บทที่ 15
ความรู้เบื้องต้นเกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์

การเสริมสร้างความมั่นคงปลอดภัยของระบบคอมพิวเตอร์เพื่อป้องกันการถูกโจมตีจากผู้ไม่หวังดีนั้น สิ่งที่สำคัญคือ การป้องกันเครือข่ายและระบบจากภัยคุกคามต่าง ๆ ทั้งจากภายนอกและภายในระบบเอง ซึ่งระบบคอมพิวเตอร์จะต้องมีการดำเนินการเตรียมความพร้อมในส่วนการตรวจสอบว่ามีการบุกรุกเข้ามาในระบบแล้วหรือไม่พร้อมทั้งต้องหาวิธีการเพื่อที่จะทำการหยุดยั้งหรือขัดขวางสิ่งที่จะก่อให้เกิดความเสียหายจากภัยคุกคามนั้น ๆ ให้สามารถที่จะปกป้องทรัพย์สินที่มีความสำคัญ ๆ โครงสร้างพื้นฐานรวมทั้งข้อมูลต่าง ๆ ของของระบบคอมพิวเตอร์ได้

การโจมตีและการรักษาความมั่นคงจากภัยคุกคาม พื้นฐานของการรักษาความมั่นคงปลอดภัย เช่น ปัญหาที่เกี่ยวข้องกับความมั่นคง ภัยคุกคามจากส่วนชุดคำสั่ง ภัยคุกคามระบบและเครือข่าย เครื่องมือและวิทยาการเข้ารหัสลับ (Cryptography) การเข้ารหัสลับ (Encryption) การพิสูจน์ตัวจริง (Authentication) และด่านกันบุกรุก (Firewall) เป็นต้น การใช้การคำนวณเพื่อทดสอบและการเข้ารหัสลับ รวมถึงการรับมือจากความหลากหลายสาเหตุเมื่อระบบถูกโจมตีจากภายนอก

ปัญหาที่เกี่ยวข้องกับความมั่นคง

การรักษาความมั่นคงของระบบเมื่อมีการใช้ทรัพยากรภายใต้ทุกสถานการณ์มักจะพบปัญหาที่เกี่ยวข้องหลายประการดังนี้

1. ผู้บุกรุก (Intruders) ผู้ที่พยายามกระทำการอย่างใดอย่างหนึ่งเพื่อเข้ามาในระบบ
2. ภัยคุกคาม (Treat) การกระทำการอย่างใดอย่างหนึ่งให้เป็นภัยต่อระบบ
3. การโจมตี (Attack) ความพยายามบุกรุกเพื่อเข้ามาทำลายระบบ

การที่ระบบคอมพิวเตอร์ มีปัญหาเกิดจากหลายสาเหตุด้วยกันหลายรูปแบบที่แตกต่างกัน ซึ่งขึ้นอยู่กับประเภทและวิธีการละเมิดที่แตกต่างกัน เช่น การไม่มีสิทธิ์ในการอ่านไฟล์ การไม่มีสิทธิ์ในการเปลี่ยนแปลงโครงสร้างไฟล์ การไม่มีสิทธิ์ในการใช้ทรัพยากรที่มีอยู่ในระบบ การใช้งานบางอย่างที่ไม่ถูกต้องตามหลักการหรือกฎเกณฑ์ที่ตั้งไว้ เป็นต้น

ประเภทของการละเมิดระบบคอมพิวเตอร์ แบ่งเป็น

1. การปลอมตัว (Masquerading) คือ การหลอกหรือแสร้งทำว่าเป็นผู้มีสิทธิ์ในการเข้าถึงระบบ
2. การโจมตีระบบอย่างต่อเนื่อง (Replay Attract) คือ การละเมิดเพื่อโจมตีระบบแบบเล่นซ้ำ โดยมีจุดประสงค์หลักเพื่อเข้ามาเปลี่ยนแปลงข้อความบางอย่างให้เกิดความผิดเพี้ยนไปจากเดิม
3. การโจมตีโดยปลอมเป็นคนกลาง (Man-in-the-Middle Attack) คือ การที่ผู้ละเมิดเข้ามาแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้ที่อยู่ในระบบ เพื่อปลอมตัวเข้าไปใช้งานในการรับหรือส่งข้อมูลในส่วนต่าง ๆ ที่เกี่ยวข้องกับระบบ
4. การขโมยข้อมูลระหว่างที่มีการสื่อสาร (Session Hijacking) คือ เป็นการขโมย สิทธิ์ในการเข้าถึงข้อมูลจากผู้ใช้นำมาใช้งาน ทำให้ผู้โจมตีมีสิทธิเท่าเทียมกับผู้ใช้งานคนนั้นเลย

ระดับมาตรการรักษาความปลอดภัยระบบคอมพิวเตอร์ แบ่งเป็น 4 ระดับ คือ

1. ระดับกายภาพ (Physical) เช่น ข้อมูลส่วนกลาง เครื่องแม่ข่ายและการติดต่อกับข้อมูลที่อยู่ปลายทาง เป็นต้น

2. ระดับบุคคล (Human) เช่น การหลอกถามข้อมูล การขโมยเอกสารต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล การหลอกลวงโดยใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูลต่าง ๆ ซึ่งอาจเป็นชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลส่วนบุคคลและการค้นข้อมูลส่วนตัวจากถังขยะ เป็นต้น

3. ระดับระบบปฏิบัติการ (Operating System) เช่น เป็นระดับกลไกการป้องกันระบบความผิดผลาดหรือช่องโหว่ของระบบปฏิบัติการแต่ละชนิด เป็นต้น

4. ระดับเครือข่าย (Network) เช่น การขัดขวางการสื่อสารข้อมูล การขัดจังหวะและการใช้งานระบบปฏิบัติการดอส เป็นต้น

ดังนั้นปัญหาที่เกี่ยวข้องกับความมั่นคง มาจากหลายสาเหตุและเกี่ยวข้องกับหลายระดับ การรักษาความมั่นคงที่ไม่เข้มงวดอาจจะสร้างปัญหาที่ตามมามากมาย จึงจำเป็นอย่างยิ่งที่จะต้องทำความเข้าใจและให้ความรู้กับผู้มีส่วนเกี่ยวข้องกับระบบทั้งหมดจึงจะทำให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดให้กับระบบคอมพิวเตอร์ที่อยู่ในหน่วยงานหรือองค์กร

ภัยคุกคามจากส่วนชุดคำสั่ง

ในสภาพแวดล้อมของระบบคอมพิวเตอร์โดยทั่วไป ที่ผู้เขียนชุดคำสั่งและผู้ใช้งานไม่ใช่บุคคลคนเดียวกัน ทำให้มีโอกาสของการใช้งานชุดคำสั่งผิดวัตถุประสงค์และทำให้เกิดภัยคุกคามที่ไม่คาดคิดเกิดขึ้นได้กับระบบ ซึ่งมีอยู่ด้วยกันหลายชนิดดังนี้

1. ม้าโทรจัน (Trojan Horses) เป็นลักษณะของส่วนชุดคำสั่งที่มีฟังก์ชันของการทำงานที่ไม่พึงประสงค์ ซึ่งฟังก์ชันนี้อาจจะเข้าไปเปลี่ยน ลบ หรือแฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่าง ๆ ได้อย่างสะดวกขึ้น

2. ประตูกับดัก (Trap Doors) เป็นลักษณะวิธีการค้นหาช่องโหว่จากการรักษาความปลอดภัยของระบบ การสร้างประตูกับดัก โดยการเขียนชุดคำสั่งแทรกไว้ในระบบเพื่อไม่มีใครสามารถจะตรวจเช็คคำสั่งนั้นได้ เช่น เขียนชุดคำสั่งขึ้นมาเพื่อให้ผู้ใช้ระบบใครก็ได้ที่ใส่ชื่อผู้ใช้ว่า “XXXXX” แล้วสามารถลงบันทึกเข้าระบบได้ ซึ่งคำสั่งปกติที่ใช้สำหรับการลงบันทึกเข้าระบบได้ไม่ว่าจะใส่รหัสผ่านอะไรก็ตาม เป็นต้น

3. ระเบิดเวลา (Logic Bomb) เป็นการเขียนรหัสชุดคำสั่งใส่เพิ่มเติมเข้าไปในระบบอย่างจงใจ โดยจะเริ่มทำงานเมื่อมีการกระตุ้นบางอย่างหรือว่าเกิดเหตุการณ์ที่ตรงกับเงื่อนไขขึ้นมา เช่น การใส่รหัสคำสั่งเข้าไปที่เครื่องแม่ข่ายแล้วจะกำหนดให้เมื่อถึงวันศุกร์ที่ 13 ขึ้นมาเมื่อไหร่ให้ระเบิดเวลาทำการจัดรูปแบบเครื่องแม่ข่ายใหม่ (Format Server)

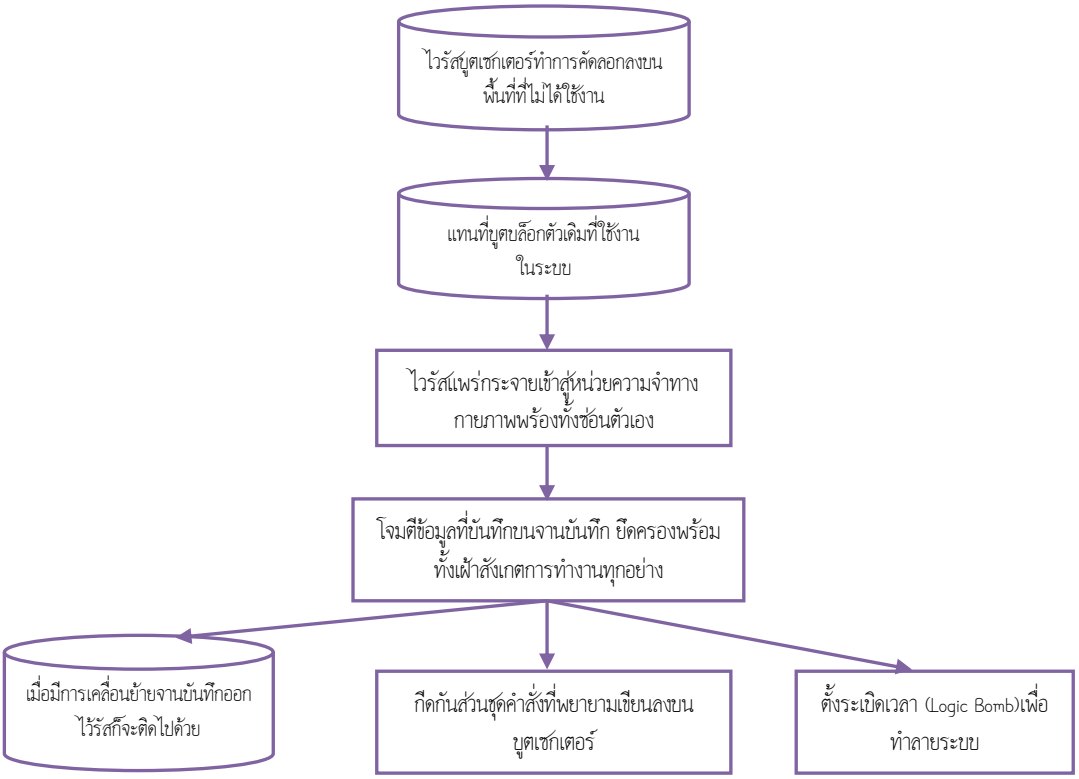
4. ไวรัส (Virus) เป็นชุดคำสั่งที่เขียนขึ้นมาเพื่อให้กระจายอยู่ชุดคำสั่งอื่น สามารถทำงานได้เหมือนกับชุดคำสั่งทั่วไป เช่น พิมพ์ข้อความ แสดงรูปภาพบนจอภาพ เล่นเพลง หรือทำทุกอย่างได้โดยที่ไม่เป็นอันตรายแต่สามารถที่จะทำการลบ แก้ไข ทำลายหรือขโมยไฟล์ โดยการส่งไวรัสไปทางอีเมล์หรือทำให้ระบบเกิดความเสียหายได้ ซึ่งสามารถแยกประเภทของไวรัส ย่อย ๆ ได้ดังนี้

1. Parasitic Virus เป็นไวรัสเก่าแก่ที่สุดเป็นรูปแบบพื้นฐานของชุดคำสั่งไวรัส โดยไวรัสชนิดนี้จะเป็นจุดเริ่มที่ทำให้ไวรัสแพร่กระจายไปติดที่ชุดคำสั่งอื่นเมื่อระบบได้มีการเรียกใช้ระบบจากจานบันทึกที่ติดไวรัส

2. Boot Sector Virus เป็นไวรัสชนิดหนึ่งที่จะทำลายที่เซกเตอร์แรกที่มีผลทำให้ระบบปฏิบัติการไม่สามารถทำงานในการปลุกเครื่อง (Boot) เพื่อเริ่มระบบขึ้นมาใช้งานได้ แสดงได้ดังภาพที่ 11.2

3. Steailth Virus เป็นไวรัสที่มีรูปแบบแน่นอนที่ถูกออกแบบมาเพื่อซ่อนตัวเองจากการป้องกันจากชุดคำสั่งตรวจหาไวรัส

4. Polymorphic Virus เป็นไวรัสที่สามารถทำการเปลี่ยนแปลงตัวเองทุกครั้งที่มีการแพร่กระจายตัวเอง



ภาพแสดงการทำงานของไวรัสบูตเซกเตอร์ (Boot-sector Computer Virus)

จากภาพ ไวรัสบูตเซกเตอร์จะทำการคัดลอกตัวเองเข้าไปแทนที่บูตบล็อกตัวเดิมบนพื้นที่ที่ไม่ได้ใช้งานพื้นที่ใดพื้นที่หนึ่งบนจานบันทึก หลังจากที่ฝังตัวลงบนไวรัสบูตเซกเตอร์แล้วไวรัสยังแพร่กระจายเข้าสู่หน่วยความจำทางกายภาพพร้องทั้งทำการซ่อนตัวเองภายในหน่วยความจำ เริ่มโจมตีข้อมูลที่บันทึกลงบนจานบันทึก ทำการยึดครองพร้อมทั้งเฝ้าสังเกตการทำงานทุกอย่างเพื่อกีดกันส่วนชุดคำสั่งที่พยายามเขียนลงบนบูตเซกเตอร์ ตัวไวรัสยังมีความสามารถตั้งระเบิดเวลา (Logic Bomb) เพื่อให้ทำลายระบบได้และเมื่อมีการคลื่อนย้ายจานบันทึกออกจากระบบไวรัสก็ยังสามารถที่จะติดไปกับจานบันทึกนั้น ๆ ได้ด้วย

ภัยคุกคามระบบและเครือข่าย

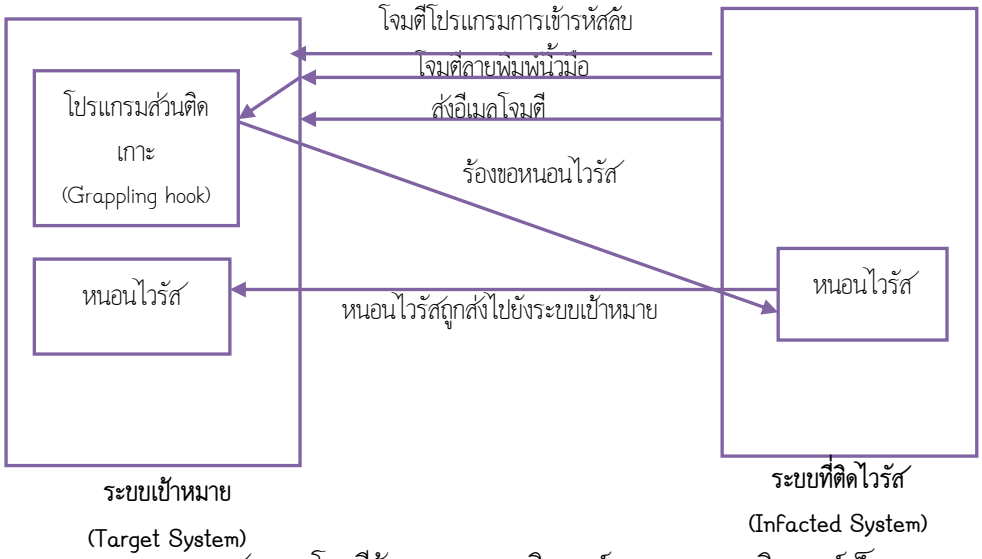
ระบบเครือข่ายในปัจจุบันเป็นระบบ "เปิด" ทำให้การรักษาความปลอดภัยหรือการจัดการภัยคุกคามเครือข่ายยากที่จะตรวจสอบและป้องกันภัยภิบัติ (Disaster) ที่เกิดขึ้นกับระบบ เป็นความเสียหายทั้งทางด้านกายภาพและด้านข้อมูล ส่วนเครื่อง ส่วนชุดคำสั่ง แฟ้มข้อมูล และอุปกรณ์อื่น ๆ ถูกทำลายให้เกิดความเสียหายหรืออาจทำให้ระบบล่มไม่สามารถใช้งานได้ ประเภทของภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่ายนั้น สามารถจำแนกได้ 2 ประเภท ดังนี้

1. ภัยคุกคามทางตรรกะ (Logical) หมายถึง ภัยคุกคามทางด้านข้อมูล

2. ภัยคุกคามทางกายภาพ (Physical) หมายถึง ภัยคุกคามที่เกิดกับตัวเครื่องและอุปกรณ์ เช่น ภัยจากธรรมชาติ ภัยจากการกระทำบางอย่างของมนุษย์ที่ทำความเสียหายให้กับตัวเครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง เป็นต้น ส่วนชุดคำสั่งที่เป็นภัยคุกคามระบบและเครือข่าย ซึ่งมีอยู่ด้วยกันหลายชนิด ดังนี้

1. สแปมเมล์ (Spam Mail) คือ การส่งข้อความที่ไม่เป็นที่ต้องการให้กับบุคคลจำนวนมาก ๆ โดยที่ผู้รับไม่เคยรู้จักหรือติดต่อกันมาก่อน โดยมากมักอยู่ในรูปของจดหมายอิเล็กทรอนิกส์ (E-mail) ทำให้ผู้รับเกิดความรำคาญและต้องเสียเวลาในการลบข้อความเหล่านั้นอีกทั้งยังทำให้ประสิทธิภาพการส่งข้อมูลบนระบบเครือข่ายอินเทอร์เน็ตลดลงด้วย

2. หนอนคอมพิวเตอร์ (Worm) คือ ไวรัสชนิดหนึ่งที่เขียนส่วนชุดคำสั่งขึ้นมาทำให้เป็นขบวนการของกลไกในการบังคับประสิทธิภาพการทำงานของระบบ หนอนคอมพิวเตอร์จะทำสำเนาตัวเอง โดยใช้ทรัพยากรของระบบหรือบางทีจะทำการป้องกันไม่ให้กระบวนการอื่น ๆ ใช้ทรัพยากรของระบบ ในระบบเครือข่ายหนอนคอมพิวเตอร์จะมีความสามารถมากที่จะทำสำเนาตัวเองและแพร่กระจายไปในแต่ละเครื่องที่อยู่บนระบบเครือข่ายและสั่งการทำให้เครื่องที่อยู่ในระบบหยุดทำงานทันทีหรือสามารถที่จะทำลายเครื่องคอมพิวเตอร์ที่ติดไวรัสที่อยู่ในระบบได้ แสดงได้ดังภาพที่ 11.3



ภาพแสดงการโจมตีด้วยหนอนคอมพิวเตอร์ (Worm) ทางอินเทอร์เน็ต

จากภาพ เมื่อระบบคอมพิวเตอร์ติดไวรัสหนอนคอมพิวเตอร์และต้องการแพร่กระจายหนอนไวรัสไปยังระบบเป้าหมายก็จะทำการโจมตีทุกรูปแบบไปยังระบบเป้าหมายไม่ว่าจะเป็น การส่งอีเมลโจมตี โจมตีลายพิมพ์นิ้วมือ โจมตีโปรแกรมการเข้ารหัสลับ เมื่อทำการโจมตีระบบเป้าหมายสำเร็จก็จะทำการฝังโปรแกรมส่วนติดเกาะ (Grappling hook) เพื่อทำการร้องขอหนอนไวรัสจากระบบที่ติดไวรัสและแพร่กระจายหนอนไวรัสไปยังระบบเป้าหมายเพื่อทำลายเครื่องที่อยู่ในระบบเป้าหมายตามวัตถุประสงค์ที่ต้องการ

เครื่องมือและวิทยาการเข้ารหัสลับ

การรักษาความมั่นคงระบบและเครือข่ายมีเครื่องมือให้เลือกใช้อยู่มาก โดยวัตถุประสงค์หลายประการ เช่น การรักษาอุปกรณ์ภายในระบบคอมพิวเตอร์ที่มีการกำหนดแหล่งที่มาและปลายทางของข้อความที่ได้รับ การเลือกใช้ระบบปฏิบัติที่มีประสิทธิภาพ การใช้ รหัสในการควบคุมกระบวนการที่ใช้งานเป็นการระบุช่องทางเข้า/ออก (Port) เพื่อใช้ควบคุมการติดต่อสื่อสารข้อมูลจากต้นทางและปลายทางของข้อความบนเครือข่าย การระบุเลขที่อยู่ไอพี (IP Address) ในการเชื่อมต่อทางอินเทอร์เน็ต เป็นต้น ซึ่งมีวิธีให้เลือกใช้หลายอย่าง ดังนี้

1. วิทยาการเข้ารหัสลับ (Cryptography) หมายถึง การให้ความสำคัญซึ่งกันและกันระหว่างผู้ส่งต้นทาง (Senders) และผู้รับปลายทาง (Receivers) โดยกำหนดให้มีการใช้กุญแจลับ (Secret Key) เพื่อยื่นการส่งข้อมูลจากฝั่งส่งไปยังผู้รับปลายทางซึ่งวิธีที่ได้รับความนิยม เช่น

1.1 การเข้ารหัสลับ (Encryption) เป็นการเข้ารหัสข้อมูลก่อนทำการส่งไปบนระบบอินเตอร์เน็ตและเมื่อข้อมูลถึงปลายทาง อุปกรณ์ปลายทางจะทำการถอดรหัสข้อมูลให้เป็นเหมือนเดิม เพื่อนำมาใช้งานต่อไป โดยวิธีการนี้เป็นการป้องกันข้อมูลจากการถูกโจรกรรมโดยกลุ่มผู้ไม่หวังดี แสดงได้ดังภาพ

ภาพแสดงการเข้ารหัสลับ (Encryption)

จากภาพ ผู้ส่งต้องการส่งข้อมูลก็จะทำการเข้ารหัสลับ (Encryption) ด้วยกุญแจสาธารณะ (Public Key) พร้อมกับกวนสัญญานข้อความ (Scrambled Massage) ก่อนจะส่งไปยังฝั่งรับ ฝั่งผู้รับจะทำการถอดรหัสลับ (Decryption) โดยใช้กุญแจส่วนตัว (Private Key) เพื่อใช้ในการเปิดอ่านข้อความที่ส่งมา

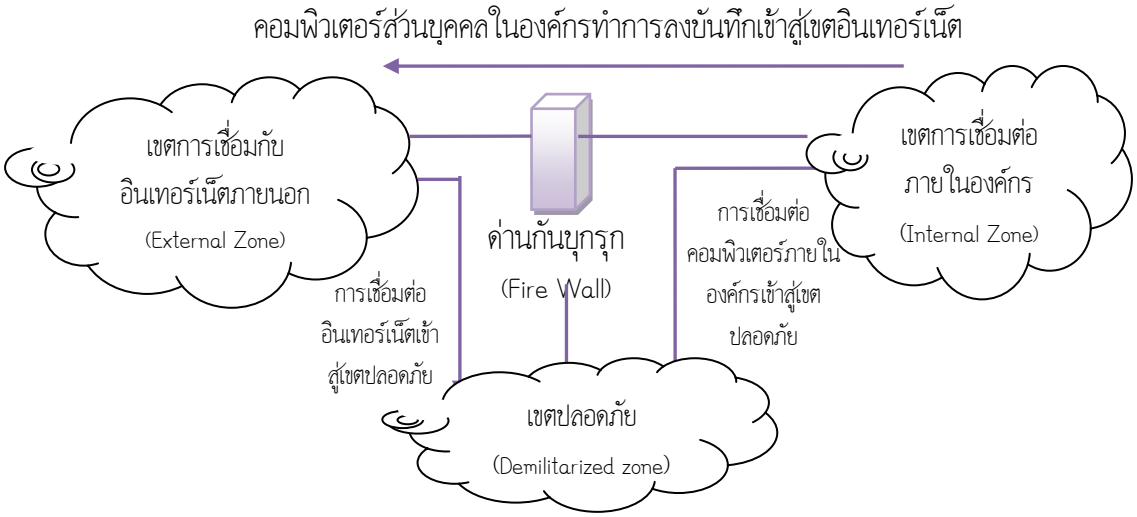
2. การพิสูจน์ตัวจริง (Authentication) เป็นรูปแบบของระบบความปลอดภัยที่เป็น การยืนยันผู้ใช้งานหรือยืนยันข้อมูลที่มีการรับส่งว่ามาจากด้านที่ได้รับขอนุญาตอย่างแท้จริง แบ่งออกเป็นได้หลายวิธี ดังนี้

2.1 ลายมือชื่อดิจิตอล (Digital Signature) หรือลายเซ็นดิจิตอล ใช้ในการระบุตัวบุคคลเพื่อแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้น ๆ เพื่อป้องกันการปฏิเสธความรับผิดชอบอีกทั้งยังสร้างความน่าเชื่อถือในการทำธุรกรรมร่วมกัน

2.2 การพิสูจน์ตัวจริงโดยชื่อผู้ใช้งาน (User Name Authentication) และการระบุรหัสผ่าน (Password) เป็นการกำหนดชื่อผู้ใช้งานพร้อมทั้งรหัสผ่านเพื่อสิทธิ์ในการลงบันทึกเข้า (Login) สู่ระบบคอมพิวเตอร์

ด่านกันบุกรุก (Firewall)

ด่านกันบุกรุก เป็นระบบรักษาความปลอดภัยที่มีหน้าที่ป้องกันไม่ให้ผู้ที่มิได้รับอนุญาตเข้ามาใช้งานในระบบเครือข่ายพร้อมกับควบคุมกระแสการนำข้อมูลเข้าหรือส่งข้อมูลออกของข้อมูลระหว่างที่มีการสื่อสารบนระบบเครือข่ายคอมพิวเตอร์ โดยการพิจารณาจาก กฎระเบียนหรือตัวกรองที่กำหนดไว้ในแต่ละระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ที่แตกต่างกันออกไป หน้าที่ของด่านกันบุกรุกมีทั้งข้อดีและข้อเสีย ซึ่งข้อดีคือ มีกระบวนการพิสูจน์ตัวจริงของผู้ใช้ มีการบันทึกสถิติและกิจกรรมที่เกิดขึ้นระหว่างเครือข่ายทำให้ระบบเครือข่ายมีความปลอดภัยมากขึ้น ส่วนข้อเสียคือ การเกิดความหนาแน่นของการสื่อสารข้อมูล เพราะปริมาณของข้อมูลติดต่อสื่อสารกันทั้งหมดจะต้องผ่านด่านกันบุกรุกเพียงจุดเดียวหรือหากด่านกันบุกรุกไม่สามารถทำงานได้ตามปกติจะทำให้การสื่อสารระหว่างเครือข่ายหยุดชะงักลงทันที แสดงได้ดังภาพที่ 11.5



ภาพแสดงด่านกันบุกรุกกับการป้องกันความมั่นคงปลอดภัยของระบบคอมพิวเตอร์

จากภาพ คอมพิวเตอร์ส่วนบุคคลในองค์กรที่ทำการลงบันทึกเข้าสู่เขตการเชื่อมต่ออินเทอร์เน็ตทั้งภายในและภายนอกองค์กร ผลพวงที่ได้รับอาจเกิดปัญหาในเรื่องการไวรัสและสิ่งที่สำคัญอีกส่วนหนึ่งคือการถูกเจาะระบบโดยผู้ไม่ประสงค์ดี อย่างไรก็ตามการติดต่อสื่อสารก็ยังจำเป็นจะต้องเกิดขึ้น ดังนั้นจึงจำเป็นต้องมีการป้องกันและมีการจัดแบ่งระบบเครือข่ายขององค์กรเป็นเขต (Zone) เพื่อให้เกิดความสะดวกในการควบคุมและจัดการ โดยเฉพาะการติดตั้งระบบด่านกันบุกรุก โดยแบ่งเขตการเชื่อมต่อออกเป็น

1. เขตการเชื่อมต่อภายใน (Internal Zone) หมายถึง ระบบเครือข่ายภายในองค์กร ซึ่งถือว่าเป็นเขตที่มีความปลอดภัยและน่าเชื่อถือสูงสุด

2. เขตการเชื่อมภายนอก (External Zone) หมายถึง ระบบเครือข่ายภายนอกองค์กรซึ่งถือว่าเป็นเขตที่มีความปลอดภัยต่ำ เมื่อมีการติดต่อกับเครือข่ายภายนอกจึงจำเป็นจะต้องมีการควบคุมการติดต่อสื่อสาร ร่วมทั้งระบบเครือข่ายอินเทอร์เน็ตที่ติดต่ออยู่ด้วย

3. เขตปลอดภัย (Demilitarized Zone) หมายถึง เป็นเขตติดต่อสื่อสารพิเศษสามารถติดต่อโดยตรงทั้งเขตการเชื่อมต่อภายในและเขตการเชื่อมภายนอก เช่น เครื่องบริการอีเมล (Mail server), เครื่องบริการเว็บ (Web Server) เป็นต้น

ชนิดของด่านกันบุกรุก พิจารณาจากรูปแบบการทำงานว่ามีความสอดคล้องกับระดับชั้นใดในแบบจำลองโอเอสไอ สามารถจัดแบ่งได้เป็น 3 ชนิด คือ

1. ด่านกันบุกรุกแบบกรองกลุ่มข้อมูล (Packet Filtering Firewall) เป็นรูปแบบพื้นฐานที่ใช้กันอย่างแพร่หลาย มีลักษณะการทำงานที่เรียบง่ายโดยการเปรียบเทียบค่าที่อยู่ส่วนหัว (Header) ของแต่ละกลุ่มข้อมูลกับกฎที่ได้กำหนดไว้ ค่าที่อยู่ส่วนหัวนำมาเปรียบเทียบ ได้แก่ เลขที่อยู่ไอพีต้นทาง เลขที่อยู่ไอพีปลายทาง ชนิดของโพรโตคอล ช่องทางเข้าและช่องทางออก

2. ด่านกันบุกรุกแบบตรวจเต็มสถานะ (Stateful Packet Inspection Firewall) เป็นรูปแบบการตรวจเต็มสถานะมีการทำงานเหมือนกับแบบกรองกลุ่มข้อมูล แต่มีการเปรียบเทียบค่าอื่นที่เพิ่มเติมขึ้นคือ สถานะการเชื่อมต่อ (Connection State) โดยความสัมพันธ์ระหว่างกลุ่มข้อมูลก่อนหน้ากับกลุ่มข้อมูลปัจจุบันจะนำมาใช้ในการพิจารณาว่าจะอนุญาตให้ชุดของกลุ่มข้อมูลใดผ่านเข้าหรือออกจากเครือข่ายของระบบได้หรือไม่

3. ด่านกันบุกรุกแบบเกตเวย์หรือพร็อกซี่ (Application Gateways/Proxies Firewall) เกตเวย์ที่ทำงานใน

ระดับชั้นแอพพลิเคชั่นของมาตรฐานการเชื่อมต่อโอเอสไอโดยการเปรียบเทียบค่าข้อมูล (Data Payload) กับกฎซึ่งด่านกันบุกรุกสองแบบข้างต้นที่ผ่านมาไม่สามารถทำได้ เช่น การบุกรุกของไวรัสบางชนิดมีการระบุค่าข้อมูลในกลุ่มข้อมูลเป็นรหัสที่ทำให้ระบบปฏิบัติการเกิดความสับสน ดังนั้นหากเลือกใช้ด่านกันบุกรุกสองชนิดแรกจะไม่สามารถป้องกันการบุกรุกแบบนี้ได้ ต้องใช้ด่านกันบุกรุกแบบเกตเวย์เท่านั้นที่สามารถตรวจจับได้