กิจกรรมส่งเสริมและพัฒนาความรู้ด้าน ICT

การป้องกันและรักษาความปลอดภัยบนเครือข่าย

www.mict4u.net

สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารประกอบการอบรม

การป้องกันและรักษาความปลอดภัยบนเครือข่าย

Network Security

www.mict4u.net

กิจกรรมส่งเสริมและพัฒนาความรู้ด้าน ICT

จัดโดย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เอกสารประกอบการอบรม หลักสูตรการป้องกันและรักษาความปลอดภัยบนเครือข่าย

เอกสารเผยแพร่ สงวนลิขสิทธิ์ พ.ศ. 2554
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เขียนโดย
ดร.สานนท์ ฉิมมณี (CEH ECSA)
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต
นายภส จันทรศิริ (CEH ECSA)
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

จัดทำและเผยแพร่โดย
สำนักส่งเสริมและพัฒนาการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม 2550
อาคารรวมหน่วยราชการ บี (ชั้น 6) ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ (02) 141 7041, (02) 141 7046 โทรสาร (02) 141
เว็บไซต์ www.mict4u.net

จัดพิมพ์โดย
บริษัท ล็อกซเล่ย์ จำกัด (มหาชน)
102 ถนน ณ ระนอง แขวงคลองเตย เขตคลองเตย กรุงเทพฯ 10110
โทรศัพท์ (02) 515 8343 โทรสาร (02) 515 8342

คำนำ

โดยทั่วไปแล้วทุกท่านคงได้รับการอบรมชี้แนะเกี่ยวกับความมั่นคงปลอดภัยในการใช้ชีวิตประจำวันมาตั้งแต่เป็นเด็กอยู่แล้ว เช่น อย่ารับของจากคนแปลกหน้า, อย่าไปในที่ลับหูลับตาคนเดียวโดยเฉพาะในเวลากลางคืน เป็นต้น แต่ในโลกของคอมพิวเตอร์แล้ว ไม่ได้มีการแนะนำอบรมกันอยู่ทั่วไปทั้งที่ในปัจจุบันคงปฏิเสธไม่ได้ว่าทุกคนต้องเกี่ยวข้องกับมันไม่ทางตรงก็ทางอ้อม ดังนั้นการให้ความรู้ความเข้าใจในความมั่นคงปลอดภัยของคอมพิวเตอร์จึงเป็นสิ่งที่จำเป็นอย่างยิ่งในยุคสมัยต่อจากนี้ไป ทั้งนี้พวกเราต้องพึงระลึกไว้เสมอด้วยว่า “ไม่มีระบบการป้องกันใดที่ปลอดภัยร้อยเปอร์เซ็นต์” การรักษาความมั่นคงปลอดภัยนั้นเป็นทั้งศาสตร์และศิลป์ การมีระบบความมั่นคงปลอดภัยที่แข็งแกร่งที่สุดนั้นไม่ได้หมายความว่าข้อมูล ระบบคอมพิวเตอร์ และองค์กรจะปลอดภัยจากอันตรายทั้งปวง การรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์นั้นจำเป็นต้องใช้กลไกต่างๆ (Mechanisms) เพื่อให้เป็นไปตามนโยบาย (Polices) การรักษาความมั่นคงปลอดภัย ซึ่งไม่ใช่แค่การติดตั้งระบบการรักษาความมั่นคงปลอดภัยที่เหมาะสมที่สุด แต่จะรวมถึงการวิเคราะห์และบริหารความเสี่ยง (Risk) ที่เกิดจากภัยคุกคาม (Threat) และช่องโหว่หรือจุดอ่อน (Vulnerability) ขององค์กร โดยทั้งหมดนี้ต้องกระทำอยู่อย่างสม่ำเสมอ

เอกสารฉบับนี้ได้จัดทำขึ้นเพื่อใช้ประกอบการอบรมหลักสูตร **การป้องกันและรักษาความมั่นคงปลอดภัยบนเครือข่าย** ที่จัดทำขึ้นโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดมุ่งหมายเพื่อแนะนำแนวทางหรือวิธีปฏิบัติที่เหมาะสมสำหรับการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์และเครือข่าย อย่างไรก็ตามอาจมีรายละเอียดของการอบรมบางส่วนที่แตกต่างไปจากในเอกสารฉบับนี้ ทำให้เอกสารฉบับนี้สามารถใช้อ่านเพิ่มเติมหลังการอบรมได้ แต่จะไม่สามารถใช้อ่านทดแทนการเข้าอบรมตามหลักสูตรได้

ภส จันทรศิริ

สารบัญ

บทที่ 1
การรักษาความมั่นคงปลอดภัยข้อมูล

ปัจจุบันเครือข่ายอินเทอร์เน็ตเติบโตอย่างรวดเร็ว เกือบจะทุกองค์กรจำเป็นต้องเชื่อมต่อเครือข่ายตนเองเข้ากับอินเทอร์เน็ตเพื่อใช้ประโยชน์จากแหล่งข้อมูลที่ใหญ่ที่สุดในโลกนี้ อินเทอร์เน็ตนั้นเปรียบเสมือนดาบสองคม ประโยชน์ที่ได้รับจากอินเทอร์เน็ตนั้นอาจมากเกินกว่าที่จะจินตนาการ แต่โทษนั้นก็มีมากมายเช่นกัน เหตุผลหนึ่งก็เนื่องจากข้อมูลและเครื่องมือที่ใช้สำหรับเจาะระบบนั้น สามารถค้นหาและดาวน์โหลดจากอินเทอร์เน็ตได้อย่างง่ายดาย และเครื่องมือหรือโปรแกรมเหล่านี้ยังง่ายต่อการใช้งาน ถึงแม้ว่าคนที่ไม่มีความรู้เกี่ยวกับคอมพิวเตอร์มากนักก็สามารถใช้เครื่องมือโจมตีเครือข่ายเหล่านี้ได้ไม่ยากนัก ดังนั้น ฝ่ายสารสนเทศหรือผู้ที่มีหน้าที่ดูแลระบบจึงจำเป็นที่จะต้องวิเคราะห์ความเสี่ยง, ออกแบบและติดตั้งระบบรักษาความมั่นคงปลอดภัยตลอดจนเฝ้าระวังระบบรักษาความมั่นคงปลอดภัยในเครือข่ายให้มีใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา

1.1 ประวัติของการรักษาความมั่นคงปลอดภัย

รูปแบบของการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินอื่นๆ นั้นได้มีวิวัฒนาการกับกาลเวลาเหมือนกับสังคมและเทคโนโลยีอื่นๆ การเรียนรู้และเข้าใจวิวัฒนาการนี้จะช่วยให้เข้าใจระบบการรักษาความมั่นคงปลอดภัยที่มีอยู่ในปัจจุบันและอาจเป็นบทเรียนที่ช่วยให้เราไม่ต้องทำผิดเหมือนกับที่เกิดขึ้นในอดีตได้

1.1.1 การรักษาความมั่นคงปลอดภัยด้านกายภาพ (Physical Security)

แต่ก่อนนั้นทรัพย์สินส่วนใหญ่จะเป็นวัตถุที่จับต้องได้ ข้อมูลที่สำคัญก็อยู่ในรูปแบบวัตถุเช่นกัน เนื่องจากข้อมูลจะถูกบันทึกไว้บนแผ่นหิน แผ่นหนัง หรือกระดาษ และบุคคลสำคัญในอดีตส่วนใหญ่จะไม่นิยมบันทึกข้อมูลที่สำคัญมากๆ ลงบนสื่อถาวร

เช่นแผ่นหนังหรือกระดาษ และจะไม่สนทนาเกี่ยวกับข้อมูลเหล่านี้กับบุคคลอื่นนอกเหนือจากบุคคลที่ไว้ใจได้เท่านั้น ดังรูปที่ 1.1 ซึ่งนี่อาจเป็นที่มาของคำว่า *"ความรู้คืออำนาจ (Knowledge is power)"* ซึ่งหมายความว่า ผู้ที่มีความรู้คือ ผู้ที่มีอำนาจนั่นเอง และนี่อาจเป็นรูปแบบการรักษาความมั่นคงปลอดภัยที่ดีที่สุดในตอนนั้นก็ได้ ซุนวู นักปรัชญาชาวจีน ได้กล่าวไว้ว่า *"ความลับที่รู้โดยคนมากกว่าหนึ่งคนก็ไม่ถือว่าเป็นความลับอีกต่อไป"* การที่จะปกป้องทรัพย์สินที่เป็นวัตถุนั้นก็ต้องใช้การปกป้องทางด้านกายภาพ เช่น กำแพง ประสาท หรือยาม เป็นต้น

ถ้าต้องมีการส่งข้อมูลไปที่อื่นก็จะใช้ผู้ส่งข่าว และส่วนใหญ่ก็จะมีผู้คุ้มกันติดตามไปด้วย ภัยอันตรายนั้นจะอยู่ในรูปแบบทางกายภาพทั้งสิ้น ไม่มีทางที่จะได้ข้อมูลมาโดยที่ไม่ได้คว้ามาด้วยมือ โดยส่วนใหญ่ทรัพย์สิน เช่น เงิน ทอง หรือข้อมูลที่บันทึกลงบนสื่อ จะถูกขโมย หรือถูกแย่งไปจากเจ้าของ

รูปที่ 1.1 แสดงการถ่ายทอดความรู้ผ่านทางบุคคลซึ่งเป็นที่นิยมกว่าการจดบันทึก

1.1.2 **การรักษาความมั่นคงปลอดภัยด้านสื่อสาร** (Communication Security)

อย่างไรก็ตามการรักษาความมั่นคงปลอดภัยเฉพาะทางด้านกายภาพด้านเดียวนั้นก็มีข้อบกพร่องหรือจุดอ่อนกล่าวคือ ถ้าข้อมูลถูกขโมยระหว่างการรับส่ง ศัตรูก็สามารถเปิดอ่านและเข้าใจข้อมูลนั้นได้ทันที จนกระทั่งเมื่อคราวยุคของจูเลียส์ ซีซ่าส์

ข้อบกพร่องนี้ได้ถูกแก้ไข โดยในสมัยนั้นได้มีการคิดค้นวิธีที่ใช้สำหรับ “ซ่อน” ข้อมูล หรือการเข้ารหัสข้อมูล (Encryption) ซึ่งข้อมูลจะถูกเข้ารหัสก่อนที่จะส่งไปให้อีกฝ่ายหนึ่ง ดังนั้น ถ้ามีการขโมยข้อมูลระหว่างทาง ผู้อ่านก็จะไม่เข้าใจข้อมูลถ้าไม่รู้วิธีการถอดรหัส

แนวคิดนี้ได้ถูกพัฒนามาใช้ในช่วงสงครามโลก ครั้งที่ 2 เยอรมันใช้เครื่องมือที่เรียกว่า “เอ็นนิกมา (Enigma)” ดังแสดงในรูปที่ 1.2 สำหรับเข้ารหัสข้อมูลที่รับส่งระหว่างหน่วยทหาร ในขณะนั้นเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสลับนี้ได้ถ้ามีการใช้งานอย่างถูกต้อง อย่างไรก็ตามเป็นข้อผิดพลาดที่เกิดจากผู้ใช้งานเครื่องนี้เองที่เกิดความประมาณและไม่มีการเปลี่ยนคีย์ (key) ที่ใช้ในการเข้ารหัส จนเป็นผลทำให้ฝ่ายพันธมิตรสามารถถอดรหัสและอ่านข้อมูลได้ในที่สุด

รูปที่ 1.2 Enigma เครื่องเข้ารหัสเครื่องแรกของโลก

การสื่อสารทางด้านการทหารนั้นจะใช้รหัสแทนชื่อหน่วยหรือสถานที่อยู่แล้ว ตัวอย่างเช่น ญี่ปุ่นนั้นก็ใช้รหัสแทนชื่อเรียกทั่วไปในการสื่อสารกัน ถึงแม้ว่าสหรัฐฯ จะสามารถถอดรหัสข้อมูลได้ แต่ก็ยังต้องทำความเข้าใจกับรหัสที่ใช้แทนชื่อทั่วไปนี้อีก ซึ่งเป็นการเพิ่มความยากในการเข้าใจข้อมูลจริงๆ ตัวอย่างเช่น ในช่วงก่อนที่จะเกิดสงครามที่เกาะมิดเวย์ระหว่างญี่ปุ่นและสหรัฐฯ ในตอนนั้นสหรัฐฯสามารถถอดรหัสลับของญี่ปุ่นได้แล้ว แต่ยังไม่เข้าใจรหัสแทนชื่อสถานที่ โดยในข้อความที่ส่งนั้นญี่ปุ่นจะโจมตี

เป้าหมายที่มีรหัสว่า “AF” แต่ในที่สุดสหรัฐฯก็สามารถถอดรหัสนี้ได้และรู้ว่า “AF” นั้นหมายถึง มิดเวย์นั่นเอง วิธีการถอดรหัสก็โดยสหรัฐฯ จะส่งข้อความว่า “เกาะมิดเวย์ขาดแคลนน้ำจืด” โดยข้อความนี้ไม่ได้เข้ารหัส ทำให้ญี่ปุ่นอ่านข้อความนี้ได้ จึงเข้ารหัสและส่งข้อความนี้ให้หน่วยอื่นทราบ สหรัฐฯสามารถดักอ่านข้อความนี้ได้และถอดรหัสออกมา แล้วในข้อความนั้นมีอักษรว่า “AF” ที่ระบุสถานที่ ทำให้สหรัฐฯรู้ได้ทันทีว่าอักษร “AF” นั้นหมายถึง เกาะมิดเวย์ นั่นเอง

ข้อความไม่ใช่แค่ตัวอังษรที่เข้ารหัสในระหว่างการสื่อสารกัน ข้อความที่สื่อสารด้วยเสียง เช่น วิทยุและโทรศัพท์ก็เป็นข้อมูลอีกประเภทหนึ่งที่ต้องเข้ารหัสเพื่อปกป้องความลับของข้อมูล หรือเพื่อป้องกันการดังฟังการสื่อสารด้วยเสียง สหรัฐฯเข้ารหัสเสียงโดยใช้ นาวาโฮโค้ดทอล์คเกอร์ (Navaho Code Talker) นาวาโฮเป็นชนเผ่าหนึ่งที่มีภาษาเป็นของตัวเอง ผู้รับส่งข่าวนั้นจะใช้ภาษานี้ในการสื่อสารกัน ซึ่งถ้าฝ่ายศัตรูมีการดักฟังวิทยุที่สื่อสารกันอาจได้ยินแต่คงไม่เข้าใจภาษาได้

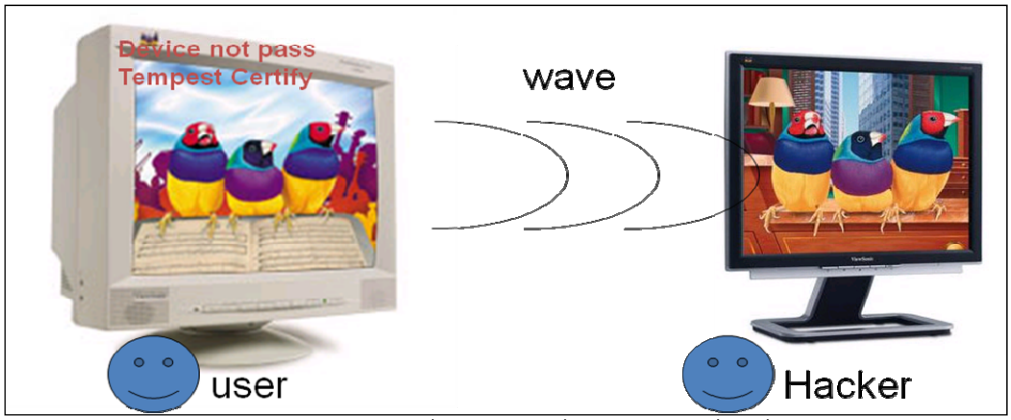
หลังจากสงครามโลกครั้งที่ 2 สหภาพโซเวียตได้ใช้ *“One Time Pad”* เพื่อเข้ารหัสข้อมูลที่รับส่งโดยสายลับ ซึ่งใช้การเข้ารหัสโดยการส่งข้อความบนปึกกระดาษซึ่งแต่ละหน้าจะประกอบด้วยตัวเลขที่เป็นเลขสุ่ม แต่ละหน้านั้นจะใช้แทนหนึ่งข้อความเท่านั้น รูปแบบการเข้ารหัสแบบนี้จะไม่สามารถถอดรหัสได้ถ้ามีการใช้อย่างถูกต้องคือใช้หนึ่งคีย์ต่อการเข้ารหัสหนึ่งข้อความ แต่สหภาพโซเวียตใช้อย่างไม่ถูกต้อง โดยมีการใช้คีย์มากกว่าหนึ่งครั้ง ทำให้ข้อความที่ส่งนั้นถูกถอดรหัสได้โดยง่าย อย่างไรก็ตามถึงแม้ว่าจะมีการใช้อย่างถูกต้องแล้วก็ตามก็ยังคงเป็นวิธีการเข้ารหัสที่มีปัญหาในเรื่องของการส่งมอบคีย์อยู่ดี

1.1.3 **การรักษาความมั่นคงปลอดภัยการแผ่รังสี** (Emissions Security)

นอกจากการใช้งานอย่างถูกต้องแล้วการเข้ารหัสข้อมูลที่ดีเป็นสิ่งที่ยากต่อการถอดรหัสได้ ดังนั้นจึงได้มีความพยามยามที่จะคิดค้นวิธีใหม่สำหรับอ่านข้อมูลที่เข้ารหัสและอยู่ในระหว่างการรับส่ง ในช่วงทศวรรษที่ 1950 ได้มีการค้นพบว่าข้อมูลที่รับส่งนั้นสามารถอ่านได้โดยการอ่านสัญญาณไฟฟ้าที่ส่งผ่านสายโทรศัพท์ และอุปกรณ์

อิเล็กทรอนิกส์ทุกประเภทจะมีการแผ่รังสีออกมา ซึ่งรวมถึงเครื่องพิมพ์โทรสารและเครื่องสำหรับเข้าและถอดรหัสข้อมูลด้วย ทั้งนี้เครื่องเข้ารหัสจะรับเข้าข้อความแล้วเข้ารหัสและส่งไปบนสายโทรศัพท์ ช่วงนั้นได้มีการค้นพบว่าสัญญาณไฟฟ้าที่แทนข้อมูลที่ยังไม่ได้เข้ารหัสก็ถูกส่งไปบนสายโทรศัพท์ด้วยเช่นกัน นั่นหมายความว่าข้อมูลเดิมที่ยังไม่ได้ถูกเข้ารหัสนั้นสามารถกู้คืนได้ถ้าใช้เครื่องมือที่ดี

ปัญหานี้เป็นเหตุให้สหรัฐฯต้องกำหนดมาตรฐานที่ชื่อ เท็มเปสต์ (TEMPEST) ซึ่งเป็นมาตรฐานที่ควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์ และใช้กับระบบที่สำคัญๆ จุดหมายก็เพื่อลดการแผ่รังสีที่อาจใช้สำหรับการกู้คืนข้อมูลได้



รูปที่ 1.3 แสดงตัวอย่างการดักจับคลื่นแม่เหล็กที่แผ่มาจากเครื่องที่ไม่ผ่าน TEMPEST

1.1.4 **การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์** (Computer Security)

การเข้ารหัสข้อมูลและการควบคุมการแผ่รังสีเป็นมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เพียงพอ ถ้าระบบสื่อสารข้อมูลนั้นมีเพียงแค่การใช้เครื่องส่งโทรสาร แต่ต่อมาได้มีการนำคอมพิวเตอร์เข้ามาใช้งานแทนเครื่องส่งโทรสาร และข้อมูลส่วนใหญ่ก็อยู่ในรูปแบบดิจิตอล และได้มีการพัฒนาคอมพิวเตอร์เพื่อให้ใช้งานง่ายและสะดวกมากขึ้นเรื่อยๆ ทำให้ผู้ที่สามารถใช้เครื่องคอมพิวเตอร์ได้สามารถที่จะเข้าถึง

ข้อมูลทั้งหมดที่จัดเก็บในเครื่องนั้นด้วยเช่นกัน ทำให้ไม่มีความมั่นคงปลอดภัยในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์

ต่อมาในช่วงทศวรรษที่ 1970 เดวิด เบลล์ และ ลีโอนาร์ด ลา พาดูลา ได้พัฒนาแม่แบบสำหรับการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ แม่แบบนี้พัฒนาจากแนวคิดในการจัดระดับความมั่นคงปลอดภัยของข้อมูลของรัฐบาลสหรัฐฯ ซึ่งแบ่งออกได้เป็น 4 ชั้นคือ ไม่ลับ ลับ ลับมาก และลับที่สุด (Unclassified, Confidential, Secret, Top Secret) และระดับสิทธิ์ของผู้เข้าถึงข้อมูลลับนี้ (Clearance) ซึ่งมี 4 ระดับเหมือนกัน หลักการของระบบนี้คือ ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้จะต้องมีสิทธิ์ (Clearance) เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนั้น ผู้ที่มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์ก็จะไม่สามารถเข้าถึงไฟล์นั้นได้

แนวคิดนี้ได้ถูกนำไปใช้ในกระทรวงกลาโหมของสหรัฐฯ โดยชื่อว่า มาตรฐาน 5200.28 หรือ *TCSEC (Trusted Computing System Evaluation Criteria)* หรือเป็นที่รู้จักทั่วไปว่า ออเรนจ์บุ๊ค (Orange Book) ดังรูปที่ 1.4 ซึ่งในมาตรฐานนี้ได้กำหนดระดับความมั่นคงปลอดภัยของคอมพิวเตอร์ออกเป็นระดับต่างๆ ดังนี้

D : Minimal Protection or Unrated

C1 : Discretionary Security Protection

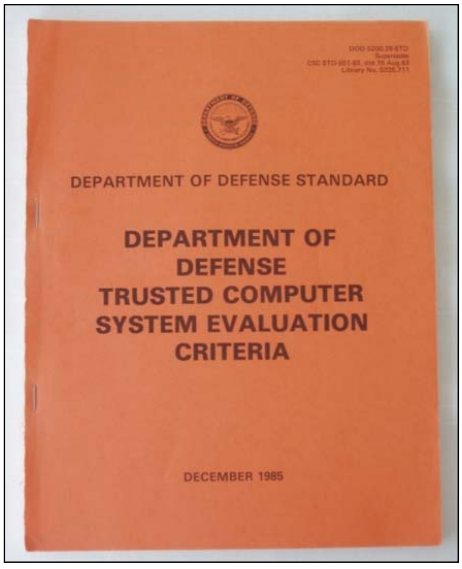
C2 : Controlled Access Protection

B1 : Labeled Security Protection

B2 : Structured Protection

B3 : Security Domains

A1 : Verified Design



รูปที่ 1.4 แสดงหน้าปกของ Orange Book

ในแต่ละระดับของ Orange Book ได้กำหนดฟังก์ชันต่างๆ ที่ระบบต้องมีและการประกัน ดังนั้น ระบบที่ต้องการใบรับรองว่าจัดอยู่ในระดับใด ระบบนั้นต้องมีทั้งฟังก์ชันต่างๆที่กำหนดในระดับนั้นพร้อมทั้งการรับประกันในระดับนั้นด้วย ข้อกำหนดเกี่ยวกับการรับประกันสำหรับระบบเพื่อให้เป็นไปตามมาตรฐานนั้น ต้องใช้เวลาและค่าใช้จ่ายสูงสำหรับบริษัทผู้ผลิต นี่เป็นผลที่ทำให้มีไม่กี่ระบบที่ได้รับการรับรองเหนือกว่าระดับ C2 ที่ผ่านมามีแค่ระบบเดียวเท่านั้นที่ได้รับใบรับรองในระดับ A1 นั่นคือ ระบบ Honeywell SCOMP แต่ระบบนี้ล้าสมัยไปในตอนที่ผ่านกระบวนการตรวจสอบเสร็จ

หลังจากนั้นได้มีการกำหนดมาตรฐานใหม่ขึ้นมาแทนเพื่อแก้ข้อบกพร่องในเรื่องของเวลาที่ใช้ในการตรวจสอบเพื่อออกใบรับรอง เช่น German Green Book (1989), Canadian Criteria (1990), ITSEC: Information Technology Security Evaluation Criteria (1991) และ Federal Criteria (1992) ซึ่งแต่ละมาตรฐานที่กล่าวมานี้ก็เพื่อกำหนดกระบวนการในการออกใบรับรองว่าระบบคอมพิวเตอร์นั้นมีความมั่นคงปลอดภัยระดับไหน อย่างไรก็ตามคอมพิวเตอร์มีวิวัฒนาการอย่างรวดเร็ว ระบบปฏิบัติการสมัยใหม่และฮาร์ดแวร์ใหม่ๆ ได้ถูกพัฒนาขึ้นแทนที่ระบบเก่าเร็วกว่าก่อนที่ระบบเก่าจะได้รับใบรับรอง

1.1.5 การรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security)

ปัญหาหนึ่งที่เกี่ยวกับการตรวจทดลองเพื่อออกใบรับรองมาตรฐานระดับความมั่นคงปลอดภัยให้แก่ระบบคอมพิวเตอร์ก็คือ การขาดความเข้าใจเกี่ยวกับเรื่องเครือข่าย เมื่อคอมพิวเตอร์ถูกเชื่อมต่อกันเข้าเป็นเครือข่ายปัญหาใหม่ก็เกิดขึ้นและปัญหาเก่าก็เกิดจากอีกทางหนึ่ง ยกตัวอย่างเช่น การสื่อสารคอมพิวเตอร์นั้นเปลี่ยนจาก WAN มาเป็นแบบ LAN ซึ่งมีแบนด์วิธที่สูงมากและอาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆ อาจไม่ได้ผล การแผ่รังสีจากสายทองแดงที่ใช้สื่อสารนั้นสูงมาก เพราะสายจะกระจายทั่วทั้งห้องหรือทั่วทั้งอาคารก็ได้

Orange Book ไม่ได้มีข้อกำหนดเกี่ยวกับเครือข่ายคอมพิวเตอร์ ดังนั้น การเชื่อมต่อคอมพิวเตอร์เข้ากับเครือข่ายอาจทำให้ใบรับรองเป็นโมฆะหรือไม่มีประโยชน์

ทางออกสำหรับปัญหานี้คือ การใช้งานมาตรฐาน *TNI (Trusted Network Interpretation)* ของ TCSEC หรือที่รู้จักในชื่อ เรดบุ๊ค (Red Book) ซึ่งออกมาในปี 1987 ข้อกำหนดใน Red Book มากจาก Orange Book ทั้งหมดและได้เพิ่มส่วนที่เกี่ยวข้องกับเครือข่ายเข้าไป อย่างไรก็ตามเนื่องจากมีข้อกำหนดเกี่ยวกับฟังก์ชันและการรับประกันมากทำให้ใช้เวลามากเกินไปในการตรวจสอบระบบ ทำให้มีเพียงบางระบบเท่านั้นที่ผ่านการตรวจสอบของ INT และในระบบที่ได้รับใบรับรองนั้นไม่มีระบบใดเลยที่ใช้ในเชิงพาณิชย์

1.1.6 **การรักษาความมั่นคงปลอดภัยข้อมูล** (Information Security)

จากประวัติศาสตร์ที่ได้กล่าวมานั้นเราสามารถสรุปได้ว่าไม่มีวิธีการใดที่สามารถแก้ปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยได้ทั้งหมด แท้ที่จริงแล้วการรักษาความมั่นคงปลอดภัยที่ดีนั้นจะต้องใช้ทุกๆวิธีการที่กล่าวมาร่วมกัน การรักษาความมั่นคงปลอดภัยทางด้านกายภาพก็ยังเป็นวิธีการที่ดีสำหรับการปกป้องทรัพย์สินที่เป็นวัตถุ การรักษาความมั่นคงปลอดภัยด้านการสื่อสาร (COMSEC) เป็นวิธีที่ใช้ปกป้องข้อมูลในระหว่างการสื่อสาร การรักษาความมั่นคงปลอดภัยเกี่ยวกับการแผ่รังสี (EMSEC) เป็นสิ่งที่จำเป็นเมื่อฝ่ายตรงกันข้ามมีเครื่องมือที่สามารถอ่านข้อมูลจากรังสีที่แผ่ออกจากระบบคอมพิวเตอร์ การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ (COMPSEC) เป็นสิ่งจำเป็นสำหรับการควบคุมการเข้าถึงระบบคอมพิวเตอร์ และการรักษาความมั่นคงปลอดภัยเครือข่าย (NETSEC) ก็เป็นสิ่งที่จำเป็นสำหรับการควบคุมการใช้งานเครือข่าย และวิธีการที่กล่าวมาทั้งหมดนี้รวมกันสามารถให้บริการการรักษาความมั่นคงปลอดภัยข้อมูล (INFOSEC) ได้

แต่สิ่งที่ยังขาดคือ กระบวนการที่รวดเร็วสำหรับการตรวจสอบเพื่อออกใบรับรองว่าระบบคอมพิวเตอร์นั้นปลอดภัย เนื่องจากในปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลงที่เร็วมากกว่าเวลาที่ใช้กับกระบวนการตรวจสอบความมั่นคงปลอดภัยของระบบ นอกจากนี้ยังเป็นการยากมากหรือแทบจะเป็นไปไม่ได้เลยเกี่ยวกับการที่จะพิสูจน์ว่าระบบใดปลอดภัยหรือไม่

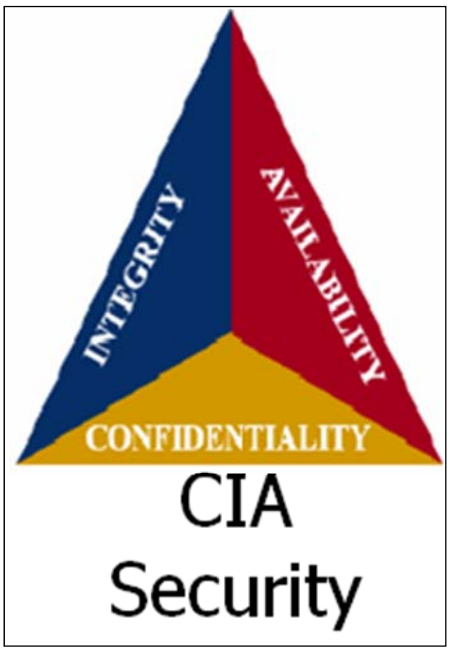
Note **Rainbow Series หรือ Rainbow Books** เป็นลำดับชุดมาตรฐานของ computer security ที่สร้างขึ้นโดยรัฐบาลสหรัฐฯในระหว่างปี 1980 ถึง 1999 ดังตาราง

[ข้อมูลจาก http://en.wikipedia.org/wiki/Rainbow_Series]

Title	Date	Color
DoD Trusted Computer System Evaluation Criteria	15 Aug 1983	Orange Book
DoD Password Management Guideline	12 Apr 1985	Green Book
Guidance for applying TCSEC in Specific Environments	25 Jun 1985	Yellow Book
A Guide to Understanding Audit in Trusted Systems	1 Jun 1988	Tan Book
Trusted Product Security Evaluation Program	22 Jun 1990	Bright Blue Book
Discretionary Access Control in Trusted Systems	30 Sep 1987	Neon Orange Book
Glossary of Computer Security Terms	21 Oct 1988	Aqua Book
Trusted Network Interpretation	31 Jul 1987	Red Book
Configuration Management in Trusted Systems	28 Mar 1988	Amber Book
A Guide to Understanding Design Documentation in Trusted Systems	6 Oct 1988	Burgundy Book
A Guide to Understanding Trusted Distribution in Trusted Systems	15 Dec 1988	Dark Lavender Book
Computer Security Subsystem Interpretation of the TCSEC	16 Sep 1988	Venice Blue Book
A Guide to Understanding Security Modeling in Trusted Systems	October 1992	Aqua Book
Trusted Network Interpretation Environments Guideline (TNI)	1 August 1990	Red Book
RAMP Program Document	1 March 1995	Pink Book
Guidelines for Formal Verification Systems	1 Apr 1989	Purple Book
Guide to Understanding Trusted Facility Management	18 Oct 1989	Brown Book
Guidelines for Writing Trusted Facility Manuals	October 1992	Yellow-Green Book
Identification and Authentication in Trusted Systems	September 1991	Light Blue Book
Object Reuse in Trusted Systems	July 1992	Light Blue Book
Trusted Product Evaluation Questionnaire	2 May 1992	Blue Book
Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX® System	7 July 1989	(Silver Book)
Trusted Database Management System Interpretation of the TCSEC (TDI)	April 1991	(Purple Book)
Trusted Recovery in Trusted Systems	30 December 1991	(Yellow Book)
Security Testing and Test Documentation in Trusted Systems		(Bright Orange Book)
Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements	December 1992	(Purple Book)
Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work	30 June 1993	(Purple Book)
Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description	28 February 1994	(Purple Book)
Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document	Publication TBA	(Purple Book)
Guide to Understanding Data Remanence in Automated Information Systems.	September 1991	Forest Green Book
Writing the Security Features User's Guide for Trusted Systems	September 1991	(Hot Peach Book)
Information System Security Officer Responsibilities for Automated Information Systems	May 1992	(Turquoise Book)
Assessing Controlled Access Protection	25 May 1992	(Violet Book)
Certification and Accreditation Concepts	January 1994	(Blue Book)
Covert Channel Analysis of Trusted Systems	November 1993	Light Pink Book

1.2 องค์ประกอบของความมั่นคงปลอดภัย

การที่จะบอกได้ว่าข้อมูลนั้นมีความมั่นคงปลอดภัยหรือไม่ก็โดยการวิเคราะห์คุณสมบัติทั้ง 3 ด้านคือ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability)



รูปที่ 1.5 คุณสมบัติของความมั่นคงปลอดภัย

1.2.1 **ความลับ** (Confidentiality)

การรักษาความลับของข้อมูล หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เนื่องจากข้อมูลบางอย่างมีความสำคัญและจำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้

ความต้องการในการรักษาความลับของข้อมูลนั้นเริ่มจากด้านการทหารที่ต้องการปกปิดข้อมูลเกี่ยวกับกองทัพไม่ให้ฝ่ายตรงข้ามทราบ เช่น ที่ตั้งหน่วยทหาร

แผนการโจมตี จำนวนกำลังพล และอาวุธที่ใช้ เป็นต้น ต่อมาหลักการนี้ได้มีการประยุกต์ใช้กับทางด้านธุรกิจเช่นกัน ดังเช่นบริษัทผู้ผลิตสินค้าอาจต้องการที่จะเก็บข้อมูลเกี่ยวกับการออกแบบผลิตภัณฑ์ของตัวเองให้เป็นความลับ เพราะถ้าถูกขโมยไปหรือถูกเปิดเผย บริษัทคู่แข่งอาจนำไปเลียนแบบได้ง่าย อีกตัวอย่างหนึ่งคือ องค์กรจำเป็นที่จะต้องเก็บข้อมูลส่วนตัวของพนักงานหรือข้อมูลลูกค้าของตัวเองเป็นความลับ เพราะถ้าเปิดเผยอาจเป็นการละเมิดสิทธิส่วนบุคคลได้

กลไกหนึ่งที่ใช้ในการรักษาความลับคือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและคีย์ในการเข้าหรือถอดรหัส โดยกุญแจ (Key) หรือรหัสผ่าน (Password) เป็นกุญแจที่ใช้สำหรับการเข้าและถอดรหัสข้อมูลได้ อย่างไรก็ตามการรักษาคีย์หรือรหัสผ่านก็เป็นอีกปัญหาหนึ่งที่เพิ่มขึ้นมาในกลไกควบคุมการเข้าถึง

ตัวอย่างที่เห็นได้ชัดในปัจจุบัน เช่น ในการซื้อขายสินค้าบนอินเทอร์เน็ตหรืออีคอมเมิร์ซ วิธีจ่ายเงินที่เป็นที่นิยมมากที่สุดวิธีหนึ่งคือ การใช้บัตรเครดิต โดยผู้ใช้ต้องกรอกหมายเลขบัตรและวันหมดอายุในแบบฟอร์มสั่งซื้อผ่านทางเว็บ หลังจากนั้นเมื่อลูกค้ายืนยันการสั่งซื้อ ข้อมูลนี้ก็จะถูกส่งจากเครื่องของลูกค้าไปยังเซิร์ฟเวอร์ของบริษัทผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งในระหว่างที่ข้อมูลเดินทางผ่านอินเทอร์เน็ตนั้นต้องผ่านหลายจุด ในแต่ละจุดที่ข้อมูลส่งผ่านนั้นไม่มีการรับรองความมั่นคงปลอดภัยของข้อมูลเลย ถ้าข้อมูลนี้ถูกขโมยไปอย่างง่ายดายก็แสดงว่าข้อมูลนี้ขาดการรักษาความลับของข้อมูล อย่างไรก็ตามโดยส่วนใหญ่ในการสั่งซื้อสินค้านั้นข้อมูลที่รับส่งระหว่างเครื่องลูกข่ายและเซิร์ฟเวอร์นั้นจุถูกเข้ารหัสไว้โดยใช้คีย์หรือรหัสผ่าน ดังนั้น คนอื่นก็จะไม่สามารถอ่านข้อมูลนี้ได้ถ้าไม่มีคีย์หรือรหัสผ่าน แต่ถ้าบุคคลอื่นสามารถขโมยคีย์ได้และสามารถถอดรหัสข้อมูลในการสั่งซื้อได้ ก็แสดงว่าความลับของข้อมูลถูกทำลายหรือถูกเปิดเผย (Compromised) ทำให้ข้อมูลนั้นไม่มีความมั่นคงปลอดภัย

การเข้ารหัสข้อมูลเป็นการปกป้องความลับของข้อมูลในระหว่างการส่งผ่านเครือข่ายที่ไม่มีความมั่นคงปลอดภัย นอกจากนี้ยังมีกลไกอื่นของระบบที่ใช้สำหรับ

ปกป้องความลับของข้อมูลที่จัดเก็บไว้ในระบบ นั่นคือ กลไกควบคุมการเข้าถึง (Access Control) กลไกการควบคุมนี้จะพิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบว่าเป็นผู้ที่ได้รับอนุญาตหรือไม่ ซึ่งวิธีการที่นิยมมากที่สุดคือ “การล็อกอินเข้าสู่ระบบ” โดยกลไกนี้จะแตกต่างจากการเข้ารหัสข้อมูล เนื่องจากข้อมูลอาจถูกอ่านได้ถ้ากลไกนี้ไม่ทำงานหรือทำงานผิดพลาด หรือการหลีกเลี่ยงการใช้งานกลไกนี้ ดังนั้นข้อดีข้อเสียของทั้งสองกลไกจะเป็นคนละจุดกัน กลไกการควบคุมการเข้าถึงนั้นเป็นการปกป้องทั้งระบบ ส่วนการเข้ารหัสข้อมูลนั้นเป็นการรักษาความลับของข้อมูลนั้นๆ อย่างไรก็ตามถ้ากลไกควบคุมการเข้าถึงระบบทำงานผิดพลาดหรือล้มเหลว ข้อมูลที่จัดเก็บในระบบนั้นก็จะอยู่ในสภาพที่ไม่ปลอดภัยเช่นกัน อย่างไรก็ตามทั้งสองวิธีนี้สามารถใช้งานพร้อมกันได้

การรักษาความลับของข้อมูลนั้นยังรวมถึงการรักษาไว้ซึ่งการมีอยู่ของข้อมูล ซึ่งบางกรณียังมีความสำคัญมากกว่าเนื้อข้อมูลเสียอีก ยกตัวอย่างเช่น การได้รู้ข้อมูลที่ว่า ผลการสำรวจความนิยมของนักการเมืองคนหนึ่งสูงมาก ข้อมูลนี้อาจมีความสำคัญน้อยกว่าข้อมูลที่ว่า ผลการสำรวจความคิดเห็นนี้ได้จากการสำรวจความคิดเห็นจากสมาชิกของพรรคหรือกลุ่มผู้ที่สนับสนุนผู้สมัครนั้นเป็นส่วนใหญ่ หรืออีกอย่างหนึ่งคือ ข้อมูลที่ว่า รัฐบาลมีรูปแบบในการละเมิดสิทธิมนุษยชนของประชาชนอย่างไร อาจมีความสำคัญน้อยกว่าข้อมูลที่ว่า รัฐบาลได้ละเมิดสิทธิมนุษยชนของประชาชนตัวเอง ทั้งนี้กลไกควบคุมการเข้าถึงบางครั้งก็เป็นการปกปิดไว้ซึ่งการมีอยู่ของข้อมูล เพื่อเป็นการป้องกันความลับของข้อมูลอีกชั้นหนึ่ง กล่าวคือ ถ้าไม่รู้ว่าข้อมูลนั้นมีอยู่ก็จะไม่มีความพยายามที่จะขโมยข้อมูลนั้นเกิดขึ้น

การซ่อนหรือปกปิดทรัพยากรก็เป็นอีกมุมหนึ่งของการรักษาความลับของข้อมูล ยกตัวอย่างเช่น องค์กรอาจต้องการที่จะปกปิดข้อมูลเกี่ยวกับโครงสร้างของระบบหรือการปรับแต่งของระบบที่องค์กรนั้นใช้งานอยู่ หรือการปกปิดไม่ให้ทราบว่าองค์กรใช้อุปกรณ์เฉพาะใดบ้าง เพราะมันอาจถูกใช้โดยที่ไม่ได้รับอนุญาตหรือใช้ในทางที่ไม่เหมาะสมก็ได้ กลไกการควบคุมการเข้าถึงอาจใช้เพื่อการปกป้องทรัพยากรเหล่านี้ได้เช่นกัน

1.2.2 **ความถูกต้อง** (Integrity)

การรักษาความถูกต้องและสมบูรณ์ของข้อมูล หมายถึง การทำให้ข้อมูลมีความน่าเชื่อถือได้ ซึ่งประกอบด้วย 2 ส่วนคือ ข้อมูลนั้นไม่ได้ถูกแก้ไขหรือเปลี่ยนแปลงจากแหล่งที่มาเดิม ส่วนที่สองคือ ความน่าเชื่อถือของแหล่งที่มา ตัวอย่างเช่น หนังสือพิมพ์รายงานข่าวว่าอาจมีการก่อการร้ายเกิดขึ้น ซึ่งข่าวนี้อาจรั่วมาจากสำนักข่าวกรองของรัฐบาล แต่เนื่องจากหนังสือพิมพ์ได้ข่าวมาด้วยวิธีการที่ผิด จึงรายงานว่าข่าวนี้ได้มาจากแหล่งอื่น เนื้อข่าวที่ตีพิมพ์ไปนั้นยังคงสภาพเดิมจากแหล่งที่มา ซึ่งเป็นการรักษาความถูกต้องของข้อมูล แต่แหล่งข้อมูลที่ได้มานั้นเปลี่ยนไป ดังนั้น ความถูกต้องของข้อมูลนี้ก็จะถูกกทำลายไปเช่นกัน

กลไกในการรักษาความถูกต้องของข้อมูลนั้นประกอบด้วย 2 ส่วนคือ

- **การป้องกัน** (Prevention) เป็นความพยามยามที่จะแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต ตัวอย่างเช่น องค์กรหนึ่งใช้ระบบงานบัญชี ถ้ามีพนักงานคนหนึ่งได้เจาะเข้าระบบ และแก้ไขเงินโบนัสของตัวเอง
- **การตรวจสอบ** (Detection) เป็นความพยายามที่จะแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ได้รับอนุญาตแต่พยายามแก้ไขข้อมูลนอกเหนือขอบเขตที่ตัวเองมีสิทธิ์ ตัวอย่างเช่น องค์กรหนึ่งใช้ระบบงานบัญชี โดยผู้ดูแลระบบบัญชีของบริษัทเองซึ่งได้รับอนุญาตให้ใช้งานระบบ แต่ได้ดำเนินการแก้ไขข้อมูลโดยการโอนเงินเข้าบัญชีตัวเองและพยายามปกปิดการกระทำนี้

กลไกในการป้องกันนี้มีจุดมุ่งหมายเพื่อรักษาความถูกต้องของข้อมูล ซึ่งทำได้โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต โดยใช้ *การพิสูจน์ตัวตน (Authentication)* และ *การควบคุมการเข้าถึง (Access Control)* จะเป็นกลไกที่ใช้สำหรับการป้องกันการบุกรุกประเภทแรกได้เป็นอย่างดี ส่วนการป้องกันความ

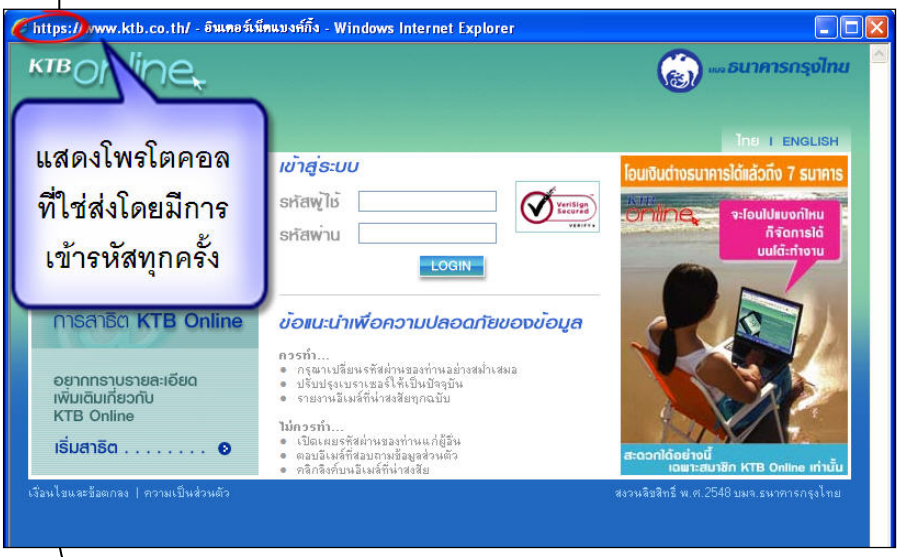
พยายามจากผู้ที่ได้รับอนุญาตนั้นต้องใช้ *กลไกการตรวจสอบสิทธิ์ (Authorization)* และกลไกอื่นๆเพิ่มขึ้นมา

ทั้งนี้กลไกในการตรวจสอบความถูกต้องของข้อมูล (Integrity Detection) นั้นไม่ใช่กลไกในการรักษาให้ข้อมูลคงสภาพเดิม แต่เป็นกลไกที่ตรวจสอบว่าข้อมูลยังคงมีความเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถทำได้โดยการตรวจเช็คและวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ หมายรวมถึงทั้งที่เกิดจากระบบเองและผู้ใช้งานระบบด้วย เพื่อตรวจสอบว่ามีปัญหาเกิดขึ้นหรือไม่ หรืออาจจะตรวจสอบและวิเคราะห์ข้อมูลว่ามีคุณสมบัติที่สำคัญหรือที่คาดหวังไว้ยังคงสภาพเดิมอยู่หรือไม่ และกลไกนี้อาจมีรายงานด้วยว่าส่วนไหนของข้อมูลหรือไฟล์มีการแก้ไขหรืออาจรายงานว่าทั้งไฟล์นั้นถูกเปลี่ยนไปจากสภาพเดิมโดยสิ้นเชิง

การทำงานของการรักษาความถูกต้องของข้อมูลนั้นแตกต่างจากการรักษาความลับของข้อมูลมาก การรักษาความลับของข้อมูลนั้นเป็นการตรวจสอบว่าข้อมูลถูกขโมยหรือไม่ แต่การรักษาความถูกต้องของข้อมูลนั้นเกี่ยวกับการรักษาความถูกต้องของข้อมูลและการรักษาความน่าเชื่อถือของข้อมูลด้วยแหล่งที่มาของข้อมูล (ข้อมูลได้มาอย่างไรและจากใคร) ข้อมูลถูกป้องกันดีแค่ไหนก่อนที่จะมาถึงปลายทาง และข้อมูลถูกป้องกันอย่างไรในระหว่างที่จัดเก็บอยู่ในระบบนั้น ซึ่งทั้งหมดนี้เป็นผลกระทบต่อความถูกต้องของข้อมูลทั้งสิ้น ดังนั้น การตรวจสอบความถูกต้องของข้อมูลนั้นเป็นสิ่งที่กระทำได้ยาก เนื่องจากมันจะขึ้นอยู่กับสมมติฐานเกี่ยวกับแหล่งที่มาและความน่าเชื่อถือของแหล่งที่มานั้น ซึ่งเป็นจุดหนึ่งที่มักจะถูกมองข้ามบ่อย

Note:

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) เป็นการส่งข้อมูลโดยมีการเข้ารหัสทุกครั้ง ซึ่งถือได้ว่ามีความมั่นคงปลอดภัยคอนข้างสูง แต่ข้อเสียอย่างหนึ่งก็คือในการส่งข้อมูลทุกครั้งต้องมีการเข้ารหัส ทำให้การสื่อสารสามารถทำได้ช้ากว่าแบบ HTTP (Hypertext Transfer Protocol) อยู่พอสมควร ดังนั้นในการสื่อสารข้อมูลทั่วไปจึงไม่มีการใช้โพรโตคอลนี้ในการสื่อสาร



2.3 **ความพร้อมใช้งาน** (Availability)

การรักษาไว้ซึ่งความพร้อมต่อการใช้งาน หมายถึง การให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลหรือทรัพยากรได้เมื่อต้องการ ความพร้อมใช้งานเป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) เนื่องจากการที่ระบบไม่พร้อมใช้งานก็จะแย่พอๆกับการที่ไม่มีระบบเลย ส่วนหนึ่งของความพร้อมใช้งานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยการทำให้ระบบไม่สามารถใช้งานได้ การออกแบบระบบนั้นส่วนใหญ่จะใช้ข้อมูลทางด้านสถิติเกี่ยวกับรูปแบบหรือพฤติกรรมในการใช้งานระบบของผู้ใช้ ระบบจะถูก

ออกแบบเพื่อให้เหมาะสมกับสภาพแวดล้อมดังกล่าว ดังนั้น กลไกในการรักษาความพร้อมใช้งานนั้นจะทำงานในกรณีที่ระบบไม่ได้ทำงานในสภาพที่ปกติหรือที่ออกแบบไว้ ซึ่งถ้ากลไกนี้ไม่ทำงานส่วนใหญ่ระบบจะล่มหรือไม่พร้อมใช้งาน

ยกตัวอย่างเช่น ธนาคารแห่งหนึ่งเก็บข้อมูลบัญชีลูกค้าไว้ในฐานข้อมูลโดยใช้เซิร์ฟเวอร์ 2 เครื่องทำงานโหลดบาลานซิ่ง (Load balancing) ซึ่งกันและกัน โดยเมื่อลูกค้าต้องการที่จะฝาก ถอน โอนเงิน หรือธุรกรรมอื่นๆ ก็จะต้องเข้ามาเช็คข้อมูลที่เซิร์ฟเวอร์นี้ก่อน เมื่อเซิร์ฟเวอร์หนึ่งไม่ทำงานอีกเซิร์ฟเวอร์หนึ่งก็จะทำงานแทน แต่ถ้าธนาคารมีแค่เซิร์ฟเวอร์เดียวและถ้าเซิร์ฟเวอร์นั้นไม่ทำงาน ซึ่งอาจจะถูกโจมตีหรือเซิร์ฟเวอร์ล่มเสียเอง ความพร้อมใช้งานของข้อมูลก็จะขาดไป ซึ่งทำให้ข้อมูลไม่มีความมั่นคงปลอดภัยด้านความพร้อมการใช้งาน

ความพยายามที่จะทำลายความพร้อมใช้งานจะเรียกว่า การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) ซึ่งเป็นการโจมตีที่อาจตรวจจับได้ยากที่สุด เนื่องจากในการวิเคราะห์ต้องพิจารณาว่าอะไรที่เป็นความพยายามที่ทำให้ระบบใช้งานไม่ได้ หรือเป็นเพียงเหตุการณ์ที่เกิดจากการใช้งานปกติ ซึ่งการวิเคราะห์นั้นจะอาศัยหลักการทางด้านสถิติเข้ามาช่วยในการวิเคราะห์ และสภาวะแวดล้อมการทำงานของแต่ละระบบก็แตกต่างกันไปด้วย ทำให้การวิเคราะห์เพื่อตัดสินว่าเป็นการโจมตีแบบปฏิเสธการให้บริการหรือไม่นั้นยากยิ่งขึ้นไปอีก

"คุณต้องทำการชั่งน้ำหนักความสำคัญให้ดีว่าองค์กรของคุณเน้นไปที่
การรักษาความลับของข้อมูลหรือความสามารถในการพร้อมใช้งาน
เพราะในความเป็นจริงแล้วเป็นไปได้ยากที่จะทำให้ทั้งสองอย่างนี้เกิดขึ้นอย่างเท่าๆกัน"

1.3 **ภัยคุกคาม** (Threat)

ภัยคุกคาม หมายถึงสิ่งที่อาจจะก่อให้เกิดความเสียหารต่อองค์ประกอบของความปลอดภัยด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรือถ้ามีการเตรียมการที่ดีเมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายได้ การกระทำที่อาจก่อให้เกิดความเสียหายเราเรียกว่า “การโจมตี (Attack)” ส่วนผู้ที่ทำเช่นนั้น หรือผู้ที่เป็นเหตุให้เหตุการณ์ดังกล่าวเกิดขึ้นจะเรียกว่า “ผู้โจมตี (Attacker)” หรือบางทีก็เรียกว่า “แอคเกอร์ (Hacker)” หรือ “แคร็คเกอร์ (Cracker)”

เครือข่ายเป็นเทคโนโลยีที่น่าอัศจรรย์ แต่ก็ยังคงมีความเสี่ยงอยู่มากถ้าไม่มีการควบคุมหรือป้องที่ดี การโจมตีหรือผู้บุกรุกเครือข่าย หมายถึง ความพยายามที่จะเข้าใช้ระบบ การแก้ไขข้อมูล (Configuration) ของระบบ การทำให้ระบบไม่สามารถใช้การได้ และการทำให้ข้อมูลเป็นเท็จ ทั้งนี้การรักษาความปลอดภัยขององค์ประกอบทั้ง 3 ด้าน คือ ความลับ (Confidentiality), ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) จะเป็นสิ่งที่ต้านภัยคุกคามที่อาจจะเกิดขึ้น เราสามารถแบ่งภัยคุกคามที่อาจจะเกิดขึ้นกับข้อมูลได้ 4 ประเภทคือ

- **การเปิดเผย** (Disclosure): การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือข้อมูลนั้นถูกเปิดเผยให้กับผู้ที่ไม่ได้รับอนุญาต
- **การหลอกลวง** (Deception): การให้ข้อมูลที่เป็นเท็จ
- **การขัดขวาง** (Disruption): การทำลายข้อมูล หรือกันไม่ให้กระทำต่อข้อมูลอย่างถูกต้อง
- **การควบคุมระบบ** (Usurpation): การเข้าควบคุมบางส่วนหรือทั้งระบบโดยไม่ได้รับอนุญาต

ภัยคุกคามทั้ง 4 ประเภทนี้จะครอบคลุมภัยทั้งหมดที่อาจเกิดขึ้นได้ เนื่องจากภัยคุกคามนั้นมีความหลากหลาย ดังนั้น การทำความเข้าใจพื้นฐานกับภัยประเภทต่างๆ จะทำให้สามารถเข้าใจระบบการรักษาความปลอดภัยมากขึ้น

1.4 แนวโน้มการโจมตี (Attack)

เนื่องด้วยเทคโนโลยีในปัจจุบันมีความก้าวหน้าไปมาก ระบบการป้องกันเองก็ได้ถูกพัฒนาไปด้วยเช่นกัน ทำให้การโจมตีกับระบบที่มีการป้องกันปรับปรุงให้ทันสมัยอยู่อย่างสม่ำเสมอจะสามารถทำได้ยากขึ้น หรือจำเป็นต้องใช้เวลาโจมตีมากขึ้นทำให้แนวโน้มของการโจมตีในปัจจุบันจึงมักเน้นไปที่บุคคลเป็นสำคัญ กล่าวคือเป็นการมุ่งเน้นโจมตีไปที่ความผิดพลาดของบุคคลเป็นหลัก เช่น การที่ผู้ใช้ไม่ทำการอัพเดทข้อมูลไวรัสให้กับโปรแกรมป้องกันไวรัส, ใช้การหลอกหลวงให้ติดตั้งโปรแกรมประสงค์ร้ายต่างๆโดยผู้ใช้เอง หรือการหลอกถามและแอบขโมยรหัสผ่านที่ผู้ใช้ทำการจดแล้ววางไว้บนโต๊ะทำงาน เป็นต้น ซึ่งจากตัวอย่างจะเห็นว่าผู้โจมตีไม่ได้ทำการโจมตีไปที่เทคโนโลยีโดยตรง แต่เป็นการโจมตีไปที่บุคคลซึ่งมักเกิดความประมาทและผิดพลาดได้ง่ายกว่า ทั้งนี้ในทางเทคนิคแล้วเราเรียกการโจมตีแบบนี้ว่า “วิศวกรรมสังคม (Social Engineering)” [ศึกษารายละเอียดเพิ่มเติมได้ที่หัวข้อ 3.2.1]

1.5 เครื่องมือสำหรับการรักษาความปลอดภัย

เนื่องจากภัยอันตรายนั้นมีรอบด้าน เราไม่สามารถที่จะใช้เพียงเครื่องมือประเภทใดประเภทหนึ่งเพื่อรักษาความปลอดภัยให้กับข้อมูลขององค์กรได้ และเราก็มาสามารถใช้เครื่องมือการรักษาความปลอดภัยเพียงประเภทเดียวสำหรับป้องกันระบบคอมพิวเตอร์และเครือข่ายทั้งองค์กรได้เช่นกัน เราจึงจำเป็นที่จะต้องใช้ผลิตภัณฑ์หลายประเภทจากหลากหลายบริษัททำงานร่วมกันอย่างเป็นระบบเพื่อป้องกันและรักษาความปลอดภัย ต่อไปนี้เป็นตัวอย่างประเภทของเครื่องมือที่ใช้สำหรับระบบการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่าย

- การเข้ารหัสข้อมูล (Data Encryption) [ศึกษารายละเอียดได้ในบทที่ 4]
- ไฟล์วอลล์ (Firewall) [ศึกษารายละเอียดได้ในบทที่ 5]
- ระบบตรวจจับการบุกรุก (IDS/IPS) [ศึกษารายละเอียดได้ในบทที่ 6]
- ซอฟต์แวร์ป้องกันไวรัส (Antivirus Software) [ศึกษารายละเอียดได้ในบทที่ 7]

1.6 มาตรฐานการรักษาความมั่นคงปลอดภัย

ปัจจุบันมีแม่แบบของการบริหารความปลอดภัยข้อมูลมากมายขึ้นอยู่กับว่าใครเป็นผู้ให้บริการ แต่แม่แบบที่ได้รับความนิยมมากที่สุด และได้กำหนดให้เป็นมาตรฐานนานาชาติคือ BS 7799 ซึ่งเป็นมาตรฐานที่พัฒนาโดยประเทศอังกฤษ มาตรฐานนี้ประกอบด้วย 2 ส่วนคือ

- BS 7799-1 ซึ่งต่อมาได้เปลี่ยนเป็นมาตรฐาน ISO/IEC 17799: Information Technology Code of Practice for Information Security Management
- BS 7799-2 ซึ่งต่อมาก็ได้รับการยอมรับเป็นมาตรฐาน ISO 27001: Information security Management: Specification with Guidance for Use

มาตรฐานนี้เป็นมาตรฐานที่มีลิขสิทธิ์ องค์กรใดที่ต้องการได้ใบรับรองจะต้องจ่ายค่าดำเนินการทั้งหมด จุดมุ่งหมายของมาตรฐานนี้ก็เพื่อให้คำแนะนำสำหรับการบริหารการรักษาความปลอดภัยสำหรับผู้ที่มีหน้าที่ในการเริ่มต้นออกแบบติดตั้ง และดูแลระบบการรักษาความปลอดภัยขององค์กร เป็นพื้นฐานสำหรับการพัฒนามาตรฐานการรักษาความปลอดภัยขององค์กร และระเบียบปฏิบัติที่มีประสิทธิภาพเพื่อสร้างความมั่นใจให้กับองค์กร และหน่วยงานอื่นที่เกี่ยวข้อง

Note!

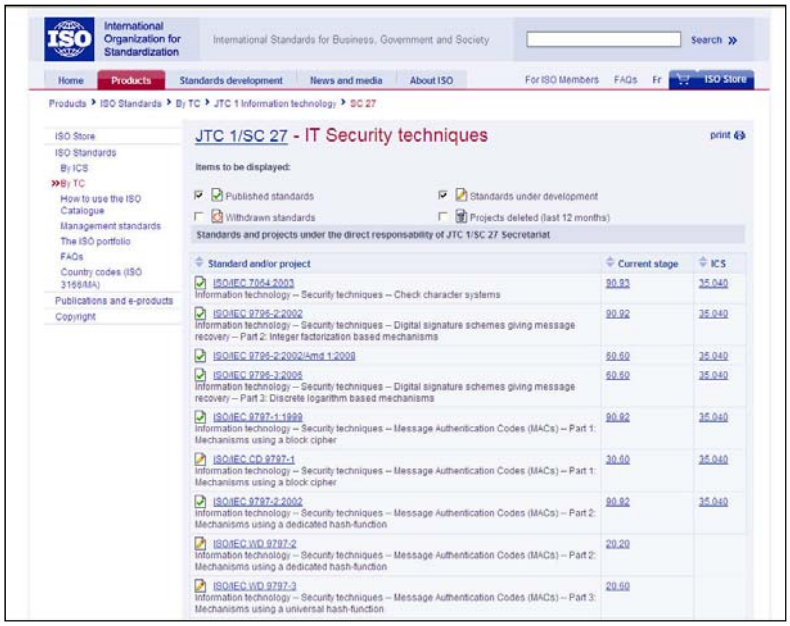
BS ย่อมาจาก British Standards

ISO ย่อมาจาก the International Organization for Standardization

IEC ย่อมาจาก the International Electrotechnical Commission

ท่านสามารถติดต่อขอซื้อเอกสารข้อกำหนดที่องค์กรต้องทำเพื่อให้ได้มาตรฐานที่ได้กล่าวมาแล้ว ได้ที่ http://www.iso.org โดยเข้าไปที่ **Products> ISO Standards> By**

TC> JTC 1 Information technology> SC 27 นอกจากนี้ในปัจจุบันยังมีมาตรฐานตัวใหม่คือ ISO 27006:2007 ซึ่งก็สามารถซื้อได้ที่เว็บไซต์ที่ส่วน SC27 นี้เช่นกัน



บทที่ 2

กระบวนการในการรักษาความปลอดภัยข้อมูล

2.1 การบริหารความเสี่ยง (ICT Risk Management)

ความเสี่ยง หมายถึง ภัยคุกคามที่อาจจะเกิดขึ้น หรือโอกาสที่จะเป็นไปได้กับระบบเครือข่ายขององค์กร แม้ว่าองค์กรนั้นจะมีนโยบายด้านความปลอดภัยหรือไม่มีก็ตาม สำหรับองค์กรที่ไม่มีนโยบายความปลอดภัยเครือข่ายแล้วจะมีโอกาสได้รับความเสี่ยงที่สูงกว่าองค์กรที่มีการกำหนดนโยบาย ดังนั้นเพื่อเป็นการลดหรือบรรเทาความเสี่ยงต่อระบบเครือข่ายขององค์กร ได้มีกระบวนการที่เรียกว่าการบริหารความเสี่ยงเกิดขึ้น กระบวนการบริหารความเสี่ยงมีกระบวนการย่อย 2 ขั้นตอนสำหรับใช้บริหารความเสี่ยง คือ

1. การค้นหาและประเมินความเสี่ยง (Risk Identification & Assessment)
2. การควบคุมความเสี่ยง (Risk Control)

โดยทั่วไปแล้วการบริหารความเสี่ยงเป็นกระบวนการประเมินความเสี่ยงต่อระบบเครือข่ายสารสนเทศขององค์กร และพิจารณาว่าความเสี่ยงเหล่านั้นจะถูกควบคุมหรือบรรเทาอย่างไร

2.1.1 การค้นหาความเสี่ยง (Risk Identification)

ขั้นตอนการตรวจสอบตัวเองถือเป็นกระบวนการแรกสำหรับการค้นหาความเสี่ยง ดังนั้นสำหรับการค้นหาความเสี่ยงมีขั้นตอนการพิจารณาดังนี้

- การสร้างรายการสินทรัพย์สารสนเทศ ประกอบด้วย คน กระบวนการ ข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์ และระบบเครือข่าย

- การจัดแบ่งสินทรัพย์เป็นหมวดหมู่อย่างมีความหมาย
- การกำหนดมูลค่าของแต่ละสินทรัพย์ของสารสนเทศ การพิจารณาเพื่อกำหนดมูลค่าสินทรัพย์ที่มีมูลค่ามากที่สุดสามารถกระทำได้ดังนี้
  - พิจารณาสินทรัพย์สารสนเทศใดมีความสำคัญที่สุดต่อความสำเร็จขององค์กร
  - พิจารณาสินทรัพย์สารสนเทศใดก่อให้เกิดกำไรสูงสุด
  - พิจารณาสินทรัพย์สารสนเทศใดแพงที่สุดในการทดแทน
  - พิจารณาสินทรัพย์สารสนเทศใดแพงที่สุดในการป้องกัน
  - พิจารณาสินทรัพย์สารสนเทศใดทำความเสียหายมากที่สุด หรือทำให้เป็นหนี้มากที่สุดถ้าเกิดการสูญหาย หรือถูกลักขโมย
- การค้นหาภัยคุกคามที่มีต่อสินทรัพย์
- การค้นหาสินทรัพย์ที่มีจุดอ่อนโดยการค้นหาการคุกคามที่มีต่อสินทรัพย์หนึ่งๆ

2.2 **การประเมินความเสี่ยง** (Risk Assessment)

การประเมินค่าความเสี่ยงสามารถประเมินได้จากความเป็นไปได้ที่จะเกิดจุดอ่อน คูณด้วยมูลค่าสินทรัพย์สารสนเทศ และลบด้วยเปอร์เซ็นต์ของการลดความเสี่ยง บวกด้วยความไม่แน่นอนของการรู้จุดอ่อน

เพื่อเพิ่มประสิทธิภาพในการประเมินความเสี่ยง ค่าความเป็นไปได้ที่จะเกิดจุดอ่อนได้ถูกกำหนดโดยกาถามคำถามดังต่อไปนี้

- การคุกคามแบบใดที่เป็นอันตรายต่อสินทรัพย์ขององค์กรในสิ่งแวดล้อมที่กำหนด
- การคุกคามแบบใดที่เป็นอันตรายมากที่สุดต่อสินทรัพย์สารสนเทศขององค์กร
- จำนวนเงินเท่าไรที่ต้องเสียในการฟื้นฟูระบบจากการถูกโจมตีที่สำเร็จ

- การคุกคามแบบใดที่ต้องใช้จำนวนเงินมากที่สุดในการป้องกัน

สำหรับค่าความไม่แน่นอนผู้ทำการประเมินสามารถประมาณการได้จากการตัดสินใจและจากประสบการณ์

2.3 การออกแบบและติดตั้งระบบรักษาความปลอดภัย

2.3.1 การรักษาความปลอดภัยเชิงกายภาพ (Physical Security)

การรักษาความปลอดภัยเชิงกายภาพ หมายถึง การป้องกันการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายในทางกายภาพ สามารถแบ่งออกได้เป็น 2 กลุ่ม กลุ่มที่หนึ่งคือกลุ่มที่เป็นสาเหตุทำให้เครื่องสูญหาย และกลุ่มที่สองคือกลุ่มที่เป็นสาเหตุทำให้เครื่องไม่สามารถทำงานได้หรือชำรุด

กลุ่มที่ทำให้เครื่องสูญหายนั้น เป็นกลุ่มที่เกิดจากความประมาทของผู้ดูแลระบบเป็นส่วนใหญ่ การที่ทำให้เครื่องสูญหายได้อาจเกิดจากการที่การรักษาความปลอดภัยของสถานที่เก็บเครื่องบริการหรือโครงข่ายไม่ได้มาตรฐานเพียงพอ เครื่องบริการควรจะถูกแยกออกเป็นส่วนของระบบเอง เพื่อให้ง่ายต่อการดูแลรักษาและความปลอดภัย โดยพื้นที่ดังกล่าวนั้นควรที่จะต้องมีการจำกัดสิทธิ์การใช้งานในพื้นที่นั้นๆ เช่น ห้องเครื่องบริการอาจจะมีการใส่กุญจาหรือประตูอัตโนมัติ เป็นต้น และทุกครั้งที่มีการใช้งานควรจะมีการเก็บบันทึกประวัติการเข้าออกจากพื้นที่ หรือบางทีอาจจะมีการติดกล้องวีดีโอวงจงปิดเลยทีเดียว

กลุ่มที่ทำให้เครื่องไม่สามารถทำงานได้หรือชำรุด สาเหตุสามารถเกิดขึ้นได้หลายสาเหตุ ไม่ว่าจะเกิดจากระบบการทำงานเองหรือภัยธรรมชาติก็ตาม สาเหตุต่างๆ เหล่านี้มีทั้งสาเหตุที่ควบคุมได้และควบคุมไม่ได้ เช่น น้ำท่วม ไฟฟ้าดับ เป็นสิ่งที่เราควบคุมไม่ได้ แต่การทำงานของเครื่องจนเครื่องร้อนเกินไป ขณะที่อุปกรณ์ทำความเย็นไม่สามารถทำงานได้ปกติ เป็นสิ่งที่ควบคุมได้ ดังนั้น การวางแผนที่ดีจึงเป็นสิ่งที่จำเป็น ซึ่งแผนนี้เรียกว่า Physical Security Plan โดยการวางนโยบายควรจะประกอบด้วยสิ่งเหล่านี้

1. ข้อกำหนดของทรัพยากรที่ต้องการจะปกป้อง (Description of physical assets)
2. ข้อกำหนดของขอบเขตพื้นที่ที่ต้องการจะปกป้อง (Description of physical area)
3. ข้อกำหนดของขอบเขตความปลอดภัย
4. ภัยคุกคามต่างๆ (Threats)
5. วิธีการป้องกันเชิงกายภาพ (Physical Security Defense) และการวิเคราะห์ต้นทุน (Cost Analysis)

2.3.2 การรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่ายและลูกข่าย

เป้าหมายการโจมตีหลักของผู้บุกรุกระบบคอมพิวเตอร์และเครือข่ายก็คือคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่ายที่มีข้อมูลสำคัญ ผู้บุกรุกหรือแฮกเกอร์มักจะโจมตีด้วยวิธีการต่างๆ เช่น เข้าถึงคอมพิวเตอร์แม่ข่ายที่ไม่ได้ป้องกัน (รหัสผ่านว่างเปล่า รหัสผ่านดีฟอลต์ หรือตั้งรหัสผ่านง่ายเกินไป) เข้าถึงคอมพิวเตอร์แม่ข่ายที่มีช่องโหว่ (เช่น ช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของ Application และช่องโหว่ของ Web Application) โจมตีเครื่องแม่ข่ายเพื่อไม่ให้สามารถใช้การได้ หรือทำให้ประสิทธิภาพลดลง(Dos: Denial of Service) และเข้าถึงคอมพิวเตอร์ลูกข่าย เพื่อขโมย/แก้ไข/ทำลายข้อมูลผู้ใช้ภายในองค์กร เป็นต้น วิธีการที่แฮกเกอร์ใช้ในการเข้าถึงและการป้องกันมีดังต่อไปนี้

- การเข้าถึงคอมพิวเตอร์แม่ข่ายที่ไม่ได้ป้องกัน
- การเข้าถึงคอมพิวเตอร์แม่ข่ายที่มีช่องโหว่
- การโจมตีเครื่องแม่ข่ายเพื่อไม่ให้สามารถใช้การได้ หรือทำให้ประสิทธิภาพลดลง
- การเข้าถึงคอมพิวเตอร์ลูกข่าย เพื่อขโมย/แก้ไข/ทำลายข้อมูลผู้ใช้ภายในองค์กร

2.3.3 การรักษาความปลอดภัยของระบบเครือข่ายและอุปกรณ์เครือข่าย

หลังจากที่รัฐบาลได้ออกกฎเพื่อควบคุมการบันทึกการใช้งานระบบเครือข่าย ซึ่งก่อนการเข้าใช้งานระบบเครือข่ายจะต้องมีการพิสูจน์ทราบตัวตน (Authentication) ด้วยนั้น รูปแบบการโจมตีระบบเครือข่ายภายในก็เริ่มที่จะพบเห็นได้บ่อยขึ้นนั่นคือการแฮกเพื่อเข้าใช้งานเครือข่ายโดยไม่ต้องผ่าน Authentication เช่น การโกงโดยที่แฮกเกอร์ปลอมแปลงค่า Mac Address ที่ระบบอนุญาต เป็นต้น ดังนั้นจึงควรมีการป้องกันการลักลอบเข้าถึงระบบเครือข่ายและป้องกันการลักลอบใช้งานระบบเครือข่ายอินเตอร์เน็ต นอกจากนั้นการโจมตีจากภายนอกก็ยังมีให้เห็นอยู่ เช่น เข้าถึงอุปกรณ์เครือข่ายจากระยะไกล ซึ่งทั้งหมดนี้จำเป็นต้องวางแผนรับมือการโจมตีรูปแบบต่างๆและใช้มาตรการป้องกันด้วยวิธีดังนี้

- ป้องกันการโจมตีด้วยวิธีการปลอม MAC Address
- ป้องกันการโจมตีแบบ ARP Spoof/Poisoning
- ป้องกันการโจมตีโดยใช้ Rogue DHCP
- เพิ่มความปลอดภัยให้กับระบบ LAN, Wireless LAN
- ทำการ Hardening ระบบปฏิบัติการ (firmware) และการตั้งค่าของอุปกรณ์เครือข่าย

2.3.4 การรักษาความปลอดภัยของข้อมูล

ข้อมูลหลักที่เราต้องปกป้องคือ ข้อมูลขององค์กร เช่น ข้อมูลรายละเอียดการสั่งซื้อสินค้า ข้อมูลรายรับรายจ่ายของบริษัท ข้อมูลเงินเดือนพนักงาน ข้อมูลรหัสผ่านของเจ้าหน้าที่ระบบเครือข่าย เป็นต้น ซึ่งข้อมูลเหล่านี้จะอยู่ใน Database Server หรืออยู่ในเครื่องแม่ข่ายอื่นๆ การป้องกันและรักษาความปลอดภัยของข้อมูลจะมีความเกี่ยวข้องกับการรักษาความปลอดภัยของเครื่องแม่ข่ายและระบบเครือข่าย นอกจากข้อมูลที่สำคัญเหล่านี้แล้ว หากแฮกเกอร์ได้ข้อมูลอย่างอื่นที่ดูแล้วไม่ค่อยมีความสำคัญแต่แฮกเกอร์สามารถนำข้อมูลดังกล่าวไปใช้เพิ่มประสิทธิภาพในการโจมตี/ควบคุมระบบ

ให้ส่งผลมากขึ้นได้ ข้อมูลนั้นก็ควรที่จะถูกปกป้องไว้เช่นกัน ตัวอย่างเช่น ข้อมูลแผนภาพของระบบเครือข่าย, รุ่น/ยี่ห้อของอุปกรณ์แต่ละตัว, ข้อมูลชื่อ/นามสกุล วัน/เดือน/ปีเกิดของพนักงานและของเจ้าหน้าที่ระบบเครือข่าย เป็นต้น

การควบคุมการเข้าถึงข้อมูลสำคัญจากระยะไกลจะต้องมีการประเมินความเสี่ยง หาช่องโหว่และอุดช่องโหว่ที่พบ เช่น ป้องกันการข้ามผ่านการตรวจสอบสิทธิ์แบบ SQL Injection ซึ่งสามารถที่จะล้วงเอาข้อมูลใน Database ได้ ป้องกันการโจมตีแบบ XSS ที่สามารถขโมย Cookie/Session ID ของ Webmaster แล้วเข้าสู่เว็บไซต์ด้วยสิทธิ์ของ Webmaster ซึ่ง Webmaster มักจะจัดการข้อมูลใน Database ผ่านทางเว็บ

นอกจากการปกป้องข้อมูลขององค์กรแล้ว จำเป็นต้องมีการปกป้องข้อมูลลูกค้าด้วย เช่น ข้อมูลเกี่ยวกับบัตรเครดิตของลูกค้าที่อยู่ใน Database ของเว็บไซต์ e-commerce ต่างๆ

2.4 การฝึกอบรม

การฝึกอบรมมีทั้งแบบอบรมทั่วไปและแบบสอบใบประกาศนียบัตร (Certificate) ในส่วนการสอบใบประกาศนียบัตรมีหลายแบบสามารถแบ่งได้ดังนี้

ระดับพื้นฐาน CCSA , CWNA , i-Net+ , Security+

ระดับกลาง CCSE , CCSPA , CIW Security Analyst , CWSP

ระดับสูง Solaris 9 Security , CCMSE , CCSE Plus , CCSP , CISSP , SSCP

2.5 การตรวจสอบ (Audit)

ปัจจุบันผู้ตรวจสอบระบบสารสนเทศ หรือ IT/IS Auditor เป็นอาชีพที่ต้องการผู้เชี่ยวชาญเฉพาะทางมาทำหน้าที่ตรวจสอบฝ่ายปฏิบัติการและฝ่ายพัฒนาระบบสารสนเทศ ซึ่งปัญหาใหญ่ ก็คือ ปัญหาการขาดแคลนผู้ตรวจสอบระบบสารสนเทศทั่วโลก ในขณะนี้หลายคนยังคงเข้าใจว่า “ผู้ตรวจสอบภายใน” หมายถึง “ผู้ตรวจสอบระบบสารสนเทศ” คำกล่าวนี้ไม่ผิดแต่ก็ไม่ถูก หมายความว่า ผู้ตรวจสอบระบบสารสนเทศนั้นแบ่งออกเป็นสองประเภท ได้แก่ ผู้ตรวจสอบระบบสารสนเทศภายใน (IT/IS Internal

Auditor) และผู้ตรวจสอบระบบสารสนเทศภายนอก (IT/IS External Auditor) ซึ่งความแตกต่างก็คือ ผู้ตรวจสอบระบบสารสนเทศภายในนั้น เป็นพนักงานขององค์กรเองไม่ได้มาจากคนนอก ปกติโดยผู้ตรวจสอบระบบสารสนเทศภายในจะสังกัดแผนกตรวจสอบระบบสารสนเทศภายใน ซึ่งจะขึ้นตรงกับ Board of director มีหน้าที่ในการตรวจสอบระบบสารสนเทศโดยรวมในองค์กร โดยมีความอิสระจากการควบคุมของฝ่ายระบบสารสนเทศ หรือ อิสระจากการควบคุมของ CIO ส่วนผู้ตรวจสอบระบบสารสนเทศภายนอกนั้น องค์กรมักจะทำการจัดจ้างหน่วยงานมืออาชีพภายนอก (3rd Party Security Audit Firm) มาทำหน้าที่เป็นผู้ตรวจสอบระบบสารสนเทศในมุมมองของคนนอกองค์กร ซึ่งความแตกต่างที่เห็นได้ชัดเจน คือ ความเป็นมืออาชีพ และความเป็นอิสระของ IT External Auditor กล่าวโดยสรุปคือ ทั้ง IT Internal Auditor และ IT External Auditor ล้วนมีบทบาทสำคัญในการตรวจสอบระบบสารสนเทศขององค์กร แต่อาจอยู่ในมุมมอง และ หน้าที่ที่แตกต่างกัน โดย IT Internal Auditor จะเน้นที่การตรวจสอบเป็นระยะๆ ตามตารางการตรวจสอบประจำปี จุดมุ่งหมายโดยส่วนใหญ่เพื่อตรวจสอบการปฏิบัติงานของฝ่ายสารสนเทศ ว่าเป็นไปตาม “IT Security Best Practices” ต่างๆ เช่น ISO/IEC17799 หรือ ISO/IEC 27001 ตลอดจนการตรวจสอบตาม IT Governance Framework เช่น CobiT 4.0 ของ ITGI (IT Governance Institute) โดยนำมาเป็น Audit Guideline เป็นต้น ในส่วนของ IT External Audit จุดมุ่งหมายจะเน้นไปที่ความปลอดภัยของระบบสารสนเทศในมุมมองของผู้เชี่ยวชาญด้านความปลอดภัยข้อมูล โดยรูปแบบและเทคนิคของการตรวจสอบแบ่งออกเป็น 3 ระดับขั้นดังนี้

ขั้นตอนที่ 1 Best Practices Checklist or Interview Techniques

ขั้นตอนนี้เป็นขั้นตอนพื้นฐานที่ควรทำในเบื้องต้นก่อน บางครั้งเรานิยมเรียกว่า “Gap Analysis” โดยใช้ ISO/IEC 27001 Best Practice หรือ CobiT Framework นำมาประยุกต์เป็น Audit Checklist เพื่อนำไปสัมภาษณ์ (Interview session) การตรวจสอบในขั้นตอนนี้มุ่งเน้นไปที่ PP (People and Process) ใน PPT (People,

Process and Technology) Concept กล่าวคือ ทำให้ผู้ตรวจสอบระบบสารสนเทศได้เข้าใจแนวคิดและความตระหนักเรื่องความปลอดภัยข้อมูลของผู้บริหารองค์กร ผู้ดูแลระบบสารสนเทศ ตลอดจน ผู้ใช้งานคอมพิวเตอร์ทั่วไปที่อยู่ในตารางการสัมภาษณ์ (Interview Schedule) ซึ่งปกติไม่ควรเกิน 10 คน ซึ่งแต่ละคนไม่ควรสัมภาษณ์เกิน 1 ชั่วโมง และทำให้ผู้ตรวจสอบระบบสารสนเทศได้เห็นว่า องค์กรได้นำ Information Security Best Practice หรือ Framework มาประยุกต์ใช้ในองค์กรหรือไม่ ซึ่งทางองค์กรอาจจะยังไม่ “Comply” ตาม Best Practice ดังกล่าวในบางหัวข้อ ทำให้องค์กรได้รับทราบจุดอ่อนของตนเอง เพื่อเป็นแนวทางในการตรวจสอบในขั้นตอนต่อไป

ขั้นตอนที่ 2 Vulnerability Assessment Techniques

ขั้นตอนนี้มุ่งเน้นการตรวจสอบในมุมมองของ T (Technology) ใน PPT (People, Process and Technology) Concept เป็นการตรวจสอบทางเทคนิคที่ลึกกว่าการสัมภาษณ์โดยใช้ Best Practices Checklist (ในขั้นตอนที่ 1) ซึ่งจะช่วยให้ผู้ตรวจสอบระบบสารสนเทศได้เจาะลึกถึงช่องโหว่ (Vulnerability) หรือ จุดอ่อนของระบบสารสนเทศที่สามารถตรวจสอบโดยใช้ Vulnerability Scanner เช่น Nessus (Opensource Scanner) เพื่อให้ผู้ดูแลระบบสารสนเทศเกิดความตระหนักและเห็นถึงปัญหาที่เกิดจากช่องโหว่ของระบบที่ยังไม่ได้รับการแก้ไข โดยควรนำเสนอในรูปแบบของระดับความเสี่ยงเช่น High Risk, Medium Risk หรือ Low Risk เป็นต้น

ผู้ตรวจสอบสารสนเทศจึงจำเป็นต้องมีความรู้พื้นฐานด้าน Information Security ในระดับหนึ่ง และควรมีทักษะในการใช้ Vulnerability Scanner ซึ่งถือเป็น “Tool” หรือเครื่องมือในการตรวจสอบ ที่ผู้ตรวจสอบฯ จำเป็นต้องมีไว้ใช้งาน การแปลผลจาก Vulnerability Scanner และนำเสนอผลในรูปแบบที่เข้าใจง่ายเป็นจุดสำคัญของการทำ VA หรือ Vulnerability Assessment เพราะหากแปลผลผิด เช่น ไม่ยึดตามมาตรฐาน SANS TOP 20 หรือ OWASP Web Application Security Standard ก็จะทำให้ผิดวัตถุประสงค์ในการอ้างอิงกับมาตรฐานสากล ดังนั้นการแปลผลจาก Vulnerability Scanner ควรนำมาตรฐานต่างๆ มาช่วยในการนำเสนอในรูปแบบ

PowerPoint ที่ผู้บริหารสามารถเข้าใจได้ง่าย เห็นภาพปัญหาที่อาจเกิดขึ้นกับระบบสารสนเทศได้อย่างชัดเจน

ขั้นตอนที่ 3 Penetration Testing (Pen-test) Techniques

ขั้นตอนนี้เป็นขั้นตอนสุดท้ายที่ควรจะทำต่อจากขั้นตอนที่ 2 เนื่องจากให้ผลลัพธ์ที่ลึกซึ้งและละเอียดอ่อน กว่าการทำ Vulnerability Assessment หลักการของการทำ Pen-Test หรือ การลองเจาะระบบคล้ายกับการเจาะระบบของไวรัส หรือ แฮกเกอร์ (Ethical Simulated Hacking) ทำให้ผู้ดูแลระบบเกิดความตื่นตัวในการป้องกันระบบของตน เพราะผู้ตรวจสอบฯ สามารถเข้าไปถึงข้อมูลสำคัญๆ ในระบบโดยที่ผู้ตรวจสอบฯ ไม่มี Username หรือ Password แต่อย่างใด อาศัยฝีมือในการเจาะระบบล้วนๆ เทคนิคการเจาะระบบแบ่งออกเป็นข้อย่อยดังนี้

a. Black-Box Penetration Testing

หมายถึง การเจาะระบบโดยไม่มีข้อมูลของระบบนั้นมาก่อน รู้เพียงตำแหน่งของเป้าหมาย เช่น URL หรือ IP Address ของ Web site ทาง Penetration Tester ต้องแสดงความสามารถในการเจาะระบบเข้ามา โดยอาจจะเป็นแบบ Double Blind Testing คือ ไม่บอกล่วงหน้าให้ทราบก่อนเจาะระบบ เพื่อตรวจสอบความพร้อมของผู้ดูแลระบบว่ามีการเตรียมพร้อมรับการโจมตีทุกรูปแบบทุกเวลาหรือไม่

b. White-Box Penetration Testing

หมายถึง การเจาะระบบจากภายในขององค์กร เช่น จากระบบ LAN ภายในเป็นต้น เพื่อจำลองสถานการณ์ของไวรัส หรือ เวอร์ม ที่อาจแพร่กระจายอยู่ในองค์กร หรือ จำลองว่ามีผู้บุกรุกจากข้างในองค์กรเองก็ได้เช่นกัน การเจาะระบบแบบนี้จะให้ผลลัพธ์ที่ชัดเจนกว่ามาก เพราะการเจาะระบบจากข้างในย่อมง่ายกว่าการเจาะระบบจากข้างนอกระบบเครือข่าย

ในปัจจุบัน ธนาคารแห่งประเทศไทย (Bank of Thailand) ได้ประกาศให้ High Risk Services ของธนาคารพาณิชย์ทุกแห่ง (เช่น Internet Banking) ต้องทำ

“Penetration Testing” ก่อนให้บริการระบบแก่ผู้ใช้งานทั่วไป เพื่อพิสูจน์ระดับของความปลอดภัยที่ได้มาตรฐาน เช่น OWASP Web Application Security Standard เป็นต้น จะเห็นว่า ขั้นตอนในการตรวจสอบ ทั้ง 3 ขั้นตอน เป็นแนวทางที่ผู้ตรวจสอบระบบสารสนเทศภายนอกนิยมนำมาใช้ ขณะเดียวกันผู้ตรวจสอบระบบสารสนเทศภายใน ได้มีการนำมาประยุกต์ใช้เช่นกัน กล่าวคือ การทำVulnerability Assessment นั้น สามารถทำได้โดยผู้ตรวจสอบระบบสารสนเทศภายใน โดยปกติแล้ว แนวทางการทำ Vulnerability Assessment ควรเปลี่ยนแนวทางเป็น Vulnerability Management โดยการหา Vulnerability Management Solution มาใช้แทนการทำ Vulnerability Assessment เพราะ Vulnerability Management สามารถตรวจสอบระบบได้ตลอด 24 ชั่วโมงแทนผู้ตรวจสอสำหรับการทำ Pen-test ภายใน แนะนำว่าให้จ้าง External IT Auditor มาทำจะดีกว่า เพราะถ้าผู้ตรวจสอบระบบสารสนเทศภายใน ไม่รู้วิธีในการโจมตีระบบ หรือ “Ethical Hacking” ระบบ การทำ Pen-test จึงไม่เหมาะกับผู้ตรวจสอบภายใน เรามัก “Outsource” Pen-testing ออกไปยัง MSSP (Managed Security Service Provider) หรือ Third Party Security Expert ที่มีความเชี่ยวชาญด้านนี้โดยเฉพาะ จะประหยัดค่าใช้จ่ายได้มากกว่า โดยที่ทางองค์กรไม่ต้องลงทุนกับ Vulnerability Scanner และ Pen-testing tools ในการเจาะระบบ โดย MSSP Security Expert หรือ IT External Auditor เป็นผู้รับผิดชอบแทนมาดูในส่วนของความแตกต่างระหว่างผู้ตรวจสอบภายใน (Internal Audit) หรือ ผู้ตรวจสอบที่ผ่านการรับรองโดย IIA ได้แก่ CIA หรือ (Certified Internal Auditor) และ ผู้ตรวจสอบระบบสารสนเทศภายใน (IT/IS Internal Audit) หรือ ผู้ตรวจสอบที่สอบผ่านการรับรองโดย ISACA ได้แก่ CISA (Certified Information System Auditor) ความแตกต่างที่เห็นได้ชัดคือ ผู้ตรวจสอบภายในจะมุ่งเน้นไปที่ “Internal Control” หรือ “Corporate Governance” แต่ผู้ตรวจสอบระบบสารสนเทศภายใน จะมุ่งเน้นไปที่ “IT Control” หรือ “IT Governance” โดยตรง ผู้ตรวจสอบภายในมักใช้ COSO หรือ ERM (Enterprise Risk Management) เป็น Framework ในการตรวจสอบ ขณะที่ผู้ตรวจสอบระบบสารสนเทศภายใน นิยมใช้

CobiT Framework (ปัจจุบันเป็น Version 4.0) มาเป็นแนวทางในการตรวจสอบ ผู้ตรวจสอบระบบสารสนเทศภายในมีความจำเป็นต้องเรียนรู้พื้นฐานระบบเครือข่าย เช่น OSI Model และ TCP/IP Protocol ตลอดจนพื้นฐาน Platform ที่ต้องเข้าไปตรวจสอบ เช่น Window Server 2003, UNIX/LINUX หรือ Network Devices เช่น Cisco Router เป็นต้น ตามมาตรฐาน SANS TOP20 ซึ่งอยู่ในส่วนของ General Audit สำหรับส่วนของ Application Audit ผู้ตรวจสอบระบบสารสนเทศภายในควรมีความรู้ทางด้าน Application Server เช่น Web Server IIS หรือ Apache ตลอดจนความรู้ด้านฐานข้อมูล RDBMS เช่น Oracle หรือ SQL Server รวมถึง ความรู้พื้นฐานด้าน Web Application Security เช่น มาตรฐาน OWASP ของ Open Web Application Security Project. จะเห็นได้ว่า ผู้ตรวจสอบระบบสารสนเทศฯ ต้องมีความรู้พื้นฐานด้านเทคนิค T (Technic) ใน PPT Concept มากพอสมควร ขณะที่ผู้ตรวจสอบภายใน เน้นไปที่ PP (People and Process) ใน PPT Concept มากกว่า ปัญหาปัจจุบันของการตรวจสอบระบบสารสนเทศ ก็คือ ผู้ตรวจสอบฯ ขาดความรู้พื้นฐาน และขาดประสบการณ์ในการตรวจสอบเชิงลึกในทางเทคนิค ซึ่งทำให้การตรวจสอบไม่ค่อยสัมฤทธิ์ผลเท่าที่ควร เช่น ระบบถูกตรวจสอบผ่านในมุมมองของผู้ตรวจสอบฯ แต่ระบบยังมีปัญหาติดไวรัส หรือถูกแฮกเกอร์เข้าโจมตีอยู่บ่อยๆ สาเหตุก็เนื่องมาจาก ผู้ตรวจสอบไม่ได้เจาะลึกลงไปในรายละเอียดเรื่องเทคนิคนั้นเอง ดังนั้นการตรวจสอบภายในขั้นตอนที่ 3 คือ “Penetration Testing” จึงได้รับความนิยมมากขึ้น โดยเฉพาะในกลุ่มของสถาบันการเงิน และกลุ่มสื่อสาร ที่มาตรฐานระดับของความปลอดภัยค่อนข้างสูงกว่ากลุ่มธุรกิจอื่นๆ ตลอดจนต้อง “Comply” ตาม Law และ Regulation ต่างๆ ไม่ว่าจะเป็น SOX, GLBA, HIPAA หรือ Basel II เป็นต้น

สำหรับผู้ตรวจสอบภายในนั้นสามารถพัฒนาตนเองให้เป็นผู้ตรวจสอบระบบสารสนเทศภายในได้ เช่น ผู้สอบผ่าน CIA ก็สามารถศึกษาและสอบ CISA ได้ ในทางกลับกันผู้สอบผ่าน CISA ก็อาจหันมาศึกษาและสอบ CIA เพื่อให้เข้าใจมุมมองของ “ผู้ตรวจสอบภายใน” ได้เช่นกัน กล่าวโดยสรุป ผู้บริหารระดับสูงขององค์กรควรแบ่งแยกหน้าที่ความ

รับผิดชอบของ “ผู้ตรวจสอบภายใน” และ “ผู้ตรวจสอบระบบสารสนเทศภายใน” ตลอดจนวางแผนโครงสร้างฝ่ายตรวจสอบภายใน ให้ชัดเจน และ ให้สอดคล้องกับยุคสมัยที่ความปลอดภัยข้อมูลสารสนเทศ ถือเป็นเรื่องสำคัญที่ทุกคนในองค์กรไม่ควรจะมองข้าม

บทที่ 3
การป้องกันการเจาะระบบ

รู้เขารู้เรา เป็นคำกล่าวที่ยังคงใช้ได้เสมอเมื่อมีการรบ หรือสงคราม การป้องกันการโจมตีในรูปแบบต่างๆ ก็จำเป็นที่จะต้องรู้ศัตรูว่าเขาเหล่านั้นเป็นใคร และมีจุดประสงค์หรือแรงจูงใจอะไรที่ต้องทำอย่างนั้น ดังนั้น สิ่งแรกที่ต้องรู้คือ ทำความรู้จักกับธรรมชาติของศัตรู หรือผู้ที่อาจโจมตีทำลายระบบที่ดูแลอยู่ เมื่อรู้ศัตรูแล้วก็จะสามารถกำหนดมาตรการป้องกันได้อย่างถูกทาง

ผู้ที่พยายามจะโจมตีระบบคอมพิวเตอร์ หรือข้อมูลนั้นสามารถจัดได้เป็นหลายประเภท ขึ้นอยู่กับแรงจูงใจที่กระทำอย่างนั้น ผู้โจมตีแต่ละประเภทนั้นก็ใช้เครื่องมือที่หลากหลายตั้งแต่เครื่องมือพื้นฐานไปจนถึงเครื่องมือที่ซับซ้อนและมีอำนาจการทำลายสูง เราสามารถแบ่งประเภทของผู้โจมตีระบบได้ดังนี้

ผู้โจมตี	ระดับความชำนาญ
แฮคเกอร์ (Hacker)	ปานกลาง – สูง
แคร็คเกอร์ (Cracker)	ปานกลาง – สูง
สคลิปต์คิดดี้ (Script-kiddy)	ต่ำ
สายลับ (Spy)	สูง
พนักงาน (Employee)	หลากหลาย
ผู้ก่อการร้าย (Terrorist)	ปลานกลาง – สูง

3.1 แฮคเกอร์ (Hacker)

การเจาะระบบหรือการแฮค (Hacking) คืออะไร? ซึ่งถ้าเป็นความหมายจากพจนานุกรมออนไลน์ www.dictionary.com ได้ให้ความหมายอยู่ 2 ความหมายคือ

- To write or refine computer programs skillfully.
- To use one's skill in computer programming to gain illegal or unauthorized access to a file or network: hacked into the company's intranet.

คำว่าแฮคเกอร์ (Hacker) นั้นมีความหมาย 2 แบบ โดยส่วนใหญ่เมื่อพูดถึงแฮคเกอร์ก็จะเข้าใจว่า หมายถึง บุคคลที่พยายามจะเจาะเข้าระบบโดยไม่ได้รับอนุญาต หรืออาจเรียกได้อีกชื่อหนึ่งว่าผู้โจมตี ในอีกความหมายหนึ่ง ซึ่งเป็นความหมายดั้งเดิมของคำว่า แฮคเกอร์ ซึ่งหมายถึงบุคคลผู้ใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์แต่ไม่ได้มีจุดมุ่งหมายเพื่อทำลายหรือในด้านลบ ดังนั้น ในความหมายที่สองนี้จะเป็นผู้ที่ใช้ความรู้ในทางบวก เช่น การสำรวจเครือข่ายเพื่อค้นหาเครื่องแปลกปลอม เป็นต้น อย่างไรก็ตาม การเจาะเข้าระบบคอมพิวเตอร์คนอื่นนั้นเป็นสิ่งผิดกฎหมาย แต่แฮคเกอร์จะมองว่าเป็นเรื่องที่ถูกจริยธรรม ถ้าไม่มีการขโมยข้อมูล ล้วงความลับ หรือทำลายระบบ ซึ่งนี่ก็คือจรรยาบรรณของแฮคเกอร์ (Hacker code of ethics) นั่นเอง

แรงจูงใจของแฮคเกอร์นั้นก็เพื่อการพัฒนา หรือปรับปรุงระบบเพื่อให้มีความปลอดภัยมากขึ้น ซึ่งเป็นความรับผิดชอบของพวกเขาที่ต้องค้นหาช่องโหว่หรือจุดอ่อนระบบ และแก้ไขหรือปิดช่องโหว่นั้นก่อนที่จะเกิดเหตุการณ์ที่ไม่พึงประสงค์เกิดขึ้น ความจริงก็คือโดยส่วนใหญ่ช่องโหว่หรือปัญหาของซอฟต์แวร์หรือระบบนั้นจะถูกค้นพบก่อนโดยแฮคเกอร์ไม่ใช่นักพัฒนาซอฟต์แวร์หรือฮาร์ดแวร์ แฮคเกอร์ที่มีจรรยาบรรณก็จะประกาศว่าพบช่องโหว่หรือติดต่อเจ้าของซอฟต์แวร์เพื่อให้แก้ไขปัญหาดังกล่าว ทั้งนี้แฮคเกอร์นั้นจะพยายามทำให้เกิดความเสียหายต่อระบบน้อยที่สุด และเขาเชื่อว่าสิ่งที่เขาพยายามจะทำนั้นก็เพื่อบริการสังคมโดยรวม แต่ถ้ามีผลเสียกับระบบก็จะไม่ถือว่าเป็นเรื่องอาชญากรรม และแทนที่จะโทษตัวเองก็จะกล่าวหาเจ้าของระบบว่าไม่มีการระมัดระวังหรือป้องกันที่ดี อย่างไรก็ตามไม่ว่าแฮคเกอร์จะมีแรงจูงใจในทางที่ดีหรือไม่เพียงใด แต่สิ่งที่เขาทำนั้นก็ยังเป็นคำถามอยู่ว่า เป็นเรื่องที่ถูกต้องหรือไม่

3.2 ประวัติของการรักษาความมั่นคงปลอดภัย

การโจมตีมีอยู่หลายรูปแบบ ซึ่งต่อไปนี้จะเป็นรูปแบบของการโจมตีที่มักพบเห็นหรือได้ยินอยู่เป็นประจำ

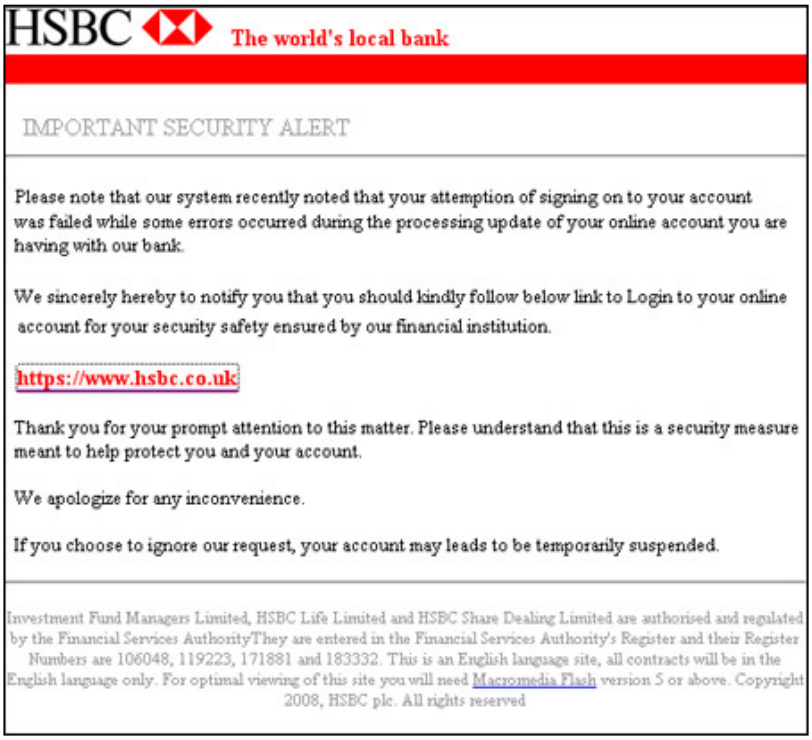
3.2.1 วิศวกรรมสังคม (Social Engineering)

การโจมตีแบบวิศวกรรมสังคม คือ ปฏิบัติการทางจิตวิทยาซึ่งเป็นวิธีที่เรียบง่ายที่สุดในการโจมตี เนื่องจากไม่จำเป็นต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์มากนัก และส่วนใหญ่จะใช้ได้ผลดี การโจมตีแบบวิศวกรรมสังคมจะเกี่ยวกับการหลอกให้บางคนหลงกลเพื่อเข้าถึงระบบ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ เป็นต้น วิศวกรรมสังคมถือเป็นจุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน

การโจมตีแบบวิศวกรรมสังคมโดยส่วนใหญ่จะใช้โทรศัพท์ถามข้อมูลโดยหลอกว่าตนเป็นผู้ที่ได้รับอนุญาตหรือเป็นผู้มีอำนาจ อีกวิธีหนึ่งก็โดยการค้นหาข้อมูลจากถังขยะ (Dumpster Diving) เพื่อค้นหาข้อมูลจากเอกสารที่ถูกทิ้งแล้ว ซึ่งในนั้นอาจมีคู่มือการใช้งาน รหัสผ่านที่เขียนไว้ในเศษกระดาษ เป็นต้น อีกวิธีหนึ่งคือ **ฟิสชิ่ง** (Phising) ซึ่งทำโดยการส่งอีเมลเพื่อหลอกให้ส่งข้อมูลให้โดยหลอกว่ามาจากผู้ที่ได้รับอนุญาต ดังรูปที่ 3.1 ยกตัวอย่างเช่น ผู้โจมตีอาจส่งอีเมลและบอกว่ามาจากองค์กรที่ถูกกฎหมายแล้วหลอกให้คลิกเข้าไปยังเว็บไซต์อื่น แทนที่จะไปเว็บไซต์จริงๆ แต่กลับเป็นเว็บไซต์หลอกที่มีหน้าตาเหมือนเว็บไซต์จริง ผู้ใช้จะถูกถามให้กรอกชื่อผู้ใช้ และรหัสผ่านเพื่อยืนยันเจ้าของบัญชีธนาคาร หรือข้อมูลเกี่ยวกับบัตรเครดิต ซึ่งผู้โจมตีก็จะได้ข้อมูลนั้นไป

การป้องกันวิศวกรรมสังคมสามารถทำได้สองทาง วิธีแรกก็โดยการทำให้องค์กรมีขั้นตอนการปฏิบัติที่เข้มงวด หรือนโยบายที่เข้มงวดเกี่ยวกับการบอกรหัสผ่านให้กับคนอื่นทราบ ส่วนอีกวิธีหนึ่งก็โดยการจัดให้มีการอบรมพนักงานเกี่ยวกับนโยบาย และการบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัย อย่างไรก็ตาม Web Browser รุ่นใหม่ส่วนใหญ่ในปัจจุบันมักที่ฟังก์ชันในการป้องกัน Phising อยู่ด้วย โดยใช้การเปรียบเทียบระหว่าง Hyper Link ที่ผู้ใช้คลิกเลือก (ไม่ใช่เว็บไซต์ที่เชื่อมไป) กับ IP

Address ที่ไปจริงๆว่าตรงกันหรือไม่ ถ้าไม่ตรงก็จะมีการแจ้งเตือนเพื่อให้ผู้ใช้ตัดสินใจเองอีกครั้ง รวมถึงเทียบกับฐานข้อมูลของการโจมตีจาก Web Browser นั้นๆ ดังรูปที่ 3.2


HSBC The world's local bank

IMPORTANT SECURITY ALERT

Please note that our system recently noted that your attemption of signing on to your account was failed while some errors occurred during the processing update of your online account you are having with our bank.

We sincerely hereby to notify you that you should kindly follow below link to Login to your online account for your security safety ensured by our financial institution.

https://www.hsbc.co.uk

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, your account may leads to be temporarily suspended.

Investment Fund Managers Limited, HSBC Life Limited and HSBC Share Dealing Limited are authorised and regulated by the Financial Services AuthorityThey are entered in the Financial Services Authority's Register and their Register Numbers are 106048, 119223, 171881 and 183332. This is an English language site, all contracts will be in the English language only. For optimal viewing of this site you will need Macromedia Flash version 5 or above. Copyright 2008, HSBC plc. All rights reserved

รูปที่ 3.1 ตัวอย่างอีเมล์ของการโจมตีแบบ Phising

(ที่มา: http://blog.activeservers.com/CategoryView,category,Dev.aspx)

รูปที่ 3.2 ตัวอย่างการแจ้งเตือนการโจมตีแบบ Phising จาก Web Browser

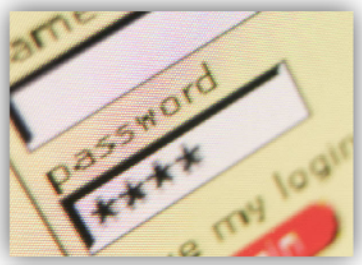
(ที่มา: http://blog.activeservers.com/CategoryView,category,Dev.aspx)

3.2.2 **การเดารหัสผ่าน** (Password Guessing)

รหัสผ่าน (Password) คือ กลุ่มตัวอักษร สัญลักษณ์ และตัวเลขที่ใช้สำหรับการพิสูจน์ทราบตัวจริงของผู้ใช้ และเป็นความลับที่เฉพาะเจ้าของเท่านั้นที่ควรทราบ รหัสผ่านจะใช้คู่กับชื่อผู้ใช้ (Username) สำหรับล็อคอินเข้าสู่ระบบ ซึ่งโดยส่วยใหญ่จะมีฟอร์มรับข้อมูล ชื่อผู้ใช้จะมีความเฉพาะไม่ซ้ำกับในระบบใดระบบหนึ่ง เช่น Administrator, Webmaster, User เป็นต้น ชื่อผู้ใช้นั้นเป็นส่วนที่เปิดเผยได้แต่รหัสผ่านนั้นเฉพาะเจ้าของเท่านั้นที่ทราบ

Note!!

ถึงแม้ว่าชื่อผู้ใช้จะเป็นข้อมูลที่ไม่ถือว่าเป็นความลับ แต่ระบบก็ไม่ควรมีการแสดงชื่อผู้ใช้ให้เองโดยอัตโนมัติ รวมถือว่าไม่ให้คำแนะนำในการกรอกชื่อผู้ใช้หรือรหัสผ่านขณะทำการล็อคอินเข้าสู่ระบบ เช่น ชื่อผู้ใช้จะมีความยาวเท่ากับ 8-10, ห้ามใช้สัญลักษณ์กับรหัสผ่าน เป็นต้น ควรมีการเตือนแค่ว่า “ชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง” หรืออาจเพิ่มเติมว่า “โปรดตรวจสอบการกดปุ่ม Caps Looks ของท่านเป็นต้น



ถึงแม้ว่ารหัสผ่านจะเป็นกลไกการรักษาความปลอดภัยแรก แต่บางครั้งก็เป็นขั้นตอนเดียวที่ใช้ป้องกันระบบ รหัสผ่านนั้นอาจถือได้ว่าเป็นจุดอ่อน เพราะผู้ใช้ในปัจจุบันโดยส่วนใหญ่จะมีชื่อผู้ใช้และรหัสผ่านประมาณ 10 คู่ที่ต้องใช้สำหรับล็อคอินเข้าสู่ระบบต่างๆ เช่น คอมพิวเตอร์ที่ทำงาน ที่บ้าน อีเมล บัญชีธนาคาร บัญชีที่สมัครใช้งานร้านค้าบนอินเทอร์เน็ต และการเข้าใช้งานของเว็บไซต์ต่างๆ เป็นต้น ดังนั้น จึงเป็นการยากที่คนๆหนึ่งจะสามารถจดจำรหัสผ่านได้มากมาย นอกจากนี้รหัสผ่านของบางระบบก็

มีอายุการใช้งาน เช่น 30 วัน หลังจากหมดอายุแล้วก็จะใช้งานไม่ได้ ต้องสร้างหรือกำหนดรหัสผ่านใหม่ ซึ่งยิ่งทำให้ยากที่จะจำรหัสผ่านปัจจุบันได้ นอกจากนี้บางระบบคอมพิวเตอร์มีระบบป้องกันไม่ให้ใช้รหัสผ่านเก่าที่เคยใช้แล้วกลับมาใช้อีก ด้วยเหตุผลเหล่านี้ทำให้ผู้ใช้หลายคนเลือกที่จะมีรหัสผ่านที่ง่ายต่อการจำ ซึ่งทำให้เป็นจุดอ่อนของระบบการรักษาความปลอดภัย รหัสผ่านที่ถือว่าง่ายต่อการเดานั้นมีคุณสมบัติคือ

- รหัสผ่านที่สั้น เช่น xyz, abc เป็นต้น
- คำที่รู้จักและคุ้นเคย เช่น password, blue, admin เป็นต้น
- มีข้อมูลส่วนตัวในรหัสผ่าน เช่น ชื่อ หมายเลขโทรศัพท์ วันเกิด เป็นต้น
- ใช้รหัสผ่านเดียวกันกับทุกๆระบบที่ใช้
- เขียนรหัสผ่านไว้บนแผ่นกระดาษแล้วเก็บไว้ในที่ๆหาได้ง่าย
- ไม่เปลี่ยนรหัสผ่านเป็นประจำถ้าไม่ถูกบังคับ

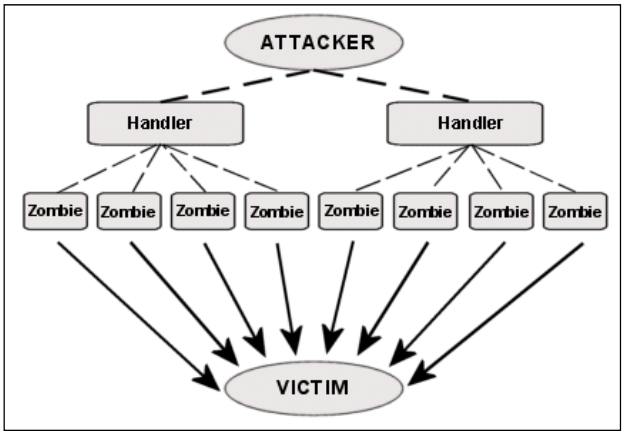
ผู้โจมตีนั้นจะใช้ประโยชน์จากจุดอ่อนนี้โดยใช้เทคนิคการเดารหัสผ่าน (Password Guessing)

3.2.3 **การโจมตีแบบปฏิเสธการให้บริการ** (Denial of Service)

การปฏิเสธการให้บริการ หมายถึง การที่เซิร์ฟเวอร์ไม่สามารถให้บริการได้เป็นเวลานาน การโจมตีแบบนี้อาจเกิดที่เครื่องเซิร์ฟเวอร์ โดยการขัดขวางไม่ให้เซิร์ฟเวอร์ใช้ทรัพยากร (Resources) ที่ทำเป็นสำหรับการให้บริการหรืออาจเกิดที่ปลายทาง โดยการขัดขวางช่องสื่อสารไปยังเซิร์ฟเวอร์ หรืออาจเกิดในระหว่างทางโดยการละทิ้งแพ็กเก็ตข้อมูลที่รับส่งระหว่างเซิร์ฟเวอร์ การรักษาความพร้อมใช้งานเป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้ได้ การโจมตีแบบปฏิเสธการให้บริการหรือการหน่วงเวลาอาจเป็นการโจมตีระบบโดยตรง หรืออาจจะเกิดปัญหาที่ไม่เกี่ยวข้องกับระบบการรักษาความปลอดภัยก็ได้

การโจมตีแบบกระจายเพื่อให้เกิดการปฏิเสธการให้บริการ (DDoS: Distributed Denial of Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถ

ให้บริการได้ ซึ่งโดยปกติจะทำโดยการใช้ทรัพยากรของเซิร์ฟเวอร์จนหมดหรือถึงขีดจำกัดของเซิร์ฟเวอร์ ทั้งนี้การโจมตีมักทำโดยผู้โจมตี (Attacker) จะทำการให้ผู้ใช้งานระบบอินเทอร์เน็ตทั่วไปสามารถเข้ามาเลือกใช้บริการต่างๆของเค้าได้ เช่นการดาวน์โหลดโปรแกรมต่างๆ เป็นต้น ผ่านทางเว็บไซต์หรือวิธีการอื่น เรียกว่า เครื่องมือ (Handler) และจะมีการแนบ Malware จำพวกม้าโทรจันไปด้วย ซึ่งเครื่องที่ติดจะเรียกว่า เครื่องผีดิบ (Zombie) ซึ่งเครื่องผีดิบเหล่านี้จะไม่แสดงอาการผิดปกติใดๆทั้งสิ้น แต่เมื่อมีการติดมากพอตามความต้องการของผู้โจมตีแล้ว (ในบางครั้งอาจเป็นล้านเครื่อง) ผู้โจมตีจะมีการสั่งให้เครื่องผีดิบเหล่านั้นทำการเรียกใช้บริการเดียวกันจากเครื่องเซิร์ฟเวอร์ของเหยื่อ (Victim) พร้อมๆกัน ดังรูปที่ 1.7 ทำให้ผู้ใช้ที่ต้องการใช้บริการจริงๆไม่สามารถใช้งานได้ หรือบางครั้งอาจทำให้เครื่องเซิร์ฟเวอร์ที่ถูกโจมตีนั้นไม่สามารถให้บริการใดๆได้อีกเลย การโจมตีแบบนี้อาจใช้โปรโตคอลที่ใช้บนอินเทอร์เน็ตทั่วไป เช่น TCP (Transmission Control Protocol) หรือ ICMP (Internet Control Message Protocol) เป็นต้น นอกจากนี้การโจมตีแบบนี้มักเป็นการโจมตีจุดอ่อนของระบบหรือเซิร์ฟเวอร์ มากกว่าการโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่อื่นของระบบรักษาความปลอดภัย อย่างไรก็ตามการโจมตีอาจทำให้ประสิทธิภาพของระบบเครือข่ายลดลงด้วย เนื่องจากการส่งแพ็กเก็ตจำนวนมากที่ถือว่าเป็นข้อมูลขยะเข้าไปในระบบเครือข่ายนั้นย่อมไปแย่งการใช้ทรัพยากรของข้อมูลที่ใช้งานอยู่จริงอย่างมาก



รูปที่ 3.3 แสดงโครงสร้างการโจมตีแบบ DDos (Distributed Denial of Service)

3.2.4 **การโจมตีการรหัสลับข้อมูล** (Cryptanalysis)

หลักการรหัสลับข้อมูล (Cryptography) เป็นคำที่มีรากศัพท์มาจากภาษากรีก 2 คำคือ Crypto ซึ่งหมายความว่า “ซ่อน” และคำว่า “Graph” หมายถึง การเขียน เมื่อนำมารวมกันแล้วจึงหมายถึง “ศาสตร์ในการแปลงข้อมูลเพื่อให้ความปลอดภัยเมื่อมีการสื่อสารหรือจัดเก็บไว้ที่ใดที่หนึ่ง” การเข้ารหัสไม่ใช่ความพยายามที่จะปกปิดความมีอยู่ของข้อมูล (Steganography) แต่เป็นการย่อยละเอียดแล้วทำให้เปลี่ยนไปอย่างเป็นระบบเพื่อให้ข้อมูลนั้นไม่สามารถอ่านได้โดยผู้ที่ไม่ได้รับอนุญาต

การเข้ารหัสเริ่มใช้เมื่อหลายศตวรรษก่อน ผู้ที่ได้รับการยกย่องว่ามีชื่อเสียงในการนำประโยชน์จากการเข้ารหัสข้อมูลมาใช้ได้เป็นคนแรกคือ จูเลียส ซีซาร์ (Julius Caesar) เมื่อเขาต้องส่งข้อมูลไปให้บรรดานายพลผู้ควบคุมกองทัพต่างๆ ซีซาร์จะเลื่อนแต่ละตัวอักษรไปสามตำแหน่งตามลำดับตัวอักษร เช่น ตัวอักษร A ก็จะถูกแทนที่ด้วยตัวอักษร D และตัวอักษร Z ก็จะถูแทนที่ด้วยตัวอักษร C เป็นต้น ซึ่งการเปลี่ยนข้อมูลเดิมให้เป็นข้อมูลที่อ่านไม่ได้เรียกว่า *“การเข้ารหัส (Encrytion)”* เมื่อนายพลต่างๆของซีซาร์ได้รับข้อความก็ทำขั้นตอนตรงกันข้าม เช่น แทนที่ตัวอักษร D ด้วยตัวอักษร A เพื่อแปลงข้อมูลให้กลับไปเป็นข้อมูลดังเดิม กระบวนการนี้เรียกว่า *“การถอดรหัส (Decrytion)”*

รูปที่ 3.4 แสดงภาพของ Julius Caesar

ความสำเร็จของความปลอดภัยในการเข้ารหัสข้อมูลนั้นขึ้นอยู่กับกระบวนการที่ใช้สำหรับการเข้าและถอดรหัสข้อความ กระบวนการนี้ขึ้นอยู่กับขั้นตอนที่เรียกว่า “วิธีคิด (Algorithm)” โดยวิธีคิดจะใช้ค่าที่เรียกว่า กุญแจ (Key)” ที่ต้องใช้ในการเข้าและถอดรหัส ยกตัวอย่างเช่น เมื่อซีซาร์ได้รับคำแนะนำให้ใช้การเลื่อนตำแหน่งตัวอักษรในการเข้ารหัส ซึ่งซีซาร์เลือกที่จะเลื่อนไป 3 ตำแหน่ง ดังนั้น ตัวเลข 3 ถือว่าเป็นคีย์ในการเข้าและถอดรหัส อย่างไรก็ตาม การเข้ารหัสด้วยการแทนที่ตัวอักษรคล้ายของซีซาร์นั้นถือว่าเป็นวิธรที่ง่ายเกินไปในปัจจุบัน ผู้โจมตีอาจตรวจสอบข้อมู,ที่เข้ารหัสแล้วและสามารถวิเคราะห์หาคีย์ได้ไม่ยาก และก็สามารถถอดรหัสทั้งข้อความได้โดยง่าย ดังนั้นวิธีคิดในการเข้ารหัสข้อมูลในปัจจุบันนั้นจะมีความซับซ้อนมากกว่า และมีขั้นตอนหรือวิธีคิดในการเข้ารหัสที่เปิดเผยเป็นที่รู้จักกันดีโดยทั่วไป แต่สิ่งที่ปกปิดให้เป็นความลับของการเข้ารหัสคือ กุญแจ โดยความยาวของกุญแจนั้นจะเป็นสิ่งที่บอกถึงความเข้มแข็งของการเข้ารหัส ยิ่งคีย์มีความยาวมากยิ่งทำให้กระบวนการในการค้นหากุญแจยากมากขึ้น แต่ในทางตรงกันข้าม ยิ่งกุญแจมีความยาวมากก็ยิ่งใช้เวลานามขึ้นในการเข้าและถอดรหัสข้อมูลด้วย

สำหรับกุญแจที่สร้างรูปแบบข้อมูลที่เหมือนกันหลายๆครั้ง จนทำให้สามารถวิเคราะห์ได้ว่า ถ้าข้อมูลมีรูปแบบนี้แสดงว่าใช้กุญแจนี้อย่างแน่นอน กุญแจประเภทนี้จะเรียกว่า “กุญแจอ่อน (Week key)” ทุกๆวิธีคิดจะมีกลุ่มของกุญแจที่มีลักษณะเช่นนี้ แต่ไม่ได้หมายความว่า วิธีคิดเหล่านี้จะใช้ไม่ได้ วิธีที่ดีที่สุดในการป้องกันก็คือ การระวังที่ไม่ให้ใช้กุญแจอ่อน โดยทั่วไปกุญแจที่มีความยาวอย่างน้อย 128 บิตนั้นจะถือว่าปลอดภัยเพียงพอในการเข้ารหัสข้อมูล

การโจมตีการเข้ารหัส (Cryptanalysis) เป็นกระบวนการที่จะให้ได้มาซึ่งกุญแจในการเข้ารหัสข้อมูล ซึ่งมีหลากหลายวิธี และวิธีหนึ่งก็คือ การใช้กระบวนการทางคณิตศาสตร์ (Mathematical Attack) ซึ่งเกิดจากการใช้การวิเคราะห์ทางสถิติของตัวอักษรที่พบในข้อความที่เข้ารหัสแล้ว แล้วใช้วิธีทางสถิติเพื่อวิเคราะห์หากุญแจที่ใช้

เข้ารหัส แล้วก็ถอดรหัสข้อมูล การป้องกันการโจมตีทางคณิตศาสตร์นี้ป้องกันได้โดยการไม่ส่งข้อมูลเหมือนกันหลายครั้ง ถ้าผู้โจมตีรู้ข้อมูลดั้งเดิมการส่งข้อมูลเดียวกันก็อาจทำให้วิเคราะห์หากุญแจได้ง่าย

3.2.5 **การสอดแนม** (Snooping)

การสอดแนมหรือการดักจับข้อมูล (Snooping) และบางทีก็มักจะใช้คำว่า สนิฟฟิง (Sniffing) หรืออาจเรียกว่า อีฟดรอปปิง (Eavesdropping) แทนก็ได้ ซึ่งหมายถึง การดักเพื่อแอบดูข้อมูล ซึ่งจัดอยู่ในประเภทการเปิดเผย การสอดแนมเป็นการโจมตีแบบไม่แสดงตัวตน (Passive) คือการกระทำที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล ยกตัวอย่างเช่น การดักอ่านข้อมูลในระหว่างที่ส่งผ่านเครือข่าย การอ่านไฟล์ที่จัดเก็บอยู่ในระบบ และการแท็ปสายข้อมูล (Wiretapping) ก็เป็นอีกวิธีหนึ่งของการสอดแนมเพื่อเฝ้าดูข้อมูลที่วิ่งบนเครือข่าย เป็นต้น

การรักษาความลับของข้อมูล เช่น การเข้ารหัสข้อมูล (Encryption) จะเป็นสิ่งที่ช่วยป้องกันภัยคุกคามประเภทนี้ได้ และนอกจากนี้การดักจับแพ็กเก็ต (Packet Sniffer) ก็อีกเป็นอีกรูปแบบหนึ่งของการโจมตีแบบสอดแนม ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกย่อยเป็นชุดเล็กๆ ซึ่งเรียกว่า แพ็กเก็ต (Packet) แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยที่ไม่ได้เข้ารหัส (Clear Text) ดังนั้น ข้อมูลอาจถูกคัดลอกและจัดการโดยเครื่องอื่นที่ไม่ใช่เครื่องปลายทางก็ได้ ทั้งนี้เน็ตเวิร์คโปรโตคอลจะเป็นตัวกำหนดหมายเลขของแต่ละแพ็กเก็ต ซึ่งเป็นสิ่งที่คอมพิวเตอร์ใช้สำหรับระบุว่าแพ็กเก็ตนั้นส่งจากไหนไปไหน เนื่องจากโปรโตคอลที่ใช้ส่วนใหญ่ เช่น TCP/IP เป็นโปรโตคอลมาตรฐานและเป็นที่รู้จักกันโดยทั่วไป ทำให้มีการพัฒนาแอพพลิเคชันที่สามารถดักจับแพ็กเก็ตที่วิ่งบนเครือข่ายได้ และที่น่ากลัวคือสามารถหาดาวน์โหลดได้จากอินเทอร์เน็ตอย่างง่ายดาย โดยที่ผู้ใช้งานไม่จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์มากก็สามารถใช้ซอฟต์แวร์เหล่านี้ได้ แพ็กเก็ตสนิฟเฟอร์เป็นโปรแกรมใช้ “เน็ตเวิร์คการ์ด (Network card หรือ LAN card)” ในโหมดโพรมิสเซียส (Promiscuous

Mode) ซึ่งในโหมดนี้เน็ตเวิร์คการ์ดจะรับทุกๆแพ็กเก็ตที่วิ่งบนสายสัญญาณแล้วส่งต่อไปยังแอพพลิเคชันเพื่อวิเคราะห์ต่อไป

Tip! *Hub VS Switch*

เมื่อเครือข่ายนั้นมีการติดตั้งอุปกรณ์ ฮับ (Hub) ซึ่งมีหน้าที่กระจายสัญญาณออกไปทุกพอร์ตที่ต่ออยู่ ทำให้ผู้ไม่หวังดีที่อยู่ในเครือข่ายเดียวกันนั้น สามารถดักจับข้อมูลทุกอย่างที่อยู่ในเครือข่ายได้ การดักจับข้อมูลแบบนี้คือ "**การสอดแนมแบบไม่แสดงตัวตน (Passive Sniffing)**" เนื่องจากผู้ดักจับไม่จำเป็นต้องแสดงตนในเครือข่าย ทำให้การตรวจหาว่าใครเป็นคนดักจับข้อมูลในเครือข่ายทำได้ยาก

ดังนั้นในเครือข่ายควรเลือกใช้อุปกรณ์ สวิตช์ (Switch) มากกว่าที่จะเลือกใช้ฮับ เนื่องจากอุปกรณ์สวิตช์นั้นจะมีการระบุปลายทางของการรับส่งข้อมูลด้วย IP Address หรือ MAC address ก่อน ถึงจะส่งข้อมูลออกไปตามสาย นั่นทำให้ผู้ไม่หวังดีที่จะดักจับข้อมูลทำได้ยากขึ้น ต้องใช้กรรมวิธีที่ยากขึ้นไปอีก ถ้าไม่อยากถูกจับได้ก็ต้องปลอมแปลง IP Address โดยเรียกการดักจับข้อมูลแบบนี้ว่า "**การสอดแนมแบบปลอมแปลงตัวตน (Active Sniffing)**" นอกจากนี้ในปัจจุบันราคาของฮับและสวิตช์ก็ไม่ได้ต่างกันแล้ว ทั้งนี้สำหรับเครื่องมือที่ผู้ไม่หวังดีใช้ในการดักจับข้อมูลสำคัญในระบบก็มีอยู่มากมาย เช่น *arpspoof*, *dnsspoof* และ *dsniff* เป็นต้น

3.2.6 การเปลี่ยนแปลงข้อมูล (Modification)

การเปลี่ยนแปลง หมายถึง การแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต ซึ่งภัยนี้จะจัดอยู่ใน 3 ประเภท คือ อาจเป็นการหลอกหลวง (Deception) ถ้าฝ่ายรับต้องใช้ข้อมูลที่ถูกเปลี่ยนแปลงแล้ว หรือข้อมูลที่ได้รับเป็นข้อมูลที่ผิดแล้วนำไปใช้งาน ถ้าการเปลี่ยนแปลงข้อมูลแล้วทำให้ระบบถูกควบคุมได้ก็จะจัดอยู่ในประเภทการทำให้ยุ่งและการควบคุมระบบ และการเปลี่ยนแปลงข้อมูลถือเป็นการแบบปลอมแปลงตัวตน (Active) ตัวอย่างเช่น การโจมตีแบบผ่านคนกลาง (Man-in-the-middle attack) เป็นต้น [ดูรายละเอียดในหัวข้อ 1.4.12]

3.2.7 **การปลอมตัว** (Spoofing)

การปลอมตัว (Spoofing) หมายถึง การทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นอีกบุคคลหนึ่ง การโจมตีประเภทนี้จัดอยู่ในทั้งประเภทการหลอกหลวงและการควบคุมระบบ การปลอมตัวเป็นการหลอกให้คู่สนทนาเชื่อว่าตนกำลังสนทนากับฝ่ายที่ต้องการสนทนาจริงๆ ยกตัวอย่างเช่น สมมติว่าผู้ใช้ต้องการที่จะล็อกอินเข้าสู่ระบบผ่านทางอินเทอร์เน็ต แต่เมื่อมีการหลอกให้ล็อกอินเข้าอีกระบบหนึ่งซึ่งผู้ใช้คนนั้นเข้าใจว่าเป็นระบบที่ตนเองต้องการล็อกอินจริงๆ หรืออีกตัวอย่างหนึ่งคือ ผู้ใช้ต้องการที่จะอ่านไฟล์แต่ผู้บุกรุกได้จัดการให้ผู้ใช้อ่านอีกไฟล์หนึ่งแทน การโจมตีแบบนี้อาจเป็นไม่แสดงตัวตนได้ กล่าวคือข้อมูลได้ถูกเปลี่ยนแปลง แต่ส่วนใหญ่จะเป็นแบบที่ปลอมแปลงตัวตน ทั้งนี้การรักษาความคงสภาพโดยการใช้การพิสูจน์ทราบตัวตน (Authentication) จะเป็นวิธีที่ใช้สำหรับป้องกันการโจมตีประเภทนี้ได้

การหลอกหลวงแบบปลอมแปลง (Masquerading) ก็เป็นอีกวิธีหนึ่งที่ใช้สำหรับปลอมตัวซึ่งจะคล้ายกับการมอบอำนาจ (Delegation) ซึ่งจะหมายถึง การที่คนหนึ่งมอบอำนาจให้อีกคนหนึ่งทำหน้าที่บางอย่างแทน การเข้าใจข้อแตกต่างระหว่างการมอบอำนาจ และการปลอมตัวนั้นเป็นสิ่งที่สำคัญ กล่าวคือ การมอบอำนาจนั้นเป็นการอนุญาตให้อีกบุคคลหนึ่งทำหน้าที่แทนตนในสิ่งใดสิ่งหนึ่ง ซึ่งผู้ที่ได้รับมอบอำนาจนั้นจะประกาศให้คนอื่นทราบด้วย และเมื่อจะกระทำการใดก็จะประกาศบอกก่อน ส่วนการปลอมตัวนั้นจะไม่มีใครรู้การกระทำนั้นเลยซึ่งรวมทั้งผู้ที่ถูกปลอมตัวด้วย ถ้าเกี่ยวกับการรักษาความปลอดภัยแล้ว การปลอมตัวเป็นสิ่งที่ผิด ส่วนการมอบอำนาจนั้นเป็นสิ่งที่ถูก

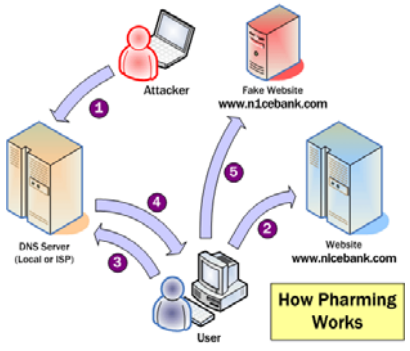
การปลอมไอพี (IP Spoofing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแสร้งว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ IP Address ข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบนี้เป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปในแพ็กเก็ตที่รับส่งระหว่างเครื่องลูกข่าย (Client) และเครื่องแม่ข่าย (Server) หรือคอมพิวเตอร์ที่สื่อสารกันในเครือข่าย การที่จะ

ทำอย่างนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติงเทเบิล (Routing table) ของเราท์เตอร์ (Router) เพื่อให้ส่งต่อแพ็กเก็ตไปที่เครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือ การที่ผู้บุกรุกสารมารถแก้ไขให้แอพพลิเคชันส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลิเคชันนั้นผ่านทางอีเมล หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชันได้โดยใช้ข้อมูลดังกล่าว

อย่างไรก็ตาม ถ้าผู้บุกรุกสามารถปรับเปลี่ยนเราติงเทเบิลเพื่อให้ส่งข้อมูลไปยังเครื่องปลอมได้ ผู้บุกรุกสามารถรับส่งข้อมูลกับแอพพลิเคชันนั้นเสมือนเป็นผู้หนึ่งในผู้ใช้ทั่วๆไปได้ การปลอมไอพีไม่จำเป็นจะต้องเป็นคอมพิวเตอร์ที่อยู่นอกเครือข่ายเท่านั้น แต่อาจจะเป็นผู้ใช้ที่อยู่ข้างในที่ไม่มีสิทธิ์ก็ได้ ซึ่งอย่างที่ทราบกันดีว่า การโจมตีเครือข่ายนั้น 90% จะเป็นการโจมตีที่เกิดจากภายในเครือข่ายเอง

Note! How Pharming Work

1. ผู้โจมตีทำการเลือกเป้าหมายเครื่อง DNS Server ที่ผู้ใช้ใช้อยู่ โดย Server นี้จะเป็นเครื่องที่ให้บริการ DNS อยู่บน LAN หรืออาจเป็น DNS Server ของ ISP ของผู้ใช้ทั้งหมดก็ได้ ผู้โจมตีจะใช้เทคนิคหลายอย่างเพื่อจัดการเปลี่ยนแปลง IP address ของชื่อเว็บไซต์ที่ต้องการมากเป็น IP address ของเครื่อง Web Server ที่ผู้โจมตีทำหลายไว้ให้มีหน้าตาเหมือนกับเว็บไซต์ตนแบบทุกประการ
2. ผู้ใช้ต้องการไปที่เว็บไซต์ที่ต้องการโดยทำการพิมพ์ชื่อเว็บไซต์ที่ Web browser
3. เครื่องคอมพิวเตอร์ของผู้ใช้ร้องถาม IP Address ของเว็บไซต์ที่ต้องการกับ DNS Server
4. DNS server ที่ถูกวางยา (Poisoned) จากผู้โจมตีจะทำการส่งค่า IP Address ของเว็บไซต์หลอกไปยังเครื่องคอมพิวเตอร์ของผู้ใช้
5. คอมพิวเตอร์ของผู้ใช้จะทำการไปยัง IP Address ที่ได้รับมาซึ่งนั้นเป็นเว็บไซต์หลอก



3.2.8 **การปฏิเสธแหล่งที่มา** (Repudiation of Origin)

การปฏิเสธแหล่งที่มา หมายถึง การไม่ยอมรับเกี่ยวกับข้อมูลที่ส่งหรือสร้างแล้วส่งไปให้ผู้รับ ยกตัวอย่างเช่น สมมติว่าบริษัทเปิดบริการขายสินค้าผ่านทางเว็บไซต์ แล้วมีลูกค้าสั่งซื้อสินค้าออนไลน์ เมื่อบริษัทได้รับการสั่งซื้อแล้วก็ส่งสินค้าให้กับลูกค้าคนนั้น เมื่อลูกค้าได้รับสินค้าแล้วแต่ปฏิเสธที่จะจ่ายเงิน โดยปฏิเสธว่าไม่ได้สั่งสินค้านั้น ลูกค้าได้ปฏิเสธแหล่งที่มาของข้อมูลนั้น ถ้าบริษัทไม่สามารถพิสูจน์ได้ว่าการสั่งซื้อนั้นมาจากลูกค้าดังกล่าวการโจมตีก็สำเร็จ การรักษาความคงสภาพเป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้ได้

3.2.9 **การปฏิเสธการได้รับ** (Repudiation of Receipt)

การปฏิเสธการได้รับข้อมูล หมายถึง การที่ผู้รับได้รับข้อมูลแล้วแต่ปฏิเสธว่าไม่ได้รับ ยกตัวอย่างเช่น ลูกค้าได้สั่งซื้อสินค้าที่มีราคาแพง ดังนั้น ทางร้านค้าจึงขอให้ลูกค้าจ่ายเงินก่อน เมื่อลูกค้าจ่ายเงินแล้วทางร้านจึงส่งสินค้าให้กับลูกค้าคนนั้น เมื่อลูกค้าได้รับสินค้าแล้วก็ทำเป็นว่าไม่ได้รับสินค้า จึงร้องขอให้บริษัทส่งสินค้าให้ใหม่ ถ้าบริษัทไม่สามารถพิสูจน์ได้ว่าลูกค้าคนนั้นได้รับสินค้าจริง การโจมตีแบบปฏิเสธการได้รับก็สำเร็จ การรักษาความคงสภาพ และการรักษาความพร้อมใช้จะเป็นสิ่งที่ใช้ป้องกันการโจมตีแบบนี้ได้

3.2.10 **การหน่วงเวลา** (Delay)

การหน่วงเวลา หมายถึง การยับยั้งไม่ให้ข้อมูลส่งถึงตามเวลาที่ควรจะเป็น การส่งข้อความหรือข้อมูลนั้นต้องใช้เวลาในการส่ง สมมติว่าโดยปกติข้อความนั้นจะส่งถึงปลายทางภายในเวลา t แต่ถ้าผู้บุกรุกสามารถหน่วงเวลาให้ข้อมูลส่งถึงปลายทางมากกว่าเวลา t แล้ว แสดงว่าการโจมตีแบบหน่วงเวลาเป็นผลสำเร็จ ซึ่งการโจมตีแบบนี้ผู้บุกรุกต้องสามารถควบคุมระบบบางส่วนได้ เช่น เซิร์ฟเวอร์หรือเครือข่าย เป็นต้น ยกตัวอย่างเช่น สมมติว่าผู้ใช้ต้องการที่จะเข้าควบคุมเซิร์ฟเวอร์ที่ให้บริการอยู่ 2

เซิร์ฟเวอร์ คือ เซิร์ฟเวอร์หลัก (Primary Server) และเซิร์ฟเวอร์สำรอง (Secondary Server) โดยเมื่อเซิร์ฟเวอร์หลักไม่สามารถให้บริการได้เซิร์ฟเวอร์สำรองก็จะทำหน้าที่แทนทันที สมมติว่าผู้บุกรุกสามารถเจาะเข้าระบบและสามารถควบคุมเซิร์ฟเวอร์สำรองได้ เมื่อผู้ใช้พยายามที่จะล็อกอินเข้าเซิร์ฟเวอร์หลัก ผู้บุกรุกก็พยายามหน่วงเวลาไว้จนทำให้ผู้ใช้เข้าใจว่าเซิร์ฟเวอร์หลักไม่สามารถให้บริการในขณะนั้นได้ จะเปลี่ยนไปล็อกอินเข้าเซิร์ฟเวอร์สำรอง ซึ่งผู้บุกรุกได้ควบคุมไว้ ดังนั้น การโจมตีแบบหน่วงเวลาก็เป็นผลสำเร็จ การรักษาความพร้อมใช้งานจะสามารถป้องกันการโจมตีแบบนี้ได้

3.2.11 การโจมตีวันเกิด (Birthday Attacks)

เมื่อเราเจอใครครั้งแรก ก็มีโอกาส 1 ใน 365 (0.27%) ที่จะมีวันเกิดเดียวกัน อย่างไรก็ตามถ้าเราเจอคนมากขึ้นโอกาสที่จะมีคนที่มีวันเกิดเหมือนกันนั้นจะเพิ่มขึ้นอย่างมาก โดยเมื่อเจอคน 23 คน เราจะมีโอกาส 50% ที่จะมีคนเกิดเหมือนกันแทนที่จะเป็น 6.3% (23 ใน 365) ถ้ามีคน 60 คน โอกาสที่จะมีคนเกิดตรงกันนั้นมีมากกว่า 99% ปรากฏการณ์นี้เรียกว่า “*Birthday Paradox*”

Note! ข้อมูลจาก http://www.securesphere.net/download/papers/dnsspoof.htm

ในกระบวนการนี้หมายถึง หากคุณถามคนที่ 1 โอกาสที่จะไม่เกิดวันเดียวกับคุณคือ 364/365 เพราะหนึ่งปีมีอีก 364 วันที่ไม่ใช่วันเกิดคุณ ซึ่งหารได้ออกมาเป็น 0.997 ดังนั้นโอกาสที่จะเป็นวันเดียวกันคือ 1 - 364/365 = 1 - 0.997 = 0.003 เมื่อถามคนที่ 2 โอกาสที่จะไม่เกิดวันเดียวกันกับคุณ และคนก่อนหน้าคือ (364/365) * (363/365) = 0.992 ดังนั้นโอกาสที่จะเกิดวันเดียวกัน จะเพิ่มเป็น 1 - 0.992 = 0.008 หากคูณวนไปเรื่อยๆ จะได้ผลดังตารางนี้

People	2	9	16	23	30	37	44	65	79
Chances	0.0027	0.0946	0.2836	0.5073	0.7063	0.8487	0.9329	0.9977	0.9999

จะเห็นได้ว่าที่ 23 คนจะมีคนที่วันเกิดตรงกันประมาณ 50% และที่ 65 คนจะพบคนที่มีวันเกิดซ้ำกันค่อนข้างแน่นอนคือประมาณ 99%

ในการเข้ารหัสข้อมูลนั้นปรากฏการณ์วันเกิดนั้นมีนัยสำคัญอย่างมาก เมื่อเราเข้ารหัสข้อมูลเราอาจจะคิดว่าวิธีที่ดีที่สุดในการเลือกกุญแจ (Key) ที่แตกต่างคือการเลือกใช้กุญแจแบบสุ่มเลือก อย่างไรก็ตามถ้าเราเลือกกุญแจแบบสุ่มเลือก โอกาสที่จะได้คีย์เหมือนกันนั้นมีมากกว่าที่เราคาดเหมือนกับปรากฏการณ์

3.2.12 **การโจมตีแบบคนกลาง** (Man-in-the-Middle Attacks)

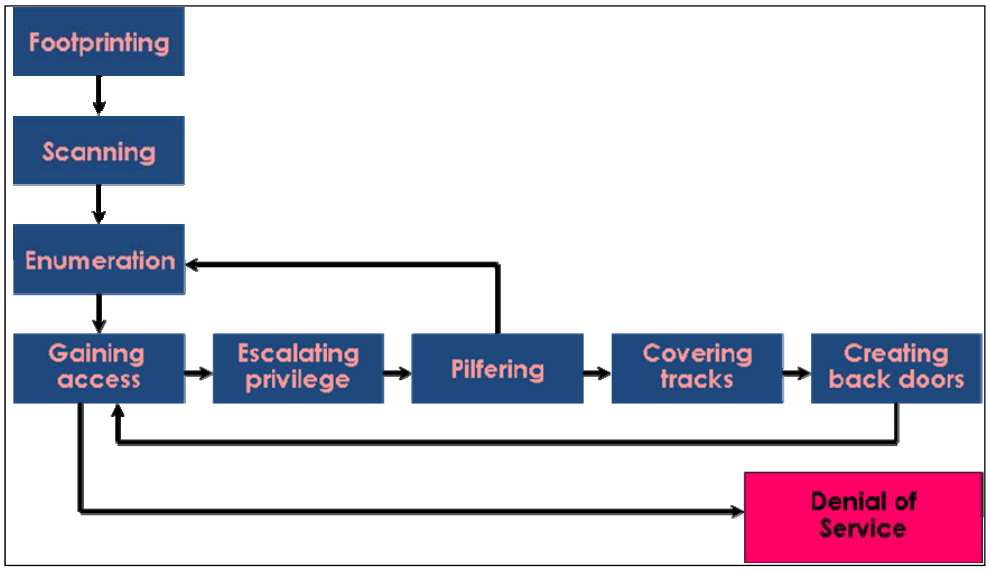
อีกรูปแบบหนึ่งของการโจมตีคือ การพยายามที่จะใช้บัญชีผู้ใช้ที่ถูกต้องในการล็อกอินเข้าไปในระบบ ซึ่งการให้ได้มาซึ่งข้อมูลเหล่านี้ก็โดยการใช้การโจมตีแบบคนกลาง (Man-in-the-middle) กล่าวคือ สมมติว่าอลิสเป็นนักเรียนชั้นประถมซึ่งสอบได้คะแนนไม่ดี ครูประจำชั้นก็เลยส่งจดหมายไปให้พ่อแม่ของอลิสให้มาพบครู อลิสทราบดีและคอยดูว่าจะมีจดหมายส่งมาถึงพ่อแม่ตัวเองเมื่อไร เมื่อจดหมายมาถึงอลิสทำการเปลี่ยนข้อความในจดหมายบอกถึงความชื่นชมในตัวอลิสที่ทำคะแนนได้ดีในวิชาคณิตศาสตร์ แล้วเธอก็เขียนจดหมายปลอมว่ามาจากพ่อแม่ของตัวเองว่าไม่สามารถเข้าร่วมประชุมได้ เมื่อพ่อแม่ได้อ่านจดหมายแล้วก็รู้สึกภาคภูมิใจในตัวลูก ในขณะที่ครูก็ไม่สงสัยว่าทำไมพ่อแม่ของอลิสไม่ยอมมาพบ อลิสใช้วิธีการโจมตีแบบคนกลางในการสื่อสารระหว่างครูกับพ่อแม่ของตัวเอง

การโจมตีแบบคนกลางของการสื่อสารผ่านระบบคอมพิวเตอร์เป็นรูปแบบที่พบเห็นได้ทั่วไป การโจมตีประเภทนี้จะทำให้คอมพิวเตอร์สองเครื่องดูเหมือนว่าจะสื่อสารกันอยู่โดยที่ไม่รู้ว่ามีคนกลางคอยเปลี่ยนแปลงข้อมูลอยู่ การป้องกันการโจมตีแบบคนกลางก็อาจใช้วิธีการเข้ารหัสข้อมูลควบคู่กับการพิสูจน์ทราบตัวจริงของคู่รับคู่ส่ง การโจมตีแบบนี้แบ่งออกเป็น 2 ประเภทคือ แบบปลอมแปลงตัวตน (Active) คือ ข้อความที่ส่งถึงคนกลางจะถูกเปลี่ยนแปลงแล้วค่อยส่งต้อถึงผู้รับ และแบบไม่แสดงตัวตน (Passive) คือการส่งต่อข้อความเดิมที่ได้รับ

การโจมตีอีกแบบหนึ่งซึ่งคล้ายกับการโจมตีแบบคนกลางคือ การโจมตีแบบทำซ้ำ (Replay Attack) คือ ข้อความที่ได้รับจากผู้ส่งจะถูกจัดเก็บไว้แล้วส่งต่อไปอีกครั้งหนึ่งเมื่อเวลาผ่านไประยะหนึ่ง

3.3 ขั้นตอนการเจาะระบบ

การเจาะระบบโดยทั่วไปแล้วสามารถแสดงได้ดังรูปที่ 3.5 ซึ่งมีขั้นตอนดังต่อไปนี้



รูปที่ 3.5 ลำดับวิธีการโดยทั่วไปของการเจาะระบบ

A. **การแกะรอย** (Footprinting)

การแกะรอย – มีเป้าหมายเพื่อให้ได้มาซึ่ง ช่วงของ Target address, ชื่อเครื่องหรือชื่อส่วนที่ต้องการบุกรุก ตลอดจนข้อมูลอื่นๆ ที่จะสามารถนำมาใช้ประกอบการโจมตีได้ แต่ทั้งนี้ข้อมูลที่หาได้ในขั้นตอนนี้ยังถือได้ว่าไม่มีรายละเอียดอะไรมากนัก

B. **การสำรวจ** (Scanning)

การสำรวจ – เป้าหมายส่วนใหญ่ของขั้นตอนนี้คือสำรวจบริการหรือช่องทางต่างๆที่เป้าหมายมีการเปิดให้บริการหรือใช้งานอยู่ แล้วทำการกำหนด หรือระบุให้ได้ว่าบริการหรือช่องทางใดที่จะใช้ในการโจมตี

C. **การระบุ** (Enumeration)

การระบุ – เป็นขั้นตอนที่ทดลองทำการรบกวนหรือบุกรุกในหลายช่องทางหรือวิธีการ เพื่อให้สามารถระบุได้ว่าควรทำการโจมตีที่ User account ใด หรือทรัพยากรส่วนใดที่มีการป้องกันไม่เข้มแข็งพอ

D. **การพยายามเข้าถึง** (Gaining Access)

การพยายามเข้าถึง – ทำการรวบรวมข้อมูลที่มีอยู่ทั้งหมดที่ต้องใช้ในการโจมตี แล้วพยายามโจมตีด้วยข้อมูลต่างๆที่มีเพื่อให้ได้มาซึ่งสิทธิ์ในการเข้าถึง (Access) ยังเป้าหมาย

E. **การเพิ่มสิทธิ์** (Escalating Privilege)

การเพิ่มสิทธิ์ – ถ้าสามารถทำการเจาะระบบจนได้สิทธิ์การเข้าถึงเป็น User ในระดับต่างๆ (จะเห็นว่าไม่ควรให้สิทธิ์กับผู้ใช้ในระบบเกินที่ต้องใช้งานจริง เพราะถ้าผู้โจมตีจะสามารถได้รับสิทธิ์เช่นเดียวกับ User ที่เจาะได้) ขั้นตอนนี้ก็จะต้องพยายามหาวิธีให้ได้สิทธิ์ที่เพิ่มขึ้น และสุดท้ายก็คือการให้ได้มาซึ่งสิทธิ์ที่สามารถเข้าควบคุมได้ทั้งระบบ (เช่น การสามารถเข้าใช้งานด้วย root เป็นต้น)

F. **การแสวงหาผลประโยชน์** (Pilfering)

การแสวงหาผลประโยชน์ – เมื่อผู้โจมตีสามารถทำอะไรกับระบบเป้าหมายได้ตามต้องการแล้ว ขั้นตอนนี้ก็จะเป็นการตักตวงผลประโยชน์ต่างๆ ที่ต้องการ ไม่ว่าจะเป็นการรวบรวมข้อมูลต่างๆ ที่ต้องการ จนกระทั้งการเพิ่มช่องทางการเข้าถึงใหม่หรือข้อมูลอื่นๆ ที่เกินกว่าที่ระบบควรจะมีหรือเคยมี ตามจุดประสงค์ของการโจมตีในครั้งนั้นๆ

G. **การกลบเกลื่อนร่องรอย** (Covering Tracks)

การกลบเกลื่อนร่องรอย – อย่างหนึ่งที่จำเป็นต้องทำเสมอเพื่อให้การโจมตีครั้งนั้นสามารถหลุดลอดความผิดไปได้ก็คือ ต้องทำการซ่อนทุกๆการกระทำที่เกี่ยวกับการโจมตีนั้น (เฉพาะที่เกี่ยวกับการโจมตีเท่านั้น)

H. **การสร้างประตูหลัง (ลับ)** (Creating Back Doors)

การสร้างประตูหลัง (ลับ) – ขั้นตอนสุดท้ายก่อนที่ผู้โจมตีจะออกจากระบบเป้าหมายก็คือ การสร้างช่องทางลับในการเข้าสู่ระบบที่จะสามารถทำให้ได้มาซึ่งสิทธิ์ต่างๆที่เคยได้มาอีกครั้งในทุกเมื่อที่ต้องการอย่างง่ายได้

I. **การทำให้เกิดสภาวะปฏิเสธการให้บริการ** (Denial of Service)

การทำให้เกิดสภาวะปฏิเสธการให้บริการ – โดยมากแล้วถ้าผู้โจมตีไม่ประสบความสำเร็จในการเจาะระบบในขั้นตอนของ Gaining access ผู้โจมตีก็มักจะทำให้ระบบเป้าหมายมีปัญหาให้มากที่สุดเท่าที่จะทำได้

3.4 การป้องกันการถูกเจาะระบบ

ผู้ใช้งานโดยทั่วไปควรมีหลักปฏิบัติเพื่อลดโอกาสที่จะถูกเจาะระบบได้สำเร็จดังต่อไปนี้

- **ใช้วิธีการจำรหัสผ่าน ดีกว่าการจดเอาไว้** แต่ถ้าคุณจำเป็นต้องจดเอาไว้ก็ต้องเก็บมันไว้ให้ไกลจากคอมพิวเตอร์ของคุณ และควรเก็บแยกจากกันกับรหัสผู้ใช้ของคุณ ถ้าให้ดีก็ควรเก็บไว้ในที่ที่ล็อคไว้ หรือในที่ที่ปลอดภัย
- **เลือกใช้วลียาว ๆ สำหรับรหัสผ่านของคุณ** นโยบายเป็นสิ่งสำคัญ และการฝ่าฝืนนโยบายอาจนำมาซึ่งความสูญเสียและความอับอาย
- **อย่าใช้รหัสผ่านที่สามารถเดาได้ง่าย** ไม่ว่าจะเป็นคำหรือตัวเลขต่างๆ เช่น ชื่อ, เลขที่บัตรประกันสังคม, วันเดือนปีเกิด เป็นต้น รวมถึงคำว่า “password” และอีกมากมายที่ง่ายในการเดา ควรเลือกใช้วลีหรือคำผสมเป็นรหัสผ่าน เพื่อทำให้การจำง่ายขึ้น
- **อย่าจดรหัสผ่านของคุณลงกระดาษแล้ววางไว้ในที่สาธารณะหรือกึ่งสาธารณะโดยเด็ดขาด** นั่นจะทำให้คุณถูกขโมยรหัสผ่านได้โดยง่าย
- **อย่าแบ่งปันรหัสผ่านของคุณกับใคร** เรียนรู้ที่จะปฏิเสธต่อคำขอ ไม่ว่าจะยากแค่ไหนก็ตาม
- **อย่าบอกรหัสผ่านของคุณให้ใครรู้** รวมถึงสามี-ภรรยา หรือแม้แต่ผู้ดูแลระบบ

- **อย่าลืมติดตั้งโปรแกรมต่อต้านไวรัสไว้บนคอมพิวเตอร์ของคุณ** และตรวจสอบไวรัสทุกครั้งก่อนเปิดใช้โปรแกรมดาวน์โหลดต่างๆ และเอกสารที่แนบมากับอีเมล์
- **ระมัดระวังในการเปิดอีเมล์** ที่มีเอกสารแนบมาด้วยโดยเฉพาะในกรณีที่คุณไม่รู้จักผู้ส่ง
- **อย่าเปิดไฟล์แนบมาด้วยนอกจากคุณรู้จริง ๆ** ว่าใครเป็นผู้ที่ส่งมันมาและรู้ว่าเป็นไฟล์แนบที่มีความจำเป็นทางธุรกิจ
- **รับมือกับอีเมล์ที่คาดว่าเป็นอีเมล์หลอกหลวงด้วยความเฉลียวฉลาด** โดยการตรวจสอบจากเว็บไซต์ ถ้ามันเป็นอีเมล์หลอกหลวงก็ให้ลบมันไป แต่ถ้ามันเป็นคำเตือนจริงๆ ก็ให้ติดต่อกับผู้จัดการฝ่ายไอทีขององค์กรคุณ
- **อย่าเข้าไปในเว็บไซต์ใด ๆ ที่คุณจะไม่เข้าหากมีผู้อื่นสังเกตการณ์อยู่** นั่นจะเป็นการป้องกันความเสี่ยงที่อาจเกิดขึ้นกับหน้าที่การงานของคุณได้
- **อย่าติดตั้งโปรแกรมใด ๆ ที่คุณไม่รู้จักที่มีถึงที่มาอย่างชัดเจน** มันอาจมีไวรัสที่สามารถทำอันตรายให้แก่การทำงานของคอมพิวเตอร์และระบบของคุณได้แฝงอยู่
- **เข้ารหัสข้อมูลที่สำคัญไว้ให้ดี** เพื่อป้องกันไม่ให้ผู้อื่นสามารถนำมันไปใช้ได้
- **กำหนดรหัสผ่านสำหรับการใช้อุปกรณ์พกพาต่าง ๆ รวมถึงเข้ารหัส**
- **ออกจากระบบโดย Log off หรือล็อคหน้าจอคอมพิวเตอร์ทุกครั้งที่ไม่อยู่ที่หน้าจอ** แม้ว่าจะเพียงไม่กี่นาทีก็ตาม
- **การลบข้อมูลหรือการ Format อุปกรณ์ที่ใช้เก็บข้อมูลไม่ได้เป็นการลบข้อมูลออกไปอย่างแท้จริง** ข้อมูลเหล่านั้นอาจยังอยู่หากการลบข้อมูลของคุณไม่มีประสิทธิภาพเพียงพอ โดยวิธีที่ง่ายและได้ผลคือ การ ด้วยโปรแกรมเฉพาะทาง

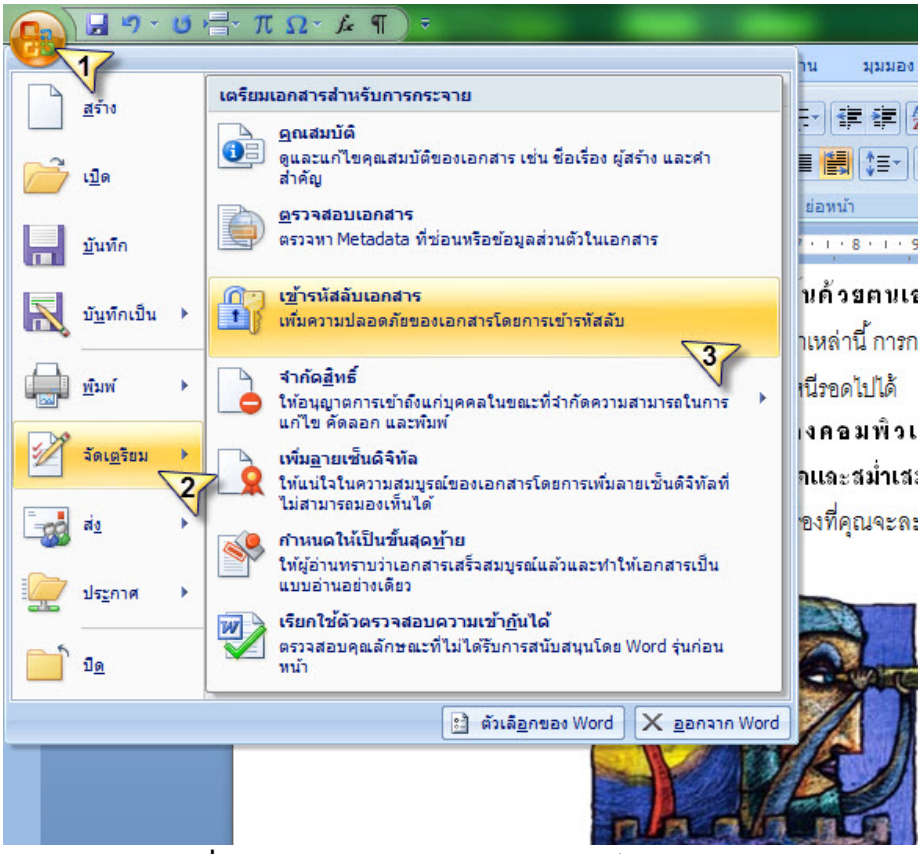
- **อย่าให้ข้อมูลข่าวสารใดๆ แก่ผู้ที่คุณไม่รู้จัก** ไม่มีบุคคลที่ไม่มีอำนาจหรือบุคคลที่ไม่อยู่ในองค์กรคนใดที่จะถามคุณเกี่ยวกับรหัสผ่านต่างๆ หรือข้อมูลอื่นๆที่คล้ายๆกันนี้
- **ทำให้แน่ใจว่าหน้าจอคอมพิวเตอร์ของคุณไม่สามารถมองเห็นได้โดยง่ายจากผู้ที่เดินผ่านโต๊ะของคุณ** เพราะมันอาจกำลังแสดงผลข้อมูลความลับอยู่ก็ได้
- **อย่าตระหนก เมื่อคุณคิดว่ามีเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยของคอมพิวเตอร์เกิดขึ้น** ให้ติดต่อไปยังทีมงานที่รับผิดชอบ เช่น CIRT (Computer Incident Response Team) หรือทีมอื่นๆที่มีหน้าที่รับผิดชอบในหน่วยงานของคุณ
- **อย่าพยายามแก้ปัญหาที่เกิดขึ้นด้วยตนเอง** CIRT มีเครื่องมือและประสบการณ์ในการจัดการกับปัญหาเหล่านี้ การกระทำของคุณอาจทำลายหลักฐานซึ่งทำให้ผู้กระทำความผิดหนีรอดไปได้
- **การรักษาความปลอดภัยของคอมพิวเตอร์ที่มีประสิทธิภาพจำเป็นต้องกระทำอย่างชาญฉลาดและสม่ำเสมอ** แม้ว่าในบางเรื่องคุณไม่ควรกังวลเกี่ยวกับมัน แต่ก็มีบางเรื่องที่คุณจะละเลยมันไม่ได้

บทที่ 4
การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูล (Encryption) เป็นกลไกหลักสำหรับป้องกันข้อมูลที่อยู่ระหว่างการสื่อสาร ถ้ามีการเข้ารหัสที่ดี ข้อมูลก็จะถูกป้องกันไม่ให้สามารถอ่านได้จากผู้ที่ไม่มีสิทธิ์ อย่างไรก็ตามผู้ใช้ที่ส่งและรับจะต้องสามารถเข้าและถอดรหัสข้อมูลนี้ได้ ระบบการเข้าและถอดรหัสไม่สามารถจะแยกแยะได้ระหว่างผู้ใช้ที่ได้รับอนุญาต หรือผู้บุกรุกถ้าผู้นั้นมีกุญแจ (Key) สำหรับการถอดรหัสข้อมูล ดังนั้น การเข้ารหัสข้อมูลอย่างเดียวไม่สามารถปกป้องข้อมูลได้ ถ้าจะให้การเข้ารหัสข้อมูลได้ผลต้องมีระบบที่ป้องกันการขโมยกุญแจที่ใช้ถอดรหัส และต้องมีการป้องกันระบบโดยส่วนรวมด้วย โดยกระบวนการเข้าและถอดรหัสนี้เหล่าเรียกว่า "หลักการรหัสลับข้อมูล (Cryptography)"

4.1 ประโยชน์ของการเข้ารหัส

การรักษาความลับของข้อมูลถือได้ว่าเป็นองค์ประกอบที่สำคัญอย่างหนึ่งของการรักษาความมั่นคงปลอดภัยของข้อมูล ซึ่งการเข้ารหัสข้อมูลจะเป็นการทำให้ข้อมูลที่เก็บหรือส่งต่อให้ผู้อื่นจะกลายเป็นข้อมูลที่ผู้ไม่มีส่วนเกี่ยวข้องสามารถเข้าใจได้ โดยในทางปฏิบัติแล้วเราจะใช้โปรแกรมต่างๆในการเข้ารหัสและถอดรหัส ซึ่งส่วนมากแล้วจะใช้รหัสผ่านในกระบวนการดังกล่าว ในที่นี้ขอยกตัวอย่างที่ท่านสามารถเข้ารหัสข้อมูลเอกสารได้ง่ายๆด้วยโปรแกรม Microsoft Word 2007 คือเลือกที่ เมนู (ไอคอน Window) > จัดเตรียม > เข้ารหัสลับเอกสาร ดังรูปที่ 4.1 แล้วทำการกรอกรหัสผ่านที่ต้องการ จากนั้นจึงเซฟไฟล์เอกสารอีกครั้ง และเมื่อจะทำการเปิดไฟล์เอกสารดังกล่าวก็จำเป็นต้องกรอกรหัสผ่านให้ถูกต้องก่อน ทั้งนี้มีข้อควรระวังก็คือถ้าลืมรหัสผ่านจะทำให้ไม่สามารถเปิดไฟล์เอกสารนั้นได้ จำเป็นต้องหาโปรแกรมในการถอดการเข้ารหัสมาใช้เพิ่มเติม



รูปที่ 4.1 แสดงภาพตัวอย่างการเข้ารหัสไฟล์เอกสาร

นอกจากนี้ยังสามารถใช้งานโปรแกรมฟรีต่างๆที่สามารถดาวน์โหลดได้จากอินเตอร์เน็ต เช่น Advanced File Shredder, Hermetic Stego, Hot Crypt และ LLCryptoLib เป็นต้น เพื่อใช้ในการเข้ารหัสไฟล์หรือโฟรเดอร์ต่างๆได้อีกด้วย

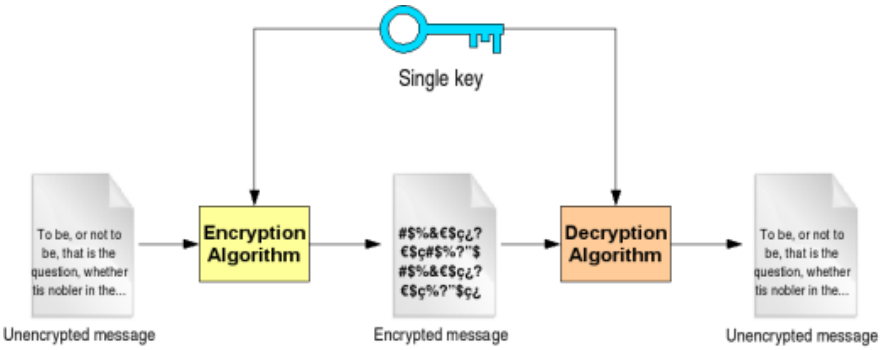
4.2 ระบบการเข้ารหัสข้อมูล (Cryptography)

รูปแบบของการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินอื่นๆ นั้นได้มีวิวัฒนาการกับกาลเวลาเหมือนกับสังคมและเทคโนโลยีอื่นๆ การเรียนรู้และเข้าใจวิวัฒนาการนี้จะช่วยให้เข้าใจระบบการรักษาความมั่นคงปลอดภัยที่มีอยู่ในปัจจุบันและอาจเป็นบทเรียนที่ช่วยให้เราไม่ต้องทำผิดเหมือนกับที่เกิดขึ้นในอดีตได้

4.2.1 Symmetric key cryptography (**หรือ** Secret key cryptography)

เป็นทฤษฎีแห่งการเก็บความลับที่ใช้ Key อันเดียวทั้งการเข้ารหัส (encryption) และการถอดรหัส (decryption) นั้นคือจะใช้key เหมือนกันทั้งผู้ส่ง และผู้รับ ซึ่งkeyที่ใช้จะมีวิธีคิด (algorithm) แบบไม่ค่อยซับซ้อนนัก ทำให้มีจุดเด่นตรงที่สามารถ encryption และdecryption ได้อย่างรวดเร็ว แต่นี้ก็เป็นข้อเสียเหมือนกัน เพราะข้อมูลนี้เมื่อ ถูกดักจับ (wiretapping) ก็จะถูกลักลอบถอดรหัสได้ไม่ยากเช่นกัน

ตัวอย่างที่นิยมที่สุดคือ *Data Encryption Standard (DES)* ซึ่ง DES คิดค้นโดย IBM แต่กลายมาเป็นมาตรฐานทีหลัง DES ใช้ key 56 bits + 8 parity bits = 64 bits โดยเข้ารหัสเป็น block ขนาด 64 bits การเข้ารหัสจะแบ่ง block ออกเป็นสองซีกซ้าย-ขวาแล้วเข้ารหัสด้วย key จากนั้นทำการสลับด้านซ้าย-ขวา ได้เป็น key ใหม่จาก key เดิม แล้วนำมาเข้ารหัสแบบเดิม ทำแบบนี้ 16 รอบถึงจะได้ออกมาเป็น *“cipher text”* (ข้อมูลที่ยังไม่เข้ารหัสจะเรียกว่าเป็น *“plain text”* พอเข้าแล้วก็จะเรียกว่า cipher text)



รูปที่ 4.2 แสดงภาพ Secret key cryptography

[ภาพจาก http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s02.html]

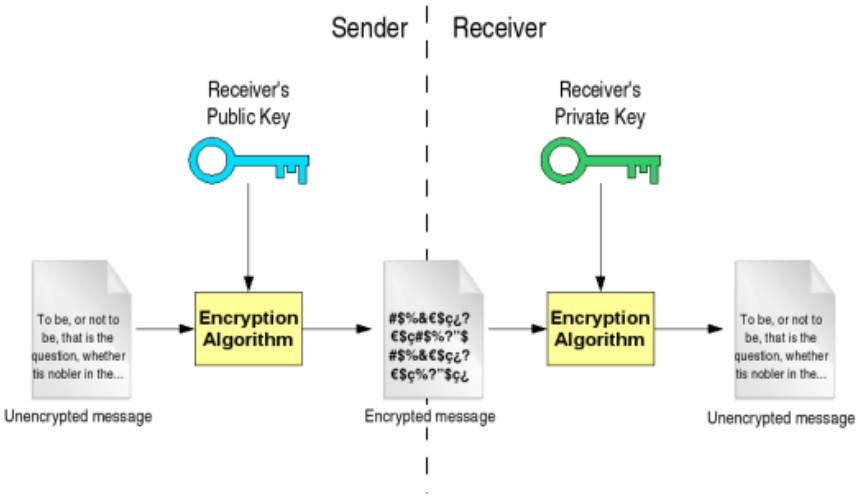
นอกจากนี้ยังมี symmetric key cryptography ที่สำคัญอยู่อีกอย่างคือ*One-time pad* คิดค้นในปี 1917 โดยบริษัท AT&T วิธีเข้ารหัสและถอดรหัสใช้แค่ exclusive-OR gates (XOR gates) อย่างเดียวและทำแค่ครั้งเดียว key ก็สร้างง่าย คือ เป็นข้อมูล

สุ่มธรรมดาทำให้ถ้าไม่มีkeyนี้จะไม่สามารถถอดรหัสได้เลย แต่ข้อเสียคือ key จะมีขนาดใหญ่มากคือเท่ากับขนาดของข้อมูลที่จะเอามาเข้ารหัส เนื่องจาก key สุ่มมา พอ XOR กับข้อมูลอะไรก็ตามมันก็จะกลายเป็นข้อมูลที่ไม่มีรูปแบบ เป็นข้อมูลที่เรียกว่า truely random แต่ก็มีปัญหาคือเรื่องการกระจายkey (key distribution) เนื่องจากต้องทำ key distribution ทุกครั้งก่อนมีการรับส่งข้อมูล ซึ่ง key อาจถูกดักจับได้ในทุกครั้ง

4.2.2 Asymmetric key cryptography (**หรือ** Public key cryptography)

เป็นทฤษฎีแห่งการเก็บความลับที่จะมี key อันหนึ่งที่ประกาศให้บุคคลทั่วไปรู้ได้ไม่เป็นความลับเรียกว่า public key และจะมี key ที่เข้าคู่กับ public key ซึ่งเก็บไว้เองเรียกว่า private key การใช้งานก็คือถ้าเราต้องการส่งข้อมูลลับไปให้ใครบางคน ก็เข้ารหัสด้วย public key ของคนนั้น เมื่อส่งไปถึง ผู้รับก็จะdecryptionข้อมูลที่เข้ารหัสได้โดยใช้ private key ซึ่งเป็นคู่ของ public key ที่เข้ารหัสมา ดังนั้นถึงจะถูกดักจับข้อมูลไปได้แต่ถ้าไม่มี private key ที่เป็นคู่ของมันก็จะdecryptionไม่ได้ โดยที่การเข้ารหัสจะใช้หลักคณิตศาสตร์ที่เรียกว่า ฟังก์ชันทางเดียว(one-way function)กลุ่มของฟังก์ชันทางเดียวส่วนหนึ่งมีความเกี่ยวข้องกับเลขจำนวนเฉพาะ(prime number)คือถ้าเอาเลขจำนวนเฉพาะสองตัวมาคูณกัน ก็จะได้จำนวนที่มีตัวประกอบเป็นเลข 2 ตัวนั้นเท่านั้น สมมติเป็น 11,927 กับ 20,903 จะได้ 249,310,081 ซึ่งการคูณ 11,927 กับ 20,903 นี้ง่ายกว่าหาตัวประกอบของ 249,310,081ยิ่งเลขจำนวนเฉพาะมีค่ามากเท่าไหร่ยิ่งจะแยกตัวประกอบยากขึ้นเท่านั้น สมมติว่า 249,310,081 เป็นข้อมูลที่เราได้รับและถ้าเรารู้จำนวนเฉพาะตัวหนึ่งเสมือนเป็นprivate key เราจะหาอีกตัวหนึ่งได้อย่างไม่ยาก

ตัวอย่างที่นิยมเช่น *RSA Cryptosystem* ซึ่ง RSA cryptosystem ตีพิมพ์โดย Ron Rivest, Adi Shamir และ Leonard Adleman ในปี 1978 โดยความเป็นจริงในปัจจุบันการเข้ารหัสด้วย 2 คีย์นี้ ระบบจะเป็นผู้คำนวณคีย์ของทั้ง 2 ฝ่ายให้เองแล้วผู้ใช้ทั้ง 2 จึงนำไปใช้ ระบบที่ว่าก็คือ Public Key Infrastructure (PKI) ดังรูปที่ 4.9 โดยใช้ฟังก์ชั่นที่เรียกว่า Modular Arithmetic (Mod)



รูปที่ 4.3 แสดงภาพ Public key cryptography

[ภาพจาก http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html]

ข้อเสียของ Asymmetric key cryptography คือการEncryption และ decryption จะใช้เวลามาก (ประมาณ100-1,000เท่าของ DES) แต่ก็จะเห็นว่า Asymmetric key cryptography นั้นมีความปลอดภัยสูงมาก เช่น RSA Cryptosystem ใช้key ขนาด 1024bits (ประมาณ 309 หลัก) ซึ่งมีkeyที่เป็นไปได้ถึง 2^{1024} แบบ สมมติให้ computer ทั่วไปทดสอบ key ได้ 1ล้านkey ต่อวินาที ใช้จำนวน1ล้านเครื่อง และใช้วิธีลองทุกทางที่เป็นไปได้ ก็ยังต้องใช้เวลาที่มากกว่าอายุของจักรวาล

4.3 การซ่อนพร่างข้อมูล (Steganography) และการป้องกัน

Steganography เป็นเทคนิคการซ่อนข้อความบนรูปภาพคล้ายลายน้ำบนธนบัตรหรือการนำสบู่มาใช้ เขียนข้อความลงบนกระดาษซึ่งกระดาษยังคงดูเหมือนกระดาษธรรมดาทั่วไป แต่เมื่อทำให้กระดาษเปียกน้ำก็จะปรากฏข้อความที่ถูกเขียนด้วยสบู่ขึ้น แต่ในเชิงดิจิตอลแล้วก็คล้ายกันคือการซ่อนไฟล์หรือข้อความลงบนไฟล์รูปภาพแบบดิจิตอลซึ่งดูภายนอกก็คล้ายกับไฟล์รูปภาพธรรมดาและยังมีการเข้ารหัสข้อมูลทำให้บุคคลที่ไม่มีรหัสผ่านที่ถูกต้องก็จะไม่สามารถเข้าถึงข้อความที่ซ่อนอยู่ ภายในภาพได้เช่นกัน

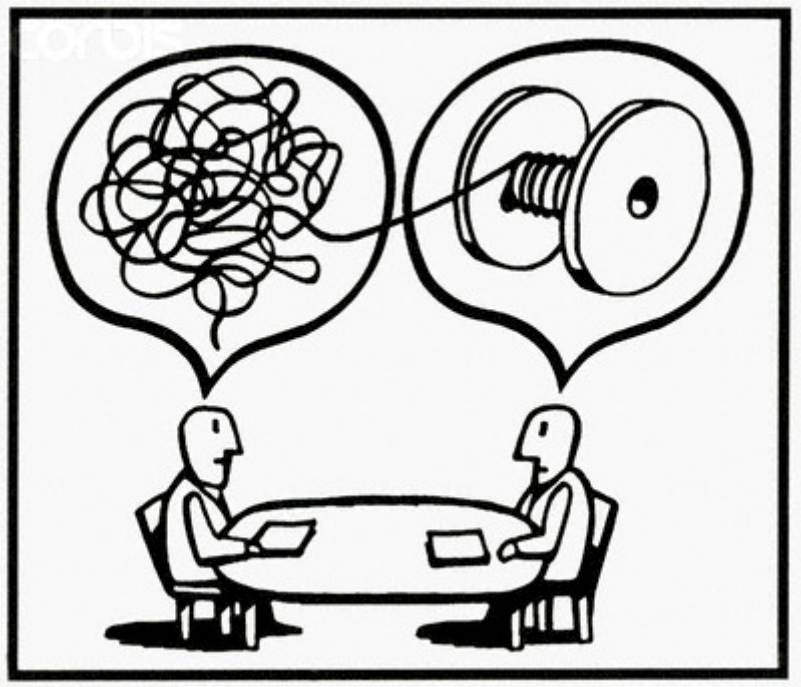
การทำ Steganography นั้นถือเป็นการเข้ารหัสทางคอมพิวเตอร์วิธีหนึ่งที่มีการใช้กันอย่างแพร่หลาย และ มีประสิทธิภาพสูง มีการใช้ Steganography ไปในทางที่ผิด ตัวอย่างเช่น ใช้ในการก่อการร้ายถล่มตึก World Trade Center โดยผู้ก่อการร้ายทำการซ่อนข้อความลับหรือไฟล์ลับลงในไฟล์รูปภาพธรรมดารูปหนึ่ง ซึ่งดูเหมือนไฟล์รูปภาพปรกติธรรมดาทั่วไปแล้วทำการส่ง Email ให้กับผู้ก่อการร้ายอีกกลุ่มหนึ่ง ทางฝ่ายที่ได้รับรูปภาพที่แฝงข้อความลับไว้จะต้องทำการถอดรหัสรูปภาพรูปนั้นด้วยการถอดรหัสทางคอมพิวเตอร์ ผู้ที่จะสามารถถอดรหัสได้จะต้องมีเครื่องถอดรหัสหรือ key ซึ่งมีกลไกการเข้ารหัสที่ตรงกับฝั่งต้นทางที่เข้ารหัสไว้ก็จะสามารถถอดรหัสเพื่อเข้าถึงข้อความลับที่ซ่อน อยู่ภายในรูปภาพได้

รูปที่ 4.4 แสดงภาพตัวอย่างโปรแกรมที่ใช้ในการซ่อนพรางข้อมูล

[ภาพจาก http://xiao-steganography.en.softonic.com/]

ในการป้องกันภาพที่มีการทำ Steganography สามารถทำได้หลายวิธี เช่น ตรวจสอบโดยใช้ โปรแกรม md5sum.exe, โปรแกรมป้องกันโปรแกรมประสงค์ร้าย หรือโปรแกรมอื่นๆที่ต้องกับการใช้ Steganography นั้นๆ รวมถึงการสังเกตขนาดของไฟล์ว่าใหญ่ผิดปกติหรือไม่ด้วยตนเอง เป็นต้น นอกจากนี้ในทางเทคนิคก็ยังมีการตรวจสอบที่

รหัสข้อมูล (Data code) ซึ่งสามารถตรวจสอบได้โดยผู้เชี่ยวชาญ แต่ทั้งนี้ปัญหาที่แท้จริงคือโดยทั่วไปไว้ผู้ที่ไม่เกี่ยวข้องกับกระบวนการซ่อนนั้นๆ ก็จะไม่สนใจกับไฟล์ต่างๆที่พบเจอว่ามีการใช้เทคนิค Steganography หรือไม่ ดังนั้นการป้องกันที่ดีที่สุดสำหรับผู้ใช้ทั่วไปก็คือการมั่นตรวจสอบไฟล์ที่มีความผิดปกติ (เช่นขนาดใหญ่มากกว่าปกติ) และไม่รับไฟล์ทุกประเภทจากแหล่งที่ไม่ทราบที่มา



บทที่ 5
หลักการทำงานของไฟล์วอลล์ (Firewall)

ไฟล์วอลล์ (Firewall) หากจะแปลตรงตัวจะแปลว่ากำแพงไฟ แต่แท้ที่จริงแล้วอุปกรณ์ไฟล์วอลล์ทำหน้าที่เป็นเสมือนกำแพงที่มีไว้เพื่อป้องกันไฟ ส่วนสาเหตุที่ทำไมสัญลักษณ์ของ ไฟล์วอลล์จึงเป็นกำแพงอิฐสีส้ม เนื่องจากว่าสิ่งปลูกสร้างต่างๆ มักจะนิยมทำด้วยอิฐเพื่อแยกส่วนต่างๆ ของสิ่งปลูกสร้างออกจากกัน เพื่อที่ว่าในเวลาที่เกิดไฟไหม้ ไฟจะได้ไม่ลุกลามไปถึงสิ่งก่อสร้างในส่วนอื่นๆ ตามศัพท์บัญญัติจะแปลไฟล์วอลล์ว่าเป็นด่านกันการบุกรุก [1] อุปกรณ์ไฟล์วอลล์สามารถแบ่งได้เป็นสองประเภทได้แก่ แบบซอฟต์แวร์หรือแบบฮาร์ดแวร์ในระบบเครือข่าย ทั้งสองแบบนี้ทำหน้าที่เป็นตัวกรองข้อมูลสื่อสารระหว่างเขตต่างๆ

5.1 ประเภทของไฟล์วอลล์

การแบ่งประเภทตามการทำงานของไฟล์วอลล์โดยทั่วไปจะถูกแบ่งออกเป็น 3 ประเภทคือ Network Level Firewall, Circuit-Level Firewall และ Application Level Firewall แต่ในบทนี้จะกล่าวถึงเฉพาะแบบแรก

5.1.1 Network Level Firewall

เรียกอีกอย่างว่า Packet Filter โดยจะพิจารณจากข้อมูลในส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้ ซึ่งมีหลักการทำงานเหมือนกับเราท์เตอร์โดยทั่วไปเพียงแต่เป็นการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข การทำงานของไฟล์วอลล์ประเภทนี้จะอยู่ตั้งแต่เลเยอร์ที่สามถึงเลเยอร์ที่สี่

การกรองข้อมูลในเลเยอร์สาม (Internet layer) จะพิจารณาจากฟิลด์ (filed) ต่างๆ ดังนี้

- ไอพีต้นทาง
- ไอพีปลายทาง
- ชนิดของโปรโตคอล (TCP UDP และ ICMP)

การกรองข้อมูลในเลเยอร์สี่ (Transport layer) จะพิจารณาจากฟิลด์ (filed) ต่างๆ ดังนี้

- พอร์ตต้นทาง
- พอร์ตปลายทาง
- แฟล็ก (Flag ซึ่งจะมีเฉพาะในเฮดเดอร์ของแพ็กเก็ต TCP)
- ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์ คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 22 หมายถึง SSH, พอร์ต 23 หมายถึง Telnet เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ Packet Filtering สามารถอิมพลีเมนต์ (implement) ได้จาก 2 แพล็ตฟอร์ม คือ

1. เราเตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว)
2. คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์ อย่างเช่น ลีนุกซ์เซิร์ฟเวอร์ ซึ่งสามารถใช้ iptables ในการทำ Packet Filtering

5.1.2 Stateful Inspection Firewall

Stateful Inspection Firewall มีหลักการทำงานทุกอย่างเช่นเดียวกันกับ Packet Filtering Firewall แต่มีส่วนที่เพิ่มขึ้นมาคือ จะมีการบันทึกเกี่ยวกับการเชื่อมต่อที่เกิดขึ้นลงใน **State Table** (หรือบางครั้งอาจเรียกว่า State Info) ก่อนที่จะส่ง packet นั้น

ต่อไปให้ Layer อื่น ซึ่ง State Table นี้จะใช้สำหรับการบันทึกข้อมูลของแต่ละการเชื่อมต่อที่เกิดขึ้น โดยปกติจะเก็บข้อมูลเกี่ยวกับ Source IP Address, Destination IP Address, Protocol Type, Port Number และ Flag แต่ก็มี Firewall บางยี่ห้อที่เก็บข้อมูล **sequence number** เพิ่มด้วย เพื่อใช้ในการตรวจสอบ packet ที่กำลังจะเข้ามาและป้องกันการทำ **session hijacking** (เป็น การเข้าควบคุม TCP communication session ที่กำลังใช้งานอยู่ระหว่าง client กับ server)

เมื่อ Firewall ได้รับ packet ก็จะทำการตรวจสอบข้อมูลกับของ State Table ว่าเป็นส่วนของการเชื่อมต่อที่สร้างไว้แล้วหรือไม่ โดยพิจารณาจากข้อมูล Source IP Address, Destination IP Address, Source Port และ Destination Port ซึ่งจะต้องสอดคล้องกับ State Table และถ้าเป็นส่วนหนึ่งของการเชื่อมต่อจริงก็ไม่มีความจำเป็นที่จะต้องตรวจสอบซ้ำอีกครั้ง (ใน Firewall บางยี่ห้อนั้นจะพิจารณา sequence number ของ packet เพิ่มเติมด้วย เช่น Cisco PIX ในขณะที่ Checkpoint Firewall-1 จะไม่พิจารณา sequence number แต่อย่างใด) จึงทำให้ Stateful Inspection Firewall ทำงานได้เร็วมากในกรณีนี้

แต่ถ้า Packet ที่ส่งมาไม่ตรงกับการเชื่อมต่อที่สร้างไว้ และไม่ใช่ SYN packet ก็จะทำให้ packet นั้นถูกทิ้งไป และแม้แต่ packet ที่มี Flag แปลกๆ อย่างเช่น **SYN/FIN** (เป็นกระบวนการหนึ่งในการทำ Scaning Port) ก็จะถูกทิ้งไปเช่นเดียวกัน ทั้งนี้ Firewall ส่วนใหญ่จะสามารถบันทึก Log file ได้ด้วย ซึ่งขึ้นอยู่กับการตั้งค่าของผู้ดูแลระบบเองว่าต้องการเก็บข้อมูลใด และข้อมูลที่เก็บไว้ใน Log file นี้ก็อาจนำมาใช้วิเคราะห์และรายงานเกี่ยวกับความพยายามที่จะเจาะเข้ามาในระบบโดยไม่ได้รับอนุญาตได้อีกด้วย

ในกรณีที่ Firewall ได้รับ UDP packet นั้น เนื่องจากโปรโตคอล UDP ไม่มีกระบวนการ 3-Way handshake ทำให้ไม่มี sequence number แต่ทั้งนี้ก็ยังมี Source IP Address, Destination IP Address, Source Port และ Destination Port ซึ่งจะถูกสร้างขึ้นใน State Table ทำให้ยังสามารถใช้งานได้อยู่ในระดับหนึ่ง ถึงอย่างนั้นด้วยเหตุ

ที่ UDP ไม่มี FIN หรือ RST ซึ่งใช้สำหรับยกเลิกการเชื่อมต่อเหมือนกับ TCP ดังนั้นอาจทำให้ต้องมีการตั้งเวลา **Timeout** เพื่อลบข้อมูลออกจาก State Table ด้วย อย่างไรก็ตามจำเป็นต้องมีวิธีในการลบข้อมูลออกจาก State Table โดยเฉพาะสำหรับการเชื่อมต่อแบบ TCP เช่นกัน เนื่องจากอาจถูกโจมตีโดยการส่ง SYN Packet จำนวนมากเข้ามาใน Firewall (**SYN Flood**) ซึ่งถือเป็นการโจมตีแบบ DoS เพราะอาจทำให้ State Table เต็ม ปัญหานี้สามารถแก้ไขได้โดยการตั้ง Timeout ของแต่ละการเชื่อมต่อไว้เช่นเดียวกับ UDP

ในกรณีของ Packet Filtering Firewall เราจำเป็นต้องกำหนดนโยบาย (Policy) ทั้งสำหรับ packet ที่วิ่งเข้ามาในเครือข่าย และ packet ที่จะส่งออกไปข้างนอก ในขณะที่ Stateful Inspection Firewall นั้นสามารถระบุได้แค่ข้างเดียวเท่านั้น เนื่องจาก packet ที่ส่งตอบกลับมานั้นจะถือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่ได้สร้างไว้ก่อนแล้ว แต่มีข้อยกเว้นเหมือนกัน เช่น Checkpoint Firewall-1 นั้นต้องการระบุนโยบายแยกกันสำหรับการใช้งาน ICMP Echo Request และ ICMP Echo Reply

5.1.3 Application Layer Firewall

Application Layer Firewall เป็น Firewall ที่ทำงานในระดับ Application (ในบางครั้งก็ถูกเรียกว่า **Proxy Firewall**) ซึ่งอาจหมายถึงโปรแกรมที่ทำงานบนระบบปฏิบัติการทั่วไป เช่น Window Server หรือ UNIX เป็นต้น หรืออาจหมายถึง Hardware ที่ติดตั้ง Software มาพร้อมใช้งานแล้วก็ได้ โดย Firewall นี้จะมี Network Card หลายตัวเพื่อไว้สำหรับเชื่อมต่อกับเครือข่ายต่างๆ ซึ่งนโยบายการรักษาความมั่นคงปลอดภัยจะเป็นสิ่งที่กำหนดว่า Traffic ใดสามารถถ่ายโอนระหว่างเครือข่ายได้บ้าง ถ้านโยบายไม่ได้ระบุอย่างชัดเจนว่า Traffic นั้นอนุญาตให้ผ่านไปได้หรือไม่ Firewall ก็จะไม่ส่งผ่าน packet เหล่านั้นทันที ทั้งนี้ในเรื่องของนโยบายนั้นจะถูกบังคับใช้โดย Proxy ของ Firewall ใน Application Layer โดยทุกๆโปรโตคอลที่อนุญาตให้ผ่านได้จะต้องมี Proxy สำหรับโปรโตคอลนั้นๆ ด้วย ซึ่ง Proxy ที่ดีที่สุดก็ควรหมายถึง Proxy ที่ออกแบบมาสำหรับจัดการกับโปรโตคอลนั้นๆ โดยเฉพาะ

Proxy Firewall จะตรวจสอบข้อมูลใน Network Layer และยังสามารถตรวจสอบความถูกต้องใน Application Layer ได้อีกด้วย ซึ่งทำให้ Proxy Firewall สามารถกรองคำสั่ง, โปรโตคอล, ความยาวของ packet, สิทธิ์ในการใช้งาน, เนื้อหาข้อความ และความถูกต้องของ Header หรือสามารถส่งผ่าน packet ไปได้เลย และอาจมองได้ว่า Proxy Firewall เป็น Stateful Inspection Firewall ที่จะทำการสร้าง IP packet ใหม่ เพื่อส่งต่อไปยังเป้าหมายทั้งนี้ก็เพื่อป้องกันการสร้าง packet ที่ผิดปกติ โดยจะสร้างและส่งต่อไปเมื่อ packet นั้นผ่านการตรวจสอบแล้ว

สำหรับ Firewall ที่ทำงานใน Application Layer นั้นทกๆ การเชื่อมต่อจะสิ้นสุดที่ Firewall โดยการเชื่อต่อจะเริ่มจาก Client ส่งการร้องขอไปยัง Firewall หลังจากนั้น Firewall ก็จะตรวจสอบกับนโยบายด้านความมั่นคงปลอดภัยว่าจะให้อนุญาต Traffic นี้ผ่านหรือไม่ ถ้าอนุญาต Firewall ก็จะสร้างการเชื่อมต่อกับ Server แทน Client เอง และนอกจาก Firewall ยังสามารถควบคุมการเชื่อมต่อจากภายในไปภายนอกได้แล้ว Firewall ยังสามารถควบคุมการเชื่อมต่อจากภายนอกมาภายในได้เช่นกัน ดังนั้น Firewall จึงสามารถป้องกันการโจมตีเครือข่ายในระดับ Application ได้ *อย่างไรก็ตามตัวของ Firewall เองจะต้องมีความปลอดภัยจากการโจมตีด้วยเช่นกัน*

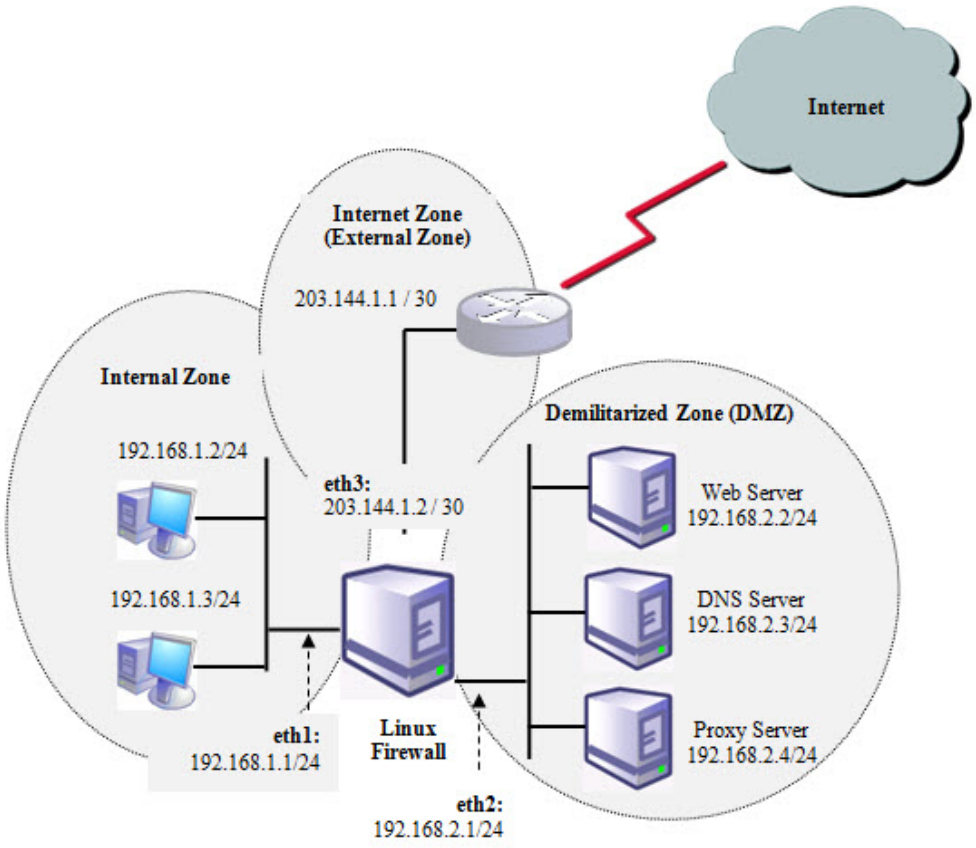
Firewall ที่ทำงานในระดับ Application ส่วนใหญ่ในปัจจุบันจะมี Proxy สำหรับโปรโตคอลที่นิยมใช้ เช่น HTTP, SMTP, FTP และ Telnet เป็นต้น ถ้าโปรโตคอลใดไม่มี Proxy ก็จะไม่สามารถผ่าน Firewall ได้ นอกจากนี้แล้ว Firewall ประเภทนี้ยังสามารถซ่อน IP Address ของระบบภายในได้ด้วย เนื่องจากการเชื่อต่อทั้งหมดจะสิ้นสุดที่ Firewall ดังนั้นเครื่องที่อยู่ภายนอกจะมองเห็นเฉพาะหมายเลข IP Address ของ Firewall เท่านั้น ถ้าผู้โจมตีไม่รู้โครงสร้างภายในโอกาสที่จะสามารถเจาะระบบได้จึงน้อยลงไป

5.2 นโยบายการรักษาความปลอดภัย

โดยพื้นฐานจะแบ่งเขตออกเป็น 3 เขต (zone) ได้แก่ เขตแรกคือ อินเทอร์เน็ตซึ่งเป็นเขตที่ไม่น่าเชื่อถือเนื่องจากเป็นส่วนที่อยู่หน้าอุปกรณ์ไฟล์วอลล์ เขตที่สองคือ อินทราเน็ตซึ่งเป็นเขตปลอดภัยเนื่องจากอยู่หลังอุปกรณ์ไฟล์วอลล์ โดยทั่วไปเครื่อง

คอมพิวเตอร์ของยูสเซอร์ทั่วไปจะอยู่ในเขตนี้ และในเขตที่สามคือ DMZ (Demilitarized Zone) ซึ่งโดยทั่วไปเครื่องเซิร์ฟเวอร์จะอยู่ส่วนนี้ ทั้งสามเขตนี้แสดงดังรูปที่ 13.1

ในไฟล์วอลล์จะมีการกำหนดกฎและระเบียบมาบังคับใช้ซึ่งกฎเหล่านี้นิยมเรียกว่าเป็นโพลิซี (Policy) โดยหลักการทำงานของไฟล์วอลล์ประกอบไปด้วยกลไกสองส่วน โดยส่วนแรกมีหน้าที่ในการกั้น Traffic และส่วนที่สองมีหน้าที่ในการปล่อย Traffic ให้ผ่านไปได้



รูปที่ 5.1 แสดงการเชื่อมต่อของระบบเครือข่ายคอมพิวเตอร์

5.3 นโยบายการรักษาความปลอดภัย

ประเภทของไฟล์วอลล์ที่มีอยู่โดยทั่วไปในปัจจุบันมีอยู่ 2 ประเภทขั้นตอนแรกในการเลือกไฟล์วอลล์คือการพิจารณาว่าไฟล์วอลล์ประเภทใดที่เหมาะกับการใช้งานของคุณ โดยดูจากตัวเลือกต่อไปนี้

- ซอฟต์แวร์ไฟล์วอลล์

  เป็นโปรแกรมไฟล์วอลล์ที่ใช้ติดตั้งบนเซิร์ฟเวอร์

  ข้อดีคือ ราคาไม่แพง

  ข้อเสียคือ มีประสิทธิภาพไม่สูงในการประมวลผล

- ฮาร์ดแวร์ไฟล์วอลล์

  เป็นอุปกรณ์ไฟล์วอลล์ที่ทำหน้าที่ในการเป็นไฟล์วอลล์โดยเฉพาะ

  ข้อดีคือ มีประสิทธิภาพสูงในการประมวลผล

  ข้อเสียคือ ราคาแพง

บทที่ 6
การใช้งานระบบตรวจจับการบุกรุก IDS/IPS

ในบทนี้จะกล่าวถึงระบบตรวจจับการบุกรุก หรือ Intrusion Detection System (IDS) ซึ่งเป็นระบบรักษาความปลอดภัยสารสนเทศพื้นฐานที่ทุกองค์กรควรติดตั้งไว้ IDS จะสามารถค้นหาสิ่งผิดปกติในเครือข่ายหรือในระบบที่อาจจะเป็นการบุกรุก เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบและองค์กร ในหัวข้อที่จะกล่าวถึงได้แก่ หลักการของ IDS ชนิดของ IDS วิธีหรือกลไกในการตรวจจับ เทคโนโลยีของ IDS การออกแบบเพื่อติดตั้งในระบบ รวมทั้งวิธีการติดตั้งและใช้งาน Snort IDS ซึ่งเป็น IDS ที่เป็นที่นิยมในปัจจุบัน [1]

ระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) เป็นชุดฮาร์ดแวร์หรือซอฟท์แวร์ที่ทำหน้าที่คอยเฝ้าระวังและตรวจจับสิ่งผิดปกติที่อาจเป็นการบุกรุก หรือพฤติกรรมที่เป็นการละเมิดมาตรการรักษาความปลอดภัยสารสนเทศ ทั้งที่เกิดขึ้นบนระบบคอมพิวเตอร์และในเครือข่าย (network) ซึ่งเหตุการณ์ผิดปกติทางด้านความปลอดภัยสารสนเทศ (incident) ดังกล่าว อาจเกิดจากการแพร่กระจายของไวรัสคอมพิวเตอร์ การเข้าถึงระบบโดยมิได้รับอนุญาตจากผู้ใช้งานจากอินเทอร์เน็ต การกระทำของผู้ใช้งานระบบที่เป็นการละเมิดมาตรการรักษาความปลอดภัยสารสนเทศ เช่น การพยายามเข้าถึงข้อมูลที่ตนไม่มีสิทธิ หรือการพยายามเพิ่มสิทธิในการใช้งานระบบ เป็นต้น

6.1 ประเภทของ IDS

สามารถแบ่งชนิดของ IDS ได้ดังนี้

6.1.1 Network-based IDS

เป็น IDS ที่ถูกติดตั้งในลักษณะขวาง network traffic บริเวณจุดที่เป็นทางเข้าหรือทางออกของ network segment ที่ต้องการตรวจจับ เพื่อให้อุปกรณ์ IDS สามารถมองเห็นข้อมูลที่เข้าออกทั้งหมดและวิเคราะห์พฤติกรรมการรับส่งข้อมูลทั้งในระดับ network layer และ application layer

6.1.2 Host-based IDS

IDS ชนิดนี้จะเป็น software ที่ติดตั้งอยู่บน server ที่มีความสำคัญ เพื่อตรวจจับเหตุการณ์หรือพฤติกรรมผิดปกติที่เกิดขึ้นเฉพาะ server นั้น เช่น การ login เข้าระบบผิดซ้ำกันหลายครั้ง การเข้าระบบในช่วงเวลาที่ไม่ใช่เวลาทำงานปกติ หรือการส่งไฟล์ขนาดใหญ่ออกไปยังเครื่องคอมพิวเตอร์อื่น เป็นต้น โดยทั่วไปแล้วเหตุการณ์ที่ Host-based IDS สามารถเฝ้าระวังได้ ได้แก่ network traffic (ของ server นี้เท่านั้น), system log, running process, application activity, การเข้าถึงและการเปลี่ยนแปลงของไฟล์, การเปลี่ยนแปลงของค่า configuration ของระบบ

6.1.3 Network Behavior Analysis IDS

ใช้ตรวจหา network traffic flow ที่ผิดปกติ เช่น การโจมตีแบบ Denial of Service (DoS), การเข้ามาของ malware, การกระทำผิดต่อมาตรการรักษาความปลอดภัยสารสนเทศ เช่น มีการรับส่งข้อมูลระหว่าง server โดยที่ไม่ได้รับอนุญาต ฯลฯ โดยทั่วไปจะติดตั้งเพื่อเฝ้าระวัง traffic flow ในเครือข่ายภายในขององค์กร หรือระหว่างองค์กรกับภายนอก

6.1.4 Wireless IDS

ใช้เฝ้าระวัง wireless network traffic เพื่อวิเคราะห์การรับส่งข้อมูลผ่าน protocol ของ wireless ใน network layer โดยเฉพาะ เช่น การเข้าถึงโดยไม่ได้รับอนุญาต, rogue access point, การพยายามโจมตีค้นหา WEP key ฯลฯ และไม่มีวัตุ

ประสงค์ในการตรวจจับหาสิ่งผิดปกติที่เกิดขึ้นใน layer ที่สูงกว่าเช่น transport หรือ application

6.2 การวิเคราะห์และตรวจจับการบุกรุก

6.2.1 การใช้งาน IDS

IDS ถูกใช้งานเพื่อค้นหาการเหตุการณ์ที่เป็นไปได้ว่าจะเป็นการบุกรุกจากผู้ไม่ประสงค์ดีเป็นหลัก สามารถตรวจจับการโจมตีเมื่อมีผู้บุกรุกสามารถเข้าถึงระบบได้สำเร็จผ่านทางช่องโหว่ต่างๆของระบบ เมื่อพบการบุกรุกดังกล่าว IDS จะส่งสัญญาณเตือน (alert) ไปยังผู้ดูแลระบบเพื่อให้ดำเนินการตรวจสอบและยับยั้งการบุกรุกนั้นต่อไป การติดตั้ง IDS จึงช่วยในการลดระดับความรุนแรงของความเสียหายต่อทรัพย์สินขององค์กรได้

นอกจากนี้ IDS ยังสามารถบันทึก log ของเหตุการณ์ผิดปกติได้อย่างครบถ้วน เพื่อใช้ในการนำมาวิเคราะห์พิสูจน์หาต้นเหตุ เลือกวิธีการจัดการกับเหตุการณ์ผิดปกตินั้น และเก็บเป็นหลักฐานสำคัญที่จะแสดงการบุกรุกได้

การตั้งค่าหรือกำหนด rule ของ IDS จำเป็นต้องทำให้สอดคล้องกับนโยบายความปลอดภัยขององค์กร เช่น ให้มีความสอดคล้องกับ rule ของ firewall เพื่อให้ IDS ตรวจจับสิ่งผิดปกติได้ตรงกับความต้องการ

ตัวอย่างของความสามารถของ IDS

- ตรวจจับการคัดลอกฐานข้อมูลขนาดใหญ่จากเซิร์ฟเวอร์ (server) ไปยังเครื่องลูกข่าย (Client) ของพนักงาน
- ตรวจจับการทำ port scan ทั้งที่ทำโดยผู้บุกรุก และจาก malware ต่างๆ เช่น worm
- ตรวจจับการทำโจมตีที่ช่องโหว่ของ NetBIOS ของระบบปฏิบัติการ Windows

นอกจากที่จะใช้ IDS ในการตรวจจับการบุกรุก และช่วยการจัดการกับเหตุการณ์ผิดปกติต่างๆแล้ว IDS ยังมีประโยชน์ในด้านอื่นๆอีกได้แก่

- **การตรวจสอบความถูกต้องของ** Security policy

เนื่องจาก IDS เป็นอุปกรณ์ด่านที่ 2 ต่อจาก firewall ที่สามารถตรวจจับการบุกรุกได้ ดังนั้นในบางครั้งข้อมูลจาก IDS สามารถบ่งบอกการตั้งค่ากฎในด้านความปลอดภัย (Rule) ของ ไฟลวอลล์ (Firewall) ที่ผิดพลาดได้ เช่น พบ traffic ที่ควรป้องกัน (Block) แต่ไม่ได้ตั้งค่า กฎในด้านความปลอดภัย (Rule) ที่ไฟลวอลล์ (Firewall) เพื่อให้ป้องกัน (Block)

- **บันทึกภัยคุกคามขององค์กร**

เนื่องจาก IDS จะบันทึกเหตุการณ์ผิดปกติ การโจมตี ของภัยคุกคาม (threat) ต่างๆที่ตรวจจับได้เอาไว้ด้วย ทำให้สามารถนำข้อมูลเหล่านี้ไปวิเคราะห์ ทำเป็นสถิติศึกษารูปแบบการโจมตี เพื่อที่จะนำมาใช้หายุทธวิธีในการป้องกัน และพัฒนาระบบรักษาความปลอดภัยสารสนเทศได้ต่อไป ข้อมูลเหล่านี้ยังทำให้ผู้บริหารได้เข้าใจถึงความเสี่ยงขององค์กรจากภัยคุกคามด้านคอมพิวเตอร์ด้วย

- **ลดการกระทำผิดต่อ** Securlty policy

หากมีการประกาศใช้งาน IDS ผู้ใช้งานระบบทั่วไปจะเกิดความระมัดระวังในการใช้งานระบบ หรือกลัวในการกระทำผิด เพราะการกระทำใดๆบนระบบจะถูกจับตามองโดย IDS ตลอดเวลา ทำให้การละเมิดต่อ security policy ลดน้อยลง

6.2.2 **รูปแบบการตรวจจับของ** IDS

กลไลในการตรวจจับสิ่งผิดปกติของ IDS แบ่งออกได้เป็น 3 รูปแบบ ได้แก่

- Signature-Based Detection

ใช้วิธีการเปรียบเทียบลักษณะของข้อมูลทุก packet ที่ผ่านเข้ามากับฐานข้อมูลของสิ่งผิดปกติ (Signature database) เพื่อตรวจหาการบุกรุก ลักษณะคล้ายกับโปรแกรม anti-virus คำว่า signature หมายถึงรูปแบบของภัยคุกคามที่เกิดขึ้นมาแล้ว เมื่อพบ packet ที่มีลักษณะตรงกับ signature IDS จะทำการบันทึกเหตุการณ์และแจ้งเตือนทันที ตัวอย่างของ signature ได้แก่

- การพยายาม telnet เข้ายังเครื่อง server ด้วย username เป็น root ซึ่งเป็นการละเมิดต่อ security policy
- Email ที่มี subject เป็น “Free pictures!” และมีไฟล์แนบเป็น “freepics.exe” ซึ่งเป็นลักษณะของ malware
- การพบ log ของ OS ที่ระบบบันทึกเข้ามาใหม่เป็น code หมายเลข 645 ซึ่งหมายถึง การ disable ระบบตรวจสอบของเครื่อง (auditing)

Signature-Based detection มีความสามารถในการตรวจจับการบุกรุกที่เคยเกิดขึ้นมาแล้วและมีข้อมูลในฐานข้อมูลได้ดีมาก แต่ไม่สามารถที่จะตรวจจับการบุกรุกที่พึ่งเกิดขึ้นและยังไม่ได้ผลิตเป็น signature นอกจากนี้การดัดแปลงรูปแบบการบุกรุกให้ต่างออกไปจากเดิมเพียงเล็กน้อยก็สามารถหลบหลีกการตรวจจับ IDS ประเภทนี้ได้ เช่น หากผู้บุกรุกใช้ malware ส่งมากับ email ตามตัวอย่างด้านบน แต่เปลี่ยนชื่อไฟล์แนบจากเดิมเป็น “freepics2.exe” ก็มีความเป็นไปได้สูงที่จะทำให้ IDS ตรวจจับไม่ได้

Signature-Based detection เป็นรูปแบบกลไลการตรวจจับที่ง่ายที่สุดเพราะใช้วิธีการเปรียบเทียบกับข้อมูล signature ในฐานข้อมูลเท่านั้น จึงไม่สามารถทำความเข้าใจลักษณะการรับส่งข้อมูลในระดับ network หรือ application protocol ได้ ไม่สามารถจดจำ state ของการรับส่งได้ ไม่สามารถจดจำการ request ข้อมูลก่อนหน้าขณะที่กำลังตรวจสอบ request ปัจจุบัน ทำให้ไม่สามารถตรวจจับการบุกรุกที่ซับซ้อนได้

- **Anomaly-Based Detection**

Anomaly-based detection ใช้วิธีการหาเหตุการณ์ที่เบี่ยงเบนไปจากเหตุการณ์ปกติ ในการตรวจจับ ซึ่งการทำงานเป็นการเปรียบเทียบเชิงสถิติ ดังนั้นการใช้งาน IDS ประเภทนี้จำเป็นต้องให้ IDS เรียนรู้ลักษณะ traffic ปกติก่อนในช่วงระยะเวลาหนึ่ง (training period) เพื่อใช้สร้างฐานข้อมูลที่เรียกว่า profile จากนั้นจึงจะเริ่มใช้งานได้ profile จะเก็บค่าเหตุการณ์ของระบบที่อยู่ในสภาวะปกติ เช่น user, host, bandwidth, การเชื่อมต่อ เป็นต้น ยกตัวอย่างเช่น profile ของเครือข่ายบอกว่าปกติแล้วมีการรับส่งข้อมูลประเภท web ที่ Internet gateway คิดเป็น 20% ของ bandwidth

ในช่วงเวลาทำงานปกติ ทันทีที่ IDS พบว่ามีการรับส่งข้อมูลประเภท web ที่ Internet gateway เกินค่า threshold ที่คาดไว้ จะมีการส่งแจ้งเตือนไปยังผู้ดูแลระบบทันที

นอกจากนี้ยังสามารถปรับเปลี่ยน profile ให้ตรวจจับตามที่ต้องการได้ เช่น กำหนดจำนวน email ที่รับส่งใน 1 วันต่อ 1 ผู้ใช้งาน หรือ จำนวนการ login เข้า server ทั้งที่สำเร็จและไม่สำเร็จต่อวัน หรือ ระดับการทำงานของ CPU ของเครื่อง server เป็นต้น และเนื่องจาก IDS ประเภทนี้ไม่จำเป็นต้องอัพเดท signature เหมือน signature-based IDS ทำให้สามารถตรวจจับการบุกรุกแบบ zero-day attack ได้ ยกตัวอย่าง เช่น มีการบุกรุกจาก malware ชนิดใหม่ ที่ทำให้เกิดการใช้งาน CPU อย่างมาก มีการส่ง email จำนวนมาก สร้าง network connection จำนวนมากในระยะเวลาอันสั้น ซึ่งทำให้เกิดเหตุการณ์ที่เบี่ยงเบนไปจากเหตุการณ์ปกติอย่างชัดเจน

ปัญหาของวิธีการตรวจจับวิธีนี้คือ ความถูกต้องของ profile เนื่องจากรูปแบบของการรับส่งข้อมูลมีความซับซ้อนมากขึ้นเรื่อยๆ ในบางองค์กรที่มีการใช้งานหลากหลาย application หลาย protocol ยิ่งทำให้ยากในการปรับจูน profile ทำให้เกิดปัญหาของการเกิด false positive จำนวนมาก ยกตัวอย่างเช่น ในการทำงานบำรุงรักษาระบบปกติจะมีการสำรองข้อมูล (backup) ซึ่งจะมีการส่งไฟล์ขนาดใหญ่ เดือนละ 1 ครั้ง ซึ่งเป็นไปได้ว่าขณะที่ IDS กำลังเรียนรู้พฤติกรรมปกติเพื่อทำ profile ไม่ได้เห็นเหตุการณ์นี้ ทำให้ IDS แจ้งเตือนการ backup ข้อมูลนี้ว่าเป็นเหตุการณ์ผิดปกติได้

- **Stateful Protocol Analysis**

การตรวจจับแบบ Stateful Protocol Analysis เป็นการตรวจจับหาสิ่งปกติ บน protocol เฉพาะนั้นๆ โดยการเปรียบเทียบกับ protocol profile ที่ถูกจัดทำไว้แล้ว Stateful Protocol Analysis ต่างจาก Anomaly-based detection ตรงที่ profile ถูกสร้างขึ้นไว้แล้วจาก vendor แต่ละรายที่ใช้ protocol นั้นๆ ในการรับส่งข้อมูล ไม่ได้เกิดจากการเรียนรู้ลักษณะพฤติกรรมปกติของเครือข่ายหรือเครื่องบนเครื่องข่าย

คำว่า stateful นั้นหมายความว่า IDS จะสามารถจดจำ request ก่อนหน้าของการรับส่งข้อมูลได้ ทำให้ IDS เข้าใจและติดตาม state ของ network, transport, และ

application protocol ได้ ยกตัวอย่างเช่น FTP stateful protocol-based profile จะสามารถตรวจจับสิ่งผิดปกติหรือการบุกรุกบนการรับส่งผ่าน FTP ได้โดยละเอียด สามารถตรวจจับการรับส่งข้อมูลโดยไม่ได้ผ่านการ authentication ได้ เนื่องจาก IDS จะสามารถจดจำ authentication state ของทุก session ไว้ได้ หรือสามารถตรวจจับการรับส่งข้อมูลไปยังเครื่องอื่นหลังจาก authentication สำเร็จจากเครื่องอีกเครื่องหนึ่งได้ (FTP bounce attack)

ความสามารถในการจดจำกระบวนการ authentication และการติดตาม session ของ authenticator ทำให้ข้อมูลจาก IDS ประเภทนี้ช่วยในการตรวจสอบ incident ได้อย่างมาก

ข้อจำกัดของการตรวจจับประเภทนี้คือ รายละเอียดหรือ specification ของ protocol ต่างๆมักไม่มีความสมบูรณ์ทำให้ไม่สามารถสร้าง profile ที่สมบูรณ์ได้ การตรวจจับจึงได้ผลที่ไม่ถูกต้อง และเมื่อมีการเปลี่ยนแปลงปรับปรุง protocol จำเป็นต้อง update profile ที่ IDS ด้วย นอกจากนี้ IDS ประเภทนี้จำเป็นต้องใช้ hardware ที่มี specification สูง เพราะต้องใช้ในการคำนวณที่ซับซ้อน ทำให้มีราคาที่แพง

6.3 **ช่องโหว่ของระบบคอมพิวเตอร์** (Computer Vulnerabilities)

ช่องโหว่ของระบบหรือโปรแกรม (Vulnerability) หมายถึงจุดอ่อนหรือช่องโหว่ในระบบ ช่องโหว่ของระบบอาจเกิดจากบั๊กหรือข้อบกพร่องจากการออกแบบระบบ ช่องโหว่ของระบบสามารถเกิดขึ้นได้จากการละเลยหรือความไม่ใส่ใจของผู้ออกแบบโปรแกรม รวมถึงสาเหตุอื่นๆ ซึ่งทำให้ระบบอนุญาตให้ผู้เข้ามาทำลายระบบ (รวมถึงแคร็กเกอร์, แฮ็คเกอร์และนูคเกอร์) หลอกแอปพลิเคชัน (application) ให้ผู้ทำลายนำข้อมูลของตัวเองมาใส่และซ่อนข้อมูลดังกล่าว, สั่งการระบบที่ควบคุมแอปพลิเคชันนั้นๆ หรืออาศัยข้อบกพร่องของระบบเพื่อเข้าถึงข้อมูลและความจำของระบบโดยไม่ได้รับอนุญาตเพื่อสั่งใช้โค้ดต่างๆ

การแก้ปัญหาช่องโหว่ของระบบส่วนใหญ่มักทำได้โดยการติดตั้งโปรแกรมต่อต้านไวรัสคอมพิวเตอร์, ไฟล์วอลล์และ IDS หรือการติดตั้งแพทช์ของผู้ผลิตโปรแกรม

บทที่ 7
การป้องกันไวรัส

ไวรัส (Virus) หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยจะแพร่กระจายไปยังไฟล์อื่นๆที่อยู่ในเครื่องเดียวกัน ไวรัสสามารถทำลายเครื่องได้ตั้งแต่ลบไฟล์ทั้งหมดที่อยู่ในฮาร์ดดิสก์ไปจนถึงเป็นแค่โปรแกรมที่สร้างความรำคาญให้กับผู้ใช้เครือข่าย เช่น แค่เปิดวินโดวส์แล้วเปิดป๊อปอัพเพื่อแสดงข้อความบางอย่าง โดยธรรมชาติแล้วไวรัสไม่สามารถที่จะแพร่กระจายไปยังเครื่องอื่นๆ ได้ตัวตัวเอง แต่การแพร่กระจายไปยังเครื่องอื่นต้องอาศัยโปรแกรมอื่นหรือมนุษย์ เช่น การแชร์ไฟล์โดยใช้ Flash Dive เป็นต้น และไวรัสนั้นไม่สามารถรันได้ด้วยตัวเอง ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัสนั้นจึงจะทำงานได้

7.1 วิวัฒนาการของไวรัสคอมพิวเตอร์

โปรแกรมที่สามารถสำเนาตัวเองได้เกิดขึ้นเป็นครั้งแรกในปี พ.ศ.2526 โดย ดร. เฟรดเดอริก โคเฮน นักวิจัยของมหาวิทยาลัยเพนซิลวาเนีย สหรัฐอเมริกา ได้ทำการศึกษาโปรแกรมลักษณะนี้และได้ตั้งชื่อว่า "ไวรัส" แต่ไวรัสที่แพร่ระบาดและสร้างความเสียหายให้กับเครื่องคอมพิวเตอร์ตามที่มี การบันทึกไว้ครั้งแรกเมื่อปี พ.ศ. 2529 ด้วยผลงานของไวรัสที่ชื่อ "เบรน (Brain)" ซึ่งเขียนขึ้นโดยโปรแกรมเมอร์สองพี่น้องชาวปากีสถาน ชื่อ อัมจาด (Amjad) และ เบซิท (Basit) เพื่อป้องกันการคัดลอกทำสำเนาโปรแกรมของพวกเขาโดยไม่จ่ายเงิน โดยทั้ง 2 คนนี้ยังได้เปิดร้านขายผลิตภัณฑ์คอมพิวเตอร์อยู่ที่เมือง Lahore ประเทศปากีสถาน สินค้าสวนใหญ่ที่สองพี่น้องนี้ขาย ก็คือ software (โปรแกรม) ต่างๆ ที่เขาทำการ copy ขาย ในราคาที่ถูกมากๆ พร้อมทั้งแอบปล่อยไวรัสเบรนไปกับแผนโปรแกรมเหล่านั้นด้วย และเนื่องจากการที่ประเทศปากีสถานไม่มีกฎหมายคุ้มครองลิขสิทธิ์ software จึงทำให้กิจการของสองพี่น้องทำ

ดำเนินไปได้อย่างดี โดยมีผู้นิยมซื้อโปรแกรมเหล่านี้ไปใช้จำนวนมาก ทั้งที่ชาวปากีสถานเองและชาวต่างประเทศที่เดินทางไปท่องเที่ยว ทำให้ไวรัสเบรนระบาดออกไปอย่างรวดเร็ว ทั่วโลก

ไวรัส คอมพิวเตอร์ในยุคแรกๆ จะระบาดโดยการสำเนาซอฟท์แวร์เถื่อนหรือซอฟท์แวร์ละเมิดลิขสิทธิ์ที่มี โปรแกรมไวรัสคอมพิวเตอร์ติดอยู่ ด้วยการใช้แผ่น FLOPPY DISK หรือซีดีรอม แต่ในปัจจุบันเนื่องจากการเติบโตของเครือข่ายคอมพิวเตอร์ทำให้ไวรัสยุคหลังๆ มีความสามารถในการทำสำเนาคัดลอกและแพร่กระจายตัวเองได้มากขึ้น รวมทั้งมีความรุนแรงมากกว่าเดิมในปัจจุบันนี้พบว่ามีมากกว่า 40,000 ชนิด และยังเกิดเพิ่มขึ้นอีกอยู่ทุกๆ วัน อย่างน้อยวันละ 4-6 ตัว

7.2 **มัลแวร์** (Malware)

"Malicious logic เป็นชุดของคำสั่งที่สร้างปัญหาในการละเมิดนโยบายด้านความปลอดภัยทางเทคโนโลยีสานสรเทศ" หรือส่วนใหญ่แล้วเรามักเรียกกันว่า "โปรแกรมประสงค์ร้าย (Malware: ***MAL****icious* soft**WARE**)" เนื่องจากที่พบเห็นจริงๆ มักอยู่ในรูปของโปรแกรม (Software) แล้ว ทั้งนี้ที่ผ่านมาภัยคุกคามของชุดคำสั่งประสงค์ร้ายนั้นดูจะเป็นสิ่งที่สร้างปัญหาและมีการกล่าวถึงมากที่สุดในบรรดารูปแบบของภัยคุกคามที่มีทั้งหมด

อย่างไรก็ตามนอกจากโปรแกรมประสงค์ร้ายที่เรารู้จักในปัจจุบันแล้ว กลุ่มนักวิชาการทางคอมพิวเตอร์หลายท่านคาดการณ์ว่า "ในปัจจุบันอาจมีชุดคำสั่งประสงค์ร้ายบางอย่างที่เราไม่รู้จักและไม่สามารถอธิบายได้ในปัจจุบัน ได้แฝงตัวอยู่ในระบบเครือข่ายที่พวกเรากำลังใช้งานอยู่ และรอเพียงเวลาที่มันจะทำงานอย่างเต็มรูปแบบโดยที่พวกเราไม่สามารถจะคาดเดาได้เลยว่าผลกระทบของมันจะออกมาเป็นอย่างไร"

7.3 **คุณสมบัติของมัลแวร์** (Malware)

โดยทั่วไปแล้วสามารถแบ่งชนิดของโปรแกรมประสงค์ร้ายได้โดยดูจากพฤติกรรม 3 ข้อดังนี้

- ชุดคำสั่ง (Code) นี้อยู่ได้อิสระหรือไม่ (Need host?)
- สามารถเดินทางได้ด้วยตัวเองหรือไม่ (Propagation?)
- สามารถสำเนาตัวเองได้หรือไม่ (Self-replicating?)

7.3.1 **ไวรัส** (Virus)

ไวรัส คือ โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง โดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือเจริญเติบโตเองได้ ขยายและแพร่กระจายตัวเองได้ สามารถอยู่รอดได้ด้วยการอำพรางตน เหมือนกับไวรัสที่เป็นเชื้อโรคร้ายทำลายสิ่งมีชีวิตทั้งหลายนั่นเอง

Need host – เป็นชุดคำสั่งที่จำเป็นต้องอยู่กับโปรแกรมอื่นหรือชุดคำสั่งอื่น

Not Propagation – เป็นชุดคำสั่งที่ต้องใช้ตัวกลางอื่นในการแพร่กระจาย

Self-replicating – เป็นชุดคำสั่งที่จะพยายามทำสำเนาตัวเองกระจายไปยังชุดคำสั่งอื่น

7.3.2 **หนอน** (Worm)

หนอน (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆที่อยู่ในเครือข่าย หนอนจะใช้ประโยชน์จากแอพพลิเคชั่นที่รับส่งไฟล์โดยอัตโนมัติ และไม่ต้องอาศัยคนเพื่อเปิดไฟล์ใดๆ เพราะหนอนมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ เวิร์มนั้นบางที่อาจอาศัยอีเมล์ในการแพร่กระจายตัวเองเหมือนไวรัส โดยแนบไฟล์ไปกับอีเมล์ เมื่อผู้รับเปิดจดหมายอ่านหนอนก็จะเริ่มทำงานทันที อย่างไรก็ตามในครั้งแรกที่เกิดหนอนขึ้นในวงการคอมพิวเตอร์นั้นเพื่อใช้ช่วยเพิ่มความสะดวกในการลงโปรแกรมให้กับเครื่องคอมพิวเตอร์ที่มีอยู่ในระบบของตนเอง ซึ่งในบางครั้งอาจมีกว่าร้อยเครื่อง โดยหนอนจะทำการส่งตัวเองไปพร้อมกับโปรแกรมที่จะทำการลงไปยังทุกๆเครื่องในระบบแล้วทำการลงโปรแกรมนั้นๆให้เองโดยอัตโนมัติไปเรื่อยๆจนครบทุกเครื่อง

Self-sub physical – เป็นชุดคำสั่งที่สามารถอยู่เป็นโปรแกรมเดียวๆเองได้

Propagation – เป็นชุดคำสั่งที่พยายามเคลื่อนที่ไปติดเครื่องอื่น ทั้งไปเองหรือสำเนาตัวเองไป

Not replicating – เป็นชุดคำสั่งที่จะไม่ทำสำเนาตัวเองภายในเครื่องเดิม

7.3.3 **ม้าโทรจัน** (Trojan Horse)

ม้าโทรจัน (Trojan horse) นี้เป็นคำที่มาจากสงครามโทรจันระหว่างทรอย (Troy) และกรีซ (Greek) ซึ่งเปรียบถึงม้าโครงไม้ขนาดใหญ่ที่ชาวกรีซสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างใน จากนั้นทำทีเป็นว่าถอนทัพกลับ เมื่อชาวทรอยออกมาดูเห็นม้าโครงไม้ทิ้งไว้และคิดว่าเป็นบรรณาการที่ทหารกรีซทิ้งไว้ให้เพื่อไม่ให้ตามไปโจมตีคืน จึงนำกลับเข้าเมืองไปด้วย แต่พอตกดึกทหารกรีซที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีซเข้าไปทำลายเมืองทรอยได้ในที่สุด สำหรับในความหมายทางคอมพิวเตอร์แล้ว ม้าโทรจัน หมายถึง โปรแกรมที่ทำลายระบบความปลอดภัยของคอมพิวเตอร์ไม่ทางใดก็ทางหนึ่ง โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม, สกรีนเซิร์ฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่างๆเหล่านี้มา และเมื่อติดตั้งแล้วรันโปรแกรม ม้าโทรจันที่แฝงมาด้วยก็จะทำลายระบบความปลอดภัยของคอมพิวเตอร์ เช่น เปิดช่องทางการสื่อสาร (Port) ที่ไม่ได้ใช้เอง เพื่อเป็นการสร้างประตูหลังให้กับโปรแกรมอื่นเข้ามาทำลายระบบได้ หรืออาจทำการบันทึกการใช้งานต่างๆของผู้ใช้งาน (Logs) เพื่อให้เจ้าของม้าโทรจันนั้นสามารถเข้ามาดูข้อมูลที่บันทึกไว้ได้ เป็นต้น

Self-sub physical – เป็นชุดคำสั่งที่สามารถอยู่เป็นโปรแกรมเดียวๆเองได้

Not Propagation – เป็นชุดคำสั่งที่ต้องถูกชักนำเข้ามาจากผู้ถูกโจมตีเอง ไม่สามารถเคลื่อนที่เองได้

Not replicating – เป็นชุดคำสั่งที่จะไม่ทำสำเนาตัวเอง

ทั้งนี้ม้าโทรจันอาจมีชื่อเรียกอื่นซึ่งอธิบายถึงลักษณะการทำงานของมัน เช่น

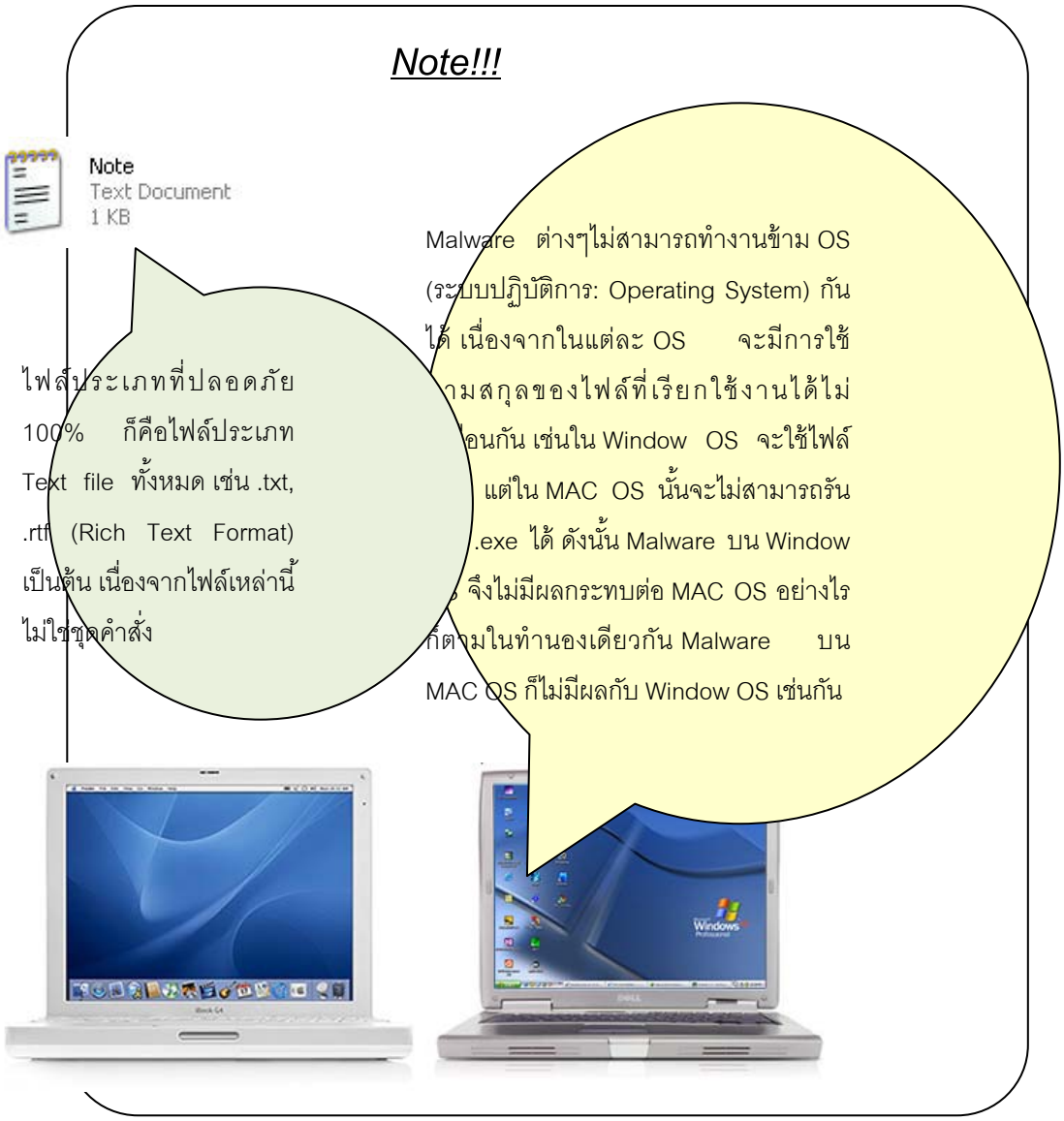
รูทคิท (Rootkits) เป็นชุดโปรแกรมขนาดเล็กที่หลอกให้ผู้ใช้เชื่อว่าจำเป็นต่อการทำงานของระบบคอมพิวเตอร์ โดยพวกผู้โจมตีนิยมใช้สำหรับเจาะเข้าระบบเพื่อควบคุมระบบหรือขโมยข้อมูล โปรแกรมประเภทนี้อาจใช้เทคนิคต่างๆ เช่น การเฝ้าดูสิ่งที่

ผู้ใช้พิมพ์บนคีย์บอร์ด (Key Stroke), แก้ไขไฟล์บันทึก (Log file) ของระบบ, สร้างประตูหลัง (Back door) เพื่อสำหรับการเจาะเข้าระบบในภายหลัง หรืออาจใช้ระบบนี้เพื่อเป็นฐานในการโจมตีระบบอื่นๆผ่านทางเครือข่าย โดยทั่วไปรูทคิทจะถูกจัดไว้เป็นชุดเพื่อใช้สำหรับโจมตีระบบปฏิบัติการประเภทใดประเภทหนึ่งโดยเฉพาะ รูทคิทเกิดขึ้นครั้งแรกในปี 1990 โดยในช่วงนั้นระบบปฏิบัติการซันยูนิกซ์ (SUN Unix) และลีนุกซ์ (Linux) เป็นเป้าหมายของการโจมตี แต่ในปัจจุบันมีรูทคิทหลายประเภทเพื่อใช้กับระบบปฏิบัติการต่างๆ ซึ่งรวมถึงไมโครซอฟท์วินโดวส์ (Microsoft Window) และแม็คอินทอช (Mac OS) ด้วย

Remote Access Trojan (RAT) เป็นม้าโทรจันที่จะสร้างประตูหลัง (Back door) ให้ผู้โจมตีสามารถเข้ามาในระบบเพื่อขโมยข้อมูลหรือควบคุมระบบจากระยะไกล ตัวอย่างเช่น แบ็คออริไฟซี (Back Orifice), คาฟีน (Cafeene) และซับเซเว่น (SubSeven) เป็นต้น

ข้อสังเกตอย่างหนึ่งคือ ถึงแม้ว่าชุดโปรแกรม RAT หรือรูทคิดบางโปรแกรมเป็นเครื่องมือที่สามารถใช้งานอย่างถูกต้องตามกฎหมายเพื่อจุดประสงค์สำหรับการดูแลระบบ (Monitoring System) อย่างไรก็ตามเครื่องมือเหล่านี้อาจเป็นอันตรายต่อระบบหรือองค์กรได้ถ้ามีการใช้งานในทางที่ผิด

รูปที่ 7.1 แสดงภาพม้าโทรจันที่มีการซ่อนคนไว้ภายใน



6.3 เทคนิคการตรวจจับไวรัส

ซอฟต์แวร์ป้องกันไวรัสเป็นสิ่งที่จำเป็นสำหรับการป้องกัน และรักษาความปลอดภัยให้กับคอมพิวเตอร์ ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง มันสามารถที่จะลดความเสี่ยงต่อโปรแกรมประสงค์ร้ายต่างๆได้ อย่างไรก็ตามมันไม่สามารถที่จะป้องกัน

ไวรัสได้ทุกชนิด เนื่องจากปัจจุบันจะมีไวรัสใหม่ๆออกมาอยู่เรื่อยๆ การใช้งานซอฟต์แวร์ป้องกันไวรัสนั้นจำเป็นที่ต้องอัพเดตฐานข้อมูลไวรัส (Virus Signature) เป็นประจำพร้อมทั้งสแกนระบบเป็นประจำเช่นกัน แต่ทั้งนี้โปรแกรมป้องกันไวรัสก็ไม่สามารถที่จะป้องกันผู้บุกรุกจากที่อื่นที่เจาะระบบเข้ามาแล้วรับโปรแกรมประสงค์ร้ายได้ นอกจากนี้โปรแกรมป้องกันไวรัสยังไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาตแต่พยายามที่จะเข้าถึงไฟล์หรือโปรแกรมที่ไม่ได้รับอนุญาตได้

ทั้งนี้ท่านทราบหรือไม่ว่าเราสามารถลงโปรแกรมป้องกันไวรัสได้มากกว่า 1 โปรแกรมใน 1 เครื่อง แต่ทั้งนี้จะสามารถทำได้กับโปรแกรมป้องกันไวรัสบางตัวเท่านั้น เช่น คุณสามารถลงAntiVir ร่วมกับ NOD32 และ bitdefend เนื่องจากโปรแกรมเหล่านี้จะไม่ทำการเข้าไปยุ่งกับการทำงานของระบบในจุดที่มีผลกระทบซึ่งกันและกัน แต่สำหรับ Norton Antivirus แล้วจะไม่สามารถลงร่วมกับโปรแกรมป้องกันไวรัสตัวอื่นได้เลยเพราะมันจะมองว่าโปรแกรมป้องกันไวรัสตัวอื่นๆเป็นโปรแกรมประสงค์ร้ายด้วย เป็นต้น แต่ถึงกระนั้นก็ไม่ได้หมายความว่าโปรแกรมป้องกันไวรัสที่ไม่สามารถลงร่วมกับโปรแกรมไวรัสตัวอื่นไม่ได้นั้นไม่ดีเสมอไป ทั้งนี้อาจเป็นเพราะโปรแกรมป้องกันไวรัสเหล่านั้นอาจมีการป้องกันที่ครอบคลุมการทำงานของระบบในแทบจะทุกส่วน หรือมีความอ่อนไหวและทำการป้องกันต่อการโจมตีแม้เพียงเล็กน้อย ซึ่งสิ่งเหล่านี้ก็จะทำให้โปรแกรมป้องกันไวรัสเหล่านั้นยิ่งมีประสิทธิภาพมากยิ่งขึ้น (แต่การอ่อนไหวมากก็อาจสร้างความรำคาญให้แก่ผู้ใช้ได้พอสมควรเช่นกัน!)

อย่างไรก็ตามผู้เชี่ยวชาญส่วนใหญ่ไม่แนะนำให้ทำการลงโปรแกรมป้องกันไวรัสมากกว่า 1 โปรแกรมต่อเครื่อง เพราะถึงแม้ว่าจะช่วยให้การป้องกันดีขึ้น แต่ก็ไม่ทำให้สามารถป้องกันได้ 100% อยู่ดี อีกทั้งยังทำให้ระบบการทำงานของคอมพิวเตอร์ช้าลงเป็นอย่างมากหรืออาจมีปัญหาการทำงานในบางส่วนได้อีกด้วย

และหากเราต้องการทดสอบว่าโปรแกรมป้องกันไวรัสที่เราใช้อยู่นั้น ตอบสนองกับพวก Script หรือมัลแวร์ได้ดีแค่ไหน เราสามารถทดสอบด้วยการนำ Script ต่อไปนี้สร้างไว้เป็น Text file ธรรมดา โดยอาจเปิด NotePad ขึ้นมาจากนั้นให้ก็อปปี้ Script นี้ลงไป

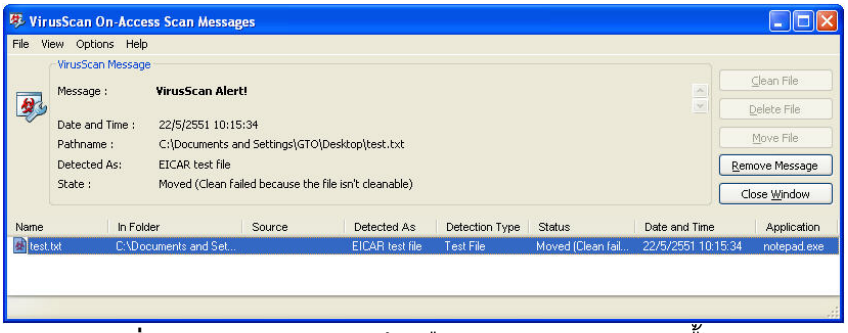
```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

จากนั้นให้ตั้งชื่อไฟล์และบันทึกลงในเครื่อง ในจังหวะนี้เองให้ดูว่า เครื่องเรามีการตอบสนองอย่างไรบ้าง เช่น

1. แจ้งเตือน (Alert!) ขึ้นมาทันที และไม่ยอมให้บันทึกไฟล์นั้น
2. ยอมให้บันทึกไฟล์นั้นลงไป แต่เมื่อพยายามเปิดไฟล์นั้นขึ้นมา ถึงจะมีการแจ้งเตือน พร้อมทั้งลบไฟล์นั้นออกจากเครื่องของคุณทันที
3. ยอมให้บันทึกไฟล์นั้นลงไป แต่เมื่อพยายามเปิดไฟล์นั้นขึ้นมา ถึงจะมีการแจ้งเตือน
4. ยอมให้บันทึกไฟล์ และแม้ว่าจะเปิดไฟล์ขึ้นมาดูอีกครั้งก็ไม่มีการแจ้งเตือนใดๆทั้งสิ้น

หากเครื่องของใครเข้าข่ายการตอบสนองแบบที่ 4 ก็ให้คุณหาโปรแกรมแอนตี้ไวรัสตัวอื่นมาใช้แทน สำหรับเครื่องที่ตอบสนองตามแบบที่ 1 จะให้ผลลัพธ์ดีที่สุด ซึ่งตัวอย่างของโปรแกรมก็เช่น McAfee, NOD32, Kaspersky เป็นต้น ส่วนการตอบสนองในแบบที่ 2 หรือ 3 นั้นก็เป็นปกติทั่วไป โดยแบบที่ 2 จะดูดีกว่าแบบที่ 3

อนึ่ง Script ตัวนี้เป็นเพียง Script ที่เอาไว้สำหรับทดสอบ ซึ่งไม่มีผลกระทบที่ก่อให้เกิดอันตรายแก่ระบบแต่อย่างใด ดังนั้นจึงไม่ต้องกังวล โดยสามารถดาวน์โหลดได้ที่ http://www.eicar.org/anti_virus_test_file.html



รูปที่ 7.2 แสดงภาพการแจ้งเตือนจากโปรแกรมแอนตี้ไวรัส

บทที่ 8
การกู้คืนระบบ

การกู้คืนระบบ (System Restore) จะตรวจสอบการเปลี่ยนแปลงแฟ้มระบบ เพื่อว่าหากมีสิ่งใดผิดปกติ เราจะสามารถกู้ระบบให้กลับสู่สถานะเดิมโดยที่ข้อมูลไม่สูญหาย ปกติทั้ง Windows XP และ Windows ME จะมีเครื่องมือชื่อว่า System Restore ให้มาด้วย โดย มันทำหน้าที่เหมือนโกดังเก็บข้อมูลต่างๆ เกี่ยวกับการทำงานของ Windows และไฟล์แอพพลิเคชัน ต่างๆ ที่ติดตั้งในระบบ เมื่อต้องการเรียกคืนสถานภาพการทำงานในช่วงเวลาก่อนหน้านี้ให้กับระบบก็สามารถทำได้ด้วยการเลือกวันที่ต้องการย้อนกลับไป และหน้าที่ของ System Restore ของ Windows System Restore จะสามารถสร้างจุดในการเรียกคืนระบบ (restore point) ได้หลายวิธีด้วยกัน ซึ่งปกติจะมีการสร้างข้อมูลที่ใช้ในการเรียกคืนระบบทุกๆ 24 ชั่วโมง ในกรณีที่คอมพิวเตอร์เปิดทำงานตลอดเวลา แต่ถ้าเครื่องคอมพ์ปิดอยู่การทำ restore point จะถูกสร้างขึ้นเมื่อเราเปิดเครื่องขึ้นทำงาน

8.1 การวิเคราะห์การถูกโจมตี

วิเคราะห์การถูกโจมตีเป็นการวิเคราะห์ถึงปัญหาด้านการรักษาความปลอดภัยที่เกิดขึ้นว่าเกิดมาจากสาเหตุใด เช่น เกิดจากซอฟต์แวร์ไม่ทันสมัย เกิดจากการปฏิบัติไม่ถูกต้องของผู้ใช้คอมพิวเตอร์ เป็นต้น เพื่อได้ทราบแนวทางในการป้องกันและรักษาความปลอดภัยของการโจมตีในครั้งนี้และนำไปปรับปรุงระบบรักษาความปลอดภัยให้ดีขึ้น ซึ่งปัจจุบันมีเครื่องมือที่ช่วยให้เราวิเคราะห์ทำให้สามารถสามารถทำงานได้ง่ายขึ้น โดยเราสามารถวิเคราะห์การโจมตีได้จากสิ่งดังต่อไปนี้

1. ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) หรือซอฟต์แวร์ว่ามีเปลี่ยนแปลงหรือเพิ่มขึ้นหรือไม่

2. ตรวจสอบไฟล์ข้อมูลอื่นในระบบ นอกเหนือจากไฟล์ระบบปฏิบัติการ โดยเข้าไปตรวจสอบไฟล์ที่เก็บข้อมูลสำคัญๆ ของหน่วยงานด้วย

3. ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้ โดยในการบุกรุกเกือบทุกครั้งผู้บุกรุกจะติดตั้งโปรแกรมหรือ ข้อมูลที่ใช้ในการตรวจสอบ หรือควบคุมการเข้าใช้ระบบ โดยทั่วไปไฟล์ที่มีผู้บุกรุกทิ้งไว้หลักๆ เช่น Network Sniffers, Trojan Horse Programs, Backdoors เป็นต้น

4. ตรวจสอบจากไฟล์ที่ถูกสร้างขึ้นใหม่ อาจจะเป็นไฟล์ที่มีชื่อคุ้นคุยแต่อยู่ผิดที่

5. การวิเคราะห์ล๊อคไฟล์ (Log file)

6. ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

8.2 การควบคุมสถานการณ์

การควบคุมสถานการณ์เป็นขั้นตอนที่จะกระทำเมื่อเกิดเหตุการณ์ไม่ปกติขึ้นในระบบรักษาความปลอดภัย คือ เมื่อเกิดมีภัยคุกคามเกิดขึ้น เช่น ไวรัส หนอนคอมพิวเตอร์ แฮกเกอร์ เป็นต้น ส่งที่ต้องกระทำคือต้องปฏิบัติแผนปฏิบัติการในกรณีฉุกเฉินที่เตรียมไว้ และปฏิบัติดังต่อไปนี้

1. ตรวจสอบภัยคุกคามว่าสามารถแก้ไขได้หรือไม่ เป็นภัยคุกคามที่เกิดขึ้นใหม่หรือเคยเกิดขึ้นแล้ว โดยติดต่อผู้เชี่ยวชาญด้านการรักษาความปลอดภัย เพื่อแก้ไขปัญหา

2. ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่ายหรือระบบอินเทอร์เน็ต หากเป็นชนิดแบบมีสายให้ถอดสายแลนออก และหากเป็นระบบไร้สายให้ปิดการบริการสำหรับเครื่องดังกล่าวโดยทันที เพื่อเป็นระงับความรุนแรงหรือการแพร่กระจายความเสียหายที่จะเกิดขึ้นต่อคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ

3. เตรียมการสำหรับการกู้คืนระบบ โดยพิจารณาถึงการส่งผลกระทบต่อธุรกิจหรือองค์กรเป็นหลัก ต้องกระทำด้วยความรวดเร็ว ต้องไม่ทำลายหลักฐานต่างๆ ที่จะใช้

ในการสืบหาตัวผู้กระทำความผิดและสำเนาใช้ข้อมูลดังกล่าวในการศึกษาวิเคราะห์หาวิธีการหรือเทคนิคการป้องกันและรักษาความปลอดภัยเพิ่มเติม

8.3 ขั้นตอนการกู้คืนระบบ

เมื่อดำเนินการวิเคราะห์การโจมตี และเก็บหลักฐานต่างๆที่จะใช้ดำเนินการตามกฎหมายแล้วนั้น ขั้นต่อไปคือการพยายามทำให้ระบบคอมพิวเตอร์กับมาใช้งานได้เป็นปกติโดยเร็ว และข้อมูลหรือสารสนเทศเกิดความเสียหายน้อยที่สุด

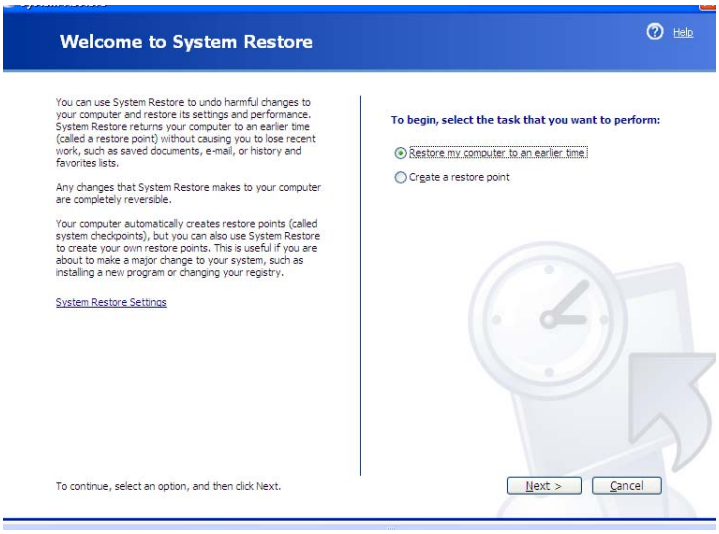
8.3.1 กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย

โดยหากข้อมูลในระบบยังพอสามารถกู้คืนได้ โดยใช้โปรแกรมคอมพิวเตอร์ต่างๆ ซึ่งต้องแน่ใจว่าข้อมูลที่กู้คืนกลับมาต้องมีความปลอดภัยร้อยเปอร์เซ็นต์ เช่น หากข้อมูลติดไวรัสต้องมั่นใจได้ว่าข้อมูลของเราต้องปราศจากไวรัสแล้วเท่านั้น แต่ถ้าหากไม่สามารถกู้คืนได้ ให้พิจารณานำไฟล์ข้อมูลที่สำรอง (BackUp) ที่จัดเก็บไว้มาใช้งานแทน

อนึ่งเรารู้หรือไม่ว่าระบบปฏิบัติการวินโดวส์ที่ใช้นั้น ก็มีเครื่องมือหรือโปรแกรมที่ช่วยให้เราสามารถสำรองข้อมูล (Backup) และเรียกข้อมูลกลับคืนให้เราใช้งานได้โดยไม่ต้องไม่หาโปรแกรมอื่นๆ เข้ามาช่วย โดยสรุปเครื่องมือที่ระบบปฏิบัติการวินโดว์เตรียมไว้ให้ได้ดังนี้

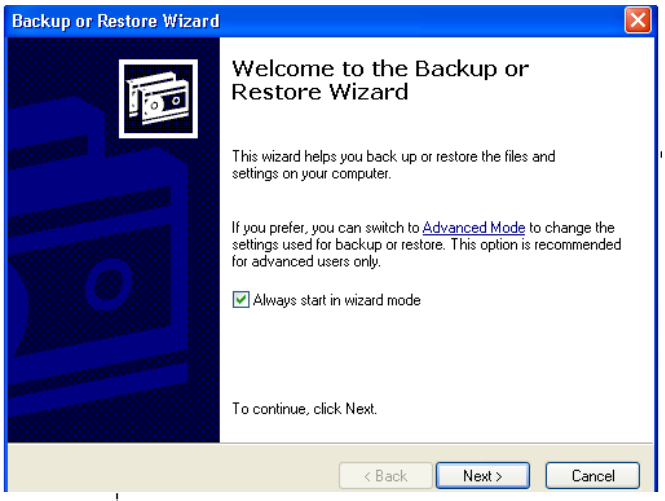
- **System Restore** เริ่มต้นจากคลิกปุ่ม Start เลือก All Programs หรือ Programs (ขึ้นกับระบบปฏิบัติการที่ใช้) เลือก Accessories ตามด้วย System Tools และ System Restore ตามลำดับ ไดอะล็อกบ๊อกซ์วิซาร์ดของการทำงานจะเปิดขึ้นมา ระบบจะให้เลือกว่า ต้องการที่จะสร้าง restore point (Create a restore point) หรือเลือกวันที่ก่อนหน้านี้ที่ต้องการให้ระบบย้อนคืนกลับไป (Restore my computer to an earlier time) เลือกออปชันที่ต้อง การแล้วคลิ้กปุ่ม Next กรณีที่เลือกรีสตอร์ หลังจากคลิกปุ่ม Next จะมีปฏิธินปรากฏขึ้นมา ตัวเลขวันที่ที่เป็นตัวหนา จะหมายถึงวันที่ มีการทำ restore point ถ้าพบว่า โปรแกรมที่ติดตั้งเข้าไปทำ

ให้ระบบมีปัญหา เลือกวันที่ติดตั้ง โปรแกรมดังกล่าว จะสังเกตเห็นรายชื่อโปรแกรมที่ติดตั้งปรากฏขึ้นมาในกล่องด้านขวา คลิกเลือก แล้วคลิก ปุ่ม Next ในหน้าต่างยืนยันให้คลิก Next ซึ่ง Windows จะเริ่มรีสตอร์ และบู๊ตเครื่องใหม่ หลังจากรัน System Restore ระบบจะมีการสร้าง restore point ไว้ด้วย



รูปที่ 8.1 โปรแกรม System Restore ใน Windows XP

- **Backup Utility** โปรแกรมตัวที่สองนี้ ค่อนข้างมีสมรรถนะการทำงานที่สูงพอตัว เพราะไมโครซอฟท์ได้เลือกใช้ซอฟต์แวร์ของ VERITAS ซึ่งเป็นบริษัทที่มีชื่อเสียงด้านซอฟต์แวร์โซลูชันและดาต้าเบส Backup Utility ช่วยให้ผู้ใช้ที่ต้องการแบ็กอัพข้อมูลและไฟล์ระบบสามารถทำได้ง่ายขึ้นเพราะมีโหมดการทำงานอย่าง Wizard ที่เพียงแคคลิ้กเมาส์ตามก็ได้เช่นกัน ซึ่งโปรแกรมก็ได้เตรียมเครื่องไม้เครื่องมือต่าง ๆ มาให้ คุณสามารถใช้โปรแกรม Backup Utility โดยไปที่ Start->All Programs -> Accessories -> System Tools ->Backup จะปรากฏดังรูปที่ 8.2



รูปที่ 8.2 โปรแกรม Backup ใน Windows XP

ทั้งนี้นอกจากการสำรองข้อมูลด้วยโปรแกรมแล้วเรายังสามารถแบ็กอัพข้อมูลด้วยอุปกรณ์ฮาร์แวร์ได้ด้วย การแบ็กอัพข้อมูลโดยใช้อุปกรณ์นั้น แน่นอนว่าย่อมลดความ เสี่ยงจากการที่ข้อมูลอาจสูญหายได้อีกขั้น นั่นก็เพราะคุณได้สำรองข้อมูลเอาไว้มากกว่าหนึ่งที่ ซึ่งอาจจะไม่ใช่ในฮาร์ดดิสก์เพียงอย่างเดียวอุปกรณ์ที่ใช้สำหรับแบ็กอัพข้อมูลในปัจจุบันก็ได้แก่ฮาร์ดดิสก์แบบติดตั้งภายนอกผ่านพอร์ต USB บันทึกเก็บไว้บนสื่อ DVD/CD นอกจากนั้นยังมีการใช้แฟลชเมโมรี่ความจุสูง รวมทั้งไมโครไดรฟ์ที่ใช้กับอุปกรณ์โมบายมาแบ็กอัพข้อมูลด้วยเช่นกันซึ่งทำให้ข้อมูลสำคัญๆ ของคุณยังคงถูกรักษาเอาไว้ แม้ฮาร์ดดิสก์หลักของระบบจะได้รับความเสียหายก็ตาม

8.3.2 ติดตั้งระบบปฏิบัติการทั้งหมดใหม่

ในกรณีที่คอมพิวเตอร์ถูกเจาะระบบ System ต่างๆ รวมทั้ง kernel ข้อมูล ไฟล์ต่างๆ โพรเซสและหน่วยความจำ อาจจะถูกแก้ไขโดยที่เราไม่รู้ วิธีเดียวที่ให้ความมั่นใจได้ว่าระบบมีความปลอดภัยอีกครั้ง โดยการติดตั้งระบบปฏิบัติการทั้งหมดใหม่จากตัวแทนจำหน่ายและติดตั้งข้อแก้ไข (Patch) ก่อนจะต่อเข้าระบบเครือข่ายอีกครั้ง

งดใช้เซอร์วิสที่ไม่จำเป็นปรับเปลี่ยนระบบเพื่อให้ใช้บริการเฉพาะเซอร์วิสที่ระบบนั้นตั้งใจจะให้บริการและไม่มีเซอร์วิสอย่างอื่น ตรวจสอบให้แน่ใจว่าไม่มีจุดอ่อนในคอน

ฟิกเกอร์ไฟล์ โดยทั่วไป วิธีที่ดีที่สุดคือขั้นแรกเริ่มจากการงดทุกๆ เซอร์วิส และต่อไปก็เปิดให้ใช้เฉพาะเซอร์วิสที่จำเป็นเท่านั้น

8.3.4 ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล

จากผู้แจกจ่ายระบบปฏิบัติการ แนะนำให้ตรวจสอบจากตัวแทนจำหน่ายว่าทุกๆ ข้อแก้ไข (Patch) ของระบบระบบปฏิบัติการที่ใช้อยู่ ได้ถูกใช้ปรับเข้ากับระบบแล้วเพื่อความปลอดภัย สิ่งนี้เป็นขั้นตอนที่สำคัญอย่างยิ่งในการป้องกันระบบจากการถูกทำลาย

8.3.5 เปลี่ยนแปลงพาสเวิร์ดใหม่

หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว แนะนำให้ทำการเปลี่ยนพาสเวิร์ดของผู้ใช้ทุกๆ คนบนระบบ ตรวจสอบให้แน่ใจว่าพาสเวิร์ดของแต่ละผู้ใช้นั้นยากที่จะคาดเดาได้ ซึ่งทาง AusCERT ได้บรรยายคุณลักษณะของพาสเวิร์ดที่ดีไว้ที่ http://www.auscert.org.au/Information/Auscert_info/Papers/good_password.html

8.3.6 ปรึกษากับศูนย์ประสานงาน CERT

หรือหน่วยงานที่เกี่ยวข้องในการรักษาความปลอดภัยสนับสนุนให้ศึกษาเอกสารของ CERT และหน่วยงานที่เกี่ยวข้อง และให้ปฏิบัติตามข้อปฏิบัติที่เกี่ยวกับการรักษาความปลอดภัย โดยหาข้อมูลจาก

- http://www.cert.org/advisories
- http://www.cert.org/summaries
- ftp://ftp.cert.org/pub/cert_bulletins
- http://thaicert.nectec.or.th

บทที่ 9
การทำความเข้าใจวิธีการเจาะระบบและการป้องกันระบบความปลอดภัยข้อมูลใน Unix/Linux, Windows Server, Webmail และ Website

9.1 Webmail

Mail Server คือคอมพิวเตอร์ที่ทำหน้าที่ให้บริการรับส่งอีเมลให้กับเครื่องคอมอื่นๆ ในเครือข่าย ทั้งจากในเครือข่ายเดียวกัน (LAN) หรือเครือข่ายอินเทอร์เน็ต เช่น อีเมลยอดฮิตอย่าง Hotmail หรือ Yahoo ก็ต้องมีเครื่อง Mail Server เพื่อให้บริการกับสมาชิกที่เข้ามาสมัครขอใช้อีเมล Web Mail คือโปรแกรมบริการรับ-ส่งเมล์ที่ติดตั้งอยู่บน Server โดยสามารถเรียกใช้งานเพื่อรับและส่งเมล์ผ่าน Web Browser ได้การติดตั้ง Webmail นี้คงเหมาะสำหรับ คนที่มี Server เป็นของตัวเอง และต้องการจัดทำ Webmail ให้กับหน่วยงานของตัวเอง แทนที่จะไปใช้ Webmail ที่อื่นๆ เช่น พวก Hotmail และ Yahoo Mail เป็นต้น ซึ่ง Webmail เหล่านี้ตั้งอยู่ต่างประเทศ การเรียกดูหรือส่ง Mail ในแต่ละครั้งจึงเป็นการติดต่อกับ Server ที่อยู่ต่างประเทศ ทำให้ปริมาณข้อมูลที่วิ่งออกไปต่างประเทศมีจำนวนมากเปลืองวงจรที่เช่าไปต่างประเทศ ดังนั้นถ้าหันมาใช้ Webmail ขององค์กรเองก็จะช่วยทำให้ลดปริมาณข้อมูลตรงนี้ลงได้ครับ การเรียกดูข้อมูลต่างๆ จากต่างประเทศก็จะเร็วขึ้น

ข้อควรระวังในการใช้งาน

1. ไม่ควรอนุญาตให้โปรแกรมคอมพิวเตอร์จัดเก็บ username & password ของเราไว้กับเครื่องโดยเด็ดขาด เพื่อป้องกันไม่ให้ผู้อื่นแอบมาใช้ email account ของเราโดยไม่ได้รับอนุญาต

2. ห้ามให้ username & password แก่ผู้อื่นโดยเด็ดขาด และกองเทคโนโลยีสารสนเทศไม่เคยมีนโยบายขอ user name & password จากผู้ใช้ในการบำรุงรักษาระบบอีเมล์แต่อย่างใด

3. ควรเปลี่ยน password เป็นประจำ อย่างน้อยทุก ๓ เดือน เพื่อทำให้ระบบ email account ของเรามีความปลอดภัยยิ่งขึ้น

9.2 Website

ทุกวันนี้ คงไม่มีบริษัทใดที่ไม่มี Website เป็นของตัวเอง บางบริษัทอาจจะเช่า Web Hosting อยู่ หรือ บางบริษัทอาจมี Web Site เป็นของตนเองอยู่ในระบบเครือข่ายของบริษัท โดยมีการต่อเชื่อมเครือข่ายของบริษัทด้วย Frame Relay, ADSL หรือ Leased Line เข้ากับระบบเครือข่ายของ ISP ซึ่งส่วนใหญ่ก็จะมีการจัดซื้อ Firewall มาใช้ป้องกันระบบเครือข่ายภายในของบริษัท กับ ระบบอินเทอร์เน็ตจาก ISP และ มีการเปิดให้คนภายนอกสามารถเข้ามาเยี่ยมชม Web Site ได้ โดยเปิด Port TCP 80 (http) และ Port TCP 443 (https) ในกรณีที่ใช้โปรโตคอล SSL ในการเข้ารหัสข้อมูลเพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น

ปัญหาก็คือ ในเมื่อทุกบริษัทต้องเปิดทางให้มีการเข้าชม Web Site ทั้งแบบ Plain text traffic (Port 80) และแบบ Encrypted text traffic (port 443) ทำให้แฮกเกอร์สามารถจู่โจม Web Site ของเราโดยไม่ต้องเจาะผ่าน Firewall เนื่องจากเป็น Port ที่ Firewall มีความจำเป็นต้องเปิดใช้อยู่แล้ว

ในโลกของ E-Commerce มีอัตราการใช้งาน Web Server ที่เพิ่มขึ้นทุกวัน (ดูข้อมูลจากwww.netcraft.com) และ จากข้อมูลของ UNCTAD (http://www.unctad.org) พบว่า Web Server ทั่วโลก มีทั้งแบบที่เข้ารหัสด้วย SSL แล้ว และ แบบไม่เข้ารหัสด้วย SSL ก็ยังคงมีใช้กันอยู่

ในเมื่อแฮกเกอร์มองเห็นช่องที่เรามีความจำเป็นต้องเปิดใช้งานผ่านทาง Web Server และ Web Application แฮกเกอร์ในปัจจุบันจึงใช้วิธีที่เรียกว่า “Web

Application Hacking" ในการเจาะเข้าสู่ระบบขององค์กรต่างๆ ทั่วโลก ขณะนี้มีการจู่โจมระบบโดยกลุ่มแฮกเกอร์ที่ต้องการทำสถิติ ในการเจาะ Web Site ดูรายละเอียดได้ที่ http://www.zone-h.org ดังนั้น ผู้ที่มี Web Site อยู่ และ โดยเฉพาะผู้ที่ต้องการหันมาทำธุรกิจในลักษณะของ E-commerce ซึ่งต้องมี Web Site ที่ใช้ Web server ที่เชื่อถือได้ และมีการเขียน Web application โดยคำนึงถึงเรื่อง ?Security? เป็นหลัก จึงมีความจำเป็นอย่างยิ่งที่ต้องเรียนรู้ช่องโหว่ (Vulnerability) ของ Web application ที่แฮกเกอร์ชอบใช้ในการเจาะระบบ Web application ของเราซึ่งรวบรวมได้ทั้งหมด 10 วิธีด้วยกัน (Top 10 Web Application Hacking)

ตลอดจนเรียนรู้วิธีการป้องกันที่ถูกต้อง เพื่อที่จะไม่ให้ตกเป็นเหยื่อของเหล่าแฮกเกอร์ที่จ้องคอยเจาะระบบเราอยู่ผ่านทาง Web Site ที่ยังไงเราก็ต้องเปิดให้เข้าถึง และยังมี Virus Worm ตัวใหม่ๆ ที่เขียนขึ้นเพื่อจู่โจม Port 80 (HTTP)และ Port 443 (SSL) โดยเฉพาะอีกด้วย รายละเอียดของ Top 10 Web Application Hacking มี 10 วิธี ดังนี้

1. Unvalidated Input

หมายถึง การที่ข้อมูลจากฝั่ง client ที่ส่วนใหญ่แล้ว จะมาจาก Internet Explorer (IE) Browser ไม่ได้รับการตรวจสอบก่อนถูกส่งมาประมวลผลโดย Web Application ที่ทำงานอยู่บน Web Server ทำให้แฮกเกอร์สามารถดักแก้ไขข้อมูลในฝั่ง client

ก่อนที่จะถูกส่งมายังฝั่ง server โดยใช้โปรแกรมที่สามารถดักข้อมูลได้ เช่น โปรแกรม Achilles เป็นต้น ดังนั้น ถ้าเรารับข้อมูลจากฝั่ง client โดยไม่ระมัดระวัง หรือคิดว่าเป็นข้อมูลที่เราเป็นคนกำหนดเอง เช่น เทคนิคการใช้ Hidden Field หรือ Form Field ตลอดจนใช้ข้อมูลจาก Cookies เราอาจจะโดนแฮกเกอร์แก้ไขข้อมูลฝั่ง client ด้วย โปรแกรมดังกล่าวแล้วส่งกลับมาฝั่ง server ในรูปแบบที่แฮกเกอร์ต้องการ และมีผลกระทบกับการทำงานของ Web Application ในฝั่ง web server

- วิธีการป้องกัน

เราควรจะตรวจสอบข้อมูลที่รับมาจากทั้ง 2 ฝั่ง คือ ข้อมูลที่รับมาจาก client ผ่านทาง Browser และข้อมูลที่รับมาประมวลผลที่ web server โดยตรวจสอบที่ web server อีกครั้งก่อนนำไปประมวลผลด้วย Web application เราควรมีการฝึกอบรม Web Programmer ของเราให้ระมัดระวังในการรับ input จากฝั่ง client ตลอดจนมีการ Review Source code ไม่ว่าจะเขียนด้วย ASP, PHP หรือ JSP Script ก่อนที่จะนำไปใช้งานในระบบจริง ถ้ามีงบประมาณด้านรักษาความปลอดภัย ก็แนะนำให้ใช้ application level firewall หรือ Host-Based IDS/IPS ที่สามารถมองเห็น Malicious content และป้องกันในระดับ application layer

2. Broken Access Control

หมายถึง มีการป้องกันระบบไม่ดีพอเกี่ยวกับการกำหนดสิทธิของผู้ใช้ (Permission) ที่สามารถจะ Log-in /Log-on เข้าระบบ Web application ได้ ซึ่งผลที่ตามมาก็คือ ผู้ที่ไม่มีสิทธิเข้าระบบ (Unauthorized User) สามารถเข้าถึงข้อมูลที่เราต้องการป้องกันไว้ไม่ให้ Unauthorized User เข้ามาดูได้ เช่น เข้ามาดูไฟล์ข้อมูลบัตรเครดิตลูกค้าที่เก็บอยู่ใน Web Server หรือ เข้าถึงไฟล์ข้อมูลในลักษณะ Directory Browsing โดยเห็นไฟล์ทั้งหมดที่อยู่ใน web Server ของเรา ปัญหานี้เกิดจากการกำหนด File Permission ไม่ดีพอ และ อาจเกิดจากปัญหาที่เรียกว่า Path Traversal หมายถึง แฮกเกอร์จะลองสุ่มพิมพ์ path หรือ sub directory ลงไปในช่อง URL เช่น http://www.abc.com/../../customer.mdb เป็นต้น นอกจากนี้อาจเกิดจากปัญหาการ cache ข้อมูลในฝั่ง client ทำให้ข้อมูลที่ค้างอยู่ cache ถูกแฮกเกอร์เรียกกลับมาดูใหม่ได้ โดยไม่ต้อง Log-in เข้าระบบก่อน

- วิธีการป้องกัน

พยายามอย่าใช้ User ID ที่ง่ายเกินไป และ Default User ID ที่ง่ายต่อการเดา โดยเฉพาะ User ID ที่เป็นค่า default ควรลบทิ้งให้หมด สำหรับปัญหา Directory Browsing หรือ Path Traversal นั้น ควรมีการ set file system permission ให้รัดกุม

เพื่อป้องกัน ช่องโหว่ที่อาจถูกโจมตี และ ปิด file permission ใน sub directory ต่างๆ ที่ไม่ได้ใช้ และ ไม่มีความจำเป็นต้องให้คนภายนอกเข้า เพื่อป้องกันแฮกเกอร์สุ่มพิมพ์ path เข้ามาดึงข้อมูลได้ และควรมีการตรวจสอบ Web Server log file และ IDS/IPS log file เป็นระยะๆ ว่ามี Intrusion หรือ Error แปลกๆ หรือไม่

3. Broken Authentication and Session Management

หมายถึง ระบบ Authentication ที่เราใช้อยู่ในการเข้าถึง Web Application ของเรานั้นไม่แข็งแกร่งเพียงพอ เช่น การตั้ง Password ง่ายเกินไป, มีการเก็บ Password ไว้ในฝั่ง Client โดยเก็บเป็นไฟล์ Cookie ที่เข้ารหัสแบบไม่ซับซ้อนทำให้แฮกเกอร์เดาได้ง่าย หรือใช้ชื่อ User ที่ง่ายเกินไป เช่น User Admin เป็นต้น บางทีก็ใช้ Path ที่ง่ายต่อการเดาได้ เช่น www.abc.com/admin หมายถึง การเข้าถึงหน้า admin ของระบบ แฮกเกอร์สามารถใช้โปรแกรมประเภท Dictionary Attack หรือ Brute Force Attack ในการลองเดาสุ่ม Password ของระบบ Web Application ของเรา ตลอดจนใช้โปรแกรมประเภท Password Sniffer ดักจับ Password ที่อยู่ในรูปแบบ Plain Text หรือ บางทีแฮกเกอร์ก็ใช้วิธีง่ายๆ ในการขโมย Password เรา โดยแกล้งปลอมตัวเป็นเรา แล้วแกล้งลืม Password (Forgot Password) ระบบก็จะถามคำถามกลับมา ซึ่งถ้าคำถามนั้นง่ายเกินไป แฮกเกอร์ก็จะเดาคำตอบได้ไม่ยากนัก ทำให้แฮกเกอร์ได้ Password เราไปในที่สุด

- วิธีการป้องกัน

ที่สำคัญที่สุด คือการตั้งชื่อ User Name และ Password ควรจะมีความซับซ้อน ไม่สามารถเดาได้ง่าย มีความยาวไม่ต่ำกว่า 8 ตัวอักษร และมีข้อกำหนดในการใช้ Password (Password Policy) ว่าควรมีการเปลี่ยน Password เป็นระยะๆ ตลอดจนให้มีการกำหนด Account Lockout เช่น ถ้า Logon ผิดเกิน 3 ครั้ง ก็ให้ Lock Account นั้นไปเลยเป็นต้น การเก็บ Password ไว้ในฝั่ง Client นั้น ค่อนข้างที่จะอันตราย ถ้ามีความจำเป็นต้องเก็บในฝั่ง Client จริงๆ ก็ควรมีการเข้ารหัสที่ซับซ้อน

(Hashed or Encrypted) ไม่สามารถถอดได้ง่ายๆ การ Login เข้าระบบควรผ่านทาง https protocol คือ มีการใช้ SSL เข้ามาร่วมด้วย เพื่อเข้ารหัส Username และ Password ให้ปลอดภัยจากพวกโปรแกรม Password Sniffing ถ้ามีงบประมาณควรใช้ Two-Factor Authentication เช่น ระบบ One Time Password ก็จะช่วยให้ปลอดภัยมากขึ้น การใช้ SSL ควรใช้ Digital Certificate ที่ได้รับการ Sign อย่างถูกต้องโดย CA (Certificate Authority) ถ้าเราใช้ CA แบบ Self Signed จะทำให้เกิดปัญหา Man in the Middle Attack (MIM) ทำให้แฮกเกอร์สามารถเจาะข้อมูลเราได้แม้ว่าเราจะใช้ SSL แล้วก็ตาม (ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับ SSL Hacking ดูที่ http://www.acisonline.net)

4. Cross Site Scripting (XSS) Flaws

หมายถึง แฮกเกอร์สามารถใช้ Web Application ของเรา เช่น ระบบ Web Board ในการฝัง Malicious Script แฝงไว้ใน Web Board แทนที่จะใส่ข้อมูลตามปกติ เมื่อมีคนเข้า Refresh หน้า Web Board ก็จะทำให้ Malicious Script ที่ฝังไว้นั้นทำงานโดยอัตโนมัติ ตามความต้องการของแฮกเกอร์ หรือ อีกวิธีหนึ่ง แฮกเกอร์จะส่ง e-mail ไปหลอกให้เป้าหมาย Click ไปที่ URL Link ที่แฮกเกอร์ได้เตรียมไว้ใน e-mail เมื่อเป้าหมาย Click ไปที่ Link นั้น ก็จะไปสั่ง Run Malicious Script ที่อยู่ในตำแหน่งที่แฮกเกอร์ทำดักรอไว้ วิธีการหลอกแบบนี้ในวงการเรียกว่า PHISHING ซึ่งโดนกันไปแล้วหลายองค์กร เช่น Citibank, eBay เป็นต้น (ข้อมูลเพิ่มเติมดูได้ที่ http://www.acisonline.net)

- วิธีการป้องกัน

อย่างแรกเลยต้องมีการให้ข้อมูลกับผู้ใช้คอมพิวเตอร์ทั่วไป ที่ใช้ e-mail และ web browser กันเป็นประจำให้ระมัดระวัง URL Link แปลกๆ หรือ e-mail แปลกๆ ที่เข้ามาในระบบก่อนจะ Click ควรจะดูให้รอบคอบก่อน เรียกว่า เป็นการทำ ?Security Awareness Training? ให้กับ User ซึ่งควรจะทำทุกปี ปีละ 2-3 ครั้ง เพื่อให้รู้ทันกลเม็ด

ของแฮกเกอร์ และไวรัสที่ชอบส่ง e-mail มาหลอกอยู่เป็นประจำ สำหรับในฝั่งของผู้ดูและระบบ เช่น Web Master ก็ควรจะแก้ไข source codeใน Web Board ของตนให้ฉลาดพอที่จะแยกแยะออกว่ากำลังรับข้อมูลปกติ หรือรับข้อมูลที่เป็น Malicious Script ซึ่งจะสังเกตได้ไม่ยาก เพราะ Script มักจะมีเครื่องหมาย < > ( ) # & ให้ Web Master ทำการกรองเครื่องหมายเหล่านี้ก่อนที่จะนำข้อมูลไปประมวลผลโดย Web application ต่อไป

5. Buffer Overflow

หมายถึง ในฝั่งของ Client และ Server ไม่ว่าจะเป็น IE Browser และ IIS Web Server หรือ Netscape Browser และ Apache Web Server ที่เราใช้กันอยู่เป็นประจำ ล้วนมีช่องโหว่ (Vulnerability) หรือ Bug ที่อยู่ในโปรแกรม เมื่อแฮกเกอร์สามารถค้นพบ Bug ดังกล่าว แฮกเกอร์ก็จะฉวยโอกาสเขียนโปรแกรมเจาะระบบที่เราเรียกว่า “Exploit” ในการเจาะผ่านช่องโหว่ที่ถูกค้นพบ ซึ่งช่วงหลังๆ แม้แต่ SSL Modules ทั้ง IIS และ Apache web server ก็ล้วนมีช่องโหว่ให้แฮกเกอร์เจาะผ่านทาง Buffer Overflow ทั้งสิ้น

- วิธีการป้องกัน

จะเห็นว่าปัญหานี้มาจากผู้ผลิตไม่ใช่ปัญหาการเขียนโปรแกรม Web application ดังนั้นเราต้องคอยหมั่นติดตามข่าวสาร New Vulnerability และ คอยลง Patch ให้กับระบบของเราอย่างสม่ำเสมอ และลง ให้ทันท่วงทีก่อนที่จะมี exploit ใหม่ๆ ออกมาให้แฮกเกอร์ใช้การเจาะระบบของเรา สำหรับ Top 10 Web Application Hacking อีก 5 ข้อ ที่เหลือผมขอกล่าวดังในฉบับต่อไปนะครับ

6. Injection Flaws

หมายถึง แฮกเกอร์สามารถที่จะแทรก Malicious Code หรือ คำสั่งที่แฮกเกอร์ใช้ในการเจาะระบบส่งผ่าน Web Application ไปยังระบบภายนอกที่เราเชื่อมต่ออยู่

เช่น ระบบฐานข้อมูล SQL โดยวิธี SQL Injection หรือ เรียก External Program ผ่าน shell command ของระบบปฏิบัติการ เป็นต้น

ส่วนใหญ่แล้วแฮกเกอร์จะใช้วิธีนี้ในช่วงการทำ Authentication หรือการ Login เข้าระบบผ่านทาง Web Application เช่น Web Site บางแห่งชอบใช้ /admin ในการเข้าสู่หน้า Admin ของ ระบบ ซึ่งเป็นช่องโหว่ให้แฮกเกอร์สามารถเดาได้เลยว่า เราใช้ http://www.mycompany.com/admin ในการเข้าไปจัดการบริหาร Web Site ดังนั้นเราจึงควรเปลี่ยนเป็นคำอื่นที่ไม่ใช่ /admin ก็จะช่วยได้มาก

วิธีการทำ SQL injection ก็คือ แฮกเกอร์จะใส่ชื่อ username อะไรก็ได้แต่ password สำหรับการทำ SQL injection จะใส่เป็น Logic Statement ยกตัวอย่างเช่น or 1′ = 1 หรือ or 1″= 1

ถ้า Web Application ของเราไม่มีการเขียน Input Validation ดัก password แปลกๆ แบบนี้ แฮกเกอร์ก็สามารถที่จะ bypass ระบบ Authentication ของเราและ Login เข้าสู่ระบบเราโดยไม่ต้องรู้ username และ password ของเรามาก่อนเลย

วิธีการเจาะระบบด้วย SQL injection ยังมีอีกหลายแบบจากที่ยกตัวอย่างมา ซึ่งแฮกเกอร์รุ่นใหม่สามารถเรียนรู้ได้ทางอินเทอร์เน็ตและวิธีการทำก็ไม่ยาก อย่างที่ยกตัวอย่างมาแล้ว

- วิธีการป้องกัน

นักพัฒนาระบบ (Web Application Developer) ควรจะระมัดระวัง input string ที่มาจากทางฝั่ง Client (Web Browser) และไม่ควรใช้วิธีติดต่อกับระบบภายนอกโดยไม่จำเป็น

ควรมีการกรองข้อมูลขาเข้าที่มาจาก Web Browser ผ่านมาทางผู้ใช้ Client อย่างละเอียด และ ทำการกรองข้อมูลที่มีลักษณะที่เป็น SQL injection statement ออกไปเสียก่อนที่จะส่งให้กับระบบฐานข้อมูล SQL ต่อไป

การใช้ Stored Procedure หรือ Trigger ก็เป็นทางออกหนึ่งในการเขียนโปรแกรมสั่งงานไปยังระบบฐานข้อมูล SQL ซึ่งมีความปลอดภัยมากกว่าการใช้ Dynamic SQL Statement กับฐานข้อมูล SQL ตรงๆ

7. Improper Error Handling

หมายถึง มีการจัดการกับ Error message ไม่ดีพอ เวลาที่มีผู้ใช้ Web Application หรืออาจจะเป็นแฮกเกอร์ลองพิมพ์ Bad HTTP Request เข้ามาแต่ Web Server หรือ Web Application ของเราไม่มีข้อมูล จึงแสดง Error message ออกมาทางหน้า Browser ซึ่งข้อมูลที่แสดงออกมาทำให้แฮกเกอร์สามารถใช้เป็นประโยชน์ ในการนำไปเดาเพื่อหาข้อมูลเพิ่มเติมจากระบบ Web Application ของเราได้ เนื่องจากเมื่อการทำงานของ Web application หลุดไปจากปกติ ระบบมักจะแสดงค่า Error Message ออกมาแสดงถึงชื่อ user ที่ใช้ในการเข้าถึงฐานข้อมูล, แสดง File System Path หรือ Sub Directory Name ที่ชี้ไปยังไฟล์ฐานข้อมูล ตลอดจนทำให้แฮกเกอร์รู้ว่าเราใช้ระบบอะไรเป็นฐานข้อมูลเช่น ใช้ MySQL เป็นต้น

- วิธีการแก้ปัญหา

ควรมีการกำหนดนโยบายการจัดการกับ Error message ให้กับระบบ โดยทำหน้า Error message ที่เตรียมไว้รับเวลามี Bad HTTP Request แปลกๆ เข้ามายัง Web Application ของเราโดยหน้า Error message ที่ดีไม่ควรจะบอกให้ผู้ใช้รู้ถึงข้อมูลระบบบางอย่างที่ผู้ใช้ทั่วไปไม่ควรรู้ และถ้าผู้ใช้คนนั้นเป็นแฮกเกอร์ซึ่งย่อมมีความรู้มากกว่าผู้ใช้ธรรมดา การเห็นข้อมูล Error message ก็อาจนำไปใช้เป็นประโยชน์สำหรับแฮกเกอร์ได้

8. Insecure Storage

หมายถึง การเก็บรหัสผ่าน (password), เบอร์บัตรเครดิตลูกค้า หรือ ข้อมูลลับของลูกค้า ไว้อย่างไม่มีความปลอดภัยเพียงพอ ส่วนใหญ่จะเก็บแบบมีการเข้ารหัส (Encryption) ไว้ในฐานข้อมูลหรือ เก็บลงในไฟล์ที่อยู่ใน Web server และคิดว่าเมื่อ

เข้ารหัสแล้วแฮกเกอร์คงไม่สามารถอ่านออก แต่ สิ่งที่เราคิดนับว่าเป็นการประเมินแฮกเกอร์ต่ำเกินไป เนื่องจากอาจเกิดข้อผิดพลาดในการเข้ารหัส เช่น การเข้ารหัสนั้นใช้ Algorithm ที่อ่อนเกินไป ทำให้แฮกเกอร์แกะได้ง่ายๆ หรือมีการเก็บกุญแจ (key) หรือ รหัสลับ (Secret password) ไว้เป็นไฟล์แบบง่ายๆ ที่แฮกเกอร์ สามารถเข้าถึงได้ หรือสามารถถอดรหัสได้โดยใช้เวลาไม่มากนัก

- วิธีการแก้ไข

ควรมีการเข้ารหัสไฟล์ โดยใช้ Encryption Algorithm ที่ค่อนข้างซับซ้อนพอสมควร หรือแทนที่จะเก็บรหัสผ่านที่เข้ารหัสไว้ ให้หันมาเก็บค่า Message Digest หรือ ค่า HASH ของรหัสผ่านทาง โดยใช้ Algorithm SHA-1 เป็นต้น

การเก็บกุญแจ (key), ใบรับรอง ดิจิตัล (Digital Certificate) หรือ ลายมือชื่อดิจิตัล (Digital Signature) ควรเก็บไว้อย่างปลอดภัย เช่น เก็บไว้ใน Token หรือ Smart Card ก็จะปลอดภัยกว่าการเก็บไว้เป็นไฟล์ในฮาร์ดดิสค์ เป็นต้น (ถ้าเก็บเป็นไฟล์ก็ควรทำการเข้ารหัสไว้ทุกครั้ง)

9. Denial of Service

หมายถึงระบบ Web Application หรือ Web Server ของเรา อาจหยุดทำงานได้เมื่อเจอกับ Bad HTTP Request แปลกๆ หรือ มีการเรียกเข้ามาอย่างต่อเนื่องจำนวนมาก ทำให้เกิดการจราจรหนาแน่นบน Web Server ของเรา โดยปกติ Web Server จะจัดการกับ Concurrent session ได้จำนวนหนึ่ง ถ้ามี HTTP Request เข้ามาเกินค่าที่ Web Server จะสามารถรับได้ ก็จะเกิด Error ขึ้น ทำให้ผู้ใช้ไม่สามารถเข้า Web Site เราได้ นอกจากนี้ อาจจะทำให้เครื่องเกิด CPU Overload หรือ Out of Memory ก็เป็นรูปแบบหนึ่งของ Denial of Service เช่นกัน กล่าวโดยรวมก็คือ ทำให้ระบบของเรามีปัญหาเรื่อง Availability

- วิธีการแก้ไข

การป้องกัน DoS หรือ DDoS Attack นั้นไม่ง่าย และ ส่วนใหญ่ ไม่สามารถป้องกันได้ 100% การติดตั้ง Hardware IPS (Intrusion Prevention System) เป็นอีกทางเลือกหนึ่ง แต่ก็มีค่าใช้จ่ายค่อนข้างสูง หากต้องการประหยัดงบประมาณก็ควรต้องทำการ Hardening ระบบให้เรียบร้อย เช่น Network OS ที่ใช้อยู่ก็ควรจะลง Patch อย่างสม่ำเสมอ, Web Server ก็เช่นเดียวกัน เพราะมีช่องโหว่ เกิดขึ้นเป็นประจำ ตลอดจนปรับแต่งค่า Parameter บางค่าของ Network OS เพื่อให้รองรับกับการโจมตีแบบ DoS /DDoS Attack

10. Insecure Configuration Management

หมายถึง เป็นปัญหาที่เกิดขึ้นจากผู้ดูแลระบบ หรือ ผู้ติดตั้ง Web Server มักจะติดตั้งในลักษณะ Default Configuration ซึ่งยังคงมีช่องโหว่มากมาย หรือบางครั้งก็ไม่ได้ทำการ Update Patch ระบบให้ครบถ้วนจนถึง Patch ล่าสุด

ปัญหาที่เจอบ่อยๆ ก็คือมีการกำหนดสิทธิในการเข้าถึงไฟล์ต่างๆ ใน Web Server ไม่ดีพอทำให้มีไฟล์หลุดออกมาให้ผู้ใช้เข้าถึงได้ เช่น แสดงออกมาในลักษณะ Directory Browsing ตลอดจนค่า default ต่างๆ ไม่ว่าจะเป็น Default Username และ Default Password ก็มักจะถูกทิ้งไว้โดยไม่ได้เปลี่ยนอยู่เป็นประจำ

- วิธีการแก้ปัญหา

ให้ทำการแก้ไขค่า Default ต่างๆ ทันทีที่ติดตั้งระบบเสร็จ และทำการ Patch ระบบให้จถึง Patch ล่าสุด และ ตาม Patch อย่างสม่ำเสมอ เรียกว่า ทำการ Hardening ระบบนั่นเอง Services ใดที่ไม่ได้ใช้ก็ไม่ต้องเปิดบริการ เราควรตรวจสอบสิทธิ File and Subdirectory Permission ในระบบว่าตั้งไว้ถูกต้อง และ ปลอดภัยหรือไม่ ตลอดจนเปิดระบบ Web Server log file เพื่อที่จะได้สามารถตรวจสอบ (Audit) HTTP Request ที่ส่งมายัง Web Server ได้ โดยดูจาก Web Server log file ที่เราได้เปิดไว้ และ เราควรหมั่นติดตามข่าวสารเรื่องช่องโหว่ (Vulnerability) ใหม่ๆ อย่างสม่ำเสมอ

และ มีการตรวจวิเคราะห์ Web Server log file, Network log file, Firewal log file และ IDS/IPS log file เป็นระยะๆ

“There’s no essential different between Computer Security Awareness and Life Security Awareness”

Pos Chandrasiri
Lecturer of Information Technology, Rangsit University

“ความตระหนักในความปลอดภัยทางคอมพิวเตอร์ก็ไม่ต่างอะไรกับความตระหนักในความปลอดภัยของชีวิตประจำวัน”

ภส จันทรศิริ
อาจารย์คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

บรรณานุกรม

[1] Matt Bishop. **Introduction to Computer Security.** U.S.: Addison-Wesley

[2] Ben Rothke. **Computer Security: 20 Things Every Employee Should Know.** U.S.: McGraw-Hill International Enterprises, Inc

[3] Cisco Networking Academy Program CCNA1 and CCNA2 Companion Guide, Revised Third Edition, 2005

[4] ธวัชชัย ชมศิริ ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ พิมครั้งที่ 1: มกราคม 2553 จัดพิมพ์โดย: บริษัท โปรวิชั่น จำกัด

[5] จตุชัย แพงจันทร์. **Master in Security.** นนทบุรี: ไอดีซีฯ, 2550

[6] อำนาจ มีมงคล, ปราการ ศิริมา, พณรังสี สู่ความดี. **ช่างเทคนิค COMPUTER & NETWORK Vol.2 Network Technician.** กรุงเทพฯ: สำนักพิมพ์ บาย เนเจอร์ พับลิชชิง

[7] ไฟล์วอลล์, จากวิกิพีเดีย สารานุกรมเสรี, หน้านี้แก้ไขล่าสุดเมื่อ ตุลาคม 2552 สืบค้นจาก http://th.wikipedia.org/wiki/ไฟล์วอลล์, เมื่อ ตุลาคม 2552

[8] ช่องโหว่ของระบบ, จากวิกิพีเดีย สารานุกรมเสรี, หน้านี้แก้ไขล่าสุดเมื่อ 15 พฤศจิกายน 2553 เวลา 11:11 น.
สืบค้นจาก http://th.wikipedia.org/wiki/, เมื่อ 20/01/54

[9] แหล่งข้อมูลข่าวสาร บทความ บทวิเคราะห์ เรื่องราวท่องเที่ยว ใน จังหวัดชลบุรี. (เว็บ) www.chonmeedee.com, 20/01/54

[10] แหล่งข้อมูลข่าวสาร บทความ ความเสี่ยง E - mail เทคโนโลยีการป้องกัน (เว็บ) http://www.softcov.com/web-client/e-mail-security-risk-prevention-technology.html, 20/01/54

[11] แหล่งข้อมูลข่าวสาร บทความเทคนิคการใช้เว็บเมล Mahidol University (PDF) http://muit.mahidol.ac.th/km_network/MUIT_073153.pdf, 20/01/54

[12] แหล่งข้อมูลข่าวสาร บทความ ความเสี่ยง E - mail เทคโนโลยีการป้องกัน (เว็บ) http://www.naitam.com/naitam-webdesign/view.php?id=22, 20/01/54

[13] http://guru.google.co.th/guru/thread

[14] http://www.atriumtech.com/cgi-bin/hilightcgi?Home=/home/InterWeb2000&File=/home2/searchdata/Forums2/http/www.pantip.com/tech/comsci/topic/CT2234479/CT2234479.html

[15] http://www.eicar.org/anti_virus_test_file.htm

[16] http://www.etcommission.go.th

[17] www.dusit.ac.th/~surasit_son/perfomance/paperIt-security/11it6-6.doc , 20/01/54