ความปลอดภัยคอมพิวเตอร์ (424)

ศัพท์ทางความมั่นคงไซเบอร์

ทรงฤทธิ์ กิติศรีวรพันธุ์

Email : songrit@npu.ac.th

สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

Revised 2020-06-26

Lecture plan

- **1.1 ข้อมูลเบื้องต้น**
- 1.2 ชนิดช่องโหว่ด้านความปลอดภัย
- 1.3 ชนิดการโจมตี
- 1.4 แรงจูงใจผู้ร้าย
- 1.5 ตัวอย่างการโจมตี: shellshock

Security 2 ด้าน

ป้องกัน

โจมตี

This Photo by Unknown Author is licensed under CC BY-SA

ข้อมูลเผยแพร่ และ ข้อมูลความลับ

- **ข้อมูลเผยแพร่** เป็น ข้อมูลที่ไม่เจาะจงผู้รับ มีเจตนาให้แพร่หลาย
  - เว็บเพจ
  - ภาพยนตร์
  - ข่าว และ ข้อมูลอื่นๆ
- **ข้อมูลความลับ**
  - ข้อมูลที่เจาะจงผู้อ่าน
  - อีเมล์
  - รหัสผ่าน
  - ข้อมูลบัญชีเงินเดือน / รายได้ / ธนาคาร
  - ข้อมูลสุขภาพ

ความปลอดภัยของข้อมูล

- สามารถปกป้องความลับ
  - Confidential
- สามารถรักษาความสมบูรณ์
  - Integrity
- สามารถรักษาเวลา
  - Availability

ความสามารถในการปกป้องความลับ

- Confidentiality
  - เก็บความลับ
- ข้อมูลส่งถึงปลายทางโดยสมบูรณ์ แต่....
  - ถูกเปิดอ่านระหว่างทาง
  - โดยคนอื่น

ความสามารถด้านการป้องกันการแก้ไข

- Integrity
- ความสามารถรักษาต้นฉบับให้คงเดิม
- อาจเป็นข้อมูลความลับ หรือเป็นข้อมูลเผยแพร่ได้
- ข้อมูล**เผยแพร่**เช่น กฎหมาย
  - กฎหมายต้องไม่ถูกแก้ไขโดยไม่มีใครสามารถตรวจสอบได้
  - ข่าว หรือข้อความ ที่มีการโพส ต้องมีระบบตรวจป้องกันการแก้ไขต้นฉบับ
- เพื่อไม่ให้เกิดการปฏิเสธความรับผิด-รับชอบ(Non-repudiation) ภายหลัง

ความสามารถด้านการรักษาเวลา

- Avialability
- มีระบบป้องกันไม่ให้เกิดความล่าช้า
- เช่น การโจมตีให้เข้าถึงเครื่องแม่ข่ายได้ช้า
  - Denied-of-Service (DoS) ทำให้เครื่องปฏิเสธการให้บริการ
  - Distributed DoS (DDoS) การโจมจาก cloud bot
  - การกระทำใดๆ ให้เกิดความล่าช้า
    - ครม.ไฟเขียวเลื่อนบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลฯ ออกไป 1 ปี (พค. 2564)
    - Personal Data Protection Act B.E. 2562 ???

ความจำเป็นป้องกันภัยคุกคามทางไซเบอร์

- เครือข่ายอินเทอร์เน็ต ถือเป็นโครงสร้างพื้นฐานสำคัญต่อการพัฒนาประเทศ
- การใช้และเปลี่ยนข้อมูลสำคัญ ผ่านเครือข่ายอินเทอร์เน็ต
  - ปริมาณน้ำในเขื่อน / การควบคุมเปิดปิดเขื่อน / ระบบไฟฟ้า
- ความมั่นคงของประเทศ ที่มีความเสี่ยงจากการคุกคามโดย
  - ทางบก ทางเรือ ทางอากาศ
  - ทางอวกาศ
  - ทางไซเบอร์
- เมื่อเทคโนโลยีอินเทอร์เน็ตมีความสำคัญต่อประเทศ
  - การรักษาความมั่นคงทางไซเบอร์ จึงมีต้องการผู้มีความรู้ ความเชี่ยวชาญ
  - คอยรับมือจากภัยทางไซเบอร์ที่จะเพิ่มสูงขึ้นในอนาคต

ประเทศไทย กฎหมายด้านไซเบอร์

- พรบ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)
  - Electronic Transactions Development Agency
  - ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
  - เป็นองค์กรมหาชน → หน่วยงานรัฐบาลเภทที่ 3 ไม่เป็นราชการ ไม่เป็นรัฐวิสาหกิจ
- พรบ.พัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
- พรบ.สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
- พรบ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
- พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์
- พรบ.คุ้มครองข้อมูลส่วนบุคคล

พรบ. ไซเบอร์ (2562)

- พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒
- "**ไซเบอร์**" คือ ข้อมูลหรือการสื่อสารผ่านครือข่าย หรือ ระบบอินเทอร์เน็ต รวมดาวเทียมและเครือข่ายที่คล้ายคลึงกัน
- **ภัยคุกคามทางไซเบอร์** คือ การกระทำโดย**มิชอบ**ผ่านทางไซเบอร์
- **การรักษาความมั่นคงไซเบอร์** คือ มาตรการหรือการดำเนินการเพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

21:50
Thai PBS HD
Traffic Overview
Cyber security
& Cyber Warfare
Thai PBS

ความมั่นคงทางไซเบอร์ (นโยบาย)

- กฎหมายด้านไซเบอร์ประเทศไทย
  - นายกรัฐมนตรีเป็นประธานกรรมการ
  - กรรมการโดยตำแหน่ง
    - รัฐมนตรีกระทรวงกลาโหม
    - รัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
    - ปลัดกระทรวงการคลัง
    - ปลัดกระทรวงยุติธรรม
    - ผู้บัญชาการตำรวจแห่งชาติ
    - เลขาธิการสภาความมั่นคงแห่งชาติ
- กรรมการผู้ทรงคุณวุฒิ
  - ไม่เกิน 7 คน
  - แต่งตั้งโดย คณะรัฐมนตรี
  - เป็นผู้เชี่ยวชาญเกี่ยวข้อง
    1. ด้านรักษาความมั่นคงปลอดภัยไซเบอร์
    2. ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
    3. ด้านการคุ้มครองข้อมูลส่วนบุคคล
    4. ด้านวิทยาศาสตร์
    5. ด้านวิศวกรรมศาสตร์
    6. ด้านกฎหมาย
    7. ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง

พรบ.คุ้มครองข้อมูลส่วนบุคคล(2562)

- ครม.ไฟเขียวเลื่อนบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลฯ ออกไป 1 ปี (พค. 2564)
  - https://www.ilaw.or.th/node/5669
- ข้อมูลส่วนบุคคล คือ
  - *"ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ" ม.5(2) PDPA (2562)*
- วัตถุประสงค์ พรบ. : การเก็บรวมรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของผู้อื่นจะทำได้ก็ต่อเมื่อเจ้าของข้อมูลได้ให้ความยินยอมโดยชัดแจ้ง

ปัญหาความปลอดภัย

- จุดเริ่มต้นจากระบบมีช่องโหว่ **(Vulnerability)**
- Attacker หาช่องโหว่ ระบบเป้าหมาย
- Attacker เขียนโค้ดเจาะระบบ จากช่องโหว่ที่พบ
- เรียกโค้ดเจาะระบบว่า **Exploit**
  - การค้นหาช่องโหว่และเขียนโค้ดสำหรับเจาะระบบ ต้องการความคิดสร้างสรรค์และความฉลาดอย่างมาก
  - ต้องการความรู้ในแนวกว้าง (หลากหลายด้าน)

Lecture plan

- 1.1 ข้อมูลเบื้องต้น
- **1.2 ชนิดช่องโหว่ด้านความปลอดภัย**
- 1.3 ชนิดการโจมตี
- 1.4 แรงจูงใจผู้ร้าย
- 1.5 ตัวอย่างการโจมตี: shellshock