หนังสือคอมพิวเตอร์ที่มีผู้อ่านมากที่สุด

INFOPRESS GROUP

info PRESS NETWORK SERIES

ผลงานจากผู้แต่ง
เจาะระบบ Network 2nd Edition
หนังสือเครือข่ายที่
ขายดีที่สุด 5 ปีซ้อน

ผู้แต่ง จตุชัย แพงจันทร์
บรรณาธิการ อรรณพ ขันธิกุล
CCNP, CCDP, MCSE2003+Security

Master in SECURITY 2nd Edition

รวมศาสตร์ด้าน Security ไว้ครบทุกแขนง
เล่มเดียวที่ครบถ้วนสมบูรณ์ที่สุด

อยากเป็น Admin เก่งๆ และเงินเดือนแพงๆ
ไม่ควรพลาดเล่มนี้

- Information Security
- Network Security
- Hacking & Virus
- Endpoint Security
- Physical Security & Cyber Crime Laws

"ผู้เชี่ยวชาญ รู้ลึก รู้จริง ในสาขาความรู้ด้าน iT"

Firewall, Windows Security, Linux Security, Wireless LAN Security, INFOSEC, IPsec, ISO 17799, Cryptography, DES, 3DES, AES, Virus, Worm, Trojan Horse, Vulnerability, Risk Assessment, Anti Hacking, Outbreak Control and recovery

IDC PREMIER e-Book VERSION


Infopress Group
10th Anniversary
10th
ANNIVERSARY
BEST COMPUTER BOOK
Everything IT, Everything we're expert.

Master in Security 2nd Edition

Author จตุชัย แพงจันทร์ jatuchai@gitex.co.th

Editorial อรรณพ ขันธิกุล unnopk@infopress.co.th

Production

Graphic Designer อนัน วาโซะ

Page Layout วุฒิพันธ์ สมพระเมฆ
จตุรงค์ ศรีวิลาศ

Proofreaders สุนทรี บรรลือศักดิ์
มนฤดี ศรีอุทโยภาส

Publishing สุพัตรา อาจปรุ
ฉัตรชนก แก้วจันทร์

Create By **อินโฟเพรส (infopress)**

MASTER GUIDE

Published By

บริษัท ไอดีซี พรีเมียร์ จำกัด
200 หมู่ 4 ชั้น 19 ห้อง 1906
อาคารจัสมินอินเตอร์เนชั่นแนลทาวเวอร์
ถ.แจ้งวัฒนะ อ.ปากเกร็ด จ.นนทบุรี 11120
โทรศัพท์ 0-2962-1081 (อัตโนมัติ 10 คู่สาย)
โทรสาร 0-2962-1084

สำหรับลูกค้า
ลูกค้าสัมพันธ์
โทรศัพท์ 0-2962-1081 ต่อ 121
โทรสาร 0-2962-1084
สำหรับร้านค้าและตัวแทนจำหน่าย
โทรศัพท์ 0-2951-1300-2,
0-2591-9446
โทรสาร 0-2591-9447

ราคา 185 บาท

พิมพ์ครั้งที่ 1 ตุลาคม 2554

ข้อมูลทางบรรณานุกรม
จตุชัย แพงจันทร์
Master in Security 2 nd Edition
นนทบุรี : ไอดีซีฯ, 2554
624 หน้า
1. ความปลอดภัยของข้อมูล
I ชื่อเรื่อง
005.8
ISBN 978-616-200-177-2

บริษัท ไอดีซี พรีเมียร์ จำกัด จัดตั้งขึ้นเพื่อเผยแพร่ความรู้เทคโนโลยีสารสนเทศทั้งในระดับพื้นฐานและระดับสูง เรายินดีรับงานเขียนของนักวิชาการและนักเขียนทุกท่าน โดยเฉพาะงานที่เกี่ยวข้องกับสารสนเทศ ท่านผู้สนใจกรุณาติดต่อผ่านทางอีเมลที่ editor@infopress.co.th หรือโทรศัพท์หมายเลข 0-2962-1081 (อัตโนมัติ 10 คู่สาย) โทรสาร 0-2962-1084

EDITOR'S NOTE

วันหนึ่งใครจะคิดว่า การสื่อสารส่วนใหญ่นั้นจะต้องส่งผ่านระบบคอมพิวเตอร์ทั้งข้อมูล ภาพ เสียง และวิดีโอ ทั้งหมดนี้อาจจะเป็นข้อมูลสาธารณะ หรือข้อมูลลับ หากเป็นข้อมูลเชิงธุรกิจ ทางราชการ หรือความมั่นคงนั้น ส่วนใหญ่จะเป็นความลับ การปกป้องความลับและการรักษาความปลอดภัยข้อมูลนั้นถือเป็นศาสตร์ที่มีความยากและวุ่นวาย หากเป็นผู้ใช้ทั่วๆ ไปแล้วแทบไม่เข้าใจว่าระบบดังกล่าวทำงานอย่างไร แต่ในฐานะ Admin ผู้ดูแลระบบเครือข่าย ผู้บริหารระดับสูงก็ต้องมีความรู้ทางด้าน Security เพื่อให้สามารถดำเนินธุรกิจได้อย่างต่อเนื่องและไม่สะดุด การเรียนรู้ด้านนี้จำเป็นต้องมีความรู้พื้นฐานทางด้าน Network มาก่อน ซึ่งผู้อ่านสามารถศึกษาได้จากหนังสือเจาะระบบ Network หากไม่มีประสบการณ์ใดๆ แล้วมาเปิดอ่านอาจจะทำความเข้าใจได้ไม่เต็มร้อย ในการอ่านไม่ควรรีบเร่งเพราะเนื้อหามีความยากและมีจำนวนมาก เนื่องจากผู้แต่งคือ น.ต. จตุชัย แพงจันทร์ ได้พยายามรวบรวมเนื้อหาให้ครบทุกด้านทั้ง Information Security, Network Security, Hacking & Virus, Endpoint Security, Physical Security & Cyber Crime Law (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐)

หนังสือ Master in Security 2nd Edition นั้นถูกปรับให้มีเนื้อหาเพิ่มขึ้นจาก 12 บทในเล่มก่อนเป็น 15 บทในเวอร์ชันนี้ ถือว่าเป็นหนังสือด้าน Security ฉบับภาษาไทยที่มีความสมบูรณ์ที่สุด ถูกใช้ในการเรียนการสอนทั้งระดับปริญญาตรีและโท ถ่ายทอดความรู้และประสบการณ์จากผู้เชี่ยวชาญโดยตรง มุ่งเน้นให้ผู้อ่านมีความรู้ทางด้านทฤษฎี แม้ว่าจะค่อนข้างยากแต่ก็เป็นพื้นฐานที่ดีสำหรับการต่อยอดกับระบบรักษาความปลอดภัยได้ทุกรูปแบบ เพราะ Hacker ไม่มีวันหยุดงาน ถ้าคุณอยากเป็น Admin เก่งๆ เงินเดือนแพงๆ ก็อย่าหยุดอัพเดตความรู้ รอยรั่วเพียงเล็กน้อย (Security Breach) อาจจะส่งผลใหญ่หลวงกับธุรกิจ ชีวิตของใครบางคน ซึ่งการป้องกันอาจจะง่ายเพียงแค่แพตช์อัพเดตเท่านั้น หวังว่าหนังสือเล่มนี้จะเป็นประโยชน์กับผู้สนใจไม่มากก็น้อย

อรรณพ ขันธิกุล
บรรณาธิการ
CCNP,CCDP, MCSE2003+Security,
MCITP Enterprise Admin
ตุลาคม 2553

ป.ล. บางคนใช้ชีวิตบนโลกออนไลน์มากกว่าโลกแห่งความเป็นจริง แล้วปัญหา Security ล่ะ จะมองข้ามไปได้อย่างไร

PREFACE

การรักษาความปลอดภัยกลายเป็นเรื่องที่สำคัญอย่างยิ่ง และเป็นเรื่องที่มีการให้ความสนใจอย่างมากในปัจจุบัน เนื่องจากภัยคุกคามมีความรุนแรงเพิ่มขึ้น โดยเฉพาะความเสียหายด้านการเงินของบริษัทที่ทำธุรกิจบนอินเทอร์เน็ต ซึ่งมีสาเหตุมาจากเหล่าแฮคเกอร์ที่มีจำนวนเพิ่มมากขึ้นตามจำนวนผู้ใช้อินเทอร์เน็ต จนบางครั้งการแฮคระบบกลายเป็นงานอดิเรกของนักท่องอินเทอร์เน็ตบางคนไปแล้ว นอกจากนี้นักแฮคเกอร์ก็ได้พัฒนาฝีมือตัวเองเพิ่มขึ้นเรื่อยๆ การโจมตีของแฮคเกอร์ในสมัยก่อนนั้นจะเป็นแบบเพื่อความคึกคะนองหรือความสนุกสนาน โดยเมื่อแฮคระบบหรือเว็บไซต์ใดได้สำเร็จแล้วก็จะไปประกาศในเว็บบอร์ดเพื่อให้คนอื่นชื่นชมว่าตัวเองเก่ง ปัจจุบันนั้นแฮคเกอร์ประเภทนี้ก็ยังมีอยู่แต่ถือว่าไม่เป็นอันตรายมากนัก เนื่องจากไม่ได้มีเจตนาที่จะสร้างความเสียหายขั้นรุนแรง อย่างไรก็ตามปัจจุบันแรงจูงใจหลักของเหล่าแฮคเกอร์คือ เงิน และมีเป้าหมายที่จะโจมตีระบบหรือเว็บไซต์ที่มีความสำคัญ เช่น การเจาะระบบเพื่อเข้าไปขโมยข้อมูลบัตรเครดิตของลูกค้า การโจมตีเว็บไซต์อีคอมเมิร์ซของคู่แข่ง การโจมตีระบบของรัฐบาลโดยผู้ก่อการร้าย ซึ่งการที่จะทำอย่างนี้ได้ต้องอาศัยผู้ที่มีความรู้ความชำนาญอย่างมาก นอกจากความชำนาญของแฮคเกอร์แล้วรูปแบบการโจมตีและเครื่องมือของแฮคเกอร์นั้นก็มีการพัฒนาเพิ่มขึ้น เช่น SQL Injection, Cross site scripting และ Botnet เป็นต้น อย่างไรก็ตามรูปแบบการโจมตีแบบเก่าๆ ก็ยังใช้ได้ผล เช่น การโจมตีแบบ Phishing ซึ่งใช้เทคนิควิศวกรรมสังคม หรือการหลอกให้ผู้ใช้ทำอะไรบางอย่างแล้วผลจากการกระทำนั้นก็สร้างความเสียหายให้กับตัวเอง

นอกจากความน่ากลัวของนักแฮคเกอร์นานาชาติที่อยู่บนอินเทอร์เน็ตแล้ว ไวรัสหรือมัลแวร์ก็เป็นภัยคุกคามอันดับต้นๆ ที่สร้างปัญหาให้กับฝ่ายไอทีที่ต้องดูแลระบบให้สามารถใช้งานได้อย่างมีประสิทธิภาพ ไวรัสส่วนใหญ่จะเป็นสิ่งที่สร้างความรำคาญให้กับผู้ใช้งาน แต่ก็มีบางตัวที่สร้างความเสียหายให้กับระบบหรือข้อมูล การจัดการกับไวรัสนั้นเป็นเรื่องที่ยุ่งยากเนื่องจากจะเกี่ยวข้องกับผู้ใช้ด้วย ผู้ใช้เองจำเป็นต้องใส่ใจในการใช้งานคอมพิวเตอร์ เช่น ไม่เปิดเมลแปลกๆ โดยเฉพาะที่มีไฟล์แนบมาด้วย ไม่คลิกป๊อบอัพวินโดวส์เพื่อติดตั้งโปรแกรมหรือ add on ของเว็บบราวเซอร์เมื่อเข้าไปดูเว็บไซต์ที่ไม่น่าเชื่อถือ การแก้ปัญหาที่ดีที่สุดคือการให้การศึกษากับผู้ใช้ โดยแนะนำให้มีการสแกนไวรัสเป็นประจำ โดยเฉพาะสแกน USB drive ที่มาเสียบเพื่อแชร์ไฟล์ข้อมูลกัน ส่วนการป้องกันไวรัสภายในองค์กรอย่างได้ผลนั้นจำเป็นทั้งทางฝั่งไคลเอนท์และทางฝั่งเซิร์ฟเวอร์และในระดับเครือข่าย การป้องกันที่ดีที่สุดคือการติดตั้งแพตช์เพื่อปิดช่องโหว่ที่ไวรัสหรือมัลแวร์ใช้ประโยชน์เป็นประจำเป็นการป้องกันไวรัสได้เกือบ 100% แล้ว

จากภัยคุกคามต่างๆ ที่ได้กล่าวข้างต้น คำถามที่ทุกคนทราบคือ แล้วจะมีวิธีป้องกันอย่างไรถึงจะได้ผล คำตอบคือไม่มีเครื่องมือใดที่จะป้องกันได้อย่างสมบูรณ์ วิธีที่ดีที่สุดคือการลดโอกาสการถูกโจมตี การรักษาความปลอดภัยนั้นเป็นกระบวนการเชิงรุก โดยมีวัตถุประสงค์เพื่อบริหารความเสี่ยงอยู่ในระดับที่ยอมรับได้ ดังนั้น การรักษาความปลอดภัยควรเริ่มจากการประเมินความเสี่ยงแล้วกำหนดมาตรการเพื่อให้ความเสี่ยงนั้นลดลงหรือหายไป ซึ่งกระบวนการนี้ได้มีกำหนดไว้อย่างเป็นระบบในชุดมาตรฐาน ISO 27000 ซึ่งในมาตรฐานนี้จะนำเอาหลักการบริหารแบบ Plan-Do-Check-Act มาใช้เพื่อพัฒนากระบวนการรักษาความปลอดภัย นอกจากมาตรฐานนี้แล้วยังมีมาตรฐานอื่นที่บางองค์กรอาจนำมาใช้เพื่อเป็นพัฒนาการใช้งานระบบไอทีได้อย่างมีประสิทธิภาพ เช่น COBIT, ITIL เป็นต้น

SPECIAL'S THANK

แด่พระคุณพ่อพระคุณแม่
แด่ภรรยา (หมอตี๋) และลูกๆ (แอนดริว, คำแพง)

ในหนังสือเล่มนี้แน่นอนคงไม่ได้มีวัตถุประสงค์เพื่อที่จะสอนให้ท่านเป็นแฮคเกอร์ที่เก่งกาจเหมือนอย่างอาชญากรดังได้กล่าวข้างต้น แต่หนังสือเล่มนี้มีเนื้อหาเพื่อเป็นการปูพื้นฐานเพื่อที่จะเป็นผู้ชำนาญการด้านการรักษาความปลอดภัยที่รู้เท่าทัน หรือหาวิธีป้องกันแฮคเกอร์เหล่านี้ได้อย่างมีประสิทธิภาพ โดยผู้เขียนได้วางโครงสร้างของการนำเสนอเนื้อหาโดยแบ่งออกเป็น 5 ส่วน โดยมีเนื้อหาโดยสรุปดังนี้

Part I : Information Security

หลักการที่สำคัญในการรักษาความปลอดภัยข้อมูลคือการรักษาไว้ซึ่งความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) โดยเครื่องมือที่ใช้สำหรับการปกป้องคุณสมบัติเหล่านี้ ได้แก่ การเข้ารหัสข้อมูล (Cryptography), การพิสูจน์ทราบตัวตน (Authentication), การอนุญาตให้ใช้งาน (Authorization), การตรวจสอบได้ (Accountability) เป็นต้น

Part II : Network Security

โปรโตคอล TCP/IP นั้นโดยธรรมชาติจะไม่มีความปลอดภัยในตัว ข้อมูลที่รับ/ส่งโดยดีฟอลต์นั้นจะไม่มีการเข้ารหัสข้อมูลซึ่งสุ่มเสี่ยงต่อการถูกแอบดังอ่านข้อมูลได้ โปรโตคอลในทุกๆ เลเยอร์นั้นจะมีการเข้ารหัส เช่น HTTPS, S/MIME, PGP, IPSec, WPA เป็นต้น การป้องกันในระดับเน็ตเวิร์คจำเป็นต้องติดตั้งเครื่องมือ อย่างเช่น ไฟร์วอลล์, IDS/IPS, NAC เป็นต้น

Part III : Hacking and Virus

ภัยคุกคามหลักของระบบไอทีคือแฮคเกอร์และไวรัส การเข้าใจธรรมชาติของสิ่งเหล่านี้จะช่วยให้สามารถหามาตรการป้องกันที่เหมาะสมและได้ประสิทธิภาพได้ โดยวิธีที่ดีที่สุดคือการติดตั้ง Patch เพื่อปิดช่องโหว่ของระบบหรือแอพพลิเคชันที่ติดตั้งในระบบนั้นๆ

Part IV : Endpoint Security

นอกจากการป้องกันในระดับเน็ตเวิร์คแล้วการป้องกันที่ปราการด่านสุดท้ายก็สำคัญ ไม่ว่าจะเป็นไคลเอนท์หรือเซิร์ฟเวอร์ ซึ่งอาจจะเป็นทั้งระบบวินโดวส์และลีนุกซ์ การป้องกันคือการอัพเดตระบบและแอพพลิเคชัน ติดตั้งโปรแกรมป้องกันไวรัส และอัพเดตซิกเนเจอร์และสแกนไวรัสเป็นประจำ

Part V : Physical Security & Cyber Crime Law

การป้องกันทางด้านกายภาพ เช่น การป้องกันการขโมย การป้องกันอัคคีภัย ระบบไฟฟ้า ระบบ HVAC และ ระบบ Access Control เพื่อควบคุมการเข้าออกพื้นที่ที่เป็นหัวใจสำคัญของระบบไอที อย่างเช่น ดาต้าเซ็นเตอร์ ส่วนสุดท้ายคือการปฏิบัติตามกฎหมาย โดยเฉพาะปัจจุบันมี พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ซึ่งมีผลบังคับให้แต่ละองค์กรจะต้องเก็บล็อกเพื่อไว้สำหรับการตรวจพิสูจน์หลักฐาน

สุดท้ายต้องขอขอบคุณท่านผู้อ่านทุกท่านที่ให้การสนับสนุนเป็นอย่างมากในหนังสือฉบับแรก (Master in Security) ซึ่งนั่นก็เป็นแรงบันดาลใจให้ต้องเขียน 2nd Edition นี้ขึ้นมา หลังจากที่ได้ตีพิมพ์ฉบับแรกออกมาก็มีหลายๆ อย่างที่ได้เปลี่ยนแปลงไป หนังสือเล่มนี้ได้ปรับปรุงจากฉบับก่อนหน้าเพื่อให้เนื้อหาทันสมัย ทันต่อเทคโนโลยีใหม่ๆ รวมถึงภัยคุกคามใหม่ๆ และเทคนิคในการป้องกันภัยคุกคามเหล่านั้นด้วย โดยได้มีการจัดลำดับเนื้อหาในการนำเสนอใหม่ และเพิ่มบทใหม่คือ Access Control, Physical Control และกฎหมายที่เกี่ยวกับคอมพิวเตอร์ ผู้เขียนหวังว่าหนังสือเล่มนี้จะเป็นประโยชน์สำหรับท่านผู้อ่านที่ต้องการเปลี่ยนมาทำงานในฟิวด์ซิเคียวรีตี้ หรือแม้กระทั่งผู้บริหารองค์กรที่ต้องการมีความรู้ทางด้านนี้

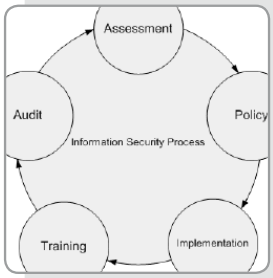
จตุชัย แพงจันทร์

CONTENTS

Part 1 Information Security

บทที่ 1 พื้นฐานการรักษาความปลอดภัย

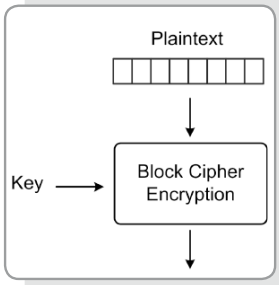
บทที่ 2 ระบบบริหารความปลอดภัยสารสนเทศ



CONTENTS

บทที่ 3 Authentication

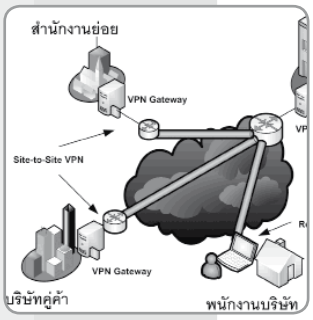
บทที่ 4 Cryptography



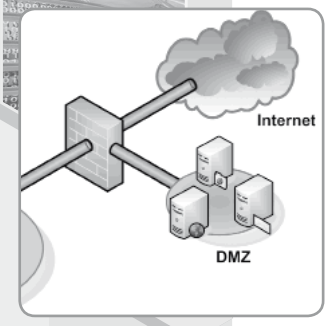
CONTENTS

Part 2 Network Security

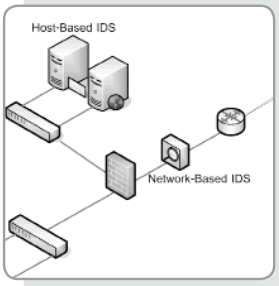
บทที่ 5 Network Security



บทที่ 6 Firewall

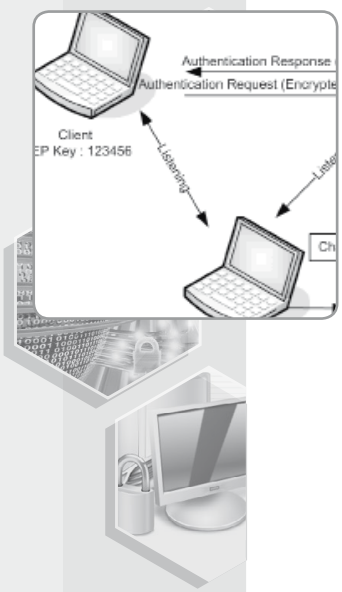


บทที่ 7 IDS/IPS และ NAC



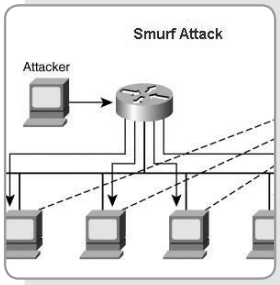
CONTENTS

บทที่ 8 Wireless LAN Security



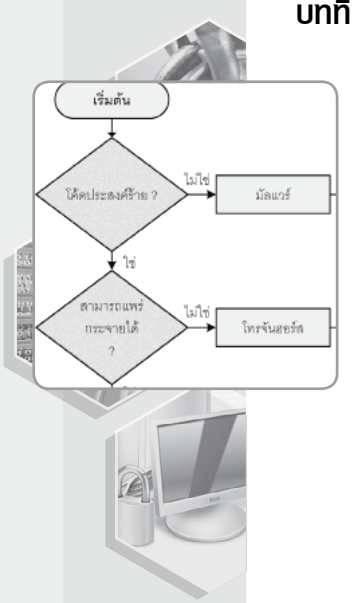
Part 3 Hacking & Virus

บทที่ 9 การเจาะระบบ



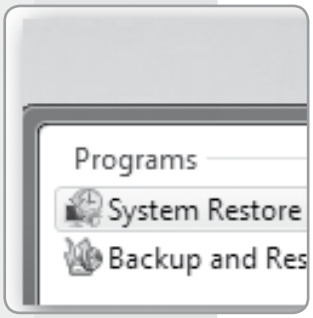
CONTENTS

บทที่ 10 การป้องกันไวรัส



CONTENTS

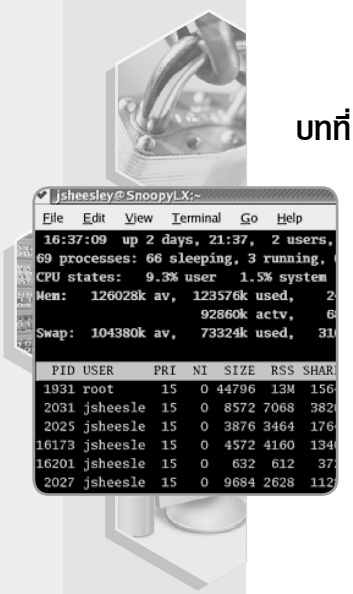
บทที่ 11 การกู้คืนระบบ



Part 4 Endpoint Security

บทที่ 12 Windows Security

CONTENTS

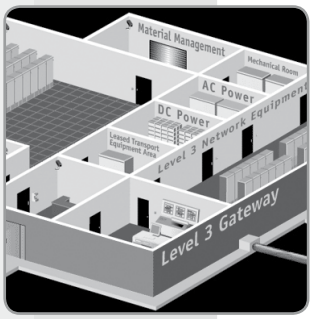


บทที่ 13 Linux Security

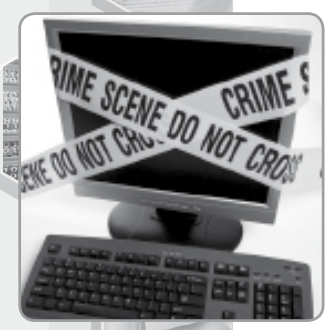
CONTENTS

Part 5 Physical Security & Cyber Crime Laws

บทที่ 14 Physical Security



บทที่ 15 กฎหมายอาชญากรรมคอมพิวเตอร์



MASTER IN SECURITY 2nd EDITION

PART 1

Information Security

หลักการในการรักษาความปลอดภัยนั้นคือการรักษาไว้ซึ่งคุณสมบัติทั้ง 3 มิติคือ ความลับ (Confidentiality), ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) การรักษาความปลอดภัยที่มีประสิทธิภาพนั้นประกอบด้วย 3 ส่วนคือ คน (People), กระบวนการ (Process) และ เทคโนโลยี (Technology) โดยมาตรฐานและเป็นที่ยอมรับได้แก่ ISO 27001, COBIT, ITIL เป็นต้น โดยกระบวนการนั้นจะเริ่มต้นด้วยการวิเคราะห์ความเสี่ยง แล้วกำหนดมาตรการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การที่ระบบใดระบบหนึ่งจะมีความปลอดภัยนั้นจำเป็นที่ต้องมีการควบคุมการเข้าถึง การปกปิดความลับของข้อมูลที่ดีที่สุดคือการเข้ารหัสข้อมูล (Encryption) ซึ่งเฉพาะผู้มีคีย์ (Key) เท่านั้นถึงจะเข้าถึงเนื้อหาของข้อมูลได้

CHAPTER 1

พื้นฐานการรักษาความปลอดภัย

วัตถุประสงค์

- รู้และเข้าใจความหมายของการรักษาความปลอดภัยข้อมูล
- รู้และเข้าใจประวัติของการรักษาความปลอดภัยข้อมูล
- รู้และเข้าใจองค์ประกอบและหลักการในการรักษาความปลอดภัยข้อมูล
- รู้และเข้าใจภัยคุกคามรูปแบบต่างๆ ในปัจจุบันและแนวโน้มในอนาคต
- รู้และเข้าใจเครื่องมือและมาตรการรักษาความปลอดภัยที่สำคัญ

ในยุคแห่งข้อมูลข่าวสาร สิ่งหนึ่งที่มีค่ามากที่สุดขององค์กรคือ ข้อมูล หรือสารสนเทศ ดังนั้น การปกป้องรักษาข้อมูลหรือสารสนเทศจึงเป็นสิ่งที่สำคัญและจำเป็น ซึ่งในยุคนี้ผู้ที่ครอบครองสารสนเทศมากกว่าย่อมเป็นผู้ได้เปรียบเสมอ ดังนั้น ถ้าสารสนเทศถูกจารกรรมหรือถูกทำให้เข้าถึงใช้งานไม่ได้ก็จะมีผลกระทบต่อเจ้าของแน่นอน ข้อมูลที่ถูกจัดเก็บไว้ในระบบสารสนเทศนั้นมีความเสี่ยงที่จะถูกโจมตีจากหลายแหล่ง เช่น ผู้ใช้งานที่รู้เท่าไม่ถึงการณ์ การโจมตีจากทั้งภายในและภายนอก การแพร่กระจายของไวรัส เวิร์ม โทรจันฮอร์ส ซึ่งอาจผ่านมาทางอีเมล เว็บ หรืออาจมีผู้ไม่หวังดีหรือ

แฮคเกอร์จากอินเทอร์เน็ตพยายามที่จะเจาะเข้าระบบเพื่อทำลายระบบ ลบ เปลี่ยนแปลง ขโมย หรือทำให้เข้าถึงข้อมูลไม่ได้ ดังนั้น ระบบสารสนเทศจึงจำเป็นที่ต้องมีระบบรักษาความปลอดภัยที่แข็งแกร่งพอที่จะรับมือกับภัยคุกคามต่างๆ ได้

ปัจจุบันเครือข่ายอินเทอร์เน็ตเติบโตอย่างรวดเร็ว เกือบจะทุกองค์กรจำเป็นต้องเชื่อมต่อเครือข่ายตนเองเข้ากับอินเทอร์เน็ตเพื่อใช้ประโยชน์จากแหล่งข้อมูลที่ใหญ่ที่สุดในโลกนี้ อินเทอร์เน็ตนั้นเปรียบเสมือนดาบสองคม ประโยชน์ที่ได้รับจากอินเทอร์เน็ตนั้นอาจมากเกินกว่าที่จะจินตนาการ แต่โทษนั้นก็มีมากมายเช่นกัน เหตุผลหนึ่งก็เนื่องจากข้อมูลและเครื่องมือที่ใช้สำหรับการเจาะระบบนั้น สามารถค้นหาและดาวน์โหลดจากอินเทอร์เน็ตได้อย่างง่ายดาย และเครื่องมือหรือโปรแกรมเหล่านี้ยังง่ายต่อการใช้งาน ถึงแม้ว่าคนที่ไม่มีความรู้เกี่ยวกับคอมพิวเตอร์มากนักก็สามารถใช้เครื่องมือโจมตีเครือข่ายเหล่านี้ได้ไม่ยากนัก ดังนั้น ฝ่ายสารสนเทศหรือผู้ที่มีหน้าที่ดูแลระบบจึงจำเป็นที่ต้องวิเคราะห์ความเสี่ยง ออกแบบติดตั้ง ระบบรักษาความปลอดภัย และเฝ้าระวังระบบรักษาความปลอดภัยในเครือข่ายให้มีใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา ดังนั้น การรักษาความปลอดภัยในเครือข่ายจึงเป็นสิ่งที่สำคัญและจำเป็นสำหรับองค์กร

"ไม่มีระบบใดที่ปลอดภัยร้อยเปอร์เซ็นต์**"** ยังเป็นคำกล่าวที่เป็นจริงเสมอ การรักษาความปลอดภัยนั้นเป็นทั้งศาสตร์และศิลป์ การมีระบบรักษาความปลอดภัยที่ดีที่สุดนั้นไม่ได้หมายความว่า ข้อมูล ระบบคอมพิวเตอร์ และองค์กรจะปลอดภัยจากอันตรายทั้งปวง การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการที่ไม่ใช่แค่การติดตั้งระบบการรักษาความปลอดภัยที่ดีที่สุด แต่จะรวมถึงการวิเคราะห์และบริหารความเสี่ยง (Risk) ที่เกิดจากภัยคุกคาม (Threat) และช่องโหว่หรือจุดอ่อน (Vulnerability) ขององค์กร การกำหนดนโยบายการรักษาความปลอดภัย การบังคับใช้นโยบาย การเฝ้าระวังเหตุการณ์อยู่ตลอดเวลา หนังสือเล่มนี้เขียนขึ้นโดยมีจุดมุ่งหมายเพื่อแนะนำแนวทางหรือวิธีปฏิบัติที่เหมาะสมสำหรับการรักษาความปลอดภัยข้อมูลขององค์กร

ก่อนที่จะเรียนรู้เกี่ยวกับกระบวนการรักษาความปลอดภัยของข้อมูล ก็ควรมาทำความรู้จักเกี่ยวกับคำว่าการรักษาความปลอดภัยข้อมูลหรือสารสนเทศ (Information Security) กันก่อน เราสามารถแยกคำนี้ออกเป็นสองคำคือ สารสนเทศ (Information) หมายถึง ความรู้ ความคิด ข่าวสาร และข้อเท็จจริง ส่วนการรักษาความปลอดภัย (Security) หมายถึง การทำให้รอดพ้นจากอันตราย หรือการทำให้รอดพ้นจากความกลัว ความทุกข์ใจ หรือความกังวล ดังนั้น เมื่อเรานำสองคำนี้มารวมกันก็จะได้ว่า การรักษาความปลอดภัยสารสนเทศหมายถึง การทำให้ความรู้ ความคิด ข่าวสาร และข้อเท็จจริง รอดพ้นจากอันตราย และถ้าตีความให้เข้ากับไอทีก็จะได้ว่า การรักษาความปลอดภัยสารสนเทศหมายถึง มาตรการที่ใช้สำหรับป้องกันผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งานความรู้ แนวคิด และข้อเท็จจริง

ความหมายที่กล่าวถึงข้างต้นนั้นเป็นความหมายที่กว้างมาก ซึ่งจะรวมถึงมาตรการทุกอย่างที่อาจใช้สำหรับป้องกันไม่ให้สิ่งไม่ดีเกิดขึ้นกับความรู้ ความคิด ข่าวสาร และข้อเท็จจริง นอกจากนี้รูปแบบของข้อมูลก็ยังไม่ได้จำกัดเฉพาะรูปแบบใดรูปแบบหนึ่ง มันอาจเป็นความรู้ หรืออาจเป็นความสามารถก็ได้ อย่างไรก็ตามมาตรการในการรักษาความปลอดภัยข้อมูลนั้นไม่สามารถที่จะรับรองได้ว่าข้อมูลจะปลอดภัยร้อยเปอร์เซ็นต์ ยกตัวอย่างเช่น ถึงแม้ว่าเราจะสามารถสร้างกำแพงเมืองได้ใหญ่และแข็งแรงมากแค่ไหน แต่ศัตรูก็อาจสามารถสร้างปืนใหญ่ที่สามารถทำลายกำแพงลงได้อย่างง่ายดาย หรือถึงแม้ว่าเราจะมีไฟร์วอลล์ที่มีประสิทธิภาพดีมากแค่ไหนแต่ผู้โจมตีนั้นอาจอยู่ภายในเครือข่าย เป็นต้น การรักษาความปลอดภัยนั้นจึงเป็นการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

ประวัติของการรักษาความปลอดภัย

รูปแบบของการรักษาความปลอดภัยของข้อมูลและทรัพย์สินอื่นๆ นั้นได้มีวิวัฒนาการกับกาลเวลาเหมือนกับสังคมและเทคโนโลยีอื่นๆ การเรียนรู้และเข้าใจวิวัฒนาการนี้จะช่วยให้เข้าใจระบบการรักษาความปลอดภัยที่มีอยู่ในปัจจุบัน และอาจเป็นบทเรียนที่ช่วยให้เราไม่ต้องทำผิดเหมือนกับที่เกิดขึ้นในอดีตได้

การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

แต่ก่อนนั้นทรัพย์สินส่วนใหญ่จะเป็นวัตถุที่จับต้องได้ ข้อมูลที่สำคัญก็อยู่ในรูปแบบวัตถุเช่นกันเนื่องจากข้อมูลจะถูกบันทึกไว้บนแผ่นหิน แผ่นหนัง หรือกระดาษ และบุคคลสำคัญในอดีตส่วนใหญ่จะไม่นิยมบันทึกข้อมูลที่สำคัญมากๆ ลงบนสื่อถาวร เช่น แผ่นหนังหรือกระดาษ และจะไม่สนทนาเกี่ยวกับข้อมูลเหล่านี้กับบุคคลอื่นนอกเหนือจากที่บุคคลที่ไว้ใจได้เท่านั้น นี่อาจเป็นที่มาของคำว่า **"ความรู้คืออำนาจ (Knowledge is power)"** ซึ่งหมายความว่า ผู้ที่มีความรู้คือผู้ที่มีอำนาจนั่นเอง และนี่อาจเป็นรูปแบบการรักษาความปลอดภัยที่ดีที่สุดในขณะนั้นก็ได้ ซันซู (Sun Tzu) นักปราชญ์ชาวจีนได้กล่าวไว้ว่า **"ความลับที่รู้โดยคนมากกว่าหนึ่งคนก็ไม่ถือว่าเป็นความลับอีกต่อไป"** การที่จะปกป้องทรัพย์สินที่เป็นวัตถุนั้นก็ต้องใช้การปกป้องทางด้ายกายภาพ เช่น กำแพง ประสาท หรือยาม เป็นต้น

ถ้าต้องมีการส่งข้อมูลไปที่อื่นก็จะใช้ผู้ส่งข่าว และส่วนใหญ่ก็จะมีผู้คุ้มกันติดตามไปด้วย ภัยอันตรายนั้นจะอยู่ในรูปแบบทางกายภาพทั้งสิ้น ไม่มีทางที่จะได้ข้อมูลมาโดยที่ไม่ต้องไม่คว้ามาด้วยมือ โดยส่วนใหญ่ทรัพย์สิน เช่น เงิน ทอง หรือข้อมูลที่บันทึกลงบนสื่อจะถูกขโมย หรือถูกแย่งไปจากเจ้าของ

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

อย่างไรก็ตามการรักษาความปลอดภัยเฉพาะทางด้านกายภาพด้านเดียวนั้นก็มีข้อบกพร่องหรือจุดอ่อนกล่าวคือ ถ้าเอกสารหรือวัตถุที่ใช้บันทึกข้อมูลถูกขโมยระหว่างการรับ/ส่ง ศัตรูก็สามารถเปิดอ่านและเข้าใจข้อมูลนั้นได้เลยทันที จนกระทั่งเมื่อราวยุคของจูเลียสซีซาร์ (Julius Caesar) ข้อบกพร่องนี้ได้ถูกค้นพบ โดยในสมัยนั้น (ยุคศตวรรษที่ 2) ได้มีการคิดค้นวิธีที่ใช้สำหรับ **"ซ่อน"** ข้อมูล หรือการเข้ารหัสข้อมูล (Encryption) ซึ่งข้อมูลจะถูกเข้ารหัสก่อนที่จะส่งไปให้อีกฝ่ายหนึ่ง ดังนั้น ถ้ามีการขโมยข้อมูลระหว่างทางผู้อ่านก็จะไม่เข้าใจข้อมูลถ้าไม่รู้วิธีถอดรหัส

รูปที่ 1.1 : Enigma เครื่องมือเข้า/ถอดรหัสที่ใช้ในช่วงสงครามโลกครั้งที่ 2

แนวคิดนี้ได้ถูกพัฒนามาใช้ในช่วงสงครามโลกครั้งที่ 2 เยอรมันใช้เครื่องมือที่เรียกว่า เอ็นนิกมา (Enigma) ดังแสดงในรูปที่ 1.1 สำหรับเข้ารหัสข้อมูลที่รับ/ส่งระหว่างหน่วยทหาร ในขณะนั้นเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสลับนี้ได้ถ้ามีการใช้งานอย่างถูกต้อง อย่างไรก็ตามข้อผิดพลาดนั้นเกิดจากผู้ใช้งานเครื่องนี้เอง จนเป็นผลทำให้ฝ่ายพันธมิตรสามารถอ่านข้อมูลได้

การสื่อสารทางด้านการทหารนั้นจะใช้รหัสแทนชื่อหน่วยหรือสถานที่อยู่แล้ว ตัวอย่างเช่น ญี่ปุ่นนั้นก็ใช้รหัสแทนชื่อเรียกทั่วไปในการสื่อสารกัน ถึงแม้ว่าสหรัฐฯ จะสามารถถอดรหัสข้อมูลได้แต่ก็ยังต้องทำความเข้าใจกับรหัสที่ใช้แทนชื่อทั่วไปนี้อีก ซึ่งเป็นการเพิ่มความยากในการเข้าใจข้อมูลจริงๆ ตัวอย่างเช่น ในช่วงก่อนที่จะเกิดสงครามที่

เกาะมิดเวย์ระหว่างญี่ปุ่นและสหรัฐฯ ในตอนนั้นสหรัฐฯสามารถถอดรหัสลับของญี่ปุ่นได้ แต่ยังไม่เข้าใจรหัสที่ใช้แทนชื่อสถานที่ โดยในข้อความที่ส่งนั้นญี่ปุ่นจะโจมตีเป้าหมายที่มีรหัสว่า "AF" แต่ในที่สุดสหรัฐฯ ก็สามารถถอดรหัสนี้ได้และรู้ว่า "AF" นั้นหมายถึง มิดเวย์นั่นเอง วิธีการถอดรหัสก็โดยสหรัฐฯ จะส่งข้อความว่า "เกาะมิดเวย์ขาดแคลนน้ำจืด" โดยข้อความนี้ไม่ได้เข้ารหัสทำให้ญี่ปุ่นอ่านข้อความนี้ได้ จึงเข้ารหัสและส่งข้อความให้หน่วยอื่นทราบ สหรัฐฯ สามารถดักอ่านข้อความนี้ได้ และถอดรหัสออกมาแล้วในข้อความนั้นมีอักษรว่า "AF" ที่ระบุสถานที่ ทำให้สหรัฐฯ รู้ได้ทันทีว่าอักษร "AF" นั้นหมายถึง เกาะมิดเวย์นั่นเอง

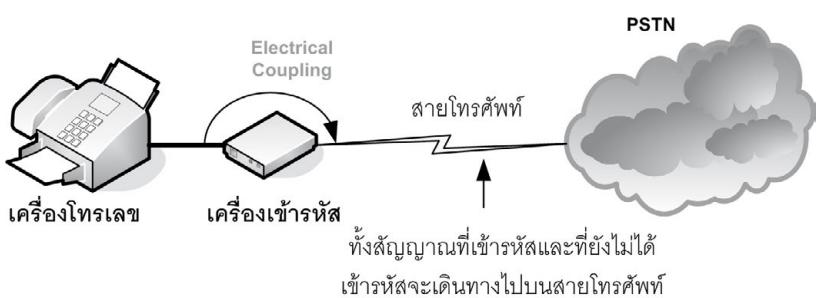
ข้อความไม่ใช่แค่ตัวอักษรที่เข้ารหัสในระหว่างการสื่อสารกัน ข้อความที่สื่อสารด้วยเสียง เช่น วิทยุ และโทรศัพท์ก็เป็นข้อมูลอีกประเภทหนึ่งที่ต้องเข้ารหัสเพื่อปกป้องความลับของข้อมูล หรือเพื่อป้องกันการดักฟังการสื่อสารด้วยเสียง สหรัฐฯ เข้ารหัสเสียงโดยใช้ "นาวาโฮโค้ดทอล์คเกอร์ (Navaho Code Talker)" นาโวโฮเป็นชนเผ่าหนึ่งที่มีภาษาเป็นของตัวเอง ผู้รับ/ส่งข่าวนั้นจะใช้ภาษานี้ในการสื่อสารกัน ซึ่งถ้าฝ่ายศัตรูมีการดักฟังวิทยุที่สื่อสารกันก็อาจจะได้ยินแต่คงไม่เข้าใจภาษาได้

หลังจากสงครามโลกครั้งที่ 2 สหภาพโซเวียตได้ใช้วันไทม์แพ็ด (One time pad) เพื่อเข้ารหัสข้อมูลที่รับ/ส่งโดยสายลับ วันไทม์แพ็ดใช้การเข้ารหัสโดยการส่งข้อความบนปึกกระดาษโดยแต่ละหน้าจะประกอบด้วยตัวเลขที่เป็นเลขสุ่ม และแต่ละหน้านั้นจะใช้แทนหนึ่งข้อความเท่านั้น รูปแบบการเข้ารหัสแบบนี้จะไม่สามารถถอดรหัสได้ถ้ามีการใช้อย่างถูกต้องคือ ใช้หนึ่งคีย์ต่อการเข้ารหัสหนึ่งข้อความ แต่สหภาพโซเวียตได้ใช้คีย์มากกว่าหนึ่งครั้ง ทำให้ข้อความที่ส่งนั้นถูกถอดรหัสได้โดยง่าย

การรักษาความปลอดภัยการแพ่รังสี (Emissions Security)

นอกจากการใช้งานอย่างถูกต้องแล้วการเข้ารหัสข้อมูลที่ดีเป็นสิ่งที่ยากต่อการถอดรหัสได้ ดังนั้น จึงได้มีความพยายามที่จะคิดค้นวิธีใหม่สำหรับอ่านข้อมูลที่เข้ารหัสและอยู่ในระหว่างการรับ/ส่ง ในช่วงทศวรรษ 1950 ได้มีการค้นพบว่าข้อมูลที่รับ/ส่งนั้นสามารถอ่านได้โดยการอ่านสัญญาณไฟฟ้าที่ส่งผ่านสายโทรศัพท์ อุปกรณ์อิเล็กทรอนิกส์ทุกประเภทจะมีการแผ่รังสีออกมา ซึ่งรวมถึงเครื่องพิมพ์โทรสารและเครื่องสำหรับเข้าและถอดรหัสข้อมูลด้วย เครื่องเข้ารหัสจะรับเข้าข้อความแล้วเข้ารหัสและส่งไปบนสายโทรศัพท์ ช่วงนั้นได้มีการค้นพบว่าสัญญาณไฟฟ้าที่แทนข้อมูลที่ยังไม่ได้เข้ารหัสก็ถูกส่งไปบนสายโทรศัพท์ด้วยเช่นกันนั่นหมายความว่า ข้อมูลเดิมที่ยังไม่ได้ถูกเข้ารหัสนั้นสามารถกู้คืนได้ถ้าใช้เครื่องมือที่ดี

ปัญหานี้เป็นเหตุให้สหรัฐฯ ต้องก Tempest) ซึ่งเป็นมาตรฐานที่ควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์ และใช้กับระบบที่สำคัญๆ จุดมุ่งหมายก็เพื่อลดการแผ่รังสีที่อาจใช้สำหรับการกู้คืนข้อมูลได้



รูปที่ 1.2 : สัญญาณที่ส่งผ่านสายโทรศัพท์

การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

การเข้ารหัสข้อมูลและการควบคุมการแผ่รังสีเป็นมาตรการการรักษาความปลอดภัยของข้อมูลที่เพียงพอ ถ้าระบบสื่อสารข้อมูลนั้นมีเพียงแค่การใช้เครื่องส่งโทรสารเหมือนดังใน รูปที่ 1.2 แต่ต่อมาได้มีการนำคอมพิวเตอร์เข้ามาใช้งานแทนเครื่องส่งโทรสาร และข้อมูลส่วนใหญ่ก็อยู่ในรูปแบบดิจิตอล และได้มีการพัฒนาคอมพิวเตอร์เพื่อให้ใช้งานง่ายและสะดวกมากขึ้นเรื่อยๆ ทำให้ผู้ที่มีเครื่องคอมพิวเตอร์สามารถเข้าถึงข้อมูลทั้งหมดที่จัดเก็บในเครื่องนั้นด้วยเช่นกัน จึงเกิดปัญหาความไม่ปลอดภัยในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์

ต่อมาในช่วงทศวรรษ 1970 เดวิด เบลล์ (David Elliott Bell) และลีโอนาร์ด ลา พาดูลา (Leonard J. La Padula) ได้พัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ (Bell-La Padula Model) แม่แบบนี้พัฒนาจากแนวคิดในการจัดระดับความปลอดภัยของข้อมูลของรัฐบาลสหรัฐฯ ซึ่งแบ่งออกได้เป็น 4 ชั้นคือ ไม่ลับ ลับ ลับมาก และลับที่สุด (Unclassified, Confidential, Secret, Top Secret) และระดับสิทธิ์ของผู้ที่เข้าถึงข้อมูลลับนี้ (Clearance) ซึ่งมี 4 ระดับเหมือนกัน หลักการของระบบนี้คือ ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้จะต้องมีสิทธิ์ (Clearance) เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนั้น ผู้ที่มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์ก็จะไม่สามารถเข้าถึงไฟล์นั้นได้

แนวคิดนี้ได้ถูกนำไปใช้ในกระทรวงกลาโหมของสหรัฐฯ โดยได้ชื่อว่า มาตรฐาน 5200.28 หรือ TCSEC (Trusted Computing System Evaluation Criteria) หรือเป็นที่รู้จักทั่วไปว่าออเรนจ์บุ๊ค (Orange Book) ในมาตรฐานนี้ได้กำหนดระดับความปลอดภัยของคอมพิวเตอร์ออกเป็นระดับต่างๆ 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

ในแต่ละระดับออเรนจ์บุ๊คได้กำหนดฟังก์ชันต่างๆ ที่ระบบต้องมีและการประกัน ดังนั้น ระบบที่ต้องการใบรับรองว่าจัดอยู่ในระดับใด ระบบนั้นต้องมีทั้งฟังก์ชันต่างๆ ที่กำหนดในระดับนั้นพร้อมทั้งการรับประกันในระดับนั้นได้ด้วย ข้อกำหนดเกี่ยวกับการรับประกันสำหรับระบบเพื่อให้เป็นไปตามมาตรฐานนั้น ต้องใช้เวลาและค่าใช้จ่ายสูงสำหรับบริษัทผู้ผลิต นี่จะเป็นผลที่ทำให้มีไม่กี่ระบบที่ได้รับการรับรองเหนือกว่าระดับ C2 ที่ผ่านมามีแค่ระบบเดียวเท่านั้นที่ได้รับใบรับรองในระดับ A1 นั่นคือระบบ Honeywell SCOMP แต่ระบบนี้ล้าสมัยไปในตอนที่ผ่านกระบวนการตรวจสอบเสร็จ

หลังจากนั้นได้มีการกำหนดมาตรฐานใหม่ขึ้นมาแทนออเรนจ์บุ๊ค เพื่อแก้ข้อบกพร่องในเรื่องของเวลาที่ใช้ในการตรวจทดสอบเพื่อออกใบรับรอง เช่น German Green Book (1989), Canadian Criteria (1990), ITSEC : Information Technology Security Evaluation Criteria (1991), และ Federal Criteria (1992) ซึ่งแต่ละมาตรฐานที่กล่าวมานี้ก็เพื่อกำหนดกระบวนการในการออกใบรับรองว่าระบบคอมพิวเตอร์นั้นมีความปลอดภัยระดับไหน อย่างไรก็ตามคอมพิวเตอร์มีวิวัฒนาการอย่างรวดเร็ว ระบบปฏิบัติการสมัยใหม่และฮาร์ดแวร์ใหม่ๆ ได้ถูกพัฒนาขึ้นมาแทนที่ระบบเก่าเร็วกว่าก่อนที่ระบบเก่าจะได้รับใบรับรอง

การรักษาความปลอดภัยเครือข่าย (Network Security)

ปัญหาหนึ่งที่เกี่ยวกับการตรวจทดลองเพื่อออกใบรับรองมาตรฐานระดับความปลอดภัยให้แก่ระบบคอมพิวเตอร์ก็คือ การขาดความเข้าใจเกี่ยวกับเรื่องเครือข่าย เมื่อคอมพิวเตอร์ถูกเชื่อมต่อกันเข้าเป็นเครือข่ายปัญหาใหม่ก็เกิดขึ้นและปัญหาเก่าก็เกิดจากอีกทางหนึ่ง ยกตัวอย่างเช่น การสื่อสารคอมพิวเตอร์นั้นเปลี่ยนจาก WAN มาเป็นแบบ LAN ซึ่งมีแบนด์วิธที่สูงมาก และอาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆ อาจไม่ได้ผล การแผ่รังสีจากสายทองแดงที่ใช้สื่อสารนั้นมีสูงมาก เพราะสายจะกระจายทั่วทั้งห้องหรือทั่วทั้งอาคารก็ได้ และสุดท้ายก็มีผู้ใช้หลายๆ คนที่สามารถล็อกอินได้จากหลายๆ ที่โดยที่อาจมีระบบบริหารจัดการที่เป็นศูนย์กลาง

ออเรนจ์บุ๊คไม่ได้มีข้อกำหนดเกี่ยวกับเครือข่ายคอมพิวเตอร์ ดังนั้น การเชื่อมต่อคอมพิวเตอร์เข้ากับเครือข่ายอาจทำให้ใบรับรองเป็นโมฆะหรือไม่มีประโยชน์ ทางออกสำหรับปัญหานี้คือ การใช้มาตรฐาน TNI (Trusted Network Interpretation) ของ TCSEC หรือที่รู้จักในชื่อ เรดบุ๊ค (Red Book) ซึ่งออกมาในปี 1987 ข้อกำหนดในเรดบุ๊คมาจากออเรนจ์บุ๊คทั้งหมดและได้เพิ่มส่วนที่เกี่ยวข้องกับเครือข่ายเข้าไป อย่างไรก็ตามเนื่องจากมีข้อกำหนดเกี่ยวกับฟังก์ชันและการรับประกันมาก ทำให้ใช้เวลามากเกินไปในการตรวจทดลองระบบ ทำให้มีเพียงบางระบบเท่านั้นที่ผ่านการตรวจทดลองของ TNI และในระบบที่ได้รับใบรับรองนั้นไม่มีระบบใดเลยที่ใช้ในเชิงพาณิชย์

การรักษาความปลอดภัยข้อมูล (Information Security)

จากประวัติศาสตร์ที่ได้กล่าวมานั้นเราสามารถสรุปได้ว่า ไม่มีวิธีการใดที่สามารถแก้ปัญหาเกี่ยวกับการรักษาความปลอดภัยได้ทั้งหมด แท้ที่จริงแล้วการรักษาความปลอดภัยที่ดีนั้นจะต้องใช้ทุกๆ วิธีการที่กล่าวมาร่วมกัน การรักษาความปลอดภัยทางด้านกายภาพก็ยังเป็นวิธีการที่ดีสำหรับการปกป้องทรัพย์สินที่เป็นวัตถุ การรักษาความปลอดภัยด้านการสื่อสาร (COMSEC) เป็นวิธีที่ใช้ปกป้องข้อมูลในระหว่างการสื่อสาร การรักษาความปลอดภัยเกี่ยวกับการแผ่รังสี (EMSEC) เป็นสิ่งที่จำเป็นเมื่อฝ่ายตรงกันข้ามมีเครื่องมือที่สามารถอ่านข้อมูลจากรังสีที่แผ่ออกจากระบบคอมพิวเตอร์ การรักษาความปลอดภัยคอมพิวเตอร์ (COMPSEC) เป็นสิ่งที่จำเป็นสำหรับการควบคุมการเข้าถึงระบบคอมพิวเตอร์ และการรักษาความปลอดภัยเครือข่าย (NETSEC) ก็เป็นสิ่งจำเป็นสำหรับการควบคุมการใช้งานเครือข่าย และวิธีการที่กล่าวมาทั้งหมดนี้รวมกันก็สามารถให้บริการการรักษาความปลอดภัยข้อมูล (INFOSEC) ได้

แต่สิ่งที่ยังขาดคือ กระบวนการสำหรับการตรวจทดลองเพื่อออกใบรับรองว่า ระบบคอมพิวเตอร์นั้นปลอดภัย เทคโนโลยีมีการเปลี่ยนแปลงที่เร็วมากกว่าเวลาที่ใช้กับกระบวนการตรวจทดลองความปลอดภัยของระบบ เพราะเป็นการยากมากหรือแทบจะเป็นไปไม่ได้เลยเกี่ยวกับการที่จะพิสูจน์ว่าระบบใดปลอดภัยหรือไม่

องค์ประกอบหลักของความปลอดภัยของข้อมูล

การที่จะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่ก็โดยการวิเคราะห์คุณสมบัติทั้ง 3 ด้านคือ ความลับ ความถูกต้อง และความพร้อมใช้งานว่ามีอยู่ครบหรือไม่ ถ้าขาดคุณสมบัติด้านใดด้านหนึ่งก็แสดงว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้น การรักษาความปลอดภัยข้อมูลจึงเป็นการปกป้องรักษาคุณสมบัติทั้ง 3 ด้านของดังต่อไปนี้

- **ความลับ (Confidentiality)** หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- **ความถูกต้อง (Integrity)** หมายถึง การรักษาความคงสภาพข้อมูลจากแหล่งที่มา หรือไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต

- **ความพร้อมใช้งาน** (Availability) หมายถึง การทำให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้เมื่อต้องการ

รูปที่ 1.3 : คุณสมบัติของความปลอดภัยข้อมูล

ความลับ (Confidentiality)

การรักษาความลับของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ หรือถ้ามองอีกมุมหนึ่งก็จะหมายถึง การปกป้องข้อมูลไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้นั่นเอง ข้อมูลบางอย่างมีความสำคัญ และจำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้

ความต้องการในการรักษาความลับของข้อมูลนั้นเริ่มจากด้านการทหารที่ต้องการปกปิดข้อมูลเกี่ยวกับกองทัพไม่ให้ฝ่ายตรงกันข้ามทราบ เช่น ที่ตั้งหน่วยทหาร แผนการโจมตี จำนวนกำลังพล และอาวุธที่ใช้ เป็นต้น ต่อมาหลักการนี้ก็ได้มีการประยุกต์ใช้ได้กับทางด้านธุรกิจเช่นกัน เช่น บริษัทผู้ผลิตสินค้าอาจต้องการที่จะเก็บข้อมูลเกี่ยวกับการออกแบบผลิตภัณฑ์ของตัวเองให้เป็นความลับ เพราะถ้าถูกขโมยไปหรือถูกเปิดเผย บริษัทคู่แข่งอาจนำไปเลียนแบบได้ง่าย อีกตัวอย่างหนึ่งคือ องค์กรจำเป็นที่ต้องเก็บข้อมูลส่วนตัวของพนักงาน หรือข้อมูลลูกค้าของตัวเองเป็นความลับ เพราะถ้าเปิดเผยอาจเป็นการละเมิดสิทธิส่วนบุคคลได้

กลไกหนึ่งที่ใช้ในการรักษาความลับคือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและคีย์ในการเข้าและถอดรหัสคีย์ (Key) หรือรหัสผ่าน (Password) เป็นกุญแจที่จะใช้สำหรับการเข้าและถอดรหัสข้อมูลได้ อย่างไรก็ตามการรักษาคีย์หรือรหัสผ่านก็เป็นอีกปัญหาหนึ่งที่เพิ่มขึ้นมาในกลไกควบคุมการเข้าถึง

ตัวอย่างที่เห็นได้ชัดในปัจจุบัน เช่น ในการซื้อขายสินค้าบนอินเทอร์เน็ตหรืออีคอมเมิร์ซ วิธีจ่ายเงินที่เป็นที่นิยมมากที่สุดวิธีหนึ่งคือการใช้บัตรเครดิต โดยผู้ใช้ต้องกรอกหมายเลขบัตรและวันหมดอายุในแบบฟอร์มสั่งซื้อผ่านทางเว็บ หลังจากนั้นเมื่อลูกค้ายืนยันการสั่งซื้อข้อมูลนี้ก็จะถูกส่งจากเครื่องของลูกค้าไปยังเซิร์ฟเวอร์ของบริษัทผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งในระหว่างที่ข้อมูลเดินทางผ่านอินเทอร์เน็ตนั้นต้องผ่านหลายจุด โดยในแต่ละจุดที่ข้อมูลส่งผ่านนั้นไม่มีการรับรองความปลอดภัยของข้อมูลเลย ถ้าข้อมูลนี้ถูกขโมยไปได้อย่างง่ายดายก็แสดงว่าข้อมูลนี้ขาดการรักษาความลับของข้อมูล อย่างไรก็ตามโดยส่วนใหญ่ในการสั่งซื้อสินค้านั้นข้อมูลที่รับ/ส่งระหว่างเครื่องไคลเอนท์และเซิร์ฟเวอร์นั้นจะถูกเข้ารหัสไว้โดยใช้คีย์หรือรหัสผ่าน ดังนั้น คนอื่นก็จะไม่สามารถอ่านข้อมูลนี้ได้ถ้าไม่มีคีย์หรือรหัสผ่าน แต่ถ้าบุคคลอื่นสามารถขโมยคีย์ได้และสามารถถอดรหัสข้อมูลในการสั่งซื้อได้ ก็แสดงว่าความลับของข้อมูลถูกทำลายหรือหรือข้อมูลถูกเปิดเผย (Compromised) ทำให้ข้อมูลนั้นไม่มีความปลอดภัย

การเข้ารหัสข้อมูลเป็นการปกป้องความลับของข้อมูลในระหว่างการส่งผ่านเครือข่ายที่ไม่มีความปลอดภัย นอกจากนี้ยังมีกลไกอื่นของระบบที่ใช้สำหรับปกป้องความลับของข้อมูลที่จัดเก็บไว้ในระบบนั่นคือ กลไกการควบคุมการเข้าถึง (Access Control) กลไกการควบคุมนี้จะพิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบว่าเป็นผู้ที่ได้รับอนุญาต

หรือไม่ วิธีการที่นิยมมากที่สุดคือการล็อกอินเข้าสู่ระบบ กลไกนี้จะแตกต่างจากการเข้ารหัสข้อมูลเนื่องจากข้อมูลอาจถูกอ่านได้ถ้ากลไกนี้ไม่ทำงาน หรือทำงานผิดพลาด หรือการหลีกเลี่ยงการใช้งานกลไกนี้ ดังนั้น ข้อดีข้อเสียของทั้งสองกลไกจะเป็นคนละจุดกัน กลไกควบคุมการเข้าถึงนั้นเป็นการปกป้องทั้งระบบ ส่วนการเข้ารหัสข้อมูลนั้นเป็นการรักษาความลับของข้อมูลนั้นๆ อย่างไรก็ตามถ้ากลไกควบคุมการเข้าถึงระบบทำงานผิดพลาดหรือล้มเหลวข้อมูลที่จัดเก็บในระบบนั้นก็จะอยู่ในสภาพที่ไม่ปลอดภัยเช่นกัน แต่ถ้าอย่างไรทั้งสองวิธีนี้ก็สามารถใช้พร้อมกันได้

การรักษาความลับของข้อมูลนั้นยังรวมถึงการรักษาไว้ซึ่งการมีอยู่ของข้อมูล ซึ่งบางทีก็อาจจะมีความสำคัญมากกว่าเนื้อข้อมูลก็ได้ ยกตัวอย่างเช่น การได้รู้ข้อมูลที่ว่า ผลของการสำรวจความนิยมของนักการเมืองคนหนึ่งสูงมาก ข้อมูลนี้อาจมีความสำคัญน้อยกว่าข้อมูลที่ว่า ผลการสำรวจความคิดเห็นนี้ได้มาจากการสำรวจความคิดเห็นจากสมาชิกของพรรค หรือกลุ่มผู้ที่สนับสนุนผู้สมัครนั้นเป็นส่วนใหญ่ หรืออีกอย่างหนึ่งคือข้อมูลที่ว่า รัฐบาลมีรูปแบบในการละเมิดสิทธิมนุษยชนของประชาชนอย่างไร อาจมีความสำคัญน้อยกว่าข้อมูลที่ว่า รัฐบาลได้ละเมิดสิทธิมนุษยชนของประชาชนตัวเอง กลไกควบคุมการเข้าถึงบางครั้งก็เป็นการปกปิดไว้ซึ่งการมีอยู่ของข้อมูล ซึ่งเป็นการป้องกันความลับของข้อมูลอีกชั้นหนึ่ง กล่าวคือถ้าไม่รู้ว่าข้อมูลนั้นมีอยู่ก็จะไม่มีความพยายามที่จะขโมยข้อมูลนั้นเกิดขึ้น

การซ่อนหรือปกปิดทรัพยากรก็เป็นอีกมุมหนึ่งของการรักษาความลับของข้อมูล ยกตัวอย่างเช่น องค์กรอาจต้องการที่จะปกปิดข้อมูลเกี่ยวกับโครงสร้างของระบบ หรือการคอนฟิกของระบบรวมถึงระบบที่องค์กรนั้นใช้งานอยู่ หรือการปกปิดไม่ให้ทราบถึงว่าองค์กรใช้อุปกรณ์เฉพาะใดบ้าง เพราะมันอาจถูกใช้โดยที่ไม่ได้รับอนุญาต หรือใช้ในทางที่ไม่เหมาะสมก็ได้ กลไกการควบคุมการเข้าถึงอาจใช้เพื่อการปกป้องทรัพยากรเหล่านี้ได้เช่นกัน

ความถูกต้อง (Integrity)

ความถูกต้องของข้อมูล (Integrity) หมายถึง ความเชื่อถือได้ของข้อมูลและการทำให้สารสนเทศที่อ่อนไหว และ/หรือมีคุณค่า ไม่ถูกเปิดเผยโดยคนที่ไม่ได้รับอนุญาตแหล่งที่มา ซึ่งการรักษาความถูกต้องของข้อมูลนั้นหมายถึง การป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงจากสภาพเดิม หรือการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเปลี่ยนแปลงข้อมูลได้ ความถูกต้องของข้อมูลนั้นประกอบด้วยสองส่วนคือ ความถูกต้องของเนื้อหาข้อมูล และความถูกต้องของแหล่งที่มาของข้อมูล แหล่งที่มาของข้อมูลอาจมีผลต่อความถูกต้องและความน่าเชื่อถือของข้อมูล

ตัวอย่างเช่น หนังสือพิมพ์รายงานข่าวว่าอาจมีการก่อการร้ายเกิดขึ้น ซึ่งข่าวนี้อาจรั่วมาจากสำนักข่าวกรองของรัฐบาล แต่เนื่องจากหนังสือพิมพ์ได้ข่าวมาด้วยวิธีการที่ผิดจึงรายงานว่าข่าวนี้ได้มาจากแหล่งอื่น เนื้อข่าวที่ตีพิมพ์ไปนั้นยังคงสภาพเดิมจากแหล่งที่มา ซึ่งเป็นการรักษาความถูกต้องของข้อมูล แต่แหล่งข้อมูลที่ได้มานั้นเปลี่ยนไป ดังนั้น ความถูกต้องของข้อมูลนี้ก็จะถูกทำลายไปเช่นกัน

กลไกในการรักษาความถูกต้องของข้อมูลนั้นประกอบด้วย 2 ส่วนคือ

- **การป้องกัน** (Prevention)
- **การตรวจสอบ** (Detection)

กลไกในการป้องกันนี้มีจุดมุ่งหมายเพื่อรักษาความถูกต้องของข้อมูล ซึ่งทำได้โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต ข้อแตกต่างระหว่างความพยายามทั้งสองประเภทนี้สำคัญ โดยในความพยายามข้อแรกนั้นเป็นความพยายามที่จะแก้ไข หรือเปลี่ยนแปลงข้อมูลโดยที่ผู้ที่พยายามนั้นไม่ได้รับอนุญาต แต่ความพยายามอีกข้อหนึ่งนั้นเกิดจากการที่ผู้ที่ได้รับอนุญาตพยายามที่จะแก้ไขข้อมูลนอกเหนือขอบเขตที่ตัวเองมีสิทธิ์ ยกตัวอย่างเช่น องค์กรหนึ่งใช้ระบบงานบัญชี ถ้ามีพนักงานคนหนึ่งได้เจาะเข้าระบบและแก้ไขเงินโบนัสของตัวเอง นี่เป็นการเปลี่ยนแปลงข้อมูลโดยที่ไม่ได้รับอนุญาต

ในกรณีที่สอง ผู้ดูแลระบบบัญชีของบริษัทเองซึ่งได้รับอนุญาตให้ใช้ระบบงาน แต่แก้ไขข้อมูลโดยการโอนเงินเข้าบัญชีตัวเองและพยายามปกปิดการกระทำนี้ ในกรณีนี้เป็นการเปลี่ยนแปลงข้อมูลจากผู้ที่ได้รับอนุญาต แต่เป็นการเปลี่ยนแปลงในทางที่ผิดหรือทำเกินกว่าสิทธิ์ที่ตัวเองมี การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) จะเป็นกลไกที่ใช้สำหรับการป้องกันการบุกรุกประเภทแรกได้เป็นอย่างดี ส่วนการป้องกันความพยายามจากผู้ที่ได้รับอนุญาตนั้นต้องใช้กลไกการตรวจสอบสิทธิ์ (Authorization) และกลไกอื่นๆ เพิ่มขึ้นมา

กลไกในการตรวจสอบความถูกต้องของข้อมูล (Detection) นั้นไม่ใช่กลไกในการรักษาให้ข้อมูลคงสภาพเดิม แต่เป็นกลไกที่ตรวจสอบว่าข้อมูลยังคงมีความเชื่อถือได้อยู่หรือไม่ กลไกในการตรวจสอบความถูกต้องของข้อมูลนั้นคือการตรวจเช็คและวิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบ ซึ่งรวมถึงเหตุการณ์ที่เกิดโดยระบบหรือผู้ใช้เอง เพื่อตรวจว่ามีปัญหาเกิดขึ้นหรือไม่ หรืออาจจะตรวจสอบและวิเคราะห์ข้อมูลว่า คุณสมบัติที่สำคัญหรือที่คาดหวังไว้ยังคงสภาพเดิมอยู่หรือไม่ กลไกนี้อาจรายงานว่าส่วนไหนของข้อมูลหรือไฟล์มีการแก้ไขหรืออาจรายงานว่าทั้งไฟล์นั้นถูกเปลี่ยนไปจากสภาพเดิมโดยสิ้นเชิง

การทำงานของการรักษาความถูกต้องของข้อมูลนั้นแตกต่างจากการรักษาความลับของข้อมูลมาก การรักษาความลับของข้อมูลนั้นเป็นการตรวจสอบว่าข้อมูลถูกขโมยหรือไม่ แต่การรักษาความถูกต้องของข้อมูลนั้นจะเกี่ยวกับการรักษาความถูกต้องของข้อมูลและการรักษาความน่าเชื่อถือของข้อมูลด้วย แหล่งที่มาของข้อมูล (ข้อมูลได้มาอย่างไรและจากใคร) ข้อมูลถูกป้องกันดีแค่ไหนก่อนที่จะมาถึงปลายทาง และข้อมูลถูกป้องกันอย่างไรในระหว่างที่จัดเก็บอยู่ในระบบนั้น ซึ่งทั้งหมดนี้เป็นผลกระทบต่อความถูกต้องของข้อมูลทั้งสิ้น ดังนั้น การตรวจสอบความถูกต้องของข้อมูลนั้นเป็นสิ่งที่กระทำยาก เนื่องจากมันจะขึ้นอยู่กับสมมติฐานเกี่ยวกับแหล่งที่มาและความน่าเชื่อถือของแหล่งที่มานั้น ซึ่งเป็นจุดหนึ่งที่มักจะถูกมองข้ามเป็นประจำ

ความพร้อมใช้งาน (Availability)

ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ ความพร้อมใช้งานเป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) เนื่องจากการที่ระบบไม่พร้อมใช้งานก็จะแย่พอๆ กับการที่ไม่มีระบบเลย ส่วนหนึ่งของความพร้อมใช้งานที่เกี่ยวข้องกับการรักษาความปลอดภัยคือ อาจมีผู้ไม่ประสงค์ดีพยายามที่จะทำให้ไม่สามารถเข้าถึงข้อมูลได้โดยการทำให้ระบบไม่สามารถใช้งานได้ การออกแบบระบบนั้นส่วนใหญ่จะใช้ข้อมูลทางด้านสถิติเกี่ยวกับรูปแบบหรือพฤติกรรมในการใช้งานระบบของผู้ใช้ ระบบจะถูกออกแบบเพื่อให้เหมาะกับสภาพแวดล้อมดังกล่าว ดังนั้น กลไกในการรักษาความพร้อมใช้งานนั้นจะทำงานในกรณีที่ระบบไม่ได้ทำงานในสภาพที่ปกติหรือที่ออกแบบไว้ ซึ่งถ้ากลไกนี้ไม่ทำงานส่วนใหญ่ระบบจะล่มหรือไม่พร้อมใช้งาน

ตัวอย่างเช่น ธนาคารแห่งหนึ่งเก็บข้อมูลบัญชีลูกค้าไว้ในฐานข้อมูลโดยใช้เซิร์ฟเวอร์ 2 เครื่องทำงานโหลดบาลานซิ่ง (Load Balancing) ซึ่งกันและกัน โดยเมื่อลูกค้าต้องการที่จะฝาก ถอน โอนเงิน หรือธุรกรรมอื่นๆ ก็จะต้องเข้ามาเช็คข้อมูลที่เซิร์ฟเวอร์นี้ก่อน เมื่อเซิร์ฟเวอร์หนึ่งไม่ทำงานเซิร์ฟเวอร์หนึ่งก็จะทำงานแทน แต่ถ้าธนาคารมีแค่เซิร์ฟเวอร์เดียว และถ้าเซิร์ฟเวอร์นั้นไม่ทำงานซึ่งอาจจะถูกโจมตีหรือเซิร์ฟเวอร์ล่มเสียเอง ความพร้อมใช้งานของข้อมูลก็จะขาดไป ซึ่งทำให้ข้อมูลไม่มีความปลอดภัยด้านความพร้อมใช้งาน

ความพยายามที่จะทำลายความพร้อมใช้งานจะเรียกว่า การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service : DoS) ซึ่งอาจเป็นการโจมตีที่อาจตรวจจับได้ยากที่สุด เนื่องจากในการวิเคราะห์ต้องพิจารณาว่าอะไรที่เป็นความพยายามที่ทำให้ระบบใช้งานไม่ได้ หรือเป็นเพียงเหตุการณ์ที่เกิดจากการใช้งานปกติ ซึ่งการวิเคราะห์นั้นจะอาศัยหลักการทางด้านสถิติเข้ามาช่วยในการวิเคราะห์ และสภาวะแวดล้อมการทำงานของแต่ละระบบก็จะแตกต่างกันไปด้วย ทำให้การวิเคราะห์

เพื่อติดสินว่าเป็นการโจมตีแบบปฏิเสธการให้บริการหรือไม่ยากยิ่งขึ้นอีก

หลักการเกี่ยวกับการรักษาความปลอดภัยข้อมูล

นอกจากคุณสมบัติทั้ง 3 ด้านที่กล่าวข้างต้นแล้วยังมีหลักการอื่นๆ เกี่ยวกับกับการรักษาความปลอดภัยข้อมูลอีก ซึ่งจะได้อธิบายดังต่อไปนี้

ความเป็นส่วนตัว (Privacy)

ข้อมูลที่องค์กรรวบรวม จัดเก็บ และใช้งานนั้นควรถูกใช้เพื่อจุดประสงค์ที่เจ้าของข้อมูลระบุตอนที่เก็บรวบรวมเท่านั้น แต่ถ้าใช้เพื่อจุดประสงค์อื่นก็แสดงว่าเป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูลนั้น บางองค์กรใช้ข้อมูลส่วนบุคคลในทางที่ผิด หรือบางทีอาจขายข้อมูลเหล่านี้ให้กับบุคคลหรือองค์กรอื่นโดยที่เจ้าของข้อมูลไม่รับรู้ ปัจจุบันข้อมูลส่วนบุคคลนั้นสามารถค้นหาและรวบรวมได้จากหลายๆ แหล่ง และเมื่อรวบรวมได้แล้วอาจถูกใช้ในทางที่เจ้าของนั้นไม่เห็นด้วยหรือไม่พึงประสงค์ หลายๆ คนก็เริ่มให้ความสำคัญกับกิจกรรมประเภทนี้แล้ว และได้แต่เพียงหวังว่ารัฐบาลจะมีมาตรการในการควบคุมสิทธิ์ส่วนบุคคลนี้

การระบุตัวตน (Identification)

ระบบสารสนเทศนั้นจะต้องสามารถระบุตัวตนของผู้ใช้แต่ละคนที่ใช้งานระบบได้ การระบุตัวตนเป็นขั้นแรกในการที่จะสามารถเข้าถึงข้อมูลที่มีชั้นความลับ และเป็นพื้นฐานสำหรับขั้นตอนต่อไปคือการพิสูจน์ทราบตัวตน (Authentication) และการพิสูจน์สิทธิ์ (Authorization) เมื่อใช้การระบุตัวตนและการพิสูจน์ทราบตัวตนร่วมกันเป็นส่วนสำคัญในการสร้างระดับในการเข้าถึงระบบ หรือการอนุญาตสิทธิ์มากน้อยแค่ไหนในการใช้งานระบบ รูปแบบของการระบุตัวตนที่นิยมใช้ในระบบคอมพิวเตอร์มากที่สุดก็โดยการใช้ยูสเซอร์เนม (Username)

การพิสูจน์ทราบตัวตน (Authentication)

การพิสูจน์ทราบตัวตนนั้นเกิดขึ้นเมื่อระบบควบคุมพิสูจน์ว่าผู้ใช้ใช่คนที่ผู้ใช้บอกหรือไม่ เช่น ถ้าผู้ใช้ระบุยูสเซอร์เนมแล้วก็ต้องสามารถระบุรหัสผ่านที่คู่กับยูสเซอร์นั้นได้ หรืออีกตัวอย่างหนึ่งคือ การใช้ใบรับรองอิเล็กทรอนิกส์ในการสร้างการเชื่อมต่อแบบ SSL (Secure Socket Layer) เพื่อพิสูจน์ว่าเซิร์ฟเวอร์ที่เชื่อมต่ออยู่นั้นใช่เครื่องที่ต้องการเชื่อมต่อจริงๆ

การอนุญาตใช้งาน (Authorization)

หลังจากที่สามารถพิสูจน์ทราบตัวตนแล้ว ขั้นตอนต่อไปคือ การตรวจสอบสิทธิ์ของผู้ใช้หรือไคลเอนท์นั้นว่าได้มีการกำหนดสิทธิ์ให้ใช้งานระบบได้ในระดับไหน ซึ่งสิทธิ์นั้นประกอบด้วย การเข้าถึงหรืออ่าน การแก้ไข และการลบข้อมูล เช่น การใช้ ACL (Access Control List) หรือการจัดกลุ่มของผู้ใช้ในระบบ เช่น กลุ่มผู้ใช้ในระดับผู้ดูแลระบบ (Administrators หรือ Root) นั้นมีสิทธิ์สูงสุดหรือสามารถทำอะไรก็ได้ในระบบ แต่ถ้าเป็นผู้ใช้ทั่วไปก็จะมีสิทธิ์ที่ต่ำลงมาแล้วแต่จะกำหนด อีกตัวอย่างหนึ่งคือ ระบบฐานข้อมูล หลังจากระบบพิสูจน์ทราบตัวตนแล้วขั้นตอนต่อไปก็เป็นการตรวจสอบสิทธิ์ว่าผู้ใช้คนนั้นมีสิทธิ์ในการอ่าน เขียน สร้าง และลบหรือไม่

การตรวจสอบได้ (Accountability)

ความสามารถในการตรวจสอบการใช้งานระบบได้ ก็เป็นอีกส่วนที่สำคัญเพราะเป็นการรับรองว่าทุกๆ กิจกรรม

หรือเหตุการณ์ที่เกิดขึ้นนั้นสามารถตรวจสอบได้ว่าเกิดขึ้นเพราะใครหรือโพรเซสไหน ยกตัวอย่างเช่น การเก็บล็อก (Logs) เกี่ยวกับกิจกรรมต่างๆ ที่ผู้ใช้แต่ละคนใช้งานระบบ เป็นต้น

ภัยคุกคาม (Threat)

ภัยคุกคาม (Threat) หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรือถ้ามีการเตรียมการที่ดีเมื่อมีเหตุการณ์เกิดขึ้นก็จะช่วยลดความเสียหายได้ การกระทำที่อาจก่อให้เกิดความเสียหายเราจะเรียกว่าการโจมตี (Attack) ส่วนผู้ที่ทำเช่นนั้น หรือผู้ที่เป็นเหตุให้เหตุการณ์ดังกล่าวเกิดขึ้นจะเรียกว่าผู้โจมตี (Attacker) หรือบางทีก็เรียกว่าแฮคเกอร์ (Hacker) หรือแคร็คเกอร์ (Cracker)

เครือข่ายเป็นเทคโนโลยีที่น่าอัศจรรย์ทำให้ชีวิตเราสะดวกขึ้นเป็นอย่างยิ่ง แต่ก็ยังคงมีความเสี่ยงอยู่มากหากไม่มีการควบคุมหรือป้องกันที่ดี การโจมตีหรือการบุกรุกเครือข่ายหมายถึงความพยายามที่จะเข้าใช้ระบบ การแก้ไขข้อมูลหรือคอนฟิกของระบบ การทำให้ระบบไม่สามารถใช้การได้ และการทำให้ข้อมูลเป็นเท็จ

การรักษาความปลอดภัยของคุณสมบัติข้อมูลทั้ง 3 ด้านคือ ความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) จะเป็นสิ่งที่ต้านภัยคุกคามที่อาจจะเกิดขึ้น เราสามารถแบ่งภัยคุกคามที่อาจจะเกิดขึ้นกับข้อมูลได้ 4 ประเภทคือ

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

ภัยคุกคามทั้ง 4 ประเภทนี้จะครอบคลุมภัยทั้งหมดที่อาจจะเกิดขึ้นได้ เนื่องจากภัยคุกคามนั้นมีความหลากหลาย ดังนั้น การทำความเข้าใจพื้นฐานเกี่ยวกับภัยประเภทต่างๆ จะทำให้เข้าใจระบบการรักษาความปลอดภัยมากขึ้น ด้านล่างเป็นตัวอย่างของภัยคุกคามที่อาจเกิดขึ้นได้

สิ่งที่ทำให้เกิดการโจมตีเกิดเนื่องจากการที่ผู้โจมตีมีแรงจูงใจ ดังนั้น สิ่งแรกที่นักเจาะระบบจะทำคือ การตัดสินใจในจุดมุ่งหมายของเขา ขั้นตอนนี้เป็นขบวนการคิดที่มีสติ แต่บางครั้งก็รู้เพียงแค่ว่าเขาต้องการที่จะโจมตีเป้าหมายโดยที่ไม่มีเหตุผลที่ชัดเจน การตัดสินใจนี้อาจได้รับอิทธิพลจากความเสี่ยงที่เขายอมรับได้ในขณะที่โจมตี อย่างไรก็ตามแฮคเกอร์ส่วนใหญ่จะไม่ระวัง หรือคาดเดาว่าผลที่เขาจะได้รับจากการกระทำของเขานั้นคงไม่เลวร้ายจนเกินไป เช่น ถ้ามีการโจมตีเว็บไซต์ใหญ่ อย่างเช่น CNN.COM ระบบอาจถูกกดดันด้วยสื่อจนอาจนำไปสู่การสืบค้นหาผู้กระทำผิดมาลงโทษให้ได้

รูปแบบของการโจมตีนั้นก็เปลี่ยนแปลงไปตามธรรมชาติของคอมพิวเตอร์และเครือข่ายที่มีวิวัฒนาการอย่างต่อเนื่อง ในช่วงปี 1980 นั้นเป้าหมายส่วนใหญ่จะเป็นคอมพิวเตอร์แต่ละเครื่อง แต่ในช่วงปี 1990 นั้นเป้าหมายหลักก็กลายมาเป็นระบบเครือข่าย ปัจจุบันเป้าหมายหลักคือระบบเครือข่ายที่เป็นโครงสร้างของอินเทอร์เน็ตทั่วโลก โดยทั่วไปนักโจมตีนั้นมีความรู้ความชำนาญสูง และการโจมตีนั้นจะเปลี่ยนจากการค้นหาบั๊ก หรือช่องโหว่ของซอฟต์แวร์หรือแอพพลิเคชันเฉพาะไปเป็นการโจมตีช่องโหว่ของซอฟต์แวร์หรือฮาร์ดแวร์ที่เป็นโครงสร้างของระบบ เช่น ระบบปฏิบัติการ เป็นต้น นอกจากนี้การโจมตีสมัยใหม่นั้นจะมีเวลาน้อยในการตอบโต้ เช่น ไวรัสบางตัวนั้นสามารถแพร่กระจายไปทั่วโลกโดยใช้เวลาเพียง 10 นาทีหรือน้อยกว่านั้น นอกจากนั้นการโจมตีบางอย่างนั้นก็ยากต่อการตรวจพบได้ แทนที่จะโจมตีระบบคอมพิวเตอร์ที่เป็นโครงสร้างโดยตรง การโจมตีนั้นอาจแอบแฝงมากับข้อมูล ซึ่งทำให้การตรวจจับนั้นทำได้ยาก รูปแบบของการโจมตีนั้น

มีความซับซ้อนมากขึ้น ดังนั้น ผู้ดูแลระบบต้องพยายามตามให้ทันเพื่อจะได้หาวิธีป้องกันหรือแก้ไขได้ทันเวลา

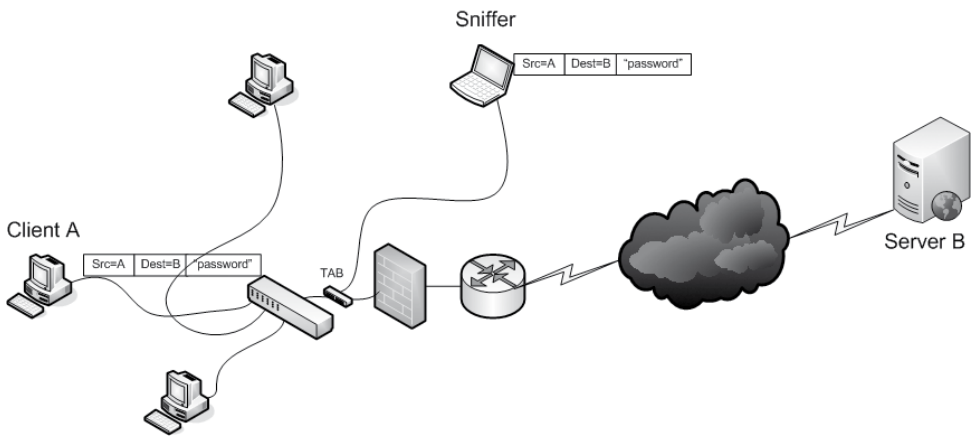
ผู้ดูแลระบบต้องเรียนรู้เกี่ยวกับรูปแบบใหม่ๆ ของการโจมตี ผู้โจมตีก็เช่นกันจะพยายามเรียนรู้รูปแบบที่หลากหลายในการโจมตี ต่อไปนี้เป็นรูปแบบการโจมตีที่มักได้ยินเป็นประจำ

การสอดแนม (Snooping)

การสอดแนม หรือสนูปปิง (Snooping) บางทีก็ใช้คำว่า สนิฟฟิง (Sniffing) หรือบางทีก็เรียกว่า อีฟดรอปปิง (Eavesdropping) ซึ่งหมายถึง การดักเพื่อแอบดูข้อมูลซึ่งจัดอยู่ในประเภทการเปิดเผย การสอดแนมเป็นการโจมตีแบบพาสซีฟ (Passive) คือ เป็นการกระทำที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล ยกตัวอย่างเช่น การดักอ่านข้อมูลในระหว่างที่ส่งผ่านเครือข่าย การอ่านไฟล์ที่จัดเก็บอยู่ในระบบ การแท็ปสายข้อมูล (Wiretapping) เป็นวิธีการหนึ่งของการสนูปปิง เพื่อเฝ้าดูข้อมูลที่วิ่งบนเครือข่ายเครือข่าย การรักษาความลับของข้อมูล เช่น การเข้ารหัสข้อมูล (Encryption) จะเป็นสิ่งที่ป้องกันภัยคุกคามประเภทนี้

แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) เป็นรูปแบบหนึ่งของการโจมตีแบบสอดแนม ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นชุดเล็กๆ ซึ่งเรียกว่า แพ็กเก็ต (Packet) แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยที่ไม่ได้เข้ารหัส หรือในรูปแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้น ข้อมูลอาจถูกคัดลอกและโพรเซสโดยเครื่องอื่นที่ไม่ใช่เครื่องปลายทางก็ได้

เน็ตเวิร์คโปรโตคอลเป็นตัวกำหนดหมายเลขของแต่ละแพ็กเก็ต ซึ่งเป็นสิ่งที่คอมพิวเตอร์ใช้สำหรับระบุว่าแพ็กเก็ตนั้นส่งจากไหนไปไหน เนื่องจากโปรโตคอลที่ใช้ส่วนใหญ่ เช่น TCP/IP เป็นโปรโตคอลมาตรฐานและเป็นที่รู้จักกันโดยทั่วไป ทำให้มีการพัฒนาแอพพลิเคชันที่สามารถดักจับเพ็กเก็ตที่วิ่งบนเครือข่ายได้ ซึ่งเทคนิคนี้เรียกว่าแพ็กเก็ตสนิฟเฟอร์ สิ่งที่น่ากลัวจริงๆ ในปัจจุบันนี้คือโปรแกรมแพ็กเก็ตสนิฟเฟอร์มีให้ดาวน์โหลดบนอินเทอร์เน็ตมากมาย และผู้ที่ใช้งานไม่จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์มากก็สามารถใช้ซอฟต์แวร์เหล่านี้ได้ แพ็กเก็ตสนิฟเฟอร์เป็นโปรแกรมใช้เน็ตเวิร์คการ์ดในโหมดโพรมิสเซียส (Promiscuous Mode) ซึ่งโหมดนี้เน็ตเวิร์คการ์ดจะรับทุกๆ แพ็กเก็ตที่วิ่งบนสายสัญญาณและส่งต่อไปให้ยังแอพพลิเคชันเพื่อโพรเซสต่อไป รูปที่ 1.4 แสดงการสอดแนมแบบสนิฟเฟอริง โดยเครื่องไคลเอนท์ A นั้นต้องการที่จะส่งข้อมูลไปให้เซิร์ฟเวอร์ B สนิฟเฟอร์อาจใช้อุปกรณ์ที่เรียกว่า “แท็ป (Tap)” เพื่อดึงสัญญาณจากสายสัญญาณที่เป็นเส้นทางผ่านของข้อมูล แพ็กเก็ตข้อมูลจะถูกส่งไปยังเครื่องของสนิฟเฟอร์ซึ่งเชื่อมต่อเข้ากับแท็ป ทำให้เครื่องนี้สามารถดักอ่านข้อมูลทุกอย่างที่ส่งผ่านในเครือข่ายได้



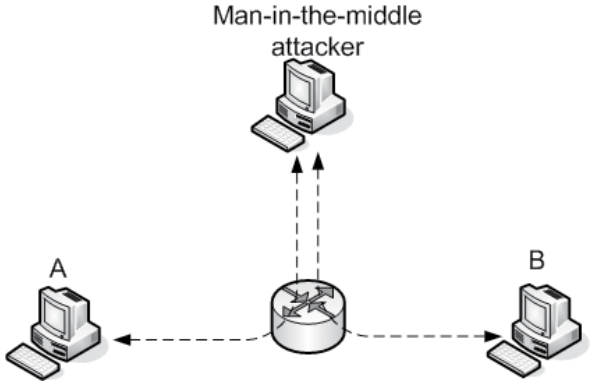
รูปที่ 1.4 : Packet Sniffing เป็นการสอดแนมแพ็กเก็ตที่อยู่ในเครือข่าย

เนื่องจากแอพพลิเคชันส่วนใหญ่จะส่งแพ็กเก็ตแบบเคลียร์เท็กซ์ แพ็กเก็ตสนิฟเฟอร์สามารถตรวจจับข้อมูลที่อาจเป็นประโยชน์ได้ เช่น ชื่อผู้ใช้และรหัสผ่าน เป็นต้น ถ้าหากมีการใช้ฐานข้อมูลผ่านเครือข่าย แพ็กเก็ตสนิฟเฟอร์อาจโจมตีโดยใช้ชื่อผู้ใช้และรหัสผ่านที่ตรวจจับได้ก็ได้ สิ่งที่น่ากลัวมากกว่าคือ ผู้ใช้มักจะใช้ชื่อผู้ใช้ และรหัสผ่านเหมือนกันทุกๆ แอพพลิเคชันหรือระบบ ทำให้ผู้บุกรุกสามารถโจมตีแอพพลิเคชันหรือระบบต่างๆ ได้อย่างง่ายดาย และอาจทำให้เครือข่ายเกิดความเสียหายมากกว่าที่คิด

การเปลี่ยนแปลงข้อมูล (Modification)

การเปลี่ยนแปลง หมายถึง การแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต ซึ่งภัยนี้จะจัดอยู่ใน 3 ประเภทคือ อาจเป็นการหลอกหลวง (Deception) ถ้าฝ่ายรับต้องใช้ข้อมูลที่ถูกเปลี่ยนแปลงแล้ว หรือข้อมูลที่ได้รับเป็นข้อมูลที่ผิดแล้วนำไปใช้งาน ถ้าการเปลี่ยนแปลงข้อมูลแล้วทำให้ระบบถูกควบคุมได้ก็จะจัดอยู่ในประเภทการทำให้ยุ่งและการควบคุมระบบ การสนูปปิง (Snooping) เป็นแบบพาสซีฟแต่การเปลี่ยนแปลงข้อมูล (Modification) เป็นแบบแอ็คทีฟ ตัวอย่างเช่น การโจมตีแบบผ่านคนกลาง (Man-in-the-middle attack) ซึ่งผู้บุกรุกอ่านข้อมูลจากผู้ส่งแล้วแก้ไขก่อนที่จะส่งต่อไปให้ผู้รับ โดยคาดหวังว่าผู้รับและผู้ส่งไม่รู้ว่ามีบุคคลที่สามเข้ามาเกี่ยวข้อง การรักษาความถูกต้อง (Integrity) เป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้

การโจมตีแบบผ่านคนกลางนั้นผู้โจมตีต้องสามารถเข้าถึงแพ็กเก็ตที่ส่งระหว่างเครือข่ายได้ เช่น ผู้โจมตีอาจอยู่ที่ ISP ซึ่งสามารถตรวจจับแพ็กเก็ตที่รับส่งระหว่างเครือข่ายภายในและเครือข่ายอื่นๆ โดยผ่าน ISP การโจมตีนี้จะใช้แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) เป็นเครื่องมือเพื่อขโมยข้อมูล หรือใช้เซสชันเพื่อแอ็กเซสเครือข่ายภายใน หรือวิเคราะห์การจราจรของเครือข่ายหรือผู้ใช้



รูปที่ 1.5 : Man-in-the-middle attack

การปลอมตัว (Spoofing)

การปลอมตัวหรือสปู๊ฟฟิง (Spoofing) หมายถึง การทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นอีกบุคคลหนึ่ง การโจมตีประเภทนี้จัดอยู่ในทั้งประเภทการหลอกลวงและการควบคุมระบบ การสปู๊ฟฟิงเป็นการหลอกให้คู่สนทนาเชื่อว่าตนกำลังสนทนากับฝ่ายที่ต้องการสนทนาจริงๆ ยกตัวอย่างเช่น สมมติว่าผู้ใช้ต้องการที่จะล็อกอินเข้าสู่ระบบผ่านทางอินเทอร์เน็ต แต่เมื่อมีการหลอกให้ล็อกอินเข้าอีกระบบหนึ่งซึ่งผู้ใช้คนนั้นเข้าใจว่าเป็นระบบที่ตนเองต้องการล็อกอินจริงๆ หรืออีกตัวอย่างหนึ่งคือ ผู้ใช้ต้องการที่จะอ่านไฟล์แต่ผู้บุกรุกได้จัดการให้ผู้ใช้อ่านอีกไฟล์หนึ่งแทน การโจมตีแบบนี้อาจเป็นแบบพาสซีฟกล่าวคือข้อมูลไม่ได้ถูกเปลี่ยนแปลง แต่ส่วนใหญ่จะเป็นแบบแอ็คทีฟ หรือข้อมูลมีการเปลี่ยนแปลง การรักษาความถูกต้อง โดยการใช้การตรวจสอบตัวตน (Authentication) จะเป็นวิธีที่ใช้สำหรับป้องกันการโจมตีประเภทนี้ได้

การหลอกลวงแบบมาสคิวเรดดิ้ง (Masquerading) ก็เป็นอีกวิธีหนึ่งที่ใช้สำหรับปลอมตัวซึ่งจะคล้ายกับการมอบอำนาจ (Delegation) ซึ่งจะหมายถึง การที่คนหนึ่งมอบอำนาจให้อีกคนหนึ่งทำหน้าที่บางอย่างแทน การเข้าใจข้อแตกต่างระหว่างการมอบอำนาจและการปลอมตัวนั้นเป็นสิ่งที่สำคัญกล่าวคือ การมอบอำนาจนั้นเป็นการอนุญาตให้อีกบุคคลหนึ่งทำหน้าที่แทนตนในสิ่งใดสิ่งหนึ่ง ซึ่งผู้ที่ได้รับมอบอำนาจนั้นจะประกาศให้คนอื่นทราบด้วย และเมื่อจะกระทำการใดก็จะประกาศบอกก่อน ส่วนการปลอมตัวนั้นจะไม่มีใครรู้การกระทำนั้นเลยซึ่งรวมทั้งผู้ที่ถูกปลอมตัวด้วย ถ้าเกี่ยวกับการรักษาความปลอดภัยแล้ว การปลอมตัวเป็นสิ่งที่ผิดส่วนการมอบอำนาจนั้นเป็นสิ่งที่ถูก

ไอพีสปูฟฟิง (IP Spoofing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแสร้งว่าเป็นว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ไอพีแอดเดรสข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบไอพีสปูฟฟิงเป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปในแพ็กเก็ตที่รับ/ส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์สื่อสารกันในเครือข่าย การที่จะทำอย่างนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติ้งเทเบิลของเราท์เตอร์เพื่อให้ส่งต่อแพ็กเก็ตไปที่เครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือการที่ผู้บุกรุกสามารถแก้ไขให้แอพพลิเคชันส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลิเคชันนั้นผ่านทางอีเมล หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชันได้โดยใช้ข้อมูลดังกล่าว

อย่างไรก็ตามถ้าผู้บุกรุกสามารถปรับเปลี่ยนเราท์ติ้งเทเบิลเพื่อให้ส่งข้อมูลไปยังเครื่องปลอมได้ ผู้บุกรุกสามารถรับ/ส่งข้อมูลกับแอพพลิเคชันนั้นเสมือนเป็นหนึ่งในผู้ใช้ทั่วๆ ไปได้ ไอพีสปูฟฟิงไม่จำเป็นจะต้องเป็นคอมพิวเตอร์ที่อยู่นอกเครือข่ายเท่านั้น แต่อาจจะเป็นผู้ใช้ที่อยู่ข้างในที่ไม่มีสิทธิ์ก็ได้ ซึ่งเป็นที่ทราบกันดีว่า การโจมตีเครือข่ายนั้น 90% จะเป็นการโจมตีที่เกิดจากภายในเครือข่ายเอง

การปฏิเสธการให้บริการ (Denial of Service : DoS)

การปฏิเสธการให้บริการ (Denial-of-Service) หมายถึง การขัดขวางการให้บริการของเซิร์ฟเวอร์เป็นเวลานาน การโจมตีแบบนี้อาจเกิดที่เครื่องเซิร์ฟเวอร์ โดยการขัดขวางไม่ให้เซิร์ฟเวอร์ใช้รีซอร์สที่จำเป็นสำหรับการให้บริการ หรืออาจเกิดที่ปลายทาง โดยการขัดขวางช่องสื่อสารไปยังเซิร์ฟเวอร์ หรืออาจเกิดในระหว่างทาง โดยการละทิ้งแพ็กเก็ตข้อมูลที่รับ/ส่งระหว่างเซิร์ฟเวอร์ การรักษาความพร้อมใช้งาน (Availability) เป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้ได้ การโจมตีแบบปฏิเสธการให้บริการ หรือการหน่วงเวลาอาจเป็นการโจมตีระบบโดยตรง หรืออาจจะเกิดปัญหาที่ไม่เกี่ยวข้องกับระบบการรักษาความปลอดภัยก็ได้

การโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DoS (Denial-of-Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งโดยปกติจะทำโดยการใช้รีซอร์สของเซิร์ฟเวอร์จนหมด หรือถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ (Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่นๆ ไม่สามารถเข้ามาใช้บริการได้ การโจมตีแบบนี้อาจใช้โปรโตคอลที่ใช้บนอินเทอร์เน็ตทั่วๆ ไป เช่น TCP (Transmission Control Protocol) หรือ ICMP (Internet Control Message Protocol) การโจมตีแบบดีไนล์ออฟเซอร์วิส เป็นการโจมตีจุดอ่อนของระบบหรือเซิร์ฟเวอร์มากกว่าการโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่ของระบบการรักษาความปลอดภัย อย่างไรก็ตามการโจมตีอาจทำให้ประสิทธิภาพของเครือข่ายลดลงโดย การส่งแพ็กเก็ตที่เป็นขยะจำนวนมากเข้าไปในเครือข่าย ทำให้เราท์เตอร์และสวิตช์เสียเวลารับ/ส่งแพ็กเก็ตขยะนั้นๆ

การโจมตีที่มีความเสี่ยงน้อยที่สุดคือ การโจมตีแบบปฏิเสธการให้บริการ (Denial of service) โดยการโจมตีนั้นจะใช้คอมพิวเตอร์ที่ไม่มีระบบการรักษาความปลอดภัยที่แข็งแกร่ง และทำให้เห็นผลทันทีและทำให้ผู้โจมตีพอใจ เช่น การทำให้เว็บเซิร์ฟเวอร์ล่ม เป็นต้น อย่างไรก็ตามการโจมตีแบบปฏิเสธการให้บริการนี้ก็ทำอะไรได้ไม่มากนัก และอีกอย่างคือการโจมตีแบบนี้ส่วนใหญ่ผู้โจมตีจะไม่ค่อยได้ประโยชน์อะไรมากนัก

การโจมตีแบบเจาะเข้าระบบเพื่อขโมยข้อมูล อย่างเช่น หมายเลขบัตรเครดิต หรือเจาะเข้าระบบเพื่อใช้เป็นฐานในการโจมตีไซต์อื่นต่อไป ผู้โจมตีที่ถูกจับได้ส่วนใหญ่จะเป็นพวกที่มีความมั่นใจสูงเกินไป คิดว่าตัวเองจะไม่โดนจับ และก็พยายามโจมตีไซต์อื่นๆ ไปเรื่อยๆ ในช่วงเวลาเป็นวันหรือสัปดาห์ ถ้าผู้โจมตีรู้ว่าต้องหยุดช่วงไหนแล้วพยายามหนีก็อาจทำให้การสืบหานั้นเป็นเรื่องที่ยากขึ้น

ยิ่งแฮคเกอร์ที่มีความรู้และความชำนาญน้อย การกระทำของเขายิ่งเซ่อซ่าและโง่ สคริปต์คิดดี้ส์ (Script Kiddies) อาจไม่ใส่ใจในการสำรวจสภาวะของระบบหรือเครือข่ายก่อนโจมตีเลย เขาอาจดาวน์โหลดโปรแกรมและทดลองโจมตีโดยเลือกเป้าหมายแบบสุ่ม การโจมตีแบบนี้จะถูกตรวจจับได้ง่ายโดยไฟร์วอลล์หรือ IDS (Intrusion Detection System) และมีการแจ้งเตือน การโจมตีแบบนี้ส่วนใหญ่จะไม่สำเร็จถ้ามีการอัพเดตระบบหรือซอฟต์แวร์ให้ทันสมัยตลอดเวลา แฮคเกอร์ที่มีความชำนาญส่วนใหญ่จะวิเคราะห์เบื้องต้นเกี่ยวกับระบบหรือเครือข่ายเป้าหมายก่อน โดยปกติจะใช้เครื่องมือ เช่น Traceroute และข้อมูลเกี่ยวกับ DNS ยกตัวอย่างเช่น ถ้ามีคนรีเวอร์ส DNS เพื่อค้นหาชื่อโดเมนของหมายเลข IP ภายในเครือข่ายแลนขององค์กร อาจไม่ได้รับการตักเตือนหรือถามถึงเลย เนื่องจากอาจมองว่าเป็นเรื่องที่ไม่ได้สร้างความเสียหายใดๆ และอีกอย่างไม่มีวิธีที่จะป้องกันการกระทำอย่างนี้ได้เลย เพราะการทำเช่นนี้อาจเกิดจากซอฟต์แวร์จัดการเครือข่าย และการที่จะเก็บล็อกเพื่อวิเคราะห์นั้นอาจเป็นการต้องเก็บข้อมูลมหาศาล อีกวิธีหนึ่งก็โดยการสแกนสายโทรศัพท์เพื่อค้นหาสายโทรศัพท์ที่เชื่อมต่อกับโมเด็มที่ไม่มีระบบการรักษาความปลอดภัย แฮคเกอร์ที่มีความชำนาญอาจพยายามใช้เทคนิค วิศวกรรมสังคม (Social Engineering) เพื่อให้ได้ข้อมูลที่สำคัญ เช่น ยูสเซอร์เนมและพาสเวิร์ด เป็นต้น การกระทำเช่นนี้จะไม่เห็นในกลุ่มแฮคเกอร์สองประเภทแรก เนื่องจากมันต้องเกี่ยวข้องกับคนและยากที่จะทำได้สำเร็จ ยิ่งแฮคเกอร์มีความชำนาญมากการโจมตีนั้นจะค่อนข้างเฉียบแหลมและได้ผลสูง

การปฏิเสธแหล่งที่มา (Repudiation of Origin)

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

การปฏิเสธการได้รับ (Repudiation of Receipt)

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

การหน่วงเวลา (Delay)

การหน่วงเวลา หมายถึง การยับยั้งไม่ให้ข้อมูลส่งถึงตามเวลาที่ควรจะเป็น การส่งข้อความหรือข้อมูลนั้นต้องใช้เวลาในการส่ง สมมติว่าโดยปกติข้อความนั้นจะส่งถึงปลายทางภายในเวลา t แต่ถ้าผู้บุกรุกสามารถหน่วงเวลาให้ข้อมูลส่งถึงปลายทางมากกว่าเวลา t แล้ว แสดงว่าการโจมตีแบบหน่วงเวลาเป็นผลสำเร็จ ซึ่งการโจมตีแบบนี้ผู้บุกรุก

ต้องสามารถควบคุมระบบบางส่วนได้ เช่น เซิร์ฟเวอร์หรือเครือข่าย ยกตัวอย่างเช่น สมมติว่าผู้ใช้ต้องการที่จะแอ็กเซสเซิร์ฟเวอร์ โดยมีเซิร์ฟเวอร์ที่ให้บริการอยู่สองเซิร์ฟเวอร์ คือเซิร์ฟเวอร์หลัก (Primary Server) และเซิร์ฟเวอร์สำรอง (Secondary Server) โดยเมื่อเซิร์ฟเวอร์หลักไม่สามารถให้บริการได้เซิร์ฟเวอร์สำรองก็จะทำหน้าที่แทนทันที สมมติว่าผู้บุกรุกสามารถเจาะเข้าระบบ และสามารถควบคุมเซิร์ฟเวอร์สำรองได้ เมื่อผู้ใช้พยายามที่จะล็อกอินเข้าเซิร์ฟเวอร์หลัก ผู้บุกรุกก็พยายามหน่วงเวลาไว้จนทำให้ผู้ใช้เข้าใจว่าเซิร์ฟเวอร์หลักไม่สามารถให้บริการในขณะนั้นได้ จะเปลี่ยนไปล็อกอินเข้าเซิร์ฟเวอร์สำรอง ซึ่งผู้บุกรุกได้ควบคุมไว้ ดังนั้น การโจมตีแบบหน่วงเวลาก็เป็นผลสำเร็จ การรักษาความพร้อมใช้งานจะเป็นวิธีที่ใช้ป้องกันการโจมตีแบบนี้

ไวรัส เวิร์ม และโทรจันฮอร์ส

มัลแวร์ (Malware) หรือบางทีก็เรียกว่า มัลลิเชียสโค้ด (Malicious Code) เป็นโปรแกรมประสงค์ร้ายที่ออกแบบเพื่อเจาะเข้าทำลายหรือเพื่อสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ โปรแกรมประสงค์ร้ายที่เป็นที่คุ้นเคยกันดี เช่น ไวรัส เวิร์ม โทรจันฮอร์ส ลอจิกบอมบ์ และแบ็คดอร์ เป็นต้น

ไวรัส (Virus) หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยจะแพร่กระจายไปยังไฟล์อื่นๆ ที่อยู่ในเครื่องเดียวกัน ไวรัสสามารถทำลายเครื่องได้ตั้งแต่ลบไฟล์ทั้งหมดที่อยู่ในฮาร์ดดิสก์ ไปจนถึงแค่เป็นโปรแกรมที่สร้างความรำคาญให้กับผู้ใช้ในเครือข่าย เช่น แค่เปิดวินโดวส์แล้วเปิดป็อบอัพเพื่อแสดงข้อความบางอย่าง โดยธรรมชาติแล้วไวรัสไม่สามารถที่จะแพร่กระจายไปยังเครื่องอื่นๆ ได้ด้วยตัวเอง แต่การแพร่กระจายไปยังเครื่องอื่นต้องอาศัยโปรแกรมอื่นหรือมนุษย์ เช่น การแชร์ไฟล์โดยใช้แผ่นดิสก์ เป็นต้น และไวรัสนั้นไม่สามารถรันด้วยตัวเองได้ ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัสและค่อยทำงาน

เวิร์ม (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่ในเครือข่าย เวิร์มจะใช้ประโยชน์จากแอพพลิเคชันที่รับ/ส่งไฟล์โดยอัตโนมัติ และไม่ต้องอาศัยคนเพื่อเปิดไฟล์ใดๆ เพราะเวิร์มมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ เวิร์มนั้นบางทีอาจอาศัยอีเมลในการแพร่กระจายตัวเองเหมือนไวรัส โดยแนบไฟล์ไปกับอีเมล เมื่อผู้รับเปิดจดหมายอ่านเวิร์มก็จะเริ่มทำงานทันที

โทรจันฮอร์ส (Trojan Horse) เป็นคำที่มาจากสงครามโทรจันระหว่างทรอย (Troy) และกรีก (Greek) ซึ่งเปรียบถึงม้าโครงไม้ขนาดใหญ่ที่ชาวกรีกสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างในแล้วทำทีถอนทัพกลับ พอชาวทรอยออกมาดูเห็นม้าโครงไม้ทิ้งไว้ก็คิดว่าเป็นของขวัญที่ทหารกรีกทิ้งไว้ให้จึงนำกลับเข้าเมืองไปด้วย พอตกดึกทหารกรีกที่ซ่อนอยู่ในม้าโครงไม้นี้ก็ออกมาและเปิดประตูให้กับทหารกรีกเข้าไปทำลายเมืองทรอยได้สำเร็จ สำหรับในความหมายทางคอมพิวเตอร์แล้วโทรจันฮอร์ส หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม, สกรีนเซฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่างๆ เหล่านี้มา แต่เมื่อติดตั้งแล้วรันโปรแกรมโทรจันฮอร์สที่แฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ เช่น ลบไฟล์ ต่างๆ หรืออาจสร้างแบ็คดอร์ให้กับโปรแกรมอื่นเข้ามาทำลายระบบก็ได้

จากคำจำกัดความข้างต้น โทรจันฮอร์ส เวิร์ม และไวรัสจะมีความหมายคล้ายๆ กัน ซึ่งโปรแกรมบางตัวก็มีคุณสมบัติของทั้งสามประเภทได้ และบางคนอาจใช้คำทั้งสามนี้แทนกันก็ได้ แต่จริงๆ แล้วทั้งสามคำมีความหมายต่างกัน อย่างไรก็ตามจุดมุ่งหมายของโปรแกรมทั้ง 3 ประเภทก็เพื่อมุ่งทำลายระบบคอมพิวเตอร์เพื่อให้ใช้การไม่ได้

วิศวกรรมสังคม (Social Engineering)

การโจมตีแบบวิศวกรรมสังคม (Social Engineering) คือ ปฏิบัติการจิตวิทยาซึ่งเป็นวิธีที่ง่ายที่สุดในการโจมตี เนื่องจากไม่จำเป็นต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์มากนัก และส่วนใหญ่จะใช้ได้ผลดี การโจมตีแบบ

วิศวกรรมสังคมจะเกี่ยวกับการหลอกให้บางคนหลงกลเพื่อเข้าถึงระบบ เช่น การหลอกถามรหัสผ่าน การหลอกให้ส่งข้อมูลที่สำคัญให้ ซึ่งการโจมตีประเภทนี้ไม่จำเป็นต้องใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์หรือการเจาะระบบเลย วิศวกรรมสังคมเป็นสิ่งจุดอ่อนที่ป้องกันยากเพราะเกี่ยวข้องกับคน

การโจมตีแบบวิศวกรรมสังคมโดยส่วนใหญ่จะใช้โทรศัพท์ถามข้อมูล โดยหลอกว่าตนเป็นผู้ได้รับอนุญาตหรือเป็นผู้มีอำนาจ อีกวิธีหนึ่งก็โดยการค้นหาข้อมูลจากถังขยะ (Dumpster Diving) เพื่อค้นหาข้อมูลจากเอกสารที่ทิ้ง ซึ่งในนั้นอาจมีคู่มือการใช้งาน รหัสผ่านที่เขียนไว้ในเศษกระดาษ เป็นต้น อีกวิธีหนึ่งคือ ฟิชชิง (Phishing) ซึ่งทำโดยการส่งอีเมลเพื่อหลอกให้ส่งข้อมูลให้โดยหลอกว่ามาจากผู้ที่ได้รับอนุญาต ยกตัวอย่างเช่น ผู้โจมตีอาจส่งอีเมลและบอกว่ามาจากองค์กรที่ถูกกฎหมายแล้วหลอกให้คลิกเข้าไปยังเว็บไซต์ แทนที่จะไปเว็บไซต์จริงๆ แต่กลับเป็นเว็บไซต์หลอกที่มีหน้าตาเหมือนเว็บไซต์จริง ผู้ใช้จะถูกถามให้กรอกยูสเซอร์เนมและพาสเวิร์ดเพื่อยืนยันเจ้าของบัญชีธนาคาร หรือข้อมูลเกี่ยวกับบัตรเครดิต ซึ่งผู้โจมตีก็จะได้ข้อมูลนั้นไป

การป้องกันวิศวกรรมสังคมสามารถทำได้สองทาง วิธีแรกก็โดยการทำให้องค์กรมีขั้นตอนการปฏิบัติที่เข้มงวดหรือนโยบายที่เข้มงวดเกี่ยวกับการบอกรหัสผ่านให้คนอื่นทราบ ส่วนอีกวิธีหนึ่งก็โดยการจัดให้มีการอบรมพนักงานเกี่ยวกับนโยบาย และการบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัย

ฟิชชิง (Phishing)

ฟิชชิง (Phishing) คือ การโจมตีแบบวิศวกรรมสังคมประเภทหนึ่งที่ใช้การปลอมแปลงอีเมลหรือเว็บไซต์รูปแบบหนึ่ง โดยส่วนใหญ่จะมีวัตถุประสงค์เพื่อต้องการข้อมูลที่สำคัญจากผู้ถูกหลอก เช่น Username, Password และหมายเลขบัตรเครดิต เป็นต้น โดยฟิชชิงส่วนมากจะเสแสร้งว่ามาจากบริษัทที่มีความน่าเชื่อถือ หรือว่ามาจากบริษัทที่เหยื่อเป็นสมาชิกอยู่ เช่น eBay.com, PayPal.com และเว็บไซต์ธนาคารต่างๆ เป็นต้น ฟิชชิงนั้นมีการค้นพบครั้งแรกในปี ค.ศ. 1987 และในปี 1996 จึงมีการตั้งชื่อให้ว่า ฟิชชิง (phishing) โดยแผลงมาจากคำว่า Fishing ซึ่งมีการใช้ Ph แทน F ซึ่งก็เหมือนกับการตกปลาโดยต้องมีการใส่เหยื่อลงไป และรอให้คนมาติดเบ็ดเองซึ่งเป็นการกระทำที่ไม่ยากเย็นอะไรเลย

กรรมวิธีที่ใช้ในการทำฟิชชิงจะมีการส่งข้อมูลข่าวสารไปหาเหยื่อ โดยมีข้อความประมาณว่าเซิร์ฟเวอร์ของทางบริษัทได้รับความเสียหายข้อมูลต่างๆ ของลูกค้าสูญหายทั้งหมด จึงต้องการให้ผู้ใช้บริการกรอกข้อมูลใหม่ให้แก่ทางบริษัท โดยช่องทางที่ใช้ในการส่งข้อมูลข่าวสารก็มักจะใช้อีเมล ภายในอีเมลจะมีลิงค์ไปหาเว็บไซต์ให้กรอกข้อมูลโดยเว็บนั้นจะคล้ายกับเว็บไซต์ของจริงทุกประการอย่างแยกกันไม่ออก ซึ่งอาจมีการจดโดเมนให้เหมือนกับทางเว็บนั้นโดยคาดการณ์ว่าจะต้องมีการพิมพ์ผิดอย่างแน่นอน เช่น www.onlinebanking.com ก็จะจดเป็น www.onlinebanling.com เป็นต้น หลังจากนั้นถ้าเรากรอกข้อมูลลงไปข้อมูลต่างๆ นั้นจะถูกส่งไปหาผู้ประสงค์ร้ายได้อย่างง่ายดาย

การเดารหัสผ่าน (Password Guessing)

รหัสผ่าน (Password) คือ กลุ่มตัวอักษรและเลขที่ใช้สำหรับการพิสูจน์ทราบตัวจริงของผู้ใช้ และเป็นความลับที่เฉพาะเจ้าของเท่านั้นที่ควรทราบ รหัสผ่านจะใช้คู่กับชื่อผู้ใช้หรือยูสเซอร์เนม (Username) สำหรับล็อกอินเข้าสู่ระบบ ซึ่งโดยส่วนใหญ่จะมีฟอร์มรับข้อมูล ยูสเซอร์เนมจะมีความเฉพาะไม่ซ้ำกันในระบบใดระบบหนึ่ง เช่น Administrator, Jatuchai, webmaster เป็นต้น ยูสเซอร์เนมนั้นเป็นส่วนที่เปิดเผยได้แต่รหัสผ่านนั้นต้องเฉพาะเจ้าของเท่านั้นที่ทราบ

ถึงแม้ว่ารหัสผ่านจะเป็นกลไกการรักษาความปลอดภัยแรก แต่บางครั้งก็เป็นขั้นตอนเดียวที่ใช้ป้องกันระบบ รหัสผ่านนั้นอาจถือได้ว่าเป็นจุดอ่อน เพราะผู้ใช้ในปัจจุบันโดยส่วนใหญ่จะมียูสเซอร์เนมและรหัสผ่านประมาณ 10 คู่ที่ต้องใช้สำหรับล็อกอินเข้าสู่ระบบต่างๆ เช่น คอมพิวเตอร์ที่ทำงาน ที่บ้าน อีเมล บัญชีธนาคาร และบัญชีที่สมัครใช้

งานร้านค้าบนอินเทอร์เน็ต ดังนั้น จึงเป็นการยากที่คนๆ หนึ่งจะสามารถจดจำรหัสผ่านได้มากมาย นอกจากนี้รหัสผ่านของบางระบบก็มีอายุการใช้งาน เช่น 30 วัน หลังจากหมดอายุแล้วก็จะใช้การไม่ได้ ต้องสร้างหรือกำหนดรหัสผ่านใหม่ ซึ่งยิ่งทำให้ยากที่จะจำรหัสผ่านปัจจุบันได้ นอกจากนี้บางระบบคอมพิวเตอร์มีระบบป้องกันไม่ให้ใช้รหัสผ่านเก่าที่เคยใช้แล้วกลับมาใช้อีก ด้วยเหตุผลเหล่านี้ทำให้ผู้ใช้หลายคนเลือกที่จะมีรหัสผ่านที่ง่ายต่อการจำ ซึ่งทำให้เป็นจุดอ่อนของระบบการรักษาความปลอดภัย รหัสผ่านที่ถือว่าง่ายต่อการเดานั้นมีคุณสมบัติ คือ

- รหัสผ่านที่สั้น เช่น xyz, abc เป็นต้น
- คำที่รู้จักและคุ้นเคย เช่น password, blue, admin เป็นต้น
- มีข้อมูลส่วนตัวในรหัสผ่าน เช่น ชื่อ หมายเลขโทรศัพท์ วันเกิด เป็นต้น
- ใช้รหัสผ่านเดียวกันกับทุกๆ ระบบที่ใช้
- เขียนรหัสผ่านไว้บนแผ่นกระดาษแล้วเก็บไว้ในที่ๆ หาได้ง่าย
- ไม่เปลี่ยนรหัสผ่านเป็นประจำถ้าไม่ถูกบังคับ

ผู้โจมตีนั้นจะใช้ประโยชน์จากจุดอ่อนนี้โดยใช้เทคนิคการเดารหัสผ่าน (Password Guessing)

การถอดรหัสข้อมูล (Cryptanalysis)

การเข้ารหัสข้อมูล หรือ Cryptography เป็นคำที่มีรากศัพท์มาจากภาษากรีกสองคำคือ Crypto ซึ่งหมายความว่า ซ่อน และคำว่า graph หมายถึง การเขียน ซึ่งหมายถึงศาสตร์ในการแปลงข้อมูลเพื่อให้ปลอดภัยเมื่อมีการสื่อสาร หรือจัดเก็บไว้ที่ใดที่หนึ่ง การเข้ารหัสไม่ใช่ความพยายามที่จะปกปิดความมีอยู่ของข้อมูล (Steganography) แต่เป็นการย่อยละเอียดแล้วคนเพื่อให้ข้อมูลนั้นไม่สามารถดูได้โดยผู้ที่ไม่ได้รับอนุญาต

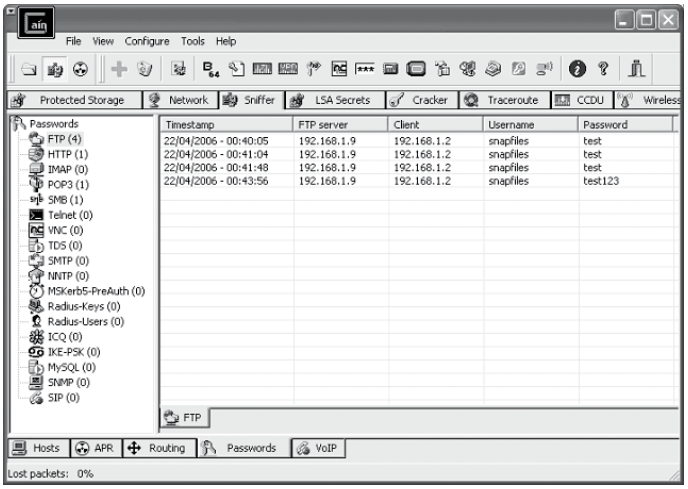
การเข้ารหัสเริ่มใช้เมื่อหลายศตวรรษก่อน ผู้ที่ได้รับยกย่องว่ามีชื่อเสียงในการเข้ารหัสข้อมูลในสมัยโบราณคนหนึ่งคือ จูเลียสซีซาร์ เมื่อเขาต้องส่งข้อมูลไปให้บรรดานายพลผู้ควบคุมกองทัพต่างๆ ซีซาร์จะเลื่อนแต่ละอักษรไปสามตำแหน่งตามลำดับตัวอักษร เช่น ตัวอักษร A ก็จะถูกแทนที่ด้วยอักษร D และอักษร B ก็จะถูกแทนที่ด้วยอักษร E เป็นต้น ซึ่งการเปลี่ยนข้อมูลเดิมให้เป็นข้อมูลที่อ่านไม่ได้เรียกว่า การเข้ารหัส (Encryption) เมื่อนายพลต่างๆ ของซีซาร์ได้รับข้อความก็ทำในขั้นตอนตรงกันข้าม เช่น แทนที่อักษร D ด้วยอักษร A เพื่อแปลงข้อมูลให้กลับไปเป็นข้อมูลดังเดิม ซึ่งขบวนการนี้เรียกว่า การถอดรหัส (Decryption)

ความสำเร็จหรือความปลอดภัยของการเข้ารหัสข้อมูลนั้นขึ้นอยู่กับขบวนการที่ใช้สำหรับการเข้าและถอดรหัสข้อความ ขบวนการนี้ขึ้นอยู่กับขั้นตอนที่เรียกว่า อัลกอริทึม (Algorithm) โดยอัลกอริทึมจะใช้ค่าที่เรียกว่า คีย์ (Key) ที่ต้องใช้ในการเข้าและถอดรหัส ยกตัวอย่างเช่น เมื่อซีซาร์ได้รับคำแนะนำให้ใช้การเลื่อนตำแหน่งอักษรในการเข้ารหัส ซึ่งซีซาร์เลือกที่จะเลื่อนตำแหน่งไป 3 ตำแหน่ง ดังนั้น ตัวเลข 3 ถือว่าเป็นคีย์ในการเข้าและถอดรหัส อย่างไรก็ตามการเข้ารหัสด้วยการแทนที่ตัวอักษรคล้ายของซีซาร์นั้นถือว่าเป็นวิธีที่ง่ายเกินไปในปัจจุบัน ผู้โจมตีอาจตรวจสอบข้อมูลที่เข้ารหัสแล้วและสามารถวิเคราะห์หาคีย์ได้ไม่ยาก และก็สามารถถอดรหัสทั้งข้อความได้โดยง่าย ดังนั้น อัลกอริทึมในการเข้ารหัสข้อมูลในปัจจุบันนั้นจะมีความซับซ้อนมากกว่า และก็ขั้นตอนหรืออัลกอริทึมในการเข้ารหัสข้อมูลนั้นจะเป็นที่รู้จักกันดีโดยทั่วไป แต่สิ่งที่ปกปิดให้เป็นความลับของการเข้ารหัสคือ คีย์ ความยาวของคีย์นั้นจะเป็นสิ่งที่บอกถึงความแข็งแกร่งของการเข้ารหัส ยิ่งคีย์มีความยาวมากยิ่งทำให้ขบวนการในการค้นหาคีย์ยากมากขึ้น แต่ในทางตรงกันข้ามยิ่งคีย์มีความยาวมาก ก็ยิ่งใช้เวลานานขึ้นในการเข้าและถอดรหัสข้อมูล

สำหรับคีย์ที่สร้างรูปแบบข้อมูลที่เหมือนกันหลายๆ ครั้งจนทำให้สามารถวิเคราะห์ได้ว่า ถ้าข้อมูลมีรูปแบบนี้แสดงว่าใช้คีย์นี้แน่นอน คีย์ประเภทนี้จะเรียกว่า คีย์อ่อน (Weak key) ทุกๆ อัลกอริทึมจะมีกลุ่มของคีย์ที่มีลักษณะเช่นนี้

แต่ไม่ได้หมายความว่าอัลกอริทึมเหล่านี้จะใช้ไม่ได้ วิธีที่ดีที่สุดในการป้องกันก็คือการระวังที่ไม่ให้ใช้คีย์อ่อน โดยทั่วไปคีย์ที่มีความยาวอย่างน้อย 128 บิตนั้นจะถือว่าปลอดภัยเพียงพอในการเข้ารหัสข้อมูล

การโจมตีการเข้ารหัส (Cryptanalysis) เป็นขบวนการที่จะให้ได้มาซึ่งคีย์ในการเข้ารหัสข้อมูล ซึ่งมีหลากหลายวิธี วิธีหนึ่งคือการใช้ขบวนการทางคณิตศาสตร์ (Mathematical Attack) ซึ่งเกิดจาการใช้การวิเคราะห์ทางสถิติของตัวอักษรที่พบในข้อความที่เข้ารหัสแล้ว แล้วใช้วิธีทางสถิติเพื่อวิเคราะห์หาคีย์ที่ใช้เข้ารหัสแล้วก็ถอดรหัสข้อมูล การป้องกันการโจมตีทางคณิตศาสตร์นี้ป้องกันได้โดยการไม่ส่งข้อมูลเหมือนกันหลายครั้ง ถ้าผู้โจมตีรู้ข้อมูลดังเดิม การส่งข้อมูลเดียวกันก็อาจทำให้วิเคราะห์หาคีย์ได้ง่าย ข้างล่างเป็นโปรแกรม Cain & Abel เป็นโปรแกรมพาสเวิร์ดแคร็คเกอร์ซึ่งใช้สำหรับถอดรหัสผ่าน



รูปที่ 1.6 : Cain & Abel Password Cracker

การโจมตีวันเกิด (Birthday Attacks)

เมื่อเราเจอใครครั้งแรกก็มีโอกาส 1 ใน 365 (0.27%) ที่จะมีวันเกิดเดียวกัน อย่างไรก็ตามถ้าเราเจอคนมากขึ้นโอกาสที่จะมีคนที่มีวันเกิดเหมือนกันนั้นจะเพิ่มขึ้นอย่างมาก โดยเมื่อเจอคน 23 คน เราจะมีโอกาส 50% ที่จะมีคนที่มีวันเกิดเหมือนกัน แทนที่จะเป็น 6.3% (23 ใน 365) ถ้ามีคน 60 คน โอกาสที่จะมีวันเกิดตรงกันนั้นมีมากกว่า 99% ปรากฏการณ์นี้เรียกว่า Birthday Paradox

ในการเข้ารหัสข้อมูลปรากฏการณ์วันเกิดนั้นมีนัยสำคัญอย่างมาก เมื่อเราเข้ารหัสข้อมูลเราอาจจะคิดว่าวิธีที่ดีที่สุดในการเลือกคีย์ที่แตกต่างคือการเลือกใช้คีย์แบบสุ่มเลือก อย่างไรก็ตามถ้าเราเลือกคีย์แบบสุ่มเลือก โอกาสที่จะได้คีย์เหมือนกันนั้นมีมากกว่าที่เราคาดเหมือนกับปรากฏการณ์

การโจมตีแบบคนกลาง (Man-in-the-Middle Attacks)

อีกรูปแบบหนึ่งของการโจมตีคือ การพยายามที่จะใช้บัญชีผู้ใช้ที่ถูกต้องในการล็อกอินเข้าไปในระบบ ซึ่งการให้ได้มาซึ่งข้อมูลเหล่านี้ก็โดยการใช้การโจมตีแบบคนกลาง (Man-in-the-middle) กล่าวคือ สมมติว่าอลิสเป็นนักเรียนชั้นประถมซึ่งสอบได้คะแนนไม่ดี ครูประจำชั้นก็เลยส่งจดหมายไปให้พ่อแม่ของอลิสให้มาพบครู อลิสทราบดีและคอยดูว่ามีจดหมายส่งมาถึงพ่อแม่ตัวเอง แล้วเปลี่ยนข้อความในจดหมายบอกถึงความชื่นชมในตัวอลิสที่ทำคะแนนได้ดีในวิชาคณิตศาสตร์ แล้วเธอก็เขียนจดหมายปลอมว่ามาจากพ่อแม่ของตัวเองว่าไม่สามารถเข้ามาร่วมประชุมได้ เมื่อพ่อแม่ได้อ่านจดหมายแล้วก็รู้สึกภาคภูมิในตัวลูก ในขณะที่ครูก็สงสัยว่าทำไมพ่อแม่ของอลิสไม่ยอมมาพบ อลิสใช้วิธีการโจมตีแบบคนกลางกับการสื่อสารระหว่างครูกับพ่อแม่ของตัวเอง

การโจมตีแบบคนกลางของการสื่อสารผ่านระบบคอมพิวเตอร์เป็นรูปแบบที่พบเห็นได้ทั่วไป การโจมตีประเภทนี้จะทำให้คอมพิวเตอร์สองเครื่องดูเหมือนว่าจะสื่อสารกันอยู่โดยที่ไม่รู้ว่ามีคนกลางคอยเปลี่ยนแปลงข้อมูลอยู่ การป้องกันการโจมตีแบบคนกลางก็อาจใช้วิธีการเข้ารหัสข้อมูลควบคู่กับการพิสูจน์ทราบตัวจริงของคู่รับคู่ส่ง การโจมตีแบบคนกลางแบ่งออกเป็นสองประเภทคือ แบบแอ็คทีฟ (Active) และแบบพาสซีฟ (Passive) สำหรับแบบแอ็คทีฟนั้นข้อความที่ส่งถึงคนกลางจะถูกเปลี่ยนแปลงแล้วค่อยส่งต่อถึงผู้รับ ส่วนแบบพาสซีฟนั้นจะส่งต่อข้อความเดิมที่ได้รับ

การโจมตีอีกแบบหนึ่งซึ่งคล้ายกับการโจมตีแบบคนกลางคือ การโจมตีแบบรีเพลย์ (Replay Attack) โดยข้อความที่ได้รับจากคนส่งจะถูกจัดเก็บไว้แล้วจะส่งต่อไปอีกครั้งหนึ่งเมื่อเวลาผ่านไประยะหนึ่ง

เครื่องมือสำหรับการรักษาความปลอดภัย

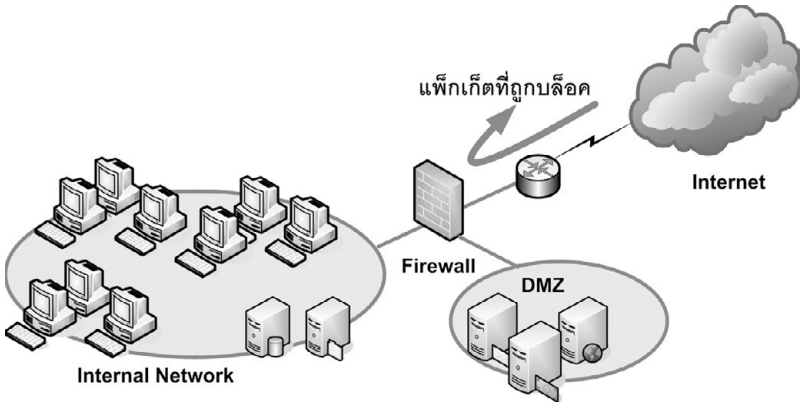
ถึงแม้ว่าการปกป้องข้อมูลเป็นสิ่งที่มีลำดับความสำคัญสูงสุด แต่การดูแลรักษาระบบหรือเครือข่ายให้ทำงานอย่างถูกต้องก็เป็นปัจจัยที่สำคัญในการปกป้องข้อมูลที่อยู่ในเครือข่ายนั้น ถ้ามีช่องโหว่ของระบบเครือข่ายที่อนุญาตให้โจมตีได้ ความเสียหายที่เกิดขึ้นอาจมากกว่าที่คาดไว้ และอาจใช้ทั้งเวลาและความพยายามอย่างมากที่จะทำให้ระบบกลับมาทำงานได้เหมือนเดิม

เนื่องจากภัยอันตรายนั้นมีรอบด้าน เราไม่สามารถที่จะใช้แค่เครื่องมือประเภทใดประเภทหนึ่งเพื่อสำหรับการรักษาความปลอดภัยให้กับข้อมูลขององค์กรได้ เช่นกันเราก็ไม่สามารถใช้เครื่องมือการรักษาความปลอดภัยเพียงประเภทเดียวเพื่อสำหรับป้องกันระบบคอมพิวเตอร์และเครือข่ายทั้งองค์กรได้ เราจำเป็นที่ต้องใช้ผลิตภัณฑ์หลายประเภทจากหลากหลายบริษัททำงานร่วมกันอย่างเป็นระบบเพื่อป้องกันและรักษาความปลอดภัย ต่อไปนี้เป็นตัวอย่างประเภทของเครื่องมือที่ใช้สำหรับระบบการรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่าย

ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) เป็นระบบควบคุมการเข้าออกเครือข่าย ซึ่งจะใช้สำหรับปกป้องเครือข่ายภายในขององค์กรจากการโจมตีจากภายนอกได้ โดยปกติแล้วไฟร์วอลล์จะติดตั้งขวางกั้นระหว่างสองเครือข่ายซึ่งส่วนใหญ่เป็นการติดตั้งระหว่างอินเทอร์เน็ตและอินทราเน็ต ถ้าไฟร์วอลล์ถูกคอนฟิกอย่างถูกต้องแล้วก็เป็นสิ่งที่จำเป็นสำหรับองค์กร อย่างไรก็ตามไฟร์วอลล์ไม่สามารถที่จะป้องกันการโจมตีที่ใช้ช่องทางปกติที่เปิดไว้โดยไฟร์วอลล์ได้ ยกตัวอย่างเช่น สมมติว่าองค์กรมีเว็บเซิร์ฟเวอร์ติดตั้งไว้ใน DMZ (DeMilitarized Zone) หรือภายในเครือข่ายและอนุญาตให้เข้าถึงได้จากอินเทอร์เน็ต และถ้าเว็บเซิร์ฟเวอร์มีช่องโหว่และจุดอ่อน ไฟร์วอลล์ก็จะไม่สามารถป้องกันการโจมตีเว็บเซิร์ฟเวอร์ได้ถ้าผู้บุกรุกใช้ช่องทางเดียวกันกับการเข้ามาดูเว็บไซต์ นอกจากนี้ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีจากภายในได้เนื่องจากผู้ใช้ที่อยู่ภายในนั้นถ้าโจมตีคอมพิวเตอร์ที่อยู่ข้างในด้วยกันก็จะไม่ต้องผ่านไฟร์วอลล์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้เต็มที่และสามารถใช้บริการเครือข่ายภายนอก เช่น อินเทอร์เน็ตได้ด้วย ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างในได้ รูปที่ 1.7 แสดงการติดตั้งไฟร์วอลล์เพื่อเชื่อมต่อเครือข่ายองค์กรกับเครือข่ายอินเทอร์เน็ต จากรูปจะเห็นได้ว่าแพ็กเก็ตที่วิ่งระหว่างเครือข่ายภายในและอินเทอร์เน็ตต้องผ่านไฟร์วอลล์เท่านั้น ดังนั้นไฟร์วอลล์จึงสามารถควบคุมการใช้เครือข่ายได้โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ไฟร์วอลล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่สองกลไกคือ การอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่าน



รูปที่ 1.7 : ไฟร์วอลล์ (Firewall)

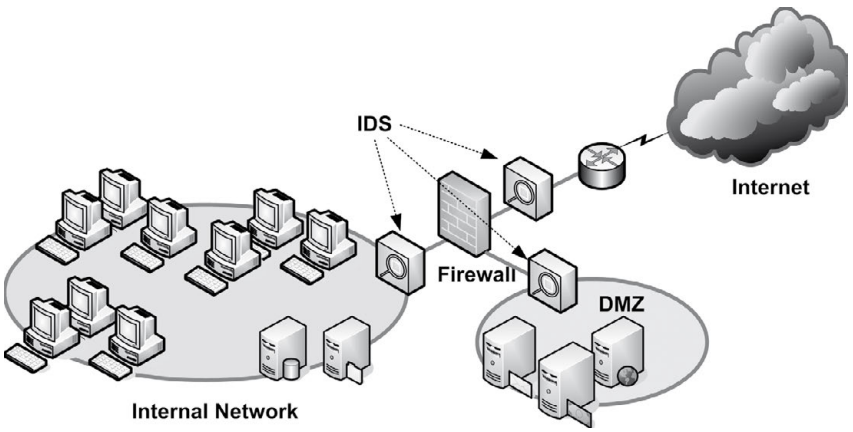
ถ้าเครือข่ายองค์กรเชื่อมต่อโดยตรงกับอินเทอร์เน็ตโดยที่ไม่มีไฟร์วอลล์ก็เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย ตัวอย่างเช่น สมมติว่าเครือข่ายมีโฮสต์หรือเซิร์ฟเวอร์เป็นร้อยๆ เครื่อง ถ้าผู้บุกรุกเครือข่ายสามารถบุกรุกเข้าเครื่องใดเครื่องหนึ่งได้ ก็ไม่เป็นการยากที่จะบุกรุกเข้าไปยังเครื่องอื่นๆ ในเครือข่าย ดังนั้น การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

ระบบตรวจจับการบุกรุก (IDS)

ระบบตรวจจับการบุกรุกหรือ IDS (Intrusion Detection System) เป็นระบบที่ใช้สำหรับการเฝ้าระวังและแจ้งเตือนภัย ถ้ามีการบุกรุกหรือมีสิ่งที่ผิดปกติเกิดขึ้นในระบบ บางระบบนั้นสามารถตรวจจับและหยุดการบุกรุกได้ อย่างไรก็ตามปัญหาของการโจมตีเครือข่ายนั้นก็คล้ายกับไวรัส เนื่องจากการโจมตีนั้นผู้บุกรุกจะพยายามโจมตีช่องโหว่หรือจุดอ่อนของระบบ และเนื่องจากมีการค้นพบช่องโหว่หรือจุดอ่อนใหม่ๆ เป็นประจำ ดังนั้น IDS ก็จำเป็นที่ต้องอัพเดตข้อมูลนี้เช่นกัน ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง IDS ก็สามารถป้องกันการโจมตีได้ อย่างไรก็ตาม IDS ไม่สามารถตรวจจับความพยามยามของผู้ใช้ที่ได้รับอนุญาตเข้าถึงไฟล์หรือใช้โปรแกรมที่ไม่ได้รับอนุญาตได้

ระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น ถ้าเปรียบกับระบบการรักษาความปลอดภัยของรถ IDS ก็อาจจะเปรียบได้กับระบบกันขโมย ซึ่งระบบนี้จะส่งสัญญาณเมื่อมีการตรวจพบความพยายามที่จะขโมยรถ เช่น การงัดประตูหรือกระจก แต่ระบบนี้จะไม่สามารถป้องกันไม่ให้ขโมยรถได้ อย่างไรก็ตามโดยธรรมชาติแล้วขโมยก็จะพยายามหลีกเลี่ยงรถที่ติดตั้งระบบนี้ ระบบเครือข่ายก็เช่นกัน ถ้ามีระบบตรวจจับและแจ้งเตือนการบุกรุก พวกแฮคเกอร์ก็จะหลีกเลี่ยงการบุกรุกเครือข่ายนี้

หน้าที่หลักของ IDS คือ แจ้งเตือนการเข้าใช้เครือข่ายที่ผิดปกติ สิ่งที่เป็นประเด็นสำคัญในการออกแบบระบบ IDS ก็คือ เหตุการณ์ใดคือสิ่งที่ถือว่าผิดปกติ ดังนั้น การใช้ IDS นั้นก็ขึ้นอยู่กับว่าอะไรที่จะแจ้งเตือนให้ทราบ คำตอบนั้นไม่ใช่แค่ถูกหรือผิด หรือขาวหรือดำ แต่จะขึ้นอยู่กับสภาวะของระบบในขณะนั้น



รูปที่ 1.8 : Intrusion Detection System **ระบบตรวจจับการบุกรุก**

จากรูปด้านบนโฮสต์เบสไอดีเอส (Host-based IDS) จะติดตั้งที่เครื่องเว็บเซิร์ฟเวอร์เพื่อตรวจจับความพยายามที่จะแฮคเว็บเซิร์ฟเวอร์เอง ส่วนเน็ตเวิร์คไอดีเอส (Network-based IDS) นั้นจากรูปจะติดตั้งระหว่างเราท์เตอร์และไฟร์วอลล์ เพื่อที่จะตรวจทราฟฟิกที่วิ่งเข้าออกระหว่างเครือข่ายและอินเทอร์เน็ต

การเข้ารหัสข้อมูล (Encryption)

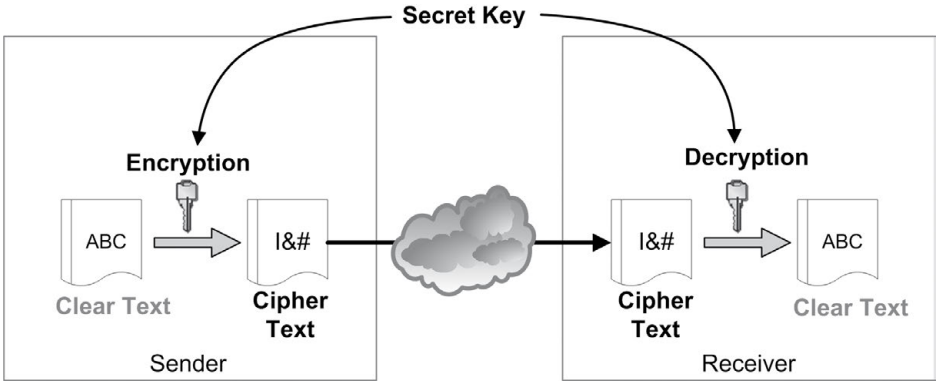
การเข้ารหัสข้อมูลหรือเอ็นคริปชัน (Encryption) เป็นกลไกหลักสำหรับป้องกันข้อมูลที่อยู่ระหว่างการสื่อสาร ถ้ามีการเข้ารหัสที่ดีข้อมูลก็จะถูกป้องกันไม่ให้สามารถอ่านได้จากผู้ที่ไม่ประสงค์ดี อย่างไรก็ตามผู้ใช้ที่ส่งและรับจะต้องสามารถเข้าและถอดรหัสข้อมูลนี้ได้ ระบบการเข้าและถอดรหัสไม่สามารถจะแยกแยะได้ระหว่างผู้ใช้ที่ได้รับอนุญาตหรือผู้บุกรุกถ้าผู้นั้นมีคีย์สำหรับการถอดรหัสข้อมูล ดังนั้น การเข้ารหัสข้อมูลอย่างเดียวไม่สามารถปกป้องข้อมูลได้ ถ้าจะให้การเข้ารหัสข้อมูลได้ผลต้องมีระบบที่ป้องกันการขโมยคีย์ที่ใช้ถอดรหัส และต้องมีการป้องกันระบบโดยส่วนรวมด้วย

โดยทั่วไปแล้วข้อมูลที่รับ/ส่งผ่านเครือข่ายนั้นจะอยู่ในรูปเคลียร์เท็กซ์ (Clear Text) ซึ่งข้อมูลนี้อาจถูกอ่าน หรือคัดลอกได้โดยใช้เทคนิคที่เรียกว่า สนิฟเฟอริง (Sniffering) เครื่องมือต่างๆ เช่น โปรโตคอลอะนาไลเซอร์ หรือโปรแกรมการดูแลระบบเครือข่ายที่ส่วนใหญ่จะมีมาในระบบปฏิบัติการปัจจุบันนั้น สามารถที่จะใช้ตรวจดูข้อมูลที่รับส่งผ่านเครือข่ายได้ เพื่อป้องกันการขโมยข้อมูลที่รับ/ส่งผ่านเครือข่ายที่ไม่มีความปลอดภัยนี้ ข้อมูลจำเป็นต้องมีการเข้ารหัส การเข้ารหัสข้อมูล (Data Encryption) คือ วิธีที่ใช้สำหรับแปลงเคลียร์เท็กซ์ให้เป็นไซเฟอร์เท็กซ์ (Cipher Text) หรือข้อมูลที่เข้ารหัสแล้ว ซึ่งข้อมูลนี้จะถูกส่งไปให้ผู้รับ เมื่อผู้รับได้รับข้อมูลก็จะถอดรหัสข้อมูล (Decryption) เพื่อให้ได้ข้อมูลเดิม การเข้าและถอดรหัสข้อมูลจะเรียกว่า คริปโตกราฟี (Cryptography) ปัจจุบันการเข้ารหัสข้อมูลจะแบ่งออกเป็น 2 ประเภท คือ

- Symmetric Key Cryptography
- Public Key Cryptography

ส่วนรายละเอียดของแต่ละประเภทจะได้กล่าวในหัวข้อถัดไป

การเข้าและถอดรหัสข้อมูลแบบซีเคร็ทคีย์ (Secret Key) เป็นวิธีที่ทั้งการเข้ารหัสและการถอดรหัสจะใช้คีย์ (Key) หรือรหัสลับเดียวกัน หรือเรียกอีกอย่างหนึ่งว่า การเข้าและถอดรหัสแบบซิมเมตริก (Symmetric) คีย์ที่ใช้จะมีความยาวคงที่ การไหลของข้อมูลเป็นเหมือนแสดงในรูปที่ 1.9 จากรูปดังกล่าวเครื่องส่งนำข้อมูลที่ต้องการส่งคือ "abc" มาเข้ารหัสโดยใช้คีย์ซึ่งผลที่ได้คือ "I&#" แล้วส่งผ่านเครือข่าย เมื่อถึงปลายทางเครื่องรับก็จะถอดรหัสข้อมูลโดยใช้คีย์เดียวกัน ซึ่งข้อมูลก็จะถูกเปลี่ยนกลับมาเป็น "abc" เหมือนเดิม



รูปที่ 1.9 : Secret Key Cryptosystem การเข้ารหัสโดยใช้ Secret Key

การเข้ารหัสแบบซีเคร็ทคีย์เป็นวิธีที่ค่อนข้างเร็ว มีหลายอัลกอริทึมที่ใช้สำหรับการเข้ารหัสข้อมูลประเภทนี้ เช่น RC-4, DES, Triple-DES และ FWZ-1 เป็นต้น ซึ่งอย่างหนึ่งที่แตกต่างกันระหว่างอัลกอริทึมต่างๆ เหล่านี้คือ ความยาวของคีย์ (Key Length) ซึ่งจะหมายถึงความแข็งแกร่งของการเข้ารหัสด้วย เนื่องจากยิ่งความยาวคีย์ยาวมากขึ้นเท่าไรยิ่งทำให้ยากต่อการถอดรหัส

อย่างไรก็ตามการเข้ารหัสข้อมูลแบบซีเคร็ทคีย์นี้มีข้อเสียคือ ส่วนใหญ่อัลกอริทึมที่ใช้เข้าและถอดรหัสนั้นจะถูกตีพิมพ์เพื่อให้สาธารณะทราบหรือเป็นมาตรฐานที่ทุกคนรู้ และเนื่องจากคีย์ที่ใช้เข้าและถอดรหัสเป็นคีย์ตัวเดียวกัน ดังนั้น ใครก็ตามที่ได้คีย์นี้ไปก็สามารถที่จะถอดรหัสข้อมูลได้ ทำให้ระบบทั้งหมดตกอยู่ในอันตราย ดังนั้น การส่งมอบคีย์จะต้องใช้วิธีที่ปลอดภัย เช่น อาจส่งมอบโดยการบอกปากต่อปาก หรือผ่านทางโทรศัพท์ เป็นต้น ถ้ามีโหนดที่ต้องเข้ารหัสน้อย การแจกจ่ายคีย์ก็เป็นเรื่องที่ไม่ยุ่งยากมากนัก แต่ถ้ามีการขยายเครือข่ายซึ่งอาจต้องแจกจ่ายคีย์ให้กับหลายๆ โหนดการจัดการคีย์อาจเป็นเรื่องที่ยุ่งยากและไม่ปลอดภัยก็ได้

ซอฟต์แวร์ป้องกันไวรัส

ปัจจุบันภัยคุกคามที่มีผลกระทบต่อองค์กรมากที่สุดคือ ไวรัส เวิร์ม และโทรจัน ซึ่งได้สร้างความเสียหายอย่างมากให้กับคอมพิวเตอร์และเครือข่ายที่เชื่อมต่อเข้ากับอินเทอร์เน็ต ดังนั้น การป้องกันและจำกัดไวรัสจึงเป็นสิ่งที่สำคัญในลำดับต้นๆ

ซอฟต์แวร์ป้องกันไวรัสเป็นสิ่งที่จำเป็นสำหรับการป้องกันและรักษาความปลอดภัยให้กับคอมพิวเตอร์ ถ้ามีการติดตั้งและใช้งานอย่างถูกต้อง เพราะมันสามารถที่จะลดความเสี่ยงต่อโปรแกรมประสงค์ร้ายได้ อย่างไรก็ตามมันไม่สามารถที่จะป้องกันไวรัสได้ทุกชนิด เนื่องจากปัจจุบันจะมีไวรัสใหม่ๆ ออกมาเรื่อยๆ การใช้งานซอฟต์แวร์ป้องกันไวรัสนั้นจำเป็นที่ต้องอัพเดตฐานไวรัสซิกเนเจอร์ (Virus Signature) เป็นประจำพร้อมทั้งสแกนระบบเป็นประจำเช่นกัน อย่างไรก็ตามโปรแกรมป้องกันไวรัสนั้นไม่สามารถที่จะป้องกันผู้บุกรุกจากที่อื่นเจาะระบบเข้ามาแล้วรันโปรแกรมประสงค์ร้ายได้ นอกจากนี้โปรแกรมป้องกันไวรัสยังไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาตแต่พยายามที่จะเข้าถึงไฟล์หรือโปรแกรมที่ไม่ได้รับอนุญาตได้

ระบบการรักษาความปลอดภัยทางด้ายกายภาพ

ระบบการรักษาความปลอดภัยทางด้านกายภาพนั้น ก็อาจเป็นเครื่องมือหนึ่งที่ช่วยเพิ่มความปลอดภัยให้กับข้อมูลและระบบคอมพิวเตอร์ขององค์กรได้ นอกจากนี้อาจมีราคาถูกก็ได้ เราอาจสร้างตึกที่แข็งแรงหรือห้องใต้ดินที่มิดชิดแล้วนำระบบคอมพิวเตอร์ไปเก็บไว้ในนั้นแล้วล็อกด้วยกุญแจที่แน่นหนา พร้อมทั้งไม่อนุญาตให้ใครเข้าไปข้างในได้ อย่างไรก็ตามวิธีดังกล่าวไม่ใช่การรักษาความปลอดภัยที่ดีหรือเหมาะสม พนักงานบริษัทจำเป็นที่ต้องสามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ได้เพื่อที่องค์กรจะสามารถทำหน้าที่ได้ ดังนั้น ระบบการรักษาความปลอดภัยทางด้านกายภาพจะต้องอนุญาตให้คนสามารถเข้าถึงระบบได้ นอกจากนี้ระบบคอมพิวเตอร์อาจต้องเชื่อมต่อเข้ากับเครือข่ายเพื่อให้การทำงานสะดวกและมีประสิทธิภาพมากที่สุด ถ้าต้องเป็นอย่างนี้ระบบการรักษาความปลอดภัยทางด้ายกายภาพอย่างเดียวไม่สามารถที่จะป้องกันการโจมตีผ่านทางเครือข่ายแทนที่จะเข้ามาทางประตูได้

Smart Cards

การพิสูจน์ตัวตนของผู้ใช้นั้นสามารถทำได้โดยการใช้การตรวจสอบคุณสมบัติ 3 อย่างที่ของผู้ใช้คือ สิ่งที่คุณรู้ (Something you know), สิ่งที่คุณมี (Something you have) และสิ่งที่คุณเป็น (Something you are) ในอดีตที่ผ่านมาการพิสูจน์ตัวตนนั้นจะใช้รหัสผ่าน (Password) ซึ่งจัดอยู่ในประเภทสิ่งที่คุณรู้ แต่ที่ผ่านมาเรารู้ว่าการใช้การพิสูจน์ตัวตนเฉพาะการตรวจสอบสิ่งที่คุณรู้อย่างเดียวนั้นอาจจะไม่ใช่วิธีที่ดีที่สุด เนื่องจากรหัสผ่านนั้นอาจถูกเดาได้ หรืออาจมีการขโมยรหัสผ่านโดยวิธีใดวิธีหนึ่ง เพื่อป้องกันปัญหาเหล่านี้การพิสูจน์ตัวตนนั้นก็ได้เริ่มจะหันมาใช้แบบสิ่งที่คุณมี และสิ่งที่คุณเป็นแทน

สมาร์ทการ์ด (Smart Card) จัดอยู่ในประเภทสิ่งที่คุณมี สามารถใช้สำหรับการพิสูจน์ตัวตนได้ ดังนั้น จึงสามารถป้องกันการเดารหัสผ่านได้ อย่างไรก็ตามถ้าสมาร์ทการ์ดถูกขโมยไป และถ้าสมาร์ทการ์ดเป็นสิ่งเดียวที่ใช้สำหรับการพิสูจน์ตัวตนเพื่อเข้าสู่ระบบ ผู้ที่ได้สมาร์ทการ์ดไปอาจสามารถปลอมตัวเป็นผู้ใช้คนนั้นเองก็ได้ ดังนั้น ระบบจึงไม่สามารถป้องกันการโจมตีจากผู้บุกรุกคนนั้นได้ เนื่องจากระบบนั้นจะไว้วางใจและเชื่อว่าผู้ที่ล็อกอินนั้นเป็นผู้ใช้ที่ได้รับอนุญาตจริงๆ

Biometrics

ไบโอเมตริก (Biometrics) เป็นรูปแบบของการพิสูจน์ตัวตนอีกประเภทหนึ่งซึ่งจัดอยู่ในประเภทสิ่งที่คุณเป็น ดังนั้น การใช้งานจึงสามารถป้องกันการเดารหัสผ่านหรือการขโมยสมาร์ทการ์ดได้ ไบโอเมตริกถือได้ว่าเป็นระบบพิสูจน์ตัวตนแบบที่แข็งแกร่งที่สุด การใช้งานนั้นจะเกิดประสิทธิภาพสูงสุดก็ต่อเมื่อการเข้าถึงระบบนั้นต้องผ่านทางที่กำหนดไว้เท่านั้น ดังนั้น ถ้าผู้บุกรุกสามารถค้นพบวิธีอื่นเพื่อเข้าสู่ระบบได้โดยที่ไม่ต้องผ่านระบบนี้ไบโอเมตริกส์ไม่สามารถป้องกันได้

สรุปท้ายบท

สิ่งที่มีค่ามากที่สุดขององค์กรคือข้อมูล และปัจจุบันข้อมูลส่วนใหญ่จะอยู่ในรูปแบบดิจิตอล และถูกจัดเก็บไว้ที่ใดที่หนึ่งในระบบเครือข่าย บางครั้งข้อมูลเหล่านี้อาจต้องถูกส่งผ่านเครือข่ายไปยังที่ต่างๆ เครือข่ายเป็นสิ่งที่สร้างสำหรับการรับ/ส่งข้อมูลเหล่านี้อย่างมีประสิทธิภาพ อย่างไรก็ตามข้อมูลเหล่านี้อาจถูกลักลอบนำไปใช้ในทางที่ผิดหรืออาจทำให้ใช้การไม่ได้จากผู้ที่ไม่หวังดีก็ได้ ดังนั้น การรักษาความปลอดภัยของเครือข่ายก็เป็นอีกประเด็นหนึ่งที่เราต้องให้ความสำคัญ

ในบทนี้ผู้เขียนได้กล่าวถึงเทคนิคต่างๆ ที่ผู้ไม่ประสงค์ดีจะใช้สำหรับการโจมตีหรือบุกรุกเครือข่าย เช่น แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) แมนอินเดอะมิดเดิล (Man in the Middle) ดีไนล์ออฟเซอร์วิส (DoS) เป็นต้น ซึ่งเครื่องมือหรือโปรแกรมสำหรับการโจมตีแบบต่างๆ นั้น ปัจจุบันสามารถค้นหาและดาวน์โหลดจากอินเทอร์เน็ตมาใช้งานได้ง่าย และยิ่งกว่านั้นผู้ใช้อาจไม่จำเป็นที่ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์มากนักก็สามารถใช้เครื่องมือต่างๆ เหล่านี้ได้ ดังนั้น เมื่อมีการเชื่อมต่อเครือข่ายขององค์กรเข้ากับอินเทอร์เน็ต จึงมีความจำเป็นที่ต้องมีระบบรักษาความปลอดภัยในเครือข่ายด้วย

การรักษาความปลอดภัยในเครือข่ายนั้นสิ่งแรกที่นึกถึงคือ ไฟร์วอลล์ ซึ่งเป็นระบบที่ควบคุมการใช้งานระหว่างเครือข่าย โดยเปรียบเสมือนป้อมยามที่คอยตรวจตราการเข้าออกจากสถานที่ต่างๆ นั่นเอง ไฟร์วอลล์ก็มีข้อจำกัดหลายอย่าง หรือไม่อาจที่จะป้องกันการบุกรุกได้ 100 เปอร์เซ็นต์ IDS (Intrusion Detection System) เป็นเครื่องมือการรักษาความปลอดภัยในเครือข่ายอีกประเภทหนึ่ง ที่ใช้สำหรับการตรวจจับการโจมตีหรือความพยายามที่จะโจมตีเครือข่าย

แอพพลิเคชันส่วนใหญ่จะรับ/ส่งข้อมูลในรูปแบบเคลียร์เท็กซ์ มีบางครั้งที่ผู้ใช้ในเครือข่ายจำเป็นที่ต้องสื่อสารกับคนอื่นที่อยู่นอกเครือข่าย ทั้งไฟร์วอลล์และ IDS นั้นไม่สามารถที่จะปกป้องข้อมูลที่ต้องส่งออกไปนอกเครือข่ายได้ ดังนั้น การเข้ารหัสข้อมูลก็เป็นเทคนิคที่ใช้ปกป้องข้อมูลที่ต้องวิ่งผ่านเครือข่ายที่มีความเสี่ยงต่อการลักลอบข้อมูลได้ การเข้ารหัสข้อมูลหรือคริปโตกราฟีแบ่งออกเป็น 2 ประเภทคือ ซีเคร็ทคีย์ (Secret Key) และพับลิกคีย์ (Public Key) ซึ่งทั้งสองเทคนิคนั้นก็มีข้อดีข้อเสียที่ต่างกัน สำหรับซีเคร็ทคีย์นั้นจะเข้าและถอดรหัสได้เร็วกว่า แต่จะมีปัญหาเกี่ยวกับการแจกจ่ายคีย์ เนื่องจากทั้งการเข้ารหัสและการถอดรหัสนั้นจะต้องใช้คีย์เดียวกัน ส่วนพับลิกคีย์นั้นจะใช้คีย์ที่เข้าและถอดรหัสคนละคีย์กัน ดังนั้น ก็จะเพิ่มความปลอดภัยในการแจกจ่ายคีย์

การเข้ารหัสข้อมูลที่รับ/ส่งผ่านเครือข่ายนั้นอาจทำได้ในทุกๆ เลเยอร์ของเครือข่าย เช่น ในระดับแอพพลิเคชันเลเยอร์นั้นโปรโตคอล PGP ก็เป็นเทคนิคที่ใช้สำหรับการเข้ารหัสข้อมูลที่รับ/ส่งผ่านระบบเมล ส่วนโปรโตคอล SSL ก็ทำงานในชั้นทรานสปอร์ตเลเยอร์ และในชั้นเน็ตเวิร์คเลเยอร์ก็มีโปรโตคอล IPSec ซึ่งการรักษาความปลอดภัยในแต่ละเลเยอร์นั้นก็มีข้อดีข้อเสียที่แตกต่างกัน ในบทนี้ผู้เขียนหวังว่าผู้อ่านจะได้ความรู้เกี่ยวกับการป้องกันเครือข่าย ถึงแม้อาจจะไม่สมบูรณ์หรือละเอียดมากนักแต่ก็อาจเป็นจุดเริ่มต้นและแนวทางในการสร้างและปรับปรุงระบบการรักษาความปลอดภัยของเครือข่ายต่อไป

คำถามทบทวน

1. เอ็นนิกมา (Enigma) เป็นเครื่องมือสำหรับทำอะไร คิดค้นโดยประเทศอะไร ใช้ในช่วงไหน และมีข้อพกพร่องในการใช้งานอย่างไร
2. ออเรนจ์บุ๊ค (Orange Book) คืออะไร และมีปัญหาเกี่ยวกับการนำไปใช้อย่างไร
3. C.I.A ย่อมาจากอะไร จงอธิบายความหมายและความสำคัญของแต่ละส่วน
4. จงวิเคราะห์ว่าการโจมตีแต่ละรูปแบบว่าที่มีผลกระทบโดยตรงกับ C.I.A. ด้านใดบ้าง
5. จงวิเคราะห์และประเมินว่าแนวโน้มการโจมตีในอนาคตจะเป็นอย่างไร
6. การเข้ารหัสข้อมูลเป็นการปกป้องคุณสมบัติของความปลอดภัยข้อมูลด้านใด และสามารถป้องกันการโจมตีแบบใดได้บ้าง
7. อธิบายข้อแตกต่างระหว่างไวรัส โทรจัน และเวิร์ม
8. อธิบายข้อแตกต่างระหว่างการเข้ารหัสข้อมูล (Cryptography) และการซ่อนพรางข้อมูล (Steganography)
9. การใช้รหัสผ่าน (Password) จัดอยู่ในการพิสูจน์ทราบตัวตนแบบใด
10. อธิบายข้อแตกต่างระหว่างการเข้ารหัสข้อมูลแบบซิมเมตริกคีย์เอ็นคริปชัน (Symmetric key encryption) และพับลิกคีย์เอ็นคริปชัน (Public key encryption)