ทำอย่างไรผู้ใช้อินเทอร์เน็ต จึงจะปลอดภัยจากการถูกแฮก

ยืน ภู่วรวรรณ
yuen@nontri.ku.ac.th

สำนักบริการคอมพิวเตอร์
และ
ภาควิชาวิศวกรรมคอมพิวเตอร์
มหาวิทยาลัยเกษตรศาสตร์
25 มิถุนายน 2543

หัวข้อที่จะบรรยาย

- ทำไมต้องให้ความสนใจในเรื่องความปลอดภัย
- ปัญหาที่เกิดขึ้นมีอะไรบ้าง
- อินเทอร์เน็ต กับแฮกเกอร์
- การดำเนินการให้ได้รับความปลอดภัย
- การป้องกัน และสร้างระบบรักษาความปลอดภัย
- เทคโนโลยีที่เกี่ยวข้อง
- กฎหมายและมาตรการทางสังคม
- อนาคต

ทำไมต้องให้ความสนใจในเรื่องความปลอดภัย

- ปัจจุบัน (2000/Jan ข้อมูล nw.com) มีเครื่องต่ออยู่บนอินเทอร์เน็ต 72.4 ล้านเครื่อง
- จำนวนผู้ใช้ (2000/Feb ข้อมูล NITC) มีผู้ใช้อินเทอร์เน็ตในประเทศไทย 1,000,000 คน
- จำนวนผู้ใช้ทั่วโลกคาดว่ากว่า 300 ล้านคน

สิ่งที่สำคัญในการทำให้ปัญหาเพิ่มขึ้น

- เครือข่ายคอมพิวเตอร์มีความสำคัญเพิ่มมากขึ้น
- เครือข่ายคอมพิวเตอร์ทำให้เข้าถึงได้ทุกหนทุกแห่ง
- เครือข่ายคอมพิวเตอร์มีลักษณะ Virtual ทำให้ติดตามเส้นทางยาก
- ทรัพย์สมบัติทางด้านข้อมูลมีมากขึ้น

เครือข่ายคอมพิวเตอร์ทำให้

- การเกิดของ eBusiness, eCommerce, eConomy
- การให้บริการลูกค้าที่ดีขึ้น
- การทำงานร่วมกันได้มาก
- ลดค่าใช้จ่ายสื่อสาร
- เพิ่มประสิทธิภาพการทำงานและการเชื่อมโยงภายใน
- ได้ข้อมูลข่าวสารรวดเร็ว

ด้วยเหตุนี้ทำให้การใช้งานเครือข่ายมีความจำเป็น และมีอัตราเพิ่มขึ้นอย่างรวดเร็ว

ทำไมปัญหาการแฮกบนเครือข่ายจึงเกิดขึ้นได้ง่าย

- งานทางวิศวกรรม และงานพัฒนาเทคโนโลยี ไม่พอเพียงที่จะป้องกันระบบ และของมีค่าบนเครือข่าย
- ความรู้และการปฏิบัติของผู้ใช้ทั่วไปยังไม่พอเพียงกับการป้องกันตัวเอง และการโจมตี

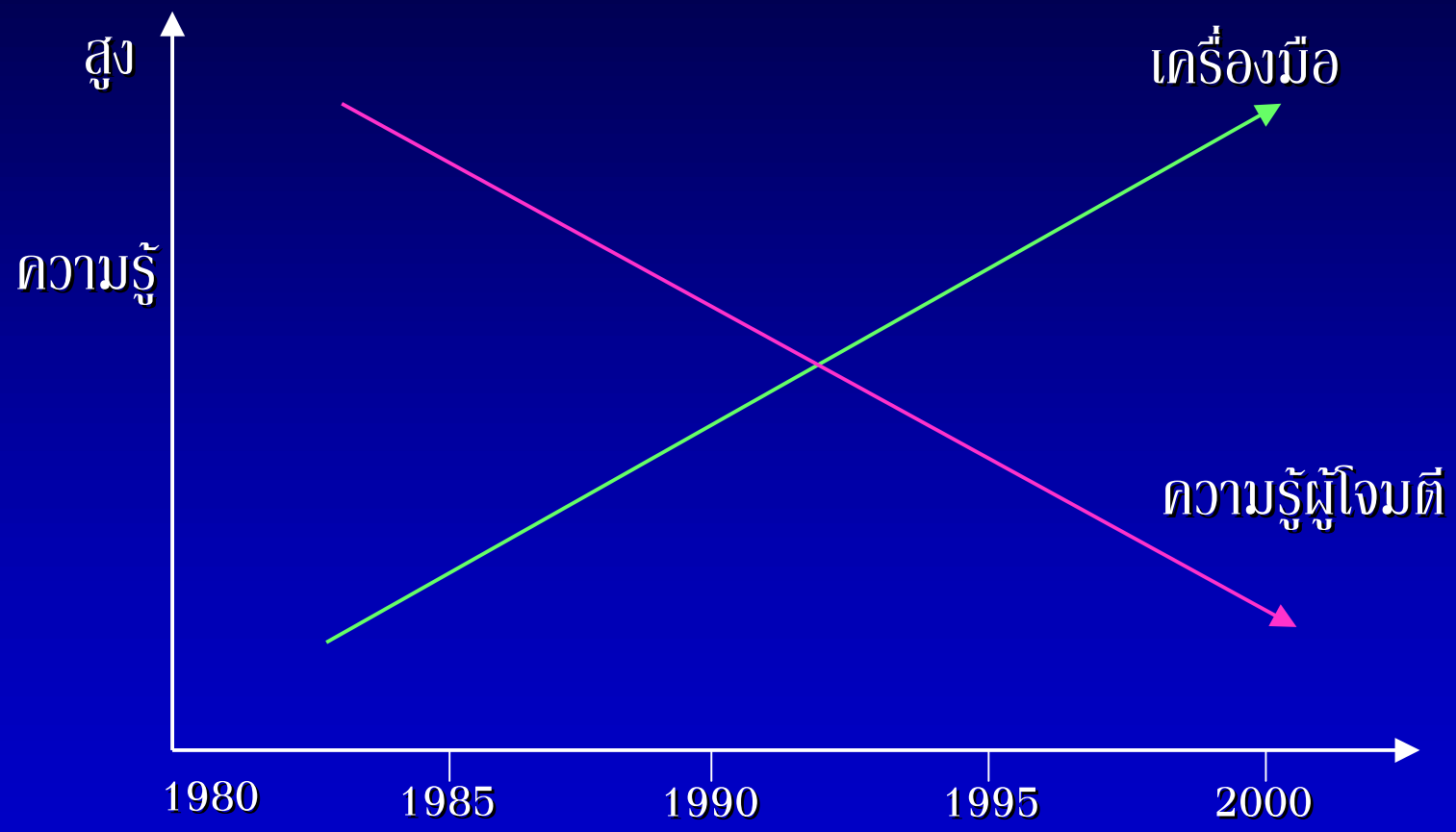
โดยปกติผู้ใช้อินเทอร์เน็ตอยู่ในมุมสว่าง แต่โจรผู้ร้ายอยู่ในมุมมืด

ความเสี่ยงที่เกิดกับผู้ใช้งานอินเทอร์เน็ต

การโจมตี และลักลอบ หรือดำเนินการใด ๆ อาจทำให้ผู้ใช้งานเกิดปัญหาการสูญเสีย

- เงิน
- เวลา
- ผลิตภัณฑ์
- เสียโอกาส
- ข้อมูลความลับ
- ความเชื่อมั่น

ทำไมการโจมตีผู้ใช้อินเทอร์เน็ตจึงง่ายขึ้น



ที่มา : รายงานของ Software Enginecring Institue
Carnegie Mellon University

ประวัติการพัฒนาเทคนิค และ tool ในการโจมตีของแฮกเกอร์

ปี 1980 - 1985	password guessing
	self-replicating code
ปี 1986 - 1990	password cracking
	expliciting known valnerable
	disabling audits
	back doors

ประวัติการพัฒนาเทคนิค (ต่อ)

ปี 1991 - 1995	hijacking session sweepers sniffers stealth diagnostics packet spoofing
ปี 1966 - ปัจจุบัน	GUI automated scan www attack denial service

ทำไมแฮกเกอร์จึง แฮกระบบได้ง่าย โดยไม่ต้องมีความรู้มาก

- เพราะมีเครื่องมือช่วยมาก และหาได้ง่ายมาก
- ตัวอย่างเครื่องมือ
  - network scanner
  - password cracking
  - packet sniffer
  - variety of trojan horse programs and libraries
  - เครื่องมือแก้ไขล็อกไฟล์ และพรางตัว
  - เครื่องมือช่วยในการตรวจสอบระบบและแก้ไข
  - เครื่องมือเปลี่ยน config ระบบ แบบอัตโนมัติ
  - เครื่องมือตรวจสอบ check sum

ผู้ใช้อินเทอร์เน็ต กับการโจมตีของแฮกเกอร์

วิธีการของแฮกเกอร์

- Probe
- Scan
- Account compromise
- Root Compromise
- Packet Sniffer
- Denial of Service
- Exploitation of Trust
- Malicious Code
- Internet Infrastructure attack

Probe

Probe คือวิธีการ และความพ ย า ย ระบบ โดยดูว่า มีประตูหรือช่องทางใดที่ไม่ถูกต้อง หรือเข้าสู่ account ที่ยังไม่มีผู้ใช้ ในระบบยูนิกซ์มีการเปิด account แบบลอย เช่น guest การเข้าสู่ระบบได้ อาจทำให้เกิดปัญหาที่รุนแรงตามมา

Scan

Scan เป็นวิธีการเข้าสู่ระบบ โดยใช้เครื่องมืออัตโนมัติ หรือเป็นโปรแกรมที่เขียนขึ้นเพื่อสแกนหาทางเข้าสู่ระบบ หรือหาช่องจากการติดตั้ง หรือการกำหนดระบบผิดพลาด

แฮกเกอร์มีเครื่องตรวจหาระบบ และโจมตี เช่น การส่งข้อมูลเข้ามาในพอร์ต POP3, IMAP เพื่อให้ระบบโอเวอร์โฟลว์ และทำงานผิดพลาด จากนั้นจะเกิดช่องที่เข้าระบบได้

Account Compromise

แฮกเกอร์จะหาทางเข้าสู่ Account ของยูสเซอร์ โดยการดักรหัส password, crack password หรือใช้วิธีการที่จะได้มาซึ่ง account การเข้าสู่ account ได้ จะทำการเหมือนมีสิทธิเป็นเจ้าของ จึงสามารถดูข้อมูล ลบ หรือเพิ่มลงในเครื่องได้ การเข้าสู่ account ได้จะกลายเป็นระดับ root account หรือระดับ admin ได้

Root Compromise

เป้าหมายของแฮกเกอร์ คือต้องการเข้าสู่ root เพื่อได้สิทธิในการดำเนินการทุกอย่าง เช่น การเข้าสู่ Account ของผู้อื่น หรือดำเนินการเสมือนเป็นเจ้าของระบบได้ ที่สำคัญคือสามารถลบช่องทางเข้า และ log file ต่าง ๆ และทำให้ยากต่อการตรวจสอบได้ และปกปิดความผิดของตัวเอง

Sniffer

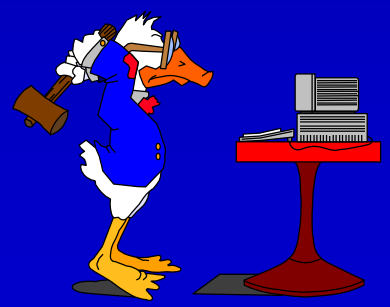
Sniffer เป็นโปรแกรมคอมพิวเตอร์ที่แฮกเกอร์จะนำไปติดตั้งไว้ อาจติดตั้งที่ในสิทธิของตน แต่สามารถเก็บข้อมูลในเครือข่ายที่ผ่านในเซกเมนต์เดียวกัน เพื่อดักเก็บชื่อ รหัสผ่าน หรือข้อมูลสำคัญต่าง ๆ ทำให้ได้รหัสผ่านที่จะดำเนินการต่อไปอีกขั้น เช่น การวาง sniffer ต่อไปอีก

Denial of Service

แฮกเกอร์จะโจมตี โดยเป้าหมายหลักที่เครื่อง หรือเครือข่าย เพื่อให้เครื่องมีภาระงานหนักจนไม่สามารถให้บริการได้ หรือถ้าเป็นเครือข่าย ก็จะเพิ่มปริมาณข้อมูลจำนวนมากจนเครือข่ายทำงานได้ช้าลง

การโจมตี Internet Infrastructure

ส่วนนี้แฮกเกอร์จะทำให้ปริมาณในเครือข่าย โดยเฉพาะอุปกรณ์หลักทำงานหนัก เช่น การส่ง ping ICMP หรือส่งแพ็กเก็ตให้วิ่งวนต่อ ๆ กัน เพื่อเพิ่มปริมาณข้อมูลในเครือข่าย



ผู้ใช้ยังคงโดนโจมตีจาก mail bomb, junk, spam หรือการใช้วาจาหยาบคาย

เนื่องจากระบบ mail บนอินเทอร์เน็ตมีจุดอ่อนมาก การส่งเมล์ทำได้ง่าย จึงง่ายต่อการสร้าง spam หรือการทำ mail bomb

Exploitation of Trust

ปกติการทำงานในระหว่างกัน เช่น ไคลแอนต์ เซิร์ฟเวอร์ หรือระบบที่คอมพิวเตอร์ติดต่อกันภายใต้ระบบงาน เพราะเป็นเครื่องที่เชื่อถือได้ แฮกเกอร์จะอาศัยช่องทางเหล่านี้ปลอมตัว เพื่อดูว่าการติดต่อนั้นใช้ช่องทางหรือ วิธีการอย่างไร เพื่อจะหาโปรแกรมมาเชื่อมแทน

Malicious Code

สิ่งที่ผู้ใช้อินเทอร์เน็ตพบมากคือ ไวรัส เวิร์ม และม้าโทรจัน แฮกเกอร์จะหลอกส่งโปรแกรมให้ และถ้าเรียกโปรแกรมนั้น โปรแกรมที่แอบซ่อนไว้ก็จะทำงานตามที่กำหนด เช่น แอบขโมยไฟล์ส่งออก หรือเป็นไวรัสแพร่กระจาย เป็นเวิร์มส่งต่อได้

การดำเนินการให้ได้รับความปลอดภัย

สิ่งที่สำคัญและต้องปฏิบัติให้ความสำคัญ กรณีของการใช้งานที่มีความสำคัญ หรือคิดว่าจะป้องกันตนเอง

- การล็อกคอมพิวเตอร์
- Bios Security
- Boot loader Security
- Local security
- File and File system security

Unix File System

ตัวอย่างระบบไฟล์

-rw-r--r-- kevin users 114 Jun 25 2000 .zlogin

- 1st bit – directory? (no)
- 2nd bit – read by owner?
- (yes, by kevin)
- 3rd bit – write by owner?
- (yes, by kevin)
- 4th bit – execute by owner?
- (no)
- 5th bit – read by group?
- (yes, by users)
- 6th bit – write by group? (no)
- 7th bit – execute by group?
- (no)
- 8th bit – read by everyone?
- (yes, by everyone)
- 9th bit – write by everyone?
- (no)
- 10th bit – execute by everyone?
- (no)

แนวทางในการป้องกันตนเอง

1. ต้องดูแลและจัดการกับ cookies
2. จัดการและเก็บข้อมูลประวัติการใช้ออกไป
3. ฟิลเตอร์ spam
4. ป้องกัน malicious code : ไวรัส เวิร์ม โทรจัน
5. สร้างระบบตรวจสอบไวรัส
6. ใช้ดิจิตอลซิกเนเจอร์ หรือเข้ารหัสเมื่อรับส่งข้อมูลสำคัญ

ต้องปฏิบัติตามนโยบายองค์กร

- ใช้เกทเวย์ หรือไฟล์วอล มี policy ชัดเจน
- ใช้ VPN กับเครือข่ายย่อย
- ดูแลเรื่อง remote access เช่น ใช้ secure shell
- ติดตั้งระบบ detection
- ใช้รหัสผ่าน และนโยบายรักษาปรับเปลี่ยนรหัสผ่าน

สิ่งที่ต้องปฏิบัติสำหรับผู้ใช้

ให้ความสำคัญกับ browser และกำหนดระบบ browser ให้อยู่ในระบบที่ปลอดภัย และต้องทำความเข้าใจ

การเซต Netscape

การเซต IE

การรับ attach file หรือสิ่งที่มากับ email

- จะต้องตรวจสอบด้วยความระมัดระวัง
- ระวังไวรัส เวริ์ม หรือโทรจัน
- ตรวจสอบด้วยโปรแกรม anti virus ก่อน

การใช้รหัสผ่าน

ระบบรหัสผ่าน มีตั้งแต่ bios เป็นระบบที่ดี เพราะป้องกันการบูตระบบได้

เซต password ของ window

password ของ account

ระบบต้องยาวกว่า 8 ตัวอักษร (หรือเท่ากัน)

หมั่น Update OS หรือ browser ให้เป็นเวอร์ชันใหม่

เพราะเวอร์ชันเก่ามักมีผู้คนพบ hole เวอร์ชันใหม่ได้แก้ไขแล้ว

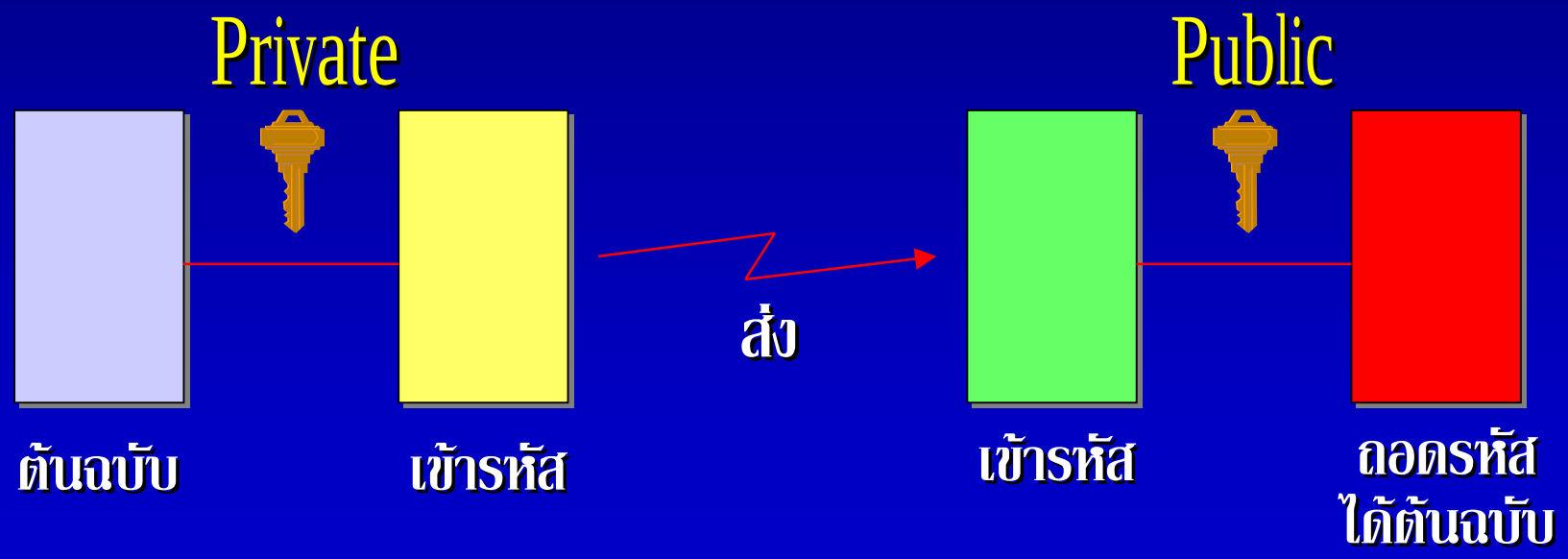
Stop Spam Mail

- อย่าตอบ spam
- ดูว่า spam มาจากไหน
  โดยทั่วไปดูจาก header ได้ ศึกษาวิธีดูหัวจดหมาย
- เขียนบ่นไปที่ ISP ที่ spam ส่ง
- บอก ISP ของคุณเกี่ยวกับ spam
- ใช้ฟิลเตอร์ตัด spam

* สำหรับผู้ติดตั้ง mail sender ต้องป้องกันไม่ให้ผู้อื่นฝากส่งได้

เทคโนโลยีที่เกี่ยวข้อง

ระบบการเข้ารหัสที่ใช้กุญแจแบบ asymmetric หรือกุญแจสองดอก คือ private และ public key



ปัจจุบันการเข้ารหัสที่ใช้

ใน Web server ⟷ Web client

https://

การ stelnet , ssh

การใช้ pgp และ Public key cryptography

ดิจิตอลซิกเนเจอร์

กฎหมายและมาตรการทางสังคม

Principles

Policies & Regulations

Organizational Management Practices

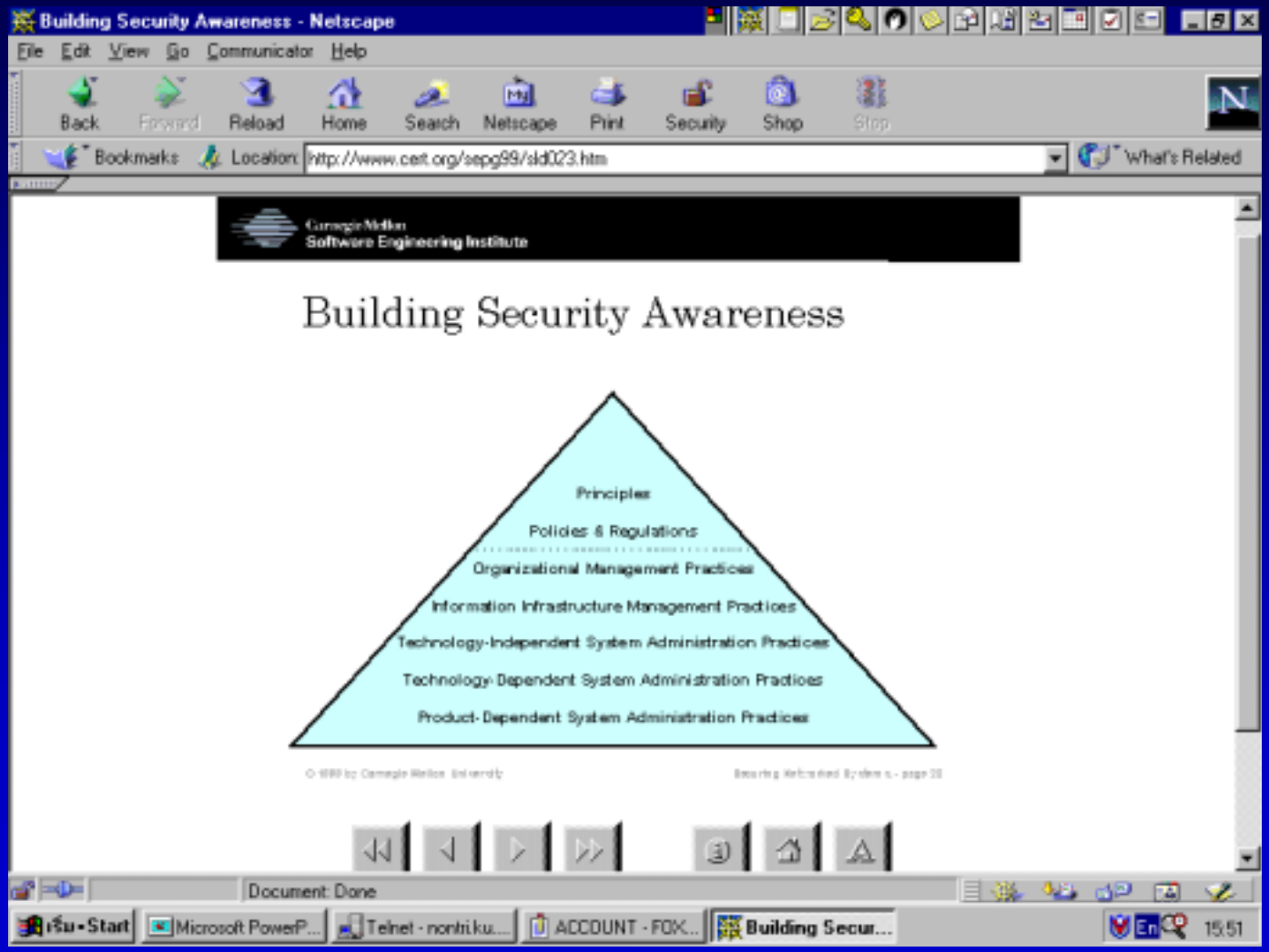
Information Infrastructure Management Practices

Technology-Independent System Administration Practices

Technology-Dependent System Administration Practices

Product-Dependent System Administration Practices

กฎหมายและมาตรการทางสังคม



อนาคต

- การพัฒนาของแฮกเกอร์ โดยเฉพาะการสร้าง tool และเผยแพร่ใน internet
- ข้อมูลที่น่าสนใจใน internet มีทั้งด้านบวกและลบ

  เช่น www.cert.org