บทเรียนที่ 12
การรักษาความปลอดภัยคอมพิวเตอร์ที่ใช้งานบนเครือข่าย

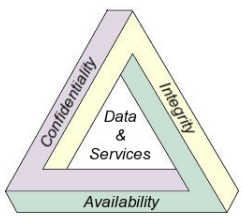
อาจารย์สาโรช เมาลานนท์

เนื้อหาประจำบท

- **การรักษาความปลอดภัยคอมพิวเตอร์ (Security)**
  - องค์ประกอบด้านความปลอดภัยข้อมูล
  - ระบบงานด้านการรักษาความปลอดภัย
- **ภัยคุกคาม (Threat)**
  - ประเภทของภัยคุกคาม
  - ตัวอย่างภัยคุกคาม
- **ปัญหาความปลอดภัยที่ใกล้ตัวเรา**
  - ไวรัส เวิร์ม และ โทรจันฮอร์ส
  - การไม่เข้าใจเกี่ยวกับแพตช์ (Patch)
  - การไม่รู้จักใช้ไฟร์วอลล์ส่วนบุคคล
  - แนวทางการป้องกันตัวให้ปลอดภัยจากภัยคุกคาม

องค์ประกอบด้านความปลอดภัยของข้อมูล

- **ความลับ** (Confidentiality)
- **ความคงสภาพ** (Integrity)
- **ความพร้อมใช้งาน** (Availability)



ระบบงานด้านการรักษาความปลอดภัย

- **การพิสูจน์ทราบตัวตน** (Authentication)
  - **การระบุตัวตน** (Identification)
    - Username/Password, Biometrics
- **การตรวจสอบสิทธิ์การใช้งาน** (Authorization)
- **การตรวจสอบได้** (Accountability)

ภัยคุกคาม (Threat)

- การโจมตี (Attack)
- ผู้โจมตี
  - แฮคเกอร์ (Hacker)
  - แคร็กเกอร์ (Cracker)

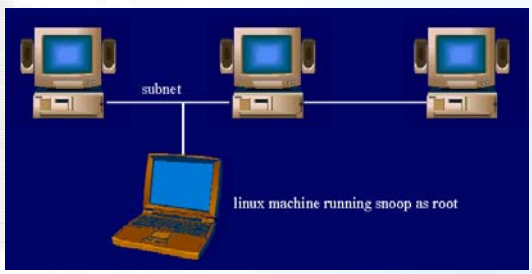
ประเภทของภัยคุกคาม

- การเปิดเผย
- การหลอกลวง
- การขัดขวาง

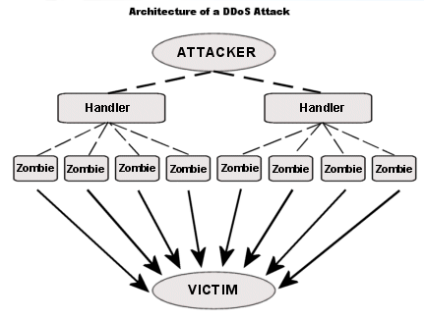
ตัวอย่างของภัยคุกคาม

- การสอดแนม (Snooping) หรือ (Sniffing)
- การเปลี่ยนแปลงข้อมูล (Modification)
- การปลอมตัว (Spoofing)
- การโจมตีให้เกิดการปฏิเสธการบริการ (Denial of Service: DoS) (Distributed Denial of Service: DDoS)

การสอดแนม



การโจมตีแบบ DDoS

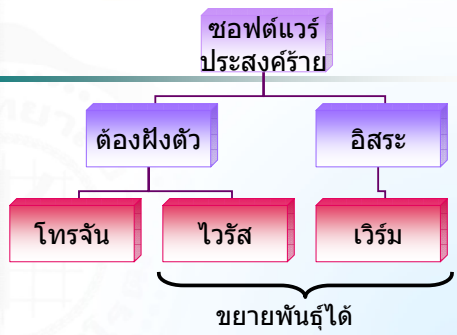


ตัวอย่างของภัยคุกคาม (ต่อ)

- โปรแกรมประสงค์ร้าย (malware)
- สแปม (Spam)
- สปายแวร์ (Spyware)

ปัญหาความปลอดภัยที่ใกล้ตัว

- มัลแวร์
  - ไวรัสคอมพิวเตอร์
  - เวิร์ม
  - ม้าโทรจัน



ปัญหาความปลอดภัยที่ใกล้ตัว (ต่อ)

- การไม่เข้าใจเกี่ยวกับแพตช์ (Patch)
- การไม่รู้จักไฟร์วอลล์ส่วนบุคคล (Personal Firewall)

แนวทางการป้องกันตัวให้ปลอดภัยจากภัยคุกคาม

- การติดตั้งโปรแกรมตรวจจับไวรัส
  - การปรับปรุงฐานข้อมูลไวรัส
  - การตรวจสอบเต็มรูป
- การติดตั้งไฟร์วอลล์ส่วนบุคคล
- การไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ
- ไม่เปิดเอกสารแนบจากบุคคลไม่รู้จัก

แนวทางการป้องกันตัวให้ปลอดภัยจากภัยคุกคาม (ต่อ)

- การปรับปรุงซอฟต์แวร์อยู่เสมอ
- การสำเนาแฟ้มข้อมูลที่สำคัญไว้

จบ