การรักษาความปลอดภัย และจริยธรรมคอมพิวเตอร์

ความสำคัญของระบบและข้อมูลคอมพิวเตอร์

การพึ่งพาระบบคอมพิวเตอร์และอินเทอร์เน็ต

- การเงินและการธนาคาร
- การประกันภัย
- การท่องเที่ยว
- การค้าบนอินเทอร์เน็ต
- การวิจัยทางวิทยาศาสตร์
- การทำทะเบียนราษฎร์

ต้องรักษาความปลอดภัยของระบบคอมพิวเตอร์และข้อมูลต่างๆ

ความเสียหายกับระบบคอมพิวเตอร์และข้อมูล

รูปแบบของความเสียหาย

- ฮาร์ดแวร์
- ซอฟต์แวร์
- ข้อมูล

สาเหตุของความเสียหาย

- เหตุสุดวิสัย เช่น ภัยธรรมชาติ อุบัติเหตุ
- ความรู้เท่าไม่ถึงการณ์ของผู้ใช้
- ผู้ประสงค์ร้ายโจมตีช่องโหว่ของระบบคอมพิวเตอร์

ความเสี่ยงต่อความปลอดภัยของคอมพิวเตอร์

- ภัยธรรมชาติ
- อาชญากรรมคอมพิวเตอร์ (Computer Crime)
- การขโมยฮาร์ดแวร์หรือซอฟต์แวร์

จริยธรรมคอมพิวเตอร์

- จรรยาบรรณ
- การประมวลผลโดยอนุรักษ์สิ่งแวดล้อม
- ความเป็นส่วนตัวของข้อมูลสารสนเทศ

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- ฐานความผิดทางอาญา
- อำนาจหน้าที่ของเจ้าหน้าที่ในการป้องกันและปราบปราม
- หน้าที่ของผู้ให้บริการในการจราจรทางคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์

การกระทำโดยตรงกับคอมพิวเตอร์	การใช้คอมพิวเตอร์เป็นเครื่องมือ
• การเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ • การเผยแพร่วิธีเข้าถึงระบบคอมพิวเตอร์ • การดักรับข้อมูล • การรบกวนระบบหรือข้อมูล • การเผยแพร่เครื่องมือ	• การส่งข้อมูลให้ผู้อื่นโดยปกปิดแหล่งที่มา • การนำข้อมูลปลอมและข้อมูลที่ไม่เหมาะสมเข้าสู่ระบบ • ผู้ให้บริการสนับสนุนหรือยินยอมให้กระทำผิด • การเผยแพร่ภาพตัดต่อ

การเข้าถึงระบบและข้อมูลคอมพิวเตอร์

การจำกัดสิทธิในการใช้งาน

- เพื่อจำกัดขอบเขตของความเสียหายที่อาจเกิดขึ้น
- ผู้ใช้ไม่มีสิทธิเข้าถึงข้อมูลของผู้ใช้อื่น
- ผู้ดูแลระบบเท่านั้นที่มีสิทธิในการติดตั้งโปรแกรม

การตรวจสอบผู้ใช้งาน

- การแสดงตนของผู้ใช้งาน (Identification)
- การยืนยันตัวตนของผู้ใช้งาน (Authentication)

การตรวจสอบผู้ใช้งาน

การแสดงตัวตน

- ใช้อ้างอิงว่าผู้ใช้เป็นใคร
- ชื่อนามสกุล ชื่อตำแหน่ง ชื่อผู้ใช้ บัตรประจำตัว

การยืนยันตัวตน

- ถามถึงสิ่งที่ผู้ใช้ตัวจริงเท่านั้นที่ทราบ/มีในครอบครอง
- รหัสผ่าน ลักษณะเฉพาะบุคคล เช่น ลายนิ้วมือ

วิธีการบางอย่างเป็นได้ทั้งการแสดงตัวตนและการยืนยันตัวตน

Backdoor

การเข้าสู่ระบบโดยลัดขั้นตอนการตรวจสอบยืนยันตัวตนผู้ใช้

มักสร้างโดยผู้ดูแลระบบเพื่อลดความยุ่งยากในการตรวจสอบและยืนยันตัวตนเมื่อต้องการเข้าระบบ

บางครั้งก็สร้างโดยผู้ประสงค์ร้ายเพื่ออำนวยความสะดวกให้ตนเองในการเข้าสู่ระบบครั้งต่อไป

Brute force attack

ใช้คอมพิวเตอร์เดารหัสผ่านไปทีละตัว

- ทดลองคำในพจนานุกรม
- ทดลองสลับสับเปลี่ยนตัวเลข

การป้องกัน

- ใช้รหัสผ่านที่เดาได้ยาก

รหัสผ่าน

เป็นวิธีการยืนยันตัวตนอย่างง่าย

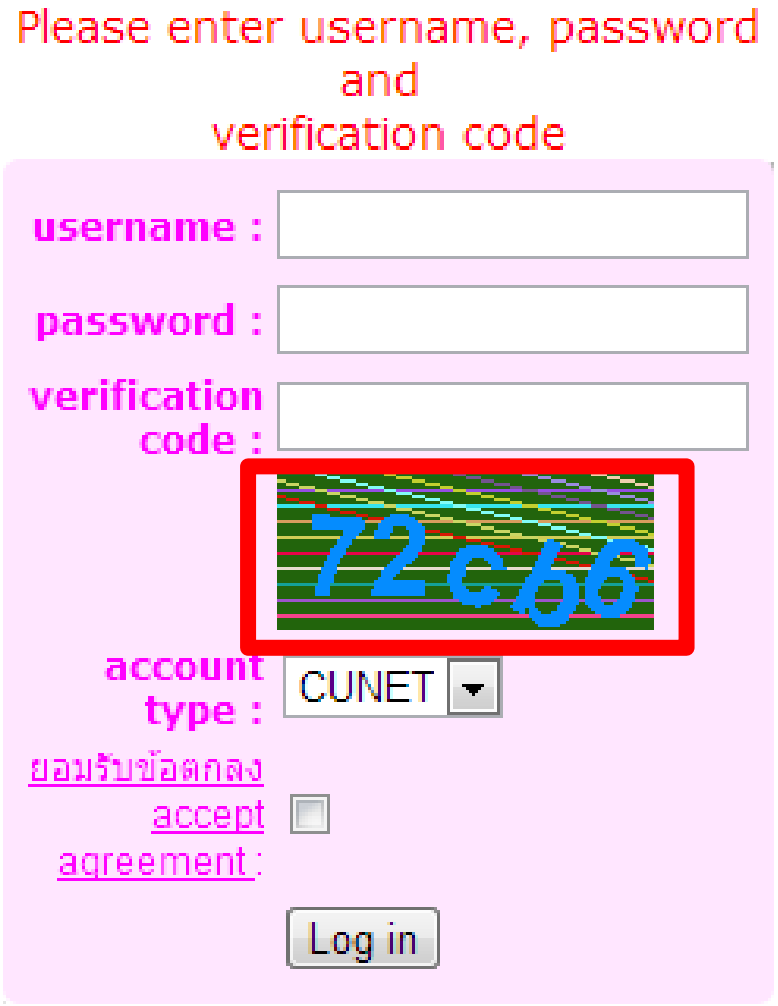
รหัสผ่านที่ไม่ดี

- สามารถเดาได้ง่าย
- วันเดือนปีเกิด หมายเลขโทรศัพท์
- คำทั่วไปในพจนานุกรม
- ตัวเลขจำนวนหลักน้อย ๆ

รหัสผ่านที่ดี

- ใช้ทั้งตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก และตัวเลขผสมกัน
- มีความยาวพอสมควร เช่น 6 ตัวอักษรขึ้นไป

CAPTCHA

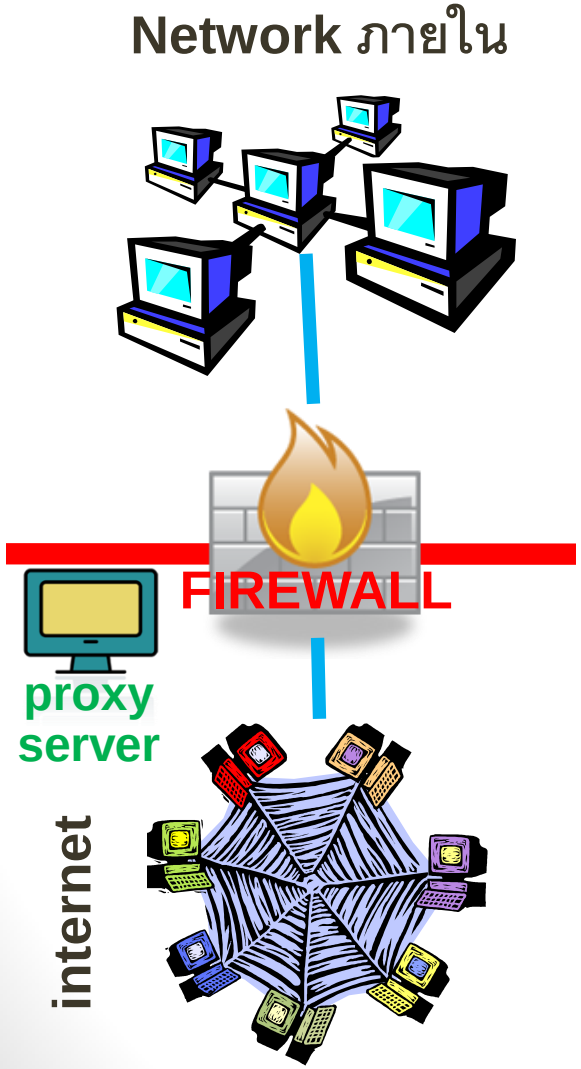


Completely Automated Public Turing test to tell Computers and Humans Apart

แยกแยะการป้อนรหัสโดยคอมพิวเตอร์ออกจากการป้อนรหัสโดยมนุษย์

มนุษย์สามารถตอบคำถามบางอย่างได้ง่ายกว่าคอมพิวเตอร์

Firewall



แยกเครือข่ายภายในออกจากเครือข่ายภายนอก

- เครือข่ายภายในปลอดภัย
- เครือข่ายภายนอกอาจมีผู้ประสงค์ร้ายอยู่

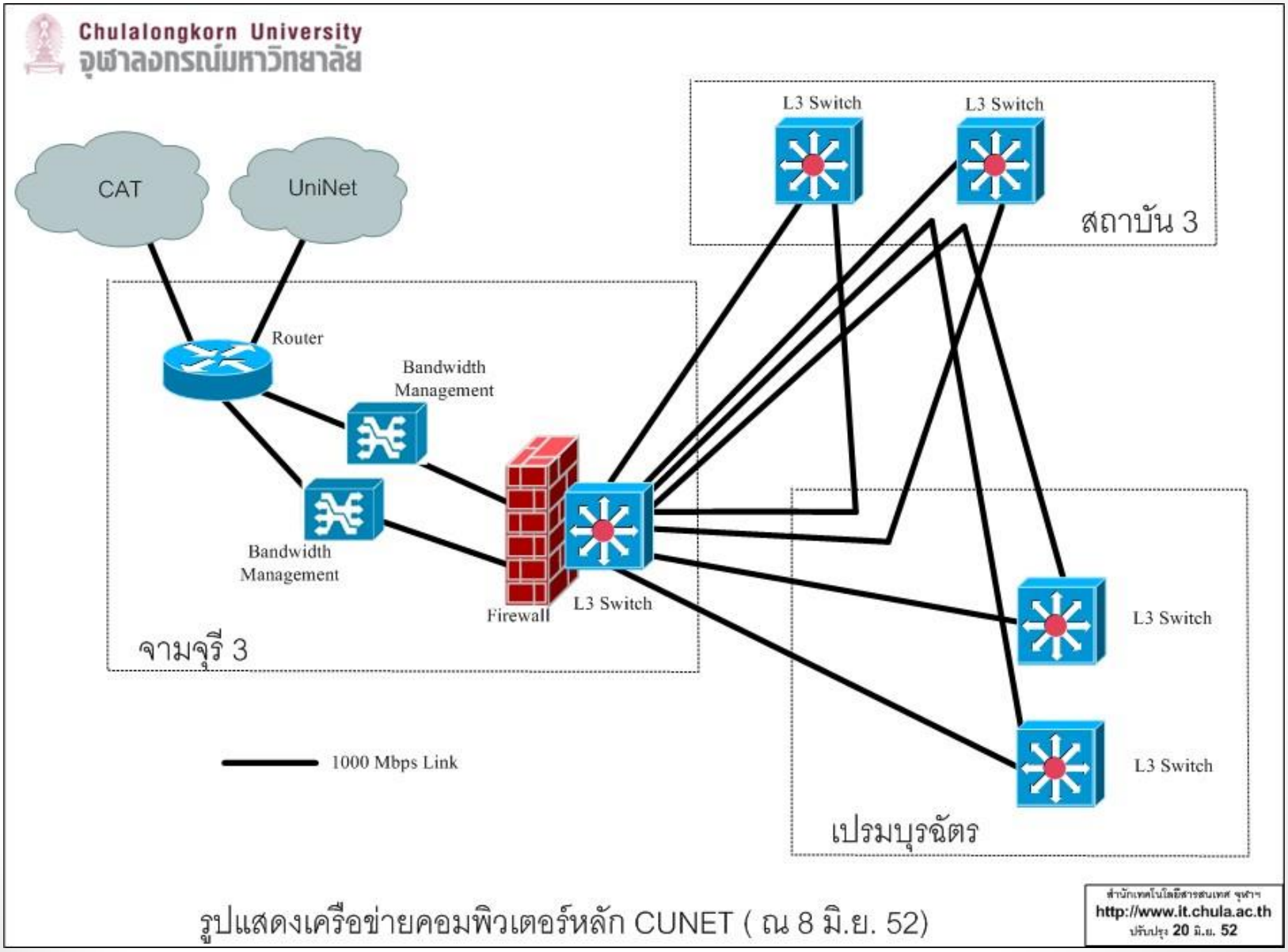
วิเคราะห์รูปแบบการรับส่งข้อมูล

- สกัดกันการรับส่งข้อมูลที่น่าสงสัย

จำกัดการเชื่อมต่อ

- อนุญาตเฉพาะการเชื่อมต่อจากแหล่งที่น่าเชื่อถือเท่านั้น
- อนุญาตเฉพาะบริการที่จำเป็น

Firewall


Chulalongkorn University
จุฬาลงกรณ์มหาวิทยาลัย
CAT
UniNet
Router
Bandwidth Management
Bandwidth Management
Firewall
L3 Switch
จามจุรี 3
L3 Switch
L3 Switch
สถาบัน 3
L3 Switch
L3 Switch
เปรมบุรฉัตร
1000 Mbps Link
รูปแสดงเครือข่ายคอมพิวเตอร์หลัก CUNET (ณ 8 มิ.ย. 52)
สำนักเทคโนโลยีสารสนเทศ จุฬาฯ
http://www.it.chula.ac.th
ปรับปรุง 20 มิ.ย. 52

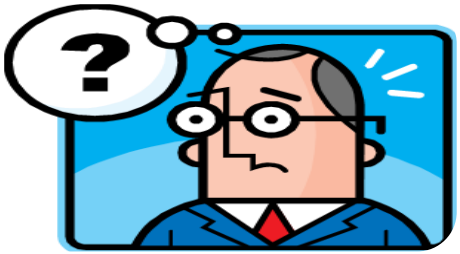
ซอฟต์แวร์เพื่อตรวจจับการบุกรุก

ใช้วิเคราะห์การจราจรของเครือข่าย

ประเมินความเสี่ยงของระบบเครือข่าย

แจ้งการบุกรุกเข้าสู่ระบบและพฤติกรรมที่สงสัยว่าถูกจู่โจม

ใช้ในระบบที่ต้องการการรักษาความปลอดภัยสูง



โปรแกรมมีความยากและซับซ้อนในการใช้งานและวิเคราะห์ผล

มีราคาสูง

Honeypot

คอมพิวเตอร์ที่ไม่มีการรักษาความปลอดภัย

ถูกแยกออกจากเครือข่ายขององค์กร

หลอกผู้บุกรุกว่าเป็นคอมพิวเตอร์ปกติในองค์กร

ให้ผู้บุกรุกโจมตีเข้ามาที่ honeypot ก่อน

รู้วิธีการที่ผู้บุกรุกใช้ในการเจาะและทำลายระบบ

หาทางสร้างการป้องกันระบบ

ใช้ใน Yahoo's และ AT&T

นโยบายการใช้งานระบบ

เพื่อลดความเสี่ยงที่จะเกิดความเสียหายกับระบบคอมพิวเตอร์และข้อมูลขององค์กร

ตัวอย่างนโยบาย

- ใช้ระบบคอมพิวเตอร์เพื่อการทำงานขององค์กรเท่านั้น
- อนุญาตให้เข้าถึงระบบคอมพิวเตอร์อื่น ๆ ภายนอกองค์กรเท่าที่จำเป็น

นโยบายที่จำกัดการใช้งานมากเกินไปก็อาจสร้างความไม่สะดวกในการทำงานได้เช่นกัน

การรบกวนระบบและข้อมูลคอมพิวเตอร์

ความสำคัญของระบบคอมพิวเตอร์

- ระบบถูกออกแบบมาให้รองรับการทำงานตามปกติของผู้ใช้
- หากระบบไม่สามารถทำงานได้ ย่อมเกิดปัญหากับผู้ใช้
  - เช่น ระบบธนาคารไม่สามารถให้บริการฝากถอนเงินได้

ความสำคัญของข้อมูลคอมพิวเตอร์

- ข้อมูลมีมูลค่าในตัวเอง
  - เช่น ความลับทางธุรกิจขององค์กร
- หากข้อมูลเสียหายย่อมเกิดความเสียหายกับองค์กร

มัลแวร์ (Malicious software)

ชุดคำสั่งซึ่งทำสิ่งอันไม่พึงประสงค์สำหรับผู้ใช้

มักทำงานโดยที่ผู้ใช้ไม่รู้ตัว

ตัวอย่างของมัลแวร์

- ไวรัสคอมพิวเตอร์
- หนอนคอมพิวเตอร์
- ม้าโทรจัน

ความเสียหายจากมัลแวร์

หน่วยความจำที่สามารถใช้งานได้ลดลงอย่างมาก

แฟ้มข้อมูลเสียหาย

โปรแกรมหรือแฟ้มข้อมูลหายไป

ปรากฏโปรแกรมหรือแฟ้มข้อมูลที่ไม่รู้จัก

จอภาพแสดงข้อความหรือรูปภาพที่ผิดปกติ

เล่นเพลงหรือเสียงรบกวนเป็นระยะ ๆ

System properties เปลี่ยนแปลงไป

ระบบปฏิบัติการทำงานได้ช้ากว่าปกติ

ระบบปฏิบัติการไม่ทำงาน (เปิดเครื่องไม่สำเร็จ ปิดเครื่องกะทันหัน)

ไวรัสคอมพิวเตอร์

ฝังตัวอยู่ในแฟ้มข้อมูล

ทำลายโปรแกรมที่มันฝังตัวอยู่

ทำลายข้อมูลในคอมพิวเตอร์

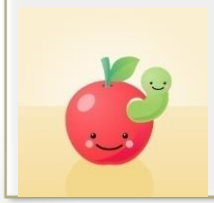
สร้างสำเนาตัวเองได้

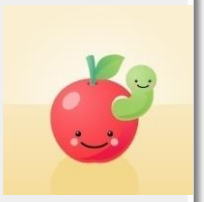
แพร่กระจายเมื่อมีการเรียกใช้ข้อมูลในบริเวณที่มีไวรัส

หนอนคอมพิวเตอร์

คล้ายไวรัสคอมพิวเตอร์

- แพร่กระจายได้





ต่างกับไวรัสคอมพิวเตอร์

- แพร่กระจายด้วยตัวเอง
- ไม่ต้องเรียกใช้งานโปรแกรมหรือแฟ้มข้อมูลที่มี worm

ม้าโทรจัน

ม้าโทรจัน

แฝงในโปรแกรมอื่น

ผู้ใช้คิดว่าเป็นโปรแกรมใช้งาน

- เอกสารที่แนบมากับอีเมล
- โปรแกรมเกม
- โปรแกรมอรรถประโยชน์

ซ่อนคำสั่งที่อันตราย

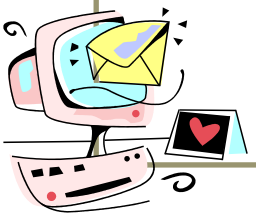
- ลอบเก็บข้อมูลสำคัญต่าง ๆ เช่น ชื่อผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต
- ทำลายข้อมูลในคอมพิวเตอร์ได้

ม้าโทรจันไม่จัดเป็นไวรัส

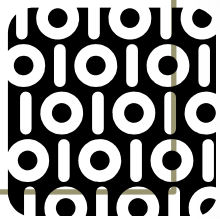
- ไม่แพร่กระจายเอง
- แพร่กระจายโดยผู้ใช้

สาเหตุของการติดมัลแวร์

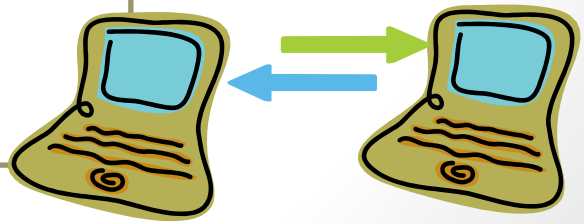
ผู้ใช้เปิดแฟ้มข้อมูลที่ติดมัลแวร์



ผู้ใช้สั่งรันโปรแกรมที่ติดมัลแวร์



เชื่อมต่อคอมพิวเตอร์ที่ไม่มีการป้องกันใด ๆ เข้ากับเครือข่าย



สาเหตุของการติดไวรัส

นำเอาแฟ้มข้อมูลหรือโปรแกรมซึ่งติดไวรัสอยู่ไปใส่ในคอมพิวเตอร์

ดาวน์โหลดไฟล์ซึ่งมีไวรัส

เกิดเหตุการณ์หรือเงื่อนไขที่กำหนด เช่น นาฬิกาของเครื่องคอมพิวเตอร์เดินมาถึงวันที่กำหนดให้มัลแวร์ทำงาน

การป้องกันมัลแวร์

ไม่เปิดแฟ้มข้อมูลที่แนบมากับอีเมลและลบเมลนั้นหากไม่น่าไว้ใจ

- ตรวจสอบการสะกดชื่ออีเมลแอดเดรสและข้อความที่ส่งมาให้ละเอียด

กำหนดระดับความปลอดภัยของมาโคร ให้เตือนเมื่อจะเปิดมาโคร

- มาโคร (Macro) คือคำสั่งที่บันทึกไว้ในซอฟต์แวร์เช่นใน word processor หรือ spreadsheet

ใช้โปรแกรมป้องกันไวรัสและปรับปรุงให้ทันสมัยอยู่เสมอ

ใช้โปรแกรมไฟร์วอลล์ส่วนบุคคล

ติดตามข่าวสารเกี่ยวกับไวรัสใหม่ ๆ และระวังอีเมลหลอกลวงเกี่ยวกับไวรัส

การตรวจจับไวรัสโดยโปรแกรมป้องกันไวรัส

ฐานข้อมูลลักษณะไวรัส (Virus definition)

ปรับปรุงให้ทันสมัยอยู่เสมอ

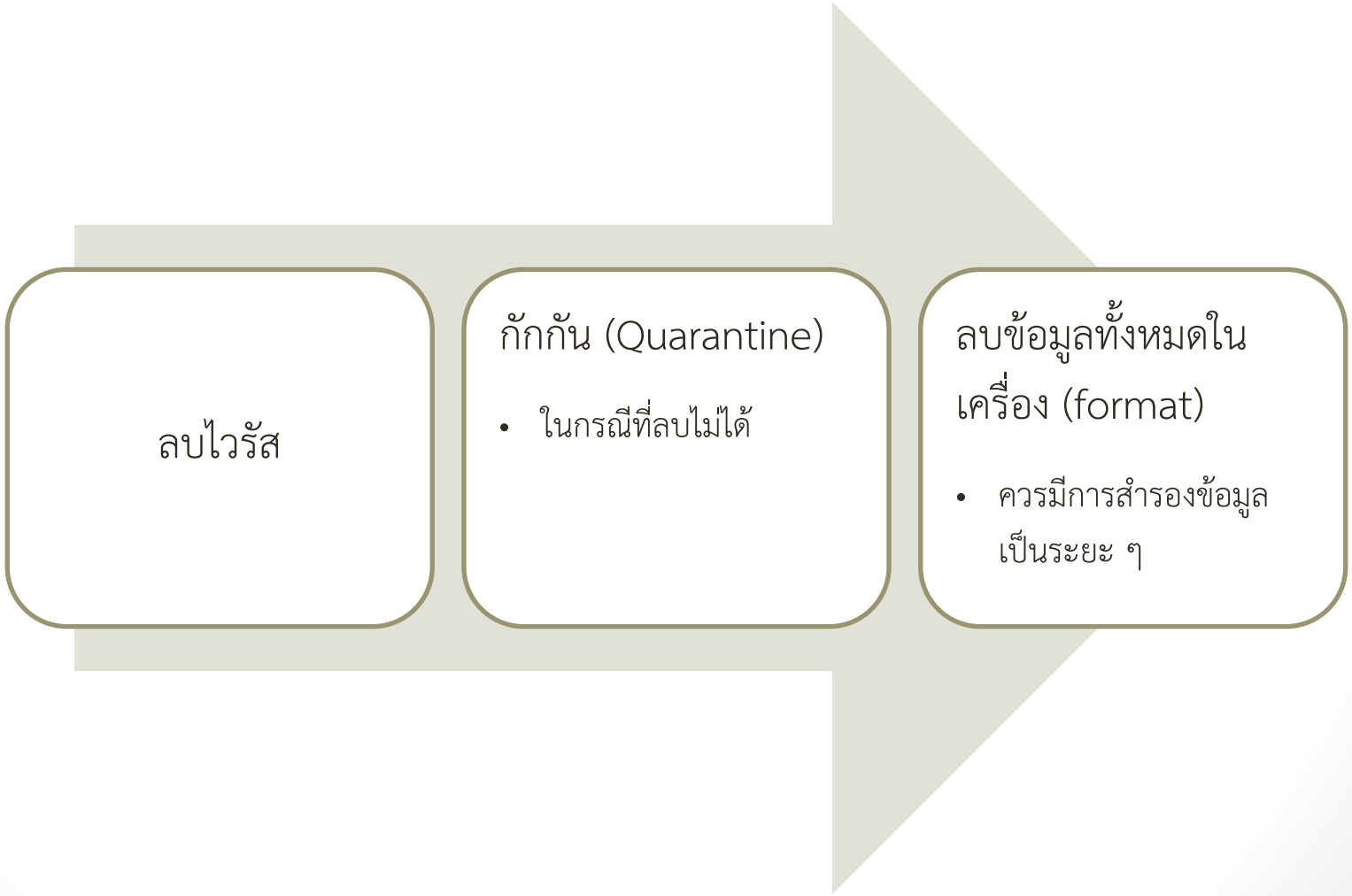
ฟังก์ชันการปรับปรุงอัตโนมัติ

Inoculation file

เก็บรายละเอียดเกี่ยวกับแฟ้มข้อมูล เช่น ขนาด วันที่สร้าง

ตรวจความผิดปกติของแฟ้มข้อมูลจาก inoculation file

การจัดการกับไวรัส



การโจมตีเพื่อปฏิเสธการให้บริการ (Denial of Service: DoS attack)

จำนวนผู้ใช้งานปกติ	ระบบคอมพิวเตอร์ให้บริการได้ตามปกติ
จำนวนผู้ใช้งานมาก	ระบบคอมพิวเตอร์อาจจะไม่สามารถตอบสนองกับผู้ใช้งานทั้งหมดได้
	ผู้ประสงค์ร้ายอาจโจมตีระบบโดยอาศัยช่องโหว่นี้

วิธีการโจมตีเพื่อปฏิเสธการให้บริการ

ระดมส่งข้อมูลปริมาณมากที่ไม่เป็นประโยชน์เข้าสู่ระบบ

- ช่องการจราจรเต็ม การรับส่งข้อมูลปกติทำได้ช้าหรือทำไม่ได้

ส่งแฟ้มข้อมูลขนาดใหญ่ขึ้นไปไว้ในพื้นที่ส่วนกลางจนเนื้อที่เต็ม

- ผู้ใช้อื่นไม่สามารถใช้บริการได้

ลบชื่อผู้ใช้ออกจากระบบ

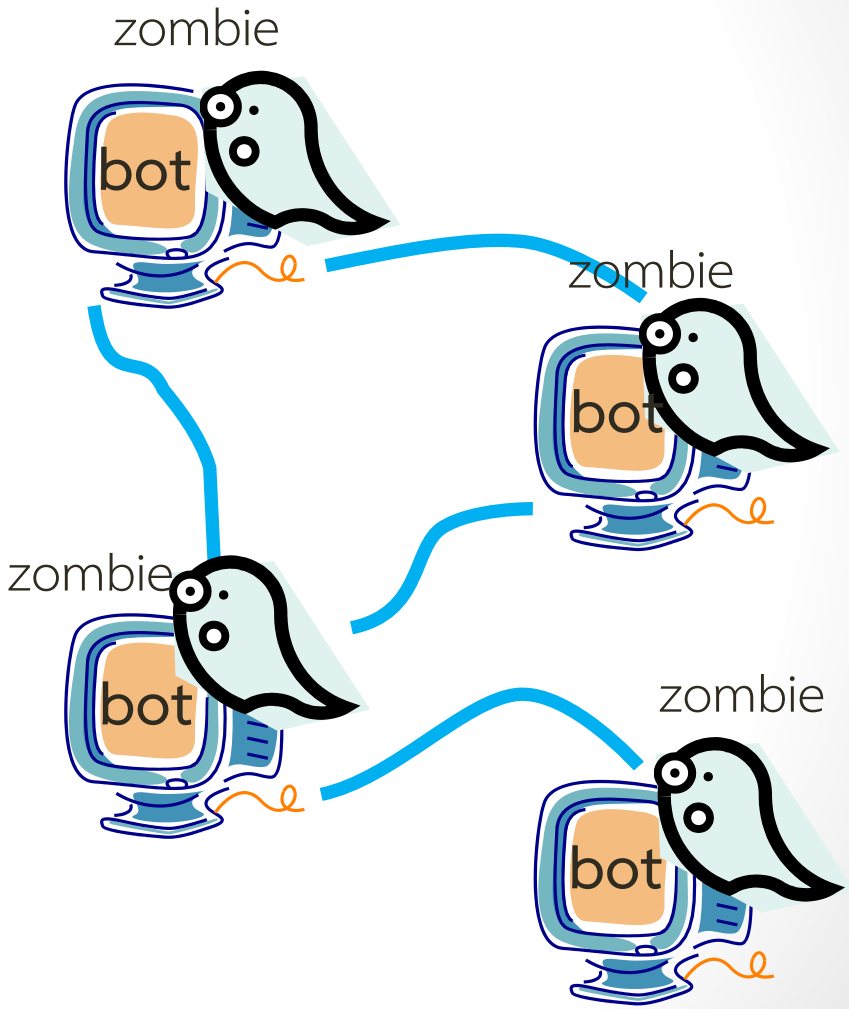
Distributed DoS Attack

อาศัยคอมพิวเตอร์หลาย ๆ เครื่องร่วมกันโจมตีเป้าหมาย

มักอาศัยเครื่องคอมพิวเตอร์ของเหยื่อซึ่งมีการป้องกันอ่อนหรือไม่มีเลยเป็นเครื่องมือ เรียกเครื่องเหยื่อนี้ว่า ซอมบี้

ซอมบี้มักมีการใช้ดิสก์สูง เชื่อมต่อกับเครือข่ายช้ามาก อุปกรณ์ต่อพ่วงไม่ตอบสนอง

บ็อตเน็ตส์ (Botnets) คือ ซอมบี้หลาย ๆ เครื่องในระบบเครือข่าย



การป้องกันการโจมตีผ่านเครือข่าย

Firewall

- แยกเครือข่ายภายในออกจากเครือข่ายภายนอก

Proxy

- ฮาร์ดแวร์ซึ่งเป็นตัวกลางในการรับส่งข้อมูลระหว่างเครือข่ายภายในกับภายนอก
  - Proxy ที่มีคุณสมบัติเป็น firewall สามารถตัดการเชื่อมต่อกับภายนอกที่น่าสงสัยได้
- สำเนาข้อมูลที่มีการเรียกใช้บ่อย (cache) เพื่อลดความหนาแน่นในการติดต่อกับเครือข่ายภายนอก

โปรแกรมโฆษณาและสปายแวร์

โปรแกรมโฆษณา

- ส่งหน้าโฆษณาขึ้นมาให้ผู้ใช้เห็น
- อาจไม่ได้สร้างความเสียหายให้ข้อมูลในระบบ
- สร้างความรำคาญ
- ต้องแบ่งช่องทางการสื่อสารมาให้โฆษณา

สปายแวร์

- เก็บข้อมูลต่าง ๆ ของผู้ใช้ส่งกลับไปให้ผู้ประสงค์ร้าย
  - ข้อมูลส่วนบุคคล หมายเลขบัตรเครดิต
- รบกวนช่องทางการสื่อสาร
- บางชนิดเป็นหนอนคอมพิวเตอร์ด้วย

การดักรับข้อมูล

การขโมยข้อมูล	ลักลอบทำสำเนา มักเกิดร่วมกับการบุกรุกเข้าระบบ
	ดักรับข้อมูลระหว่างการส่งข้ามเครือข่าย
การป้องกัน	ป้องกันการบุกรุกเข้าสู่ระบบ
	เข้ารหัสข้อมูลเพื่อให้ต้นทางและปลายทางที่กำหนดเท่านั้นที่เข้าใจข้อมูล

วิทยาการเข้ารหัสลับ

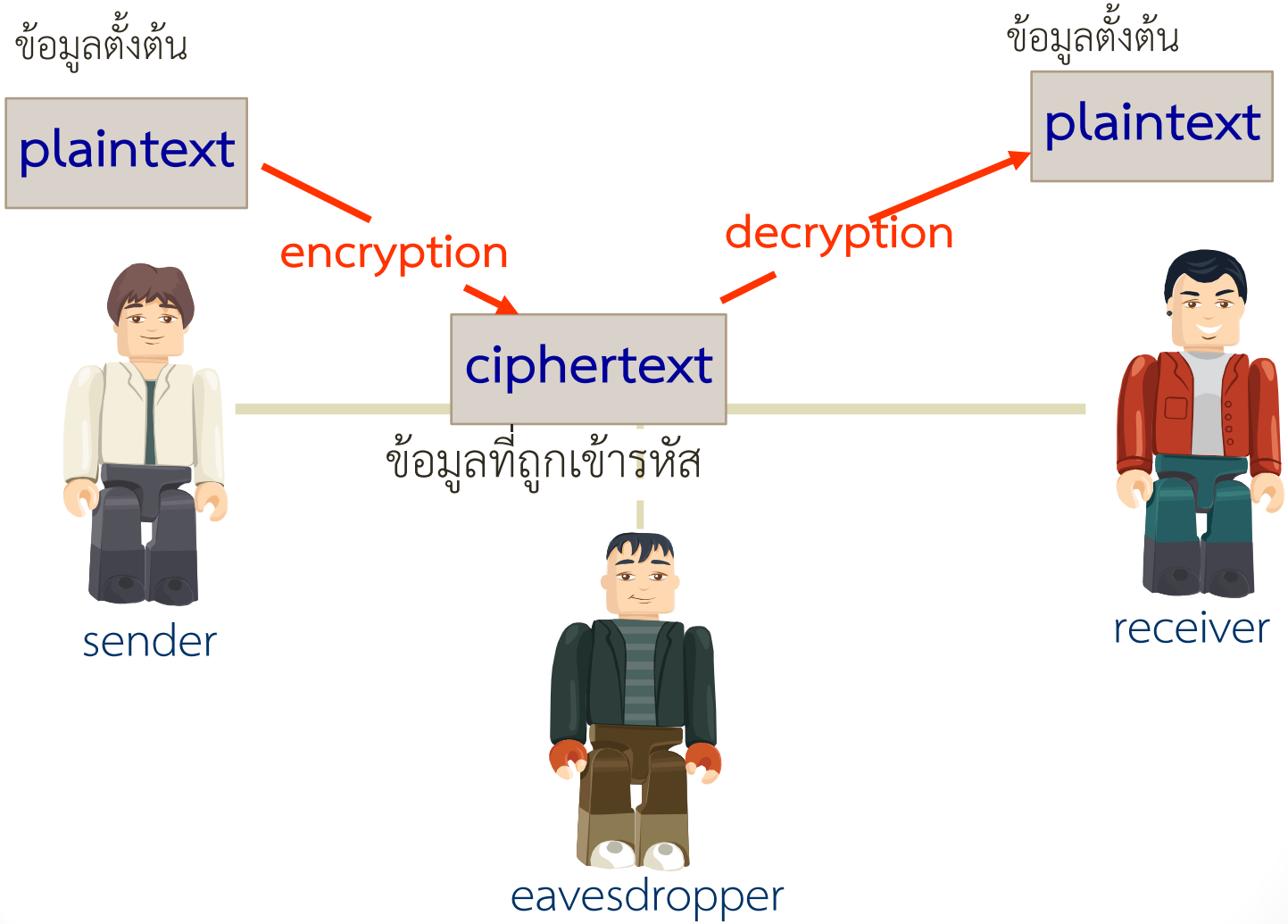
แปลงข้อมูลให้อยู่ในรูปที่ถูกเข้ารหัส

ไม่สามารถเข้าใจข้อมูลได้จนกว่าจะมีการถอดรหัส

ใช้กับข้อมูลที่เป็นความลับ เช่น ข้อมูลด้านการเงิน การธนาคาร การทหาร

มิจฉาชีพก็อาจปิดบังข้อมูลด้วยการเข้ารหัสได้เช่นกัน

วิทยาการเข้ารหัสลับ



การเข้ารหัสโดยใช้กุญแจ

กุญแจสมมาตร

- กุญแจที่ใช้ในการเข้าและถอดรหัสเป็นดอกเดียวกัน
- ถ้าผู้ประสงค์ร้ายได้กุญแจไป ก็จะถอดรหัสได้เช่นกัน

กุญแจอสมมาตร

- กุญแจที่ใช้ในการเข้าและถอดรหัสเป็นคนละดอกกัน
- ไม่มีการส่งกุญแจสำหรับการถอดรหัสให้ผู้อื่น

ตัวอย่างการเข้ารหัสโดยใช้กุญแจสมมาตร

ข้อมูลตั้งต้น

- CODEISSPY

กุญแจ

- การแทนที่ตัวอักษร A-Z ด้วยตัวเลขตามลำดับ เริ่มจาก 10-26 และ 1-9 แล้วแปลงตัวเลขที่ได้กลับมาเป็นตัวอักษร A-Z โดยเริ่มจาก 1-26

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9

CODEISSPY => 12 24 13 14 18 2 2 25 8

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

12 24 13 14 18 2 2 25 8 => LXMNRBBYH

ตัวอย่างการเข้ารหัสโดยใช้กุญแจอสมมาตร

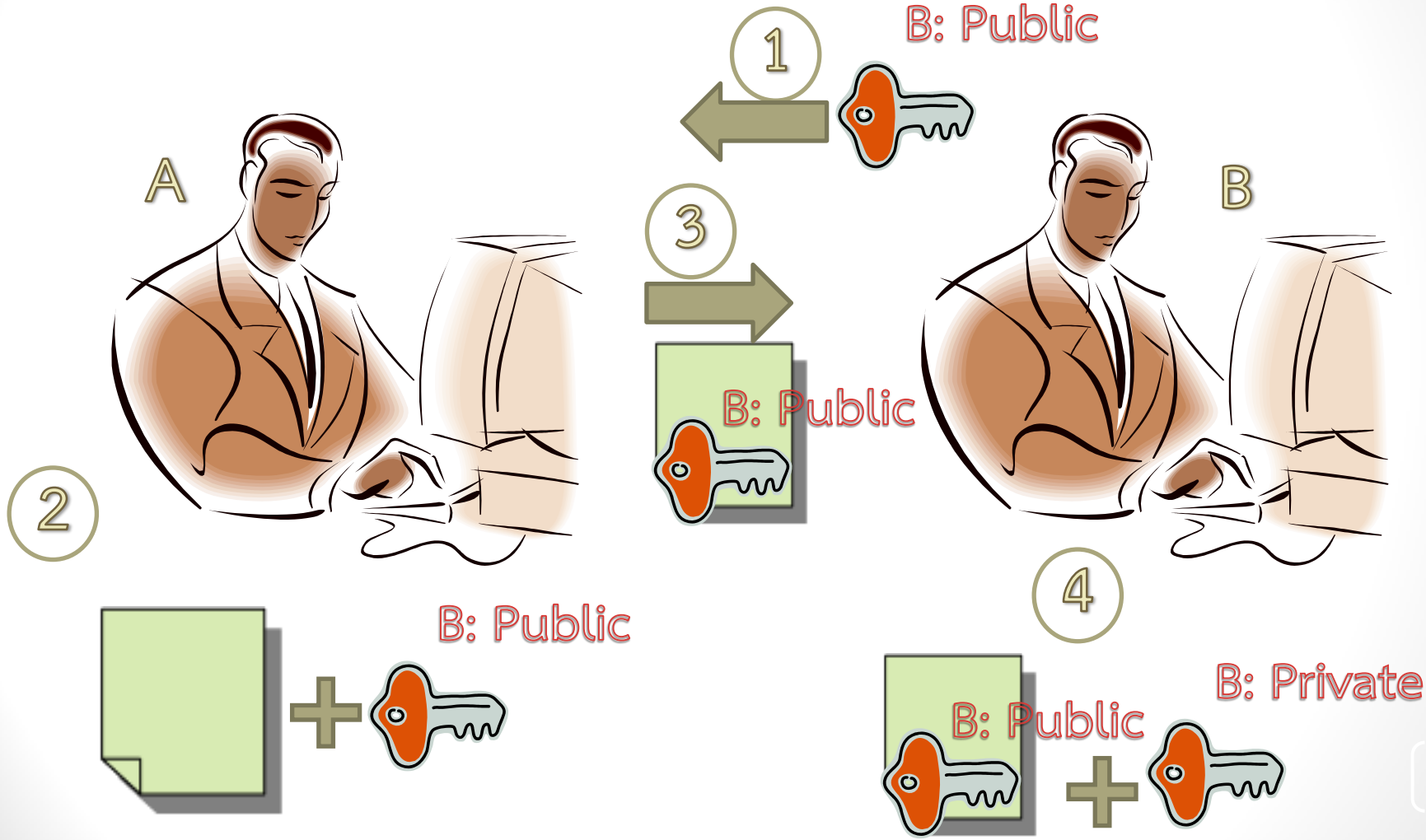
คู่กุญแจสาธารณะและกุญแจส่วนบุคคล

- กุญแจสาธารณะ แจกจ่ายให้บุคคลทั่วไป
- กุญแจส่วนบุคคล เป็นความลับ ไม่มีการส่งให้บุคคลอื่น

เข้ารหัสโดยใช้กุญแจสาธารณะของ**ผู้รับ**

ถอดรหัสโดยใช้กุญแจส่วนบุคคลของ**ผู้รับ**

การรับส่งข้อมูลโดยใช้คู่กุญแจสาธารณะและกุญแจส่วนบุคคล



การปลอมแปลงตัวตน

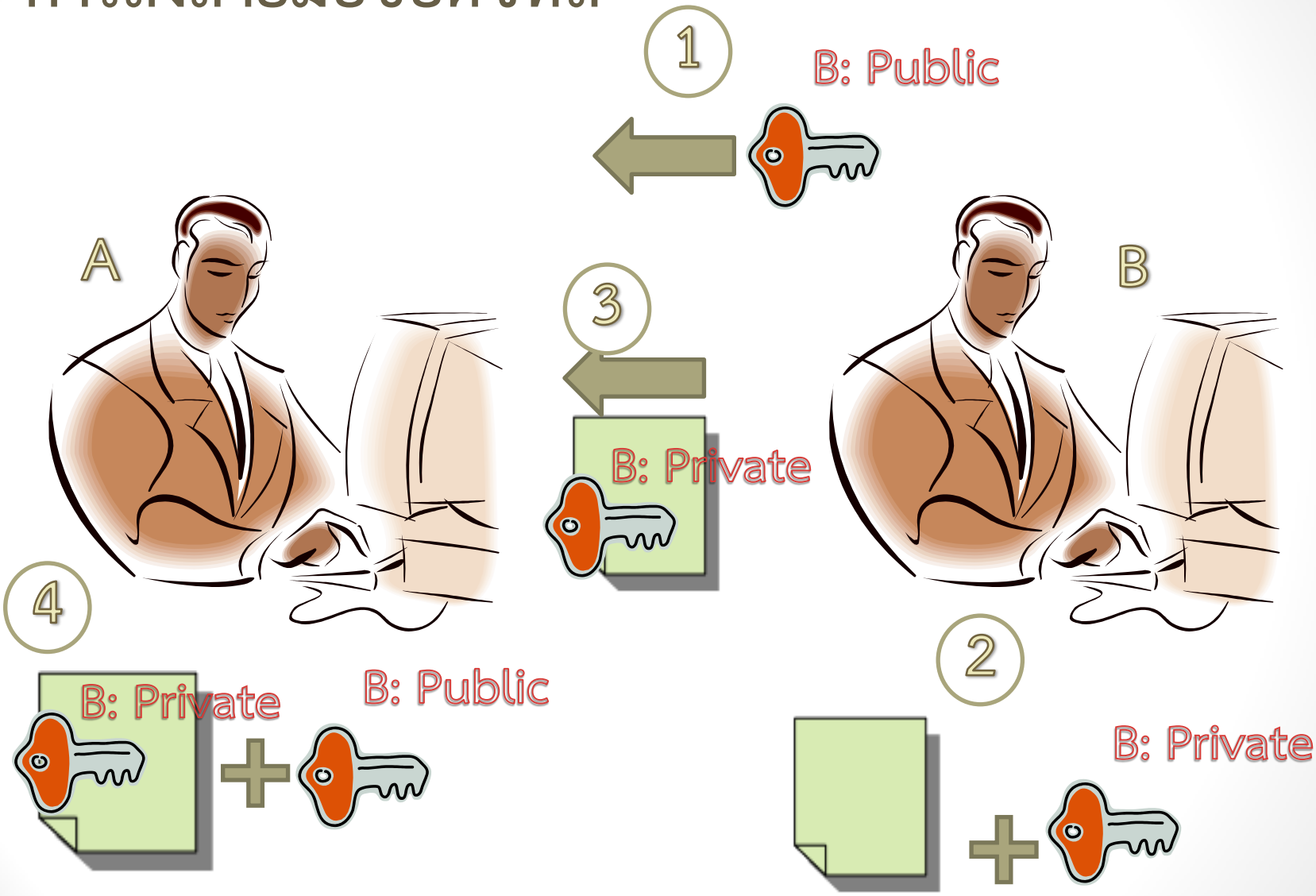
Spoofing

- การปลอมแปลงข้อมูลบางอย่างเพื่อหลอกผู้ใช้ว่ากำลังรับส่งข้อมูลกับผู้อื่นซึ่งเชื่อถือได้

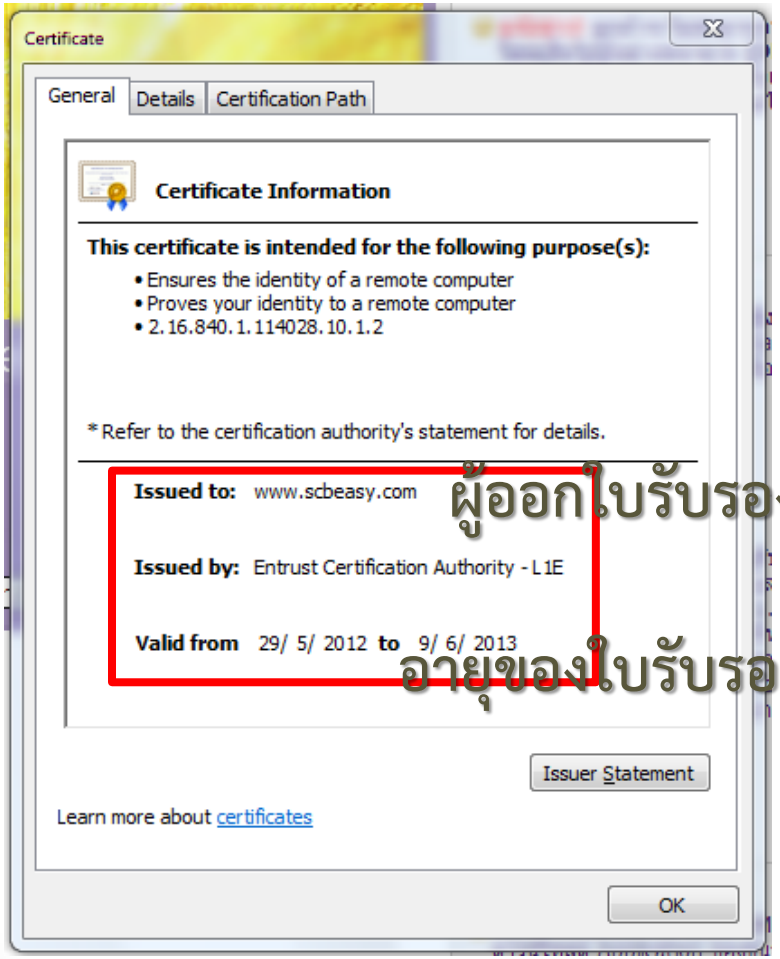
การป้องกัน

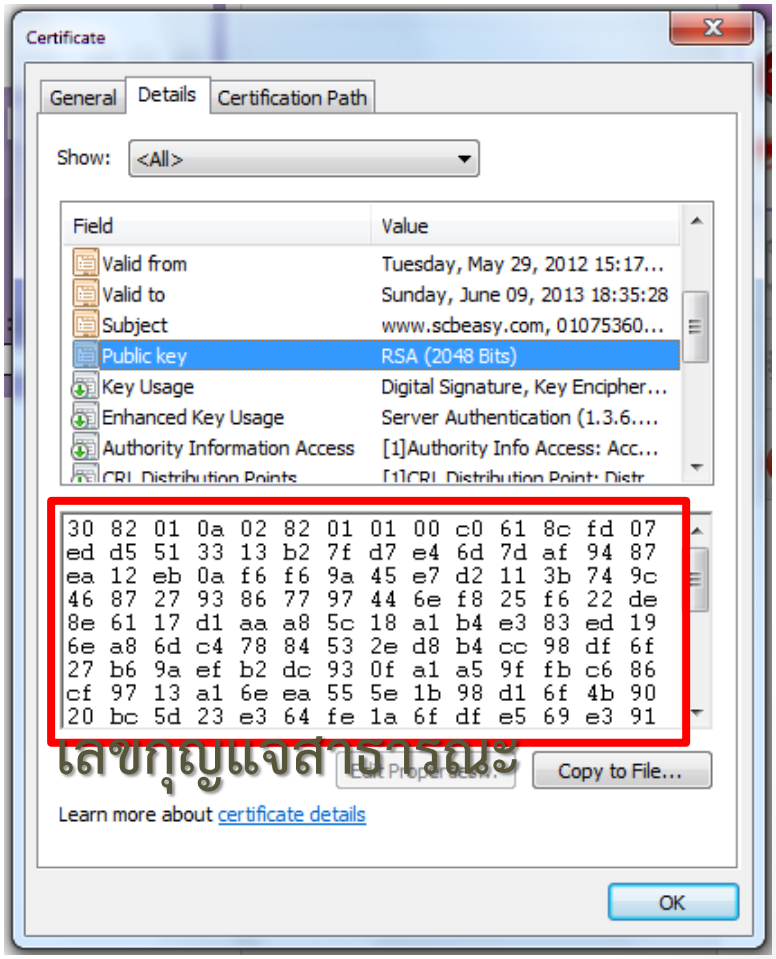
- ลายมือชื่อดิจิทัล
  - ผู้ส่งข้อมูลจะลงลายมือชื่อด้วยกุญแจส่วนบุคคลของ**ผู้ส่ง**
  - ผู้รับข้อมูลจะตรวจสอบตัวตนของผู้ส่งด้วยกุญแจสาธารณะของ**ผู้ส่ง**

การลงลายมือชื่อดิจิทัล



ใบรับรองดิจิทัล





ใบรับรองดิจิทัล

รับรองว่ากุญแจสาธารณะนั้นเป็นของผู้ส่งจริง

บุคคลหรือองค์กรที่ออกใบรับรองนั้นเชื่อถือได้

ข้อมูลในใบรับรองต้องมี

- ชื่อขององค์กรที่ออกใบรับรอง
- อายุของใบรับรอง
- กุญแจสาธารณะของผู้ถูกรับรอง

สแปม

สแปมเมล

- ส่งข้อความที่ผู้รับไม่ต้องการผ่านทางอีเมล มักส่งถึงผู้ใช้หลาย ๆ คนพร้อมกัน
- รบกวนผู้ใช้ เสียเวลาตรวจสอบอีเมล สร้างความรำคาญ
- สิ้นเปลืองช่องทางการจราจรทางคอมพิวเตอร์

การป้องกัน

- ใช้โปรแกรมช่วยกรองสแปม
- อาจให้ลบสแปมทิ้งอัตโนมัติ หรือแยกสแปมไปเก็บในที่เฉพาะ

จริยธรรมคอมพิวเตอร์

จริยธรรม

- คือหลักการว่าด้วยความถูกและผิด ซึ่งถูกนำไปใช้ โดยบุคคลเพื่อช่วยในการตัดสินใจว่าสิ่งใดสมควรหรือไม่สมควรกระทำ

แนวคิดพื้นฐานทางจริยธรรม

- การกระทำใดที่บุคคลตัดสินใจกระทำไปแล้ว บุคคลนั้นย่อมต้องรับผิดชอบต่อผลที่เกิดขึ้นจากการกระทำนั้น (responsibility)

การวิเคราะห์ทางจริยธรรม

- เมื่อนิสิตตกอยู่ในสถานการณ์ที่มีปัญหาทางด้านจริยธรรม นิสิตควรทำเช่นไร ให้ลองทำดังนี้
- ระบุและอธิบายถึงข้อเท็จจริงอย่างแจ่มชัด
  - แยกข้อเท็จจริงออกจากเรื่องเล่า
- ระบุข้อขัดแย้ง หรือภาวะที่กลืนไม่เข้าคายไม่ออก (dilemma)
  - จำไว้ว่าไม่ว่าเราจะหั่นเค้กบางแค่ไหน เค้กก็ยังมีสองด้านเสมอ
- ระบุผู้มีส่วนได้ส่วนเสีย
  - ระบุว่ามีใครบ้างที่มีส่วนเกี่ยวข้อง
- ระบุทางเลือกที่เราสามารถทำได้อย่างสมเหตุสมผล
  - จงประนีประนอม ผลลัพธ์ไม่จำเป็นต้องเป็น ขาว หรือดำ เสมอ
- ระบุผลลัพธ์ที่อาจเกิดขึ้นได้จากแต่ละทางเลือก
  - คาดการณ์ว่าผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร มันจะช่วยให้เราหาคำตอบได้ดีขึ้น

แนวคิดทางจริยธรรม (1)

- Golden rule — do unto others as you would have them do unto you.

ปฏิบัติต่อผู้อื่น ดังเช่นที่ต้องการให้ผู้อื่นกระทำต่อเรา

- Immanuel Kant's Categorical Imperative — if an action is not right for everyone to take, it is not right for anyone.

หากการกระทำนั้นไม่ใช่สิ่งถูกต้องเหมาะสมสำหรับทุกคนที่จะปฏิบัติ มันย่อมไม่ใช่การกระทำที่ถูกต้องเหมาะสมสำหรับผู้ใดเลย

- Descartes' rule of change — if an action cannot be taken repeatedly, it is not right to take at all.

หากการกระทำนั้นไม่สามารถถูกปฏิบัติซ้ำ ๆ ได้ การกระทำนั้นย่อมไม่ควรถูกปฏิบัติเลย

แนวคิดทางจริยธรรม (2)

- Utilitarian Principle — take the action that achieves the higher or greater value.

  จงเลือกการกระทำที่ให้คุณค่าสูงสุดต่อคนหมู่มาก
- Risk Aversion Principle — take the action that produces the least harm or the least potential cost.

  จงเลือกการกระทำที่ก่อให้เกิดผลเสียน้อยที่สุด หรือใช้ต้นทุนน้อยที่สุด
- Ethical “no free lunch” Rule — assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise.

  จงทึกทักเอาว่าวัตถุที่สามารถมองเห็นได้ หรือมองไม่เห็นนั้น ถูกครอบครองโดยคนใดคนหนึ่ง เว้นเสียแต่ว่ามีการประกาศไว้อย่างชัดเจน

ตัวอย่างกรณีศึกษา

- นายไก่อยู่ในทีมที่พัฒนา software สำหรับระบบรถไฟใต้ดิน แต่เกิดปัญหาที่คาดไม่ถึงทำให้งานล่าช้ากว่ากำหนด ผู้บริหารบริษัทต้องการให้ส่งมอบงานตรงตามเวลา เนื่องจากได้เซ็นสัญญาไปแล้วว่าจะส่งงานตามกำหนด ขณะนี้ได้ตรวจสอบ software ไปแล้ว 99 % เหลืออีก 1 % ที่เป็นส่วนที่เกี่ยวข้องกับระบบฉุกเฉิน ทางทีมมีมติเห็นว่าให้ส่งมอบระบบนี้เลยตามที่เซ็นสัญญาไว้ และระหว่างสองสามเดือนแรกที่เปิดใช้ระบบ ค่อยทำการตรวจสอบส่วนที่เหลือควบคู่ไป โอกาสที่ระบบจะเกิดเหตุการณ์ฉุกเฉินมีน้อยมาก สองสามเดือนแรกที่ตรวจสอบน่าจะแก้ bug ได้เสร็จทัน หากมี bug ซ่อนอยู่ หากนิสิตเป็นนายไก่นิสิตจะทำเช่นไร

จรรยาบรรณวิชาชีพ

- องค์กรทางวิชาชีพส่วนใหญ่มีจรรยาบรรณที่สมาชิกขององค์กรพึงปฏิบัติตาม
- ตัวอย่างเช่น ACM (Association for Computing Machinery) ได้กำหนดจรรยาบรรณทางวิชาชีพสำหรับวิศวกรซอฟต์แวร์

ตัวอย่างของ IT codes of conduct

พนักงานจะ

- ไม่ใช้คอมพิวเตอร์ในการทำร้ายหรือให้ร้ายผู้อื่น
- ไม่ก้าวก่ายการทำงานด้านคอมพิวเตอร์ของผู้อื่น
- ไม่ยุ่งเกี่ยวกับแฟ้มข้อมูลทางคอมพิวเตอร์ของผู้อื่น
- ไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรม
- ไม่ใช้ซอฟต์แวร์ที่ผิดกฎหมาย
- ไม่ใช้เครื่องคอมพิวเตอร์หรือชื่อผู้ใช้ของผู้อื่นหากไม่ได้รับอนุญาต
- ไม่ใช้ทรัพย์สินทางปัญญาของผู้อื่นโดยกล่าวอ้างว่าเป็นของตน
- ต้องพิจารณาถึงผลกระทบที่จะมีต่อสังคมในการเขียนโปรแกรม หรือออกแบบระบบงาน
- ใช้คอมพิวเตอร์ด้วยสำนึกรับผิดชอบและเคารพต่อผู้อื่น

ตัวอย่างประเด็นทางจริยธรรมในโลกความเป็นจริง

บุคลากรและบริษัทต้องรับมือกับประเด็นปัญหาทางจริธรรมและทางสังคมในรูปแบบต่าง ๆ เช่น

- บริษัทมีสิทธิ์อ่านอีเมลของพนักงานในบริษัทได้หรือไม่
- พนักงานควรได้รับอนุญาตให้ส่งอีเมลส่วนตัวได้หรือไม่
- พนักงานสามารถเข้าเว็บไซต์สินค้าต่าง ๆ จากเครื่องคอมพิวเตอร์ของบริษัทได้หรือไม่
- บริษัทสามารถใช้เทคโนโลยีควบคุมตรวจสอบการใช้เครื่องคอมพิวเตอร์ในระหว่างปฏิบัติงานได้หรือไม่
- บริษัทมีสิทธิ์ลบเกมส์ไพ่ Solitaire จากเครื่องของพนักงานได้หรือไม่
- หากมีพนักงานบางกลุ่มเล่นเกมส์บน Internet ระหว่างช่วงพักที่ส่งผลให้ network ในบริษัทช้ามาก บริษัทควรทำเช่นไร

The moral dimensions of information systems

- สิทธิด้านสารสนเทศ (Information rights)
- ทรัพยสิทธิ (Property right)
- คุณภาพของระบบ (System quality)
- คุณภาพชีวิต (Quality of life)

สิทธิด้านสารสนเทศ (1)

- สิทธิความเป็นส่วนตัว (Privacy) สิทธิที่บุคคลสามารถอยู่ตามลำพัง (left alone) โดยปราศจากการสอดส่องหรือเข้ารบกวนแทรกแซงจากบุคคลอื่น องค์กรหรือรัฐบาล
- ความเป็นส่วนตัวของข้อมูลสารสนเทศคือความเป็นส่วนตัวในข้อมูลและสารสนเทศส่วนบุคคล นั่นคือเจ้าของข้อมูลมีสิทธิที่จะควบคุมหรือจำกัดขอบเขตของการเก็บและใช้ข้อมูลซึ่งเป็นข้อมูลส่วนบุคคลหรือขององค์กร
  - ปัญหาด้านสิทธิความเป็นส่วนตัว
    - เรื่องความปลอดภัยของการเก็บข้อมูลแบบออนไลน์
    - เรื่องการเก็บข้อมูลการเข้าชมเว็บไซต์และอีเมลเพื่อประโยชน์ในการโฆษณา
    - เรื่องความเป็นส่วนตัวของพนักงานในการใช้คอมพิวเตอร์ขององค์กร
- การยินยอมเป็นลายลักษณ์อักษร (Informed consent) คือการให้ความยินยอม โดยทราบข้อเท็จจริงทั้งหมดที่จำเป็นจะต้องใช้ในการตัดสินใจอย่างมีเหตุผล

สิทธิด้านสารสนเทศ (2)

ประวัติส่วนตัวแบบอิเล็กทรอนิกส์

ผู้ให้บริการมักขอข้อมูลส่วนตัวของผู้รับบริการแลกกับการให้บริการต่างๆ

ผู้เก็บข้อมูลอาจนำข้อมูลส่วนตัวเหล่านี้ไปใช้ในการโฆษณา หรืออาจนำไปขายให้องค์กรอื่น

ผู้เก็บข้อมูลควรอนุญาตเจ้าของข้อมูลก่อนหากต้องการนำข้อมูลไปใช้หรือเผยแพร่ต่อ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล - กำลังอยู่ในขั้นตอนการพิจารณาของรัฐสภา

สิทธิด้านสารสนเทศ (3)

Opt-in vs. Opt-out

- Opt-in
  - การไม่อนุญาตให้เว็บไซต์จัดเก็บและใช้ข้อมูลของลูกค้า เว้นเสียแต่ว่าลูกค้าจะให้การยินยอมแก่เว็บไซต์เหล่านั้น
- Opt-out
  - ทางเว็บไซต์จะจัดเก็บข้อมูลของลูกค้าโดยอัตโนมัติ และหากลูกค้าไม่ต้องการ พวกเขาสามารถเลือกในภายหลังได้ว่าไม่ต้องการให้เก็บข้อมูล

สิทธิด้านสารสนเทศ (4)

คุกกี้คืออะไร

- เป็นวิธีการเก็บข้อมูลการใช้งานของผู้ใช้เว็บ

การทำงาน

- เว็บเซิร์ฟเวอร์สร้างแล้วส่งมาเก็บที่เครื่องของผู้ใช้
- รวบรวมข้อมูลการใช้งานต่างๆ ของผู้ใช้
- ส่งข้อมูลให้เว็บเซิร์ฟเวอร์เมื่อถูกเรียกใช้ และเรียกใช้ได้เฉพาะเว็บเซิร์ฟเวอร์ที่สร้างคุกกี้เท่านั้น
- เว็บเซิร์ฟเวอร์ไม่สามารถควบคุมการทำงานของคอมพิวเตอร์ผ่านคุกกี้ได้

ทรัพยสิทธิ (Property right)

- ทรัพย์สินทางปัญญา (Intellectual property) คือผลลัพธ์จากความพยายามอุตสาหะของบุคคลใด บุคคลหนึ่งในการสร้างสรรค์งานหรือผลิตภัณฑ์ทรงคุณค่า โดยอาศัยประสบการณ์ และวิชาความรู้
- สิทธิบัตร (Patent)
  - หนังสือสำคัญที่รัฐออกให้เพื่อคุ้มครองการประดิษฐ์ (Invention) การออกแบบผลิตภัณฑ์ (Product Design) หรือ ผลิตภัณฑ์อรรถประโยชน์ (Utility Model) ที่มีลักษณะตามที่กฎหมายกำหนด
- ลิขสิทธิ์ (Copyright)
  - ปกป้องการแสดงออกทางความคิดผ่านสื่อใด ๆ เช่น ภาพวาด รูปถ่าย งานปั้น งานเขียน ซอฟต์แวร์ ฯลฯ
- ความลับทางการค้า (Trade Secret)
  - ข้อมูลที่มีค่าทางการค้า ไม่ว่าจะเป็น สูตร กระบวนการ อุปกรณ์ ซึ่งเป็นข้อมูลที่คู่แข่งทางการค้าไม่ทราบ และทำให้บริษัทได้เปรียบในเชิงธุรกิจ
  - เช่น สูตรการผลิตโค้ก อัลกอริทึมที่ใช้ในการจัดลำดับของ Google

คุณภาพของระบบ (System quality)

สาเหตุหลัก 3 ประการที่ทำให้ระบบมีประสิทธิภาพที่แย่คือ

- bug และ ข้อผิดพลาดภายในซอฟต์แวร์
- ความขัดข้องของฮาร์ดแวร์และอุปกรณ์เสริม ที่อาจเกิดจากสาเหตุธรรมชาติ หรือสาเหตุอื่น ๆ
- การป้อนข้อมูลคุณภาพต่ำ หรือมีรูปแบบไม่ถูกต้อง

คุณภาพชีวิต (Quality of life)

เทคโนโลยีส่งผลต่อคุณภาพชีวิตในหลาย ๆ ด้าน รวมถึง

- การสูญเสียงาน: เนื่องจากคอมพิวเตอร์ถูกนำมาใช้แทนที่มนุษย์ หรืองานบางอย่างไม่มีความจำเป็นอีกต่อไป หลังจากการรื้อปรับระบบ
- ความแตกต่างในการเข้าถึงเทคโนโลยีของคนสองกลุ่ม (Digital divide) ทำให้ปัญหาความเหลื่อมล้ำทางสังคมเพิ่มมากขึ้น
- การใช้คอมพิวเตอร์อย่างแพร่หลาย เป็นการเปิดโอกาสให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้มากขึ้น
- การใช้คอมพิวเตอร์นาน ๆ ก่อให้เกิดปัญหาสุขภาพ เช่น
  - Repetitive Stress Injury
  - Computer Vision Syndrome
  - Technostress
- เทคโนโลยีส่งผลให้ขอบเขตระหว่างงาน และชีวิตส่วนตัวแยกขาดจากกันน้อยลง

การประมวลผลโดยอนุรักษ์สิ่งแวดล้อม

ใช้ทรัพยากรในการประมวลผลอย่างคุ้มค่า และคำนึงถึงผลกระทบต่อสิ่งแวดล้อม

ตัวอย่าง

- ใช้ sleep mode
- พิมพ์ draft ด้วยกระดาษใช้แล้วหน้าเดียว และใช้โหมดประหยัดหมึกพิมพ์
- Reuse อุปกรณ์บางส่วนที่ยังใช้งานได้ ไม่ทิ้งทั้งหมด