887130 Platform Technology

Asst. Prof. Patcharin Buayen

ระบบรักษาความปลอดภัยในระบบคอมพิวเตอร์

- แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย
- การโจมตีระบบคอมพิวเตอร์
- ระบบรักษาความปลอดภัย

แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย

การป้องกันและรักษาระบบของระบบปฏิบัติการ

- มีการแบ่งส่วนของระบบปฏิบัติการเป็นลำดับชั้นเป็นการป้องกันไม่ให้ผู้ใช้เข้ามาควบคุมการทำงานของระบบปฏิบัติการ
- มีระบบการป้องกันระบบจากการทำงานผิดพลาดของงานที่กำลังประมวลผลอยู่
- มีระบบการรักษาระบบที่เนื่องมาจากการทำงานของระบบบางส่วนผิดพลาด
- มีระบบการรักษางานที่ทำงานอยู่เมื่อเกิดเหตุการณ์จากภายนอก เช่น ไฟฟ้าตก
- มีระบบการกู้คืนไฟล์ระบบเมื่อระบบปฏิบัติการพบว่า มีการทำงานของระบบที่ผิดปกติ
- มีระบบการรักษาความปลอดภัยของผู้ใช้ ที่เรียกว่า User Account โดยมีการป้องกันด้วยรหัสผ่าน

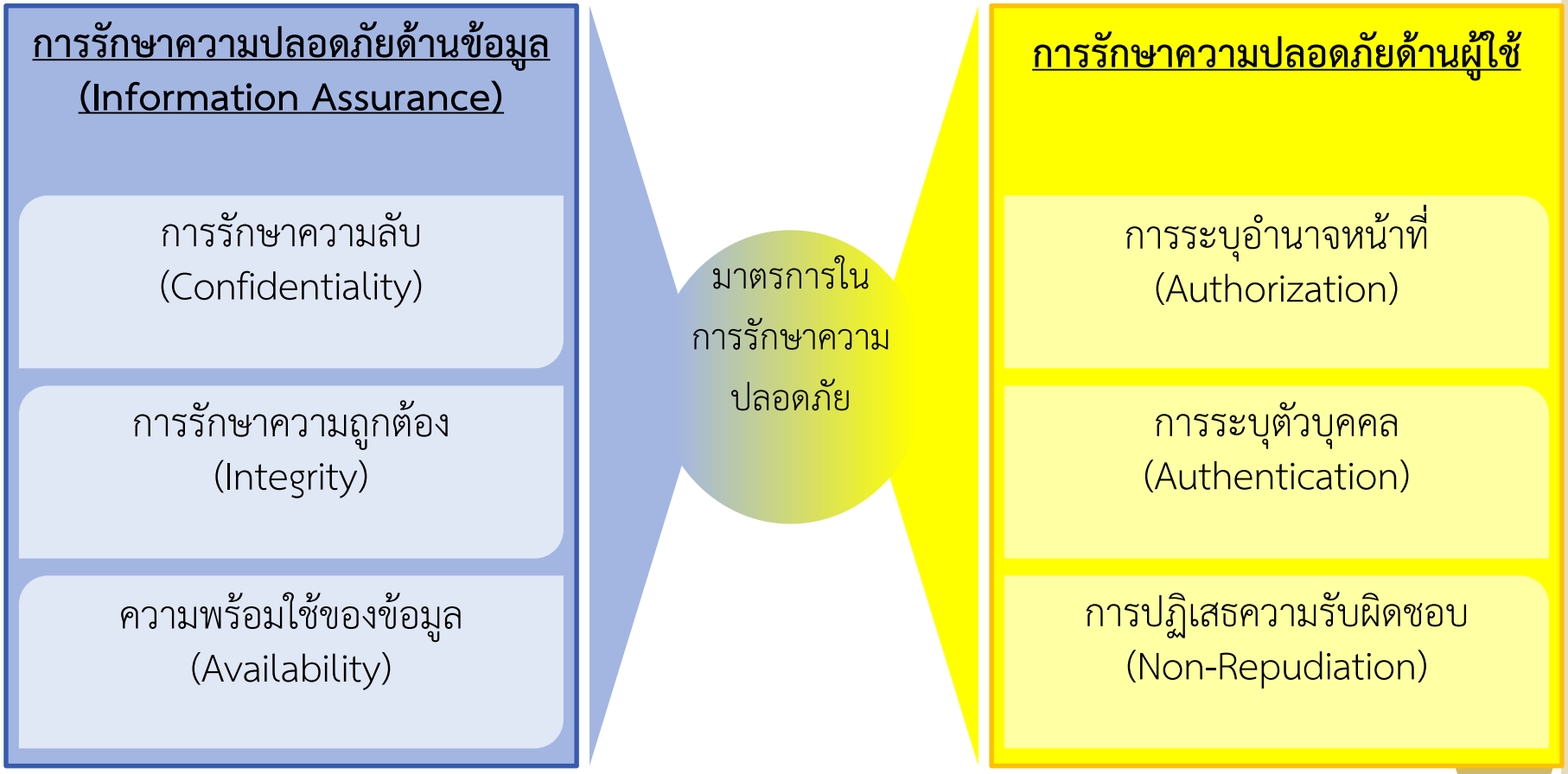
แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย

การป้องกันและรักษาระบบของระบบปฏิบัติการ

- มีการแบ่งส่วนของระบบปฏิบัติการเป็นลำดับชั้นเป็นการป้องกันไม่ให้ผู้ใช้เข้ามาควบคุมการทำงานของระบบปฏิบัติการ
- มีระบบการป้องกันระบบจากการทำงานผิดพลาดของงานที่กำลังประมวลผลอยู่
- มีระบบการรักษาระบบที่เนื่องมาจากการทำงานของระบบบางส่วนผิดพลาด
- มีระบบการรักษางานที่ทำงานอยู่เมื่อเกิดเหตุการณ์จากภายนอก เช่น ไฟฟ้าตก
- มีระบบการกู้คืนไฟล์ระบบเมื่อระบบปฏิบัติการพบว่า มีการทำงานของระบบที่ผิดปกติ

แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย

มาตรการในการรักษาความปลอดภัย



แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย

การรักษาความลับ (Confidentiality)

- เป็นการป้องกันไม่ให้บุคคลอื่นที่ไม่เกี่ยวข้องรู้ข้อมูลสำคัญ
- เครื่องมือที่ใช้คือ การเข้ารหัสข้อมูล (Data Encryption)

การรักษาความถูกต้อง (Integrity)

- เป็นการป้องกันไม่ให้ข้อมูลที่ส่งมาจากผู้ส่งถูกเปลี่ยนแปลงหรือแก้ไขจากผู้ประสงค์ร้าย
- เครื่องมือที่ใช้คือ ลายเซ็นดิจิตอล (Digital Signature)

ความพร้อมใช้ของข้อมูล (Availability)

- เป็นการสร้างความมั่นใจให้กับผู้ใช้ว่า สามารถเข้าถึงข้อมูลของเว็บและใช้บริการได้จริง
- โดยระดับการเข้าถึงข้อมูล จะขึ้นอยู่กับสิทธิ์ในการใช้งานของผู้ใช้แต่ละคน

แนวคิดเบื้องต้นของระบบรักษาความปลอดภัย

การระบุอำนาจหน้าที่ (Authorization)

- เป็นการควบคุมการเข้าถึงข้อมูล (Access) ของแต่ละบุคคลตามอำนาจและสิทธิการใช้
- เครื่องมือที่ใช้ คือ การกำหนดรหัสผ่าน การใช้ Firewall และ Biometrics

การระบุตัวบุคคล (Authentication)

- เป็นการพิสูจน์ตัวตนของผู้ส่งข้อมูล และป้องกันการแอบอ้างของผู้อื่น
- เครื่องมือที่ใช้คือ การกำหนดรหัสผ่าน ลายเซ็นดิจิตอล (Digital Signature) และ Biometrics

การปฏิเสธความรับผิดชอบ (Non-repudiation)

- เป็นการป้องกันการปฏิเสธการรับ-ส่งข้อมูลหรือการทำธุรกรรมต่างๆ
- เครื่องมือที่ใช้ คือ ลายเซ็นดิจิตอล การบันทึกเวลา และการออกใบรับประกันสินค้า

การโจมตีระบบคอมพิวเตอร์

ประเภทของผู้โจมตี (Attacker)

1. **แฮกเกอร์ (Hackers)**
   - สามารถเจาะระบบเพื่ออ่านข้อมูลหรือขโมยข้อมูลสำคัญและโจมตีระบบคอมพิวเตอร์ขององค์กรอื่น
   - เป็นผู้เชี่ยวชาญด้านระบบเครือข่าย และการใช้งานคอมพิวเตอร์
2. **อาชญากรทางคอมพิวเตอร์ (Computer Criminals)**
   - เป็นการขโมยข้อมูลที่ความลับเพื่อไปใช้ในการซื้อสินค้า หรือนำไปขายให้กับองค์กรคู่แข่ง
3. **ผู้ก่อการร้ายทางคอมพิวเตอร์ (Computer Terrorists)**
   - เป็นการใช้ประโยชน์จากระบบเครือข่ายเป็นเครื่องมือในการก่อการร้าย
4. **พนักงานหรือลูกจ้างในองค์กร**
   - เป็นบุคคลภายในองค์กรที่มีความรู้ด้านเครือข่ายเป็นอย่างดี แต่ต้องการทำทุจริต หรือไม่พอใจในองค์กร จึงสร้างความเสียหายให้ระบบ ซึ่ง*ร้ายแรงกว่าการโจมตีจากบุคคลภายนอก*

การโจมตีระบบคอมพิวเตอร์

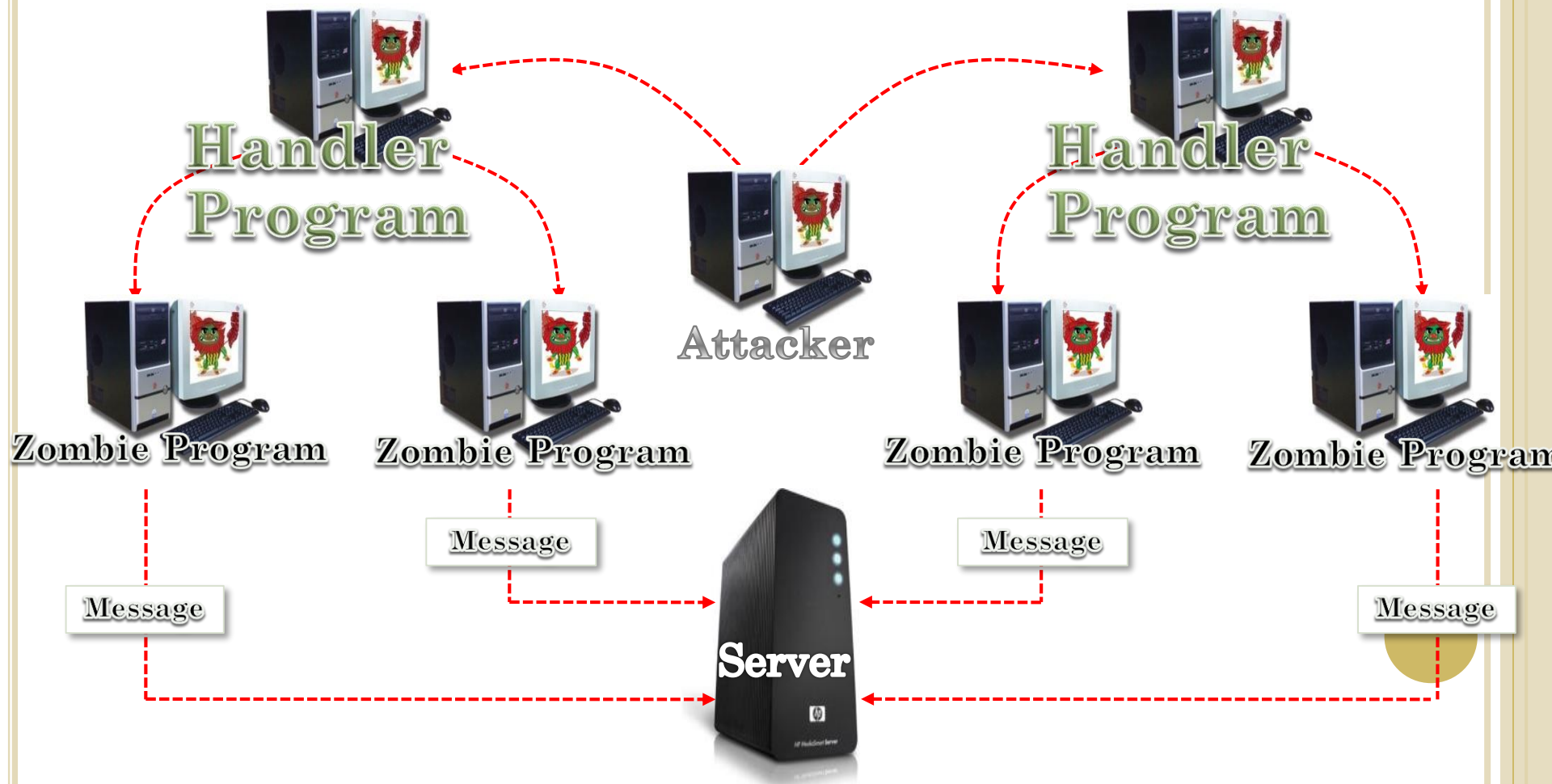
รูปแบบของการโจมตี (Kind of Attack)

1. การโจมตี Server
2. การโจมตี Client
3. การดักจับ Packet หรือ Packet Sniffer
4. การโจมตีแบบ Denial-of-Service Attacks (DoS)
   - การโจมตีโดยส่ง Message หรือ Packet จำนวนมากไปยัง Server จนไม่สามารถให้บริการแก่ Client ได้
   - การโจมตีโดยส่ง Message หรือ Packet เดียว สำหรับทำลายระบบของ Server

Message/Packet Message/Packet Message/Packet

การโจมตีระบบคอมพิวเตอร์

- การโจมตีแบบ Distributed Denial-of-Service Attacks (DDoS)
  - รุนแรงกว่า “การโจมตี Server” และ “การโจมตี Client”
  - ใช้คอมพิวเตอร์มากกว่า 1 เครื่องในการส่ง Message ไปยัง Server พร้อมกัน ทำให้ระบบล่มได้อย่างรวดเร็ว



การโจมตีระบบคอมพิวเตอร์

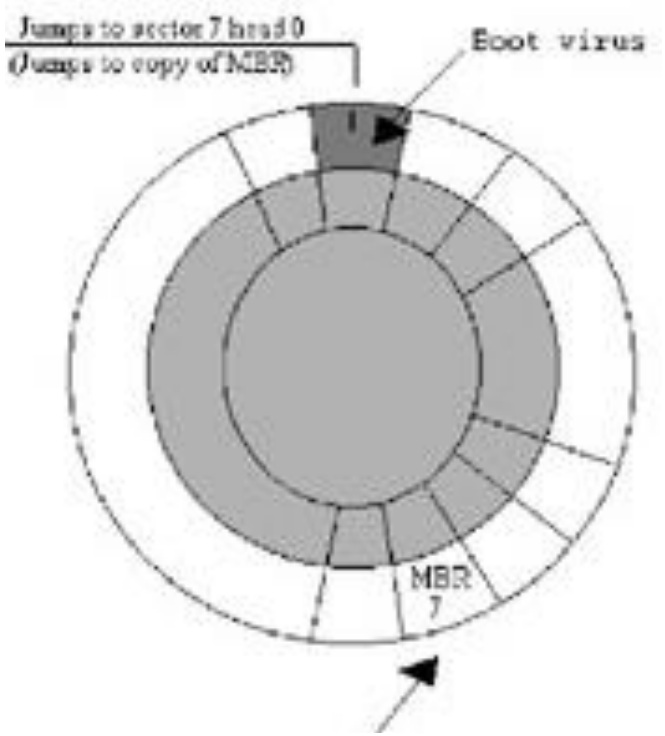
5. การโจมตีจาก Virus, Worm, Trojan horse และ Spam

- Virus : มีลักษณะการทำลายหลายรูปแบบ สามารถแพร่กระจายและสำเนาตัวเอง รวมทั้งการกระจายไปเครื่องอื่นโดยอาศัยตัวกลาง
- Worm : แพร่กระจายในระบบเครือข่าย และไม่จำเป็นต้องอาศัยตัวกลาง
- Trojan horse : จะทำการซ่อนตัวเองในโปรแกรมอื่น (โดยเฉพาะโปรแกรมที่ดาวน์โหลดจากอินเทอร์เน็ต) มีผลทั้งการขโมยข้อมูลและการทำลาย
- Spam (E-Mail bombing) : มีจุดประสงค์เพื่อการโฆษณาผ่าน E-Mail แต่มีการแอบแฝง Virus หรือ Worm หรือ เป็นการส่ง E-Mail จำนวนมากพร้อมๆ กันจนทำให้เกิดปัญหา Mailboxes

การโจมตีระบบคอมพิวเตอร์

- บูตเซกเตอร์ไวรัส (Boot sector หรือ Boot Infector Viruses)

เป็นชุดคำสั่งไวรัสที่ฝังตัวอยู่ในบูตเซกเตอร์ที่เรียกว่า Master Boot Record (MBR) ทำให้ทุกครั้งที่เปิดเครื่อง ไวรัสจะทำงานก่อนที่ระบบปฏิบัติการจะถูกโหลดเข้าสู่หน่วยความจำหลัก



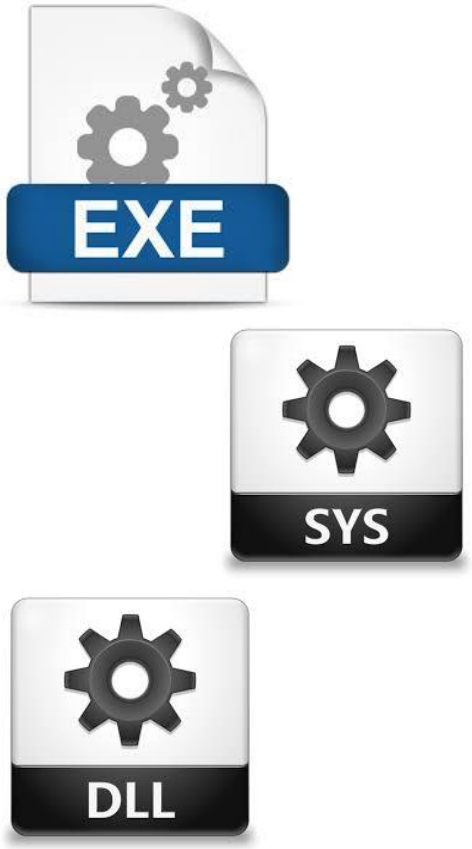
- Macro Virus

เป็นไวรัสที่ก่อกวนไฟล์ประเภทเอกสาร ได้แก่ document และ spread sheet โดยจะขัดขวางการทำงานที่เกี่ยวกับไฟล์เอกสารนั้นๆ อาทิ หยุดการทำงานโดยไม่มีสาเหตุ ทำให้ไฟล์เสียหาย หรือ ไม่ให้ไฟล์เอกสารนั้นๆ สั่งพิมพ์ได้ เป็นต้น

การโจมตีระบบคอมพิวเตอร์

- Program Viruses หรือ File Infector viruses

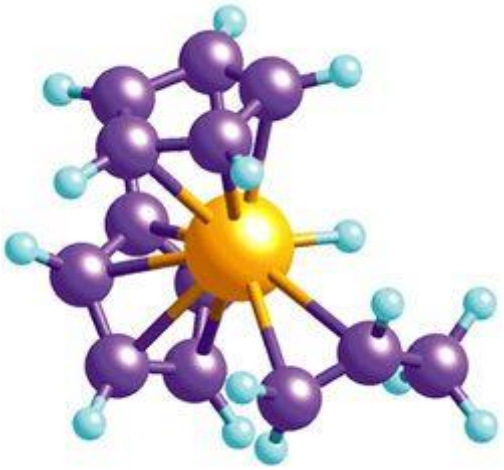
เป็นฝังตัวไปกับไฟล์โปรแกรมที่มีนามสกุล .com, .exe, .sys หรือ .dll ซึ่งเป็นไฟล์สำหรับการประมวลผลหรือไฟล์ระบบ ไฟล์ที่มีคำสั่งของไวรัสชนิดนี้ฝังอยู่จะมีขนาดไฟล์ที่ใหญ่ขึ้นเมื่อทำงาน ทำให้หน่วยความจำของเครื่องคอมพิวเตอร์ไม่เพียงพอสำหรับการทำงาน การแพร่กระจายเกิดจากการที่โปรแกรมที่ไวรัสโดยประมวลผล ซึ่งชุดคำสั่งไวรัสจะคัดลอกไปไว้ในหน่วยความจำ และเมื่อไฟล์ประมวลผลอื่นๆ ถูกประมวลผลต่อ ชุดคำสั่งไวรัสดังกล่าวจะคัดลอกตัวเองไปเป็นส่วนหนึ่งของไฟล์ประมวลผลอื่นๆ ต่อไป



การโจมตีระบบคอมพิวเตอร์

- โพลีมอร์ฟิกไวรัส (Polymorphic Viruses)

เป็นชื่อที่ใช้เรียกไวรัสที่มีความสามารถในการแปรเปลี่ยนตัวเอง ได้เมื่อมีการสร้างสำเนาตัวเองเกิดขึ้น ซึ่งอาจได้ถึงหลายร้อยรูปแบบ ผลก็คือ ทำให้ไวรัสเหล่านี้ยากต่อการถูกตรวจจัดโดยโปรแกรมตรวจหาไวรัสที่ใช้วิธีการสแกนอย่างเดียว ไวรัสใหม่ ๆ ในปัจจุบันที่มีความสามารถนี้เริ่มมีจำนวนเพิ่มมากขึ้นเรื่อย ๆ



- Scripts Viruses

เป็นไวรัสที่มาจากภาษาที่ใช้ในการเขียนโปรแกรม อาทิ javaScript ซึ่งอาจจะเขียนร่วมในไฟล์ของเว็บเพจ

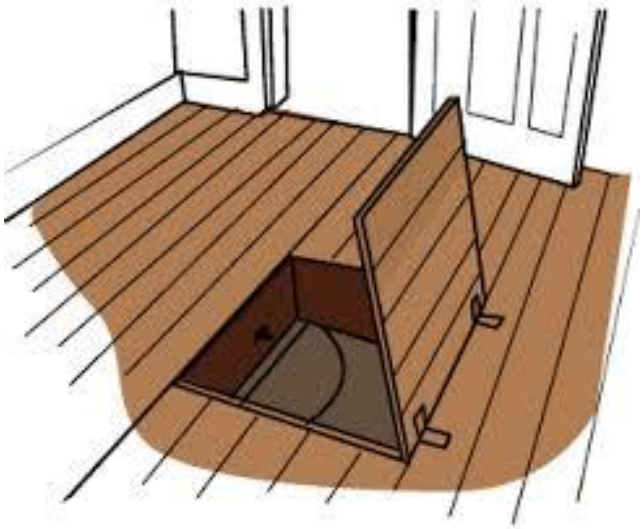
การโจมตีระบบคอมพิวเตอร์

- สทิลต์ไวรัส (Stealth Viruses)

เป็นชื่อเรียกไวรัสที่มีความสามารถในการพรางตัวต่อการตรวจจับได้ เช่น ไฟล์อินเฟกเตอร์ ไวรัสประเภทที่ไปติดโปรแกรมใดแล้วจะทำให้ขนาดของโปรแกรมนั้นใหญ่ขึ้น ถ้าโปรแกรมไวรัสนั้นเป็นแบบสทิสต์ไวรัส จะไม่สามารถตรวจดูขนาดที่แท้จริงของโปรแกรมที่เพิ่มขึ้นได้ เนื่องจากตัวไวรัสจะเข้าไปควบคุมดอส เมื่อมีการใช้คำสั่ง DIR หรือโปรแกรมใดก็ตามเพื่อตรวจดูขนาดของโปรแกรม ดอสก็จะแสดงขนาดเหมือนเดิม ทุกอย่างราวกับว่าไม่มีอะไรเกิดขึ้น

- Trap Door

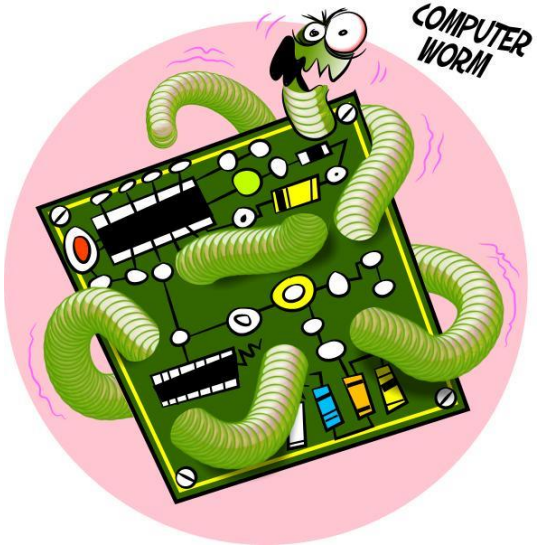
ประตูกับดัก เป็นช่องโหว่ที่ถูกสร้างโดยโปรแกรมเมอร์ของระบบ เพื่อให้ตนเองสามารถเข้าสู่ระบบได้ทุกเมื่อ



การโจมตีระบบคอมพิวเตอร์

- Worm

หนอนคอมพิวเตอร์ จะทำการคัดลอกตัวเองโดยใช้ทรัพยากรของระบบและไม่ให้โปรเซสอื่นๆ ใช้ทรัพยากรของระบบ ทำให้โปรเซสไม่สามารถทำงานได้ ซึ่งการคัดลอกตัวเองนี้สามารถทำให้ระบบคอมพิวเตอร์หรือระบบเครือข่ายไม่สามารถทำงานได้



- Trojan Horse

เป็นไวรัสประเภท Spy ที่มุ่งล้วงความลับของระบบ หรือข้อมูลในเครื่องคอมพิวเตอร์ รวมถึงการทำลายระบบการทำงานของคอมพิวเตอร์ โดยชุดคำสั่งเหล่านั้นจะฝังมากับโปรแกรมที่มักจะแจกฟรีในอินเทอร์เน็ต

ระบบรักษาความปลอดภัยในการติดต่อสื่อสาร

วัตถุประสงค์ของการรักษาความปลอดภัยในการติดต่อสื่อสาร คือ

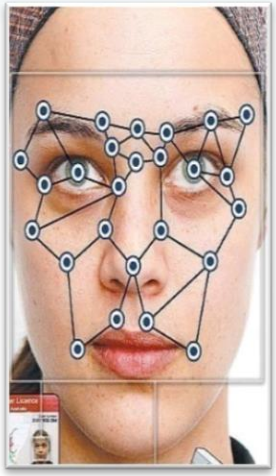
1. เพื่อรักษาความปลอดภัยของข้อมูลที่ส่งผ่านระบบเครือข่าย
2. เพื่อป้องกันผู้แอบอ้างสิทธิ์ในการเข้าถึงข้อมูลที่อยู่ในเครื่อง Client และ Server

ตัวอย่างระบบรักษาความปลอดภัย

- การพิสูจน์ด้านชีวลักษณะ (Biometrics Authentication)
- การเข้ารหัส (Encryption)
- ลายเซ็นดิจิตอล (Digital Signature)
- โปรโตคอล HTTPS (Hypertext Transfer Protocol Security)
- SSL (Security Socket Layer)

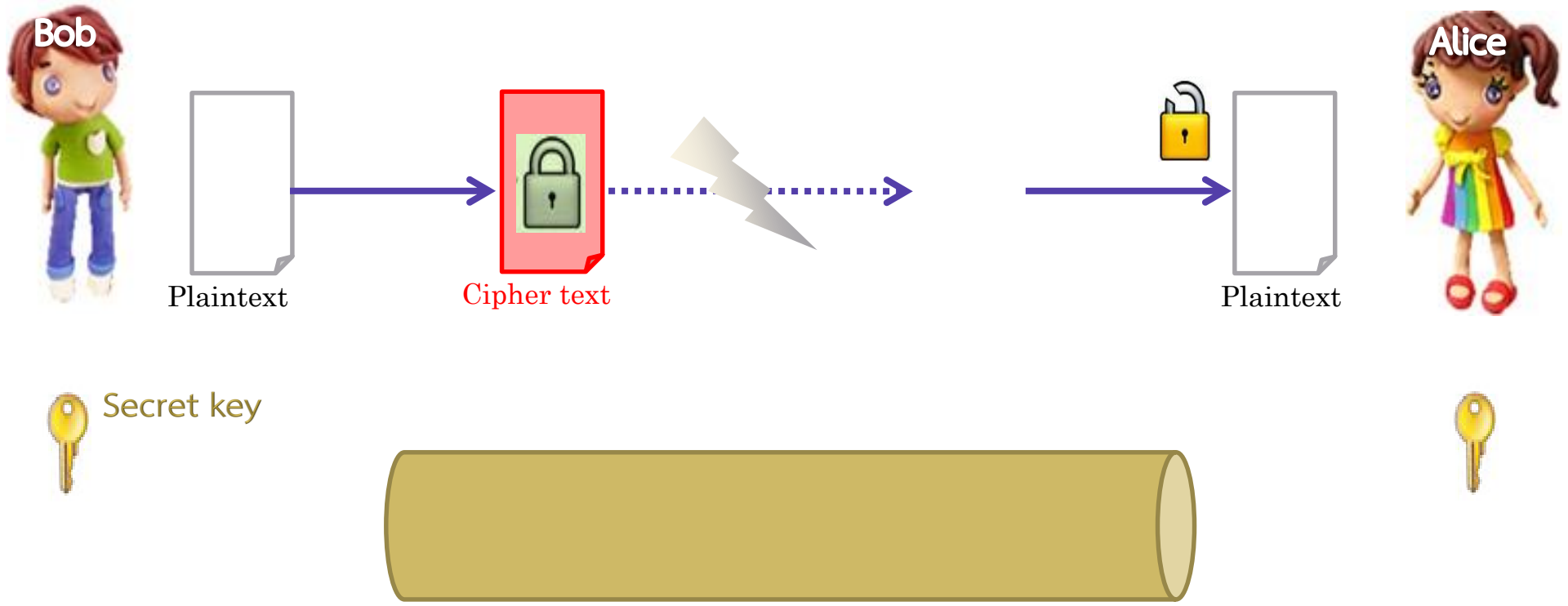
ระบบรักษาความปลอดภัย

- การพิสูจน์ด้านชีวลักษณะ (Biometrics Authentication)

Fingerprint Identification	Iris Identification	Face Identification	Voice Identification
			

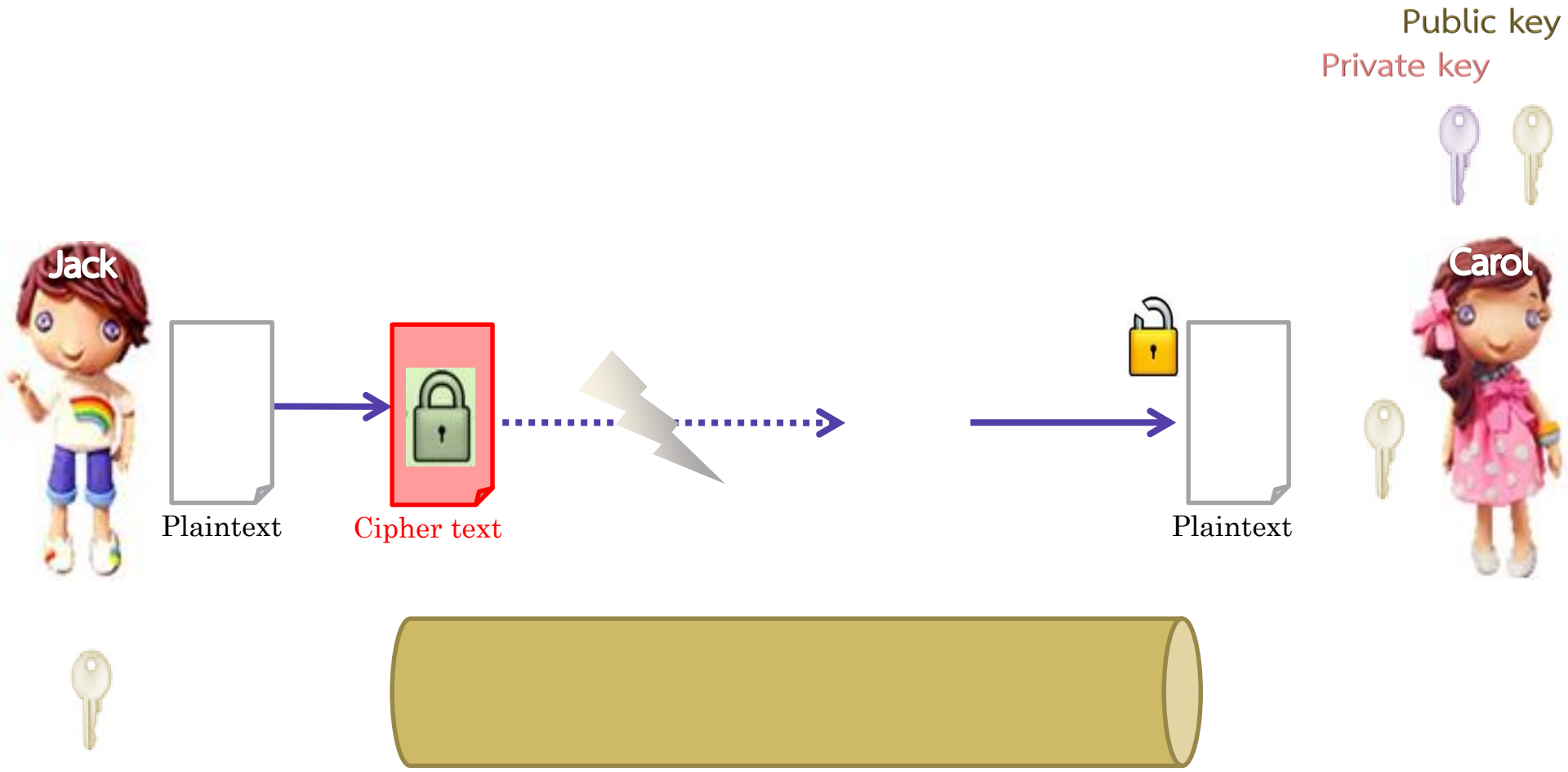
ระบบรักษาความปลอดภัย

- การเข้ารหัส (Encryption)
  - Symmetric Encryption (Secret key Encryption)



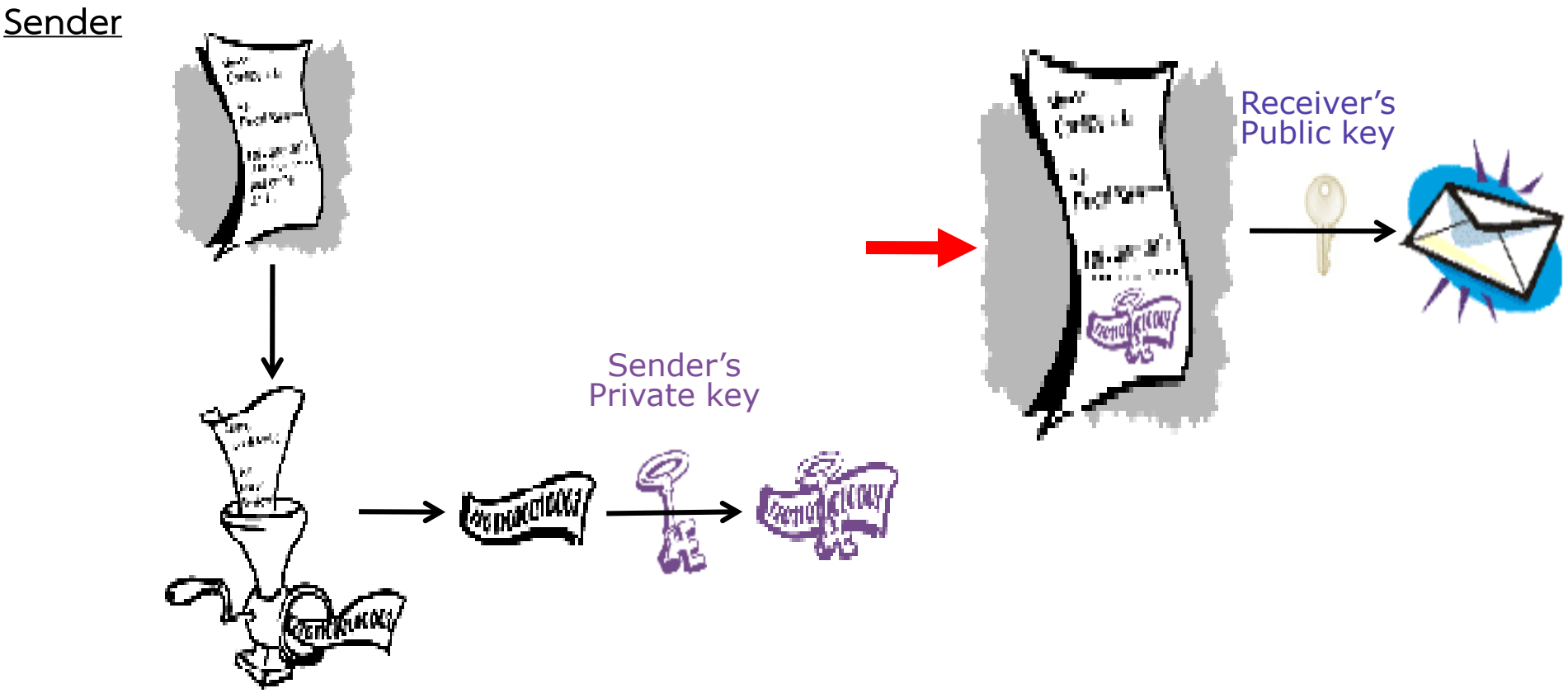
ระบบรักษาความปลอดภัย

- การเข้ารหัส (Encryption)
  - Assymmetric Encryption (Public key Encryption)



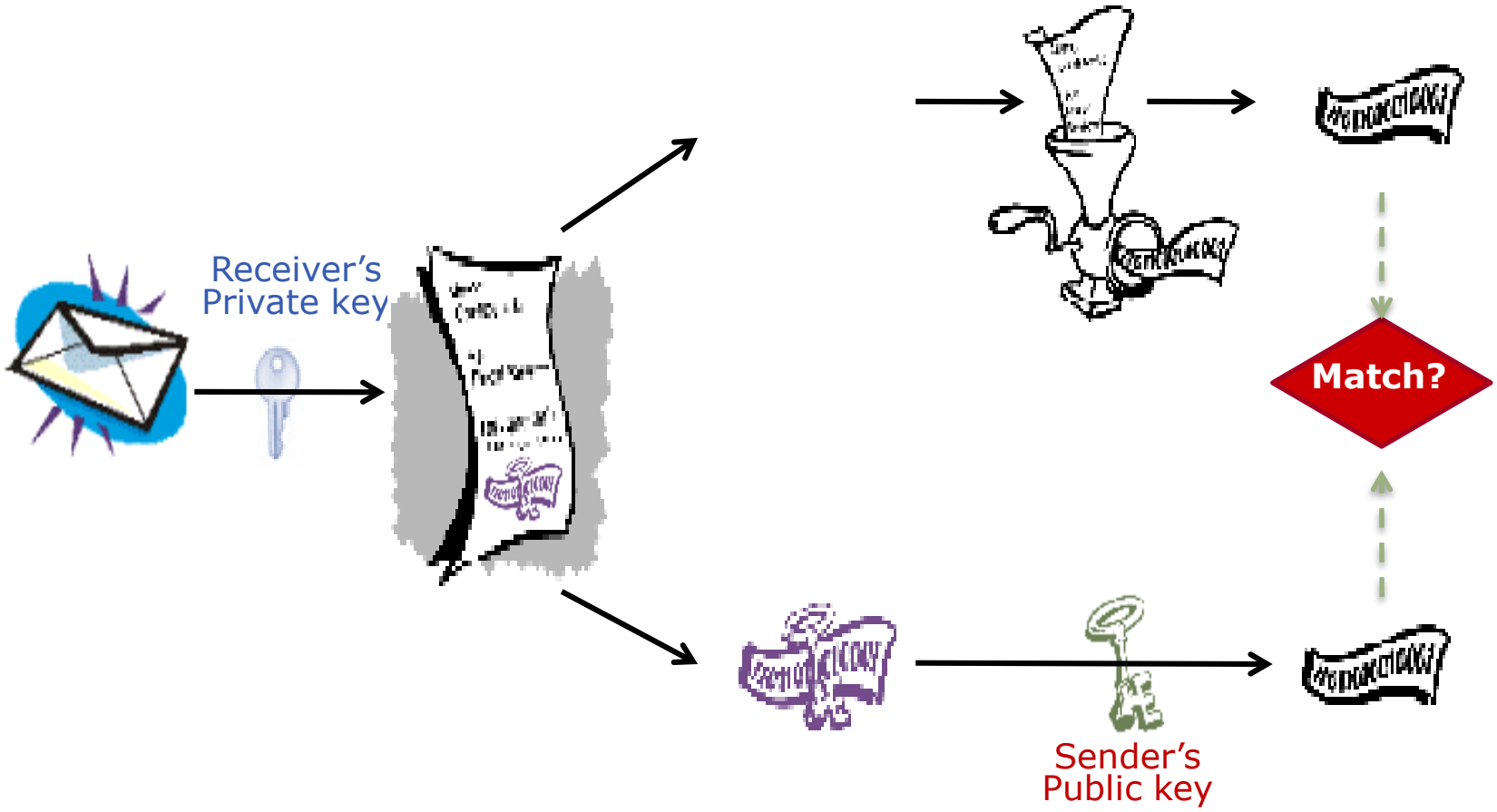
ระบบรักษาความปลอดภัย

- ลายเซ็นดิจิตอล (Digital Signature)



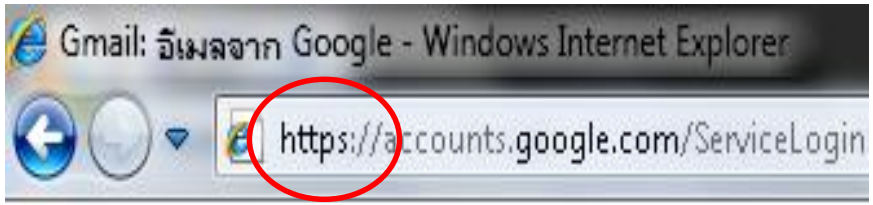
ระบบรักษาความปลอดภัย

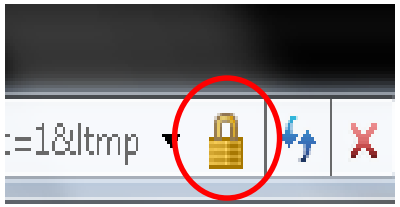
Receiver



ระบบรักษาความปลอดภัย

- โปรโตคอล HTTPS (Hypertext Transfer Protocol Security)





- ช่วยป้องกันการถอดรหัส (Decryption) เพื่อรักษาความลับของข้อมูลผู้ใช้ที่กรอก
- <u>แต่</u> ไม่สามารถป้องกันการแฝงตัวของผู้ประสงค์ร้ายได้

ระบบรักษาความปลอดภัย

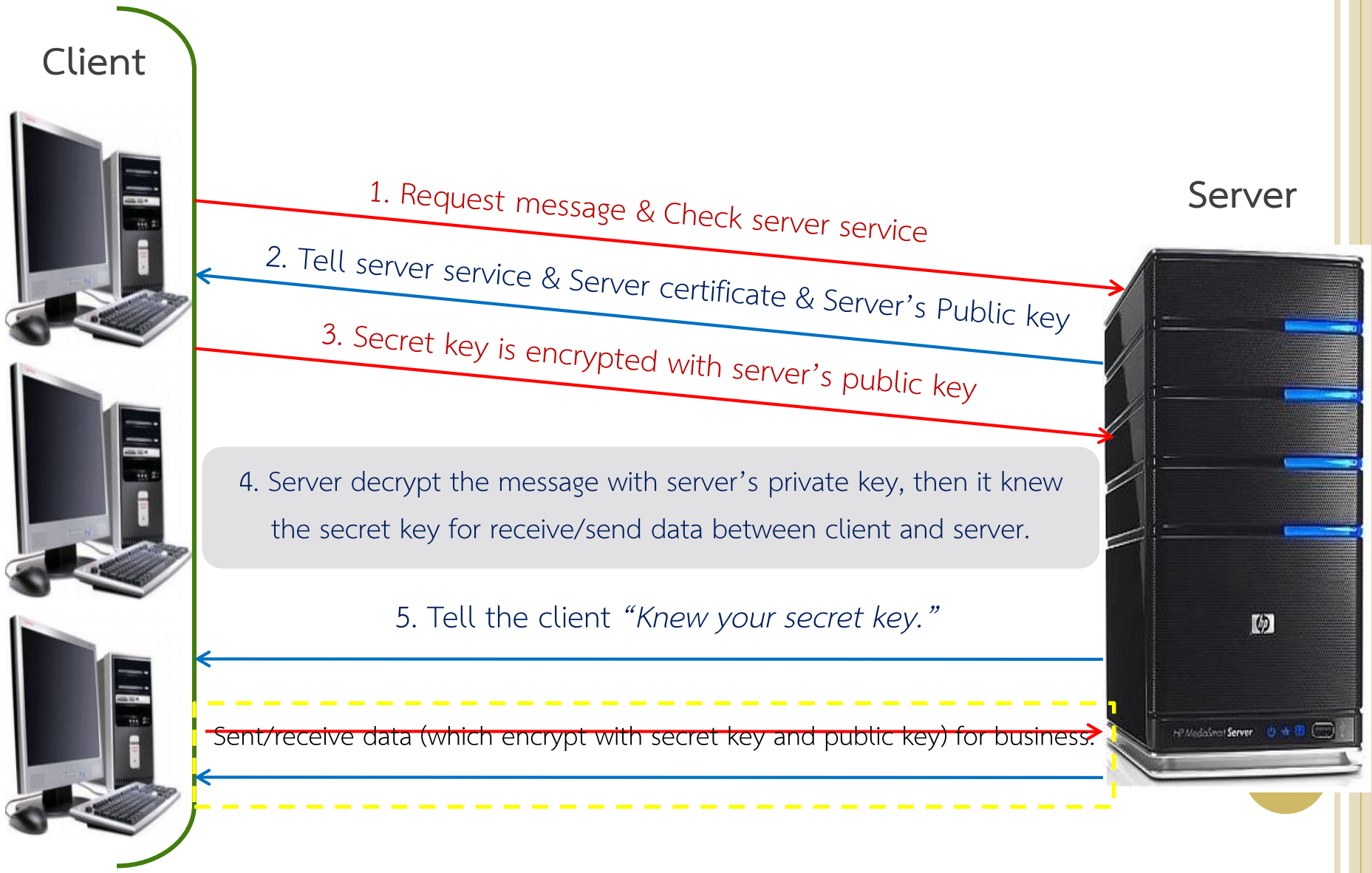
SSL (Secure Socket Layer)

- เป็นโปรโตคอลที่เพิ่มความปลอดภัยในการรับส่งข้อมูลผ่านระบบเครือข่าย ทำให้เราสามารถส่งข้อมูลที่เป็นความลับเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตผ่านระบบเครือข่ายได้ด้วยความปลอดภัย
- นอกจากผู้ส่งและผู้รับข้อมูลแล้วไม่มีใครในระบบเครือข่ายสามารถดึงข้อมูลที่เป็นความลับไปใช้ได้
- ทำงานที่ TCP/IP Layer (application layer และ transport layer) จึงสามารถเรียกอีกชื่อว่า “TLS (Transport Layer Security)”

ประโยชน์ของการใช้ SSL

- Authorization
- Confidentiality
- Authentication
- Integrity

ระบบรักษาความปลอดภัย



ระบบรักษาความปลอดภัย

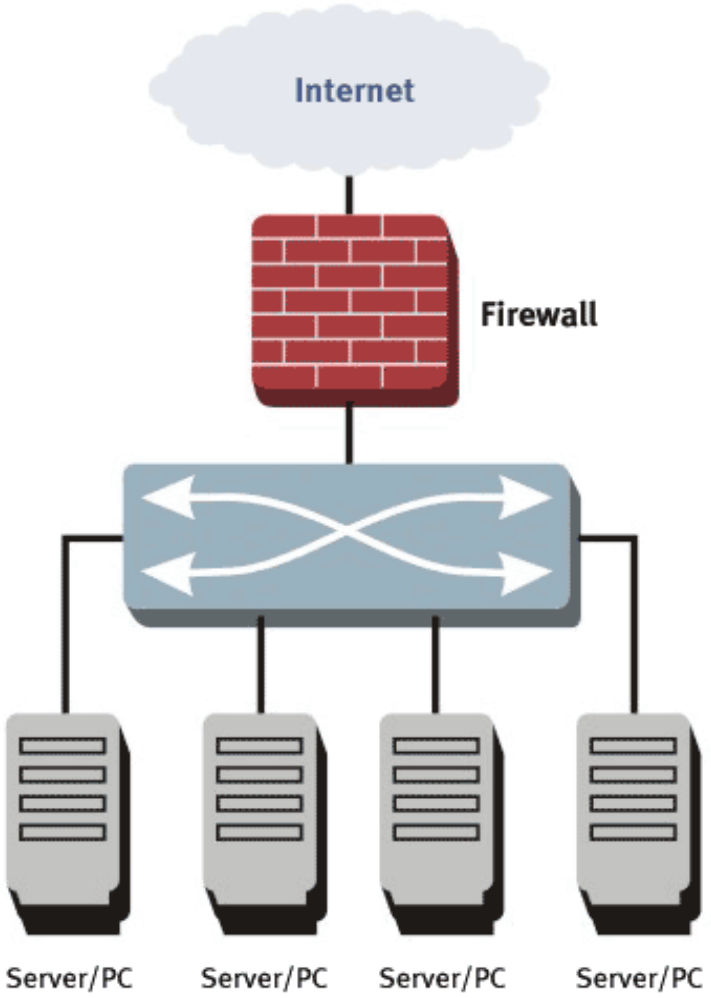
ระบบรักษาความปลอดภัยบนเครือข่าย

Firewall

เป็นเสมือนกำแพงหรือกองทหารป้องกันการโจมตีหรือการบุกรุกจากนอกองค์กร

Firewall มี 3 ชนิด ได้แก่

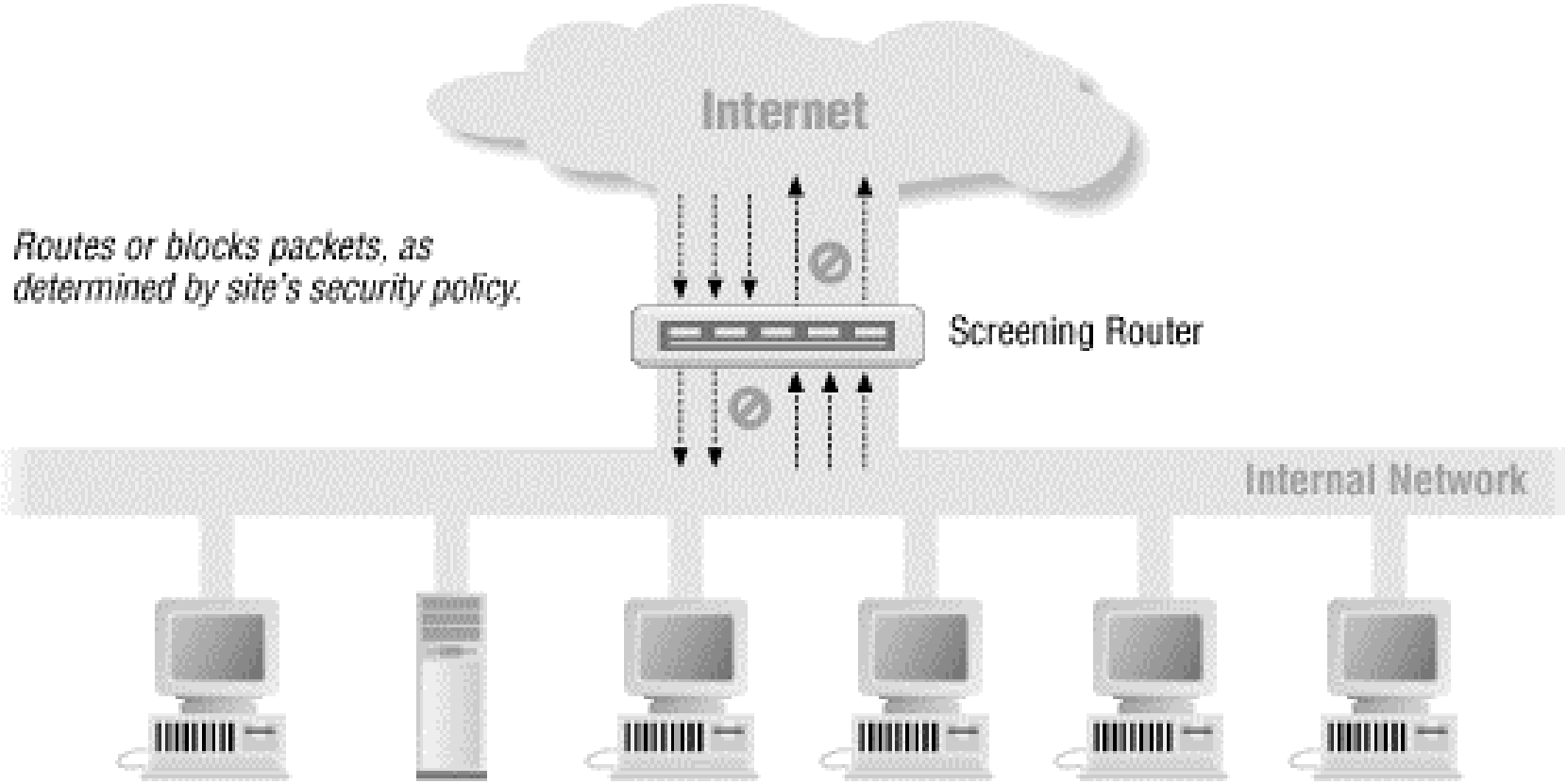
1. Package Filter Firewall
2. Application (Proxy) Firewall
3. Stateful Inspection



ระบบรักษาความปลอดภัย

1. Package Filter Firewall

ทำการตรวจสอบและกลั่นกรอง IP Package โดยเทียบคุณสมบัติ IP Package ที่เข้ามากับ Access Control Lists (ACL) หากไม่ตรงจะถือว่าเป็น Package ที่มีความเสี่ยงต่อระบบ จะไม่อนุญาตให้ Package นั้นเข้าสู่ระบบขององค์กร



ระบบรักษาความปลอดภัย

ในการพิจารณาเฮดเดอร์ Packet Filter จะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเตอร์เน็ตโมเดล

ข้อดี

- ไม่ขึ้นกับแอพพลิเคชัน
- มีความเร็วสูง
- รองรับการขยายตัวได้ดี

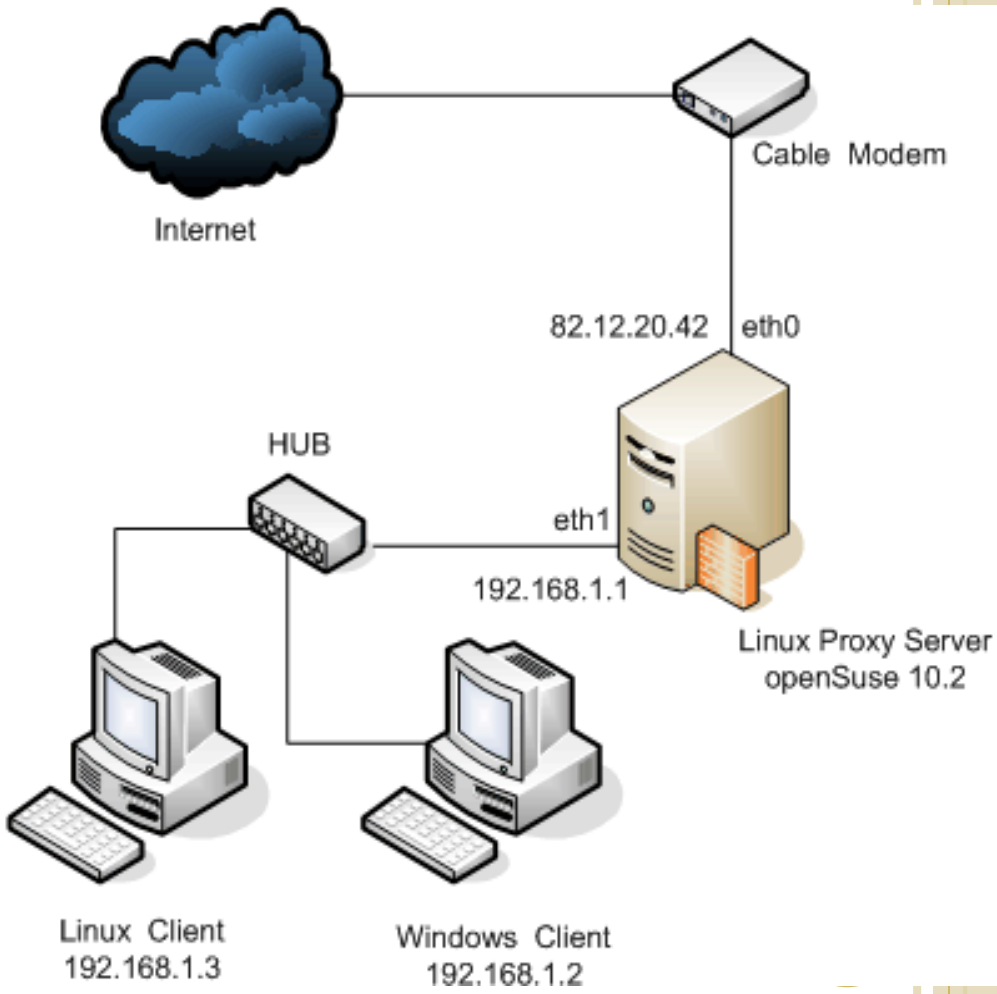
ข้อเสีย

บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ

ระบบรักษาความปลอดภัย

2. Application (Proxy) Firewall

Proxy หรือ Application Gateway เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มาก เนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์ (Application Layer)



ระบบรักษาความปลอดภัย

เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง โดยที่ Proxy จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2 ทิศทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่

ข้อดี

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสีย

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

ระบบรักษาความปลอดภัย

3. Stateful Inspection

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ข้อดี

- สามารถเพิ่มบริการอื่นๆได้
- การกำหนด Access Ruleทำได้ง่าย
- สามารถทำ IDS เพื่อป้องกันการโจมตีได้
- มีความสามารถในการทำ Authentication
- ใช้งานง่าย เพราะถูกออกแบบมาทำหน้าที่ Firewall โดยเฉพาะ
- ประสิทธิภาพสูง เพราะถูกออกแบบมาทำหน้าที่ Firewall โดยเฉพาะ
- การสื่อสารระหว่าง Firewall กับ Administration Console มีความปลอดภัยสูง

ข้อเสีย

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

ระบบรักษาความปลอดภัย

Intrusion Detection System (IDS)

คือ software หรือ hardware ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการเชื่อมต่อที่ไม่พึงประสงค์ หรือความพยายามที่จะเข้ามาทำอันตรายต่อเครือข่าย โดยผ่านระบบต่างๆ เช่น Internet, Lan เป็นต้น โดยการโจมตีนั้นอาจจะเกิดจาก cracker, Worm หรือ Malware ต่างๆ

องค์ประกอบของ IDS ได้แก่

1. Sensor คือส่วนที่จะสร้างเหตุการณ์ที่เกี่ยวกับความปลอดภัยขึ้นมา
2. Console คือส่วนที่จะตรวจจับเหตุการณ์ต่าง, แจ้งเตือน รวมไปถึงการควบคุม Sensor
3. Engine คือส่วนที่จะบันทึกเหตุการณ์จาก sensor ลงในฐานข้อมูลและจะแจ้งเตือนตามกฎที่กำหนดใน IDS

ข้อจำกัด คือไม่สามารถที่จะตรวจสอบ Packet ที่เข้ารหัสได้

ระบบรักษาความปลอดภัย

วิธีการป้องกันเครื่องในองค์กร

1. ปิดช่องโหว่ของระบบปฏิบัติการด้วยการ Update software
2. ติดตั้ง Firewall ให้กับคอมพิวเตอร์ทุกเครื่องในองค์กร
3. มีการทำ Authentication ก่อนเข้าใช้ Server
4. มีการกำหนดสิทธิ์ในการเข้าใช้ Server