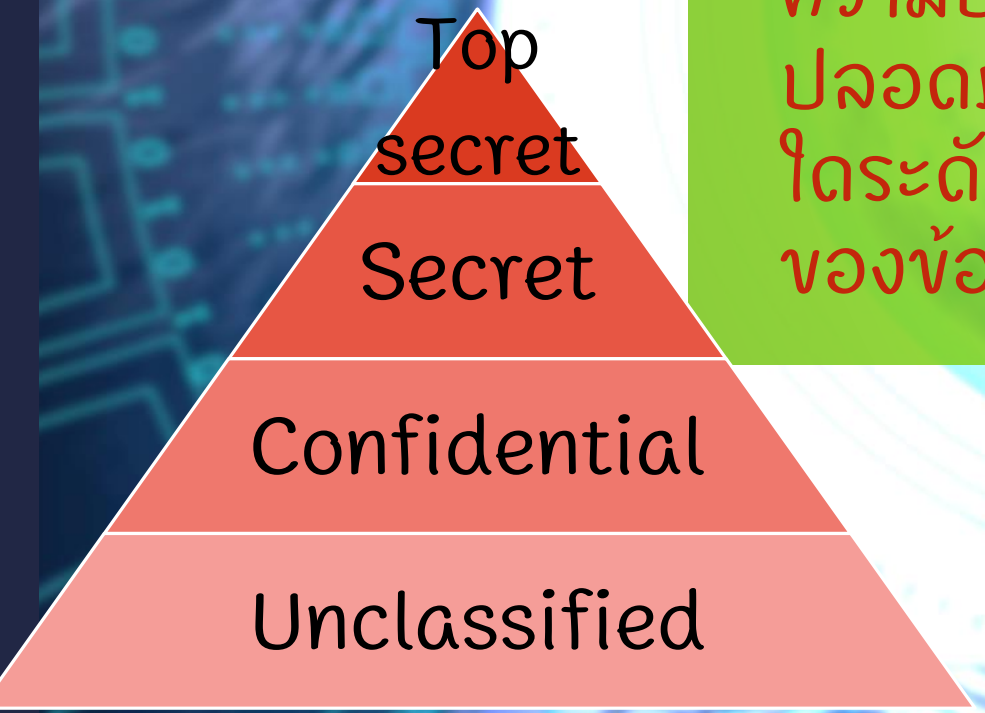


- ในยุค**จูเลียส ซีซาร์** ได้มีการคิดค้นวิธีการซ่อนข้อมูล โดยการเข้ารหัส (Encryption) ถ้ามีการขโมยข้อมูลระหว่างทาง ผู้อ่านจะไม่เข้าใจถ้าไม่รู้วิธีถอดรหัส
- ในสงครามโลกครั้งที่สอง **เยอรมันใช้เครื่องมือ Enigma** สำหรับเข้ารหัสข้อมูลทางการทหาร ซึ่งเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสจากเครื่องนี้ได้ แต่ในที่สุดฝ่ายพันธมิตรก็สามารถถอดรหัสได้ โดย **Alan Turing** ซึ่งได้ถูกสร้างเป็นภาพยนตร์ฮอลลีวู้ด ชื่อว่า The Imitation Game ในปี 2014

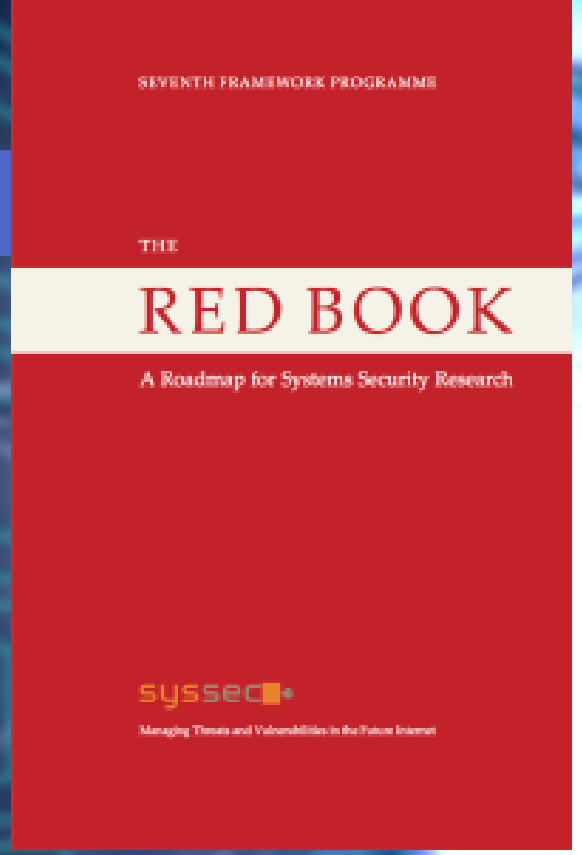
การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)



- ข้อมูลส่วนใหญ่ถูกจัดเก็บเอาไว้ในคอมพิวเตอร์ด้วยระบบดิจิตอล จึงมีความพยายามที่จะโจมตีความปลอดภัยบนเครื่องคอมพิวเตอร์
- ทศวรรษ 1970 มีการพัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ โดยแบ่งระดับความปลอดภัยเป็น 4 ระดับ ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่ง จะต้องมีสิทธิ์เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น



- ต่อมาพัฒนาเป็นมาตรฐาน TCSEC หรือรู้จักทั่วไปว่า Orange book



การรักษาความปลอดภัยเครือข่าย (Network Security)

- เมื่อคอมพิวเตอร์ถูกเชื่อมต่อกันเป็นเครือข่ายก็เกิดปัญหาใหม่ขึ้น เช่น อาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน ทำให้การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆอาจไม่ได้ผล
- ในปี 1987 มีการพัฒนามาตรฐานเกี่ยวกับเครือข่าย โดยพัฒนาต่อมาจาก Orange Book ซึ่งรู้จักกันในชื่อ Red Book ซึ่งได้เพิ่มส่วนเกี่ยวข้องกับเครือข่ายเข้าไป

การรักษาความปลอดภัยสารสนเทศ (Information Security)

- สรุปได้ว่าไม่มีวิธีการใดที่สามารถแก้ปัญหาได้อย่างเบ็ดเสร็จ
- การรักษาความปลอดภัยที่ดี**ต้องใช้ทุกวิธีการ**มารวมกันจึงจะสามารถรักษาความปลอดภัยสารสนเทศได้