

หนังสือด้าน Cybersecurity ที่สมบูรณ์แบบทั้งทฤษฎี ปฏิบัติ และกรณีศึกษา

วิศวกรรมความมั่นคงปลอดภัยข้อมูล ยุคปัญญาประดิษฐ์ (Cybersecurity Engineering in AI Era)

AI



- OWASP TOP 10
- NIST CYBERSECURITY FRAMEWORK
- CRYPTOGRAPHY
- ZERO TRUST NETWORK
- WIRED VS WIRELESS SECURITY
- GDPR&PDPA
- AI CYBERSECURITY
- POST-QUANTUM CRYPTOGRAPHY (PQC)

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์ศิริบุญ

หนังสือด้าน Cybersecurity ที่สมบูรณ์แบบทั้งทฤษฎี ปฏิบัติ และกรณีศึกษา

วิศวกรรมความมั่นคงปลอดภัยข้อมูล ยุคปัญญาประดิษฐ์

(Cybersecurity Engineering in AI Era)

- OWASP Top 10
- NIST Cybersecurity Framework
- Cryptography
- Zero Trust Network
- Wired vs Wireless Security
- GDPR&PDPA
- AI Cybersecurity
- Post-Quantum Cryptography (PQC)

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์ศรีบุญ

ลิขสิทธิ์ © 2568 (2025) โดย ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์ศิริ
สงวนลิขสิทธิ์ทุกประการ ห้ามทำซ้ำ คัดลอก จัดเก็บในระบบก๊อปปี้ หรือส่งต่อในรูปแบบใด ๆ
โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ถือลิขสิทธิ์

พิมพ์ครั้งที่: 1 พ.ศ. 2568

สำนักพิมพ์/หน่วยงาน (Publisher): มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ที่อยู่: ถนนรังสิต-นครนายก ตำบลคลองหก อำเภอธัญบุรี จังหวัดปทุมธานี
โทร: 086-393-8675 อีเมล: wichet@rmutt.ac.th เว็บไซต์: www.rmutt.ac.th

ISBN (ฉบับพิมพ์/Print):

ISBN (อิเล็กทรอนิกส์/eBook):

เลขจัดหมวดหมู่ (ถ้ามี):

ข้อจำกัดความรับผิดชอบ (Disclaimer):

หนังสือเล่มนี้จัดทำเพื่อการศึกษาและวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์

ผู้เขียนและสำนักพิมพ์ไม่รับผิดชอบต่อความเสียหายใด ๆ

อันเกิดจากการนำเนื้อหาไปใช้ผิดวัตถุประสงค์หรือผิดกฎหมาย

คำชี้แจงข้อมูลส่วนบุคคล (PDPA Notice):

เนื้อหา/ตัวอย่างข้อมูลในเล่มเป็นข้อมูลสาธารณะหรือข้อมูลสมมติและไม่สามารถระบุตัวบุคคลได้

หากมีการอ้างอิงถึงหน่วยงาน/แบรนด์ เป็นไปเพื่อการศึกษา

พิมพ์ที่ (Printer): มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

จัดพิมพ์ในประเทศไทย / Printed in Thailand

คำนำ

หนังสือ วิศวกรรมความมั่นคงปลอดภัยข้อมูลยุคปัญญาประดิษฐ์เล่มนี้ มีวัตถุประสงค์เพื่อใช้เป็นหนังสือ ตำราที่สมบูรณ์แบบฉบับภาษาไทย สำหรับระดับปริญญาตรี โท และเอก รวมทั้งผู้ที่ทำงานอยู่ในวิชาชีพด้านความ มั่นคงปลอดภัยไซเบอร์ เช่นเดียวกับหนังสือ ระบบปฏิบัติการ (วิเชษฐ์ พลายมาศ ชื่อเดิม) ที่ใช้เป็นตำราหลัก สำหรับนักศึกษาสาขาวิทยาการคอมพิวเตอร์

เนื้อหาครอบคลุมตั้งแต่พื้นฐานความมั่นคงปลอดภัยไซเบอร์ สถาปัตยกรรมความปลอดภัย ภัยคุกคาม การ ตรวจจับและป้องกันการบุกรุก ไฟร์วอลล์ ระบบอำพราง เครือข่ายส่วนตัวเสมือน วิทยาการรหัสลับ วิศวกรรม เครือข่าย การออกแบบเครือข่ายที่มั่นคงปลอดภัย เครือข่ายไร้สาย ความมั่นคงปลอดภัยเครือข่ายไร้สาย ความ มั่นคงปลอดภัยในระบบปฏิบัติการ แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแนวโน้ม วิศวกรรมความมั่นคงปลอดภัยในยุคปัญญาประดิษฐ์ ซึ่งนำเสนอแนวโน้มของปัญญาประดิษฐ์และระบบการ เข้ารหัสลับของควอนตัมคอมพิวเตอร์ ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ทั้งเชิงบวกและเชิงลบ พร้อม ทั้งมีกิจกรรมกรณีศึกษา (Case Study) ตาราง แผนภาพ และเกณฑ์การประเมินผล เพื่อให้นักศึกษาได้เรียนรู้ทั้ง เชิงทฤษฎีและการประยุกต์ในสถานการณ์จริง ในทุกบทได้เพิ่มเติมบทวิเคราะห์และมุมมองเชิงวิชาการของผู้สอนที่ ได้สั่งสมประสบการณ์จริงทั้งในวิชาชีพ การวิจัย และประสบการณ์สอนด้านความมั่นคงปลอดภัยทางไซเบอร์มา อย่างยาวนาน

หวังเป็นอย่างยิ่งว่า หนังสือเล่มนี้จะช่วยให้อาจารย์ นักศึกษา และผู้สนใจวิชาชีพ Cybersecurity เกิด ความรู้ ความเข้าใจ สามารถนำไปใช้ประกอบการทำงานด้านเทคโนโลยีสารสนเทศ และพัฒนาทักษะการแก้ปัญหา ด้านความมั่นคงปลอดภัยไซเบอร์ เป็นรากฐานสำคัญต่อการนำไปประยุกต์ใช้ในวิชาชีพด้านความมั่นคงปลอดภัย ทางไซเบอร์ตามมาตรฐานได้อย่างมีประสิทธิภาพ

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์ศิริณ

สารบัญ

คำนำ	A
สารบัญ	B
สารบัญภาพ	H
สารบัญตาราง	M
บรรณานุกรม.....	555
อภิธานศัพท์	561
บทที่ 1 ความรู้เบื้องต้นเกี่ยวกับวิศวกรรมความมั่นคงปลอดภัยข้อมูล	1
1.1 ความหมายของความมั่นคงปลอดภัยข้อมูล	6
1.2 ความมั่นคงปลอดภัยข้อมูลและความเป็นส่วนตัวของข้อมูล	10
1.3 ความสำคัญของความมั่นคงปลอดภัยของข้อมูล	11
1.4 ประเภทของความเสี่ยงและภัยคุกคามด้านความปลอดภัยของข้อมูล	15
1.5 มุมมองจากผู้มีส่วนได้ส่วนเสียต่างๆ	16
1.6 ผลกระทบและความรุนแรงของการโจมตีทางไซเบอร์	19
1.7 สถิติการค้นพบการละเมิดข้อมูล	21
1.8 ประเภทของการรักษาความปลอดภัยข้อมูล	23
1.9 กลยุทธ์การรักษาความมั่นคงปลอดภัยข้อมูล	24
1.10 แนวโน้มความปลอดภัยของข้อมูล	27
1.12 สรุปบท	28
1.13 บทวิเคราะห์และมุมมองเชิงวิชาการ : หลักการความมั่นคงปลอดภัยทางไซเบอร์	29
แบบทดสอบท้ายบท	32
บรรณานุกรมท้ายบท	35
บทที่ 2 สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล.....	37
2.1 สถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทางของ OSI	41
2.2 แบบจำลองความมั่นคงปลอดภัยเครือข่าย.....	48

สารบัญ (ต่อ)

2.3	มาตรฐานด้านความมั่นคงปลอดภัย (Security standards).....	52
2.4	กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework)	53
2.5	กลไกและการตอบสนองต่ออุบัติการณ์ตามแนวทาง NIST Cybersecurity Framework.....	61
2.6	บทวิเคราะห์เปรียบเทียบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์.....	67
2.7	สรุปบท	69
	บทวิเคราะห์เชิงวิชาการ	70
	แบบทดสอบท้ายบท	74
	บรรณานุกรมท้ายบท	78
บทที่ 3	ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์:	
	ช่องโหว่ ภัยคุกคาม พื้นฐานของมัลแวร์ และความเสียหาย	82
3.1	ช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์	87
3.2	ภัยคุกคามที่เกิดกับคอมพิวเตอร์.....	90
3.3	พื้นฐานของมัลแวร์	92
3.4	การบุกรุก (Intrusion).....	101
3.5	OWASP	108
3.6	การจัดการความเสี่ยงจากภัยคุกคาม	114
3.7	สรุปบท	118
	บทวิเคราะห์และมุมมองเชิงวิชาการ	122
	แบบทดสอบท้ายบท	124
	บรรณานุกรมท้ายบท	128
บทที่ 4	การตรวจหาการบุกรุกและการป้องกัน	129
4.1	ระบบตรวจหาการบุกรุก (IDS; Intrusion Detection Systems).....	134
4.2	ระบบป้องกันการบุกรุก Intrusion Prevention System (IPS).....	151
4.3	บทวิเคราะห์เปรียบเทียบระหว่าง IPS กับ IDS	155
4.4	สรุปบท	158
	บทวิเคราะห์และมุมมองเชิงวิชาการ	159
	แบบทดสอบท้ายบท	162

สารบัญ (ต่อ)

บรรณานุกรมท้ายบท	166
บทที่ 5 ไฟร์วอลล์และระบบอำพราง (NAT).....	167
5.1 ความหมายของไฟร์วอลล์.....	171
5.2 คุณลักษณะของไฟร์วอลล์	172
5.3 ประเภทไฟร์วอลล์	174
5.4 ระบบอำพรางโดยใช้การแปลงเลขที่อยู่เครือข่าย (Network Address Translation: NAT)	182
5.5 สรุปบท	193
บทวิเคราะห์เชิงวิชาการ	194
แบบทดสอบท้ายบท	196
บรรณานุกรมท้ายบท	200
บทที่ 6 วิศวกรรมเครือข่ายส่วนตัวเสมือน (VPN).....	201
6.1 ความหมายของเครือข่ายส่วนตัวเสมือน.....	205
6.2 คุณลักษณะของเครือข่ายส่วนตัวและเครือข่ายสาธารณะ	207
6.3 โพรโทคอลความปลอดภัยที่ใช้งาน VPN	215
6.4 ประโยชน์ของการใช้ VPN	227
6.5 สรุปบท	227
บทวิเคราะห์และมุมมองเชิงวิชาการ	230
แบบทดสอบท้ายบท	234
บรรณานุกรมท้ายบท	238
บทที่ 7 พื้นฐานวิทยาการรหัสลับ	239
7.1 ความหมายของวิทยาการรหัสลับ (Cryptography)	244
7.2 องค์ประกอบของระบบรหัสลับ	245
7.3 ประเภทของระบบรหัสลับ	244
7.4 การเข้ารหัสลับแบบกุญแจสมมาตร (Symmetric key encryption scheme).....	245
7.5 การเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric key encryption scheme)	258
7.6 ลายมือชื่อดิจิทัล (Digital signature).....	266

สารบัญ (ต่อ)

7.7 การโจมตีระบบรหัสลับ	269
7.8 สรุปบท	273
บทวิเคราะห์และมุมมองเชิงวิชาการ	274
แบบทดสอบท้ายบท	234
บรรณานุกรมท้ายบท	238
บทที่ 8 วิศวกรรมความมั่นคงปลอดภัยเครือข่ายการสื่อสาร	239
8.1 ประเภทเครือข่าย: เครือข่ายบริเวณกว้าง (WAN) และ เครือข่ายเฉพาะที่ (LAN).....	287
8.2 เครือข่ายเฉพาะที่ หรือแลน (LAN: Local Area Network)	295
8.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security).....	303
9.4 การแบ่งโซนเครือข่าย (Network zoning)	336
9.5 สรุปบท	308
บทวิเคราะห์และมุมมองเชิงวิชาการ	309
แบบทดสอบท้ายบท	311
บรรณานุกรมท้ายบท	315
บทที่ 9 การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย	316
9.1 การประยุกต์ใช้หลักการออกแบบเครือข่ายที่เหมาะสม	320
9.2 การวิเคราะห์การบุกรุกเครือข่ายจนทำให้เหยื่อสยยอม (Phases of compromise).....	331
9.3 แบบจำลองภัยคุกคาม	334
9.4 การแบ่งโซนเครือข่าย (Network zoning)	336
9.5 การจัดโซนเฝ้าระวัง (Monitoring zoning)	338
9.6 สรุปบท	343
บทวิเคราะห์และมุมมองเชิงวิชาการ	344
แบบทดสอบท้ายบท	346
บรรณานุกรมท้ายบท	350
บทที่ 10 เครือข่ายไร้สาย	352
10.1 ประเภทของเครือข่ายไร้สาย.....	356

สารบัญ (ต่อ)

10.2 การเชื่อมต่อเครือข่ายและมาตรฐาน IEEE 802.11 WLAN.....	363
10.3 สรุปบท.....	376
บทวิเคราะห์และมุมมองเชิงวิชาการ.....	377
แบบทดสอบท้ายบท.....	379
บรรณานุกรมท้ายบท.....	382
บทที่ 11 ความมั่นคงปลอดภัยของเครือข่ายไร้สาย.....	383
11.1 การโจมตีและการป้องกันเครือข่ายไร้สาย.....	385
11.2 วิศวกรรมความมั่นคงปลอดภัยในมาตรฐาน IEEE 802.11.....	391
11.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi.....	402
11.4 ภัยคุกคามเครือข่ายไร้สายและผลกระทบต่อองค์กร.....	406
11.5 มาตรการป้องกันการโจมตีทางเครือข่ายไร้สาย.....	409
11.6 สรุปบท.....	415
บทวิเคราะห์และมุมมองเชิงวิชาการ.....	416
แบบทดสอบท้ายบท.....	418
บรรณานุกรมท้ายบท.....	421
บทที่ 12 ความมั่นคงปลอดภัยในระบบปฏิบัติการ.....	422
12.1 การป้องกันและความมั่นคงปลอดภัย.....	427
12.2 โครงสร้างการป้องกัน.....	431
12.3 โดเมนของการป้องกัน.....	435
12.4 การใช้งานเมทริกซ์การเข้าถึง.....	445
12.6 การพิสูจน์ตัวตนจริง.....	449
12.7 โปรแกรมอันตราย.....	453
12.8 สรุปบท.....	457
บทวิเคราะห์และมุมมองเชิงวิชาการ.....	459
แบบทดสอบท้ายบท.....	461
บรรณานุกรมท้ายบท.....	464
บทที่ 13 แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์.....	466

สารบัญ (ต่อ)

13.1 แนวปฏิบัติและการรายงานตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์.....	471
13.2 แนวปฏิบัติและการรายงานของหน่วยงานโครงสร้างพื้นฐาน.....	480
13.3 แนวปฏิบัติการแข่งขันตามมาตรฐาน NIST CSF2.0.....	485
13.4 สารสนเทศส่วนบุคคล	489
13.5 สรุปบท	499
บทวิเคราะห์และมุมมองเชิงวิชาการ	500
แบบทดสอบท้ายบท	502
บรรณานุกรมท้ายบท	506
บทที่ 14 บทวิเคราะห์: แนวโน้มวิศวกรรมความมั่นคงปลอดภัยไซเบอร์ในยุคปัญญาประดิษฐ์.....	507
14.1 ภูมิทัศน์ของความก้าวหน้าด้านเทคโนโลยีดิจิทัลกับความมั่นคงปลอดภัยทางไซเบอร์	512
14.2 ความก้าวหน้าควอนตัมคอมพิวเตอร์: ความเสี่ยง ผลกระทบ และความท้าทาย	518
14.3 วิทยาการรหัสลับควอนตัม	527
14.4 ปัญญาประดิษฐ์กับความมั่นคงปลอดภัยข้อมูล	538
14.5 บทวิเคราะห์บูรณาการปัญญาประดิษฐ์และวิทยาการรหัสลับควอนตัม	545
บทวิเคราะห์และมุมมองเชิงวิชาการ	459
แบบทดสอบท้ายบท	551
บรรณานุกรมท้ายบท	555

สารบัญภาพ

รูป 1.1 CIA triad	Error! Bookmark not defined.
รูป 1.2 สถิติการโจมตีทางไซเบอร์เฉพาะหน่วยงานภาครัฐทั่วโลก.....	Error! Bookmark not defined.
รูป 1.3 มูลค่าความเสียหายจากอาชญากรรมไซเบอร์ในอเมริกา.....	Error! Bookmark not defined.
รูป 1.4 อัตราการเติบโตของมูลค่าความเสียหายจากภัยคุกคามไซเบอร์ทั่วโลก.	Error! Bookmark not defined.
รูป 1.5 สถิติภัยคุกคามทางไซเบอร์ 2568 ในประเทศไทย.....	Error! Bookmark not defined.
รูป 1.6 มูลค่าความเสียหายสรุปผลกระทบที่ธุรกิจอาจเผชิญตั้งแต่ปีแรกจนถึงปีที่ 3	Error! Bookmark not defined.
รูป 1.7 ประมาณการค่าเฉลี่ยความเสียหายที่เกิดขึ้นจากการค้นพบว่ามีละเมิดข้อมูล	Error! Bookmark not defined.
รูป 1.8 สัดส่วนผู้โจมตีจนเป็นให้ข้อมูลรั่วไหล.....	Error! Bookmark not defined.
รูป 2.1 แบบจำลองความมั่นคงปลอดภัยเครือข่าย	49
รูป 2.2 แบบจำลองความมั่นคงปลอดภัยในการเข้าถึงเครือข่าย	51
รูป 2.3 NIST CSF 1.1	54
รูป 2.4 NIST CSF 2.0.....	55
รูป 2.5 4 ขั้นตอนวงจรชีวิตการตอบสนองต่ออุบัติการณ์ของ NIST	62
รูป 3.1 OWASP Top 10 2021.....	108
รูป 3.2 OWASP Top 10 Mobile.....	113
รูป 4.1 IDS/IPS	134
รูป 4.2 สถาปัตยกรรมชนิดต่างๆ ของระบบการตรวจหาการบุกรุก.....	142
รูป 4.3 ระบบป้องกันการบุกรุก หรือ IPS.....	151
รูป 5.1 ไฟร์วอลล์	172
รูป 5.2 ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิติ	175
รูป 5.3 ไฟร์วอลล์ระดับแอปพลิเคชันเลเยอร์	177
รูป 5.4 การแปลงเลขที่อยู่ระหว่างเครือข่ายส่วนตัวต้นทางเข้ากับเลขที่อยู่เครือข่ายอินเทอร์เน็ต	182
รูป 5.5 แสดงแพ็กเก็ตเกิดจาก Private IP Address ที่สื่อสารกับอินเทอร์เน็ตผ่าน NAT	185
รูป 5.6 ตัวอย่างการใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิติ	187
รูป 5.7 แสดงการเชื่อมต่อ TCP/IP พื้นฐานของการ NAT.....	190
รูป 5.8 มุมมองเชิงตรรกะของการ NAT แบบกลุ่มต่อหนึ่ง (Many-to-one)	191

รูป 5.9 มุมมองเชิงตรรกะของการ NAPT แบบกลุ่มต่อกลุ่ม (Many-to-many)	192
รูป 6.1 เครือข่ายส่วนตัวเสมือน หรือ VPN	206
สารบัญภาพ (ต่อ)	
รูป 6.2 แสดงการเข้าถึงระยะไกลโดยใช้ VPN	210
รูป 6.3 การเชื่อมต่อโฮสต์ระยะไกลเข้าเครือข่ายส่วนตัวโดยอาศัย VPN หรือ Intranet VPN.....	212
รูป 6.4 แสดงการเชื่อมต่อเครือข่ายส่วนตัวเข้าด้วยกันโดยผ่าน VPN.....	213
รูป 6.5 เปรียบเทียบความแตกต่างของการสื่อสารข้อมูลระหว่างไม่มี VPN กับมี VPN	215
ภาพที่ 6.6 แสดงการห่อหุ้ม IP Datagram ไปบน PPP packet	216
รูป 6.7 แสดง PPP packet ที่ถูกเข้ารหัสด้วย GRE และถูกห่อหุ้มลงใน IP Datagram	218
รูป 6.8 โครงสร้าง L2F packet	219
รูป 6.9 โครงสร้างของ L2TP บน IP Datagram	220
รูป 6.10 โครงสร้างของ L2TP เมื่อใช้งานร่วมกับ IPSec	221
รูป 6.11 VPN ประเภท Firewall Basedรูป 6.10 โครงสร้างของ L2TP เมื่อใช้งานร่วมกับ IPSec	224
รูป 6.12 VPN ประเภทฮาร์ดแวร์	225
รูป 7.1 การทำงานของระบบการเข้ารหัสลับแบบกุญแจสมมาตร	247
รูป 7.2 แผนภาพแสดงการเข้ารหัสลับของขั้นตอนวิธีแบบ DES	249
รูป 7.3 การเข้ารหัสลับของ 2DES	250
รูป 7.4 การเข้ารหัสลับของ 2DES (researchgate.net)	251
รูป 7.5 3-KEY Triple DES	253
รูป 7.6 มาตรฐานการเข้ารหัสขั้นสูง AES (Rijndael)	255
รูป 7.7 การทำงานของระบบการเข้ารหัสลับแบบกุญแจสมมาตร	258
รูป 7.8 การใช้งานลายเซ็นดิจิทัล (Digital Signature) ด้วยระบบรหัสแบบอสมมาตร	259
รูป 7.9 การแลกเปลี่ยนข้อมูลที่เข้ารหัสลับโดยใช้ขั้นตอนวิธีของ Diffie-Hellman	261
รูป 7.10 แสดงการเปรียบเทียบการลงลายมือชื่อแบบปกติและแบบที่ใช้ในโลกดิจิทัล	267
รูป 7.11 หลักการทำงานของลายมือชื่อดิจิทัล	268
รูป 8.1 เครือข่ายเฉพาะที่ (LAN) ที่มีการเชื่อมต่อกับเครือข่ายบริเวณกว้าง (WAN).....	288
รูป 8.2 แผนภาพแนวคิดของ LAN ในบ้านพักอาศัย	296
รูป 8.3 แผนภาพแนวคิดของระบบ LAN ในสำนักงานธุรกิจขนาดเล็ก	298
รูป 8.4 โทโพโลยีต่างๆ ที่อาจใช้ใน LAN แบบมีสายแบบรวมศูนย์: ดาว วงแหวน บัส และต้นไม้	300

รูป 9.1 เครือข่ายที่ไม่มีอาณาบริเวณ (Non-perimeter network).....	322
รูป 9.2 การแบ่งส่วนเครือข่ายออกเป็นส่วนย่อยๆ แต่ละส่วนมีอาณาบริเวณที่แน่นอน.....	323
สารบัญภาพ (ต่อ)	
รูป 9.3 แสดงการนำไฟร์วอลล์มาควบคุมทราฟฟิกเข้าออกแต่ละเครือข่าย.....	324
รูป 9.4 แสดงการออกแบบเครือข่ายออกเป็นโซน	326
รูป 9.5 แสดงการมีช่องทางพิเศษสำหรับการควบคุมจากระยะไกล	327
รูป 9.6 การเชื่อมต่อโดยตรงระหว่างโฮสต์ภายในกับภายนอกแม้จะมีไฟร์วอลล์	329
รูป 9.7 การแยกจากกันของโฮสต์โดยกระบวนการ NAT	330
รูป 9.8 ขั้นตอนการบุกรุกจนทำให้เหยื่อยินยอม.....	332
รูป 9.9 โฮสต์ที่ไวใจได้กับโฮสต์ที่ไวใจไม่ได้จำเป็นต้องเชื่อมต่อเข้าด้วยกัน.....	336
รูป 9.10 การแบ่งเครือข่ายภายในออกจากเครือข่ายภายนอกโดยใช้ไฟร์วอลล์	337
รูป 9.11 การแบ่งโซนเครือข่ายองค์กร	339
รูป 9.12 การแบ่งโซนเครือข่ายพร้อมกับตำแหน่งที่เฝ้าระวัง	340
รูป 10.1 กระบวนการส่งข้อมูลไปพร้อมกับคลื่น.....	356
รูป 10.2 WLAN มักเชื่อมต่อเข้ากับอินเทอร์เน็ต	357
รูป 10.3 การทำงานร่วมกันของ WLAN กับเครือข่ายมีสายรวมทั้งการเชื่อมต่ออินเทอร์เน็ต.....	360
รูปที่ 10.4 การเชื่อมต่อแลนไร้สายในโหมด Ad-Hoc และโครงสร้างพื้นฐาน	364
รูป 10.5 แสดงวิวัฒนาการของมาตรฐาน Wi-Fi	368
รูป 10.6 วิวัฒนาการ WiFi4-WiFi7.....	372
รูป 10.7 เปรียบเทียบไวไฟแต่ละรุ่น	375
รูป 11.1 รูปแบบการโจมตีแบบ MITM โดยใช้ webMITM	390
รูป 11.2 ขั้นตอนการโจมตี WEP.....	392
รูป 11.3 4-Way Handshake	394
รูป 11.4 แสดงสถาปัตยกรรมของ 802.11i.....	395
รูป 12.5 IEEE 802.11X ที่ใช้ในระบบ 802.11i	395
รูป 11.6 ขั้นตอนการพิสูจน์ตัวตนจริงของผู้ใช้ผ่านเครื่องแม่ข่ายตามมาตรฐาน 802.11X	396
รูป 11.7 WPA/WPA2 ภายใต้มาตรฐาน 802.11i.....	397
รูป 11.8 เปรียบเทียบโปรโตคอลความปลอดภัยทั้ง 4 ประเภท	400
รูป 11.9 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi.....	404

รูป 12.1 ระบบที่ประกอบด้วย 3 โดเมนการป้องกัน	345
รูป 12.2 โครงสร้างวงแหวนของมัลติทิกซ์	349

สารบัญภาพ (ต่อ)

รูป 12.3 หนอนอินเทอร์เน็ตของมอริส (Morris Internet worm)	453
รูป 13.1 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) 8 ประเภท	481
รูป 13.2 สกมช. กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการ 5 ขั้นตอน	482
รูป 13.3 วงจรชีวิตข้อมูลส่วนบุคคล	490
รูป 13.4 หลักการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR	491
รูป 13.5 หลักการสำคัญของมาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตาม PDPA	495
รูป 13.6 การอำพรางข้อมูลส่วนบุคคลเป็นมาตรการหนึ่งในการรักษาความลับ	497
รูป 13.7 สาเหตุหลักของการรั่วไหลข้อมูลส่วนบุคคล	499
รูป 14.1 ปัจจัยที่ทำให้เกิดความซับซ้อนของธรรมชาติของความปลอดภัยทางไซเบอร์	513
รูป 14.2 ความเสี่ยงที่องค์กรกังวลมากที่สุด	514
รูป 14.3 ปัญหาความปลอดภัยทางไซเบอร์เชื่อมโยงกับ GenAI	515
รูป 14.4 การคาดการณ์ช่องโหว่ทางไซเบอร์ตั้งแต่ปี 2025 เป็นต้นไป	516
รูป 14.5 ตัวอย่างคอมพิวเตอร์ควอนตัมของ Google's quantum	523
รูป 14.6 อัลกอริทึมการเข้ารหัสลับควอนตัมของ NIST	531
รูป 14.7 การเดินทางสู่อัลกอริทึมที่ทนทานต่อควอนตัม: ความคิดริเริ่มของ NIST	533

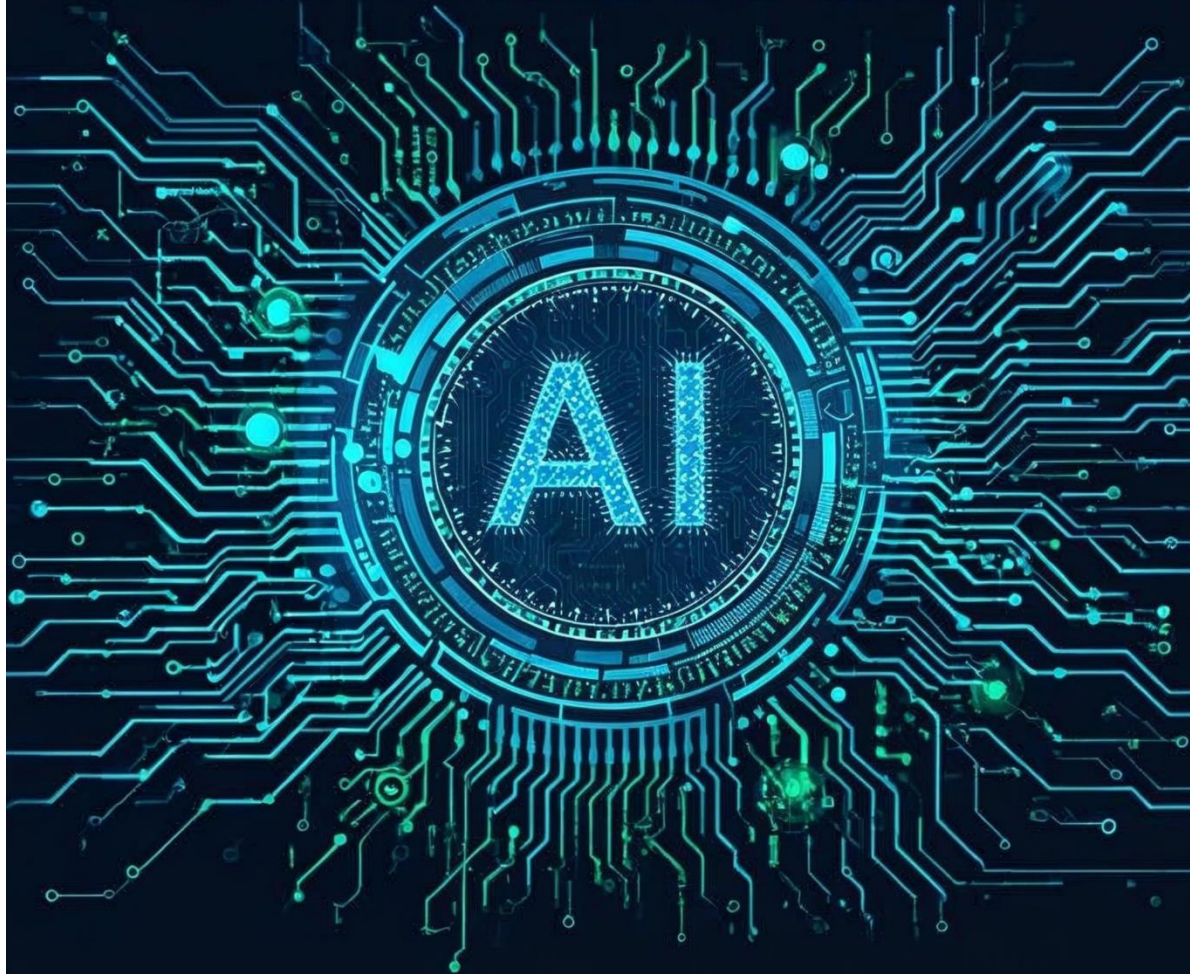
สารบัญตาราง

ตาราง 2.1 ความสัมพันธ์ระหว่างบริการและกลไกความมั่นคงปลอดภัย	46
ตาราง 3.1 ภัยคุกคามและการโจมตี (RFC 2828).....	93
ตาราง 3.2 กระบวนการจัดการความเสี่ยงจากช่องโหว่ของ NIST.....	115
ตาราง 7.1 การเข้ารหัสด้วยขั้นตอนวิธีแบบ RSA โดยที่ $n=35$ และ $e=5$	265
ตาราง 7.2 การถอดรหัสด้วยขั้นตอนวิธีแบบ RSA โดยที่ $n=35$ และ $d=29$	266
ตาราง 7.3 ขนาดกุญแจและเวลาที่ใช้ในการเข้ารหัสกุญแจ โดยคิดเวลา 1 ล้านล้านครั้งต่อวินาที.....	271
ตาราง 10.1 เปรียบเทียบข้อเด่นข้อด้อยระหว่างเทคโนโลยีใช้สายกับไร้สาย	362
ตาราง 10.2 สรุปเปรียบเทียบคุณสมบัติสำคัญของ IEEE 802.11b/a/g/n	369
ตาราง 10.3 สรุปมาตรฐาน IEEE 802.11	373
ตารางที่ 12.1 ความมั่นคงปลอดภัยและการป้องกัน: นโยบายและกลไก.....	429

บทที่ 1

ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์
Introduction to Cybersecurity

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์
CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพรธีรัญญ์

บทที่ 1 ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

(Introduction to Cybersecurity)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบหัวข้อนี้ นักศึกษาจะสามารถ:

1. ระบุและอธิบาย CIA Triad และ Security Services ตาม ITU-T X.800 ได้ถูกต้อง (Remember/Understand)
2. เปรียบเทียบความเชื่อมโยงของ Security Services ↔ ฟังก์ชันของ NIST CSF (Identify, Protect, Detect, Respond, Recover, Govern) ได้ (Understand/Analyze)
3. วิเคราะห์ ภัยคุกคามหลัก (เช่น Malware/Ransomware, Phishing, DDoS, Insider, Misconfiguration) ต่อระบบองค์กรขนาดกลาง และชี้ผลกระทบตามมุมมองผู้มีส่วนได้ส่วนเสีย (Analyze)
4. ออกแบบ มาตรการควบคุมหลายชั้น (defense in depth) ที่สอดคล้องทั้งเชิงสถาปัตยกรรม (X.800) และเชิงกระบวนการ (NIST CSF) สำหรับกรณีศึกษา (Apply/Create)
5. สังเคราะห์ แผนภาพ/ตาราง mapping “บริการความมั่นคง (Confidentiality / Integrity / Availability / Authentication / Access Control / Non-repudiation) ↔ CSF Functions” พร้อมเหตุผลเชิงหลักฐาน (Create)
6. ออกแบบมาตรการรักษาความมั่นคงปลอดภัยที่สอดคล้องกับกรอบมาตรฐานสากลได้

2. จุดประสงค์การเรียนรู้ (Learning Objectives)

- เพื่อให้ผู้เรียนเข้าใจแนวคิด Cybersecurity Governance ผ่านกรอบมาตรฐานที่สำคัญ
- เพื่อให้ผู้เรียนเห็นความสำคัญของ Security Services ในเชิงสถาปัตยกรรมระบบ (X.800/OSI) และในเชิงนโยบาย/กระบวนการ (NIST CSF 2.0)
- เพื่อพัฒนาทักษะการวิเคราะห์และการออกแบบมาตรการควบคุมที่สอดคล้องกับ Confidentiality, Integrity, Availability (CIA Triad)

3. หัวข้อการเรียนรู้

ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

1.1 ความหมายของความมั่นคงทางไซเบอร์

1.1.1 ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

1.1.2 ความสำคัญของความมั่นคงของข้อมูลในยุคดิจิทัล

1.1.3 องค์ประกอบของความมั่นคงของข้อมูล

1.1.4 ประเภทความมั่นคงปลอดภัยข้อมูล

1.2 มุมมองและผลกระทบความมั่นคงปลอดภัยทางไซเบอร์

1.2.1 มุมมองด้านความมั่นคงปลอดภัยข้อมูล

1.2.2 ผลกระทบความมั่นคงปลอดภัยทางไซเบอร์

1.2.3 ความเสี่ยงด้านความมั่นคงปลอดภัยและภัยคุกคามข้อมูล

1.2.4 สถานการณ์ภัยคุกคามต่อความมั่นคงปลอดภัยข้อมูลในปัจจุบันและแนวโน้ม

1.3 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา): “RMUTT Tele-Clinic”

สำนักบริการสุขภาพของมหาวิทยาลัยเปิด **Tele-Clinic** ให้บริการปรึกษาแพทย์ออนไลน์ เชื่อมต่อฐานข้อมูลเวชระเบียนผู้รับบริการ (PII/PHI) ระบบนัดหมาย ชำระเงิน และคลังเอกสารบนคลาวด์สาธารณะ + เก็บ Log บนศูนย์ข้อมูลในมหาวิทยาลัย มีเหตุการณ์ล่าสุด:

- ผู้ใช้บางรายแจ้งถูกส่ง **อีเมลหลอกลวง (Phishing)** ขอรหัสผ่าน
- เซิร์ฟเวอร์นัดหมาย **ทราฟฟิกพุ่งผิดปกติ** ชั่วคราว (ส่งสัย DDoS)
- พบไฟล์ถูกเข้ารหัสในโฟลเดอร์ที่แชร์ร่วม (อาจเป็น **Ransomware**)
- สิทธิ์เข้าถึงบางโฟลเดอร์ถูกปรับค่ากำหนดที่สามารถเข้าได้แบบสาธารณะ (Misconfiguration)

งานที่นักศึกษาต้องทำ (แบ่งกลุ่ม 4-5 คน, 30-45 นาที):

1. ทำ แผนที่ทรัพยากรสารสนเทศ/ข้อมูลอ่อนไหว ของ Tele-Clinic และระบุมุมมองผู้มีส่วนได้ส่วนเสีย (องค์กร/รัฐ/ประชาชน/ผู้เชี่ยวชาญ) ที่ได้รับผลกระทบ (10 นาที)
2. วิเคราะห์ ภัยคุกคามหลัก 4 ประเภทที่ปรากฏ พร้อมความเสี่ยง/ผลกระทบ ตาม CIA (10 นาที)
3. สร้างตาราง Mapping: Security Services (X.800) ↔ NIST CSF Functions ระบุ control/มาตรการที่เสนอ (เช่น MFA, DLP, Backup/BCP, RBAC/Least privilege, Patch/Hardening, Anti-Malware, DDoS protection, IR/BCP/Backup 3-2-1 ฯลฯ) (10 นาที)
4. เสนอ Roadmap 30-60 วัน (ลำดับความสำคัญ/ความเร่งด่วน) และ KPI คร่าว ๆ (Mean-time-to-Detect/Respond, RPO/RTO, อัตรา phishing click-through, % MFA adoption) (10 นาที)
5. นำเสนอ 5 นาที + Q&A 3 นาที

5. เกณฑ์ให้คะแนน (Rubric 4 ระดับ; รวม 100 คะแนน)

เกณฑ์ (น้ำหนัก)	ระดับ 4 ยอดเยี่ยม	3 ดีมาก	2 ดี	1 ควรปรับปรุง
A. ความถูกต้องเชิงวิชาการ & อ้างอิงมาตรฐาน (20%)	อธิบาย CIA/X.800/CSF ถูกต้องครบ และอ้างอิงสอดคล้อง	ถูกต้องส่วนใหญ่	ถูกต้องพอควร	มีคลาดเคลื่อนหลายจุด
B. การวิเคราะห์ภัยคุกคาม & ผลกระทบตาม CIA (20%)	วิเคราะห์เชื่อมโยงเหตุ-ผลลึก ครบ 4 ประเภท	ลึก 3 ประเภท	ครบแต่ผิวเผิน	ขาดบางประเภท
C. Mapping X.800 ↔ NIST CSF & ชัดควบคุม (30%)	Mapping ชัด เหมาะสม มีเหตุผลและครอบคลุม	Mapping ชัด 70-80%	พอใช้ มีช่องว่าง	ไม่ต่อเนื่อง
D. Roadmap & KPI/ความเป็นไปได้ (20%)	ลำดับงาน/ทรัพยากรสมจริง + KPI วัดผลได้	เกือบครบ	พอใช้	คลุมเครือ
E. การสื่อสาร/นำเสนอ (10%)	โครงสร้างดี สื่อชัด กำหนดเวลา	ชัดเจนเล็กน้อย	พอใช้	สื่อไม่ชัด

หมายเหตุ วิเคราะห์เชิงมาตรฐาน: กิจกรรมและ rubric บังคับให้นักศึกษาผูก “บริการความมั่นคง” ของ X.800 กับ “ฟังก์ชัน CSF” ตาม Learning Outcomes/Objectives ของบทเรียนโดยตรง

1.1 ความหมายของความมั่นคงปลอดภัยข้อมูล

ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร (National Cyber Security Centre หรือ NCSC) ให้ความหมายของความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ไว้อย่างกว้าง ๆ ว่า คือ “วิธีที่บุคคลหรือหน่วยงานทำเพื่อลดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์” (ที่มา: ncsc.gov.uk)

ในขณะที่ หน่วยงานความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของสหรัฐอเมริกา (Cybersecurity & Infrastructure Security Agency หรือ CISA) ให้คำนิยามไว้ว่า “ศิลปะในการป้องกันเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ทางอาชญากรรม และการทำให้มั่นใจว่าข้อมูล (information) ได้รับการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)” (ที่มา: us-cert.cisa.gov)

ความหมายดั้งเดิมที่ปรากฏในคู่มือกรอบการทำงานด้านความมั่นคงปลอดภัยคอมพิวเตอร์ NIST (Computer Security Handbook [NIST95]) ให้ความหมายว่า “การป้องกันที่มอบให้กับระบบสารสนเทศอัตโนมัติเพื่อบรรลุมิติประสงค์ที่ใช้บังคับในการรักษาความสมบูรณ์ ความพร้อมใช้งาน และความลับของทรัพยากรระบบสารสนเทศ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ ข้อมูล/ข้อมูล และโทรคมนาคม (NIST95) ต่อมากรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาโดย NIST (National Institute of Standards and Technology) ซึ่งเป็นหน่วยงานของรัฐบาลสหรัฐอเมริกา NIST Cybersecurity Framework (CSF) เป็นแนวทางปฏิบัติที่องค์กรต่างๆ ทั่วโลกนำไปใช้เพื่อจัดการความเสี่ยงและปรับปรุงความมั่นคงปลอดภัยของระบบและข้อมูล สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ ให้ความหมายว่า “กระบวนการและแนวทางในการป้องกันระบบคอมพิวเตอร์ เครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตี การทำลาย หรือการรบกวนการให้บริการองค์ประกอบหลักของความมั่นคงทางไซเบอร์ ได้แก่ **Confidentiality (ความลับ)**: ข้อมูลต้องไม่รั่วไหล, **Integrity (ความถูกต้อง)**: ข้อมูลต้องไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต และ **Availability (ความพร้อมใช้)**: ระบบต้องพร้อมให้บริการอยู่เสมอ” (National Institute of Standards and Technology. (NIST, 2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.)

พระราชบัญญัติการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Information Sharing Act :CISA) แห่งสหรัฐอเมริกา ให้นิยามว่า “ศิลปะในการป้องกันเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ทางอาชญากรรม โดยเน้นการรักษาความลับ (Confidentiality), ความครบถ้วน (Integrity), และความพร้อมใช้งาน (Availability)” (CISA, n.d.)

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU-T X.1205) ให้นิยามไว้ว่า “การรวบรวมเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัย แนวทางการบริหารความเสี่ยง

การฝึกอบรม และเทคโนโลยีต่าง ๆ ที่ใช้เพื่อปกป้องสิ่งแวดล้อมไซเบอร์และทรัพย์สินขององค์กรและผู้ใช้” โดยมีวัตถุประสงค์หลักคือ:ความพร้อมใช้งาน (Availability) ความครบถ้วนและความถูกต้อง (Integrity) และความลับของข้อมูล (Confidentiality) (ITU, 2008)

ในขณะที่ การ์ทเนอร์ บริษัท วิจัยชั้นนำของอเมริกาให้ความหมายว่า “การผสมผสานของบุคลากร นโยบาย กระบวนการ และเทคโนโลยีที่องค์กรใช้เพื่อปกป้องทรัพย์สินทางไซเบอร์” (Gartner, n.d.)

ส่วนในประเทศไทย ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้ความหมาย “การรักษาความมั่นคงปลอดภัยไซเบอร์” ไว้หมายความว่า “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ”

สอดคล้องกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ได้ให้กำหนดนิยามของ “ความมั่นคงปลอดภัย” หมายความว่า “การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล”

คำจำกัดความนี้เสนอวัตถุประสงค์หลัก 3 ประการซึ่งเป็นหัวใจสำคัญของความปลอดภัยคอมพิวเตอร์ ประกอบด้วย ความลับ (C), ความถูกต้องครบถ้วน (I) และความพร้อมใช้งาน (A) รวมเรียกว่า **CIA Triad** หรือ **สามเส้าของ CIA**

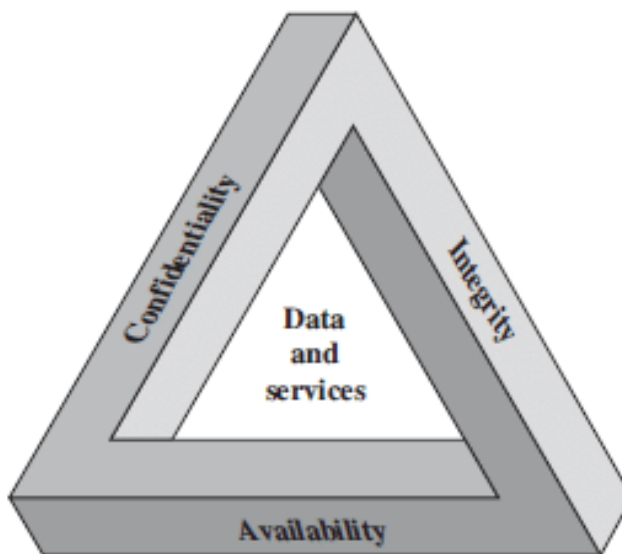
ความลับ (Confidentiality): คำนี้ครอบคลุมแนวคิดที่เกี่ยวข้องสองประการ ได้แก่ **ความลับของข้อมูล:** รับรองว่าข้อมูลส่วนตัวหรือข้อมูลลับจะไม่ถูกเปิดเผยหรือเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต **ความเป็นส่วนตัว:** รับรองว่าบุคคลสามารถควบคุมหรือมีอิทธิพลต่อข้อมูลที่เกี่ยวข้องกับตนที่อาจถูกรวบรวมและจัดเก็บ รวมถึงบุคคลที่สามารถเปิดเผยข้อมูลนั้นได้

ความถูกต้องครบถ้วน (Integrity): คำนี้ครอบคลุมแนวคิดที่เกี่ยวข้องสองประการ ได้แก่ **ความถูกต้องครบถ้วนของข้อมูล:** รับรองว่าข้อมูลและโปรแกรมจะถูกเปลี่ยนแปลงเฉพาะในลักษณะที่กำหนดและได้รับอนุญาตเท่านั้น **ความถูกต้องครบถ้วนของระบบ:** รับรองว่าระบบทำงานตามหน้าที่ที่ตั้งใจไว้โดยไม่ถูกรบกวน ปราศจากการจัดการระบบโดยไม่ได้รับอนุญาตทั้งโดยเจตนาหรือโดยไม่ตั้งใจ

ความพร้อมใช้งาน (Availability): รับรองว่าระบบทำงานได้อย่างรวดเร็วและไม่มีการปฏิเสธการให้บริการแก่ผู้ใช้ที่ได้รับอนุญาต

แนวคิดทั้งสามนี้ประกอบกันเป็นสิ่งที่มักเรียกว่า CIA triad (รูป 1.1) แนวคิดนี้รวบรวมวัตถุประสงค์ด้านความปลอดภัยพื้นฐานสำหรับทั้งข้อมูลและบริการสารสนเทศและการประมวลผล ตัวอย่างเช่น มาตรฐาน NIST

สำหรับการจัดประเภทความปลอดภัยของระบบสารสนเทศและสารสนเทศของรัฐบาลกลาง (FIPS 199) กำหนดให้ ความลับ ความสมบูรณ์ และความพร้อมใช้งาน เป็นเป้าหมายด้านความปลอดภัยสามประการสำหรับสารสนเทศ และระบบสารสนเทศ FIPS 199 ได้ให้ลักษณะเฉพาะที่เป็นประโยชน์ของวัตถุประสงค์ทั้งสามข้อนี้ในแง่ของ ข้อกำหนดและคำจำกัดความของการสูญเสียความปลอดภัยในแต่ละประเภท



รูป 1.1 CIA triad

(ที่มา: . FIPS 199)

จากรูป 1.1 แสดงให้เห็นว่า การรักษาความลับ: การรักษาข้อจำกัดที่ได้รับอนุญาตเกี่ยวกับการเข้าถึงและการเปิดเผยข้อมูล รวมถึงวิธีการปกป้องความเป็นส่วนตัวและข้อมูลที่เป็นกรรมสิทธิ์ การสูญเสียความลับคือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ความถูกต้องครบถ้วน: การป้องกันการแก้ไขหรือการทำลายข้อมูลที่ไม่เหมาะสม รวมถึงการรับรองการปฏิเสธความรับผิดชอบและความถูกต้องของข้อมูล การสูญเสียความสมบูรณ์คือการแก้ไขหรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต และความพร้อมใช้งาน: การรับรองการเข้าถึงและการใช้ข้อมูลอย่างทันท่วงทีและเชื่อถือได้ การสูญเสียความพร้อมใช้คือการขัดขวางการเข้าถึงหรือการใช้ข้อมูลหรือระบบสารสนเทศ

แม้ว่าการใช้ CIA triad เพื่อกำหนดวัตถุประสงค์ด้านความปลอดภัยจะเป็นที่ยอมรับกันดี แต่บุคลากรด้านความปลอดภัยบางส่วนรู้สึกว่าการจำเป็นต้องมีแนวคิดเพิ่มเติมเพื่อให้เห็นภาพที่สมบูรณ์ สองสิ่งที่ถูกกล่าวถึงบ่อยที่สุดได้แก่

การพิสูจน์ตัวตนจริง (Authentication): คุณสมบัติของความเป็นของแท้และสามารถตรวจสอบและเชื่อถือได้; ความเชื่อมั่นในความถูกต้องของการส่ง ข้อความ หรือผู้ส่ง ซึ่งหมายถึงการตรวจสอบว่าผู้ใช้เป็นบุคคลเดียวกับที่พวกเขาบอก และข้อมูลที่ส่งเข้ามาในระบบมาจากแหล่งที่เชื่อถือได้

ความรับผิดชอบ (Accountability): เป้าหมายด้านความปลอดภัยที่ก่อให้เกิดข้อกำหนดให้สามารถติดตามการกระทำของหน่วยงานใดหน่วยงานหนึ่งได้เฉพาะหน่วยงานนั้น สิ่งนี้สนับสนุนการปฏิเสธความรับผิดชอบ การยับยั้ง การแยกข้อผิดพลาด การตรวจจับและป้องกันการบุกรุก การกู้คืนหลังเกิดเหตุและการดำเนินคดีทางกฎหมาย

เนื่องจากระบบที่มีความปลอดภัยอย่างแท้จริงยังไม่สามารถบรรลุผลได้ เราจึงจำเป็นต้องสามารถติดตามการละเมิดความปลอดภัยไปยังฝ่ายที่รับผิดชอบได้ ระบบต้องเก็บบันทึกกิจกรรมต่างๆ เพื่อให้สามารถวิเคราะห์ทางนิติวิทยาศาสตร์ในภายหลังเพื่อติดตามการละเมิดความปลอดภัย หรือเพื่อช่วยในการโต้แย้งธุรกรรม

ความปลอดภัยของข้อมูล (Data security) คือ การปกป้องข้อมูลจากการแก้ไข ทำลาย หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (โดยบังเอิญหรือตั้งใจ) (ที่มา: NIST.gov, CNSSI-4009)

ความปลอดภัยของข้อมูล คือ หลักปฏิบัติในการปกป้องข้อมูลดิจิทัลจากการเข้าถึงโดยไม่ได้รับอนุญาต การทุจริต หรือการโจรกรรมตลอดวงจรชีวิตข้อมูล ครอบคลุมทั้งสภาพแวดล้อมทางกายภาพและดิจิทัล ซึ่งรวมถึงระบบภายในองค์กร อุปกรณ์พกพา แพลตฟอร์มคลาวด์ และแอปพลิเคชันของบุคคลที่สาม (ที่มา: IBM)

เป้าหมายหลักของการรักษาความปลอดภัยข้อมูล คือการป้องกันภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้นในปัจจุบัน เช่น แรนซัมแวร์มัลแวร์ ภัยคุกคามภายใน และข้อผิดพลาดของมนุษย์ เป็นต้น ขณะเดียวกันก็ยังคงให้สามารถใช้ข้อมูลได้อย่างปลอดภัยและมีประสิทธิภาพ

การบรรลุเป้าหมายนี้ต้องอาศัยการป้องกันหลายชั้น เทคนิคต่างๆ เช่น การปกปิดข้อมูลและการเข้ารหัส ช่วยรักษาความปลอดภัยของข้อมูลสำคัญ ขณะที่การควบคุมการเข้าถึงและโปรโตคอล การตรวจสอบสิทธิ์ช่วยให้มั่นใจได้ว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถโต้ตอบกับข้อมูลได้

มาตรการเหล่านี้ร่วมกันเป็นรากฐานสำคัญของกลยุทธ์ด้านความปลอดภัยสารสนเทศ (InfoSec) ที่ครอบคลุมยิ่งขึ้น ช่วยให้องค์กรลดความเสี่ยง ขณะเดียวกันก็รักษาการเข้าถึงข้อมูลสำคัญอย่างปลอดภัยและเชื่อถือได้ กลยุทธ์ด้านความปลอดภัยข้อมูลสมัยใหม่ต่อยอดจากรากฐานนี้ ด้วยความสามารถต่างๆ เช่น การตรวจสอบเฝ้าระวังแบบเรียลไทม์และเครื่องมือรักษาความปลอดภัยอัตโนมัติ

จากการรวบรวมและเปรียบเทียบคำจำกัดความจากแหล่งต่าง ๆ ทั้งในประเทศและต่างประเทศ สามารถสรุปสาระสำคัญของ “ความมั่นคงปลอดภัยทางไซเบอร์” ได้ดังนี้:

- เป็นแนวทางหรือระบบที่มุ่งเน้นการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- ครอบคลุมทั้ง บุคลากร, นโยบาย, เทคโนโลยี, และกระบวนการบริหารจัดการ
- มีเป้าหมายเพื่อรักษาความลับ (Confidentiality), ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบ
- ในบริบทของประเทศไทย ยังเน้นถึงผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ จึงใช้คำว่า “ความมั่นคงปลอดภัย”

กล่าวโดยสรุป ความมั่นคงปลอดภัยของข้อมูลจะปกป้องข้อมูลและความเป็นส่วนตัวของข้อมูลจะควบคุมการใช้งานข้อมูล เพื่อธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน

1.2 ความมั่นคงปลอดภัยข้อมูลและความเป็นส่วนตัวของข้อมูล

แม้จะมีการเชื่อมโยงกันอย่างลึกซึ้ง แต่ความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนตัวของข้อมูลก็เป็นแนวคิดที่แตกต่างกัน

ความมั่นคงปลอดภัยของข้อมูล (Data security) มุ่งเน้นไปที่วิธีการปกป้องข้อมูลสำคัญ โดยใช้ไฟร์วอลล์ เครื่องมือป้องกันการสูญหายของข้อมูล (Data loss protection: DLP) การเข้ารหัส (Encryption) และโพรโทคอลการพิสูจน์ตัวตนจริง (Authentication protocols) ความมั่นคงปลอดภัยข้อมูล เป็นมาตรการและกระบวนการที่ใช้ในการปกป้องข้อมูลจากการเข้าถึง การใช้งาน การเปิดเผย การเปลี่ยนแปลง หรือการทำลายโดยไม่ได้รับอนุญาต ซึ่งรวมถึงการใช้เทคโนโลยีต่างๆ เช่น การเข้ารหัส การตรวจสอบสิทธิ์ และ Firewall เพื่อป้องกันการรั่วไหลของข้อมูลและภัยคุกคามทางไซเบอร์

ในทางกลับกัน ความเป็นส่วนตัวของข้อมูล (Data privacy) จะกล่าวถึงวิธีการรวบรวม จัดเก็บ ประมวลผล และแบ่งปันข้อมูลเหล่านั้น ความเป็นส่วนตัวของข้อมูล คือ สิทธิของแต่ละบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง ไม่ว่าจะเป็นข้อมูลชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลทางการเงิน โดยครอบคลุมถึงวิธีการรวบรวม ใช้ เปิดเผย จัดเก็บ และลบข้อมูลเหล่านั้น องค์กรต้องปฏิบัติตามกฎหมาย PDPA และข้อบังคับอื่นๆ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลได้รับการจัดการอย่างถูกต้องและเป็นธรรม

กฎหมายว่าด้วยด้านความเป็นส่วนตัว เช่น ข้อบังคับทั่วไปว่าด้วยการคุ้มครองข้อมูล (GDPR) แห่งสหภาพยุโรป และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของประเทศไทย กำหนดให้องค์กรต่างๆ ต้องโปร่งใสในการใช้ข้อมูลส่วนบุคคลและให้สิทธิแก่บุคคลในการเข้าถึงข้อมูลของตน มาตรการรักษาความปลอดภัยข้อมูล

สนับสนุนข้อกำหนดเหล่านี้ โดยรับรองว่าเฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ และข้อมูลนี้ได้รับการประมวลผลอย่างปลอดภัยและเป็นไปตามข้อกำหนด

1.3 ความสำคัญของความมั่นคงปลอดภัยของข้อมูล

การเปลี่ยนฉับพลันทางดิจิทัลยังคงพัฒนาองค์กรต่างๆ อย่างต่อเนื่อง ซึ่งปัจจุบันสร้าง จัดการ และจัดเก็บข้อมูลปริมาณมหาศาลในระบบที่กระจายตัวและสภาพแวดล้อมคลาวด์ ไอบีเอ็มระบุว่า ทุกวันมีข้อมูลมากกว่า 402.74 ล้านเทราไบต์โดยที่สหรัฐอเมริกาเพียงประเทศเดียวมีศูนย์ข้อมูลมากกว่า 2,700 แห่ง

ปัจจุบันข้อมูลที่ละเอียดอ่อน เช่น ทรัพย์สินทางปัญญาและข้อมูลส่วนบุคคลแพร่กระจายไปทั่วอุปกรณ์ปลายทาง แอปพลิเคชัน แล็บท็อป และแพลตฟอร์มคลาวด์หลากหลายประเภท สภาพแวดล้อมการประมวลผลในปัจจุบันมีความซับซ้อนมากขึ้นกว่าที่เคย ครอบคลุมตั้งแต่คลาวด์สาธารณะศูนย์ข้อมูล องค์กร และ อุปกรณ์ เอดจ์ เช่น เซ็นเซอร์ อินเทอร์เน็ตออฟธิงส์ (IoT) หุ่นยนต์ และเซิร์ฟเวอร์ระยะไกล การกระจายตัวนี้เพิ่มพื้นที่การโจมตีและเพิ่มความเสี่ยงต่อเหตุการณ์ด้านความปลอดภัย

การไม่ปกป้องข้อมูลอาจก่อให้เกิดความเสียหายมหาศาล ซึ่งรวมถึงการละเมิดข้อมูลการสูญเสียทางการเงิน ความเสียหายต่อชื่อเสียง และการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เพิ่มมากขึ้นเรื่อยๆ ข้อมูลในปี พ.ศ.2568 แสดงให้เห็นว่าความเสียหายเฉลี่ยทั่วโลกจากการละเมิดข้อมูลอยู่ที่ 4.4 ล้านดอลลาร์สหรัฐ

ความปลอดภัยข้อมูลที่แข็งแกร่งไม่เพียงแต่รับประกันการปฏิบัติตามข้อกำหนดเท่านั้น แต่ยังช่วยเสริมสร้าง ความพยายาม ด้านความปลอดภัยทางไซเบอร์ ในวงกว้างอีกด้วย มาตรการรักษาความปลอดภัยที่แข็งแกร่งซึ่งได้รับการสนับสนุนจากเทคโนโลยีต่างๆ เช่นการยืนยันตัวตนแบบไบโอเมตริกซ์การยืนยันตัวตนแบบหลายปัจจัย (MFA) และการตรวจสอบอัตโนมัติ ช่วยให้สามารถกำกับดูแลข้อมูลและสร้างความไว้วางใจให้กับลูกค้าได้ เมื่อบริหารจัดการอย่างเหมาะสม การเข้าถึงข้อมูลที่ปลอดภัยจะช่วยให้มั่นใจได้ว่าข้อมูลสำคัญจะถูกนำไปใช้อย่างมีความรับผิดชอบ ลดโอกาสการถูกละเมิดหรือนำไปใช้ในทางที่ผิด

จากรายงาน “Cyber Attack Statistics to Know in 2023” [\[2\]](#) ของ Parachute เผยให้เห็นถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานภาครัฐ ดังรูป 1.2

Cyber Attack Statistics to Know in 2023



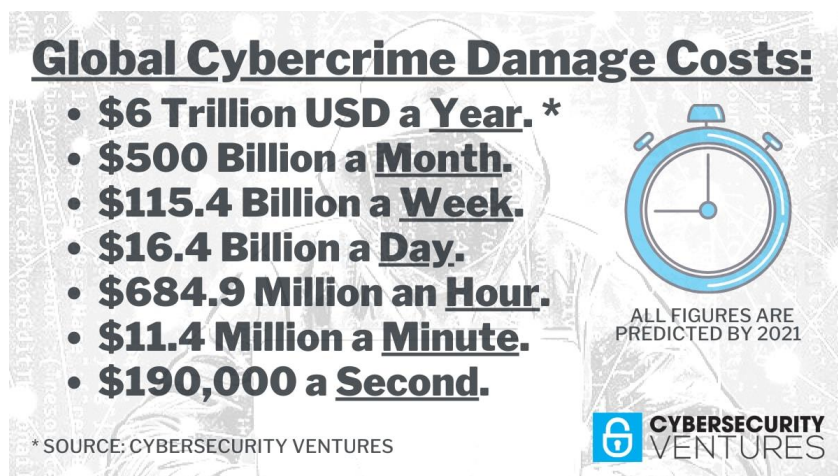
Source: <https://parachute.cloud/cyber-attack-statistics-data-and-trends/>

รูป 1.2 สถิติการโจมตีทางไซเบอร์เฉพาะหน่วยงานภาครัฐทั่วโลก

(ที่มา: <https://parachute.cloud/cyber-attack-statistics-data-and-trends/>)

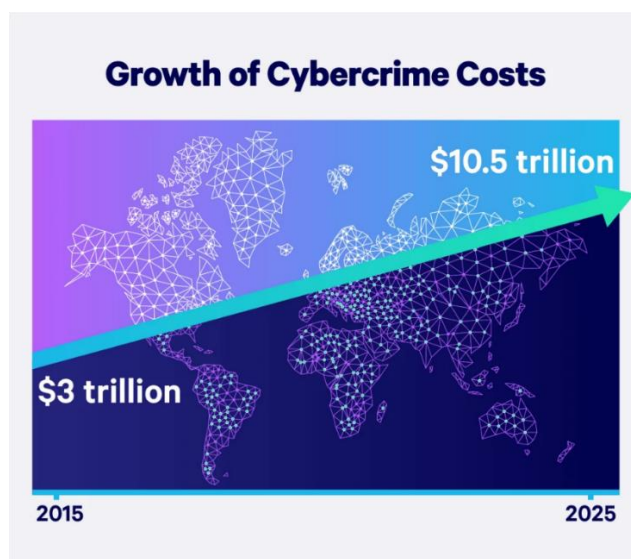
Cybersecurity Ventures คาดการณ์ว่าต้นทุนจากอาชญากรรมไซเบอร์ทั่วโลกจะเติบโตขึ้น 15 เปอร์เซ็นต์ต่อปีในอีกห้าปีข้างหน้า โดยจะสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐต่อปีภายในปี 2568 เพิ่มขึ้นจาก 3 ล้านล้านดอลลาร์สหรัฐในปี 2558 ตัวเลข นี้ถือเป็นการถ่ายโอนความมั่งคั่งทางเศรษฐกิจครั้งใหญ่ที่สุดในประวัติศาสตร์ลดความเสี่ยงต่อแรงจูงใจในการสร้างสรรค์นวัตกรรมและการลงทุน มีมูลค่าสูงกว่าความเสียหายจากภัยพิบัติทางธรรมชาติในแต่ละปีอย่างทวีคูณ และจะสร้างผลกำไรได้มากกว่าการค้ายาเสพติดผิดกฎหมายรายใหญ่ทั่วโลกรวมกัน

รายงานปี 2017 จาก Cybersecurity Ventures คาดการณ์ว่าความเสียหายจากแรนซัมแวร์จะทำให้โลกสูญเสียเงิน 5 พันล้านดอลลาร์สหรัฐในปี 2017 เพิ่มขึ้นจาก 325 ล้านดอลลาร์สหรัฐในปี 2015 หรือเพิ่มขึ้น 15 เท่าในเวลาเพียงสองปี ความเสียหายในปี 2018 ประเมินไว้ที่ 8 พันล้านดอลลาร์สหรัฐและในปี 2019 ตัวเลขเพิ่มขึ้นเป็น 11.5 พันล้านดอลลาร์สหรัฐ การคาดการณ์ล่าสุดระบุว่ามูลค่าความเสียหายจากแรนซัมแวร์ทั่วโลกจะสูงถึง 20,000 ล้านดอลลาร์ภายในปี 2021 ซึ่งเพิ่มขึ้น 57 เท่าจากปี 2015 คาดการณ์ว่าจะมีการโจมตีด้วยแรนซัมแวร์ต่อธุรกิจทุก ๆ 11 วินาทีภายในปี 2021 ซึ่งเพิ่มขึ้นจากทุก ๆ 40 วินาทีในปี 2016 รูป 1.3



รูป 1.3 มูลค่าความเสียหายจากอาชญากรรมไซเบอร์ในอเมริกา
(ที่มา: Cybersecurity VENTURES)

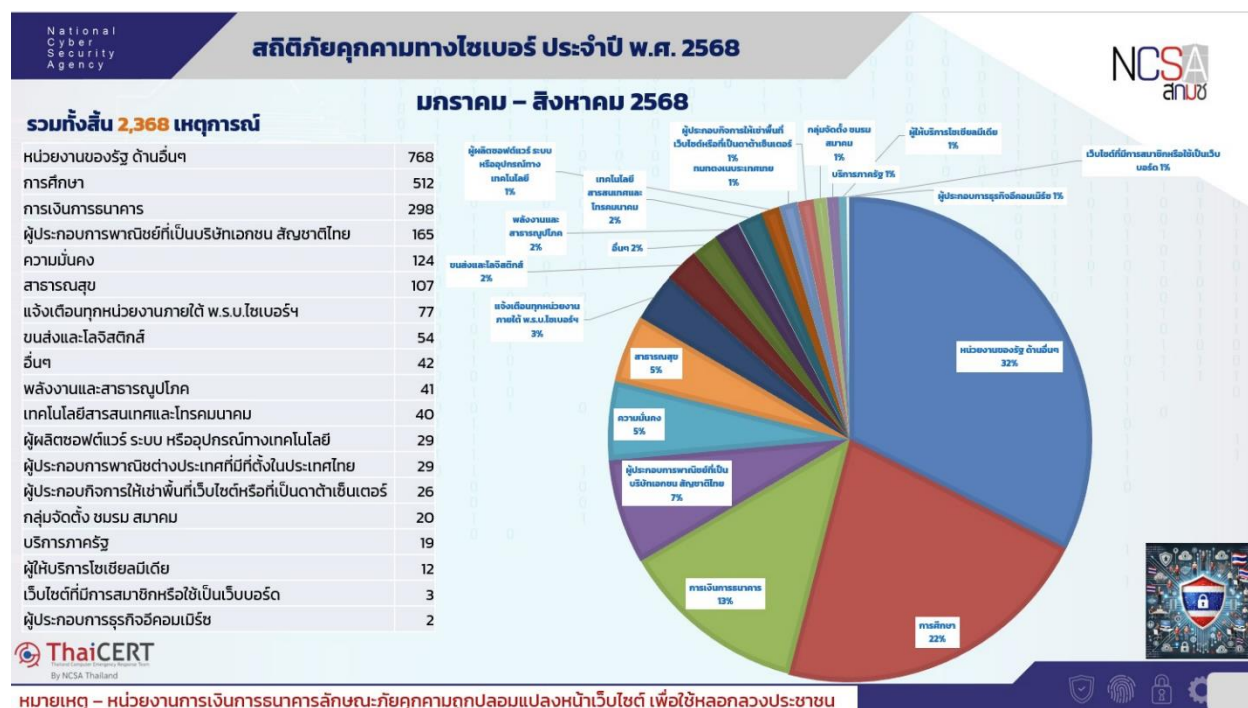
ความเสี่ยงที่ใหญ่ที่สุดจากภัยคุกคามทางไซเบอร์คือความสูญเสียทางการเงิน สถิติและแนวโน้มแสดงให้เห็นว่าอาชญากรรมไซเบอร์เป็นหนึ่งในภัยคุกคามที่สร้างความเสียหายสูงสุดต่อธุรกิจ อาชญากรรมไซเบอร์ทั่วโลกสร้างความเสียหายให้กับบริษัทต่างๆ ราว 8 ล้านล้านดอลลาร์สหรัฐในปี 2566 ซึ่งตัวเลขดังกล่าวสูงมากและคาดว่าจะเพิ่มขึ้นเป็นเกือบ 24 ล้านล้านดอลลาร์สหรัฐภายในปี 2570 รูป 1.4 แสดงถึงอัตราการเติบโตของภัยคุกคามทางไซเบอร์ที่ทำให้สูญเสียค่าใช้จ่ายจากประมาณ 3 ล้านล้านเหรียญสหรัฐในปี 2015 อีก 10 ปีต่อมาเพิ่มขึ้นเป็น 10.5 ล้านล้านเหรียญสหรัฐในปี 2025



รูป 1.4 อัตราการเติบโตของมูลค่าความเสียหายจากภัยคุกคามไซเบอร์ทั่วโลก
(ที่มา: embroker.com)

กฎระเบียบต่างๆ เช่น GDPR และ CCPA บังคับใช้ข้อกำหนดที่เข้มงวดเกี่ยวกับวิธีที่ธุรกิจจัดเก็บ ส่งต่อ และรักษาความปลอดภัยของข้อมูลส่วนบุคคล กรอบการทำงานเหล่านี้ผนวกเข้ากับกฎระเบียบที่มีมายาวนาน เช่น พระราชบัญญัติความสามารถในการโอนย้ายและความรับผิดชอบของประกันสุขภาพ (HIPAA) ซึ่งคุ้มครองบันทึกสุขภาพอิเล็กทรอนิกส์ และการปฏิบัติตามพระราชบัญญัติ Sarbanes-Oxley (SOX) ซึ่งควบคุมการรายงานทางการเงินและการควบคุมภายใน

สถิติการโจมตีในปี 2568 มีทั้งแนวโน้มทั่วโลกและเจาะจงในไทย โดยทั่วโลกมีการโจมตีที่เกี่ยวข้องกับเว็บไซต์ 44% และการโจมตีห่วงโซ่อุปทานเป็นภัยคุกคามที่น่ากังวลที่สุด ขณะที่ในไทยพบว่าการโจมตีเซิร์ฟเวอร์ในไทยเพิ่มขึ้นในไตรมาส 2 ปี 2568 และมีคดือออนไลน์ที่ประชาชนถูกหลอกเฉลี่ยวันละกว่า 1,100 เรื่อง สอดคล้องกับสถิติภัยคุกคามทางไซเบอร์ 2568 ที่รวบรวมโดย สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รูป 1.5



รูป 1.5 สถิติภัยคุกคามทางไซเบอร์ 2568 ในประเทศไทย

(ที่มา: สกมช.)

ความปลอดภัยข้อมูลที่แข็งแกร่งไม่เพียงแต่รับประกันการปฏิบัติตามข้อกำหนดเท่านั้น แต่ยังช่วยเสริมสร้าง ความพยายาม ด้านความปลอดภัยทางไซเบอร์ ในวงกว้างอีกด้วย มาตรการรักษาความปลอดภัยที่แข็งแกร่งซึ่งได้รับการสนับสนุนจากเทคโนโลยีต่างๆ เช่นการยืนยันตัวตนแบบไบโอเมตริกซ์การยืนยันตัวตนแบบหลายปัจจัย (MFA) และการตรวจสอบอัตโนมัติ ช่วยให้สามารถกำกับดูแลข้อมูลและสร้างความไว้วางใจให้กับ

ลูกค้าได้ เมื่อบริหารจัดการอย่างเหมาะสม การเข้าถึงข้อมูลที่ปลอดภัยจะช่วยให้มั่นใจได้ว่าข้อมูลสำคัญจะถูกนำไปใช้อย่างมีความรับผิดชอบ ลดโอกาสการถูกละเมิดหรือนำไปใช้ในทางที่ผิด

1.4 ประเภทของความเสียหายและภัยคุกคามด้านความปลอดภัยของข้อมูล

ข้อมูลขององค์กรมีความเสี่ยงต่อภัยคุกคามด้านความปลอดภัยมากมาย ซึ่งส่วนใหญ่มักใช้ประโยชน์จากพฤติกรรมของมนุษย์ การกำหนดค่าระบบที่ผิดพลาด หรืออุปกรณ์ปลายทางที่ถูกมองข้าม ตัวอย่างที่เห็นได้ชัดได้แก่:

มัลแวร์ (Malware): ซอฟต์แวร์อันตรายที่ออกแบบมาเพื่อทำลาย ขัดขวาง หรือขโมยข้อมูล มัลแวร์สามารถส่งผ่านการดาวน์โหลดที่ติดไวรัส เว็บไซต์ที่ถูกบุกรุก หรือไฟล์แนบในอีเมล มัลแวร์เป็นหนึ่งในความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่พบบ่อยที่สุด ปัจจุบันมีโปรแกรมมัลแวร์มากกว่า 1.2 พันล้านโปรแกรม มัลแวร์เป็นคำรวมที่ใช้เรียกซอฟต์แวร์ที่เป็นอันตรายทุกประเภทที่สามารถทำลายระบบคอมพิวเตอร์และช่วยเหลืออาชญากรไซเบอร์ได้ จำนวนโปรแกรมมัลแวร์ที่ตรวจพบลดลงเล็กน้อยในปี 2024 แต่ภัยคุกคามนี้ยังคงมีอยู่

ฟิชชิง (Phishing): รูปแบบหนึ่งของวิศวกรรมสังคมที่ผู้โจมตีปลอมตัวเป็นแหล่งข้อมูลที่น่าเชื่อถือ มักจะผ่านทางอีเมลหรือแอปส่งข้อความ เพื่อหลอกผู้ใช้ให้เปิดเผยข้อมูลประจำตัวหรือข้อมูลที่ละเอียดอ่อน ฟิชชิงและวิศวกรรมสังคม (Social engineering) วิศวกรรมสังคมเป็นอีกหนึ่งการโจมตีทางไซเบอร์ที่พบบ่อยซึ่งส่งผลกระทบต่อธุรกิจ อาชญากรไซเบอร์ใช้อำนาจชักจูงพนักงานโดยการสร้างความไว้วางใจในการเข้าถึงข้อมูลสำคัญ

การโจมตีทางวิศวกรรมสังคมที่เกิดขึ้นบ่อยที่สุดคือการฟิชชิง ผู้กระทำการฟิชชิงปลอมตัวเป็นบริษัทที่มีชื่อเสียงและส่งข้อความถึงพนักงานเพื่อพยายามขโมยข้อมูลสำคัญ รหัสผ่าน และข้อมูลธนาคาร จากข้อมูลของ Z Scaler พบว่าความพยายามฟิชชิงเพิ่มขึ้น 58.2% ในปี 2023 และอุตสาหกรรมการเงินเป็นเป้าหมายหลักที่น่าสนใจคือการโจมตีฟิชชิงที่บันทึกไว้ทั้งหมดประมาณ 43% เป็นการเลียนแบบ Microsoft

แรนซัมแวร์ (Ransomware): มัลแวร์ชนิดหนึ่งที่เข้ารหัสไฟล์สำคัญและเรียกค่าไถ่ในการถอดรหัส การโจมตีด้วยแรนซัมแวร์อาจทำให้ข้อมูลสูญหายจำนวนมาก การดำเนินงานหยุดชะงัก และเกิดความเสียหายทางการเงิน แรนซัมแวร์เป็นมัลแวร์ประเภทหนึ่งที่มุ่งหมายบังคับให้ธุรกิจจ่ายเงินจำนวนหนึ่งเพื่อปลดล็อกไฟล์และข้อมูลในระบบ ภัยคุกคามทางไซเบอร์นี้เป็นรูปแบบหนึ่งของการกรรโชกทรัพย์และเป็นหนึ่งในการโจมตีทางไซเบอร์ที่มีค่าใช้จ่ายสูงที่สุดสำหรับธุรกิจ ข้อมูลจาก embroker.com ระบุว่า การโจมตีด้วยแรนซัมแวร์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องโดยเพิ่มขึ้นประมาณ 67% ในปี 2023

การโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed denial of service attacks หรือ DDoS)

การโจมตีแบบ DDoS กำลังเป็นประเด็นที่น่ากังวลมากขึ้นสำหรับธุรกิจในปี 2568 การโจมตีแบบ DDoS เกี่ยวข้องกับอาชญากรที่โจมตีเซิร์ฟเวอร์จนล้นด้วยทราฟฟิก ซึ่งอาจทำให้ระบบหยุดทำงาน วิธีนี้ช่วยให้แฮกเกอร์สามารถโจมตีช่องโหว่ต่างๆ ได้ ในช่วงไม่กี่ปีที่ผ่านมา การโจมตีแบบปฏิเสธการให้บริการแบบกระจายมีความถี่และความซับซ้อนเพิ่มขึ้นการโจมตีแบบ DDoS เพิ่มขึ้น 13% ในสองไตรมาสแรกของปี 2567 โดยมีเหตุการณ์เกิดขึ้นมากกว่า 8 ล้านครั้ง

ภัยคุกคามจากภายใน (Insider threats): การใช้สิทธิ์การเข้าถึงในทางที่ผิด ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ โดยผู้ใช้ที่ได้รับอนุญาต เช่น พนักงานหรือผู้รับเหมา ภัยคุกคามจากภายในถือเป็นความท้าทายอย่างยิ่ง เพราะมักเกิดจากข้อมูลประจำตัวที่ถูกต้องตามกฎหมาย

การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized access): ช่องโหว่ในการยืนยันตัวตนหรือการอนุญาตที่เปิดโอกาสให้ผู้ใช้ที่ไม่ได้รับอนุญาตสามารถเจาะระบบได้ รหัสผ่านที่อ่อนแอ MFA ที่ไม่มีประสิทธิภาพ และการควบคุมการเข้าถึงและความปลอดภัยที่ไม่ดี ล้วนเป็นปัจจัยที่ทำให้เกิดช่องโหว่นี้

การกำหนดค่าผิดพลาด (Misconfigurations): ข้อผิดพลาดในระบบคลาวด์หรือระบบภายในองค์กรที่สร้างช่องโหว่ที่ไม่พึงประสงค์ ข้อผิดพลาดอาจรวมถึงการตั้งค่าที่ไม่เหมาะสม พอร์ตที่เปิดอยู่ หรือการอนุญาตที่มากเกินไปจนเปิดเผยข้อมูลสำคัญ

ข้อผิดพลาดของมนุษย์ (Human error): การลบโดยไม่ตั้งใจ การใช้รหัสผ่านที่ไม่ถูกต้อง หรือการไม่ปฏิบัติตามนโยบายความปลอดภัย อาจทำให้ข้อมูลถูกเปิดเผยโดยไม่ตั้งใจได้เช่นกัน

ภัยพิบัติทางธรรมชาติ (Natural disasters) เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือไฟฟ้าดับ ซึ่งทำให้ศูนย์ข้อมูลไม่สามารถใช้งานได้และความยืดหยุ่นของข้อมูลลดลง

ภัยคุกคามเหล่านี้ทำให้เห็นชัดเจนถึงความจำเป็นในการจัดการความเสี่ยงเชิงรุก และกลยุทธ์การป้องกันแบบหลายชั้นที่ผสมผสานการตรวจจับ การป้องกัน และการแก้ไข

1.5 มุมมองจากผู้มีส่วนได้ส่วนเสียต่างๆ

มุมมองด้านความมั่นคงปลอดภัยไซเบอร์แตกต่างกันไปตามแต่ละกลุ่มผู้มีส่วนได้ส่วนเสีย โดยองค์กรเอกชนมุ่งเน้นการป้องกันความเสียหายทางธุรกิจและความน่าเชื่อถือ, รัฐบาลให้ความสำคัญกับการปกป้องข้อมูลและความมั่นคงของชาติ, ประชาชนทั่วไปต้องการความเป็นส่วนตัวและความปลอดภัยในการใช้เทคโนโลยี, ขณะที่นักวิชาการและผู้เชี่ยวชาญมุ่งเน้นการพัฒนาเทคโนโลยีและแนวทางการรับมือภัยคุกคามอย่างต่อเนื่อง สรุปได้ดังนี้

(1) มุมมองขององค์กรเอกชน

ความกังวลหลัก:

- การสูญเสียข้อมูลลูกค้าและความเชื่อมั่น
- การหยุดชะงักของการดำเนินธุรกิจ
- ค่าใช้จ่ายในการป้องกันและกู้คืน
- การปฏิบัติตามกฎระเบียบและกฎหมาย

กลยุทธ์การจัดการ:

- การลงทุนในเทคโนโลยีความปลอดภัย
- การฝึกอบรมพนักงาน
- การจัดทำแผนตอบสนองต่อเหตุการณ์
- การซื้อประกันภัยไซเบอร์

ตัวอย่างกรณีศึกษา:

- Equifax (2017): ข้อมูลส่วนบุคคลของลูกค้า 147 ล้านคนรั่วไหล ส่งผลให้บริษัทต้องจ่ายค่าปรับ 700 ล้านดอลลาร์สหรัฐ

(2) มุมมองของรัฐบาล

ความกังวลหลัก:

- ความมั่นคงแห่งชาติ
- การปกป้องโครงสร้างพื้นฐานที่สำคัญ
- การรักษาข้อมูลความลับของรัฐ
- การปกป้องประชาชน

นโยบายและมาตรการ:

- การจัดตั้งหน่วยงานความมั่นคงทางไซเบอร์
- การออกกฎหมายและระเบียบที่เกี่ยวข้อง
- การให้ความรู้และสร้างจิตสำนึกแก่ประชาชน
- ความร่วมมือระหว่างประเทศ

ตัวอย่างการดำเนินการในประเทศไทย:

- การจัดตั้งสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (DEPA)
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- การจัดตั้งสำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช. หรือ NCSA)
- การจัดตั้งสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.)

(3) มุมมองของประชาชน

ความกังวลหลัก:

- ความเป็นส่วนตัวของข้อมูลส่วนบุคคล
- การถูกหลอกลวงทางออนไลน์
- ความปลอดภัยในการทำธุรกรรมออนไลน์
- การเข้าถึงบริการออนไลน์อย่างปลอดภัย

พฤติกรรมและทัศนคติ:

- การใช้รหัสผ่านที่แข็งแกร่ง
- การระวังการแชร์ข้อมูลส่วนตัว
- การตรวจสอบความน่าเชื่อถือของเว็บไซต์
- การใช้ซอฟต์แวร์ป้องกันไวรัส

(4) มุมมองของนักวิชาการและผู้เชี่ยวชาญ

ความสนใจหลัก:

- การพัฒนาเทคโนโลยีความปลอดภัยใหม่
- การศึกษาพฤติกรรมของผู้โจมตี
- การวิเคราะห์ความเสี่ยงและผลกระทบ
- การพัฒนาหลักสูตรและการฝึกอบรม

ข้อเสนอแนะ:

- การใช้แนวทาง Defense in Depth
- การพัฒนาความตระหนักรู้ด้านความปลอดภัย
- การวิจัยและพัฒนาอย่างต่อเนื่อง
- การสร้างมาตรฐานและแนวปฏิบัติที่ดี

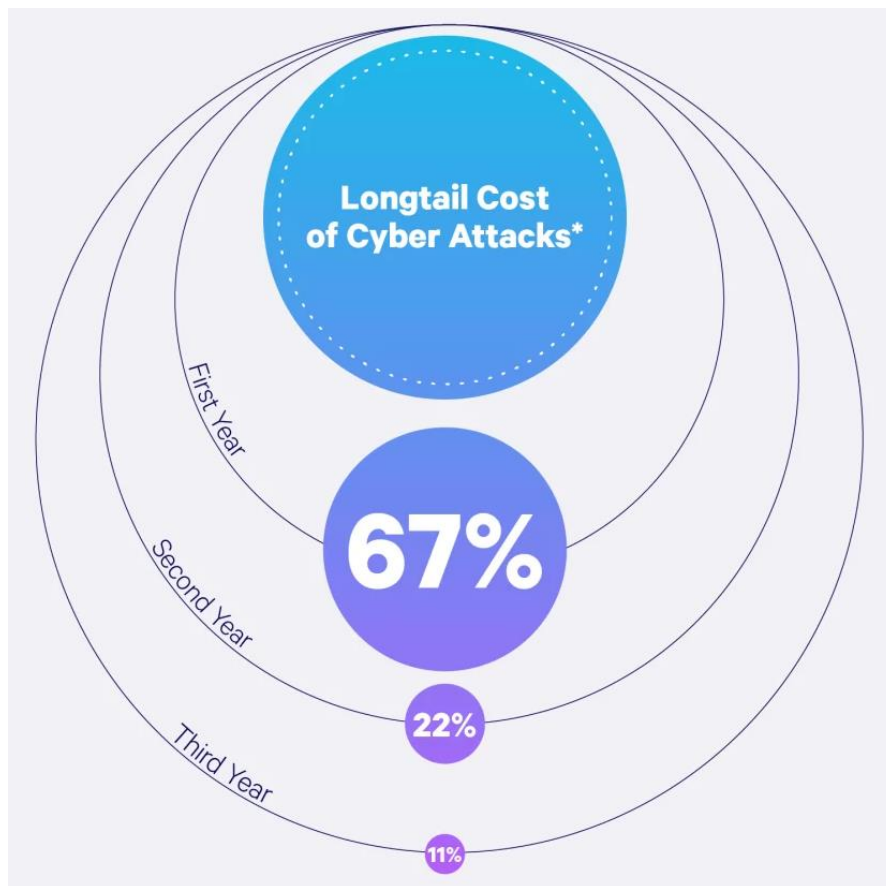
มุมมองความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ต้องอาศัยความร่วมมือและการมีส่วนร่วมจากทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และประชาชน การทำความเข้าใจและตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์จะช่วยให้เราสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยสำหรับทุกคน

1.6 ผลกระทบและความรุนแรงของการโจมตีทางไซเบอร์

การโจมตีทางไซเบอร์สามารถส่งผลกระทบต่อองค์กรได้หลายรูปแบบ ตั้งแต่การหยุดชะงักเล็กน้อยในการดำเนินงานไปจนถึงความสูญเสียทางการเงินครั้งใหญ่ ไม่ว่าจะเป็นการโจมตีจะเป็นประเภทใด ผลลัพธ์ที่ตามมาล้วนมีต้นทุนในรูปแบบใดรูปแบบหนึ่ง ไม่ว่าจะเป็นทางการเงินหรืออื่นๆ ผลกระทบจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์อาจยังคงส่งผลกระทบต่อธุรกิจของคุณในอีกไม่กี่สัปดาห์หรือหลายเดือนข้างหน้า สรุปประเด็นที่ธุรกิจอาจได้รับผลกระทบ ดังนี้

ต้นทุน ระยะยาวจากการละเมิดข้อมูลอาจกินเวลานานหลายเดือนถึงหลายปี และรวมถึงค่าใช้จ่ายจำนวนมากที่บริษัทต่างๆ ไม่ทราบหรือไม่ได้คาดการณ์ไว้ในวางแผน

ต้นทุนเหล่านี้รวมถึงข้อมูลที่สูญหาย การหยุดชะงักทางธุรกิจ การสูญเสียรายได้จากระบบหยุดทำงาน ค่าใช้จ่ายในการแจ้งเตือน หรือแม้แต่ความเสียหายต่อชื่อเสียงของแบรนด์ ในรูป 1.6 สรุปผลกระทบที่ธุรกิจอาจเผชิญตั้งแต่ปีแรกจนถึงปีที่ 3 ซึ่งรวมถึงต้นทุนของการสูญเสียข้อมูล การหยุดชะงักทางธุรกิจ การสูญเสียรายได้จากการหยุดทำงานของระบบ ต้นทุนการแจ้งเตือนและความเสียหายต่อชื่อเสียงของบริษัท และต้นทุนของลูกค้าที่สูญเสียไป



รูป 1.6 มูลค่าความเสียหายสรุปผลกระทบที่ธุรกิจอาจเผชิญตั้งแต่ปีแรกจนถึงปีที่ 3
(ที่มา: embroker.com)

การสูญเสียทางการเงิน ตามรายงานอาชญากรรมระหว่างประเทศของ FBI ชาวอเมริกันสูญเสียเงิน 12,300 ล้านดอลลาร์จากเหตุการณ์โจมตีทางไซเบอร์ในปี 2023 อาชญากรรมไซเบอร์และการละเมิดข้อมูลมีค่าใช้จ่ายสูงขึ้นเรื่อยๆ ในปี 2024 ค่าใช้จ่ายเฉลี่ยจากการละเมิดข้อมูลพุ่งสูงถึง 4.88 ล้านดอลลาร์สหรัฐ ซึ่งเป็นระดับสูงสุดเป็นประวัติการณ์ มีหลายวิธีที่บริษัทอาจสูญเสียเงินระหว่างเกิดภัยคุกคามทางไซเบอร์ เช่น การโจรกรรม ค่าปรับตามกฎหมาย ค่าใช้จ่ายด้านความรับผิด

การสูญเสียผลผลิต ผลกระทบที่เห็นได้ชัดที่สุดของการโจมตีทางไซเบอร์คือความสูญเสียทางการเงิน แต่ภัยคุกคามทางไซเบอร์ยังสามารถรบกวนการดำเนินธุรกิจทั่วไปของคุณ นำไปสู่การสูญเสียประสิทธิภาพการทำงาน มัลแวร์หรือการละเมิดความปลอดภัยที่สำคัญอาจทำให้บริษัทต้องหยุดการทำงานของระบบปฏิบัติการหลายระบบชั่วคราวเพื่อสอบสวนการโจมตี การหยุดทำงานนี้อาจนำไปสู่ความเสียหายต่อชื่อเสียง การสูญเสียลูกค้า และท้ายที่สุดคือกระแสเงินสดที่ลดลง

ความเสียหายต่อชื่อเสียง การโจมตีทางไซเบอร์อาจส่งผลกระทบต่อชื่อเสียงทางธุรกิจของเรา เมื่อเกิดการรั่วไหลของข้อมูลครั้งใหญ่ ลูกค้าอาจรู้สึกไม่มั่นใจในบริษัทของเรา ทำให้พวกเขาเก็บข้าวของและย้ายออกไป นอกจากนี้ เมื่อระบบภายในของบริษัทหยุดทำงานเป็นเวลานาน ราคาหุ้นก็อาจลดลง นี่คือนิสัยที่เกิดขึ้นจริงในเหตุการณ์ CrowdStrike IT ล่มเมื่อเร็วๆ นี้

ภัยคุกคามทางไซเบอร์อาจนำไปสู่การระงับทางการเงินทันที เช่น ค่าปรับและการจ่ายค่าเสียหาย อย่างไรก็ตาม ความเสียหายต่อชื่อเสียงอาจเป็นสิ่งที่แก้ไขได้ยากที่สุด

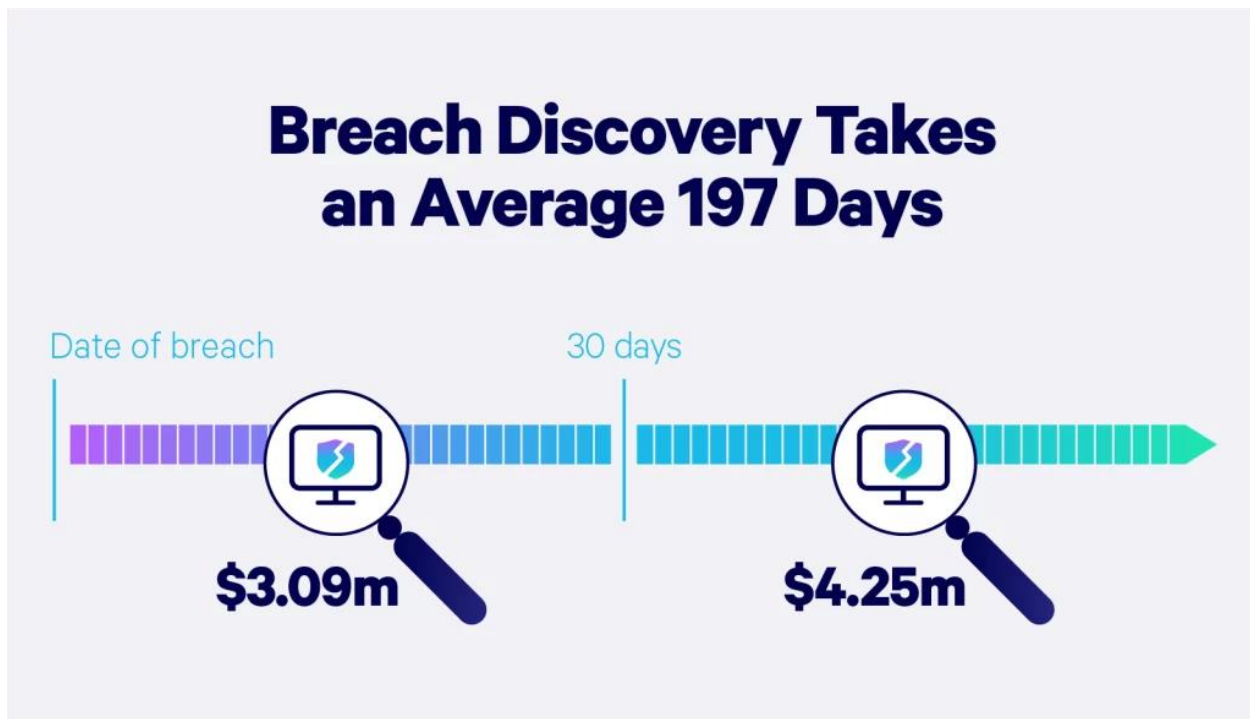
ความรับผิดทางกฎหมาย ผลกระทบสำคัญอีกประการหนึ่งที่สามารถเกิดขึ้นหลังจากการโจมตีทางไซเบอร์คือบทลงโทษทางกฎหมายและค่าปรับ หากองค์กรไม่ปฏิบัติตามมาตรการรักษาความปลอดภัยทางไซเบอร์ที่เหมาะสม และการขาดมาตรการดังกล่าวอาจนำไปสู่การโจมตีทางไซเบอร์หรือการละเมิดข้อมูล อาจถูกปรับองค์กรต้องเฝ้าระวังในการป้องกันความปลอดภัยทางไซเบอร์ และปฏิบัติตามขั้นตอนการรายงานเหตุการณ์เฉพาะเพื่อหลีกเลี่ยงบทลงโทษ

ตัวอย่างเช่น ในปี 2024 Intercontinental Exchange ถูกปรับ 10 ล้านดอลลาร์เนื่องจากการละเมิดกฎการรายงานการละเมิดข้อมูล เช่นเดียวกับในประเทศไทย สคส. ได้ประกาศต่อสาธารณะถึงบทปรับที่เกิดจากเหตุรั่วไหลข้อมูลส่วนบุคคลในปี 2568 รวมกันสูงถึง 21.6 ล้านบาท สำหรับ 8 กรณีที่มีการรั่วไหลข้อมูลส่วนบุคคลของหน่วยงานภาครัฐและเอกชน

ปัญหาความต่อเนื่องทางธุรกิจ การวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เป็นหนึ่งในขั้นตอนสำคัญที่สุดที่ธุรกิจสามารถดำเนินการได้เพื่อรับมือกับการโจมตีทางไซเบอร์ ซึ่งช่วยให้บริษัทสามารถดำเนินงานพื้นฐานต่อไปได้แม้ในภาวะฉุกเฉิน เช่น ไฟฟ้าดับ ข้อมูลรั่วไหล และการโจมตีทางไซเบอร์ ปัญหาความต่อเนื่องทางธุรกิจนี้มีความสำคัญเพิ่มมากขึ้นในช่วงไม่กี่ปีที่ผ่านมา เนื่องด้วยแทบทุกสิ่งในโลกธุรกิจกำลังก้าวเข้าสู่ยุคดิจิทัล แผนความต่อเนื่องทางธุรกิจจึงเป็นสิ่งสำคัญอย่างยิ่งยวดที่จะเป็นตัวกำหนดว่าบริษัทจะล้มเหลวหรือประสบความสำเร็จหลังจากเผชิญกับภัยคุกคามทางไซเบอร์ครั้งใหญ่

1.7 สถิติการค้นพบการละเมิดข้อมูล

“การค้นพบการละเมิด” หมายถึงช่วงเวลาที่บริษัทหรือธุรกิจทราบว่าเหตุการณ์เกิดขึ้น IBM ระบุว่าโดยเฉลี่ยแล้วบริษัทจะใช้เวลา 204 วันในการค้นพบการละเมิด และใช้เวลาถึง 73 วันในการควบคุม ดังรูป 1.7 นอกจากนี้ การใช้ AI ในระบบรักษาความปลอดภัยยังช่วยลดผลกระทบทางการเงินจากการโจมตีทางไซเบอร์ได้อย่างมาก บริษัทที่ใช้พีเจเออร์ AI ขั้นสูงสามารถค้นพบและควบคุมการละเมิดข้อมูลได้เร็วกว่าบริษัทที่ไม่ได้ใช้ถึง 108 วัน นอกจากนี้ การละเมิดข้อมูลยังทำให้บริษัทเหล่านี้สูญเสียเงินโดยเฉลี่ยน้อยกว่าถึง 1.76 ล้านดอลลาร์สหรัฐฯ



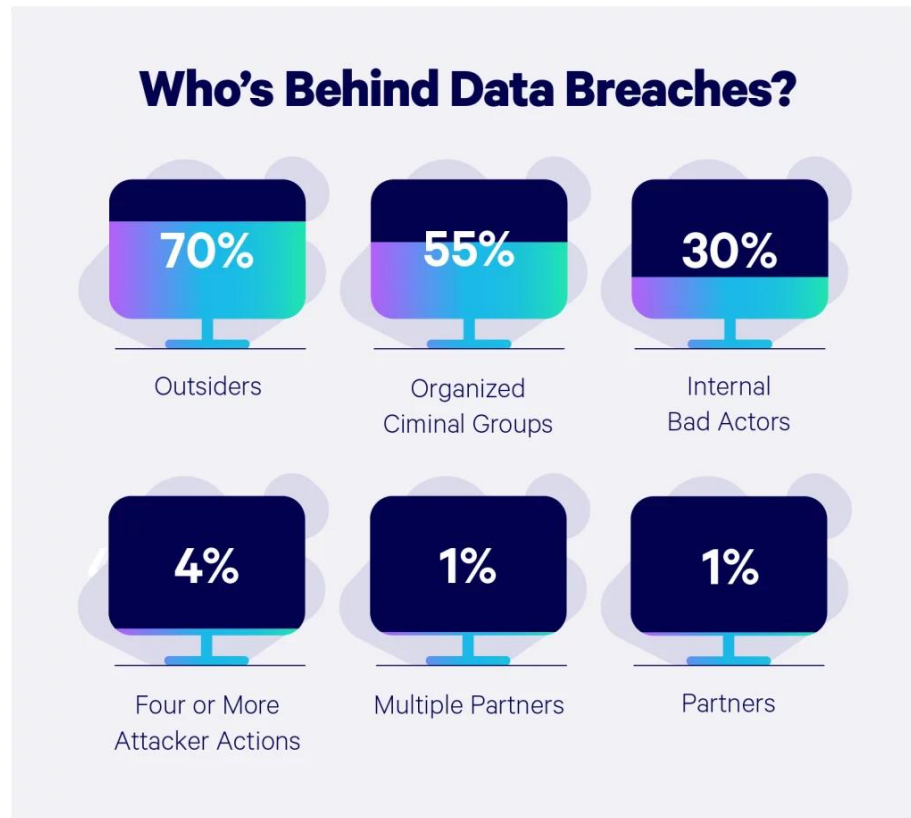
รูป 1.7 ประมาณการค่าเฉลี่ยความเสียหายที่เกิดขึ้นจากการค้นพบว่าการละเมิดข้อมูล
(ที่มา: embroker.com)

บริษัทที่ค้นพบและควบคุมการละเมิดข้อมูลได้ภายในเวลาไม่ถึง 200 วัน ประหยัดค่าใช้จ่ายได้มากกว่า 1 ล้านดอลลาร์สหรัฐฯ เมื่อเทียบกับบริษัทที่ใช้เวลามากกว่า 200 วัน การตอบสนองที่ล่าช้าต่อการละเมิดข้อมูลอาจสร้างปัญหาให้กับบริษัทมากยิ่งขึ้น ซึ่งอาจส่งผลให้สูญเสียความไว้วางใจจากลูกค้า ประสิทธิภาพการทำงาน หรือค่าปรับจำนวนมาก

จากรายงานการสืบสวนการละเมิดข้อมูลของ Verizon พบว่าการโจมตีทางไซเบอร์ส่วนใหญ่เกิดจากบุคคลภายนอก บุคคลภายใน พันธมิตรของบริษัท กลุ่มอาชญากรรม และกลุ่มที่เกี่ยวข้อง สามารถแบ่งสัดส่วนของแต่ละกรณีดังนี้ รูป 1.8

65% จากภายนอก (กลุ่มอาชญากรที่ได้รับการสนับสนุนจากรัฐ)

35% ภายใน (พนักงาน คู่ค้า ฯลฯ)



รูป 1.8 สัดส่วนผู้โจมตีจนเป็นให้ข้อมูลรั่วไหล
(ที่มา: embroker.com)

1.8 ประเภทของการรักษาความปลอดภัยข้อมูล

องค์กรต่างๆ ใช้มาตรการรักษาความปลอดภัยข้อมูลที่หลากหลายเพื่อปกป้องข้อมูลที่ละเอียดอ่อนตลอดวงจรชีวิตข้อมูล ได้แก่ การเข้ารหัสข้อมูล การลบข้อมูล การปกปิดข้อมูล และความยืดหยุ่นของข้อมูล

การเข้ารหัสข้อมูล (Data encryption)

การเข้ารหัสใช้อัลกอริทึมในการแปลงข้อมูลที่สามารถอ่านได้ (ข้อความธรรมดา) ให้เป็นรูปแบบที่อ่านไม่ได้ (ข้อความเข้ารหัสหรือข้อความไซเฟอร์) อัลกอริทึมนี้ช่วยปกป้องข้อมูลสำคัญทั้งในระหว่างการส่งและขณะจัดเก็บ เครื่องมือรักษาความปลอดภัยสำหรับการเข้ารหัสมักประกอบด้วยความสามารถในการจัดการคีย์และการควบคุมการถอดรหัส เพื่อให้มั่นใจว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

การลบข้อมูล (Data erasure)

การลบข้อมูลอย่างปลอดภัยช่วยให้มั่นใจได้ว่าข้อมูลจะถูกเขียนทับอย่างสมบูรณ์และไม่สามารถกู้คืนได้ โดยเฉพาะอย่างยิ่งเมื่อเลิกใช้อุปกรณ์จัดเก็บข้อมูล เทคนิคนี้จะเสียค่ามากกว่าการลบข้อมูลทั่วไป และช่วยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหลังจากการกำจัด

การปกปิดข้อมูล (Data masking)

การปกปิดข้อมูลเป็นการอำพรางบดบังองค์ประกอบข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคล หรือหมายเลขบัตรเครดิต โดยการแทนที่ด้วยข้อมูลสมมติแต่มีโครงสร้างคล้ายคลึงกัน วิธีนี้ช่วยให้นักพัฒนาและผู้ทดสอบสามารถทำงานกับชุดข้อมูลแบบเดียวกับการใช้งานจริงได้โดยไม่ละเมิดกฎระเบียบด้านความเป็นส่วนตัว

ความยืดหยุ่นของข้อมูล (Data resiliency)

มาตรการความยืดหยุ่นของข้อมูลช่วยสนับสนุนความสามารถขององค์กรในการกู้คืนข้อมูลจากเหตุการณ์ต่างๆ ได้อย่างรวดเร็ว ไม่ว่าจะเป็นการโจมตีทางไซเบอร์ความล้มเหลวของฮาร์ดแวร์ หรือภัยพิบัติทางธรรมชาติ การรับรองความพร้อมในการสำรองข้อมูลและความซ้ำซ้อนเป็นกุญแจสำคัญในการลดระยะเวลาหยุดทำงานให้น้อยที่สุด

1.9 กลยุทธ์การรักษาความมั่นคงปลอดภัยข้อมูล

การรักษาความปลอดภัยของข้อมูล คือ กระบวนการธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้ข้อมูล กลยุทธ์ด้านความปลอดภัยข้อมูลที่แข็งแกร่งจะผสมผสานรวมเทคโนโลยีความปลอดภัยเข้ากับกระบวนการขององค์กร โดยผนวกกระบวนการรักษาข้อมูลเข้ากับกระบวนการทำงานประจำวัน องค์กรประกอบของกลยุทธ์ด้านความปลอดภัยข้อมูลที่มีประสิทธิภาพประกอบด้วย:

- การรักษาความปลอดภัยทางกายภาพ (Physical security)
- การจัดการการเข้าถึงและการระบุตัวตน (Access and identity management)
- การแก้ไขแพตช์แอปพลิเคชันและช่องโหว่ (Application patching and vulnerability fixes)
- การสำรองข้อมูลและการกู้คืนข้อมูล (Data backup and recovery)
- การฝึกอบรมและการสร้างความตระหนักรู้แก่พนักงาน (Employee training and awareness)
- ความปลอดภัยของจุดสิ้นสุดและเครือข่าย (Endpoint and network security)

การรักษาความปลอดภัยทางกายภาพ

องค์กรต่างๆ มักจำเป็นต้องปกป้องทั้งสินทรัพย์ดิจิทัลและสินทรัพย์ทางกายภาพ ไม่ว่าจะเป็นการดำเนินงานศูนย์ข้อมูลหรือการสนับสนุนการนำอุปกรณ์ส่วนตัวมาใช้ (BYOD) สิ่งสำคัญคือสถานที่ต่างๆ จะต้องได้รับการรักษาความปลอดภัยจากการบุกรุก และติดตั้งอุปกรณ์ป้องกันสิ่งแวดล้อม เช่น ระบบดับเพลิงและการควบคุมอุณหภูมิ

การจัดการการเข้าถึงและการระบุตัวตน

ดัชนี IBM X-Force 2025 Threat Intelligence Index พบว่าการโจมตีโดยใช้ข้อมูลประจำตัวคิดเป็น 30% ของการบุกรุกทั้งหมดหลักการสิทธิ์ขั้นต่ำ (Least Privilege) ซึ่งให้สิทธิ์ผู้ใช้เฉพาะที่จำเป็นต่อการปฏิบัติงาน มักถูกนำมาใช้กับระบบต่างๆ เพื่อช่วยจำกัดการเข้าถึงตามบทบาทของผู้ใช้ การตรวจสอบสิทธิ์อย่างสม่ำเสมอช่วยลดความเสี่ยงของการละเมิดสิทธิ์ได้อีกด้วย

การแก้ไขแพตช์แอปพลิเคชันและช่องโหว่

แอปที่มีความเสี่ยงอาจเป็นเป้าหมายที่น่าสนใจสำหรับผู้โจมตี การโจมตีใช้ประโยชน์จากแอปพลิเคชันที่เผยแพร่สู่สาธารณะ การอัปเดตแอปพลิเคชันให้ทันสมัยอยู่เสมอและนำแนวทางปฏิบัติในการพัฒนาที่ปลอดภัยมาใช้ จะช่วยลดความเสี่ยงจากช่องโหว่ที่ทราบแล้วและภัยคุกคามใหม่ๆ ที่เกิดขึ้น

การสำรองข้อมูลและการกู้คืนข้อมูล

กลยุทธ์การสำรองข้อมูลมักประกอบด้วยการคัดลอกข้อมูลแบบกระจายตามพื้นที่ทางภูมิศาสตร์และแบบซ้ำซ้อนโดยเจตนา การเข้ารหัสอาจใช้เพื่อรักษาความปลอดภัยของข้อมูลสำรอง และโดยทั่วไปจะมีการทดสอบโปรโตคอลการกู้คืนเพื่อให้มั่นใจถึงความทนทานเมื่อเผชิญกับการโจมตีของแรนซัมแวร์หรือภัยพิบัติทางธรรมชาติ กฎการสำรองข้อมูล 3-2-1 Backup Rule ยังพึงกระทำตามอย่างสม่ำเสมอ

การฝึกอบรมและการสร้างความตระหนักรู้แก่พนักงาน

มนุษย์อาจเป็นปัจจัยเสี่ยงสำคัญในกลยุทธ์ด้านความปลอดภัยใดๆ ก็ตาม หลายองค์กรได้นำการฝึกอบรมเกี่ยวกับฟิชชิ่ง การใช้งาน MFA ความเป็นส่วนตัวของข้อมูล และการใช้งานอุปกรณ์เคลื่อนที่และแอปพลิเคชันอย่างปลอดภัย มาใช้เพื่อช่วยลดโอกาสเกิดวิศวกรรมสังคมและความผิดพลาดของมนุษย์

ความปลอดภัยปลายทาง เครือข่าย และคลาวด์

แนวทางที่ครอบคลุมสำหรับการรักษาความปลอดภัยบนคลาวด์อาจรวมถึงการตรวจสอบและจัดการอุปกรณ์ปลายทางเช่น แล็ปท็อปและอุปกรณ์พกพา เครื่องมือป้องกันการสูญหายของข้อมูล ไฟร์วอลล์ และซอฟต์แวร์ป้องกันไวรัส สามารถใช้เพื่อปกป้องข้อมูลสำคัญแบบเรียลไทม์

นอกจากนั้น มาตรการต่อไปนี้จะมีส่วนสนับสนุนการรักษาความมั่นคงปลอดภัยข้อมูลได้

ลดการถ่ายโอนข้อมูล

การถ่ายโอนข้อมูลระหว่างอุปกรณ์ธุรกิจและอุปกรณ์ส่วนตัวมักเป็นสิ่งที่หลีกเลี่ยงไม่ได้ เนื่องจากจำนวนพนักงานที่ทำงานจากระยะไกลที่เพิ่มขึ้น การเก็บรักษาข้อมูลสำคัญไว้ในอุปกรณ์ส่วนตัวจึงเพิ่มความเสี่ยงต่อการโจมตีทางไซเบอร์อย่างมาก

ดาวนโหลดอย่างระมัดระวัง

การดาวนโหลดไฟล์จากแหล่งที่ไม่ผ่านการตรวจสอบอาจทำให้ระบบและอุปกรณ์ของคุณมีความเสี่ยงด้านความปลอดภัย สิ่งสำคัญคือต้องดาวนโหลดไฟล์จากแหล่งที่รู้จัก และหลีกเลี่ยงการดาวนโหลดที่ไม่จำเป็นเพื่อลดความเสี่ยงที่อุปกรณ์ของเราจะติดมัลแวร์

ปรับปรุงความปลอดภัยของรหัสผ่าน

ความแข็งแกร่งของรหัสผ่านคือแนวป้องกันด่านแรกจากการโจมตีหลากหลายรูปแบบ การใช้สตริงสัญลักษณ์ที่ไม่มีความหมาย การเปลี่ยนรหัสผ่านเป็นประจำ และการไม่จดบันทึกหรือแบ่งปันรหัสผ่าน ล้วนเป็นสิ่งสำคัญอย่างยิ่งต่อการปกป้องข้อมูลสำคัญ พึงดำเนินการตามคำแนะนำเกี่ยวกับรหัสผ่านของ NIST Cybersecurity framework (CSF2.0) อย่างใกล้ชิด

อัปเดตซอฟต์แวร์อุปกรณ์

ผู้ให้บริการซอฟต์แวร์ทำงานอย่างหนักเพื่อให้ซอฟต์แวร์ของตนมีความปลอดภัยมากขึ้นอย่างต่อเนื่อง และการติดตั้งอัปเดตล่าสุดหรือการอัปเดตแพตช์เป็นประจำจะทำให้อุปกรณ์ของคุณเสี่ยงต่อการถูกโจมตีน้อยลง

ตรวจสอบการรั่วไหลของข้อมูล

การตรวจสอบข้อมูลของเราอย่างสม่ำเสมอและการระบุการรั่วไหลที่มีอยู่จะช่วยลดผลกระทบที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูลในระยะยาว เครื่องมือตรวจสอบการละเมิดข้อมูลจะตรวจสอบและแจ้งเตือนเกี่ยวกับกิจกรรมที่น่าสงสัยอยู่เสมอ

พัฒนาแผนตอบสนองต่อการละเมิด

การละเมิดข้อมูลสามารถเกิดขึ้นได้แม้กระทั่งกับบริษัทที่ระมัดระวังและมีวินัยมากที่สุด การวางแผนอย่างเป็นทางการเพื่อจัดการกับเหตุการณ์การละเมิดข้อมูลที่อาจเกิดขึ้นแผนรับมือทางไซเบอร์เบื้องต้นและแผนกู้คืนจากอาชญากรรมทางไซเบอร์จะช่วยให้องค์กรทุกขนาดสามารถรับมือกับการโจมตีที่เกิดขึ้นจริงและควบคุมความเสียหายที่อาจเกิดขึ้นได้

จะเห็นได้ชัดว่าธุรกิจต่างๆ เผชิญกับภัยคุกคามจากอาชญากรรมไซเบอร์อย่างต่อเนื่องและจำเป็นต้องดำเนินการมาตรการเพื่อปกป้องข้อมูล อย่ารอจนสายเกินไป ลงมือทำตั้งแต่วันนี้เพื่อป้องกันการละเมิดข้อมูลในอนาคต

และผลกระทบที่จะตามมา เช่นเดียวกับความจำเป็นในการมีประกันภัยความรับผิดชอบทางไซเบอร์ที่เหมาะสม การปกป้องข้อมูลที่เพียงพอจึงเป็นสิ่งสำคัญ

1.10 แนวโน้มความปลอดภัยของข้อมูล

ภูมิทัศน์ของการปกป้องข้อมูลกำลังเปลี่ยนแปลงอย่างต่อเนื่อง แนวโน้มปัจจุบันประกอบด้วย

AI และระบบอัตโนมัติ

ปัญญาประดิษฐ์ (AI) ช่วยเพิ่มความสามารถของระบบรักษาความปลอดภัยข้อมูลในการตรวจจับความผิดปกติ ตอบสนองอัตโนมัติ และวิเคราะห์ชุดข้อมูลขนาดใหญ่ ได้อย่างรวดเร็ว อัลกอริทึมอัตโนมัติรองรับทุกอย่าง ตั้งแต่การจำแนกประเภทไปจนถึงการแก้ไข ช่วยลดภาระงานที่ต้องทำด้วยมือ เนื้อหารายละเอียดจะปรากฏในบทท้าย

การรักษาความปลอดภัยแบบมัลติคลาวด์

เมื่อองค์กรต่างๆ หันมาใช้กลยุทธ์ที่ให้ความสำคัญกับระบบคลาวด์เป็นหลัก ความต้องการนโยบายที่สอดคล้องกันระหว่างผู้ให้บริการจึงเพิ่มมากขึ้น โดยเฉพาะ Cloud First Policy นโยบายภาครัฐ ทำให้สภาพแวดล้อมระบบคลาวด์ต้องได้รับการรักษาความปลอดภัยด้วยการมองเห็นแบบรวมศูนย์ การควบคุมอัตโนมัติ และการจัดการคีย์ที่แข็งแกร่ง

การประมวลผลควอนตัม

แม้ว่าการประมวลผลควอนตัมจะยังอยู่ในช่วงเริ่มต้น แต่ก็เป็นที่กังวลและความท้าทาย อัลกอริทึมการเข้ารหัสแบบดั้งเดิมอาจเสี่ยงต่อการโจมตีแบบควอนตัม ซึ่งกระตุ้นให้เกิดนวัตกรรมในการเข้ารหัสหลังควอนตัม รายละเอียดจะอยู่ในบทสุดท้าย

สถาปัตยกรรมดาต้าความปลอดภัย

สภาพแวดล้อมแบบกระจายอำนาจและไดนามิกกำลังผลักดันองค์กรต่างๆ ไปสู่สถาปัตยกรรมที่การระบุตัวตน บริบท และการบังคับใช้นโยบายปฏิบัติตามข้อมูล ไม่ใช่ขอบเขต

การนำระบบ Zero Trust มาใช้

โมเดลความปลอดภัย แบบ Zero Trust ถือว่าไม่มีผู้ใช้หรือระบบใดที่น่าเชื่อถือโดยเนื้อแท้ การเข้าถึงจะได้รับการตรวจสอบอย่างต่อเนื่อง และมีการอนุญาตสิทธิ์แบบไดนามิกตามระดับความเสี่ยง

1.12 สรุปบท

ท้ายที่สุดแล้ว การรักษาความมั่นคงปลอดภัยข้อมูลที่มีประสิทธิภาพต้องอาศัยการผสมผสานระหว่างกลยุทธ เทคโนโลยี และวัฒนธรรมองค์กร ตั้งแต่การรักษาความปลอดภัยอุปกรณ์ปลายทางและการเข้ารหัสข้อมูล ไปจนถึงการปฏิบัติตามกฎระเบียบความเป็นส่วนตัวเป็นส่วนตัวระดับโลก องค์กรที่ฝังแนวปฏิบัติด้านความปลอดภัยของข้อมูลไว้ในโครงสร้างดิจิทัลของตนจะมีความพร้อมมากขึ้นในการรับมือกับภัยคุกคามและสร้างความไว้วางใจในโลกยุคปัจจุบันที่ขับเคลื่อนด้วยข้อมูล

ความมั่นคงทางไซเบอร์เป็นประเด็นที่มีความซับซ้อนและมีผลกระทบอย่างกว้างขวางในยุคดิจิทัล การทำความเข้าใจเกี่ยวกับความหมาย วิวัฒนาการของภัยคุกคาม มุมมองของผู้มีส่วนได้ส่วนเสียต่างๆ และผลกระทบที่เกิดขึ้น จะช่วยให้เราสามารถเตรียมพร้อมและจัดการกับความท้าทายเหล่านี้ได้อย่างมีประสิทธิภาพ

การศึกษาความมั่นคงทางไซเบอร์ต้องมีการบูรณาการความรู้จากหลายศาสตร์ ทั้งด้านเทคนิค กฎหมาย เศรษฐศาสตร์ จิตวิทยา และสังคมศาสตร์ เพื่อให้เกิดความเข้าใจที่ครอบคลุมและสามารถนำไปประยุกต์ใช้ได้จริงในการทำงาน

แนวโน้มในอนาคต การโจมตีทางไซเบอร์มีแนวโน้มที่จะเพิ่มความซับซ้อนและรุนแรงมากขึ้น อาชญากรไซเบอร์ใช้เทคโนโลยีใหม่ๆ เช่น AI ในการโจมตี ความเสี่ยงจากการทำงานระยะไกล: การทำงานจากที่บ้าน หรือการใช้เครือข่ายส่วนตัวอาจเป็นช่องโหว่ที่ทำให้เกิดการโจมตี ความเสี่ยงด้านความปลอดภัยของข้อมูลบนคลาวด์ การย้ายข้อมูลไปยังคลาวด์ โดยไม่มีการเข้ารหัส หรือการตรวจสอบสิทธิ์ที่เหมาะสม อาจเป็นช่องโหว่

การป้องกันและการรับมือ การลงทุนในเทคโนโลยีและมาตรการความปลอดภัยทางไซเบอร์ การใช้เทคโนโลยีที่ทันสมัย การฝึกอบรมพนักงาน และการสร้างระบบความปลอดภัยที่แข็งแกร่งเป็นสิ่งจำเป็น การสร้างความตระหนักรู้ การให้ความรู้แก่ประชาชนและพนักงานเกี่ยวกับความเสี่ยงและวิธีการป้องกันการโจมตีทางไซเบอร์ การร่วมมือและการแลกเปลี่ยนข้อมูล การร่วมมือกันระหว่างภาครัฐ ภาคเอกชน และองค์กรระหว่างประเทศ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ การเตรียมความพร้อมสำหรับเหตุการณ์ทางไซเบอร์ การมีแผนรับมือเหตุฉุกเฉิน และการฝึกซ้อมรับมือกับสถานการณ์ต่างๆ

1.13 บทวิเคราะห์และมุมมองเชิงวิชาการ : หลักการความมั่นคงปลอดภัยทางไซเบอร์

เมื่อวิเคราะห์ภูมิทัศน์ของความมั่นคงปลอดภัยทางไซเบอร์ทั้งในบริบทของโลกและประเทศแล้ว จะพบว่า การทำความเข้าใจ "ความมั่นคงปลอดภัยทางไซเบอร์" (Cybersecurity) ไม่ได้เป็นเพียงเรื่องของเทคนิคการป้องกันข้อมูลหรือระบบสารสนเทศเท่านั้น แต่ยังสะท้อนถึง องค์ความรู้เชิงสหวิทยาการ ที่ผสมผสานระหว่างเทคโนโลยี กฎหมาย มาตรฐานสากล จริยธรรม และยุทธศาสตร์ระดับประเทศและโลก เพื่อรับมือกับภัยคุกคามที่เปลี่ยนแปลงอย่างต่อเนื่อง จากเนื้อหาในบทนี้ สามารถวิเคราะห์สรุปสาระสำคัญได้ดังนี้

1.1 ความหมายของความมั่นคงทางไซเบอร์

1.1.1 ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัยทางไซเบอร์หมายถึงกระบวนการ มาตรการ และกลไกที่ใช้ในการ ปกป้องระบบคอมพิวเตอร์ เครือข่าย ข้อมูล และบริการดิจิทัล จากการเข้าถึงโดยไม่ได้รับอนุญาต การโจมตี การรั่วไหล และการถูกทำลาย ทั้งนี้รวมถึงการดำรงไว้ซึ่งการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน (CIA Triad: Confidentiality, Integrity, Availability) อีกด้วย

1.1.2 ความสำคัญของความมั่นคงของข้อมูลในยุคดิจิทัล

ในยุคดิจิทัล ข้อมูลถือเป็น “ทรัพย์สินเชิงกลยุทธ์” (Strategic Asset) ที่มีมูลค่าไม่ต่างจากพลังงานหรือทุนทางการเงิน การรั่วไหลข้อมูลหรือการสูญหายของข้อมูลเพียงเล็กน้อยอาจนำไปสู่ผลกระทบมหาศาล เช่น ความเสียหายทางเศรษฐกิจ การละเมิดสิทธิส่วนบุคคล เสื่อมเสียชื่อเสียง และการบ่อนทำลายความเชื่อมั่นของสังคม

1.1.3 องค์ประกอบของความมั่นคงของข้อมูล

องค์ประกอบหลักของความมั่นคงปลอดภัยข้อมูลหรือสารสนเทศ (Information Security) ได้แก่

- Confidentiality: รักษาความลับ ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- Integrity: รักษาความถูกต้องครบถ้วนของข้อมูล
- Availability: รักษาความพร้อมในการใช้งานเมื่อผู้มีสิทธิร้องขอ
- Accountability & Non-repudiation: การตรวจสอบย้อนกลับและการไม่สามารถปฏิเสธความรับผิดชอบ

1.1.4 ประเภทความมั่นคงปลอดภัยข้อมูล

- Physical Security: การป้องกันทรัพยากรด้านกายภาพ (ห้องเซิร์ฟเวอร์, อุปกรณ์)
- Network Security: การป้องกันการโจมตีเครือข่าย เช่น DDoS, Man-in-the-Middle
- Application Security: ป้องกันช่องโหว่ในซอฟต์แวร์ เช่น SQL Injection, XSS
- Data Security: การเข้ารหัสและการควบคุมสิทธิการเข้าถึงข้อมูล
- Operational Security (OPSEC): การจัดการกระบวนการเพื่อไม่ให้ข้อมูลรั่วไหลจากพฤติกรรมมนุษย์

1.2 มุมมองและผลกระทบความมั่นคงปลอดภัยทางไซเบอร์

1.2.1 มุมมองด้านความมั่นคงปลอดภัยข้อมูล

Cybersecurity ต้องถูกมองทั้งใน มิติเทคโนโลยี มิติองค์กร และมิติรัฐศาสตร์ เพราะภัยคุกคามทางไซเบอร์ไม่เพียงแต่โจมตีระบบสารสนเทศ แต่ยังคุกคามต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ

1.2.2 ผลกระทบความมั่นคงปลอดภัยทางไซเบอร์

- เศรษฐกิจ: ความเสียหายจากการโจมตี Ransomware, การโจรกรรมข้อมูล
- สังคม: การบิดเบือนข้อมูล (Disinformation) กระทบต่อความเชื่อมั่นของสาธารณชน
- ความมั่นคงรัฐ: การโจมตีโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เช่น พลังงาน ไฟฟ้า น้ำ การเงิน

1.2.3 ความเสี่ยงด้านความมั่นคงปลอดภัยและภัยคุกคามข้อมูล

- ภัยคุกคามภายนอก: แฮ็กเกอร์ อาชญากรไซเบอร์ กลุ่มก่อการร้ายไซเบอร์
- ภัยคุกคามภายใน: พนักงานที่ประมาทหรือเจตนาทุจริต
- เทคโนโลยีเกิดใหม่: AI-driven attack, Deepfake, Quantum threat

1.2.4 สถานการณ์ภัยคุกคามต่อความมั่นคงปลอดภัยข้อมูลในปัจจุบันและแนวโน้ม

- การโจมตีแบบ Ransomware-as-a-Service (RaaS) กำลังเติบโต
- State-sponsored attacks เพิ่มความซับซ้อนและมีเป้าหมายเชิงยุทธศาสตร์
- การโจมตีโครงสร้างพื้นฐานดิจิทัล (Critical Information Infrastructure Protection; CIIP) เช่น ระบบ Smart Grid, Smart City
- แนวโน้มการใช้ AI และ Machine Learning ทั้งในเชิงรุกและรับ

1.3 บทวิเคราะห์มุมมองและผลกระทบความมั่นคงปลอดภัยทางไซเบอร์

การวิเคราะห์ในเชิงวิชาการสะท้อนว่า ความมั่นคงปลอดภัยทางไซเบอร์ไม่ใช่เพียงปัญหาทางเทคนิค แต่เป็นปัญหายุทธศาสตร์ระดับโลก ซึ่งเกี่ยวข้องกับอธิปไตยดิจิทัล (Digital Sovereignty) และความสามารถในการปกป้องโครงสร้างพื้นฐานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Infrastructure) โดยประเด็นที่สำคัญ ได้แก่:

- การเปลี่ยนแปลงเชิงภูมิรัฐศาสตร์ (Geopolitics): การใช้ Cyber warfare เป็นเครื่องมือทางการทหารและการทูต
- เศรษฐกิจดิจิทัล (Digital Economy): ประเทศที่ไม่สามารถรับประกันความมั่นคงปลอดภัยทางไซเบอร์ได้ จะเสียเปรียบในตลาดโลก

- สิทธิและความเป็นส่วนตัวของพลเมือง: การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA, GDPR) สะท้อนว่าความมั่นคงปลอดภัยไซเบอร์เชื่อมโยงกับหลักของสิทธิมนุษยชน
- ความจำเป็นของมาตรการรับมือกับภัยคุกคามไซเบอร์ได้อย่างยืดหยุ่น (Cyber Resilience): ไม่เพียงแต่ป้องกัน แต่จำเป็นต้องมีความสามารถในการฟื้นตัว (Recovery) และปรับตัว (Adaptation)

กล่าวโดยสรุป ความมั่นคงปลอดภัยทางไซเบอร์คือแกนกลางของการพัฒนาดิจิทัลและความมั่นคงแห่งชาติ การวิจัยและพัฒนาองค์ความรู้ในมิตินี้จึงต้องบูรณาการ ศาสตร์ทางเทคนิค การจัดการ และนโยบายสาธารณะ เพื่อสร้างสมดุลระหว่าง นวัตกรรม ความปลอดภัย และสิทธิของประชาชน

แบบทดสอบท้ายบท

ข้อสอบอัตนัย 5 ข้อ (สอดคล้องวัตถุประสงค์)

อัตนัย 1 (วัตถุประสงค์ 1): อธิบาย CIA Triad พร้อมยกตัวอย่างผลกระทบเมื่อมิติใดมิติหนึ่งเสียหาย ในบริบท Tele-Clinic

แนวคำตอบ: C—ข้อมูลเวชระเบียนรั่วไหลกระทบความเป็นส่วนตัว, I—สั่งยา/เวชระเบียนถูกแก้ไขผิดทำให้รักษาคลาดเคลื่อน, A—ระบบล่มทำให้ผู้ป่วยเข้าไม่ถึงบริการ ฯลฯ

อัตนัย 2 (วัตถุประสงค์ 2-5): จง mapping Security Services

(เช่น Confidentiality/Integrity/Availability/Authentication/Access Control/Non-repudiation) เข้ากับ NIST CSF Functions อย่างน้อย 1 มาตรการต่อเซลล์ พร้อมเหตุผล

แนวคำตอบ (ตัวอย่างบางส่วน):

Confidentiality→Protect: Encryption, DLP; →Identify: Data classification; →Detect: DLP alert; →Respond: IR playbook for data leak; →Recover: Key rotation... ฯลฯ

อัตนัย 3 (วัตถุประสงค์ 3): วิเคราะห์ภัยคุกคาม 3 ประเภท (เช่น Phishing, Ransomware, DDoS) ต่อ Tele-Clinic ระบุ กลไกการเกิด-ผลกระทบ-ตัวชี้วัด

แนวคำตอบ: Phishing→ขโมยบัญชี→การเข้าถึง PHI; Ransomware→เข้ารหัสไฟล์→หยุดบริการ, เสียหายทางการเงิน; DDoS→ระบบนัดหมายล่ม→A ลดลง; KPI: CTR ของ phishing, MTTD/MTTR, uptime, RPO/RTO ฯลฯ

อัตนัย 4 (วัตถุประสงค์ 4): เสนอ Defense-in-Depth 5 ชั้นสำหรับ Tele-Clinic โดยเชื่อมโยงกับ X.800 และ CSF

แนวคำตอบ: ชั้นอุปกรณ์/เครือข่าย (FW/IDS/IPS/DDoS), ชั้นเอนด์พอยต์ (EDR/AV), ชั้นข้อมูล (encryption/backup 3-2-1), ชั้นอัตลักษณ์ (MFA/RBAC/least privilege), ชั้นกระบวนการ (IR/BCP/อบรม phishing) + mapping ไปยัง Identify/Protect/Detect/Respond/Recover ฯลฯ

อรรถนัย 5 (วัตถุประสงค์ 3–4): อธิบายผลกระทบและความคาดหวังของ **ผู้มีส่วนได้ส่วนเสีย** 3 กลุ่มเมื่อ Tele-Clinic ถูกโจมตี และมาตรการเยียวยาระยะสั้น/ยาว

แนวคำตอบ: เอกชน/องค์กร—ความต่อเนื่องธุรกิจ ชื่อเสียง; รัฐ—ความมั่นคงข้อมูล/กฎระเบียบ; ประชาชน—ความเป็นส่วนตัว/ความเชื่อมั่น; มาตรการ—สื่อสารโปร่งใส, แจ้งผู้ใช้, hardening/patch, MFA, IR/BCP, ทบทวนนโยบาย/อบรม ฯลฯ

ข้อสอบปรนัย 4 ตัวเลือก ให้เลือกคำตอบที่ถูกต้องที่สุดเพียงตัวเลือกเดียว (10 ข้อ)

ข้อ 1. ข้อใด ไม่ใช่ มิติใน CIA Triad

A) Confidentiality B) Integrity C) Accountability D) Availability

เฉลย: C (Accountability จัดอยู่กับเป้าหมายเสริม)

ข้อ 2. ข้อใดคือ บริการความมั่นคง ตาม X.800 A) Data masking B) Authentication C) Containerization D) Hash-map

เฉลย: B

ข้อ 3. ฟังก์ชัน Respond ใน NIST CSF สอดคล้องที่สุดกับข้อใด

A) การจำแนกข้อมูล B) แผนตอบสนองเหตุการณ์ (IR) C) การสำรองข้อมูล D) ระบบ DLP

เฉลย: B

ข้อ 4. ตัวอย่างผลกระทบที่กระทบ “A” ใน CIA คือ

A) ข้อมูลถูกดัดแปลง B) ระบบล่มใช้งานไม่ได้ C) รหัสผ่านถูกเปิดเผย D) ไม่สามารถพิสูจน์ตัวจริง

เฉลย: B

ข้อ 5. ใดต่อไปนี้เข้าข่าย Phishing

A) Botnet ส่งทราฟฟิกล่มเว็บ B) อีเมลปลอมหลอกให้กรอกรหัสผ่าน C) เข้ารหัสไฟล์เรียกค่าไถ่ D) เปิดพอร์ตฐานข้อมูลสาธารณะ

เฉลย: B

ข้อ 6. Ransomware ส่งผลกระทบต่องานมากที่สุด

A) C B) I C) A D) ทั้ง B และ C

เฉลย: D (กระทบ Integrity หากไฟล์ถูกแก้/สูญ และ Availability เพราะเข้าไม่ถึงไฟล์)

ข้อ 7. Least Privilege/RBAC มุ่งควบคุมบริการใด

A) Confidentiality และ Access control B) Non-repudiation C) Availability D) Backup

เฉลย: A

ข้อ 8. ตัวอย่างมาตรการในฟังก์ชัน Protect คือข้อใด

A) การจำแนกทรัพย์สินสารสนเทศ B) การทำ Forensics หลังเหตุ C) การเข้ารหัสและ MFA D) การทดสอบ BCP

หลังฟื้นตัว **เฉลย: C**

ข้อ 9. มุมมองผู้มีส่วนได้ส่วนเสีย: ประชาชน/ผู้ใช้บริการ กังวลหลักคือ

A) ROI ขององค์กร B) ความมั่นคงของรัฐ C) ความเป็นส่วนตัว/ความปลอดภัยในการใช้บริการ D) กฎระเบียบการรายงาน

เฉลย: C

ข้อ 10. สถานการณ์ทราฟฟิกเว็บพุ่งผิดปกติ กระทบมากสุดกับบริการใด

A) Authentication B) Confidentiality C) Availability D) Non-repudiation

เฉลย: C (ส่อ DDoS ทำให้ระบบใช้งานไม่ได้)

บรรณานุกรมท้ายบท

ศิริเชษฐ์ โพธิ์ทัญญู, ผศ.ดร. (มปป.) เอกสารคำสอน: ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์, รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.

สำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ – NCSA (2568). สถิติภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ ปี 2568. <https://www.ncsa.or.th/policy/threat-statistics>

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2566). รายงานสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ประเทศไทย ปี 2566. depa.

Anderson, R. (2021). Security Engineering (Chapters 1-2).

Center for Strategic and International Studies (CSIS). (2023). Economic Impact of Cybercrime: A Global Perspective.

Cybersecurity Ventures. (2023). Global Cybercrime Damages Report 2023.

European Union Agency for Cybersecurity (ENISA). (2023). Threat Landscape Report 2023.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

International Telecommunication Union. (n.d.). ITU-T X.800: Security Architecture for OSI.

ISO. (1989). ISO/IEC 7498-2:1989. Information Processing Systems – OSI Reference Model – Security Architecture.

Johnson, J. (1997). The Evolution of British Sigint: 1653–1939. Her Majesty's Stationery Office.

Larsen, D. (2019). Creating an American culture of secrecy: Cryptography in Wilson-era diplomacy. Diplomatic History. [URL]

McKinsey & Company. (2023). Digital Transformation in the Post-Pandemic Era. McKinsey Global Institute.

Ponemon Institute. (2023). State of Cybersecurity Report 2023.

Sebag-Montefiore, H. (2011). Enigma: The Battle for the Code (p. 576). Orion. ISBN 9781780221236.

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (Chapter 1).

Symantec Corporation. (2023). Internet Security Threat Report 2023. Broadcom Inc.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.

Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.

บทที่ 2

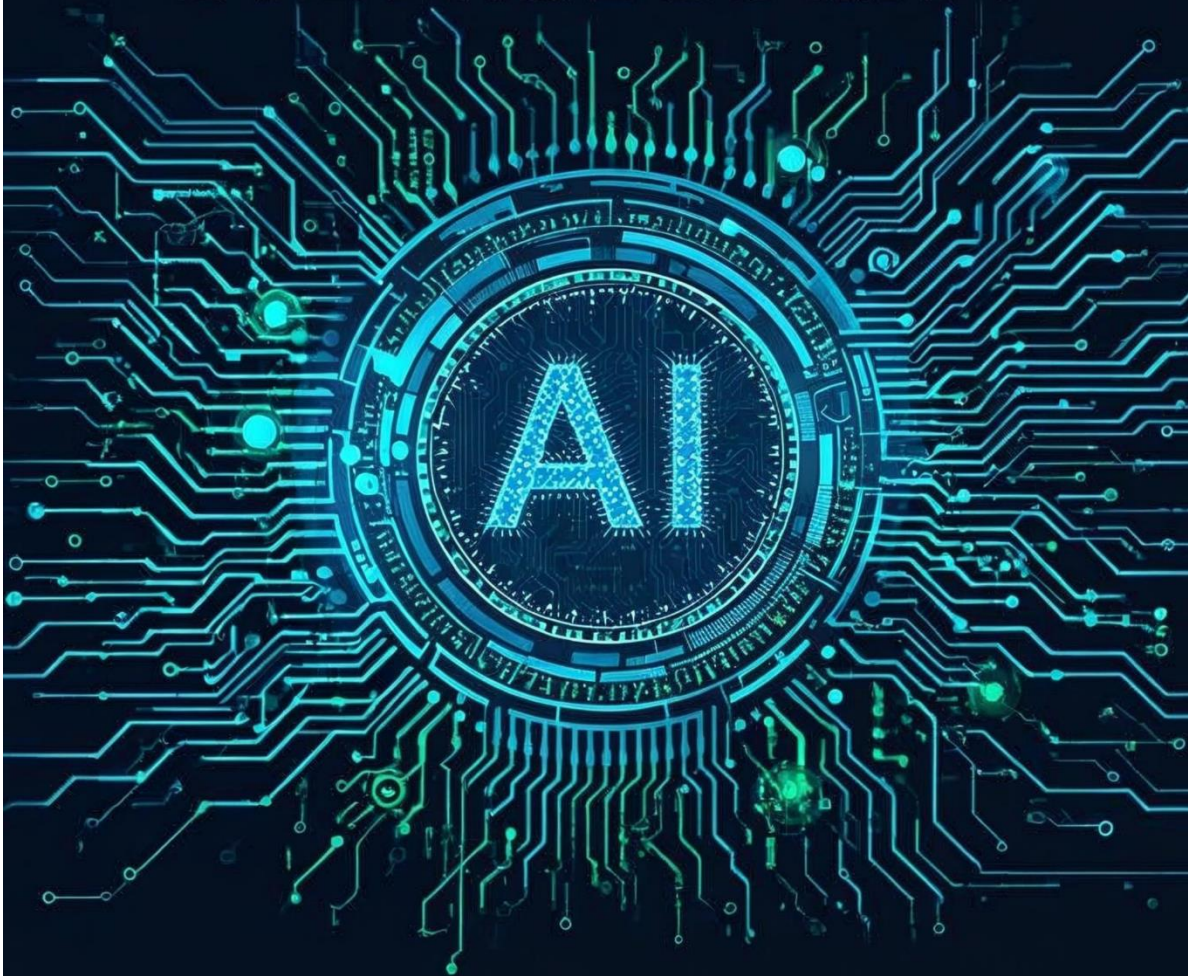
สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล

Architecture for Data Security

วิศวกรรมความมั่นคงปลอดภัยข้อมูล

ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพรธีรัตน์

บทที่ 2 สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล (Architecture for Data Security)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบหัวข้อนี้ นักศึกษาจะสามารถ:

- อธิบายโครงสร้างและองค์ประกอบของสถาปัตยกรรมความมั่นคงปลอดภัยตามแนวทาง OSI และ X.800 ได้ถูกต้อง
- จำแนกและอธิบายประเภทการโจมตีทางไซเบอร์ (Passive/Active Attacks) พร้อมยกตัวอย่างได้
- เชื่อมโยง Security Services เข้ากับ Security Mechanisms และ NIST CSF Functions ได้
- วิเคราะห์กรณีศึกษาและออกแบบมาตรการรักษาความมั่นคงปลอดภัยข้อมูลที่สอดคล้องกับมาตรฐานสากล
- ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อองค์กร พร้อมเสนอแผนควบคุมและการตอบสนองได้

2. จุดประสงค์การเรียนรู้ (Learning Objectives)

- เพื่อให้ผู้เรียนเข้าใจแนวคิด OSI Security Architecture และบริการด้านความมั่นคงปลอดภัยตามมาตรฐาน X.800
- เพื่อให้ผู้เรียนตระหนักถึงความสำคัญของ Security Services และสามารถเชื่อมโยงเข้ากับกลไกความปลอดภัย
- เพื่อให้ผู้เรียนเข้าใจโครงสร้างและฟังก์ชันของ NIST CSF 2.0 และสามารถประยุกต์ใช้ในสถานการณ์จริง
- เพื่อพัฒนาทักษะการวิเคราะห์ความเสี่ยงและออกแบบมาตรการควบคุมที่ครอบคลุมทั้งด้านเทคนิคและนโยบาย

3. หัวข้อการเรียนรู้

สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล

2.1 สถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทางของ OSI

2.1.1 การโจมตีด้านความปลอดภัย

2.1.2 บริการด้านความมั่นคงปลอดภัย

2.1.3 เป้าหมายของนโยบายด้านความมั่นคงปลอดภัย

2.2 แบบจำลองความมั่นคงปลอดภัยเครือข่าย

2.2.1 มาตรฐานด้านความมั่นคงปลอดภัย

2.2.2 กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST

2.2.3 กลไกและการตอบสนองต่อเหตุการณ์ตามแนวทาง NIST Cybersecurity Framework

2.2.4 บทวิเคราะห์เปรียบเทียบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์

2.3 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา: บริษัท RMUTT ThaiHealth Data Center ให้บริการเก็บและประมวลผลข้อมูลสุขภาพผ่านระบบ Cloud โดยมีปัญหาการโจมตีแบบ Phishing และ DoS นักศึกษาต้องวิเคราะห์และเสนอแนวทางแก้ไข

1) ระบุประเภทการโจมตีและจัดเป็น Passive หรือ Active Attack

2) วิเคราะห์ผลกระทบต่อ CIA Triad

3) เสนอ Security Services และ Mechanisms ที่เกี่ยวข้อง

4) Mapping Services → NIST CSF Functions

5) เสนอแนวทางตอบสนองและฟื้นฟูระบบ

เกณฑ์การประเมิน (Rubric 4 ระดับ)

เกณฑ์	ระดับ 4 (ยอดเยี่ยม)	ระดับ 3 (ดี)	ระดับ 2 (พอใช้)	ระดับ 1 (ควรปรับปรุง)
ความถูกต้องทางวิชาการ (30)	ครบถ้วน ถูกต้องตามกรอบ X.800/NIST	ถูกต้องส่วนใหญ่	มีข้อผิดพลาดบางส่วน	ไม่ตรงหลักวิชาการ

การวิเคราะห์ภัยคุกคามและ CIA (25)	วิเคราะห์ครบทั้ง 3 มิติ	ครบแต่ยังไม่ลึก	บางมิติเท่านั้น	ไม่ถูกต้อง
การออกแบบมาตรการ (30)	เสนอ control ครอบคลุม	ครอบคลุมบางส่วน	สอดคล้องบางส่วน	ไม่สอดคล้อง
การสื่อสาร/การนำเสนอ (15)	ชัดเจน ใช้แผนภาพ/ตาราง	ชัดเจน	พอใช้	ไม่ชัดเจน

2.1 สถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทางของ OSI

เพื่อประเมินความต้องการด้านความปลอดภัยขององค์กรอย่างมีประสิทธิภาพ รวมถึงประเมินและเลือกมาตรการและนโยบายด้านความปลอดภัยต่างๆ ผู้บริหารที่รับผิดชอบด้านความปลอดภัยของคอมพิวเตอร์และเครือข่ายจำเป็นต้องมีวิธีการที่เป็นระบบในการกำหนดข้อกำหนดด้านความปลอดภัยและกำหนดลักษณะวิธีการเพื่อตอบสนองความต้องการเหล่านั้น ในสภาพแวดล้อมการประมวลผลข้อมูลแบบรวมศูนย์ เรื่องนี้ค่อนข้างยากอยู่แล้ว แต่การใช้เครือข่ายท้องถิ่นและเครือข่ายบริเวณกว้างทำให้เกิดปัญหาต่างๆ ทวีความรุนแรงขึ้น ข้อเสนอแนะ X.800 ของ ITU-T เรื่องสถาปัตยกรรมความปลอดภัยสำหรับ OSI (OSI Security Architecture) ได้กำหนดแนวทางที่เป็นระบบดังกล่าว สถาปัตยกรรมความปลอดภัยของ OSI มีประโยชน์ต่อผู้จัดการในฐานะช่องทางหนึ่ง

คำแนะนำ X.800 ของ ITU-T เรื่องสถาปัตยกรรมความปลอดภัยสำหรับ OSI กำหนดแนวทางที่เป็นระบบดังกล่าว สถาปัตยกรรมความปลอดภัยของ OSI มีประโยชน์ต่อผู้บริหารในฐานะวิธีหนึ่งในการจัดระเบียบภารกิจในการรักษาความปลอดภัย นอกจากนี้ เนื่องจากสถาปัตยกรรมนี้ได้รับการพัฒนาให้เป็นมาตรฐานสากล ผู้จำหน่ายคอมพิวเตอร์และการสื่อสารจึงได้พัฒนาคุณลักษณะด้านความปลอดภัยสำหรับผลิตภัณฑ์และบริการของตน ซึ่งเกี่ยวข้องกับคำจำกัดความเชิงโครงสร้างของบริการและกลไกนี้

สถาปัตยกรรมความปลอดภัยของ OSI ให้ภาพรวมที่เป็นประโยชน์ แม้จะเป็นเพียงนามธรรม เกี่ยวกับแนวคิดต่างๆ ที่หนังสือเล่มนี้กล่าวถึง สถาปัตยกรรมความปลอดภัยของ OSI มุ่งเน้นไปที่การโจมตี กลไก และบริการด้านความปลอดภัย ซึ่งสามารถนิยามสั้นๆ ได้ว่า

การโจมตีด้านความปลอดภัย (Security Attack): การกระทำใดๆ ที่ก่อให้เกิดความเสี่ยงต่อความปลอดภัยของข้อมูลที่ต้องกรเป็นเจ้าของ

กลไกความปลอดภัย (Security Mechanism): กระบวนการ หรืออุปกรณ์ที่รวมกระบวนการดังกล่าวไว้ที่ออกแบบมาเพื่อตรวจจับ ป้องกัน หรือกู้คืนจากการโจมตีด้านความปลอดภัย

บริการด้านความปลอดภัย (Security Service): บริการประมวลผลหรือการสื่อสารที่ช่วยเพิ่มความปลอดภัยของระบบประมวลผลข้อมูลและการถ่ายโอนข้อมูลขององค์กร บริการเหล่านี้มีวัตถุประสงค์เพื่อต่อต้านการโจมตีด้านความปลอดภัย และใช้กลไกความปลอดภัยอย่างน้อยหนึ่งอย่างเพื่อให้บริการ ในเอกสารต่างๆ คำว่าภัยคุกคาม และ การโจมตี มักถูกใช้เพื่อหมายถึงสิ่งเดียวกัน (คำจำกัดความจาก RFC 2828, Internet Security Glossary)

2.1.1 การโจมตีด้านความปลอดภัย (Security Attack)

วิธีการจำแนกประเภทการโจมตีด้านความปลอดภัยที่มีประโยชน์ ซึ่งใช้ในทั้ง X.800 และ RFC 2828 คือการโจมตีแบบพาสซีฟ (Passive Attack) หรือแบบซ่อนเร้น และการโจมตีแบบแอคทีฟ (Active Attack) หรือซึ่ง

หน้า การโจมตีแบบพาสซีฟพยายามเรียนรู้หรือใช้ประโยชน์จากข้อมูลจากระบบ แต่ไม่ส่งผลกระทบต่อทรัพยากรระบบ การโจมตีแบบแอคทีฟพยายามเปลี่ยนแปลงทรัพยากรระบบหรือส่งผลกระทบต่อการทำงานของระบบ

การโจมตีแบบพาสซีฟ (Passive Attack)

การโจมตีแบบพาสซีฟมีลักษณะเป็นการดักฟังหรือตรวจสอบการส่งข้อมูล เป้าหมายของฝ่ายตรงข้ามคือการได้รับข้อมูลที่กำลังถูกส่ง การโจมตีแบบพาสซีฟมีสองประเภท ได้แก่ การเผยแพร่เนื้อหาข้อความ (Release of message contents) และการวิเคราะห์ปริมาณการรับส่งข้อมูล (Traffic analysis)

การเปิดเผยเนื้อหาของข้อความนั้นเข้าใจได้ง่าย การสนทนาทางโทรศัพท์ ข้อความอีเมล และไฟล์ที่ถ่ายโอน อาจมีข้อมูลที่ละเอียดอ่อนหรือเป็นความลับ เราต้องการป้องกันไม่ให้ฝ่ายตรงข้ามทราบเนื้อหาของข้อความที่ส่งมาเหล่านี้

การโจมตีแบบพาสซีฟประเภทที่สอง คือ การวิเคราะห์ทราฟฟิกซึ่งมีความละเอียดกว่า สมมติว่าเรามีวิธีการปกปิดเนื้อหาของข้อความหรือทราฟฟิกข้อมูลอื่นๆ เพื่อป้องกันไม่ให้ฝ่ายตรงข้ามแม้จะจับข้อความได้ ก็ไม่สามารถดึงข้อมูลจากข้อความนั้นได้ เทคนิคทั่วไปในการปกปิดเนื้อหาคือการเข้ารหัส หากเรามีการป้องกันการเข้ารหัส ฝ่ายตรงข้ามก็อาจยังสามารถสังเกตเห็นรูปแบบของข้อความเหล่านี้ได้ ฝ่ายตรงข้ามสามารถระบุตำแหน่งและตัวตนของโหนดที่สื่อสาร และสามารถสังเกตความถี่และความยาวของข้อความที่แลกเปลี่ยนกันได้ ข้อมูลนี้อาจเป็นประโยชน์ในการคาดเดาลักษณะของการสื่อสารที่กำลังเกิดขึ้น การโจมตีแบบพาสซีฟนั้นตรวจจับได้ยากมาก เพราะไม่มีการเปลี่ยนแปลงข้อมูลใดๆ โดยทั่วไปแล้ว ทราฟฟิกข้อความจะถูกส่งและรับในลักษณะที่ดูเหมือนปกติ และทั้งผู้ส่งและผู้รับจะไม่ทราบว่าบุคคลที่สามได้อ่านข้อความหรือสังเกตเห็นรูปแบบทราฟฟิก อย่างไรก็ตาม การโจมตีเหล่านี้สามารถป้องกันความสำเร็จได้ ซึ่งโดยปกติแล้วจะใช้การเข้ารหัส ดังนั้น การรับมือกับการโจมตีแบบพาสซีฟจึงเน้นไปที่การป้องกันมากกว่าการตรวจจับ

3.1.2 การโจมตีแบบแอคทีฟ (Active Attack)

การโจมตีแบบแอคทีฟเกี่ยวข้องกับการดัดแปลงสตรีมข้อมูลหรือการสร้างสตรีมข้อมูลปลอม และสามารถแบ่งย่อยออกเป็นสี่ประเภท ได้แก่ การปลอมแปลง (masquerade), การทำซ้ำ (replay), การปรับเปลี่ยนข้อความ (modification of messages) และการปฏิเสธการให้บริการ (denial of service)

การปลอมแปลงเกิดขึ้นเมื่อเอนทิตีหนึ่งสร้างทำเป็นเอนทิตีอื่น การโจมตีแบบปลอมแปลงมักประกอบด้วย การโจมตีแบบแอคทีฟรูปแบบอื่น ตัวอย่างเช่น ลำดับการตรวจสอบสิทธิ์สามารถถูกบันทึกและเล่นซ้ำหลังจากลำดับการตรวจสอบสิทธิ์ที่ถูกต้องเกิดขึ้น ทำให้เอนทิตีที่ได้รับอนุญาตและมีสิทธิ์เพียงเล็กน้อยสามารถได้รับสิทธิ์เพิ่มเติมโดยการปลอมตัวเป็นเอนทิตีที่มีสิทธิ์เหล่านั้น

การทำซ้ำ เกี่ยวข้องกับการจับหน่วยข้อมูลแบบพาสซีฟและการส่งข้อมูลซ้ำในภายหลังเพื่อสร้างเอฟเฟกต์ที่ไม่ได้รับอนุญาต

การแก้ไขข้อความ หมายถึงการเปลี่ยนแปลงบางส่วนของข้อความที่ถูกต้อง หรือข้อความถูกเลื่อนหรือเรียงลำดับใหม่เพื่อสร้างเอฟเฟกต์ที่ไม่ได้รับอนุญาต ตัวอย่างเช่น ข้อความที่มีความหมายว่า "อนุญาตให้สมาชิกอ่านบัญชีไฟล์ที่เป็นความลับ" ได้ถูกปรับเปลี่ยนเป็น "อนุญาตให้สมาชิกดีอ่านบัญชีไฟล์ที่เป็นความลับ"

การปฏิเสธการให้บริการ จะป้องกันหรือยับยั้งการใช้งานหรือการจัดการระบบสื่อสารตามปกติ การโจมตีนี้อาจมีเป้าหมายเฉพาะเจาะจง ตัวอย่างเช่น หน่วยงานอาจจะรับข้อความทั้งหมดที่ส่งไปยังปลายทางเฉพาะ เช่น บริการตรวจสอบความปลอดภัย อีกรูปแบบหนึ่งของการปฏิเสธการให้บริการคือการทำให้เครือข่ายทั้งหมดหยุดชะงัก ไม่ว่าจะโดยการปิดการทำงานของเครือข่ายหรือโดยการส่งข้อความมากเกินไปจนทำให้ประสิทธิภาพลดลง การโจมตีแบบแอคทีฟมีลักษณะตรงกันข้ามกับการโจมตีแบบพาสซีฟ ในขณะที่การโจมตีแบบพาสซีฟตรวจจับได้ยาก แต่ก็มีการตรวจพบได้ยาก ที่สามารถป้องกันไม่ให้เกิดความสำเร็จ ในทางกลับกัน การป้องกันการโจมตีแบบแอคทีฟนั้นค่อนข้างยาก เนื่องจากช่องโหว่ทางกายภาพ ซอฟต์แวร์ และเครือข่ายที่อาจเกิดขึ้นได้หลากหลาย เป้าหมายคือการตรวจจับการโจมตีแบบแอคทีฟและกู้คืนความเสียหายจากความขัดข้องหรือความล่าช้าที่อาจเกิดขึ้น หากการตรวจจับสามารถยับยั้งได้ ก็อาจนำไปสู่การป้องกันได้เช่นกัน

2.1.3 บริการด้านความมั่นคงปลอดภัย (Security service)

X.800 ให้คำจำกัดความของบริการด้านความปลอดภัยว่า “เป็นบริการที่จัดทำโดยเลเยอร์โพรโทคอลของระบบเปิดที่สื่อสารกัน และรับรองความปลอดภัยของระบบหรือการถ่ายโอนข้อมูลอย่างเพียงพอ” คำจำกัดความที่ชัดเจนกว่านี้อาจพบได้ใน RFC 2828 ซึ่งให้คำจำกัดความดังต่อไปนี้: “บริการประมวลผลหรือการสื่อสารที่จัดทำโดยระบบเพื่อให้การป้องกันเฉพาะเจาะจงแก่ทรัพยากรระบบ” บริการด้านความปลอดภัยจะดำเนินนโยบายด้านความปลอดภัยและดำเนินการโดยกลไกด้านความปลอดภัย X.800 แบ่งบริการเหล่านี้ออกเป็น 5 ประเภทและบริการเฉพาะ 14 ประเภท

การพิสูจน์ตัวตนหรือการรับรองความถูกต้อง (Authentication) คือการรับรองว่าเอนทิตีที่สื่อสารนั้นเป็นเอนทิตีที่อ้างสิทธิ์ ประกอบด้วย

- การรับรองความถูกต้องแบบเพียร์เอนทิตี (Peer Entity Authentication) ใช้ร่วมกับการเชื่อมต่อแบบลอจิคัลเพื่อสร้างความมั่นใจในตัวตนของเอนทิตีที่เชื่อมต่อ

- การรับรองความถูกต้องแบบ Data-Origin Authentication ในการถ่ายโอนข้อมูลแบบไร้การเชื่อมต่อ ให้การรับรองว่าแหล่งที่มาของข้อมูลที่ได้รับเป็นไปตามที่อ้างสิทธิ์

การควบคุมการเข้าถึง (Access Control) คือการป้องกันการใช้งานทรัพยากรโดยไม่ได้รับอนุญาต เช่น บริการนี้ควบคุมว่าใครสามารถเข้าถึงทรัพยากรได้ ภายใต้เงื่อนไขใดที่สามารถเข้าถึงได้ และอนุญาตให้ผู้ที่เข้าถึงทรัพยากรทำอะไรได้บ้าง

ความลับของข้อมูล (Data Confidentiality) คือการปกป้องข้อมูลจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ประกอบด้วย

- ความลับของการเชื่อมต่อ (Connection Confidentiality) คือการปกป้องข้อมูลผู้ใช้ทั้งหมดบนการเชื่อมต่อ

- ความลับแบบไร้การเชื่อมต่อ (Connectionless Confidentiality) คือการปกป้องข้อมูลผู้ใช้ทั้งหมดในบล็อกข้อมูลเดียว

- ความลับของฟิลด์ที่เลือก (Selective-Field Confidentiality) คือการปกป้องข้อมูลที่สามารถได้มาจากการสังเกตการณ์การไหลของข้อมูลที่ถูกเลือกไว้

- ความลับของการไหลของข้อมูล (Traffic-Flow Confidentiality) การปกป้องข้อมูลที่สามารถได้รับมาจากการสังเกตการณ์การไหลของข้อมูล

ความสมบูรณ์ของข้อมูล (Data Integrity)

การรับรองว่าข้อมูลที่ได้รับนั้นตรงตามที่ส่งโดยหน่วยงานที่ได้รับอนุญาต กล่าวคือ ไม่มีการแก้ไข แทรก ลบ หรือเล่นซ้ำ ประกอบด้วย

- ความสมบูรณ์ของการเชื่อมต่อพร้อมการกู้คืน (Connection Integrity with Recovery)** ครอบคลุมความสมบูรณ์ของข้อมูลผู้ใช้ทั้งหมดในการเชื่อมต่อ และตรวจจับการแก้ไข แทรก ลบ หรือเล่นซ้ำข้อมูลใดๆ ภายในลำดับข้อมูลทั้งหมด แม้ว่าจะมีความพยายามกู้คืนก็ตาม

- ความสมบูรณ์ของการเชื่อมต่อโดยไม่มีการกู้คืน (Connection Integrity without Recovery)** เช่นเดียวกับข้างต้น แต่ครอบคลุมเฉพาะการตรวจจับโดยไม่มีการกู้คืน

- ความสมบูรณ์ของการเชื่อมต่อแบบเลือกฟิลด์ (Selective-Field Connection Integrity)** ครอบคลุมความสมบูรณ์ของฟิลด์ที่เลือกภายในข้อมูลผู้ใช้ของบล็อกข้อมูลที่ถ่ายโอนผ่านการเชื่อมต่อ และดำเนินการในรูปแบบของการตรวจสอบว่าฟิลด์ที่เลือกนั้นถูกแก้ไข แทรก ลบ หรือเล่นซ้ำหรือไม่

- ความสมบูรณ์แบบไร้การเชื่อมต่อ (Connectionless Integrity)** ครอบคลุมความสมบูรณ์ของบล็อกข้อมูลแบบไร้การเชื่อมต่อ ครอบคลุมความสมบูรณ์ของบล็อกข้อมูลแบบไร้การเชื่อมต่อเดียว และอาจดำเนินการในรูปแบบของการตรวจจับการแก้ไขข้อมูล นอกจากนี้ อาจมีการตรวจจับการเล่นซ้ำในรูปแบบที่จำกัด

- ความสมบูรณ์แบบเลือกฟิลด์แบบไร้การเชื่อมต่อ (Selective-Field Connectionless Integrity)** ครอบคลุมความสมบูรณ์ของฟิลด์ที่เลือกภายในบล็อกข้อมูลแบบไร้การเชื่อมต่อเดียว มีรูปแบบการกำหนดว่าฟิลด์ที่เลือกมีการเปลี่ยนแปลงหรือไม่

การปฏิเสธการรับข้อมูล (Nonrepudiation)

ให้ความคุ้มครองจากการปฏิเสธโดยหนึ่งในหน่วยงานที่เกี่ยวข้องกับการสื่อสารว่าได้มีส่วนร่วมในการสื่อสารทั้งหมดหรือบางส่วน ประกอบด้วย

- การปฏิเสธการรับข้อมูล (Nonrepudiation) หลักฐานต้นทางที่แสดงว่าข้อความนั้นถูกส่งโดยฝ่ายที่ระบุ
- การปฏิเสธการรับข้อมูล (Nonrepudiation) หลักฐานปลายทางที่แสดงว่าฝ่ายที่ระบุได้รับข้อความนั้นแล้ว

บริการความพร้อมใช้งาน (Availability Service)

ทั้ง X.800 และ RFC 2828 กำหนดให้ความพร้อมใช้งานเป็นคุณสมบัติของระบบหรือทรัพยากรระบบที่สามารถเข้าถึงและใช้งานได้ตามความต้องการโดยหน่วยงานระบบที่ได้รับอนุญาต ตามข้อกำหนดด้านประสิทธิภาพสำหรับระบบนั้น กล่าวคือ ระบบจะพร้อมใช้งานได้หากให้บริการตามการออกแบบระบบเมื่อใดก็ตามที่ผู้ใช้ร้องขอ) การโจมตีที่หลากหลายอาจส่งผลให้ความพร้อมใช้งานลดลงหรือสูญเสียไป การโจมตีบางประเภทสามารถใช้มาตรการตอบโต้อัตโนมัติ เช่น การตรวจสอบความถูกต้องและการเข้ารหัส ในขณะที่บางประเภทจำเป็นต้องมีการดำเนินการทางกายภาพเพื่อป้องกันหรือกู้คืนจากการสูญเสียความพร้อมใช้งานขององค์ประกอบต่างๆ ของระบบแบบกระจาย X.800 ถือว่าความพร้อมใช้งานเป็นคุณสมบัติที่เชื่อมโยงกับบริการด้านความปลอดภัยต่างๆ

อย่างไรก็ตาม การเรียกใช้บริการความพร้อมใช้งานโดยเฉพาะก็สมเหตุสมผล บริการความพร้อมใช้งานคือบริการที่ปกป้องระบบเพื่อให้มั่นใจว่ามีความพร้อมใช้งาน บริการนี้ช่วยแก้ไขปัญหาด้านความปลอดภัยที่เกิดจากการโจมตีแบบปฏิเสธการให้บริการ โดยขึ้นอยู่กับการจัดการและการควบคุมทรัพยากรระบบที่เหมาะสม จึงขึ้นอยู่กับบริการควบคุมการเข้าถึงและบริการด้านความปลอดภัยอื่นๆ

2.1.4 เป้าหมายของนโยบายและกลไกด้านความมั่นคงปลอดภัย (Policy goal and Security Mechanisms)

เป้าหมายของนโยบายและกลไกความปลอดภัยที่กำหนด

ใน X.800 กลไกเหล่านี้แบ่งออกเป็นกลไกที่ใช้ในชั้นโพรโทคอลเฉพาะ เช่น TCP หรือโพรโทคอลชั้นแอปพลิเคชัน และกลไกที่ไม่ได้เฉพาะเจาะจงกับชั้นโพรโทคอลหรือความปลอดภัยใด ๆ กลไกการรักษาความปลอดภัยเฉพาะ อาจรวมเข้าในเลเยอร์โพรโทคอลที่เหมาะสมเพื่อให้บริการความปลอดภัย OSI บางส่วน ประกอบด้วย

- การเข้ารหัส (Encipherment) การใช้อัลกอริทึมทางคณิตศาสตร์เพื่อแปลงข้อมูลให้อยู่ในรูปแบบที่เข้าใจได้ยาก การแปลงและการกู้คืนข้อมูลในภายหลังขึ้นอยู่กับอัลกอริทึมและคีย์การเข้ารหัสอย่างน้อยสองอัน
- ลายเซ็นดิจิทัล (Digital Signature) ข้อมูลที่ผนวกเข้า หรือการแปลงรหัสของหน่วยข้อมูล ซึ่งช่วยให้ผู้รับหน่วยข้อมูลสามารถพิสูจน์แหล่งที่มาและความสมบูรณ์ของหน่วยข้อมูล และป้องกันการปลอมแปลง เช่น โดยผู้รับ
- การควบคุมการเข้าถึง (Access Control) กลไกที่หลากหลายที่บังคับใช้สิทธิ์การเข้าถึงทรัพยากร
- ความสมบูรณ์ของข้อมูล (Data Integrity) กลไกที่หลากหลายที่ใช้เพื่อรับรองความสมบูรณ์ของหน่วยข้อมูลหรือสตรีมของหน่วยข้อมูล

-**การแลกเปลี่ยนข้อมูลเพื่อยืนยันตัวตน** (Authentication Exchange) กลไกที่ออกแบบมาเพื่อยืนยันตัวตนของเอนทิตีโดยการแลกเปลี่ยนข้อมูล

-**การเพิ่มบิตลงในช่องว่างในสตรีมข้อมูล** (Traffic Padding) การแทรกบิตลงในช่องว่างในสตรีมข้อมูลเพื่อขัดขวางความพยายามในการวิเคราะห์การรับส่งข้อมูล

-**การควบคุมเส้นทาง** (Routing Control) ช่วยให้สามารถเลือกเส้นทางที่ปลอดภัยทางกายภาพเฉพาะสำหรับข้อมูลบางอย่าง และอนุญาตให้เปลี่ยนแปลงเส้นทางได้ โดยเฉพาะอย่างยิ่งเมื่อสงสัยว่ามีการละเมิดความปลอดภัย

-**การรับรองเอกสาร** (Notarization) การใช้บุคคลที่สามที่เชื่อถือได้เพื่อรับรองคุณสมบัติบางประการของการแลกเปลี่ยนข้อมูล

ในขณะที่ บริการด้านความมั่นคงปลอดภัยไซเบอร์ (Security Service) ประกอบด้วย

-**การตรวจสอบสิทธิ์เอนทิตีแบบเพียร์** (Peer Entity Authentication)

-**การตรวจสอบแหล่งที่มาของข้อมูล** (Data-Origin Authentication)

-**การควบคุมการเข้าถึง** (Access Control)

-**การรักษาความลับ** (Confidentiality)

-**การรักษาความลับของการไหลของข้อมูล** (Traffic-Flow Confidentiality)

-**ความถูกต้องครบถ้วนของข้อมูล** (Data Integrity)

-**การไม่ปฏิเสธความรับผิดชอบ** (Nonrepudiation)

-**ความพร้อมใช้งาน** (Availability)

ตาราง 2.1 ความสัมพันธ์ระหว่างบริการและกลไกความมั่นคงปลอดภัย

บริการ (Service)	กลไก (Mechanism)							
	การเข้ารหัส	ลายเซ็นดิจิทัล	การควบคุมการเข้าถึง	ความถูกต้องของข้อมูล	การแลกเปลี่ยนการรับรองความถูกต้อง	การเพิ่มบิตลงในช่องว่าง	การควบคุมเส้นทาง	การรับรองเอกสาร
การตรวจสอบสิทธิ์เอนทิตีแบบเพียร์	Y	Y			Y			
การตรวจสอบแหล่งที่มาของข้อมูล	Y	Y						
การควบคุมการเข้าถึง			Y					
การรักษาความลับ	Y						Y	
ความลับของการไหลของข้อมูล	Y					Y	Y	

บริการ (Service)	กลไก (Mechanism)							
	การ เข้ารหัส	ลายเซ็น ดิจิทัล	การควบคุม การเข้าถึง	ความถูกต้อง ของข้อมูล	การแลกเปลี่ยนการ รับรองความถูกต้อง	การเพิ่ม บิตลงใน ช่องว่าง	การควบคุม เส้นทาง	การรับรอง เอกสาร
ความสมบูรณ์ ถูกต้องของข้อมูล	Y	Y		Y				
การไม่ปฏิเสธความ รับผิดชอบ		Y		Y				Y
ความพร้อมใช้งาน				Y	Y			

จากตารางแสดงข้อมูลเกี่ยวกับคุณสมบัติในการบริการด้านความมั่นคงปลอดภัยของระบบ ได้แก่ การปฏิเสธความรับผิดชอบ (Nonrepudiation) และความพร้อมใช้งาน (Availability) โดยในตารางมีการระบุว่าการกลไกความสามารถในการปฏิเสธความรับผิดชอบและความพร้อมใช้งานนั้น ได้รับการรองรับในหลายจุด (แสดงด้วย "Y") ซึ่งสะท้อนให้เห็นถึงความสำคัญของคุณสมบัติเหล่านี้ในการรักษาความมั่นคงและความน่าเชื่อถือของระบบ

2.1.5 เป้าหมายของนโยบายและกลไกความปลอดภัยแบบแพร่หลาย

กลไกที่ไม่ได้จำเพาะเจาะจงสำหรับบริการรักษาความปลอดภัยตามแต่ละชั้นของ OSI หรือเลเยอร์โพรโทคอลใดๆ ประกอบด้วย

- **ฟังก์ชันการทำงานที่เชื่อถือได้ (Trusted Functionality)** สิ่งที่ได้รับรู้ว่ามีตามถูกต้องตามเกณฑ์บางประการ (เช่น ตามที่กำหนดไว้ในนโยบายความปลอดภัย)

- **ป้ายกำกับความปลอดภัย (Security Label)** เครื่องหมายที่เชื่อมโยงกับทรัพยากร (ซึ่งอาจเป็นหน่วยข้อมูล) ซึ่งระบุหรือกำหนดคุณลักษณะความปลอดภัยของทรัพยากรนั้น

- **การตรวจจับเหตุการณ์ (Event Detection)** การตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย

- **เส้นทางการตรวจสอบความปลอดภัย (Security Audit Trail)** ข้อมูลที่รวบรวมและอาจนำไปใช้เพื่ออำนวยความสะดวกในการตรวจสอบความปลอดภัย ซึ่งเป็นการตรวจสอบและการตรวจสอบบันทึกและกิจกรรมของระบบอย่างอิสระ

- **การกู้คืนความปลอดภัย (Security Recovery)** จัดการกับคำขอจากกลไกต่างๆ เช่น ฟังก์ชันการจัดการและจัดการเหตุการณ์ และดำเนินการกู้คืน

ส่วนกลไกการเข้ารหัสแบบย้อนกลับได้เป็นเพียงอัลกอริทึมการเข้ารหัสที่อนุญาตให้เข้ารหัสและถอดรหัสข้อมูลในภายหลัง กลไกการเข้ารหัสแบบย้อนกลับไม่ได้ประกอบด้วยอัลกอริทึมแฮชและรหัสยืนยันข้อความ ซึ่งใช้ในแอปพลิเคชันลายเซ็นดิจิทัลและการยืนยันข้อความ

กลไกและบริการด้านความมั่นคงปลอดภัยข้อมูลทั้งเชิงเทคนิค เช่น การควบคุมเส้นทาง การรับรองเอกสาร ฟังก์ชันการทำงานที่เชื่อถือได้ ป้ายกำกับความปลอดภัย การตรวจจับเหตุการณ์ การตรวจสอบกิจกรรม รวมถึงกลไกการกู้คืน ตลอดจนแยกประเภทกลไกการเข้ารหัสทั้งแบบย้อนกลับได้และไม่ได้ โดยแต่ละกลไกมีบทบาทสำคัญในการสร้างความมั่นคงปลอดภัยและรองรับการตรวจสอบในระบบสารสนเทศ

2.2 แบบจำลองความมั่นคงปลอดภัยเครือข่าย

แบบจำลองหรือโมเดลความมั่นคงปลอดภัยเครือข่าย (Model of network security) ทั่วไป โดยจะศึกษาว่าข้อความต่างๆ ถูกแบ่งปันระหว่างผู้ส่งและผู้รับอย่างปลอดภัยผ่านเครือข่ายได้อย่างไร นอกจากนี้ จะกล่าวถึง โมเดลความปลอดภัยการเข้าถึงเครือข่าย (Network access security model) ซึ่งออกแบบมาเพื่อปกป้องระบบจากการเข้าถึงที่ไม่พึงประสงค์ผ่านเครือข่าย

การที่ข้อความจะถูกส่งหรือรับนั้น จะต้องมีทั้งผู้ส่งและผู้รับ ทั้งผู้ส่งและผู้รับต้องตกลงร่วมกันในการแบ่งปันข้อความนั้น การส่งข้อความจากผู้ส่งถึงผู้รับจำเป็นต้องมีสื่อกลาง เช่น ช่องทางข้อมูลซึ่งเป็นบริการอินเทอร์เน็ต เส้นทางตรรกะถูกกำหนดผ่านเครือข่าย (อินเทอร์เน็ต) จากผู้ส่งไปยังผู้รับ และใช้โพรโทคอลการสื่อสารที่ทั้งผู้ส่งและผู้รับกำหนดการสื่อสาร

การแปลงข้อมูลที่เกี่ยวข้องกับความปลอดภัยเพื่อส่ง ตัวอย่างเช่น การเข้ารหัสข้อความ ซึ่งเข้ารหัสข้อความจนทำให้ฝ่ายตรงข้ามไม่สามารถอ่านได้ และการเพิ่มรหัสตามเนื้อหาของข้อความ ซึ่งสามารถใช้เพื่อยืนยันตัวตนของผู้ส่งได้

ข้อมูลลับบางอย่างที่ผู้บริหารทั้งสองแบ่งปันกัน และหวังว่าฝ่ายตรงข้ามจะไม่รู้ ตัวอย่างเช่น คีย์การเข้ารหัสที่ใช้ร่วมกับการแปลงเพื่อเข้ารหัสข้อความก่อนส่ง และถอดรหัสเมื่อได้รับ⁶

อาจจำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้เพื่อให้การส่งข้อมูลมีความปลอดภัย ตัวอย่างเช่น บุคคลที่สามอาจรับผิดชอบในการกระจายข้อมูลลับให้กับผู้รับข้อมูลทั้งสองราย โดยปกปิดข้อมูลดังกล่าวจากฝ่ายตรงข้าม หรืออาจจำเป็นต้องมีบุคคลที่สามเพื่อไกล่เกลี่ยข้อพิพาทระหว่างผู้รับข้อมูลทั้งสองรายเกี่ยวกับความถูกต้องของการส่งข้อความ

เมื่อเรากังวลเกี่ยวกับความปลอดภัยของข้อความบนเครือข่าย เมื่อข้อความนั้นมีข้อมูลที่เป็นความลับหรือเป็นข้อมูลจริง ซึ่งมีภัยคุกคามจากฝ่ายตรงข้ามที่อยู่ที่ช่องทางข้อมูล บริการรักษาความปลอดภัยใดๆ ก็ตามควรมีองค์ประกอบสามประการที่กล่าวถึง แบบจำลองทั่วไปนี้แสดงให้เห็นว่ามีงานพื้นฐานสี่ประการในการออกแบบบริการรักษาความปลอดภัยโดยเฉพาะ ประกอบด้วย

- 1) ออกแบบอัลกอริทึมสำหรับการแปลงที่เกี่ยวข้องกับความปลอดภัย อัลกอริทึมควรเป็นแบบที่ฝ่ายตรงข้ามไม่สามารถเอาชนะจุดประสงค์ของมันได้
- 2) สร้างข้อมูลลับที่จะใช้กับอัลกอริทึม

3) พัฒนารูปแบบการเผยแพร่และแบ่งปันข้อมูลลับ

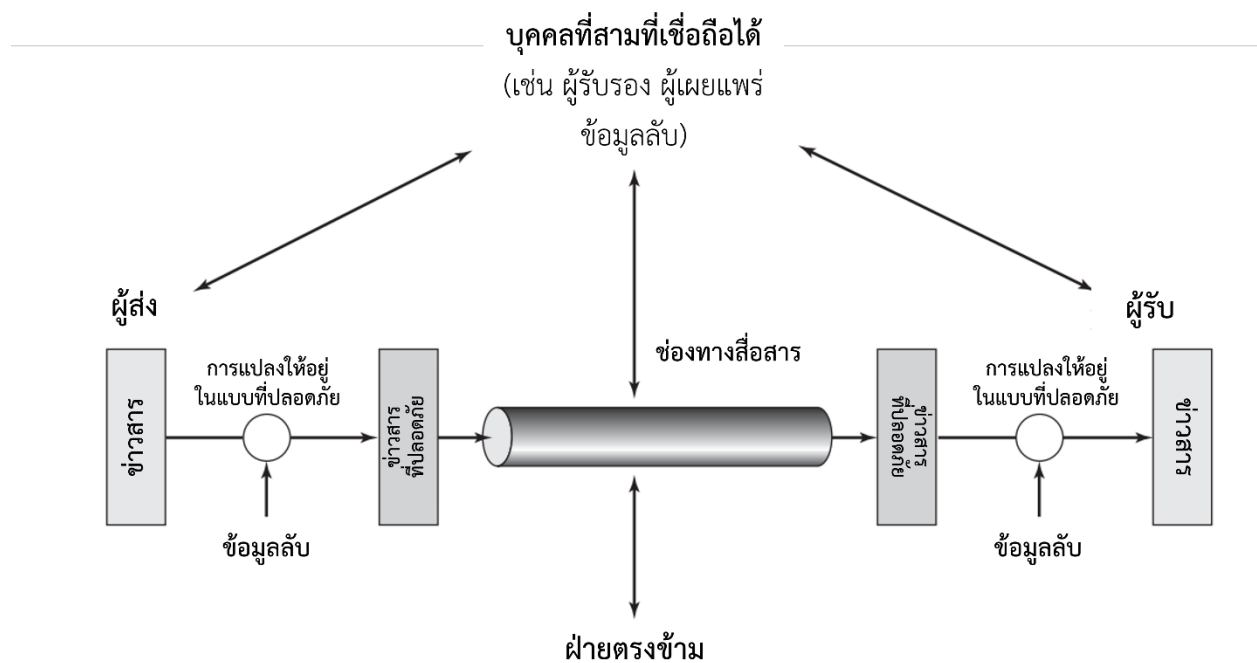
4) ระบบโพรโทคอลที่จะใช้โดยหลักการสองประการที่ใช้หลักการริเริ่มความปลอดภัยและข้อมูลลับเพื่อบรรลุบริการความปลอดภัยเฉพาะ

1) **การแปลง (Transformation)** ข้อมูลที่ต้องส่งไปยังผู้รับ เพื่อให้ฝ่ายตรงข้ามที่อยู่ ณ ช่องสัญญาณไม่สามารถอ่านข้อความได้ นี่บ่งชี้ถึงการเข้ารหัส (Encryption) ข้อความ รวมถึงการเพิ่มโค้ดระหว่างการแปลงข้อมูลที่จะใช้ในการยืนยันตัวตนผู้รับที่แท้จริงอีกด้วย

2) **การแบ่งปันข้อมูลลับ (Secret information)** ระหว่างผู้ส่งและผู้รับ ซึ่งฝ่ายตรงข้ามต้องไม่ล่วงรู้ข้อมูลใดๆ ในที่นี้คือกุญแจเข้ารหัส (Encryption key) ที่ใช้ในการเข้ารหัสข้อความที่ฝั่งผู้ส่ง และในระหว่างการถอดรหัสข้อความที่ฝั่งผู้รับ

3) **ต้องมีบุคคลที่สามที่เชื่อถือได้ (Trusted third party)** ซึ่งควรรับผิดชอบในการเผยแพร่ข้อมูลลับ (Distributing the secret information) (กุญแจ) ให้กับทั้งสองฝ่ายที่สื่อสาร และป้องกันไม่ให้ฝ่ายตรงข้ามเข้าถึงข้อมูลดังกล่าวได้

รูปแบบการรักษาความปลอดภัยเครือข่ายทั่วไป รูป 2.1



รูป 2.1 แบบจำลองความมั่นคงปลอดภัยเครือข่าย

(ดัดแปลงจาก William Stallings (2011), NETWORK SECURITY ESSENTIALS: Applications and Standards, Fourth Edition)

แบบจำลองความปลอดภัยของเครือข่ายนำเสนอ**ผู้ส่งและผู้รับที่** สื่อสารกันทั้งสองฝ่าย ซึ่งตกลงร่วมกันในการแลกเปลี่ยนข้อมูล ผู้ส่งมีข้อมูลที่จะแบ่งปันกับผู้รับ

แต่ผู้ส่งไม่สามารถส่งข้อความผ่านช่องทางข้อมูลในรูปแบบที่อ่านได้ เนื่องจากอาจมีความเสี่ยงที่จะถูกโจมตีจากฝ่ายตรงข้าม ดังนั้น ก่อนที่จะส่งข้อความผ่านช่องทางข้อมูล ควร **แปลง** ข้อความให้อยู่ในรูปแบบที่อ่านไม่ได้เสียก่อน

ข้อมูลลับจะถูกใช้ในระหว่างกระบวนการแปลงข้อความ ซึ่งจะต้องใช้เมื่อข้อความถูกแปลงอีกครั้งที่ฝั่งผู้รับ ด้วยเหตุนี้จึงจำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้ ซึ่งจะรับผิดชอบในการกระจายข้อมูลลับนี้ไปยังทั้งสองฝ่ายที่เกี่ยวข้องในการสื่อสาร

ดังนั้น เมื่อพิจารณารูปแบบทั่วไปของการรักษาความปลอดภัยเครือข่ายนี้ จะต้องพิจารณางาน 4 ประการต่อไปนี้ซึ่งจะออกแบบรูปแบบความปลอดภัย แบบจำลองทั่วไปนี้แสดงให้เห็นว่ามีงานพื้นฐาน 4 ประการในการออกแบบบริการรักษาความปลอดภัยเฉพาะ

1) ออกแบบอัลกอริทึมสำหรับการแปลงที่เกี่ยวข้องกับความปลอดภัย อัลกอริทึมควรเป็นแบบที่ฝ่ายตรงข้ามไม่สามารถเอาชนะวัตถุประสงค์ได้ เพื่อเปลี่ยนข้อความที่อ่านได้ที่ฝั่งผู้ส่งให้เป็นรูปแบบที่อ่านไม่ได้ ควรออกแบบอัลกอริทึมที่เหมาะสมเพื่อให้ฝ่ายตรงข้ามเจาะอัลกอริทึมความปลอดภัยนั้นได้ยาก

2) สร้างข้อมูลลับที่จะนำมาใช้กับอัลกอริทึม ผู้ออกแบบแบบจำลองความปลอดภัยเครือข่ายจะพิจารณาถึง**การสร้างข้อมูลลับ**ที่เรียกว่ากุญแจ ข้อมูลลับนี้จะถูกนำมาใช้ร่วมกับอัลกอริทึมความปลอดภัยเพื่อแปลงข้อความ

3) พัฒนาวิธีการสำหรับการเผยแพร่และแบ่งปันข้อมูลลับ ขณะนี้ข้อมูลลับมีความจำเป็นทั้งฝ่ายผู้ส่งและฝ่ายผู้รับ โดยฝ่ายผู้ส่งจะใช้ข้อมูลนี้เพื่อเข้ารหัสหรือแปลงข้อความให้อยู่ในรูปแบบที่อ่านไม่ได้ และฝ่ายผู้รับจะใช้ข้อมูลนี้เพื่อถอดรหัสหรือแปลงข้อความให้อยู่ในรูปแบบที่อ่านได้

ดังนั้น จึงจำเป็นต้องมี**บุคคลที่สามที่เชื่อถือได้**ซึ่งจะเป็นผู้เผยแพร่ข้อมูลลับนี้ให้กับทั้งผู้ส่งและผู้รับ ในการออกแบบแบบจำลองความปลอดภัยเครือข่าย ผู้ออกแบบต้องให้ความสำคัญกับ **การพัฒนาวิธีการเผยแพร่**กุญแจให้กับทั้งผู้ส่งและผู้รับด้วย ต้องใช้วิธีการที่เหมาะสมเพื่อส่งข้อมูลลับนี้ไปยังฝ่ายที่สื่อสารโดยไม่ถูกรบกวนจากฝ่ายตรงข้าม

4) นอกจากนี้ ยังต้องดูแลให้**โพรโทคอลการสื่อสาร**ที่ใช้โดยฝ่ายที่ทำการสื่อสารต้องรองรับอัลกอริทึมการรักษาความปลอดภัยและคีย์ลับเพื่อให้บรรลุบริการรักษาความปลอดภัย กำหนดโพรโทคอลที่จะใช้โดยสองหลักการที่ใช้อัลกอริทึมความปลอดภัยและข้อมูลลับเพื่อบรรลุบริการรักษาความปลอดภัยเฉพาะ

เนื้อหาส่วนใหญ่ของหนังสือเล่มนี้มุ่งเน้นไปที่ประเภทของกลไกและบริการด้านความปลอดภัยที่สอดคล้องกับแบบจำลองที่แสดงในรูป 2.1 อย่างไรก็ตาม ยังมีสถานการณ์ที่เกี่ยวข้องกับความปลอดภัยอื่นๆ ที่น่าสนใจซึ่งไม่ตรงกับแบบจำลองนี้โดยตรง แต่หนังสือเล่มนี้ได้พิจารณาไว้ แบบจำลองทั่วไปของสถานการณ์อื่นๆ

เหล่านี้แสดงไว้ในรูปที่ 2.2 ซึ่งสะท้อนถึงความกังวลเกี่ยวกับการปกป้องระบบสารสนเทศจากการเข้าถึงที่ไม่พึงประสงค์ ถ้าส่วนใหญ่มุ่งเน้นกับความกังวลที่เกิดจากแฮกเกอร์ที่พยายามเจาะระบบที่สามารถเข้าถึงได้ผ่านเครือข่าย แฮกเกอร์อาจเป็นบุคคลที่ไม่มีเจตนาร้ายเพียงแค่พอใจที่ได้เจาะและเข้าสู่ระบบคอมพิวเตอร์ ผู้บุกรุกอาจเป็นพนักงานที่ไม่พอใจที่ต้องการสร้างความเสียหาย หรืออาชญากรที่แสวงหาผลประโยชน์จากทรัพย์สินคอมพิวเตอร์เพื่อผลประโยชน์ทางการเงิน (เช่น การได้รับหมายเลขบัตรเครดิตหรือการโอนเงินผิดกฎหมาย)

นอกจากนั้น **ความปลอดภัยของข้อมูลหรือข้อความบนเครือข่าย**ดังที่ได้อธิบายข้างต้นนี้ จำเป็นต้องอาศัยแบบจำลองความมั่นคงปลอดภัยในการเข้าถึงเครือข่าย ซึ่งออกแบบมาเพื่อ**รักษาความปลอดภัยของระบบสารสนเทศ**ที่ผู้โจมตีสามารถเข้าถึงได้ผ่านเครือข่าย รูปแบบการรักษาความปลอดภัยเครือข่ายเพื่อรักษาความปลอดภัยระบบของคุณแสดงอยู่ในรูป 2.2



รูป 2.2 แบบจำลองความมั่นคงปลอดภัยในการเข้าถึงเครือข่าย

(ดัดแปลงจาก William Stallings (2011), NETWORK SECURITY ESSENTIALS: Applications and Standards, Fourth Edition)

จากรูป 2.2 มีสองวิธีในการปกป้องระบบจากผู้โจมตี วิธีแรกคือการใช้**ฟังก์ชันผู้ดูแลประตูเข้าออก (Gatekeeper function)** หมายถึงการใช้**รหัสล็อกอินและรหัสผ่าน**เพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์

ในกรณีที่ผู้ใช้ที่ไม่พึงประสงค์สามารถเข้าถึงระบบได้ วิธีที่สองในการรักษาความปลอดภัยระบบ คือการนำ**การควบคุมภายในด้านความมั่นคงปลอดภัย (Internal security control)** มาใช้ ซึ่งจะตรวจจับผู้ใช้ที่ไม่พึงประสงค์ที่พยายามเข้าถึงระบบโดยการวิเคราะห์กิจกรรมของระบบ วิธีที่สองนี้เราเรียกว่า **โปรแกรมป้องกันไวรัส** ซึ่งติดตั้งไว้ในระบบของเราเพื่อป้องกันไม่ให้ผู้ใช้ที่ไม่พึงประสงค์เข้าถึงระบบคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต

การเข้าถึงที่ไม่พึงประสงค์อีกประเภทหนึ่งคือการฝังตรรกะในระบบคอมพิวเตอร์ที่ใช้ประโยชน์จากช่องโหว่ของระบบ ซึ่งอาจส่งผลกระทบต่อโปรแกรมแอปพลิเคชันและโปรแกรมมัลแวร์ เช่น โปรแกรมแก้ไขและคอมไพเลอร์ โปรแกรมสามารถส่งภัยคุกคามได้สองประเภท ได้แก่

- 1) ภัยคุกคามการเข้าถึงข้อมูล สกัดกันหรือแก้ไขข้อมูลในนามของผู้ใช้ที่ไม่ควรมีสถานีเข้าถึงข้อมูลดังกล่าว
- 2) ภัยคุกคามด้านบริการ ผู้ใช้ที่ถูกต้องตามกฎหมายใช้ประโยชน์จากข้อบกพร่องในการให้บริการในคอมพิวเตอร์เพื่อยับยั้งการใช้งานโดยผู้ใช้ที่ถูกกฎหมาย

ไวรัสและเวิร์มเป็นตัวอย่างสองตัวอย่างของการโจมตี ซอฟต์แวร์การโจมตีดังกล่าวสามารถเข้าสู่ระบบได้โดยใช้สื่อที่มีรหัสประสงค์ร้ายซ่อนอยู่ในซอฟต์แวร์ที่มีประโยชน์ ไวรัสและเวิร์มยังสามารถแทรกเข้าไปในระบบผ่านเครือข่ายได้อีกด้วย ซึ่งกลไกเหล่านี้มีความสำคัญอย่างยิ่งต่อความปลอดภัยของเครือข่าย

ดังนั้น รูปแบบทั้งหมดเกี่ยวกับโมเดลความปลอดภัยของเครือข่าย ในส่วนนี้ได้อธิบายถึงโมเดลความปลอดภัยของเครือข่ายสองแบบแล้ว แบบแรก คือ การรักษาความปลอดภัยของข้อมูลบนเครือข่ายระหว่างการรับส่งข้อมูล และแบบที่สอง คือ การรักษาความปลอดภัยของระบบสารสนเทศ ซึ่งแฮกเกอร์สามารถเข้าถึงได้ผ่านเครือข่ายหรืออินเทอร์เน็ต

2.3 มาตรฐานด้านความมั่นคงปลอดภัย (Security standards)

เทคนิคและการประยุกต์ใช้ด้านความปลอดภัยจำนวนมากที่อธิบายไว้ในหนังสือเล่มนี้ได้รับการกำหนดให้เป็นมาตรฐาน นอกจากนี้ มาตรฐานยังได้รับการพัฒนาขึ้นเพื่อครอบคลุมแนวปฏิบัติด้านการจัดการและสถาปัตยกรรมโดยรวมของกลไกและบริการด้านความปลอดภัย ตลอดทั้งเล่มนี้ ได้อธิบายถึงมาตรฐานที่สำคัญที่สุดที่กำลังใช้งานหรือกำลังพัฒนาสำหรับด้านต่างๆ ของการเข้ารหัสและความปลอดภัยของเครือข่าย องค์กรต่างๆ มีส่วนร่วมในการพัฒนาหรือส่งเสริมมาตรฐานเหล่านี้ องค์กรที่สำคัญที่สุดในบริบทปัจจุบัน มีดังนี้

- **สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST):**

NIST เป็นหน่วยงานรัฐบาลกลางของสหรัฐอเมริกาที่ดูแลด้านวิทยาศาสตร์การวัด มาตรฐาน และเทคโนโลยีที่เกี่ยวข้องกับการใช้งานของรัฐบาลสหรัฐอเมริกาและการส่งเสริมนวัตกรรมภาคเอกชนของสหรัฐอเมริกา แม้จะมีขอบเขตระดับชาติ แต่มาตรฐานการประมวลผลข้อมูลแห่งชาติ (Federal Information Processing Standards หรือ FIPS) และสิ่งพิมพ์พิเศษ (Special Publications หรือ SP) ของ NIST ก็มีผลกระทบทั่วโลก

- **สมาคมอินเทอร์เน็ต (Internet Society): ISOC**

เป็นสมาคมสมาชิกวิชาชีพที่มีสมาชิกทั้งในระดับองค์กรและบุคคลทั่วโลก องค์กรนี้เป็นผู้นำในการแก้ไขปัญหาดังกล่าว ที่ส่งผลกระทบต่ออนาคตของอินเทอร์เน็ต และเป็นองค์กรที่รวบรวมกลุ่มต่างๆ ที่รับผิดชอบมาตรฐานโครงสร้างพื้นฐานอินเทอร์เน็ต ซึ่งรวมถึงคณะทำงานด้านวิศวกรรมอินเทอร์เน็ต (Internet Engineering Task Force หรือ IETF) และคณะกรรมการสถาปัตยกรรมอินเทอร์เน็ต (Internet Architecture Board หรือ IAB) องค์กรเหล่านี้พัฒนามาตรฐานอินเทอร์เน็ตและข้อกำหนดที่เกี่ยวข้อง ซึ่งทั้งหมดได้รับการเผยแพร่ในรูปแบบคำขอความคิดเห็น (Requests for Comments หรือ RFC)

2.4 กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework)

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST (National Institute of Standards and Technology: CSF) ได้รับการประกาศใช้ในปี 2014 เพื่อเป็นแนวทางปฏิบัติโดยสมัครใจสำหรับองค์กรต่างๆ เพื่อปรับปรุงแนวปฏิบัติด้านความปลอดภัยไซเบอร์ NIST CSF 1.0 ได้รับความนิยมอย่างรวดเร็วและกลายเป็นเครื่องมือที่ได้รับการยอมรับอย่างกว้างขวางในหลากหลายอุตสาหกรรม นำเสนอแนวทางที่มีโครงสร้างสำหรับการจัดการและลดความเสี่ยงด้านความปลอดภัยไซเบอร์ ในปี 2018 NIST ได้เปิดตัว CSF 1.1 ซึ่งมีการอัปเดตเพื่อจัดการกับความสำคัญที่เพิ่มขึ้นของการจัดการความเสี่ยงในห่วงโซ่อุปทาน และเพื่อให้คำแนะนำเพิ่มเติมเกี่ยวกับการตรวจสอบสิทธิ์ การอนุญาต และการพิสูจน์ตัวตน

NIST CSF 2.0 ถือเป็นการปรับปรุงที่สำคัญที่สุดของกรอบการทำงานนี้ เผยแพร่เป็นฉบับร่างสาธารณะในปี 2023 และเวอร์ชันสุดท้ายในเดือนกุมภาพันธ์ 2024 เวอร์ชันนี้นำเสนอฟังก์ชัน “Govern” ขยายฟังก์ชันหลักที่มีอยู่ และปรับกรอบการทำงานให้สอดคล้องกับความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบัน เสี่ยงตอบรับจากผู้มีส่วนได้ส่วนเสียหลายฝ่าย รวมถึงบริษัทในกลุ่ม Fortune 500 ได้นำมาสู่การพัฒนา NIST CSF 2.0 เพื่อให้แน่ใจว่าสามารถตอบสนองความต้องการขององค์กรต่างๆ ในปัจจุบันได้

กรอบงานนี้ประกอบด้วยองค์ประกอบหลักสามส่วน ได้แก่ “แกนหลัก (Core), โปรไฟล์ (Profiles) และ “ระดับ Tiers.”) แกนหลักประกอบด้วยชุดกิจกรรม ผลลัพธ์ และเอกสารอ้างอิงที่ครอบคลุมเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในแง่มุมต่างๆ ระดับการใช้งาน (Implementation Tiers) ช่วยให้องค์กรต่างๆ ประเมินแนวปฏิบัติและความซับซ้อนของความมั่นคงปลอดภัยไซเบอร์ได้ ขณะที่โปรไฟล์ช่วยให้องค์กรต่างๆ สามารถปรับแต่งกรอบงานให้สอดคล้องกับข้อกำหนดเฉพาะและการประเมินความเสี่ยงได้

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST Cybersecurity Framework: CSF) 2.0 เป็นเวอร์ชันปรับปรุงของกรอบการทำงานเดิมที่สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) นำมาใช้กรอบการทำงานนี้ออกแบบมาเพื่อช่วยให้องค์กรต่างๆ จัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST (NIST CSF) เป็นชุดแนวทางปฏิบัติที่ดีที่สุดที่มีความยืดหยุ่น ซึ่งออกแบบมาเพื่อช่วยให้องค์กรต่างๆ ปรับปรุงความปลอดภัยของข้อมูลและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

NIST CSF v2.0 แนะนำการอัปเดตที่ปรับปรุงการเน้นไปที่การกำกับดูแล (เพิ่มฟังก์ชันหลักที่หกที่เรียกว่า "Govern") การจัดการความเสี่ยงของห่วงโซ่อุปทาน และการวัดผลลัพธ์ของความปลอดภัยทางไซเบอร์ ขณะเดียวกันก็สอดคล้องกับมาตรฐานสากลมากขึ้นและปรับปรุงความยืดหยุ่นสำหรับองค์กรที่หลากหลาย

2.4.1 ฟังก์ชันและหมวดหมู่ของกิจกรรมด้านความปลอดภัยทางไซเบอร์ (Functions and categories of cybersecurity activities)

กรอบงานความมั่นคงปลอดภัยไซเบอร์ของ NIST ได้จัดเนื้อหาหลัก ("แกนหลัก") ออกเป็น 5 "ฟังก์ชัน" ซึ่งแบ่งย่อยออกเป็น 23 "หมวดหมู่" ในแต่ละหมวดหมู่ กรอบงานได้กำหนดหมวดหมู่ย่อยของผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์และการควบคุมความปลอดภัยจำนวนหนึ่ง โดยมีทั้งหมด 108 หมวดหมู่อย่อย

สำหรับแต่ละหมวดหมู่อย่อย ยังมี "แหล่งข้อมูล" ที่อ้างอิงถึงส่วนเฉพาะของมาตรฐานความปลอดภัยทางสารสนเทศอื่นๆ อีกมากมาย รวมถึง ISO 27001 , COBIT , NIST SP 800-53, ANSI/ISA-62443 และ Council on CyberSecurity Critical Security Controls (CCS CSC ซึ่งปัจจุบันอยู่ภายใต้การดูแลของศูนย์ความปลอดภัยทางอินเทอร์เน็ต)



รูป 2.3 NIST CSF 1.1
(ที่มา nist.gov)

NIST CSF 2.0 มีโครงสร้างหลัก 6 ประการ ซึ่งแต่ละประการมีความสำคัญอย่างยิ่งต่อโครงการรักษาความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ ซึ่งรวมถึงเสาหลัก 5 ประการดั้งเดิมจาก NIST 1.1 ได้แก่ ระบุตัวตน

(Identify), ป้องกัน (Protect), ตรวจจับ (Detect), ตอบสนอง (Respond) และกู้คืน (Recover) และได้เพิ่มฟังก์ชัน “Govern” เข้ามาใหม่



รูป 2.4 NIST CSF 2.0

(ที่มา nist.gov)

กรอบการทำงานนี้นำเสนอแนวทางที่ครอบคลุมสำหรับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เสาหลักเหล่านี้ถือเป็นขั้นตอนสำคัญของโครงการความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่ง ซึ่งเป็นแนวทางให้องค์กรต่างๆ เข้าใจ จัดการ และลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เสาหลักแต่ละเสาประกอบด้วยกิจกรรมสำคัญที่มีความสำคัญอย่างยิ่งต่อกลยุทธ์ความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ NIST CSF 2.0 มีรายละเอียดดังนี้

2.4.2 ฟังก์ชันใน NIST CSF 2.0

1) กำกับดูแล (ใหม่ใน NIST CSF 2.0)

ฟังก์ชัน**กำกับดูแล (GOVERN)** เป็นส่วนเพิ่มเติมที่ครอบคลุมยิ่งขึ้น เพื่อเน้นย้ำถึงความสำคัญของการกำกับดูแลในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ หน้าที่นี้มุ่งเน้นไปที่การจัดตั้งและรักษาโครงสร้างการกำกับดูแลที่จำเป็นสำหรับองค์กรในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจและข้อกำหนดทางกฎหมาย

หมวดหมู่การกำกับดูแล 6 ประเภท:

- บริบทองค์กร (GV.OC)
- กลยุทธ์การบริหารความเสี่ยง (GV.RM)
- บทบาท ความรับผิดชอบ และอำนาจหน้าที่ (GV.RR)
- นโยบาย (GV.PO)
- การกำกับดูแล (GV.OV)
- การจัดการความเสี่ยงในห่วงโซ่อุปทานความปลอดภัยทางไซเบอร์ (GV.SC)

กิจกรรมหลัก ได้แก่:

- การกำหนดเป้าหมายการจัดการความเสี่ยงโดยได้รับความยินยอมจากผู้มีส่วนได้ส่วนเสียในองค์กร
- การสร้างวิธีการมาตรฐานสำหรับการคำนวณ การบันทึก การจัดหมวดหมู่ และการจัดลำดับความสำคัญของความเสี่ยงด้านความปลอดภัยทางไซเบอร์
- การกำหนดและรักษาระดับการยอมรับความเสี่ยงและคำชี้แจงความคลาดเคลื่อนของความเสี่ยง
- รวมถึงกิจกรรมการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์และผลลัพธ์ในการจัดการความเสี่ยงขององค์กร
- การจัดตั้งและการสื่อสารบทบาท ความรับผิดชอบ และอำนาจหน้าที่ด้านความปลอดภัยทางไซเบอร์
- การทบทวนและปรับปรุงกลยุทธ์การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์เพื่อให้ครอบคลุมความเสี่ยงและข้อกำหนดขององค์กร
- การประเมินประสิทธิภาพการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ขององค์กรและการปรับเปลี่ยนที่จำเป็น
- การจัดทำช่องทางการสื่อสารสำหรับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ทั่วทั้งองค์กร รวมถึงซัพพลายเออร์และบุคคลที่สาม

กิจกรรมเหล่านี้ช่วยให้มั่นใจได้ว่าความพยายามด้านความปลอดภัยทางไซเบอร์ได้รับการประสานงานอย่างมีประสิทธิภาพ สอดคล้องกับเป้าหมายทางธุรกิจ และบริหารจัดการอย่างมีประสิทธิภาพในระดับสูงสุดขององค์กร การกำกับดูแลจึงมีความสำคัญอย่างยิ่งยวดเพื่อให้มั่นใจว่าความปลอดภัยทางไซเบอร์จะถูกผนวกเข้ากับกลยุทธ์โดยรวมขององค์กร และความเสี่ยงได้รับการจัดการอย่างสอดคล้องและมีประสิทธิภาพในทุกระดับขององค์กร

2) ระบุ (IDENTIFY)

ฟังก์ชันระบุ (Identify) ถือเป็นรากฐานสำคัญของโปรแกรมรักษาความปลอดภัยทางไซเบอร์ที่ประสบความสำเร็จ ช่วยให้องค์กรต่างๆ เข้าใจสภาพแวดล้อมและความเสี่ยงที่เกี่ยวข้องอย่างลึกซึ้ง องค์กรต่างๆ สามารถจัดลำดับความสำคัญของความปลอดภัยทางไซเบอร์ได้โดยการระบุสินทรัพย์สำคัญ จุดอ่อน และบริบททางธุรกิจที่กว้างขึ้น

ระบุ 3 หมวดหมู่:

- บริษัทจัดการสินทรัพย์ (ID.AM)
- การประเมินความเสี่ยง (ID.RA)
- การปรับปรุง (ID.IM)

กิจกรรมหลัก ได้แก่:

- การระบุสินทรัพย์ทางกายภาพและซอฟต์แวร์เพื่อสร้างพื้นฐานของโปรแกรมการจัดการสินทรัพย์
- การระบุสภาพแวดล้อมทางธุรกิจขององค์กร รวมถึงบทบาทในห่วงโซ่อุปทาน
- ระบุนโยบายความปลอดภัยทางไซเบอร์ที่จัดตั้งขึ้นเพื่อกำหนดโปรแกรมการกำกับดูแล ตลอดจนระบุข้อกำหนดทางกฎหมายและข้อบังคับที่เกี่ยวข้องกับความสามารถด้านความปลอดภัยทางไซเบอร์ขององค์กร
- การระบุจุดอ่อนของสินทรัพย์ ภัยคุกคามต่อทรัพยากรองค์กรภายในและภายนอก และกิจกรรมการตอบสนองความเสี่ยงเพื่อประเมินความเสี่ยง
- การกำหนดกลยุทธ์การจัดการความเสี่ยง รวมถึงการระบุระดับการยอมรับความเสี่ยง
- การระบุกลยุทธ์การจัดการความเสี่ยงในห่วงโซ่อุปทาน รวมถึงลำดับความสำคัญ ข้อจำกัด การยอมรับความเสี่ยง และสมมติฐานที่ใช้สนับสนุนการตัดสินใจเกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับการจัดการความเสี่ยงในห่วงโซ่อุปทาน

กิจกรรมเหล่านี้ช่วยให้องค์กรต่างๆ เข้าใจถึงสถานะความปลอดภัยทางไซเบอร์ของตนอย่างครอบคลุม และมั่นใจได้ว่าองค์กรมีความพร้อมที่จะจัดการและลดความเสี่ยงได้อย่างมีประสิทธิภาพ ฟังก์ชันระบุตัวตน (Identify) เป็นรากฐานของฟังก์ชันที่ตามมาทั้งหมด (ปกป้อง ตรวจสอบ ตอบสนอง และกู้คืน) ภายใน NIST CSF

3) ปกป้อง (PROTECT)

ฟังก์ชัน**ปกป้อง** มุ่งเน้นไปที่การนำมาตรการป้องกันที่เหมาะสมมาใช้เพื่อให้แน่ใจว่ามีการส่งมอบบริการ โครงสร้างพื้นฐานที่สำคัญและเพื่อจำกัดหรือควบคุมผลกระทบของเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้น

5 หมวดหมู่การปกป้อง:

- การจัดการข้อมูลประจำตัว การตรวจสอบสิทธิ์ และการควบคุมการเข้าถึง (PR.AA)
- การสร้างความตระหนักรู้และการฝึกอบรม (PR.AT)
- ความปลอดภัยของข้อมูล (PR.DS)
- ความปลอดภัยของแพลตฟอร์ม (PR.PS)
- ความยืดหยุ่นของโครงสร้างพื้นฐานด้านเทคโนโลยี (PR.IR)

กิจกรรมหลัก ได้แก่:

- การนำการป้องกันไปใช้สำหรับการจัดการข้อมูลประจำตัวและการควบคุมการเข้าถึงภายในองค์กร รวมถึงการเข้าถึงทางกายภาพและระยะไกล
- ส่งเสริมพนักงานผ่านการฝึกอบรมความตระหนักรู้ด้านความปลอดภัย รวมถึงการฝึกอบรมผู้ใช้ตามบทบาทและผู้ใช้ที่มีสิทธิพิเศษ
- การสร้างการป้องกันความปลอดภัยของข้อมูลที่สอดคล้องกับกลยุทธ์ความเสี่ยงขององค์กรเพื่อปกป้องความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูล
- การนำกระบวนการและขั้นตอนไปปฏิบัติเพื่อบำรุงรักษาและจัดการการปกป้องระบบสารสนเทศและสินทรัพย์
- การปกป้องทรัพยากรขององค์กรผ่านการบำรุงรักษา รวมถึงกิจกรรมการบำรุงรักษาระยะไกล
- การจัดการเทคโนโลยีเพื่อให้มั่นใจถึงความปลอดภัยและความยืดหยุ่นของระบบ สอดคล้องกับนโยบาย ขั้นตอน และข้อตกลงขององค์กร

การนำมาตรการป้องกันที่เหมาะสมมาใช้จะช่วยให้องค์กรต่างๆ ปกป้องระบบสารสนเทศและทรัพย์สินของตนจากภัยคุกคามทางไซเบอร์ ฟังก์ชันการปกป้อง (Protect) มีความสำคัญอย่างยิ่งยวดต่อการรับประกันว่าบริการสำคัญขององค์กรจะทำงานอย่างปลอดภัยและมีประสิทธิภาพ แม้ในยามที่ต้องเผชิญกับความท้าทายด้านความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น

4) ตรวจจับ (DETECT)

ฟังก์ชัน**ตรวจจับ**มุ่งเน้นไปที่การระบุเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่เกิดขึ้นอย่างทันท่วงที ฟังก์ชันนี้มีความสำคัญอย่างยิ่งต่อการรับรู้และตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นได้อย่างรวดเร็ว

หมวดหมู่การตรวจจับมี 2 ประเภท:

- การติดตามอย่างต่อเนื่อง (DE.CM)
- การวิเคราะห์เหตุการณ์ไม่พึงประสงค์ (DE.AE)

กิจกรรมหลัก ได้แก่:

- การตรวจสอบให้แน่ใจว่าตรวจพบความผิดปกติและเหตุการณ์ต่างๆ และเข้าใจถึงผลกระทบที่อาจเกิดขึ้น
- การนำความสามารถในการตรวจสอบอย่างต่อเนื่องไปใช้เพื่อติดตามเหตุการณ์ด้านความปลอดภัยทางไซเบอร์และตรวจสอบประสิทธิผลของมาตรการป้องกัน รวมถึงกิจกรรมเครือข่ายและทางกายภาพ

กิจกรรมเหล่านี้มีความสำคัญอย่างยิ่งต่อการช่วยให้องค์กรสามารถตรวจจับและตอบสนองต่อเหตุการณ์ทางไซเบอร์ได้อย่างรวดเร็ว ช่วยลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงาน ฟังก์ชันตรวจจับ (Detect) เป็นองค์ประกอบสำคัญของกลยุทธ์ความปลอดภัยทางไซเบอร์เชิงรุก ช่วยให้องค์กรสามารถระบุและบรรเทาภัยคุกคามได้ตั้งแต่เนิ่นๆ ก่อนที่จะก่อให้เกิดความเสียหายร้ายแรง

5) ตอบสนอง (RESPOND)

ฟังก์ชันตอบสนอง มุ่งเน้นการพัฒนาและดำเนินการตามมาตรการที่เหมาะสมเพื่อควบคุมผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ฟังก์ชันนี้มีความสำคัญอย่างยิ่งต่อการจัดการและบรรเทาผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ

หมวดหมู่การตอบสนอง 4 ประเภท:

- การจัดการเหตุการณ์ (RS.MA)
- การวิเคราะห์เหตุการณ์ (RS.AN)
- การรายงานและการสื่อสารการตอบสนองต่อเหตุการณ์ (RS.CO)
- การบรรเทาเหตุการณ์ (RS.MI)

กิจกรรมหลัก ได้แก่:

- การรับรองว่ากระบวนการวางแผนการตอบสนองได้รับการดำเนินการในระหว่างและหลังเหตุการณ์
- การจัดการการสื่อสารกับผู้มีส่วนได้ส่วนเสียภายในและภายนอกในระหว่างและหลังเหตุการณ์
- การวิเคราะห์เหตุการณ์เพื่อให้แน่ใจว่ามีการตอบสนองอย่างมีประสิทธิภาพและสนับสนุนกิจกรรมการฟื้นฟู รวมถึงการวิเคราะห์นิติวิทยาศาสตร์และการกำหนดผลกระทบของเหตุการณ์
- ดำเนินการบรรเทาผลกระทบเพื่อป้องกันการขยายตัวของเหตุการณ์และแก้ไขเหตุการณ์
- การนำการปรับปรุงมาใช้โดยนำบทเรียนที่เรียนรู้จากกิจกรรมการตรวจจับ/ตอบสนองในปัจจุบันและก่อนหน้านี้นี้มาใช้

กิจกรรมเหล่านี้ช่วยให้องค์กรสามารถตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ ลดความเสียหายให้น้อยที่สุด และช่วยให้สามารถฟื้นตัวได้อย่างรวดเร็ว ฟังก์ชัน Respond ช่วยให้องค์กรสามารถจัดการและฟื้นตัวจากเหตุการณ์ต่างๆ ได้อย่างมีประสิทธิภาพ พร้อมทั้งยังคงรักษาความต่อเนื่องทางธุรกิจ

6) การกู้คืน (RECOVER)

ฟังก์ชันกู้คืน (Recover) มุ่งเน้นการพัฒนาและดำเนินแผนและกิจกรรมต่างๆ เพื่อฟื้นฟูขีดความสามารถหรือบริการใดๆ ที่เสียหายจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ เป้าหมายคือเพื่อให้แน่ใจว่าสามารถกู้คืนการดำเนินงานกลับสู่ภาวะปกติได้ทันเวลาที่ และปรับปรุงความสามารถในการรับมือต่อเหตุการณ์ในอนาคต

หมวดหมู่การกู้คืน 2 ประเภท:

- การดำเนินการตามแผนฟื้นฟูเหตุการณ์ (RC.RP)
- การสื่อสารการกู้คืนเหตุการณ์ (RC.CO)

กิจกรรมหลัก ได้แก่:

- การรับรองว่าองค์กรได้นำกระบวนการและขั้นตอนการวางแผนการกู้คืนไปใช้เพื่อคืนระบบและ/หรือทรัพย์สินที่ได้รับผลกระทบจากเหตุการณ์ทางไซเบอร์

- การดำเนินการปรับปรุงตามบทเรียนที่ได้รับและการทบทวนกลยุทธ์ที่มีอยู่
- การสื่อสารภายในและภายนอกได้รับการประสานงานระหว่างและหลังการฟื้นตัวจากเหตุการณ์ทางไซเบอร์

กิจกรรมเหล่านี้ช่วยให้องค์กรฟื้นฟูการดำเนินงานได้อย่างมีประสิทธิภาพหลังเกิดเหตุการณ์ทางไซเบอร์ ลดระยะเวลาในการกู้คืน และเพิ่มความยืดหยุ่นด้วยการเรียนรู้จากเหตุการณ์แต่ละครั้ง ฟังก์ชันการกู้คืนมีความสำคัญอย่างยิ่งต่อการรักษาความต่อเนื่องทางธุรกิจ และช่วยให้มั่นใจว่าองค์กรสามารถกลับสู่การดำเนินงานตามปกติได้อย่างรวดเร็วโดยเกิดการหยุดชะงักน้อยที่สุด

2.4.4 ประโยชน์ของกรอบงาน NIST CSF 2.0

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ของ NIST (CSF) นำเสนอแนวทางเชิงโครงสร้างสำหรับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ผ่านฟังก์ชันหลัก ได้แก่ ระบุ ป้องกัน ตรวจสอบ ตอบสนอง และกู้คืน NIST CSF 2.0 ได้เพิ่มฟังก์ชันที่หก คือ กำกับดูแล ซึ่งมุ่งเน้นการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์และการปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

ประโยชน์หลัก:

- **การจัดการความเสี่ยงอย่างครอบคลุม:** นำเสนอวิธีการที่ชัดเจนในการระบุ ประเมิน และจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ โดยจัดแนวความพยายามเหล่านี้ให้สอดคล้องกับกลยุทธ์ทางธุรกิจโดยรวม
- **ความยืดหยุ่นและความสามารถในการปรับขนาด:** ปรับให้เหมาะกับองค์กรทุกขนาดหรือทุกอุตสาหกรรม พร้อมด้วยคำแนะนำที่ได้รับการปรับปรุงใน CSF 2.0 สำหรับการปรับแต่งกรอบงานให้เหมาะสมกับความต้องการเฉพาะและภัยคุกคามที่เปลี่ยนแปลงไป
- **การปฏิบัติตามกฎระเบียบ:** ช่วยตอบสนองข้อกำหนดด้านกฎระเบียบ ลดความเสี่ยงของค่าปรับและปัญหาทางกฎหมาย และฟังก์ชันการกำกับดูแลช่วยเสริมสร้างการจัดแนวการปฏิบัติตามกฎระเบียบ
- **ความยืดหยุ่นทางไซเบอร์ที่เพิ่มขึ้น:** ปรับปรุงการตรวจสอบ การตอบสนอง และการกู้คืนจากเหตุการณ์ต่างๆ รองรับความต่อเนื่องทางธุรกิจและการปรับตัวให้เข้ากับภัยคุกคามใหม่ๆ
- **การยอมรับจากอุตสาหกรรม:** NIST CSF เป็นหนึ่งในกรอบงานด้านความปลอดภัยที่ได้รับการยอมรับมากที่สุดในทุกอุตสาหกรรม และการเพิ่มฟังก์ชัน Govern สะท้อนให้เห็นถึงความสำคัญที่เพิ่มมากขึ้นของความปลอดภัยทางไซเบอร์ในธรรมาภิบาลขององค์กร
- **การรายงานผลคณะกรรมการที่ดีขึ้น:** กรอบการทำงานของ NIST ทำงานได้ดีมากสำหรับการรายงานผลในระดับคณะกรรมการ

2.5 กลไกและการตอบสนองต่ออุบัติการณ์ตามแนวทาง NIST Cybersecurity Framework

การตอบสนองต่ออุบัติการณ์ เป็นกระบวนการที่ใช้ในการรับมือกับเหตุการณ์ที่อาจมีผลกระทบต่อความมั่นคงปลอดภัย เป็นกระบวนการที่มีโครงสร้างที่องค์กรต่างๆ ใช้เพื่อระบุและจัดการกับเหตุการณ์ทางไซเบอร์ กรอบการทำงานของ NIST สำหรับการตอบสนองต่อเหตุการณ์เป็นวิธีการที่องค์กรต่างๆ ใช้ในการตรวจจับ ควบคุม และกู้คืนเหตุการณ์ด้านความปลอดภัยได้อย่างมีประสิทธิภาพ เนื้อหาในส่วนนี้ จะอธิบายวงจรชีวิต 4 ระยะของ NIST ได้แก่ การเตรียมการและการป้องกัน การตรวจจับและการวิเคราะห์ การจำกัด การกำจัด และการกู้คืน รวมถึงกิจกรรมหลังเกิดเหตุการณ์ ซึ่งถือเป็นกลยุทธ์สำคัญในการวางแผนความต่อเนื่องทางธุรกิจ (BCP: Business Continuity Plan)

2.5.1 กรอบการทำงานการตอบสนองต่อเหตุการณ์ของ NIST คืออะไร

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เป็นหน่วยงานที่ดำเนินการโดยกระทรวงพาณิชย์ สหรัฐอเมริกา ซึ่งกำหนดมาตรฐานและคำแนะนำสำหรับภาคส่วนเทคโนโลยีต่างๆ มากมาย ภายใน NIST ห้องปฏิบัติการเทคโนโลยีสารสนเทศ (ITL) มีหน้าที่รับผิดชอบในการพัฒนามาตรฐานและวิธีการวัดผลด้านไอที รวมถึงความปลอดภัยของข้อมูล ITL ได้พัฒนาแบบจำลองที่มีอิทธิพลสำหรับการตอบสนองต่อเหตุการณ์ (IR) ซึ่งก็คือ คู่มือการจัดการเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์

กรอบการทำงานการตอบสนองต่อเหตุการณ์ของ NIST (NIST Incident Response Framework) หรือกระบวนการรับมือเหตุการณ์ เป็นกิจกรรมต่อเนื่องที่ช่วยให้องค์กรต่างๆ เรียนรู้วิธีการป้องกันตนเอง ซึ่งประกอบด้วย 4 ขั้นตอนหลัก ได้แก่ การเตรียมการ การตรวจจับ/วิเคราะห์ การควบคุม/การกำจัด และการฟื้นฟู

NIST ให้คำแนะนำเกี่ยวกับการตอบสนองต่อเหตุการณ์ เพื่อช่วยให้องค์กรต่างๆ กำหนดกระบวนการจัดการเหตุการณ์ทางไซเบอร์ที่ได้มาตรฐาน มีประสิทธิภาพ และทำซ้ำได้ คำแนะนำเหล่านี้อ้างอิงจากแนวปฏิบัติที่ดีที่สุดในอุตสาหกรรมและงานวิจัยที่ครอบคลุม เพื่อให้มั่นใจว่าองค์กรต่างๆ จะสามารถบรรเทาภัยคุกคามด้านความปลอดภัยได้อย่างมีประสิทธิภาพ

NIST มุ่งมั่นที่จะส่งเสริมแนวทางที่เป็นหนึ่งเดียวในการรับมือกับเหตุการณ์ที่เกิดขึ้นในภาคอุตสาหกรรม และหน่วยงานภาครัฐ NIST จัดทำกรอบการทำงานที่ได้รับการยอมรับอย่างกว้างขวาง เพื่อให้มั่นใจว่าองค์กรทุกขนาดและทุกภาคส่วนสามารถนำแนวปฏิบัติด้านความปลอดภัยที่สอดคล้องกันไปปรับใช้ เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ทั้งในระดับประเทศและระดับโลก

นอกจากนั้น คำแนะนำของ NIST ส่งเสริมการปรับปรุงอย่างต่อเนื่อง กรอบการทำงานนี้เน้นย้ำบทเรียนที่ได้รับ ช่วยให้องค์กรต่างๆ ปรับปรุงกระบวนการรับมือเหตุการณ์ตามระยะเวลา เพื่อเตรียมความพร้อมรับมือกับภัยคุกคามในอนาคตได้ดียิ่งขึ้น

2.5.2 วงจรชีวิตการตอบสนองต่ออุบัติการณ์ของ NIST

วงจรชีวิตการตอบสนองต่ออุบัติการณ์ของ NIST (NIST Incident Response Life Cycle) กำหนดกระบวนการ 4 ขั้นตอน สำหรับการตอบสนองต่อเหตุการณ์ ดังแสดงในรูป 2.5



รูป 2.5 4 ขั้นตอนวงจรชีวิตการตอบสนองต่ออุบัติการณ์ของ NIST

1) การเตรียมพร้อม (Preparation)

ขั้นตอน "การเตรียมพร้อม" ของวงจรการตอบสนองเหตุการณ์ของ NIST มุ่งเน้นไปที่การนำ นโยบาย และ หน้าที่ในการรับมือเหตุการณ์มาใช้ รวมถึงการป้องกัน เหตุการณ์ทางไซเบอร์การเตรียมการและการป้องกัน เหตุการณ์อาจเป็นเรื่องที่น่ากังวลหากเรายังไม่ได้เผชิญกับภัยคุกคามและยังไม่ทราบถึงรูปแบบที่แท้จริงของภัยคุกคาม ในการเตรียมการสำหรับเหตุการณ์ทางไซเบอร์ NIST แนะนำให้ใช้ชุดเครื่องมือล่วงหน้า เพื่อให้พร้อมสำหรับการวิเคราะห์ แยกแยะ และตอบสนองต่อเหตุการณ์ ซึ่งรวมถึงการจัดหาเครื่องมือและสิ่งอำนวยความสะดวกด้านการสื่อสารสำหรับบุคลากรที่รับสายซึ่งจะจัดการกับเหตุการณ์สำคัญหากเกิดขึ้น หรือตั้งแต่การมีข้อมูลติดต่อที่พร้อมใช้งานสำหรับผู้มีส่วนได้ส่วนเสียและหน่วยงานที่รายงาน ไปจนถึงการซื้อสมาร์ตโฟนสำหรับทีมรับมือเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์ ไปจนถึงการมีพื้นที่ว่างสำหรับ "ศูนย์บัญชาการรบ" ที่ทีมสามารถรวมตัวกันและจัดการวิกฤตได้ นอกจากนี้ยังช่วยให้มั่นใจได้ว่าจะมีเครื่องมือและทรัพยากรที่จำเป็น เช่น ซอฟต์แวร์นิติวิทยาศาสตร์ เครื่องมือตรวจสอบ และกลไกการสื่อสารพร้อมใช้งาน

แม้ว่าเอกสารเผยแพร่พิเศษของ NIST ฉบับนี้จะได้ครอบคลุมรายละเอียดเฉพาะของการรักษาความปลอดภัยระบบสารสนเทศ แต่ก็เน้นย้ำถึงความสำคัญของการป้องกันซึ่งเป็นส่วนหนึ่งของการจัดการเหตุการณ์ การป้องกันเหตุการณ์และอุบัติการณ์ขึ้นอยู่กับการรักษาความปลอดภัยสภาพแวดล้อมไอทีของคุณ และการตรวจสอบระบบและเครือข่ายของคุณอย่างต่อเนื่องเพื่อตรวจจับความผิดปกติใดๆ NIST ขอแนะนำแนวทางปฏิบัติต่อไปสำหรับการรักษาความปลอดภัยระบบของคุณและการป้องกันอุบัติการณ์

- ดำเนินการประเมินความเสี่ยงเป็นระยะและความพยายามบรรเทาความเสี่ยงที่สอดคล้องกันเพื่อทำความเข้าใจสภาพแวดล้อมความเสี่ยงด้านไอที
- ใช้แนวทางปฏิบัติและการกำหนดค่าที่ดีที่สุดในการเสริมความแข็งแกร่งให้กับระบบและเซิร์ฟเวอร์กับโครงสร้างพื้นฐานด้านไอที
- รักษาความปลอดภัยขอบเขตเครือข่ายของคุณและปฏิเสธการเข้าถึงโดยไม่ได้รับอนุญาต
- ใช้ซอฟต์แวร์ป้องกันมัลแวร์และป้องกันไวรัสเพื่อปกป้องทรัพย์สินของบริษัท
- ฝึกอบรมผู้ใช้เกี่ยวกับนโยบาย ขั้นตอน ความตระหนักด้านความปลอดภัย และการใช้งานทรัพยากรไอทีอย่างเหมาะสม

การเตรียมการถือเป็นขั้นตอนแรกในกระบวนการรับมือเหตุการณ์ตามมาตรฐาน NIST และสามารถเกิดขึ้นได้ตลอดวงจรการจัดการเหตุการณ์ การยกระดับความสามารถด้านความปลอดภัย การใช้ระบบอัตโนมัติเพื่อเพิ่มประสิทธิภาพการควบคุม และการกำหนดมาตรฐานประสิทธิภาพระบบและปริมาณการรับส่งข้อมูลเครือข่าย ถือเป็นส่วนหนึ่งของขั้นตอนการเตรียมการ แต่สามารถทำได้แม้ในขั้นตอนอื่นๆ ของกระบวนการรับมือเหตุการณ์กำลังดำเนินไปพร้อมกัน

เพื่อเตรียมความพร้อมสำหรับเหตุการณ์ ให้รวบรวมรายการสินทรัพย์ไอที เช่น เครือข่าย เซิร์ฟเวอร์ และอุปกรณ์ปลายทาง โดยระบุถึงความสำคัญและปัจจัยสำคัญหรือข้อมูลสำคัญที่จัดเก็บข้อมูลสำคัญ ตั้งค่าการตรวจสอบเพื่อให้มีข้อมูลพื้นฐานเกี่ยวกับกิจกรรมปกติ กำหนดประเภทของเหตุการณ์ด้านความปลอดภัยที่ควรตรวจสอบ และกำหนดขั้นตอนการตอบสนองโดยละเอียดสำหรับเหตุการณ์ประเภททั่วไป

2) การตรวจจับและการวิเคราะห์ (Detection and Analysis)

การตรวจจับเกี่ยวข้องกับการรวบรวมข้อมูลจากระบบไอที เครื่องมือรักษาความปลอดภัย ข้อมูลที่เปิดเผยต่อสาธารณะ และบุคคลภายในและภายนอกองค์กร และระบุสัญญาณบ่งชี้ (สัญญาณที่บ่งบอกว่าเหตุการณ์อาจเกิดขึ้นในอนาคต) และตัวบ่งชี้ (ข้อมูลที่แสดงว่าการโจมตีได้เกิดขึ้นหรือกำลังเกิดขึ้นอยู่)

ขั้นตอนการตรวจจับและวิเคราะห์จำเป็นต้องระบุประเภทของภัยคุกคามที่กำลังเผชิญก่อน และพิจารณาว่าเป็นเหตุการณ์ที่เกิดขึ้นจริงหรือไม่ NIST ได้จัดทำรายการประเภทภัยคุกคามที่อาจเกิดขึ้น และแบ่งสัญญาณของเหตุการณ์ออกเป็นสองประเภท ได้แก่ สัญญาณบ่งชี้และสัญญาณเตือนภัย

สัญญาณเตือนล่วงหน้า (precursor) คือสัญญาณบ่งชี้ว่าเหตุการณ์อาจเกิดขึ้นในอนาคต และตัวบ่งชี้ (indicator) คือสัญญาณบ่งชี้ว่าเหตุการณ์นั้นอาจเกิดขึ้นในปัจจุบันหรือเกิดขึ้นแล้ว ตัวอย่างของสัญญาณเตือนล่วงหน้า เช่น กลุ่มแฮกเกอร์แจ้งองค์กรว่ามีแผนจะโจมตี ตัวอย่างของสัญญาณเตือน เช่น การตรวจจับกิจกรรมที่ผิดปกติในเซิร์ฟเวอร์ที่มีสิทธิ์พิเศษ นำเสียดายที่สัญญาณของการโจมตีส่วนใหญ่มักจะมองเห็นได้หลังจากการโจมตีได้เริ่มต้นขึ้นแล้ว แต่องค์กรที่มีความสามารถในการรับมือกับเหตุการณ์ล่วงหน้า (incident Response) ที่ดีอาจสามารถตรวจจับสัญญาณเตือนล่วงหน้าและป้องกันการโจมตีได้ก่อนที่จะเริ่มต้นขึ้นการใช้เครื่องมืออัตโนมัติ เช่น ระบบตรวจจับการบุกรุก (IDS) และระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย (SIEM) จะช่วยระบุเหตุการณ์ที่อาจเกิดขึ้นดังกล่าว

บริษัทส่วนใหญ่จะใช้ตัวบ่งชี้ ซึ่งจะเป็แนวทางให้สามารถระบุแหล่งที่มาของการโจมตี วิธีควบคุม และระยะเวลาในการรวบรวมหลักฐาน เทคนิคบางอย่างที่ทีมรักษาความปลอดภัยสามารถใช้ในการวิเคราะห์เหตุการณ์ ได้แก่:

- ทำความคุ้นเคยกับสภาพแวดล้อมไอทีและพฤติกรรมเชิงบรรทัดฐานเพื่ออำนวยความสะดวกในการตรวจจับความผิดปกติ
- กำหนดนโยบายการเก็บรักษาบันทึกและดูแลรักษาบันทึกในระบบต่างๆ เนื่องจากสามารถรวบรวมข้อมูลเหตุการณ์ในสถานที่และระบบต่างๆ ได้
- จัดทำแผนที่เหตุการณ์ต่างๆ ทั่วทั้งระบบเพื่อให้ได้ภาพรวมที่สมบูรณ์ของขอบเขตของการละเมิดความปลอดภัย เหตุการณ์ หรือเหตุการณ์ต่างๆ
- ซิงโครไนซ์นาฬิกาเซิร์ฟเวอร์เพื่อให้บันทึกมีความถูกต้อง
- จัดทำฐานความรู้เพื่อให้ผู้จัดการเหตุการณ์สามารถอ้างอิงได้อย่างง่ายดาย
- ใช้เทคโนโลยีการสแกน เช่น เครื่องดมแพ็กเก็ต เครื่องสแกนช่องโหว่ และเครื่องสแกนการอ้างอิง เพื่อรวบรวมข้อมูล

การวิเคราะห์เหตุการณ์ไม่ได้หยุดอยู่แค่การระบุตัวตนเท่านั้น แต่ขั้นตอนการตอบสนองเหตุการณ์นี้ยังครอบคลุมการบันทึกเหตุการณ์และจัดลำดับความสำคัญด้วย การจัดทำเอกสารถือเป็นหัวใจสำคัญของความปลอดภัย ความเสี่ยง และการปฏิบัติตามข้อกำหนด และสิ่งนี้ยังใช้ได้กับการจัดการเหตุการณ์ด้วย เหตุการณ์ควร

ได้รับการบันทึกในระบบบันทึกเหตุการณ์/ระบบติดตามปัญหา หรือระบบจัดเก็บข้อมูล โดยบันทึกสถานะและ กิจกรรมทั้งหมดที่เกี่ยวข้องกับเหตุการณ์นั้นไว้ในบันทึกเหตุการณ์ การสร้างเทมเพลตการตอบสนองเหตุการณ์จะ ช่วยอำนวยความสะดวกในการดำเนินการนี้ และช่วยให้มั่นใจได้ว่าข้อมูลที่เป็นทั้งหมดจะถูกบันทึกไว้

การจัดลำดับความสำคัญของเหตุการณ์เกี่ยวข้องกับการประเมินเหตุการณ์ที่เปิดอยู่เพื่อดูผลกระทบและความสามารถในการกู้คืน และการตัดสินใจโดยพิจารณาจากความต้องการของธุรกิจ บริษัทอาจประสบเหตุการณ์ หลายเหตุการณ์พร้อมกัน ขึ้นอยู่กับขนาดของธุรกิจและอุตสาหกรรม บริษัทนั้นอาจไม่มีทรัพยากรทั้งหมดที่จำเป็น ในการจัดการกับเหตุการณ์ที่เปิดอยู่ทั้งหมดในเวลาเดียวกัน ดังนั้น การจัดลำดับความสำคัญจึงเป็นสิ่งจำเป็น

การวิเคราะห์เกี่ยวข้องกับการระบุพื้นฐานหรือกิจกรรมปกติสำหรับระบบที่ได้รับผลกระทบ การเชื่อมโยง เหตุการณ์ที่เกี่ยวข้อง และพิจารณาว่าเหตุการณ์เหล่านั้นเบี่ยงเบนจากพฤติกรรมปกติหรือไม่ และอย่างไร

นอกจากนั้น ส่วนนี้ของวงจรยังรวมถึงการรายงานเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ภายในอย่าง ถูกต้องต่อหน่วยงานที่เกี่ยวข้อง เจ้าหน้าที่บังคับใช้กฎหมาย และ/หรือฝ่ายอื่นๆ ที่ได้รับผลกระทบ

3) การกักเก็บ การกำจัด และการฟื้นฟู (Containment, Eradication, and Recovery)

เป้าหมายของการกักเก็บ คือการหยุดยั้งการโจมตีก่อนที่จะใช้ทรัพยากรอย่างสิ้นเปลืองหรือก่อให้เกิดความเสียหาย กลยุทธ์การกักเก็บจะขึ้นอยู่กับระดับความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์ ความจำเป็นในการรักษา บริการสำคัญให้พนักงานและลูกค้าใช้งานได้ และระยะเวลาของการแก้ปัญหา ไม่ว่าจะเป็นการแก้ปัญหาชั่วคราว เพียงไม่กี่ชั่วโมงไม่กี่วัน หรือไม่ก็สัปดาห์ หรือการแก้ปัญหาแบบถาวร

ส่วนหนึ่งของการควบคุม สิ่งสำคัญคือต้องระบุโฮสต์ที่โจมตีและตรวจสอบที่อยู่ IP ของโฮสต์นั้น การทำ เช่นนี้ช่วยให้สามารถบล็อกการสื่อสารจากผู้โจมตี และระบุตัวผู้ก่อภัยคุกคาม เพื่อทำความเข้าใจรูปแบบการทำงาน ค้นหา และบล็อกช่องทางการสื่อสารอื่นๆ ที่ผู้โจมตีอาจใช้อยู่

การควบคุมการกำจัดและการฟื้นฟู เป็นส่วนสำคัญของการตอบสนองต่อเหตุการณ์ เชิงรุก ขั้นตอนนี้ของการตอบสนองต่อเหตุการณ์ประกอบด้วย การแยกภัยคุกคามและระบบที่ได้รับผลกระทบเพื่อให้แน่ใจว่าภัยคุกคาม จะไม่แพร่กระจาย อย่างไรก็ตาม เอกสาร ของ NIST ระบุอย่างชัดเจนว่ากลยุทธ์การควบคุมต้องสอดคล้องกับ ประเภทของการโจมตีและความเสียหายที่อาจเกิดขึ้นหากการโจมตียังคงดำเนินต่อไป ซึ่งจะต้องใช้กลยุทธ์การ ควบคุมทั้งระยะยาวและระยะสั้นเพื่อจำกัดผลกระทบ

นอกจากนี้ การตัดการเชื่อมต่อโฮสต์ที่โจมตีออกจากแหล่งข้อมูลเพียงอย่างเดียวอาจส่งผลเสียได้ NIST แนะนำว่าทีมตอบสนองเหตุการณ์ควรมีแผนการควบคุมเฉพาะสำหรับการโจมตีแต่ละประเภทที่คาดการณ์ไว้ โดยพิจารณาจากการประเมินและการวิเคราะห์ความเสี่ยง ขั้นตอนนี้ยังรวมถึงการระบุและวิจัยโฮสต์ที่โจมตี และ การรวบรวมหลักฐานที่สามารถนำไปใช้ในทางกฎหมายได้ NIST แนะนำว่าในบางกรณี ทีมตอบสนองอาจเลือกใช้

"แฮนด์บ็อกซ์" เพื่อควบคุมภัยคุกคามเพื่อกระตุ้นให้การโจมตีดำเนินต่อไป เพื่อให้ทีมสามารถรวบรวมข้อมูลเพิ่มเติมได้ แต่กลยุทธ์นี้มีความเสี่ยง

เมื่อควบคุมได้แล้ว ทีมรักษาความปลอดภัยไซเบอร์ของคุณจะสามารถดำเนินการกำจัดภัยคุกคาม รวมถึงการกำจัดมัลแวร์และการลบบัญชีที่ถูกบุกรุก สุดท้าย ทีมสามารถดำเนินการกู้คืนแบบเป็นขั้นตอน ซึ่งองค์กรสามารถกลับมาดำเนินงานตามปกติได้ การกู้คืนอาจรวมถึงการแก้ไขแพตช์รักษาความปลอดภัยไซเบอร์ การปรับปรุงไฟร์วอลล์ การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์และป้องกันไวรัสใหม่ การกู้คืนระบบจากการสำรองข้อมูลแบบปกติ และการเปลี่ยนรหัสผ่านทั่วทั้งองค์กร ในสภาพแวดล้อมแบบคอนเทนเนอร์ การกู้คืนอาจหมายถึงการสร้างฟังก์ชันใหม่ๆ และเครื่องเสมือนจากเทมเพลตซึ่งอาจรวมถึงการสร้างระบบใหม่ และการทดสอบอย่างละเอียดเพื่อให้แน่ใจว่าระบบปราศจากภัยคุกคาม ในสภาพแวดล้อมคอนเทนเนอร์ การกู้คืนอาจหมายถึงการสร้างฟังก์ชันใหม่และเครื่องเสมือนจากเทมเพลต อิมเมจ ด้วย

ในขั้นตอนการกำจัดและกู้คืน หลังจากควบคุมเหตุการณ์ได้สำเร็จแล้ว ควรดำเนินการเพื่อกำจัดองค์ประกอบทั้งหมดของเหตุการณ์ออกจากสภาพแวดล้อม ซึ่งอาจรวมถึงการระบุโฮสต์ที่ได้รับผลกระทบทั้งหมด การกำจัดมัลแวร์ และการปิดหรือรีเซ็ตรหัสผ่านสำหรับบัญชีผู้ใช้ที่ถูกละเมิด

นอกจากนั้น เมื่อภัยคุกคามถูกกำจัดแล้ว ให้คืนค่าระบบและกู้คืนการดำเนินการปกติโดยเร็วที่สุด โดยดำเนินการเพื่อให้แน่ใจว่าทรัพย์สินชุดเดิมจะไม่ถูกโจมตีอีก

4) กิจกรรมหลังเกิดเหตุการณ์ (Post-Incident Activity)

กระบวนการ NIST เน้นย้ำว่าการตอบสนองต่อเหตุการณ์ไม่ใช่กิจกรรมเชิงเส้นตรงที่เริ่มต้นเมื่อตรวจพบเหตุการณ์ และสิ้นสุดด้วยการกำจัดและฟื้นฟู แต่การตอบสนองต่อเหตุการณ์เป็นกิจกรรมแบบวัฏจักร ซึ่งมีการเรียนรู้และการพัฒนาอย่างต่อเนื่องเพื่อค้นพบวิธีการปกป้ององค์กรให้ดีขึ้น

NIST ระบุว่าขั้นตอน “กิจกรรมหลังเหตุการณ์” เป็นขั้นตอนที่มักถูกละเว้นมากที่สุดและสำคัญที่สุดหลังจากเกิดเหตุการณ์ ทีมควรจัดการประชุม “บทเรียนที่ได้รับ” เพื่อประมวลผลเหตุการณ์ ทบทวนกลยุทธ์ในการเก็บรักษาข้อมูลที่รวบรวมและหลักฐานที่รวบรวมได้ตลอดการประชุม และทบทวนการเตรียมความพร้อมสำหรับภัยคุกคาม ทางไซเบอร์ ในอนาคต ซึ่งจำเป็นต้องบันทึกเหตุการณ์อย่างละเอียด รวมถึงวิธีการตรวจจับ มาตรการรับมือ และผลกระทบต่อองค์กร เมื่อองค์กรได้กำหนดเกณฑ์มาตรฐานและตัวชี้วัดสำหรับโปรแกรมการจัดการเหตุการณ์แล้ว ข้อมูลเหล่านี้สามารถนำไปใช้ประเมิน ประสิทธิภาพ ของ CSIRT ในอนาคต และตรวจสอบให้แน่ใจว่าการตอบสนองต่อเหตุการณ์เป็นไปตามที่คาดการณ์ไว้

ขั้นตอนนี้ยังรวมถึงการจัดทำรายงานติดตามผลในทุกส่วนของเหตุการณ์ รายงานนี้สามารถใช้ภายในองค์กรและแชร์กับองค์กรภายนอกได้ ซึ่งองค์กรจะต้องดำเนินการเปลี่ยนแปลงตามบทเรียนที่ได้รับ เช่น การ

ปรับปรุงการควบคุมความปลอดภัย การปรับปรุงการตรวจสอบ และการให้การฝึกอบรมเพิ่มเติม การจัดการและป้องกัน ภัยคุกคาม ทางไซเบอร์มักไม่ได้จำกัดอยู่แค่องค์กรเดียว แต่จำเป็นต้องอาศัยความร่วมมือและการมีส่วนร่วมร่วมกันตลอดวงจรการรับมือเหตุการณ์ NIST รวมถึงองค์กามาตรฐานและองค์กาด้านความมั่นคงปลอดภัยทางไซเบอร์อื่นๆ สนับสนุนการแบ่งปันความรู้ด้านความปลอดภัยระหว่างบริษัทและสถาบันต่างๆ โดยเฉพาะอย่างยิ่งเมื่ออาชญากรไซเบอร์ก็ทำเช่นเดียวกัน

2.6 บทวิเคราะห์เปรียบเทียบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์

จากข้อมูลข้างต้น สามารถสรุปการวิเคราะห์เปรียบเทียบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ของ The OSI Security Architecture และ NIST Cybersecurity Framework ได้ดังนี้

2.6.1 The OSI Security Architecture (ITU-T X.800)

- เป็นสถาปัตยกรรมความมั่นคงปลอดภัยที่อิง OSI Reference Model
- กำหนด 3 องค์ประกอบหลัก:
 1. **Security Services** (บริการความมั่นคงปลอดภัย เช่น Confidentiality, Integrity, Authentication, Non-repudiation, Access Control, Availability)
 2. **Security Mechanisms** (กลไก เช่น encryption, digital signature, hashing, firewall, intrusion detection)
 3. **Security Management** (การบริหารจัดการ เช่น การออก policy, การบริหาร key, การจัดการ incident)
- มี 7 Security Services ตาม X.800
 1. **Authentication** – ยืนยันตัวตนของผู้ใช้/ระบบ
 2. **Access Control** – กำหนดสิทธิ์การเข้าถึง
 3. **Data Confidentiality** – การปกปิดข้อมูล (encryption, VPN, TLS)
 4. **Data Integrity** – การคงสภาพข้อมูล (hash, MAC, blockchain)
 5. **Non-repudiation** – ป้องกันการปฏิเสธความรับผิดชอบ (digital signature, audit log)
 6. **Availability** – การทำให้บริการใช้งานได้เสมอ (redundancy, DDoS mitigation)

7. Privacy – การคุ้มครองข้อมูลส่วนบุคคล (data minimization, anonymization)

2.6.2 NIST Cybersecurity Framework 2.0

- 6 ฟังก์ชัน (Functions): **Govern** (ใหม่), Identify, Protect, Detect, Respond, Recover
- หมวดหมู่/หมวดหมู่ย่อย (Categories/Subcategories): แบ่งย่อยเป็นกิจกรรมและแนวปฏิบัติ
- ตัวอย่างการนำไปใช้ในภาครัฐกิจ: มีแนวทางการปรับใช้ในภาครัฐกิจและหน่วยงานรัฐ
- การปรับปรุงจากเวอร์ชัน 1.1 → 2.0: เพิ่มฟังก์ชัน *Govern*, ขยาย coverage, เน้น supply chain security

2.6.3 การเปรียบเทียบ NIST CSF 2.0 กับ OSI Security Architecture / X.800

มิติ	NIST CSF 2.0	OSI Security Architecture / X.800	ความเชื่อมโยง
โครงสร้าง	Framework 6 Functions	Security Services / Mechanisms	CSF = governance/process, X.800 = service/mechanism
แนวคิดหลัก	Identify risks, manage lifecycle	ให้บริการด้านความปลอดภัยของข้อมูล	CSF เน้น “จัดการ”, X.800 เน้น “ให้บริการ”
การบังคับใช้	นโยบาย, มาตรการ, best practice	โพรโทคอล, เทคนิคทางเทคโนโลยี	CSF ตอบโจทย์ระดับองค์กร, X.800 ตอบโจทย์ระดับเครือข่าย
CIA Triad	ปรากฏใน Protect, Detect, Respond	ปรากฏใน Confidentiality, Integrity, Availability	สอดคล้องกัน
ขอบเขต	ครอบคลุม Supply chain, Governance	มุ่งโครงสร้างการสื่อสาร OSI	ทำงานเสริมกัน

2.7 สรุปบท

เนื้อหาในเอกสารนี้ได้เปรียบเทียบ Security Services ของมาตรฐาน X.800 กับ Functions ของ NIST CSF โดยชี้ให้เห็นความสอดคล้องและการทำงานร่วมกันของแนวคิด CIA Triad ในการดูแลความมั่นคงปลอดภัยของข้อมูล ทั้งในระดับองค์กรและระดับเครือข่าย พร้อมทั้งยกตัวอย่างการนำไปใช้กับกรณีโจมตี Ransomware ในโรงพยาบาล เพื่อวิเคราะห์การเลือกใช้มาตรการที่เหมาะสมในแต่ละด้านของความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้งานของข้อมูล

บทวิเคราะห์เชิงวิชาการ

หัวข้อ: เป้าหมายของนโยบายและกลไกความมั่นคงปลอดภัยทางไซเบอร์

ในชั้นเรียนระดับอุดมศึกษา เน้นให้ผู้เรียนมอง “Cybersecurity เป็นสถาปัตยกรรมและระบบนิเวศ” มากกว่าจะเป็นเครื่องมือทางเทคโนโลยีเพียงชิ้นเดียว โดยผสมเข้ากับนโยบาย (policy goals), มาตรฐาน/กรอบ (standards & frameworks), กลไกเชิงเทคนิค (mechanisms), และเวิร์กโฟลว์ขั้นตอนตอบสนองเหตุการณ์ (incident response) ที่วัดผลได้จริง ในวิชานี้ จึงออกแบบกิจกรรมการเรียนรู้ตั้งแต่ฐานคิดแบบ OSI → แบบจำลองเครือข่ายสมัยใหม่ (Zero Trust/SASE) → มาตรฐานสากล (ISO/IEC 27001/27002, NIST SP 800-53) → กรอบ NIST CSF 2.0 และแนวทางการซ้อมรับมือจริงตามวงจร Detect–Respond–Recover พร้อมเมตริกเพื่อพัฒนาอย่างต่อเนื่อง (Continual improvement). (nvlpubs.nist.gov)

บทวิเคราะห์เนื้อหาหัวข้อ: เป้าหมายของนโยบายและกลไกความมั่นคงปลอดภัยทางไซเบอร์ ในบทนี้สามารถสรุปสาระสำคัญได้ดังนี้

2.1 สถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทางของ OSI

สถาปัตยกรรมความมั่นคงแบบ OSI (ISO 7498-2) ให้ “ภาษา” กลางในการนิยาม **บริการความมั่นคง (security services)** เช่น ความลับ (confidentiality), ความถูกต้องครบถ้วน (integrity), การพิสูจน์ตัวตน (authentication), การควบคุมสิทธิ์ (access control), การปฏิเสธไม่ได้ (non-repudiation) และ**กลไก (mechanisms)** ที่รองรับ เช่น การเข้ารหัส ลายมือชื่อดิจิทัล การจัดการคีย์ เป็นต้น พร้อมชี้ตำแหน่งในเลเยอร์ที่เหมาะสม ช่วยให้ออกแบบ “การป้องกันเชิงลึก” (defense-in-depth) ได้อย่างเป็นระบบตั้งแต่กายภาพ (Physical) จนถึงแอปพลิเคชัน (Application) ([Standards ITEH](#))

2.1.1 การโจมตีด้านความปลอดภัย

การสอนด้วยมิติเลเยอร์ช่วยให้ผู้เรียนเชื่อมโยง **ภัยคุกคาม–ผลกระทบ–มาตรการ** ได้ชัด:

- **L1–L2 (Physical/Data Link):** eavesdropping, rogue AP, MAC spoofing → กลไก: port security, 802.1X, NAC
- **L3–L4 (Network/Transport):** DDoS, route hijack, TCP SYN flood → กลไก: ACL, anti-DDoS, BGP security, segmentation
- **L5–L7 (Session/Presentation/Application):** SQLi, XSS, deserialization, API abuse → กลไก: secure coding, WAF, tokenization, mTLS

2.1.2 บริการด้านความมั่นคงปลอดภัย

จาก ISO 7498-2 บริการหลักคือ Authentication, Access Control, Data Confidentiality, Data Integrity, Non-repudiation และ Availability (แม้ Availability จะถูกอธิบายในมาตรฐานอื่นด้วย) แนวทางสมัยใหม่คือ “ผูกบริการกับผลลัพธ์ที่สังเกตได้” เช่น อัตรา false accept ของการพิสูจน์ตัวตน, ระยะเวลา key rotation, error budget ของการเข้าถึงบริการ รวมถึงการ traceability เพื่อการสอบทานและความรับผิดชอบ. ([Standards ITEH](#))

2.1.3 เป้าหมายของนโยบายด้านความมั่นคงปลอดภัย

จากประสบการณ์ผู้สอนในการนำ NIST Cybersecurity framework ไปประยุกต์จริงทั้งในมหาวิทยาลัยและองค์กรอื่นๆ ค้นพบว่า เป้าหมายที่ดีควร **วัดผลได้และผูกกับภารกิจองค์กร** (mission-driven) เช่น “ลด MTTD/MTTR 30% ภายใน 12 เดือน”, “ครอบคลุม control baseline ตาม NIST SP 800-53 ระดับองค์กร”, “เสถียรภาพ service tier $\geq 99.9\%$ แม้ภายใต้เหตุการณ์ความมั่นคง” พร้อมตั้ง governance ที่ชัดเจนตาม CSF 2.0 ซึ่งยกระดับฟังก์ชัน **Govern** เป็นแกนกลางกำหนดบทบาท ความเสี่ยง และซัพพลายเชน. (nvlpubs.nist.gov)

2.2 แบบจำลองความมั่นคงปลอดภัยเครือข่าย

จากการกำหนดปริมณฑลของเครือข่าย (perimeter) แบบเดิมที่กำหนดโฮสต์ที่ไว้วางใจได้ (Secured hosts) และโฮสต์ที่ไว้วางใจไม่ได้ (Unsecured hosts) สู่ปริมณฑลแบบ **Zero Trust Architecture (ZTA)** ที่ “ไม่ไว้วางใจโดยปริยาย, ตรวจสอบเสมอ, ให้น้อยที่สุดเท่าที่จำเป็น” (continuous verification, least privilege, micro-segmentation, explicit policy enforcement) ซึ่ง NIST SP 800-207 วางหลักการและขั้นตอนการเปลี่ยนผ่านไว้ชัดเจน ตั้งแต่การระบุตัวตนของทรัพยากร การสร้าง policy engine/decision/enforcement ไปจนถึงการวัดผลย้อนกลับ (telemetry/analytics). ในระบบขนาดใหญ่ ผู้สอนได้แนะนำให้ผู้เรียนออกแบบ “ZTA pilot” ระดับบริการหนึ่งตัวก่อน แล้วค่อยขยาย (land-and-expand). (nvlpubs.nist.gov)

ตัวอย่างแบบจำลองเสริมสำหรับการสอนเชิงปฏิบัติ:

- **SASE/SSE-style edge:** รวม SWG, CASB, ZTNA, SD-WAN เพื่อแรงงานแบบ hybrid
- **Software-Defined Segmentation:** บังคับใช้นโยบายตาม identity/label แทนที่ IP-centric
- **Threat-informed defense (MITRE ATT&CK):** ออกแบบ detection & response โดยอิงเทคนิค/เทคนิคจริง (เช่น Credential Dumping $\rightarrow$ hardening/telemetry $\rightarrow$ analytic rule). ([MITRE ATT&CK](#))

2.2.1 มาตรฐานด้านความมั่นคงปลอดภัย

- ISO/IEC 27001:2022 (ISMS—ข้อกำหนด) และ ISO/IEC 27002:2022 (แนวทางควบคุม)—เป็นแกนวางระบบบริหารความมั่นคงและคอนโทรลเชิงปฏิบัติ (Annex A) ที่อัปเดตให้สอดคล้องกับบริบทคลาวด์/ความเป็นส่วนตัวยุคใหม่. ([ISO](#))
- NIST SP 800-53 Rev.5—แค็ตตาล็อก control ที่สอดคล้องเชิงความเป็นส่วนตัวและความยืดหยุ่นสามารถแมปเข้ากับ CSF 2.0 เพื่อออกแบบ baseline ระดับองค์กรรวม. ([nvlpubs.nist.gov](#))

ให้ผู้เรียน “ทำแผนที่ควบคุม” (control mapping lab) ระหว่าง ISO 27001/27002 Annex A ↔ NIST SP 800-53 ↔ CSF 2.0 Functions เพื่อเห็นภาพ *policy* → *control* → *outcome metric* ชัดเจน

2.2.2 กรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST

NIST CSF 2.0 (Feb 2024) ขยายจาก 5 ฟังก์ชันเป็น 6 ฟังก์ชัน: Govern, Identify, Protect, Detect, Respond, Recover และจัดทำ resource guide ชุดใหม่เพื่อเชื่อมโยงไปยังมาตรฐาน/แนวปฏิบัติต่าง ๆ รวมถึงซัพพลายเชนและเมตริกการปรับปรุงอย่างต่อเนื่อง—เหมาะสมอย่างยิ่งสำหรับใช้เป็น *skeleton* ในรายวิชาที่ผสมผสานเทคนิคกับการจัดการความเสี่ยง. ([nvlpubs.nist.gov](#))

2.2.3 กลไกและการตอบสนองต่ออุบัติการณ์ตามแนวทาง NIST CSF

การถอด CSF 2.0 เน้นเปรียบเทียบให้เห็นจุดแตกต่างระหว่าง CSF 1.1 กับ CSF 2.0 ในจุดสำคัญได้แก่:

1. **Detect** – ใช้ ATT&CK-informed analytics/telemetry, ตั้ง MTTD เป้าหมาย
2. **Respond** – ดำเนินการตาม ภัยเหตุการณ์ฉบับล่าสุด NIST SP 800-61 Rev.3 (2025): เตรียมความพร้อม → ตรวจจับ/วิเคราะห์ → ค้นหาเหตุการณ์/กำจัด/กู้คืนเบื้องต้น → กิจกรรมหลังเหตุการณ์ (post-incident) พร้อมบทบาท/การสื่อสารที่ชัดเจน
3. **Recover** – สร้างและทดสอบ playbook ตาม NIST SP 800-184 เพื่อฟื้นฟูบริการ เช็กจุดเปราะ และปรับปรุง policy/control ให้แข็งแกร่งในรอบถัดไป

2.2.4 บทวิเคราะห์เปรียบเทียบสถาปัตยกรรมความมั่นคงปลอดภัยทางไซเบอร์

- OSI-centric: มีระเบียบวิธีและคำศัพท์ชัด เหมาะเป็น “กระดูกสันหลัง” ของการออกแบบบริการ/กลไก แต่ยังเป็นภาพเชิงเลเยอร์มากกว่าการดำเนินการแบบไดนามิก. ([Standards ITEH](#))

- ISO 27001/27002: แข็งแรงด้าน “ระบบบริหาร” (governance, risk, compliance) ทำให้เป้าหมายเชิงนโยบายแปลงเป็นจุดควบคุมและหลักฐานได้ดี เหมาะเป็นฐานองค์กร. (ISO)
- NIST SP 800-53: ลีกริงจุดควบคุม ใช้ทำ baseline/โปรไฟล์สำหรับสภาพแวดล้อมหลากหลาย และเชื่อมไป CSF ได้ดี. (nvlpubs.nist.gov)
- NIST CSF 2.0: โฟกัสผลลัพธ์ระดับสูง (outcomes) และ “Govern” มากขึ้น ทำให้สื่อสารระหว่างผู้บริหาร-วิศวกร-ผู้ตรวจประเมินได้ร่วมกัน. (nvlpubs.nist.gov)
- Zero Trust (SP 800-207): เปลี่ยนกระบวนทัศน์จากปริมาตรสู่ identity-centric โดยเน้นการตรวจสอบต่อเนื่อง เหมาะกับสถานะมัลติคลาวด์/ไฮบริดและโครงสร้างพื้นฐานสำคัญที่ต้องการจำกัด blast radius. (nvlpubs.nist.gov)

ข้อสรุปสำหรับการเรียนการสอน

ใช้ OSI เป็นภาษากลาง, ISO 27001/27002 เป็นระบบบริหาร, NIST SP 800-53 เป็นขั้นคอนโทรล, CSF 2.0 เป็นโครงเรื่องเชิงผลลัพธ์, และ Zero Trust เป็นกลยุทธ์เปลี่ยนผ่านสู่ดิจิทัล (Digital transformation)

แนวโน้มและหลักฐานเชิงข้อมูล เพื่อปรับเป้าหมายให้ “ทันสมัยการณ”

- ภัยคุกคามเปลี่ยนผ่านสู่เทคนิคเชิงอัตโนมัติ/AI และซัพพลายเชน: ENISA TL ชี้แนวโน้มเชิงภูมิรัฐศาสตร์และอุตสาหกรรม (เช่น การเงิน/อวกาศ) ที่ซับซ้อนขึ้น, DBIR 2025 สรุปภาพรวมเหตุการณ์และ breach สูงสุดเป็นประวัติการณ์, และ IBM Cost of a Data Breach 2025 ชี้ทั้งผลบวกจากการใช้ AI ในการตรวจจับ-ตอบสนอง และความเสี่ยงจาก shadow AI ที่ต้องกำกับดูแล. (securitydelta.nl)

สรุปสำหรับผู้กำหนดนโยบายและผู้สอน

- ใช้ OSI/ISO/NIST เป็น “โครงสร้างภาษาและมาตรฐานร่วม”
- ตั้ง เป้าหมายนโยบายที่วัดได้ และผูกกับผลลัพธ์ตาม CSF 2.0
- เดินหน้า Zero Trust แบบค่อยเป็นค่อยไปและวัดผลเสมอ
- ขับเคลื่อนการเรียนรู้ด้วย ภัยคุกคามจริง-ข้อมูลจริง-การซ้อมจริง (threat-informed, exercise-driven)
- อัปเดตหลักฐานเชิงข้อมูลจาก ENISA, DBIR, IBM เพื่อปรับกลยุทธ์ตามแนวโน้มล่าสุดอย่างมีหลักฐานรองรับ. (nvlpubs.nist.gov)

แบบทดสอบท้ายบท

ข้อสอบอัตนัย พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง Passive Attack และ Active Attack พร้อมยกตัวอย่าง

แนวคำตอบ: Passive = sniffing, traffic analysis; Active = DoS, spoofing, replay

ข้อ 2. อธิบาย Security Services ตาม X.800 อย่างน้อย 4 รายการ พร้อมกลไก

แนวคำตอบ: Confidentiality (Encryption), Integrity (Hash), Authentication (Digital Signature), Access Control (RBAC)

ข้อ 3. ยกตัวอย่างการเชื่อมโยง Security Services เข้ากับฟังก์ชัน NIST CSF

แนวคำตอบ: Confidentiality → Protect, Integrity → Detect, Availability → Recover

ข้อ 4. วิเคราะห์กรณี DoS Attack ต่อ Data Center ในมุมมอง CIA และเสนอวิธีการกู้คืน

แนวคำตอบ: C-ไม่กระทบ, I-ไม่เปลี่ยน, A-สูญเสียการเข้าถึง; วิธีแก้ = redundancy, failover

ข้อ 5. อธิบายองค์ประกอบหลักของ NIST CSF 2.0 และประโยชน์ที่องค์กรได้รับ

แนวคำตอบ: 6 Functions (Govern, Identify, Protect, Detect, Respond, Recover), ช่วยจัดการความเสี่ยง

ข้อสอบปรนัย 4 ตัวเลือก พร้อมเฉลย

ข้อ 1. การดักฟังข้อมูลโดยไม่เปลี่ยนแปลง จัดเป็นการโจมตีแบบใด

ก. Active Attack

ข. Passive Attack

ค. DoS

ง. Masquerade

เฉลย: ข

ข้อ 2. การแก้ไขข้อความระหว่างการส่ง ถือเป็นการโจมตีใด

ก. Replay

ข. Modification

ค. Traffic Analysis

ง. Passive

เฉลย: ข

ข้อ 3. ข้อใดคือ Security Service ตาม X.800

ก. Containerization

ข. Access Control

ค. Blockchain

ง. Data Mining

เฉลย: ข

ข้อ 4. Confidentiality ทำได้โดย

ก. Digital Signature

ข. Hash

ค. Encryption

ง. IDS/IPS

เฉลย: ค

ข้อ 5. ฟังก์ชัน Detect ของ NIST CSF มุ่งเน้นที่

ก. นโยบายองค์กร

ข. วิเคราะห์เหตุการณ์ผิดปกติ

ค. ภัยคุกคาม

ง. เข้ารหัสข้อมูล

เฉลย: ข

ข้อ 6. Non-repudiation มีวัตถุประสงค์เพื่อ

ก. ป้องกันการเข้าถึงข้อมูล

ข. ป้องกันการปฏิเสธการกระทำ

ค. ป้องกันไวรัส

ง. ป้องกันระบบล่ม

เฉลย: ข

ข้อ 7. Availability Service เน้นแก้ปัญหา

ก. Nonrepudiation

ข. DoS

ค. ปลอมแปลงข้อมูล

ง. ดักฟังข้อมูล

เฉลย: ข

ข้อ 8. การใช้ MFA สอดคล้องกับฟังก์ชันใด

ก. Identify

ข. Protect

ค. Detect

ง. Recover

เฉลย: ข

ข้อ 9. Trusted Third Party มีหน้าที่

ก. แจกจ่าย Key

ข. ตรวจสอบ Integrity

ค. เก็บ Log

ง. กู้คืนระบบ

เฉลย: ก

ข้อ 10. Incident Response Plan สอดคล้องกับฟังก์ชัน

ก. Identify

ข. Protect

ค. Respond

ง. Detect

เฉลย: ค

บรรณานุกรมท้ายบท

ศิริเชษฐ์ โพธิ์ธีรัญ, ผศ.ดร. (ม.ป.ป.) เอกสารคำสอน: สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล, รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.

Anderson, R. (2021). Security Engineering, Chapter 1-2.

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). NIST.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.

William Stallings, (2011). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS, fourth edition.

Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

Stallings, W. & Brown, L. (2024). Computer Security: Principles and Practice, Chapter 1

ISO/IEC. (2013). *ISO/IEC 27001:2013 – Information Security Management Systems Requirements*. International Organization for Standardization.

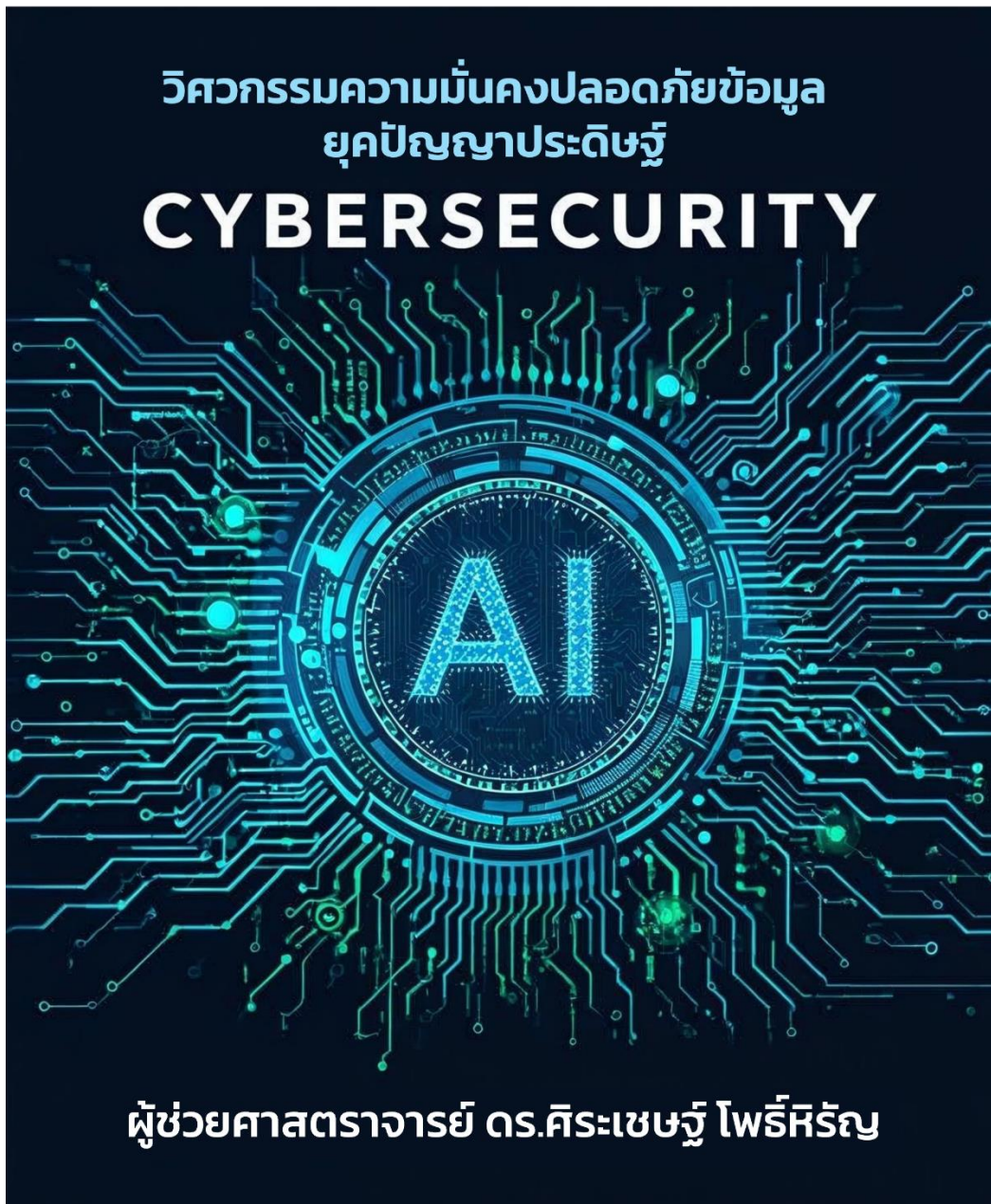
Center for Internet Security. (2021). *CIS Critical Security Controls v8*. CIS.

บทที่ 3

ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์: ช่องโหว่ ภัย

คุกคาม พื้นฐานของมัลแวร์ และความเสี่ยง

Cybersecurity Threat: *Vulnerability, Threat, Malware and Risk*



บทที่ 3 ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์:

ช่องโหว่ ภัยคุกคาม พื้นฐานของมัลแวร์ และความเสี่ยง

(Cybersecurity Threats: Vulnerability, Threat, Malware and Risk)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เพื่อให้นักศึกษา

- 1) มีความรู้ความเข้าใจเกี่ยวกับการโจมตีทางไซเบอร์และการตรวจจับการบุกรุก
- 2) เข้าใจหลักการและวิธีการทำงานของ IDS และ IPS
- 3) ออกแบบการใช้ IDS/IPS ในการป้องกันและตอบสนองต่อการโจมตีได้
- 4) เรียนรู้ผ่านการทำกรณีศึกษาและการปฏิบัติในห้องปฏิบัติการ

2. วัตถุประสงค์เชิงพฤติกรรม

เมื่อสิ้นสุดการเรียนรู้ในสัปดาห์นี้ นักศึกษาจะสามารถ:

- 1) อธิบายรูปแบบและเทคนิคการโจมตีทางไซเบอร์ที่พบบ่อยได้
- 2) อธิบายหลักการการทำงานของระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) ได้
- 3) แยกแยะความแตกต่างระหว่าง IDS และ IPS ได้อย่างชัดเจน
- 4) วิเคราะห์กรณีการโจมตีและเสนอแนวทางการใช้ IDS/IPS ในการตอบโต้ได้
- 5) นำความรู้ไปปรับใช้กับสถานการณ์จริงในงานด้านความมั่นคงปลอดภัยสารสนเทศได้

3. หัวข้อเนื้อหา:

ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์

3.1 ช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์

3.1.1 ความหมายของช่องโหว่

3.1.2 ศัพท์ที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์

3.2 ภัยคุกคามที่เกิดกับคอมพิวเตอร์

3.2.1 การคุกคาม (Threat)

3.2.2 การโจมตี (Attack)

3.3 พื้นฐานมัลแวร์

3.3.1 ประเภทของซอฟต์แวร์อันตราย

3.3.2 ไวรัส

3.3.3 แรนซัมแวร์

3.4 การบุกรุก

3.4.1 ผู้บุกรุก

3.4.2 รูปแบบพฤติกรรมผู้บุกรุก

3.4.3 เทคนิคการบุกรุก

3.5 OWASP top 10

3.5.1 OWASP top 10 web application

3.5.2 OWASP top 10 mobile

3.5 การจัดการความเสี่ยงจากภัยคุกคาม

3.5.1 การจัดการช่องโหว่ของ NIST คืออะไร?

3.5.2 เหตุใดการจัดการช่องโหว่จึงมีความสำคัญ

3.5.3 กรอบการจัดการความเสี่ยงของ NIST

3.6 การพิสูจน์ตัวตนจริง

3.6.1 แบบจำลองความปลอดภัย

3.6.2 ประเภทการพิสูจน์ตัวตนจริง

3.6.3 แนวทางการนำระบบการพิสูจน์ตัวตนจริงไปใช้งาน

3.7 บทวิเคราะห์เชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา):

บริษัท “RMUTT FinSecure Co., Ltd.” ผู้ให้บริการ Mobile Banking ถูกตรวจพบเหตุผิดปกติ:

- ผู้ใช้บางรายพบธุรกรรมที่ไม่ได้ทำ
- ระบบตรวจพบการโจมตีแบบ *SQL Injection* บน Web Application และมี *Phishing Email* ปลอมตัวเป็นฝ่ายบริการลูกค้า
- มีความเสี่ยงที่จะถูกติดตั้ง **Ransomware** ผ่านลิงก์อีเมล

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4–5 คน):

- ระบุช่องโหว่และภัยคุกคามที่พบ พร้อมจำแนกเป็น Threat, Vulnerability, Attack
- วิเคราะห์ผลกระทบต่อ CIA Triad (Confidentiality, Integrity, Availability)
- เสนอการใช้นโยบายการรับมือ (เช่น IDS, IPS, Patch Management, Awareness Training)
- เชื่อมโยงสถานการณ์นี้เข้ากับ NIST Risk Management Framework (RMF)
- สรุปเป็นรายงานกลุ่มและนำเสนอในชั้นเรียน

ประเด็นการเรียนรู้สำคัญที่แทรกในกิจกรรม:

- ความเข้าใจคำว่า Threat, Vulnerability, Attack
- ประเภทของ Malware (ไวรัส, Worm, Trojan, Ransomware)
- การเชื่อมโยงกับ OWASP Top 10
- แนวทางการจัดการความเสี่ยง (NIST RMF)

5. เกณฑ์คะแนน Rubric 4 ระดับ (รวม 100 คะแนน):

เกณฑ์	ระดับ 4 (ยอดเยี่ยม)	ระดับ 3 (ดี)	ระดับ 2 (พอใช้)	ระดับ 1 (ควรปรับปรุง)
การวิเคราะห์เชิง วิชาการ (30)	ครบถ้วน สอดคล้องกรอบ NIST/OWASP	ครบ 70– 80%	ครบเพียง บางส่วน	ไม่ครบ/ คลาดเคลื่อน
การเชื่อมโยง CIA Triad (25)	วิเคราะห์ชัดเจนทั้ง C-I-A	ครบแต่ไม่ลึก	ครบเพียงบาง มิติ	ไม่ถูกต้อง
การเสนอแนวทาง ป้องกัน (30)	เสนอมาตรการครอบคลุมและ เชื่อมโยง CSF/RMF ได้	ครอบคลุม 70%	มีบางส่วนไม่ สอดคล้อง	ขาดมาตรการ

เกณฑ์	ระดับ 4 (ยอดเยี่ยม)	ระดับ 3 (ดี)	ระดับ 2 (พอใช้)	ระดับ 1 (ควรปรับปรุง)
การนำเสนอ (15)	ชัดเจน มีสื่อ/แผนภาพประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

3.1 ช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์

3.1.1 ความหมายของช่องโหว่

ความหมายที่กำหนดตาม NIST สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของอเมริกา (National Institute of Standards and Technology) ช่องโหว่ (**Vulnerability**) หมายถึง จุดอ่อนในตรรกะเชิงคำนวณ (เช่น โค้ด) ที่พบในส่วนประกอบซอฟต์แวร์และฮาร์ดแวร์ ซึ่งเมื่อถูกใช้ประโยชน์จะส่งผลกระทบต่อความลับ ความสมบูรณ์ หรือความพร้อมใช้งาน การลดช่องโหว่ในบริบทนี้โดยทั่วไปเกี่ยวข้องกับการเปลี่ยนแปลงโค้ด แต่อาจรวมถึงการเปลี่ยนแปลงข้อกำหนด หรือแม้แต่การเลิกใช้ข้อกำหนด เช่น การลบโพรโทคอลหรือฟังก์ชันการทำงานที่ได้รับผลกระทบทั้งหมด เป็นต้น ช่องโหว่ จึงเป็นคุณลักษณะอย่างหนึ่งของระบบที่อนุญาตให้ผู้อื่นซึ่งอาจเป็นผู้ประสงค์ร้ายเข้าสู่ระบบได้ ช่องโหว่นี้มีความเสี่ยงสูงต่อการแทรกซึมเข้ามาสู่ระบบได้โดยผู้บุกรุก รู้ร่วดังกล่าวนี้ อาจเกิดขึ้นเพราะความบกพร่องของตัวระบบเอง หรืออาจเกิดจากเจตนาของผู้ออกแบบ แต่เมื่อมีช่องโหว่เกิดขึ้นในระบบใดๆ อาจเพิ่มความเสี่ยงต่อการเกิดขึ้นของพฤติกรรมที่ไม่อาจคาดการณ์ได้ซึ่งอาจเป็นอันตรายต่อระบบ

การแสวงหาประโยชน์ (Exploit)

กระบวนการใช้ประโยชน์จากช่องโหว่ของระบบเพื่อละเมิดนโยบายความปลอดภัย เครื่องมือหรือวิธีการใดๆ ที่ถูกสร้างขึ้นมาเพื่อใช้ในการละเมิดนโยบายด้านความปลอดภัยมักถูกเรียกว่า บทคำสั่งแสวงหาประโยชน์ (exploit script)

ศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์มีศัพท์หลายศัพท์ที่ใช้กันในความหมายที่ยังไม่สอดคล้องกันนัก เพื่อความเข้าใจที่ตรงกัน ในส่วนนี้จะอธิบายความหมายซึ่งเป็นสาระสำคัญของศัพท์ที่เกี่ยวข้องที่ปรากฏอยู่ในเอกสารเล่มนี้ ดังต่อไปนี้

ความสามารถในการอยู่รอด (Survivability)

เป็นแนวคิดในการออกแบบระบบที่มีขีดความสามารถในการดำเนินการกิจทั้งหมดต่อไปได้ แม้จะเกิดการโจมตี, ความขัดข้อง หรือเกิดอุบัติเหตุก็ตาม [72] ระบบที่มีความสามารถในการอยู่รอดได้นี้จะมีคุณลักษณะสำคัญ 3 ประการ [79] ได้แก่ ความทนทาน (resistance) หมายถึงความสามารถในการหลีกเลี่ยงการโจมตีได้, การรู้จำ (recognition) หมายถึง ความสามารถในการรู้จำรูปแบบการโจมตีและสามารถจำกัดขอบเขตความเสียหายได้, และการกู้คืนได้ (recovery) หมายถึง ความสามารถในการฟื้นฟูสภาพบริการที่จำเป็นระหว่างการถูกโจมตี และสามารถกู้คืนบริการทุกอย่างภายหลังการโจมตีได้

การบุกรุก (Intrusion)

การกระทำใดๆ ที่พยายามละเมิดความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของทรัพยากรคอมพิวเตอร์

การคุกคาม (Threat)

เป็นเจตนาของผู้ซึ่งไม่ได้รับอนุญาตที่พยายามเข้าถึงข้อมูล, แก้ไขข้อมูล หรือกระทำให้ระบบขาดความเชื่อถือได้หรือใช้งานไม่ได้

การโจมตี (Attack)

เป็นการกระทำที่มีความตั้งใจให้เกิดเป็นภัยหรืออันตรายต่อระบบคอมพิวเตอร์โดยตรง การโจมตีอาจกระทำได้ 2 ลักษณะ คือ การโจมตีแบบซ่อนเร้น (Passive attack) เป็นการโจมตีที่ไม่เปิดเผย ตรวจสอบได้ยาก ได้แก่ การเผยแพร่เนื้อหาไปยังบุคคลที่สาม และการวิเคราะห์ทราฟฟิก (Traffic analysis) และการโจมตีแบบเผชิญหน้า (Active attack) เป็นการเข้าไปเปลี่ยนแปลงข้อมูลหรือกระทำให้เกิดความเสียหายโดยตรงต่อระบบคอมพิวเตอร์ ได้แก่ การปลอมตัว (Masquerade) การทำซ้ำ (Replay) การเปลี่ยนข้อมูล และการทำให้ใช้การไม่ได้

ในเอกสารเล่มนี้ จะใช้คำว่า การบุกรุก, การคุกคาม, การโจมตี (Attack), การแฮ็ก (Hacking) การเจาะระบบ และการแคร็ก (Cracking) ในความหมายเดียวกัน

ผู้บุกรุก (Intruder)

บุคคลที่ทำการบุกรุก บางทีใช้คำว่า ผู้โจมตี (Attacker) ทั้งสองคำนี้จะถูกใช้ภายหลังจากการโจมตีเกิดขึ้น นอกจากนั้น ยังมีความหมายสมนัยกับคำว่า แฮ็กเกอร์ (Hacker) นักเจาะระบบ และแคร็กเกอร์ (Cracker) ซึ่งหมายถึงผู้บุกรุกที่เกิดขึ้นก่อนการโจมตีอีกด้วย

อุบัติการณ์ (Incident)

หน่วยรวมของข้อมูลที่ใช้แทนการโจมตีที่เกี่ยวข้องทั้งหมด เช่น โดยผู้โจมตี, ชนิดของการโจมตี, วัตถุประสงค์, ไซต์ หรือช่วงเวลา อุบัติการณ์จึงเป็นสถานการณ์ที่มีความเสี่ยงเกิดขึ้น [78]

ระบบการตรวจหาการบุกรุก (Intrusion detection systems หรือ IDS)

ปัญหาของการระบุอย่างเจาะจงว่าใครคือผู้ใช้ระบบคอมพิวเตอร์โดยปราศจากสิทธิ์ รวมทั้งผู้มีสิทธิ์เข้าถึงอย่างถูกต้องแต่ใช้สิทธิ์นั้นโดยประสงค์ร้าย ระบบการตรวจหาการบุกรุกจึงเป็นซอฟต์แวร์ซึ่งทำหน้าที่ตรวจหา, ระบุ และโต้ตอบต่อการกระทำใดๆ ที่ไม่ได้รับอนุญาต หรือกิจกรรมที่ผิดปกติบนระบบที่เป็นเป้าหมาย

วิธีการวิเคราะห์ (Analysis approach)

วิธีการวิเคราะห์เป็นวิธีที่ระบบการตรวจหาการบุกรุกใช้ในการวิเคราะห์เพื่อตัดสินใจว่ากิจกรรมที่เกิดขึ้นนั้นเป็นการบุกรุกหรือไม่ รายละเอียดเกี่ยวกับวิธีการวิเคราะห์รวมทั้งเปรียบเทียบข้อดีข้อด้อยของวิธีการทั้งสองแบบจะอธิบายไว้ในบทที่ 4 แต่แนวคิดหลักสำหรับการวิเคราะห์ดังกล่าวประกอบด้วย

การตรวจหาลายเซ็นของการโจมตี (Signature-based detection) บางครั้งเรียกว่า การตรวจหาการใช้สิทธิ์โดยมิชอบ (Misuse) โดยการเทียบเคียงแบบอย่างที่เราพบเข้ากับรูปแบบการโจมตีที่รู้จัก

วิธีการนี้รวมทั้งการวิเคราะห์โปรโตคอลแบบแพสซีฟที่ใช้สเนิฟเฟอร์ (Sniffer) ในโหมดผสม (promiscuous mode) นอกจากนั้น ยังรวมถึงการวิเคราะห์ลายเซ็นที่ใช้ข้อความชุดของแพ็กเกจ (หรือชิ้นของข้อมูล) ที่บรรจุไว้ในแพ็กเกจเหล่านั้น) ที่จะใช้ตัดสินว่าเป็นการโจมตีหรือไม่

ลายเซ็นการโจมตีดังกล่าวอาจปรากฏอยู่ในรายการบันทึกการตรวจสอบ, แฟ้มลงบันทึกเข้าออก หรือการเปลี่ยนแปลงที่น่าสงสัยในระบบ

การตรวจหาค่าผิดปกติ (Anomaly-base detection) ใช้ในการจำแนกกิจกรรมที่ไม่พึงประสงค์จากพฤติกรรมที่คาดหวังไว้ซึ่งได้กำหนดเอาไว้แล้วล่วงหน้าโดยวิธีสร้างข้อมูลแสดงลักษณะเฉพาะ (Profile) ทั้งแบบอัตโนมัติและไม่อัตโนมัติ ข้อมูลแสดงลักษณะเฉพาะแบบอัตโนมัตินั้นจะถูกสร้างโดยซอฟต์แวร์ที่รวบรวมและประมวลผลคุณลักษณะทั้งหมดของพฤติกรรมที่ควรจะเป็นในแต่ละช่วงเวลาและรูปแบบทั่วไปทางสถิติของพฤติกรรมกลุ่มตัวอย่าง อย่างไรก็ตาม อาจมีพฤติกรรมบางอย่างเกิดขึ้นภายหลังที่ดูอาจเหมือนกับพฤติกรรมน่าสงสัย (แต่ไม่ใช่) ก็สามารถเพิ่มเติมลงไปในรายการพฤติกรรมที่พึงประสงค์ได้ภายหลัง ระบบนี้จะใช้การวิเคราะห์ว่าพฤติกรรมใดที่ผิดไปจากพฤติกรรมที่คาดหวัง อย่างไรก็ตาม ในระบบงานขนาดใหญ่ ย่อมไม่มีทางเป็นไปได้ที่จะสามารถกำหนดพฤติกรรมที่คาดหวังไว้ล่วงหน้าได้ทั้งหมด

ระบบป้องกันการบุกรุก (Intrusion Prevention System หรือ IPS)

IPS คือระบบที่ทำงานแบบ **real-time** เพื่อตรวจจับ (detect) และ **ป้องกัน (prevent/block)** การโจมตีทางไซเบอร์โดยอัตโนมัติ แตกต่างจาก IDS ที่ทำหน้าที่แจ้งเตือนเพียงอย่างเดียว

การทำนายผิดเชิงลบ (False negative)

เป็นเหตุการณ์ที่ระบบการตรวจหาการบุกรุกไม่พบว่ามีการโจมตีใดๆ ที่เกิดการโจมตี

การทำนายผิดเชิงบวก (False positive)

เป็นเหตุการณ์ที่ระบบการตรวจหาการบุกรุกพบว่ามีการโจมตีเกิดขึ้น ทั้งๆ ที่ไม่ได้มีการโจมตี (แต่อาจมีพฤติกรรมที่คล้ายการโจมตี)

การโจมตีแบบการทำให้ใช้การไม่ได้ (DoS/DDoS; denial-of-service/Distributed DoS)

โดยทั่วไป การโจมตีแบบการทำให้ใช้การไม่ได้มีพื้นฐานการโจมตีอยู่ 3 ประเภท ประกอบด้วย [8]

การโจมตีแบนด์วิดท์ (Bandwidth) เป็นการโจมตีเพื่อให้แบนด์วิดท์ของเหยื่อท่วมตันไปด้วย पै็กเก็ตจิปเสียดร้ยของผู้โจมตีจนเหยื่อไม่เหลือแบนด์วิดท์พอที่จะรองรับการใช้งานปกติได้ เช่น การโจมตีปิง (PING attack) [9], ยูดีพีฟลัด (UDP flood) [10],

การโจมตีโพรโทคอล (Protocol attack) เป็นการโจมตีข้อบกพร่องของโพรโทคอล เช่น ซิงค์ฟลัด (SYN flood) [11], สเมอร์ฟ (Smurf) [12] และ

การโจมตีจุดอ่อนของซอฟต์แวร์ (Software attack) เช่น ปิงออฟเดธ (Ping of death) [13], เทียร์ดรอพ (Teardrop) [14] ในรายงานที่สำรวจโดยเชิร์ท [5] พบว่า ในปี พ.ศ. 2547 มีจุดอ่อนหรือช่องโหว่ของซอฟต์แวร์ที่ถูกค้นพบประมาณ 3,780 ช่องโหว่ เพิ่มขึ้นเป็น 1.7 เท่าของปี พ.ศ. 2543 ซึ่งมีเพียง 1,090 ช่องโหว่ จากสถิติดังกล่าวแสดงให้เห็นถึงอัตราการเติบโตของการโจมตีที่มีแนวโน้มเพิ่มมากขึ้นทุกปี สาเหตุหนึ่งมาจากปัจจุบันเครื่องมือที่มีประสิทธิภาพหลายชนิดที่จัดเตรียมไว้สำหรับการโจมตีแพร่หลายอยู่บนอินเทอร์เน็ตที่ทุกคนสามารถเข้าถึงโดยไม่เสียค่าใช้จ่ายและนำไปใช้ได้อย่างง่ายดาย เช่น [15], [16], [17], [18], [19] และ [20] เป็นต้น

3.2 ภัยคุกคามที่เกิดกับคอมพิวเตอร์

ภัยคุกคามที่มาทางคอมพิวเตอร์นั้นมีหลายประเภท ในที่นี้จะมุ่งไปที่ภัยคุกคาม 2 ประเภท ได้แก่ การคุกคาม และการโจมตี แม้ว่าภัยคุกคามจากทั้งสองประเภทจะมีนัยที่ใกล้เคียงกันและสามารถใช้แทนกันได้ แต่เพื่อความชัดเจน เราสามารถจำแนกภัยทั้งสองประเภทตามความหมายดังต่อไปนี้

3.2.1 การคุกคาม (Threat)

การคุกคาม หมายถึง การกระทำซึ่งมีความเป็นไปได้ที่จะก่อให้เกิดความเสียหายหรือเป็นอันตรายต่อความปลอดภัยของระบบคอมพิวเตอร์ [80] โดยทั่วไปการคุกคามแบ่งออกเป็น 4 ประเภท ได้แก่ การดักฟัง (Interception) การสะดุดหยุด (Interruption) การเปลี่ยนแปลง (Modification) และการปลอมขึ้น (Fabrication) [2]

การดักฟัง

คือ การที่มีบุคคลที่ไม่เกี่ยวข้องสามารถเข้าถึงทรัพยากรที่ตัวเองไม่มีสิทธิ์ หรือมีบุคคลที่สามดักฟังการส่งข้อมูลระหว่างผู้รับและผู้ส่ง ผู้ดักฟังอาจเป็นบุคคล โปรแกรม หรืออุปกรณ์คอมพิวเตอร์ก็ได้ เทคนิคการดักฟังรูปแบบการส่งข้อมูลที่นิยมใช้ทราฟฟิก sniffing (Traffic sniffing) ผู้บุกรุกอาจใช้เทคนิคดังกล่าวนี้เพื่อนำไปวิเคราะห์หาจุดอ่อนแล้วนำกลับมาโจมตีต่อสถาปัตยกรรมระบบการตรวจหาการบุกรุกได้

การสะดุดหยุด

คือ การที่ทรัพยากรคอมพิวเตอร์เกิดสูญหายหรือใช้การไม่ได้เป็นเหตุให้ผู้ที่ไม่สามารถเข้าถึงได้ โดยอาจเกิดจากความเสียหายทางกายภาพ เช่น ฮาร์ดแวร์เสีย หรือเกิดจากความผิดพลาดอย่างอื่น เช่น ระบบปฏิบัติการเสียหาย แฟ้มข้อมูลหรือโปรแกรมถูกลบทิ้ง เป็นต้น

การเปลี่ยนแปลง

คือ การที่ผู้ที่ไม่มีสิทธิ์เข้ามาแก้ไขเปลี่ยนแปลงเนื้อหาหรือทรัพยากรของระบบคอมพิวเตอร์ การเปลี่ยนแปลงนี้อาจเกิดจากคน โปรแกรมไวรัส โปรแกรมหนอน เป็นต้น โดยแก้ไขแฟ้มข้อมูลให้เสียหาย หรือแอบส่งเมลไปยังผู้ที่เกี่ยวข้อง

การปลอมขึ้น

คือ การสร้างข้อมูลขึ้นมาใหม่ หรือปลอมตัวเป็นบุคคลอื่นในระบบคอมพิวเตอร์ ซึ่งจะนำไปสู่การบุกรุกต่อระบบคอมพิวเตอร์ในภายหลัง

3.2.2 การโจมตี (Attack)

การโจมตี คือ การกระทำหรือความพยายามที่ตั้งใจให้เกิดอันตรายต่อระบบคอมพิวเตอร์ การโจมตีสามารถแบ่งออกเป็น 2 ประเภทใหญ่ๆ ได้แก่ การโจมตีแบบซ่อนเร้น และการโจมตีแบบเผชิญหน้า

การโจมตีแบบซ่อนเร้น (Passive attack)

การโจมตีแบบซ่อนเร้นมีจุดมุ่งหมายที่จะล่วงรู้หรือขโมยข้อมูลของระบบคอมพิวเตอร์นั้นโดยไม่มี การเปลี่ยนแปลงแก้ไขเนื้อหา การโจมตีประเภทนี้จึงยากต่อการตรวจพบความผิดปกติ เพราะข้อมูลถูกส่งไปถึงผู้รับ โดยที่เนื้อหาที่ไม่ได้ถูกแก้ไข การโจมตีประเภทนี้อาจนำข้อมูลที่ได้เป็นฐานในการวิเคราะห์เพื่อทำการบุกรุกหรือโจมตีในรูปแบบอื่นต่อไป แบ่งออกเป็น 2 ประเภท ได้แก่ การเผยแพร่เนื้อหา (Release of message content) และการวิเคราะห์ทราฟฟิก (Traffic analysis)

1) การเผยแพร่เนื้อหา คือ การเผยแพร่ข้อความไปยังบุคคลที่สามที่ไม่เกี่ยวข้องหรือต่อสาธารณะ อย่างเช่น การเผยแพร่การสนทนาทางโทรศัพท์ระหว่างเจ้านายกับเลขาฯ ในทางลับ การเผยแพร่ข้อความในเมลส่วนตัวของผู้มีชื่อเสียงลงในเว็บกระดานข่าวสาธารณะ เป็นต้น

2) การวิเคราะห์ทราฟฟิก เป็นการวิเคราะห์รูปแบบการสื่อสารโดยผู้โจมตีเพื่อนำไปวิเคราะห์ถึงแบบอย่างเฉพาะของการสื่อสารเพื่อนำไปใช้เป็นข้อมูลในการบุกรุกหรือโจมตีในภายหลัง การวิเคราะห์ดังกล่าวนี้ในปัจจุบันมีเครื่องมือที่เรียกว่า ทราฟฟิก sniffing หรือแพกเก็ต sniffing (Packet sniffing)

การโจมตีแบบเผชิญหน้า (Active attack)

การโจมตีแบบเผชิญหน้า คือ การกระทำที่ส่งผลกระทบโดยตรงต่อระบบคอมพิวเตอร์ เป็นการเข้าไปเปลี่ยนแปลงข้อมูล หรือการปลอมแปลง แบ่งออกเป็น 4 ประเภทใหญ่ๆ ได้แก่ การปลอมตน (Masquerade) การทำซ้ำ (Replay) การเปลี่ยนข้อมูล (Modification of message) และการทำให้ใช้การไม่ได้

1) การปลอมตน การที่ผู้โจมตีปลอมตนเป็นบุคคลอื่นเพื่อบุกรุกเข้าไปใช้ข้อมูลหรือทรัพยากรคอมพิวเตอร์ที่ตนเองไม่ได้รับอนุญาตให้ใช้ หรือส่งข้อมูลไปยังบุคคลอื่นเพื่อให้ผู้รับเข้าใจผิดว่าถูกส่งมาจากอีกคนหนึ่ง

2) การทำซ้ำ เป็นการนำข้อความเก่าหรือรายชื่อผู้ใช้เก่าที่หมดอายุไปแล้วนำกลับมาใช้ใหม่เพื่อจุดประสงค์ร้าย

3) การเปลี่ยนข้อมูล เปลี่ยนแก้ไขเปลี่ยนแปลงเนื้อหาของข้อความ

4) การทำให้ใช้การไม่ได้ เป็นการโจมตีที่ทำให้ทรัพยากรของเครื่องเป้าหมายไม่สามารถใช้การได้ตามปกติ

โดยทั่วไป การโจมตีอาจกระทำแบบใดแบบหนึ่ง หรือผู้บุกรุกอาจเริ่มต้นด้วยการโจมตีแบบซ่อนเร้นก่อน จากนั้น จึงโจมตีแบบเผชิญหน้าในภายหลัง ดังนั้น การโจมตีแบบใดก็ตามย่อมเกิดผลกระทบต่อความมั่นคงของความปลอดภัยของระบบคอมพิวเตอร์อย่างหลีกเลี่ยงไม่ได้ การโจมตีแบบเผชิญหน้าสามารถป้องกันได้ยากกว่าการโจมตีแบบซ่อนเร้น แต่สามารถตรวจพบได้ง่ายกว่า อย่างไรก็ตาม ระบบตรวจหาการบุกรุกสามารถตรวจพบและป้องกันการโจมตีทั้งสองแบบได้

3.3 พื้นฐานของมัลแวร์

ภัยคุกคามที่ซับซ้อนที่สุดต่อระบบคอมพิวเตอร์อาจเกิดจากโปรแกรมที่ใช้ประโยชน์จากช่องโหว่ในระบบคอมพิวเตอร์ ภัยคุกคามเหล่านี้เรียกว่า **ซอฟต์แวร์ที่เป็นอันตราย** (Malicious software) หรือ **มัลแวร์** (Malware) ในบริบทนี้ เราจะพิจารณาถึงภัยคุกคามต่อโปรแกรมแอปพลิเคชัน รวมถึงโปรแกรมมัลแวร์ประเภทต่างๆ เช่น โปรแกรมแก้ไขและคอมไพเลอร์ และโปรแกรมระดับเคอร์เนล บทนี้จะพิจารณาซอฟต์แวร์ที่เป็นอันตรายโดยเน้นเป็นพิเศษที่ไวรัสและเวิร์ม บทนี้เริ่มต้นด้วยการสำรวจมัลแวร์ประเภทต่างๆ พร้อมศึกษาลักษณะของไวรัสและเวิร์มอย่างละเอียด จากนั้น จะกล่าวถึงการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed Denial-of-Service Attack) ตลอดทั้งบท การอภิปรายจะนำเสนอทั้งภัยคุกคามและมาตรการรับมือ

3.3.1 ประเภทของซอฟต์แวร์อันตราย (Types of malicious software)

คำศัพท์เฉพาะด้านนี้ก่อให้เกิดปัญหาเนื่องจากไม่มีความเห็นพ้องต้องกันในทุกคำศัพท์ และเนื่องจากบางหมวดหมู่มีความทับซ้อนกัน ตารางที่ 3.1 เป็นแนวทางที่มีประโยชน์ มัลแวร์ (Malware) หรือซอฟต์แวร์ที่เป็นอันตราย (Malicious software) สามารถแบ่งออกเป็น 2 ประเภท ได้แก่ ซอฟต์แวร์ที่ต้องมีโปรแกรมโฮสต์ และซอฟต์แวร์ที่เป็นอิสระต่อกัน ซอฟต์แวร์ที่เป็นอันตราย ซึ่งเรียกว่าปรสิต (Parasitic) เป็นส่วนหนึ่งของโปรแกรมที่ไม่สามารถดำรงอยู่ได้โดยอิสระจากโปรแกรมแอปพลิเคชัน ยูทิลิตี้ หรือโปรแกรมระบบ

ไวรัส ลอจิกบอมบ์ และประตูลับ เป็นต้น มัลแวร์อิสระคือโปรแกรมที่ทำงานในตัวเอง ซึ่งสามารถกำหนดเวลาและเรียกใช้งานโดยระบบปฏิบัติการได้ ตัวอย่างได้แก่ เวิร์มและโปรแกรมบอท เราสามารถแยกความแตกต่างระหว่างภัยคุกคามซอฟต์แวร์ที่ไม่ทำซ้ำและภัยคุกคามซอฟต์แวร์ที่ทำซ้ำได้ ภัยคุกคามซอฟต์แวร์แบบแรกคือโปรแกรมหรือส่วนของโปรแกรมที่ถูกกระตุ้นโดยทริกเกอร์ ตัวอย่างได้แก่ ลอจิกบอมบ์ แบ็คดอร์ และโปรแกรมบอท ส่วนโปรแกรมบอท ประกอบด้วยส่วนของโปรแกรมหรือโปรแกรมอิสระ ซึ่งเมื่อถูกเรียกใช้งานแล้วอาจสร้างสำเนาของตัวเองอย่างน้อยหนึ่งชุด

ในเอกสารทางวิชาการ คำว่า ภัยคุกคาม และ การโจมตี มักถูกใช้เพื่อสื่อความหมายที่ใกล้เคียงกัน ตารางที่ 3.1 แสดงคำจำกัดความที่นำมาจาก RFC 2828, *Internet Security Glossary*

ตาราง 3.1 ภัยคุกคามและการโจมตี (RFC 2828)

ชื่อ	คำอธิบาย
ภัยคุกคาม (Threat)	ความเสี่ยงที่จะเกิดการละเมิดความปลอดภัย ซึ่งเกิดขึ้นเมื่อมีสถานการณ์ ความสามารถ การกระทำ หรือเหตุการณ์ใดๆ ที่อาจก่อให้เกิดการละเมิดความปลอดภัยและก่อให้เกิดอันตราย กล่าวคือ ภัยคุกคาม คือ อันตรายที่อาจเกิดขึ้นซึ่งอาจใช้ประโยชน์จากช่องโหว่ของระบบ
การโจมตี (Attack)	การโจมตีระบบรักษาความปลอดภัยที่เกิดจากภัยคุกคามอัจฉริยะ นั่นคือ การกระทำอันชาญฉลาดที่เป็นความพยายามโดยเจตนา (โดยเฉพาะอย่างยิ่งในแง่ของวิธีการหรือเทคนิค) เพื่อหลบเลี่ยงบริการรักษาความปลอดภัยและละเมิดนโยบายความปลอดภัยของระบบ การโจมตีระบบรักษาความปลอดภัยที่เกิดจากภัยคุกคามอัจฉริยะ นั่นคือ การกระทำอันชาญฉลาดที่เป็นความพยายามโดยเจตนา (โดยเฉพาะอย่างยิ่งในแง่ของวิธีการหรือเทคนิค) เพื่อหลบเลี่ยงบริการรักษาความปลอดภัยและละเมิดนโยบายความปลอดภัยของระบบ
ไวรัส (Virus)	มัลแวร์ไวรัสที่เมื่อถูกเรียกใช้งานจะพยายามจำลองตัวเองเป็นโค้ดปฏิบัติการอื่น ๆ เมื่อสำเร็จ โค้ดดังกล่าวจะถูกเรียกว่าติดไวรัส เมื่อโค้ดที่ติดไวรัสถูกเรียกใช้งาน ไวรัสก็จะเรียกใช้งานโค้ดนั้นด้วย

ชื่อ	คำอธิบาย
หนอน (Worm)	โปรแกรมคอมพิวเตอร์ที่สามารถทำงานได้อย่างอิสระและสามารถเผยแพร่เวอร์ชันที่ใช้งานได้สมบูรณ์ของตัวเองไปยังโฮสต์อื่นบนเครือข่ายได้
ลจิกบอมบ์ (Logic bomb)	โปรแกรมที่ถูกแทรกเข้าไปในซอฟต์แวร์โดยผู้บุกรุก ลจิกบอมบ์จะซ่อนตัวอยู่จนกว่าจะบรรลุเงื่อนไขที่กำหนดไว้ จากนั้นโปรแกรมจะกระตุ้นการกระทำที่ไม่ได้รับอนุญาต
ม้าโทรจัน (Trojan horse)	โปรแกรมคอมพิวเตอร์ที่ดูเหมือนว่าจะมีฟังก์ชันที่เป็นประโยชน์แต่ก็มีฟังก์ชันที่ซ่อนอยู่และอาจเป็นอันตรายได้ซึ่งหลบเลี่ยงกลไกการรักษาความปลอดภัย บางครั้งโดยการใช้ประโยชน์จากการอนุญาตที่ถูกต้องตามกฎหมายของเอนทิตีระบบที่เรียกใช้โปรแกรมม้าโทรจัน
ประตูลับ (Backdoor or trapdoor)	กลไกใดๆ ที่หลีกเลี่ยงการตรวจสอบความปลอดภัยปกติ อาจทำให้เข้าถึงฟังก์ชันการทำงานโดยไม่ได้รับอนุญาต
รหัสโมบาย (Mobile code)	ซอฟต์แวร์ (เช่น สคริปต์ แมโคร หรือคำสั่งพกพาอื่นๆ) ที่สามารถส่งไปยังแพลตฟอร์มที่หลากหลายโดยไม่เปลี่ยนแปลง และดำเนินการด้วยความหมายที่เหมือนกัน
การแสวงหาประโยชน์ (Exploits)	รหัสการโจมตีที่เฉพาะเจาะจงกับช่องโหว่เดียวหรือชุดของช่องโหว่
Downloaders	โปรแกรมที่ติดตั้งรายการอื่นๆ บนเครื่องที่ถูกโจมตี โดยปกติแล้วโปรแกรมดาวน์โหลดจะถูกส่งมาทางอีเมล
Auto-rooter	เครื่องมือแฮกเกอร์ที่เป็นอันตรายใช้เพื่อเจาะเข้าไปในเครื่องใหม่จากระยะไกล
ชุดสร้างไวรัส Kit (virus generator)	ชุดเครื่องมือสำหรับสร้างไวรัสใหม่โดยอัตโนมัติ
สแปม (Spammer programs)	ใช้ในการส่งอีเมลที่ไม่ต้องการจำนวนมาก
Flooders	ใช้ในการโจมตีระบบคอมพิวเตอร์เครือข่ายที่มีปริมาณการรับส่งข้อมูลจำนวนมากเพื่อดำเนินการโจมตีแบบปฏิเสธการให้บริการ (DoS)
Keyloggers	จับภาพคีย์สโตรกบนระบบที่ถูกบุกรุก
Rootkit	ชุดเครื่องมือแฮกเกอร์ที่ใช้หลังจากที่ผู้โจมตีเจาะระบบคอมพิวเตอร์และได้รับสิทธิ์การเข้าถึงระดับสูง
Zombie, bot	โปรแกรมที่เปิดใช้งานบนเครื่องที่ติดไวรัสจะถูกเปิดใช้งานเพื่อโจมตีเครื่องอื่น
Spyware	ซอฟต์แวร์ที่รวบรวมข้อมูลจากคอมพิวเตอร์และส่งไปยังระบบอื่น

ชื่อ	คำอธิบาย
Adware	โฆษณาที่ผสมรวมเข้ากับซอฟต์แวร์ ซึ่งอาจส่งผลให้เกิดโฆษณาแบบป๊อปอัพหรือการเปลี่ยนเส้นทางเบราว์เซอร์ไปยังเว็บไซต์เชิงพาณิชย์

เรายังสามารถแยกความแตกต่างระหว่างภัยคุกคามซอฟต์แวร์ที่ไม่ได้ทำซ้ำและภัยคุกคามซอฟต์แวร์ที่ทำซ้ำได้ ภัยคุกคามซอฟต์แวร์แบบแรกคือโปรแกรมหรือส่วนของโปรแกรมที่ถูกกระตุ้นโดยทริกเกอร์ ตัวอย่างเช่น ลอจิกบอมบ์ แบ็คดอร์ และโปรแกรมบอท ภัยคุกคามซอฟต์แวร์แบบหลังประกอบด้วยส่วนของโปรแกรมหรือโปรแกรมอิสระ ซึ่งเมื่อถูกเรียกใช้งานอาจสร้างสำเนาของตัวเองได้หนึ่งชุดหรือมากกว่า ไวรัสและเวิร์มสามารถเปิดใช้งานได้ในภายหลังบนระบบเดียวกันหรือระบบอื่น ตัวอย่างไวรัสและเวิร์ม

ในส่วนที่เหลือของหัวข้อนี้ เราจะสำรวจหมวดหมู่หลักของซอฟต์แวร์ที่เป็นอันตรายโดยย่อ โดยจะเลื่อนการอภิปรายเกี่ยวกับหัวข้อหลักของไวรัสและเวิร์มไปไว้ในส่วนถัดไป

ประตูลับ (Backdoor or trapdoor)

แบ็คดอร์ หรือที่รู้จักกันในชื่อแทรปดอร์ คือจุดเข้าใช้งานลับในโปรแกรมที่อนุญาตให้ผู้รู้ถึง ประตูลับเข้าถึงได้โดยไม่ต้องผ่านขั้นตอนการเข้าถึงความปลอดภัยตามปกติ โปรแกรมเมอร์ใช้ ประตูลับอย่างถูกต้องมาเป็นเวลาหลายปีเพื่อดีบั๊กและทดสอบโปรแกรม ประตูลับนี้เรียกว่า **เมนเทนแนนซ์ฮุก (Maintenance Hook)** ซึ่งมักจะเกิดขึ้นเมื่อโปรแกรมเมอร์กำลังพัฒนาแอปพลิเคชันที่มีขั้นตอนการตรวจสอบสิทธิ์ หรือการตั้งค่าที่ใช้เวลานาน ซึ่งกำหนดให้ผู้ใช้งานต้องป้อนค่าต่างๆ มากมายเพื่อรันแอปพลิเคชัน ในการดีบั๊กโปรแกรม นักพัฒนาอาจต้องการได้รับสิทธิพิเศษ หรือหลีกเลี่ยงการตั้งค่าและการตรวจสอบสิทธิ์ที่จำเป็นทั้งหมด

นอกจากนี้ โปรแกรมเมอร์อาจต้องการตรวจสอบให้แน่ใจว่ามีวิธีการเปิดใช้งานโปรแกรมในกรณีที่มีข้อผิดพลาดเกิดขึ้นกับขั้นตอนการตรวจสอบสิทธิ์ที่สร้างขึ้นในแอปพลิเคชัน ประตูลับคือโค้ดที่จดจำลำดับอินพุตพิเศษ หรือถูกเรียกใช้งานโดยรหัสผู้ใช้ที่กำหนด หรือลำดับเหตุการณ์ที่ไม่คาดคิด แบ็คดอร์กลายเป็นภัยคุกคามเมื่อโปรแกรมเมอร์ที่ร้ายกายใช้แบ็คดอร์เพื่อเข้าถึงโดยไม่ได้รับอนุญาต

ประตูลับเป็นแนวคิดพื้นฐานสำหรับช่องโหว่ที่ปรากฏในภาพยนตร์ War Games อีกตัวอย่างหนึ่งคือ ในระหว่างการพัฒนา Multics มีการทดสอบการเจาะระบบโดย "ทีมเสือ" ของกองทัพอากาศ (จำลองสถานการณ์ศัตรู) หนึ่งในกลยุทธ์ที่ใช้คือการส่งการอัปเดตระบบปฏิบัติการปลอมไปยังเว็บไซต์ที่ใช้ Multics การอัปเดตดังกล่าวมีม้าโทรจัน ซึ่งจะอธิบายในภายหลัง ที่สามารถเปิดใช้งานได้โดยแบ็คดอร์และทำให้ทีมเสือสามารถเข้าถึงระบบได้ ภัยคุกคามนี้ถูกนำไปใช้อย่างมีประสิทธิภาพมากจนนักพัฒนา Multics ไม่สามารถตรวจจับได้ แม้จะได้รับแจ้งว่ามีภัยคุกคามนี้อยู่ [ENGE80]

การควบคุมระบบปฏิบัติการสำหรับแฮคเกอร์เป็นเรื่องยาก มาตรการรักษาความปลอดภัยต้องมุ่งเน้นไปที่การพัฒนาโปรแกรมและกิจกรรมการอัปเดตซอฟต์แวร์

ลोजิกบอมบ์ (Logic Bomb)

หนึ่งในภัยคุกคามโปรแกรมที่เก่าแก่ที่สุด ซึ่งมักจะเกิดขึ้นก่อนไวรัสและเวิร์ม คือ ลोजิกบอมบ์ ลोजิกบอมบ์คือรหัสที่ฝังอยู่ในโปรแกรมที่ต้องตามกฎหมาย ซึ่งจะถูกตั้งค่าให้ "บอมบ์หรือระเบิด" เมื่อเป็นไปตามเงื่อนไขที่กำหนด ตัวอย่างของเงื่อนไขที่สามารถใช้เป็นตัวกระตุ้นสำหรับลोजิกบอมบ์ ได้แก่ การมีหรือไม่มีไฟล์บางไฟล์ วันหรือวันที่ใดวันหนึ่ง หรือผู้ใช้รายใดรายหนึ่งที่กำลังรันแอปพลิเคชัน เมื่อถูกกระตุ้น

ลोजิกบอมบ์อาจเปลี่ยนแปลงหรือลบข้อมูลหรือไฟล์ทั้งหมด ทำให้เครื่องหยุดทำงาน หรือสร้างความเสียหายอื่นๆ ตัวอย่างที่โดดเด่นของการใช้ลोजิกบอมบ์คือกรณีของทิม ลอยด์ ซึ่งถูกตัดสินว่ามีความผิดฐานวางระเบิดลोजิกที่ทำให้บริษัทโอเมก้า เอ็นจิเนียริง นายจ้างของเขาต้องสูญเสียเงินมากกว่า 10 ล้านดอลลาร์ ทำให้กลยุทธ์การเติบโตขององค์กรล้มเหลว และในที่สุดก็นำไปสู่การเลิกจ้างพนักงาน 80 คน [GAUD00] ในที่สุด ลอยด์ถูกตัดสินจำคุก 41 เดือน และสั่งให้ชดเชยค่าเสียหาย 2 ล้านดอลลาร์

ม้าโทรจัน (Trojan Horses)

ม้าโทรจันคือโปรแกรมหรือโปรซีเคอร์คำสั่งที่มีประโยชน์ หรือที่ดูเหมือนจะมีประโยชน์ ซึ่งประกอบด้วยโค้ดที่ซ่อนอยู่ ซึ่งเมื่อถูกเรียกใช้งานแล้ว จะทำงานบางอย่างที่ไม่พึงประสงค์หรือเป็นอันตราย โปรแกรมม้าโทรจันสามารถใช้เพื่อทำงานทางอ้อมที่ผู้ใช้ที่ไม่ได้รับอนุญาตไม่สามารถทำได้โดยตรง ตัวอย่างเช่น เพื่อเข้าถึงไฟล์ของผู้ใช้รายอื่นในระบบที่ใช้ร่วมกัน ผู้ใช้สามารถสร้างโปรแกรมม้าโทรจันที่เมื่อเรียกใช้งานแล้ว จะเปลี่ยนสิทธิ์ของไฟล์ของผู้ใช้ที่เรียกใช้งาน เพื่อให้ผู้ใช้ทุกคนสามารถอ่านไฟล์ได้ จากนั้น ผู้สร้างสามารถชักชวนให้ผู้ใช้เรียกใช้งานโปรแกรมโดยวางไว้ในไดเรกทอรีทั่วไปและตั้งชื่อให้ดูเหมือนเป็นโปรแกรมมัลแวร์ประโยชน์หรือแอปพลิเคชันที่มีประโยชน์ ตัวอย่างเช่น โปรแกรมที่แสดงรายการไฟล์ของผู้ใช้ในรูปแบบที่ต้องการ หลังจากที่ใช้รายอื่นเรียกใช้งานโปรแกรมแล้ว ผู้สร้างโปรแกรมจะสามารถเข้าถึงข้อมูลในไฟล์ของผู้ใช้ได้

ตัวอย่างของโปรแกรมโทรจันที่ตรวจจับได้ยากคือคอมไพเลอร์ที่ถูกดัดแปลงเพื่อแทรกรหัสเพิ่มเติมลงในบางโปรแกรมขณะที่คอมไพล์ เช่น โปรแกรมล็อกอินระบบ [THOM84] รหัสนี้จะสร้างช่องโหว่ในโปรแกรมล็อกอินที่อนุญาตให้ผู้เขียนสามารถล็อกอินเข้าสู่ระบบโดยใช้รหัสผ่านพิเศษ โทรจันฮอर्सนี้ไม่สามารถถูกค้นพบได้โดยการอ่านรหัสต้นฉบับของโปรแกรมล็อกอิน แรงจูงใจทั่วไปอีกประการหนึ่งของโทรจันฮอर्स คือการทำลายข้อมูล โปรแกรมดูเหมือนจะทำหน้าที่ที่มีประโยชน์ (เช่น โปรแกรมเครื่องคิดเลข) แต่ก็อาจลบไฟล์ของผู้ใช้บางอย่างเช่นกัน ตัวอย่างเช่น ผู้บริหารของ CBS ตกเป็นเหยื่อของโทรจันฮอर्सที่ทำลายข้อมูลทั้งหมดที่อยู่ในหน่วยความจำคอมพิวเตอร์ของเขา [TIME90] โทรจันฮอर्सถูกฝังไว้ในรูปกราฟิกที่มีอยู่ในระบบกระดานข่าวอิเล็กทรอนิกส์

ม้าโทรจันสามารถแบ่งออกเป็น 3 รูปแบบ ได้ดังนี้

- 1) ยังคงทำหน้าที่ของโปรแกรมเดิมและดำเนินกิจกรรมอันตรายแยกต่างหาก
- 2) ยังคงทำหน้าที่ของโปรแกรมเดิมแต่ปรับเปลี่ยนฟังก์ชันเพื่อดำเนินกิจกรรมอันตราย (เช่น โปรแกรมล็อกอินเวอร์ชันม้าโทรจันที่รวบรวมรหัสผ่าน) หรือเพื่อปกปิดกิจกรรมอันตรายอื่นๆ (เช่น โปรแกรมรายชื่อกระบวนการเวอร์ชันม้าโทรจันที่ไม่แสดงกระบวนการอันตรายบางอย่าง)
- 3) ดำเนินฟังก์ชันอันตรายที่แทนที่ฟังก์ชันของโปรแกรมเดิมอย่างสมบูรณ์

โมบายโค้ด (Mobile Code)

โมบายโค้ด หมายถึงโปรแกรม (เช่น สคริปต์ มาโคร หรือคำสั่งพกพาอื่นๆ) ที่สามารถส่งไปยังแพลตฟอร์มที่หลากหลายโดยไม่มีการเปลี่ยนแปลงใดๆ และทำงานด้วยความหมายที่เหมือนกัน [JANS01] คำนี้ยังใช้กับสถานการณ์ที่เกี่ยวข้องกับแพลตฟอร์มจำนวนมากที่เป็นเนื้อเดียวกัน (เช่น Microsoft Windows) โมบายโค้ดจะถูกส่งจากระบบระยะไกลไปยังระบบภายในเครื่อง แล้วจึงทำงานบนระบบภายในเครื่องโดยไม่มีคำสั่งที่ชัดเจนจากผู้ใช้ โมบายโค้ดมักทำหน้าที่เป็นกลไกสำหรับไวรัส เวิร์ม หรือม้าโทรจันที่จะถูกส่งไปยังเวิร์กสเตชันของผู้ใช้ ในกรณีอื่นๆ โมบายโค้ดจะใช้ประโยชน์จากช่องโหว่เพื่อดำเนินการโจมตี เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการบุกรุกทูล กลไกที่นิยมใช้โมบายโค้ด ได้แก่ Java applets, ActiveX, JavaScript และ VBScript วิธีที่นิยมใช้โมบายโค้ดสำหรับการดำเนินการที่เป็นอันตรายบนระบบภายในเครื่อง ได้แก่ การเขียนสคริปต์ข้ามไซต์ (cross-site scripting), เว็บไซต์แบบอินเทอร์แอคทีฟและแบบไดนามิก, การแนบไฟล์อีเมล และการดาวน์โหลดจากเว็บไซต์ที่น่าเชื่อถือหรือซอฟต์แวร์ที่น่าเชื่อถือ

3.3.2 ไวรัส (VIRUSES)

3.3.1 ธรรมชาติของไวรัส

ไวรัสคอมพิวเตอร์คือซอฟต์แวร์ที่สามารถ "แพร่เชื้อ" โปรแกรมอื่นได้โดยการแก้ไขโปรแกรมเหล่านั้น การแก้ไขนี้รวมถึงการแทรกโปรแกรมต้นฉบับด้วยโปรแกรมจำลองเพื่อสร้างสำเนาของโปรแกรมไวรัส ซึ่งจากนั้นก็แพร่เชื้อไปยังโปรแกรมอื่นได้

ไวรัสคอมพิวเตอร์ปรากฏตัวครั้งแรกในช่วงต้นทศวรรษ 1980 และคำนี้ถูกตั้งเป็นชื่อเรียกของเฟร็ด โคเฮน ในปี 1983 โคเฮนเป็นผู้เขียนหนังสือที่บุกเบิกเกี่ยวกับเรื่องนี้ [COHE94] ไวรัสชีวภาพคือเศษเสี้ยวเล็กๆ ของรหัสพันธุกรรม DNA หรือ RNA ที่สามารถเข้าควบคุมกลไกของเซลล์ที่มีชีวิตและหลอกหล่อให้สร้างสำเนาไวรัสดั้งเดิมที่ไร้ที่ติหลายพันตัว เช่นเดียวกับไวรัสชีวภาพ ไวรัสคอมพิวเตอร์มีสูตรในการสร้างสำเนาตัวเองที่สมบูรณ์แบบอยู่ในรหัสคำสั่ง

ไวรัสทั่วไปจะฝังตัวอยู่ในโปรแกรมบนคอมพิวเตอร์ จากนั้นเมื่อใดก็ตามที่คอมพิวเตอร์ที่ติดเชื้อสัมผัสกับซอฟต์แวร์ที่ไม่ติดไวรัส สำเนาใหม่ของไวรัสจะถูกส่งไปยังโปรแกรมใหม่ ดังนั้น การติดเชื้อจึงสามารถแพร่กระจายจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้โดยผู้ใช้ที่ไม่ทันระวังตัว ซึ่งอาจจะสลับดิสก์หรือส่งโปรแกรมถึงกันผ่านเครือข่าย ในสภาพแวดล้อมเครือข่าย ความสามารถในการเข้าถึงแอปพลิเคชันและบริการของระบบบนคอมพิวเตอร์เครื่องอื่นถือเป็นแหล่งเพาะพันธุ์ที่สมบูรณ์แบบสำหรับการแพร่กระจายของไวรัส ไวรัสสามารถทำอะไรก็ได้ที่โปรแกรมอื่นทำได้ ความแตกต่างคือไวรัสจะแนบตัวเองเข้ากับโปรแกรมอื่นและทำงานอย่างลับๆ เมื่อโปรแกรมโฮสต์ทำงาน เมื่อไวรัสทำงานแล้ว มันสามารถทำงานใดๆ ก็ได้ เช่น การลบไฟล์และโปรแกรมที่ได้รับอนุญาตตามสิทธิ์ของผู้ใช้ปัจจุบัน

3.3.2 ส่วนประกอบของไวรัสคอมพิวเตอร์ มี 3 ส่วน [AYCO06]:

1) กลไกการติดไวรัส (Infection mechanism): วิธีที่ไวรัสแพร่กระจาย ซึ่งทำให้ไวรัสสามารถจำลองแบบได้ กลไกนี้เรียกอีกอย่างหนึ่งว่าเวกเตอร์การติดไวรัส (Infection vector)

2) ทริกเกอร์ (Trigger): เหตุการณ์หรือเงื่อนไขที่กำหนดว่าเพย์โหลดจะถูกเปิดใช้งานหรือส่งเมื่อใด

3) เพย์โหลด (Payload): สิ่งที่ไวรัสทำ นอกเหนือจากการแพร่กระจาย เพย์โหลดอาจเกี่ยวข้องกับ ความเสียหาย หรืออาจเกี่ยวข้องกับกิจกรรมที่ไม่เป็นอันตรายแต่สามารถสังเกตเห็นได้

ในช่วงชีวิตของไวรัส ไวรัสทั่วไปจะผ่านสัระยะดังต่อไปนี้:

1) ระยะเวลาพักตัว (Dormant phase): ไวรัสไม่ได้ทำงาน ในที่สุดไวรัสจะถูกเปิดใช้งานโดยเหตุการณ์บางอย่าง เช่น วันที่ การมีโปรแกรมหรือไฟล์อื่น หรือความจุของดิสก์เกินขีดจำกัด ไวรัสบางตัวไม่ได้มีระยะนี้

2) ระยะแพร่กระจาย (Propagation phase): ไวรัสจะคัดลอกตัวเองไปยังโปรแกรมอื่นหรือในพื้นที่ระบบเฉพาะบนดิสก์ สำเนาอาจไม่เหมือนกับเวอร์ชันที่แพร่กระจาย ไวรัสมักจะเปลี่ยนรูปร่างเพื่อหลบเลี่ยงการตรวจจับ โปรแกรมที่ติดไวรัสแต่ละโปรแกรมจะมีโคลนของไวรัส ซึ่งจะเข้าสู่ระยะแพร่กระจาย

3) ระยะกระตุ้น (Triggering phase): ไวรัสจะถูกกระตุ้นเพื่อทำงานตามหน้าที่ที่ตั้งใจไว้ เช่นเดียวกับระยะพักตัว ระยะกระตุ้นอาจเกิดจากเหตุการณ์ต่างๆ ของระบบ รวมถึงการนับจำนวนครั้งที่สำเนาของไวรัสนี้สร้างสำเนาของตัวเอง

4) ระยะการดำเนินการ (Execution phase): ฟังก์ชันถูกดำเนินการ ฟังก์ชันอาจไม่เป็นอันตราย เช่น มีข้อความบนหน้าจอ หรืออาจสร้างความเสียหาย เช่น การทำลายโปรแกรมและไฟล์ข้อมูล

ไวรัสส่วนใหญ่ทำงานในลักษณะที่เฉพาะเจาะจงกับระบบปฏิบัติการหนึ่งๆ และในบางกรณีก็เฉพาะเจาะจงกับแพลตฟอร์มฮาร์ดแวร์หนึ่งๆ ด้วยเหตุนี้ ไวรัสจึงถูกออกแบบมาเพื่อใช้ประโยชน์จากรายละเอียดและจุดอ่อนของระบบนั้นๆ

3.3.3 ประเภทไวรัส (Viruses Classification)

มีการแข่งขันกันอย่างต่อเนื่องระหว่างผู้เขียนไวรัสและผู้เขียนซอฟต์แวร์ป้องกันไวรัสนับตั้งแต่ไวรัสปรากฏตัวครั้งแรก เมื่อมีการพัฒนามาตรการรับมือที่มีประสิทธิภาพสำหรับไวรัสชนิดที่มีอยู่ ไวรัสชนิดใหม่ๆ ก็ได้รับการพัฒนาขึ้นเช่นกัน ไม่มีรูปแบบการจำแนกไวรัสแบบง่ายหรือเป็นที่ยอมรับกันโดยทั่วไป ในส่วนนี้ เราจะปฏิบัติตาม [AYCO06] และจำแนกไวรัสตามแกนตั้งฉากสองแกน ได้แก่ ประเภทของเป้าหมายที่ไวรัสพยายามแพร่เชื้อ และวิธีการที่ไวรัสใช้ในการปกปิดตัวเองไม่ให้ผู้ใช้และซอฟต์แวร์ป้องกันไวรัสตรวจพบ

การจำแนกไวรัสตามเป้าหมายประกอบด้วยหมวดหมู่ต่อไปนี้

ไวรัสบูตเซกเตอร์ (Boot sector infector): ติดไวรัสมาสเตอร์บูตเรคคอร์ดหรือบูตเรคคอร์ด และแพร่กระจายเมื่อบูตระบบจากดิสก์ที่มีไวรัส

ไวรัสไฟล์ (File infector): ติดไวรัสไฟล์ที่ระบบปฏิบัติการหรือเซลล์พิจารณาว่าสามารถปฏิบัติการได้

ไวรัสแมโคร (Macro virus): ติดไวรัสไฟล์ด้วยโค้ดแมโครที่แอปพลิเคชันตีความ

3.3.4 แรนซัมแวร์ (Ransomware)

แรนซัมแวร์เป็นประเภทของการโจมตีที่เป็นอันตราย โดยผู้โจมตีจะเข้ารหัสข้อมูลขององค์กรและเรียกร้องการชำระเงินเพื่อคืนการเข้าถึง ตัวอย่างการโจมตีด้วยแรนซัมแวร์สามารถเกิดขึ้นได้อย่างไร

- 1) ผู้ใช้ถูกล่อลวงให้คลิกลิงก์อันตรายที่ดาวน์โหลดไฟล์จากเว็บไซต์ภายนอก
- 2) ผู้ใช้ดำเนินการไฟล์โดยไม่รู้ตัวว่าไฟล์ดังกล่าวเป็นแรนซัมแวร์
- 3) แรนซัมแวร์ใช้ประโยชน์จากช่องโหว่ในคอมพิวเตอร์ของผู้ใช้และคอมพิวเตอร์อื่นเพื่อแพร่กระจายไปทั่วทั้งองค์กร
- 4) แรนซัมแวร์จะเข้ารหัสไฟล์บนคอมพิวเตอร์ทุกเครื่องพร้อมกัน จากนั้นแสดงข้อความบนหน้าจอเพื่อเรียกร้องการชำระเงินเพื่อแลกกับการถอดรหัสไฟล์

แรนซัมแวร์ขัดขวางหรือทำให้การดำเนินงานขององค์กรหยุดชะงัก และก่อให้เกิดปัญหาสำหรับฝ่ายบริหารองค์กรจะจ่ายค่าไถ่และหวังว่าผู้โจมตีจะรักษาคำพูดเกี่ยวกับการคืนการเข้าถึงหรือไม่ หรือว่าองค์กรไม่จ่ายค่าไถ่และคืนการดำเนินงานด้วยตนเอง

แรนซัมแวร์เป็นภัยคุกคามที่พบบ่อยต่อธุรกิจทุกประเภท ไม่ว่าจะเล็กหรือใหญ่ แรนซัมแวร์สามารถทำให้ธุรกิจต้องปิดตัวลงหรือหยุดชะงักการดำเนินงานเป็นเวลานาน การจ่ายค่าไถ่อาจมีค่าใช้จ่ายสูงมาก และไม่มีการรับประกันว่าจะกู้คืนข้อมูลได้ หากข้อมูลถูกค่าถูกขโมย อาจนำไปสู่กฎหมายแจ้งเตือนการละเมิดข้อมูลของรัฐ

อย่างไรก็ตาม องค์กรต่างๆ สามารถเตรียมรับมือกับการโจมตีด้วยแรนซัมแวร์ได้ ซึ่งรวมถึงการปกป้องข้อมูลและอุปกรณ์จากแรนซัมแวร์ และเตรียมพร้อมรับมือกับการโจมตีด้วยแรนซัมแวร์ที่ประสบความสำเร็จ ลักษณะของแรนซัมแวร์คืออาชญากรไซเบอร์พยายามทำให้มัลแวร์แพร่กระจายไปอย่างกว้างขวางที่สุดเท่าที่จะเป็นไปได้ ส่งผลให้คอมพิวเตอร์ของบุคคลทั่วไปและธุรกิจทุกขนาดติดไวรัส

วิธีทั่วไปที่แรนซัมแวร์สามารถโจมตีได้

- อีเมล – อีเมลฟิชซึ่งสามารถหลอกให้คุณคลิกบนไฟล์แนบ (“ใบแจ้งหนี้ด่วน”) ซึ่งทำให้โปรแกรมซอฟต์แวร์ที่เป็นอันตรายเข้าควบคุมคอมพิวเตอร์ของเราได้
- มัลแวร์ – หากเครือข่ายหรือซอฟต์แวร์ของเรามีความเสี่ยง อาชญากรไซเบอร์สามารถแอบเข้ามาและฝังโค้ดอันตรายได้ โค้ดเหล่านี้อาจถูกทิ้งไว้โดยไม่มีใครสังเกตเห็นเป็นระยะเวลาหนึ่ง ทำให้ผู้ร้ายมีเวลาเข้าถึงไฟล์และขโมยข้อมูล จากนั้นจึงปล่อยแรนซัมแวร์ออกมาเพื่อให้เรามองไม่เห็นความเสียหาย

แนวปฏิบัติเพื่อรับมือกับแรนซัมแวร์ตามแนวทางของ NIST

NIST แนะนำให้องค์กรต่างๆ ปฏิบัติตามขั้นตอนพื้นฐานเหล่านี้เพื่อช่วยป้องกันแรนซัมแวร์

- ใช้ซอฟต์แวร์ป้องกันไวรัสตลอดเวลา และตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้สแกนอีเมลและสื่อบันทึกข้อมูลแบบถอดได้ (เช่น แฟลชไดรฟ์) โดยอัตโนมัติเพื่อตรวจหาแรนซัมแวร์และมัลแวร์อื่นๆ
 - อัปเดตแพตช์คอมพิวเตอร์ทุกเครื่องให้สมบูรณ์
 - ใช้ผลิตภัณฑ์หรือบริการรักษาความปลอดภัยที่บล็อกการเข้าถึงเว็บไซต์แรนซัมแวร์ที่รู้จักบนอินเทอร์เน็ต
 - กำหนดค่าระบบปฏิบัติการหรือใช้ซอฟต์แวร์ของบุคคลที่สามเพื่ออนุญาตให้เฉพาะแอปพลิเคชันที่ได้รับอนุญาตเท่านั้นที่สามารถทำงานบนคอมพิวเตอร์ได้ ซึ่งจะป้องกันไม่ให้แรนซัมแวร์ทำงาน
 - จำกัดหรือห้ามใช้อุปกรณ์ส่วนตัวบนเครือข่ายขององค์กร และสำหรับการทำงานทางไกล/การเข้าถึงระยะไกล โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อรับประกันความปลอดภัย
- ผู้ใช้ควรปฏิบัติตามเคล็ดลับเหล่านี้สำหรับคอมพิวเตอร์ที่ใช้ทำงาน
- ใช้บัญชีผู้ใช้งานมาตรฐานแทนบัญชีที่มีสิทธิ์ระดับผู้ดูแลระบบเมื่อใดก็ตามที่เป็นไปได้

- หลีกเลี่ยงการใช้แอปพลิเคชันและเว็บไซต์ส่วนตัว เช่น อีเมล แชท และโซเชียลมีเดีย จากคอมพิวเตอร์ที่ทำงาน
- หลีกเลี่ยงการเปิดไฟล์ คลิกลิงก์ ฯลฯ จากแหล่งที่ไม่รู้จักโดยไม่ตรวจสอบเนื้อหาที่น่าสงสัยก่อน เช่น เราสามารถสแกนไฟล์ด้วยโปรแกรมป้องกันไวรัส หรือดูลิงก์เพื่อดูว่าลิงก์นั้นเชื่อมโยงไปยังเว็บไซต์ที่อ้างว่าเชื่อมโยงอยู่หรือไม่

การกู้คืนจากการโจมตีด้วยแรนซัมแวร์

แม้ว่าจะมีมาตรการป้องกันที่แนะนำไว้แล้ว แต่การโจมตีด้วยแรนซัมแวร์ต่อองค์กรอาจยังคงประสบความสำเร็จ องค์กรต่างๆ สามารถเตรียมพร้อมสำหรับสิ่งนี้ได้โดยการดำเนินการเพื่อให้แน่ใจว่าข้อมูลจะไม่เสียหาย หรือสูญหาย และสามารถกลับมาดำเนินงานตามปกติได้อย่างรวดเร็ว NIST แนะนำให้องค์กรต่างๆ ปฏิบัติตาม

ขั้นตอนเหล่านี้เพื่อเร่งการกู้คืน:

- พัฒนาและนำแผนการกู้คืนเหตุการณ์ (Incident Recovery Plan) มาใช้ โดยกำหนดบทบาทและกลยุทธ์ในการตัดสินใจ จากนั้นปฏิบัติตามแผนนั้นอย่างสม่ำเสมอ
- วางแผน ดำเนินการ และทดสอบกลยุทธ์การสำรองข้อมูลและการกู้คืนข้อมูลอย่างรอบคอบ สิ่งสำคัญไม่เพียงแต่ต้องมีการสำรองข้อมูลสำคัญทั้งหมดของเราอย่างปลอดภัยเท่านั้น แต่ยังต้องแน่ใจว่ามีการแยกข้อมูลสำรองไว้ต่างหาก เพื่อไม่ให้แรนซัมแวร์แพร่กระจายไปยังข้อมูลเหล่านั้นได้ง่าย
- จัดทำรายชื่อผู้ติดต่อภายในและภายนอกสำหรับการโจมตีด้วยแรนซัมแวร์ให้เป็นปัจจุบัน รวมถึงหน่วยงานบังคับใช้กฎหมาย และทำความเข้าใจบทบาทของผู้ติดต่อแต่ละรายในการกู้คืนข้อมูล

3.4 การบุกรุก (Intrusion)

ปัญหาความปลอดภัยที่สำคัญสำหรับระบบเครือข่าย คือการบุกรุกโดยผู้ใช้หรือซอฟต์แวร์ หรืออย่างน้อยก็ไม่พึงประสงค์ การบุกรุกโดยผู้ใช้อาจอยู่ในรูปแบบการเข้าสู่ระบบโดยไม่ได้รับอนุญาต หรือในกรณีของผู้ใช้ที่ได้รับอนุญาต อาจอยู่ในรูปแบบการได้มาซึ่งสิทธิ์ หรือการดำเนินการใดๆ นอกเหนือจากที่ได้รับอนุญาต การบุกรุกโดยซอฟต์แวร์อาจอยู่ในรูปแบบไวรัส เวิร์ม หรือมัลโทรจันฮอรัส การโจมตีทั้งหมดนี้เกี่ยวข้องกับความปลอดภัยของเครือข่าย เนื่องจากการเข้าถึงระบบสามารถทำได้ผ่านเครือข่าย

อย่างไรก็ตาม การโจมตีเหล่านี้ไม่ได้จำกัดอยู่แค่การโจมตีบนเครือข่าย ผู้ใช้ที่สามารถเข้าถึงเทอร์มินัลภายในระบบอาจพยายามบุกรุกโดยไม่ต้องใช้เครือข่ายตัวกลาง ไวรัสหรือโทรจันฮอรัสอาจถูกนำเข้าสู่ระบบผ่านแผ่นดิสก์ออปติคัล มีเพียงเวิร์มเท่านั้นที่เป็นข้อเฉพาะของเครือข่าย ดังนั้น การบุกรุกระบบจึงเป็นประเด็นที่ความกังวลเกี่ยวกับความปลอดภัยของเครือข่ายและความปลอดภัยของคอมพิวเตอร์ทับซ้อนกัน

3.4.1 ผู้บุกรุก (Intruder)

หนึ่งในสองภัยคุกคามต่อความปลอดภัยที่ได้รับการเผยแพร่มากที่สุดคือ**ผู้บุกรุก** (อีกประเภทหนึ่งคือไวรัส) ซึ่งมักเรียกว่าแฮ็กเกอร์หรือแคร็กเกอร์ ในการศึกษาการบุกรุกที่สำคัญในระยะแรก แอนเดอร์สัน [ANDE80] ได้ระบุผู้บุกรุก 3 ประเภท ได้แก่:

ผู้ปลอมตัว (Masquerader): บุคคลที่ไม่ได้รับอนุญาตให้ใช้คอมพิวเตอร์และเจาะระบบเพื่อใช้ประโยชน์จากบัญชีผู้ใช้ที่ถูกต้อง

ผู้กระทำความผิด (Misfeasor): ผู้ใช้ที่ถูกต้องตามกฎหมายที่เข้าถึงข้อมูล โปรแกรม หรือทรัพยากรที่ไม่ได้รับอนุญาต หรือผู้ที่ได้รับอนุญาตให้เข้าถึงแต่ใช้สิทธิ์ในทางที่ผิด

ผู้ใช้ที่ไม่ได้รับอนุญาต (Clandestine user): บุคคลที่ยึดครองการควบคุมดูแลระบบและใช้การควบคุมนี้เพื่อหลบเลี่ยงการตรวจสอบและการควบคุมการเข้าถึง หรือเพื่อยับยั้งการรวบรวมการตรวจสอบ

ผู้ปลอมตัวมักจะเป็นคนนอก ส่วนผู้กระทำความผิดมักจะเป็นคนใน และผู้ใช้ที่แอบแฝงอาจเป็นคนนอกหรือคนในก็ได้ การโจมตีของผู้บุกรุกมีตั้งแต่ระดับไม่ร้ายแรงไปจนถึงระดับร้ายแรง ในระดับที่ไม่ร้ายแรง มีคนจำนวนมากที่ต้องการสำรวจอินเทอร์เน็ตและดูว่ามีอะไรอยู่ในนั้นบ้าง ในระดับที่ร้ายแรงคือผู้ที่พยายามอ่านข้อมูลที่มีสิทธิพิเศษ เปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือทำลายระบบ

[GRAN04] แสดงรายการตัวอย่างการบุกรุกดังต่อไปนี้:

- การดำเนินการบุกรุกทุกระยะไกลของเซิร์ฟเวอร์อีเมล
- การทำลายเว็บเซิร์ฟเวอร์
- การเดาและแคร็กพาสเวิร์ด
- การคัดลอกฐานข้อมูลที่มีหมายเลขบัตรเครดิต
- การดูข้อมูลที่ละเอียดอ่อน รวมถึงบันทึกเงินเดือนและข้อมูลทางการแพทย์โดยไม่ได้รับอนุญาต
- การรันโปรแกรมดักจับแพ็กเก็ตบนเวิร์กสเตชันเพื่อจับชื่อผู้ใช้และรหัสผ่าน
- การใช้ข้อผิดพลาดการอนุญาตบนเซิร์ฟเวอร์ FTP ที่ไม่เปิดเผยตัวตนเพื่อแจกจ่ายซอฟต์แวร์ละเมิดลิขสิทธิ์และไฟล์เพลง
- การโทรเข้าโมเด็มที่ไม่ปลอดภัยและเข้าถึงเครือข่ายภายใน
- การแอบอ้างเป็นผู้บริหาร โทรหาฝ่ายช่วยเหลือ รีเซตพาสเวิร์ดอีเมลของผู้บริหาร และเรียนรู้พาสเวิร์ดใหม่
- การใช้เวิร์กสเตชันที่เข้าสู่ระบบโดยไม่มีใครดูแลโดยไม่ได้รับอนุญาต

3.4.2 รูปแบบพฤติกรรมผู้บุกรุก

เทคนิคและรูปแบบพฤติกรรมของผู้บุกรุกเปลี่ยนแปลงอยู่ตลอดเวลา เพื่อใช้ประโยชน์จากจุดอ่อนที่เพิ่งค้นพบและหลบเลี่ยงการตรวจจับและมาตรการรับมือ อย่างไรก็ตาม โดยทั่วไปแล้วผู้บุกรุกมักปฏิบัติตามรูปแบบพฤติกรรมที่รู้จักรูปแบบใดรูปแบบหนึ่ง และรูปแบบเหล่านี้มักจะแตกต่างจากผู้ใช้ทั่วไป สรุปพฤติกรรมดังกล่าว

แฮกเกอร์ (Hacker)

โดยทั่วไปแล้ว ผู้ที่แฮ็กคอมพิวเตอร์มักทำเพื่อความตื่นเต้นหรือเพื่อสถานะ ชุมชนแฮกเกอร์เป็นระบบคุณธรรมที่แข็งแกร่ง ซึ่งสถานะถูกกำหนดโดยระดับความสามารถ ดังนั้น ผู้โจมตีจึงมักมองหาเป้าหมายที่มีโอกาสแล้วจึงแบ่งปันข้อมูลกับผู้อื่น ตัวอย่างทั่วไปคือการบุกรุกสถาบันการเงินขนาดใหญ่แห่งหนึ่งที่รายงานใน [RADCO4] ผู้บุกรุกใช้ประโยชน์จากข้อเท็จจริงที่ว่าเครือข่ายขององค์กรกำลังใช้งานบริการที่ไม่มีการป้องกัน ซึ่งบางบริการก็ไม่จำเป็นต้องใช้ด้วยซ้ำ ในกรณีนี้ ภัยคุกคามสำคัญของการบุกรุกคือแอปพลิเคชัน pcAnywhere ผู้ผลิต Symantec โฆษณาโปรแกรมนี้ว่าเป็นโซลูชันการควบคุมระยะไกลที่ช่วยให้สามารถเชื่อมต่อกับอุปกรณ์ระยะไกลได้อย่างปลอดภัย แต่ผู้โจมตีสามารถเข้าถึง pcAnywhere ได้อย่างง่ายดาย โดยผู้ดูแลระบบใช้ชื่อผู้ใช้และรหัสผ่านส่วนตัวอักษรเดียวกันกับโปรแกรม ในกรณีนี้ ไม่มีระบบตรวจจับการบุกรุกบนเครือข่ายองค์กรขนาด 700 โหนด ผู้บุกรุกถูกค้นพบเมื่อรองประธานเดินเข้าไปในสำนักงานของเธอและเห็นเคอร์เซอร์กำลังย้ายไฟล์ไปมาบนเวิร์กสเตชัน Windows ของเธอ

ตัวอย่างรูปแบบพฤติกรรมการบุกรุกบางประการ

(ก) Hacker
1. เลือกเป้าหมายโดยใช้เครื่องมือค้นหา IP เช่น NSLookup, Dig และอื่นๆ 2. จัดทำแผนที่เครือข่ายสำหรับบริการที่สามารถเข้าถึงได้โดยใช้เครื่องมือ เช่น NMAP 3. ระบุบริการที่อาจมีความเสี่ยง (ในกรณีนี้คือ pcAnywhere) 4. คาดเดารหัสผ่าน pcAnywhere 5. ติดตั้งเครื่องมือการดูแลระบบระยะไกลชื่อ DameWare 6. รอให้ผู้ดูแลระบบเข้าสู่ระบบและบันทึกการรหัสผ่าน 7. ใช้รหัสผ่านนั้นเพื่อเข้าถึงเครือข่ายที่เหลือ
(ข) องค์กรอาชญากรรม Criminal Enterprise)
1. ดำเนินการอย่างรวดเร็วและแม่นยำเพื่อให้กิจกรรมของพวกเขาหนีการตรวจจับ 2. ใช้ประโยชน์จากพื้นที่โดยรอบผ่านพอร์ตที่มีช่องโหว่ 3. ใช้ม้าโทรจัน (ซอฟต์แวร์ที่ซ่อนอยู่) เพื่อเปิดช่องทางเข้าออกได้อีกครั้ง 4. ใช้โปรแกรมดักจับรหัสผ่าน 5. อยู่อย่างจนถูกสังเกตเห็น 6. ทำผิดพลาดน้อยที่สุดหรือไม่มีเลย
(ค) ภัยคุกคามภายใน (Internal Threat)

1. สร้างบัญชีเครือข่ายสำหรับตนเองและเพื่อนๆ
2. เข้าถึงบัญชีและแอปพลิเคชันที่ปกติแล้วไม่ได้ใช้สำหรับงานประจำวัน
3. ส่งอีเมลถึงอดีตนายจ้างและนายจ้างที่กำลังจะจ้าง
4. แชนแบบลับๆ ผ่านข้อความโต้ตอบแบบทันที
5. เยี่ยมชมเว็บไซต์ที่ให้บริการแก่พนักงานที่ไม่พอใจ เช่น fdcompany.com
6. ดาวน์โหลดไฟล์ขนาดใหญ่และคัดลอกไฟล์
7. เข้าถึงเครือข่ายนอกเวลาทำการ

ผู้บุกรุกที่ไม่เป็นอันตรายอาจยอมรับได้ แม้ว่าพวกเขาจะใช้ทรัพยากรมากและอาจทำให้ประสิทธิภาพการทำงานของผู้ใช้ที่ถูกต้องลดลง อย่างไรก็ตาม ไม่มีทางทราบล่วงหน้าได้ว่าผู้บุกรุกจะเป็นแบบไม่เป็นอันตรายหรือเป็นอันตราย ดังนั้น แม้แต่ระบบที่ไม่มีทรัพยากรที่ละเอียดอ่อนเป็นพิเศษ ก็ยังมีเหตุผลที่จะควบคุมปัญหานี้ ระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) ได้รับการออกแบบมาเพื่อรับมือกับภัยคุกคามจากแฮ็กเกอร์ประเภทนี้

นอกจากการใช้ระบบดังกล่าวแล้ว องค์กรต่างๆ ยังสามารถพิจารณาจำกัดการเข้าสู่ระบบระยะไกลเฉพาะที่อยู่ IP ที่กำหนด และ/หรือใช้เทคโนโลยีเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ได้อีกด้วย หนึ่งในผลลัพธ์ของการตระหนักรู้เกี่ยวกับปัญหาผู้บุกรุกที่เพิ่มมากขึ้นคือการจัดตั้งทีมตอบสนองฉุกเฉินทางคอมพิวเตอร์ (CERT) ขึ้นหลายทีม ความร่วมมือเหล่านี้รวบรวมข้อมูลเกี่ยวกับช่องโหว่ของระบบและเผยแพร่ไปยังผู้จัดการระบบ แฮ็กเกอร์ยังอ่านรายงานของ CERT เป็นประจำ ดังนั้น ผู้ดูแลระบบจึงควรติดตั้งแพตช์ซอฟต์แวร์ทั้งหมดอย่างรวดเร็วเพื่อแก้ไขช่องโหว่ที่พบ อย่างไรก็ตาม ด้วยความซับซ้อนของระบบไอทีจำนวนมากและอัตรา การเผยแพร่แพตช์ที่สูงมาก ทำให้การดำเนินการนี้ยากขึ้นเรื่อยๆ หากปราศจากการอัปเดตอัตโนมัติ ถึงกระนั้นก็ยัง มีปัญหาที่เกิดจากความไม่เข้ากันอันเป็นผลมาจากซอฟต์แวร์ที่อัปเดต ดังนั้นจึงจำเป็นต้องมีการป้องกันหลายชั้น เพื่อจัดการกับภัยคุกคามด้านความปลอดภัยต่อระบบไอที

อาชญากร (Criminals)

กลุ่มแฮ็กเกอร์ที่จัดตั้งขึ้นกลายเป็นภัยคุกคามที่แพร่หลายและพบได้บ่อยต่อระบบอินเทอร์เน็ต กลุ่มเหล่านี้อาจทำงานให้กับบริษัทหรือรัฐบาล แต่มักเป็นกลุ่มแฮ็กเกอร์ที่มีส่วนเกี่ยวข้องอย่างหลวมๆ โดยทั่วไปแล้ว แก๊งเหล่านี้มักเป็นแฮ็กเกอร์รุ่นใหม่ มักเป็นชาวยุโรปตะวันออก รัสเซีย หรือเอเชียตะวันออกเฉียงใต้ ที่ทำธุรกิจบนเว็บ [ANTE06] พวกเขาพบปะกันในฟอรัมใต้ดินที่มีชื่ออย่าง DarkMarket.org และ theftservices.com เพื่อแลกเปลี่ยนเคล็ดลับและข้อมูล และประสานงานการโจมตี เป้าหมายที่พบบ่อยคือไฟล์บัตรเครดิตในเซิร์ฟเวอร์อีคอมเมิร์ซ ผู้โจมตีพยายามเข้าถึงสิทธิ์รัฐ หมายเลขบัตรจะถูกใช้โดยกลุ่มอาชญากรเพื่อซื้อสินค้าราคาแพง จากนั้น

จึงถูกโพสต์ไปยังเว็บไซต์บัตรเครดิต ซึ่งผู้อื่นสามารถเข้าถึงและใช้หมายเลขบัญชีได้ ซึ่งทำให้รูปแบบการใช้งานถูกบดบังและทำให้การตรวจสอบมีความซับซ้อน

ในขณะที่แฮกเกอร์แบบดั้งเดิมมองหาเป้าหมายที่เป็นโอกาส แฮกเกอร์อาชญากรมักจะมีเป้าหมายที่เฉพาะเจาะจง หรืออย่างน้อยก็ประเภทของเป้าหมายอยู่ในใจ เมื่อเว็บไซต์ถูกเจาะเข้าไป ผู้โจมตีจะดำเนินการอย่างรวดเร็ว ขโมยข้อมูลที่มีค่าให้ได้มากที่สุดเท่าที่จะทำได้และออกจากระบบไป

แม้ว่า DS และ IPS ยังสามารถใช้กับผู้โจมตีประเภทนี้ได้เช่นกัน แต่อาจมีประสิทธิภาพน้อยกว่าเนื่องจากการโจมตีประเภทนี้เข้าและออกได้อย่างรวดเร็ว สำหรับเว็บไซต์อีคอมเมิร์ซ ควรใช้การเข้ารหัสฐานข้อมูลสำหรับข้อมูลลูกค้าที่ละเอียดอ่อน โดยเฉพาะอย่างยิ่งบัตรเครดิต สำหรับเว็บไซต์อีคอมเมิร์ซที่โฮสต์ (ให้บริการโดยผู้ให้บริการภายนอก) องค์กรอีคอมเมิร์ซควรใช้เซิร์ฟเวอร์เฉพาะ (ไม่ได้ใช้เพื่อรองรับลูกค้าหลายราย) และติดตามบริการด้านความปลอดภัยของผู้ให้บริการอย่างใกล้ชิด

การโจมตีจากภายใน (Insider attacks)

การโจมตีจากภายในเป็นหนึ่งในสิ่งที่ตรวจจับและป้องกันได้ยากที่สุด พนักงานสามารถเข้าถึงและมีความรู้เกี่ยวกับโครงสร้างและเนื้อหาของฐานข้อมูลขององค์กรอยู่แล้ว การโจมตีจากภายในอาจเกิดจากความแค้นหรือเพียงแค่ความรู้สึกว่าตนมีสิทธิ์ ตัวอย่างเช่น กรณีของ Kenneth Patterson ซึ่งถูกไล่ออกจากตำแหน่งผู้จัดการฝ่ายสื่อสารข้อมูลของ American Eagle Outfitters Patterson ได้รับการดำเนินการซื้อสินค้าด้วยบัตรเครดิตของบริษัทในช่วงห้าวันของเทศกาลวันหยุดปี 2002 สำหรับความรู้สึกว่าตนมีสิทธิ์ ผู้บุกรุกมีพนักงานจำนวนมากที่รู้สึกว่ารื้อถอนมีสิทธิ์นำอุปกรณ์สำนักงานเพิ่มเติมไปใช้งานที่บ้าน แต่ปัจจุบันสิ่งนี้ขยายไปถึงข้อมูลขององค์กรด้วย ตัวอย่างเช่น รองประธานฝ่ายขายของบริษัทวิเคราะห์หุ้นแห่งหนึ่งที่ลาออกเพื่อไปหาคู่แข่ง ก่อนลาออก เธอได้คัดลอกฐานข้อมูลลูกค้าเพื่อนำติดตัวไปด้วย ผู้กระทำความผิดรายงานว่าได้รู้สึกขุ่นเคืองใจพนักงานเก่าของเธอ เธอเพียงต้องการข้อมูลดังกล่าวเพราะมันจะเป็นประโยชน์ต่อเธอ

แม้ว่าระบบ IDS และ IPS จะมีประโยชน์ในการรับมือกับการโจมตีจากภายใน แต่วิธีการอื่นๆ ที่ตรงไปตรงมามากกว่านั้นมีความสำคัญสูงกว่า ตัวอย่างเช่น

- บังคับใช้สิทธิ์ขั้นต่ำสุด โดยอนุญาตเฉพาะทรัพยากรที่พนักงานจำเป็นต้องใช้ในการทำงานเท่านั้น
 - ตั้งค่าบันทึกเพื่อดูว่าผู้ใช้เข้าถึงอะไรและป้อนคำสั่งอะไร
 - ปกป้องทรัพยากรสำคัญด้วยการตรวจสอบสิทธิ์ที่เข้มงวด
 - เมื่อสิ้นสุดการใช้งาน ให้ลบข้อมูลคอมพิวเตอร์และการเข้าถึงเครือข่ายของพนักงาน
 - เมื่อสิ้นสุดการใช้งาน ให้สร้างภาพสะท้อนของฮาร์ดไดรฟ์ของพนักงานก่อนที่จะนำกลับมาใช้ใหม่
- หลักฐานดังกล่าวอาจจำเป็นหากข้อมูลบริษัทของคุณถูกเปิดเผยต่อบริษัทคู่แข่ง

ในส่วนนี้ เราจะพิจารณาเทคนิคที่ใช้ในการบุกรุก จากนั้นเราจะพิจารณาวิธีการตรวจจับการบุกรุก

3.4.4 เทคนิคการบุกรุก (Intrusion Techniques)

วัตถุประสงค์ของผู้บุกรุกคือการเข้าถึงระบบหรือเพิ่มขอบเขตของสิทธิ์ที่สามารถเข้าถึงได้ในระบบ การโจมตีเบื้องต้นส่วนใหญ่ใช้ช่องโหว่ของระบบหรือซอฟต์แวร์ที่ทำให้ผู้ใช้สามารถรันโค้ดที่เปิดประตูหลังเข้าสู่ระบบได้ อีกทางเลือกหนึ่งคือผู้บุกรุกพยายามขโมยข้อมูลที่ควรได้รับการป้องกัน ในบางกรณี ข้อมูลนี้อาจอยู่ในรูปแบบของรหัสผ่านผู้ใช้ เมื่อทราบรหัสผ่านของผู้ใช้รายอื่น ผู้บุกรุกสามารถเข้าสู่ระบบและใช้สิทธิ์ทั้งหมดที่มอบให้กับผู้ใช้ที่ถูกต้องได้

โดยทั่วไป ระบบจะต้องรักษาไฟล์ที่เชื่อมโยงรหัสผ่านกับผู้ใช้ที่ได้รับอนุญาตแต่ละราย หากไฟล์ดังกล่าวถูกจัดเก็บโดยไม่มีการป้องกัน ก็จะสามารถเข้าถึงและเรียนรู้รหัสผ่านได้อย่างง่ายดาย ไฟล์รหัสผ่านสามารถป้องกันได้ 2 วิธี

ฟังก์ชันทางเดียว (One-way function): ระบบจะจัดเก็บเฉพาะค่าของฟังก์ชันตามรหัสผ่านของผู้ใช้ เมื่อผู้ใช้ป้อนรหัสผ่าน ระบบจะแปลงรหัสผ่านนั้นและเปรียบเทียบกับค่าที่เก็บไว้ ในทางปฏิบัติ ระบบมักจะทำการแปลงแบบทางเดียว (ไม่สามารถย้อนกลับได้) ซึ่งใช้รหัสผ่านเพื่อสร้างคีย์สำหรับฟังก์ชันทางเดียว และให้ผลลัพธ์ที่มีความยาวคงที่

การควบคุมการเข้าถึง (Access control): การเข้าถึงไฟล์รหัสผ่านถูกจำกัดไว้เพียงหนึ่งหรือไม่ก็บัญชีเท่านั้น

หากมีมาตรการรับมืออย่างใดอย่างหนึ่งหรือทั้งสองอย่าง ผู้บุกรุกอาจต้องใช้ความพยายามในการเรียนรู้รหัสผ่าน เทคนิคการเรียนรู้รหัสผ่าน ดังต่อไปนี้

- 1) ลองใช้รหัสผ่านเริ่มต้นที่ใช้กับบัญชีมาตรฐานที่มาพร้อมกับระบบ ผู้ดูแลระบบหลายคนไม่สนใจที่จะเปลี่ยนค่าเริ่มต้นเหล่านี้
- 2) ลองใช้รหัสผ่านสั้นทั้งหมดอย่างละเอียด (ที่มีความยาวหนึ่งถึงสามตัวอักษร)
- 3) ลองใช้คำศัพท์ในพจนานุกรมออนไลน์ของระบบหรือรายการรหัสผ่านที่น่าจะเป็นไปได้ ตัวอย่างรหัสผ่านแบบหลังสามารถหาได้ง่ายบนกระดานข่าวของแฮกเกอร์
- 4) รวบรวมข้อมูลเกี่ยวกับผู้ใช้ เช่น ชื่อเต็ม ชื่อคู่สมรสและบุตร รูปถ่ายในสำนักงาน และหนังสือในสำนักงานที่เกี่ยวข้องกับงานอดิเรก
- 5) ลองใช้หมายเลขโทรศัพท์ หมายเลขประกันสังคม และหมายเลขห้องพักของผู้ใช้
- 6) ลองใช้หมายเลขทะเบียนรถที่ถูกต้องทั้งหมดของรัฐนี้

7) ใช้โปรแกรมโทรจัน เพื่อข้ามข้อจำกัดการเข้าถึง

8) แตะเส้นแบ่งระหว่างผู้ใช้ระยะไกลและระบบโฮสต์

6 วิธีแรกเป็นวิธีการคาดเดารหัสผ่านที่หลากหลาย หากผู้บุกรุกจำเป็นต้องตรวจสอบการคาดเดาโดยการพยายามเข้าสู่ระบบ การโจมตีดังกล่าวจะยุ่งยากและแก้ไขได้ง่าย ตัวอย่างเช่น ระบบสามารถปฏิเสธการเข้าสู่ระบบใดๆ ได้หลังจากพยายามป้อนรหัสผ่านสามครั้ง ทำให้ผู้บุกรุกต้องเชื่อมต่อกับโฮสต์อีกครั้งเพื่อลองป้อนรหัสผ่านใหม่ ในสถานการณ์เช่นนี้ การพยายามป้อนรหัสผ่านมากกว่าไม่กี่ครั้งนั้นไม่สามารถทำได้จริง อย่างไรก็ตาม ผู้บุกรุกไม่น่าจะลองใช้วิธีการแบบหยาบๆ เช่นนี้ ตัวอย่างเช่น หากผู้บุกรุกสามารถเข้าถึงไฟล์รหัสผ่านที่เข้ารหัสด้วยสิทธิ์ระดับต่ำได้ กลยุทธ์ก็คือการดักจับไฟล์นั้น แล้วใช้กลไกการเข้ารหัสของระบบนั้นอย่างสบายๆ จนกว่าจะค้นพบรหัสผ่านที่ถูกต้องซึ่งให้สิทธิ์ที่สูงกว่า การโจมตีโดยการคาดเดาสามารถทำได้จริง และมีประสิทธิภาพสูง เมื่อมีการพยายามคาดเดาจำนวนมากโดยอัตโนมัติ และการตรวจสอบการคาดเดาแต่ละครั้งสามารถทำได้โดยที่กระบวนการคาดเดาไม่สามารถตรวจจับได้ ในบทนี้ เราจะกล่าวถึงการป้องกันการโจมตีโดยการคาดเดาไว้มากมาย

วิธีการโจมตีที่ 7 ที่กล่าวถึงก่อนหน้านี้ คือ ม้าโทรจัน ซึ่งรับมือได้ยากเป็นพิเศษ ตัวอย่างของโปรแกรมที่ข้ามการควบคุมการเข้าถึงได้กล่าวถึงใน [ALVA90] ผู้ใช้ที่มีสิทธิ์ระดับต่ำสร้างโปรแกรมเกมขึ้นมาและเชิญผู้ควบคุมระบบให้ใช้งานในเวลาว่าง โปรแกรมนั้นเล่นเกมจริง แต่เบื้องหลังยังมีโค้ดสำหรับคัดลอกไฟล์รหัสผ่านซึ่งไม่ได้เข้ารหัสแต่มีการป้องกันการเข้าถึง เข้าไปในไฟล์ของผู้ใช้ เนื่องจากเกมทำงานภายใต้โหมดสิทธิ์ระดับสูงของผู้ควบคุม จึงสามารถเข้าถึงไฟล์รหัสผ่านได้

การโจมตีที่ 8 ที่กล่าวถึง คือ การดักฟังสาย ซึ่งเป็นเรื่องของความปลอดภัยทางกายภาพ เทคนิคการบุกรุกอื่นๆ ไม่จำเป็นต้องเรียนรู้รหัสผ่าน ผู้บุกรุกสามารถเข้าถึงระบบได้โดยใช้ประโยชน์จากการโจมตี เช่น บัฟเฟอร์ล้นในโปรแกรมที่ทำงานด้วยสิทธิ์ระดับหนึ่ง การยกระดับสิทธิ์ก็สามารถทำได้ด้วยวิธีนี้เช่นกัน

มาตรการรับมือหลัก 2 ประการ ได้แก่ การตรวจจับและการป้องกัน การตรวจจับเกี่ยวข้องกับการเรียนรู้ถึงการโจมตี ไม่ว่าจะก่อนหรือหลังการโจมตีสำเร็จ การป้องกันเป็นเป้าหมายด้านความปลอดภัยที่ท้าทายและเป็น การต่อสู้ที่ยากลำบากตลอดเวลา ความยากลำบากเกิดจากข้อเท็จจริงที่ว่าฝ่ายป้องกันต้องพยายามขัดขวางการโจมตีทั้งหมดที่เป็นไปได้ ในขณะที่ฝ่ายโจมตีมีอิสระที่จะพยายามค้นหาจุดอ่อนที่สุดในห่วงโซ่การป้องกันและโจมตี ณ จุดนั้น

จะเห็นได้ว่า เราจะนำเสนอภาพรวมกว้างๆ ของข้อกังวลเหล่านี้จะครอบคลุมถึงผู้บุกรุก ชั้นแรก เราจะพิจารณาลักษณะของการโจมตี จากนั้นจึงพิจารณากลยุทธ์ที่ใช้ป้องกัน ส่วนการตรวจจับและการป้องกันนั้น จะมีรายละเอียดปรากฏในบทต่อไป

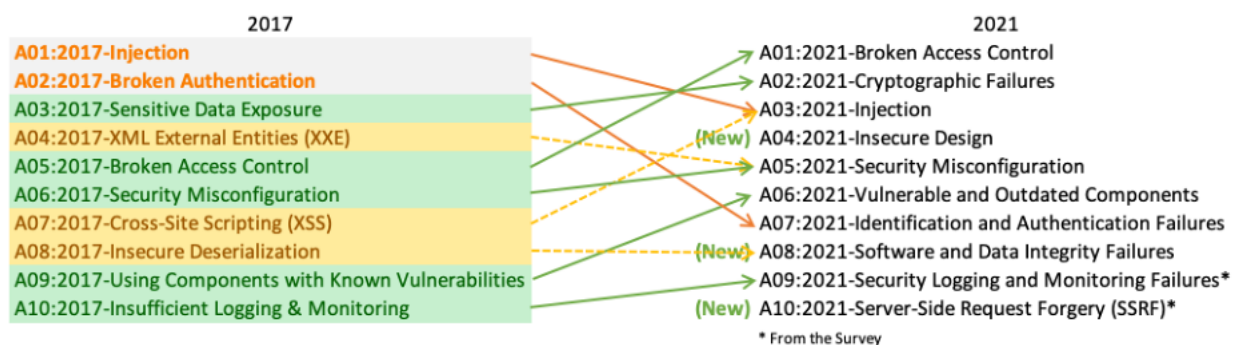
3.5 OWASP

OWASP หรือ Open Web Application Security Project จัดตั้งโดย OWASP Foundation เป็นองค์กรไม่แสวงหาผลกำไรที่ให้ความรู้เพื่อเน้นเรื่องระบบความปลอดภัยในภาพรวมในหลายแง่มุม ไม่ว่าจะเป็นการทดสอบเจาะระบบ การเขียนรหัสให้ปลอดภัย และการกำหนดนโยบายหรือมาตรฐาน ด้านความปลอดภัยให้แอปพลิเคชันทั้งทางเว็บไซต์ และความปลอดภัยของแอปพลิเคชันทางโทรศัพท์มือถือ

โครงการหนึ่งของ OWASP เรียกว่า OWASP Top 10 ที่จัดอันดับ 10 ความเสี่ยงทางด้านความปลอดภัยซึ่งทุกๆ 4 ปีจะมีการจัดอันดับช่องโหว่ใหม่เพื่อให้องค์กรต่างๆ ทั่วโลกได้นำข้อมูลไปเผยแพร่ไปใช้ปกป้องข้อมูลของตนเองได้อย่างถูกต้องและทันยุคทันสมัยต่อเหตุการณ์ต่างๆ ที่เกิดขึ้น โดยในช่วง 4 ปีที่ผ่านมา

3.5.1 OWASP Top 10 2021

มีอะไรเปลี่ยนแปลงบ้างใน 10 อันดับแรกของปี 2021 มีหมวดหมู่ใหม่ 3 หมวดหมู่ หมวดหมู่ 4 หมวดหมู่ที่มีการเปลี่ยนแปลงการตั้งชื่อและขอบเขต และการรวมบางส่วนใน 10 อันดับแรกสำหรับปี 2021 โดยได้เปลี่ยนชื่อเมื่อจำเป็นเพื่อเน้นที่สาเหตุหลักมากกว่าอาการ ดังรูป 3.1



รูป 3.1 OWASP Top 10 2021

(ที่มา: owasp.org)

อันดับที่ 1 A01:2021-Broken Access Control ขยับขึ้นจากอันดับที่ 5 มาอยู่ในหมวดหมู่ที่มีความเสี่ยงด้านความปลอดภัยของเว็บแอปพลิเคชันร้ายแรงที่สุด ข้อมูลที่ส่งมาบ้างชี้ว่าโดยเฉลี่ยแล้ว แอปพลิเคชัน 3.81% ที่ทดสอบมีการเจ็บบั๊กอ่อนร่ว่ม (Common Weakness Enumerations: CWE) อย่างน้อยหนึ่งรายการ โดยมี CWE เกิดขึ้นมากกว่า 318,000 รายการในหมวดหมู่ความเสี่ยงนี้ CWE จำนวน 34 รายการที่ถูกจับคู่กับ Broken Access Control นั้นมีเหตุการณ์เกิดขึ้นในแอปพลิเคชันมากกว่าหมวดหมู่อื่นๆ

วิธีป้องกัน

กรณีใช้ Apache ต้องตั้งค่า .htaccess เพื่อป้องกันการเข้าถึง directory ต่างๆ โดยตรง และต้องมีการตรวจสอบสถานะ Login ในทุกๆ หน้าที่เป็นหน้าของสมาชิกเว็บ รวมถึงตรวจสอบว่าหน้าสิทธิ์ของ User นี้สามารถทำอะไรได้บ้าง อ่านได้ เขียนได้ ลบได้หรือไม่? ถ้าไม่ได้ต้องแสดงข้อความว่า Access Denied ตั้งแต่แรก ต้องป้องกันไม่ให้นำเข้าถึงระบบได้

อันดับที่ 2 A02:2021-Cryptographic Failures ขยับขึ้นมาหนึ่งอันดับเป็นอันดับ 2 ซึ่งก่อนหน้านี้รู้จักกันในชื่อ A3:2017-Sensitive Data Exposure ซึ่งหมายถึงอาการทั่วไปมากกว่าสาเหตุหลัก ชื่อใหม่นี้มุ่งเน้นไปที่ความล้มเหลวที่เกี่ยวข้องกับการเข้ารหัสลับ ซึ่งก่อนหน้านี้เคยเกิดขึ้นโดยปริยาย หมายความว่ามักนำไปสู่การเปิดเผยข้อมูลสำคัญหรือการบุกรุกระบบ

วิธีป้องกัน

การไม่ได้เก็บข้อมูลรหัสผ่านแบบ Hash หรือใช้ Password Hashing Function ที่ล้าสมัยแล้วเช่น MD5, SHA1 และ password สามารถถูกใช้ฐานข้อมูล Rainbow Table ในการแกะ Hash ได้อย่างง่ายดาย

อันดับที่ 3 A03:2021- Injection เลื่อนลงมาที่ตำแหน่งที่สาม 94% ของแอปพลิเคชันได้รับการทดสอบการฉีดยาแบบ โดยมียัตราการเกิดสูงสุดที่ 19% อัตราการเกิดเฉลี่ยที่ 3.37% และ CWE จำนวน 33 รายการที่อยู่ในหมวดหมู่นี้มีการเกิดขึ้นมากเป็นอันดับสองในแอปพลิเคชัน โดยมีการเกิดขึ้น 274,000 ครั้ง ขณะนี้ Cross-site Scripting เป็นส่วนหนึ่งของหมวดหมู่นี้ในฉบับนี้

วิธีป้องกัน

ต้องใช้ Prepared Statement ในการ Query SQL หรือใช้คำสั่ง Escape Command ที่ถูกออกแบบมาโดยเฉพาะในแต่ละภาษาเพื่อป้องกันการส่ง Command โดยตรงมารัน

อันดับที่ 4 A04:2021-Insecure Design เป็นหมวดหมู่ใหม่สำหรับปี 2021 โดยมุ่งเน้นไปที่ความเสี่ยงที่เกี่ยวข้องกับข้อบกพร่องในการออกแบบ หากเราต้องการ "ก้าวไปทางด้านซ้าย" ในฐานะอุตสาหกรรมอย่างแท้จริง เราจำเป็นต้องมีการสร้างแบบจำลองภัยคุกคาม รูปแบบและหลักการการออกแบบที่ปลอดภัย และสถาปัตยกรรมอ้างอิงที่มากขึ้น การออกแบบที่ไม่ปลอดภัยไม่สามารถแก้ไขได้ด้วยการใช้งานที่สมบูรณ์แบบ เพราะตามนิยามแล้ว การควบคุมความปลอดภัยที่จำเป็นไม่เคยถูกสร้างขึ้นเพื่อป้องกันการโจมตีที่เฉพาะเจาะจง

วิธีป้องกัน

- เก็บข้อมูล Secret ใดๆ พวก api key, private key ไว้ที่ Client แม้ว่าจะมีการเข้ารหัสไว้แน่นหนา ก็ตาม ควรเก็บบน Server
- การอนุญาตให้แก้ไขข้อมูลสำคัญเช่น email โดยไม่ได้ถาม password ก่อนทำให้บุคคลอื่นสามารถกด forgot password เพื่อตั้งค่าน์รหัสผ่านใหม่ได้ทันทีที่เซตอีเมลใหม่ได้
- ใช้ระบบคำถามลึมรหัสผ่านที่ง่ายเกินไป เช่น วันเดือนปีเกิด ในการเข้าสู่ระบบเมื่อจำรหัสผ่านไม่ได้

- การ Design ที่ไม่ได้คิดเผื่อกรณีของ bot มาร่วมใช้งาน Software ด้วย เช่น การแจกเงินฟรีให้ account ใหม่ แล้วผู้ใช้งานสามารถสร้าง account มาโอนเงินฟรีให้กับ account อื่นได้ ทำให้บริษัทสูญเสียเงินจาก account เปิดใหม่เรื่อยๆ ไม่มีที่สิ้นสุดโดยไม่ได้กำไรจาก account เหล่านี้

อันดับที่ 5 A05:2021-Security Misconfiguration การกำหนดค่าความปลอดภัยผิดพลาด ขยับขึ้นจากอันดับที่ 6 ในฉบับก่อนหน้า โดยแอปพลิเคชัน 90% ได้รับการทดสอบหาการกำหนดค่าผิดพลาดในรูปแบบใดรูปแบบหนึ่ง โดยมีอัตราการเกิดเฉลี่ยอยู่ที่ 4.5% และมี CWEs มากกว่า 208,000 รายการที่ถูกจัดอยู่ในหมวดหมู่ความเสี่ยงนี้ ด้วยการเปลี่ยนแปลงไปสู่ซอฟต์แวร์ที่กำหนดค่าได้สูงมากขึ้น จึงไม่น่าแปลกใจที่หมวดหมู่นี้จะขยับขึ้นหมวดหมู่เดิมของ A4:2017-XML External Entities (XXE) ปัจจุบันเป็นส่วนหนึ่งของหมวดหมู่ความเสี่ยงนี้แล้ว

วิธีป้องกัน

อันดับที่ 6 A06:2021-Vulnerable and Outdated Components เดิมมีชื่อว่า Using Components with Known Vulnerabilities และอยู่ในอันดับที่ 2 ในการสำรวจชุมชน 10 อันดับแรก แต่ก็มีข้อมูลเพียงพอที่จะติดอันดับ 10 อันดับแรกผ่านการวิเคราะห์ข้อมูล หมวดหมู่นี้ขยับขึ้นจากอันดับที่ 9 ในปี 2017 และเป็นปัญหาที่ทราบอยู่แล้วซึ่งเราประสบปัญหาในการทดสอบและประเมินความเสี่ยง นี่เป็นหมวดหมู่เดียวที่ไม่มี Common Vulnerability and Exposures (CVE) ใดๆ ที่เชื่อมโยงกับ CWE ที่มีอยู่ ดังนั้นค่า exploit และ impact weight เริ่มต้น 5.0 จึงถูกนำมาพิจารณาในการให้คะแนน

วิธีป้องกัน

- Default Configuration หรือการใช้ค่า default ของซอฟต์แวร์โดยเฉพาะอย่างยิ่งฐานข้อมูล โดยไม่แก้ไข username และ password ก่อนใช้เลย เช่น admin, admin หรือ password วางเปล่า ส่งผลให้เดารหัสผ่านจาก google ได้ทันทีอย่างไม่ยากเย็นและเข้าถึงฐานข้อมูลได้
- เปิด Error Message ออกแสดงบนหน้า Web Browser ทำให้ผู้ใช้ทั่วไปเห็น Code หรือ Query ที่ใช้อย่างชัดเจน
- ตั้งค่า Config เป็น development mode แล้วนำ software version development ขึ้น production server สุดท้ายจึงทำงานได้ช้า และอาจไม่ได้เก็บ Error Log ลงไฟล์ ทำให้ย้อนมาดู Error ย้อนหลังไม่ได้
- Open cloud storage permission หรือตั้งค่า permission ผิด เช่น ตั้งค่าการเข้าถึง Amazon S3 เป็น Public ทั้งๆ ที่ค่า Default เป็น private ส่งผลให้ใครก็ได้เข้าถึงไฟล์บน S3 ของเราได้ทั้งหมด ถ้าเป็นข้อมูลสำคัญจะก่อให้เกิดความเสียหายมาก
- เปิด port หรือ permission ให้มากเกินไปจนจำเป็น เป็นการเปิดเผยช่องโหว่
- OS, Frameworks, Libraries ไม่มีการ config ค่าให้ปลอดภัยตามคำแนะนำก่อนขึ้น production

อันดับที่ 7 A07:2021- Identification and Authentication Failures ความล้มเหลวในการระบุตัวตนและการตรวจสอบสิทธิ์เดิมคือการตรวจสอบสิทธิ์ที่ไม่สมบูรณ์ และกำลังลดลงจากอันดับสอง และตอนนี้รวมถึง CWE ที่เกี่ยวข้องกับความปลอดภัยในการระบุตัวตนมากขึ้น หมวดหมู่นี้ยังคงเป็นส่วนสำคัญของ 10 อันดับแรก แต่ดูเหมือนว่าความพร้อมใช้งานของกรอบงานมาตรฐานที่เพิ่มขึ้นจะช่วยให้

วิธีป้องกัน

- ใช้ Multi Factor Authentication เช่น SMS เข้าช่วยยืนยันตัวตนนอกจาก password
- ไม่ส่ง default password ที่เหมือนกันทุก user โดยเฉพาะอย่างยิ่ง admin
- เพิ่มระบบ Weak password check
- ระวังการกำหนดให้ระบบจดจำ password กลายเป็นช่องโหว่ในการขอรหัสผ่านหรือสุ่มรหัสผ่านได้ง่าย
- Limit หรือ delay หากมีการ Login พลาดหลายครั้ง
- Session ID ต้องไม่ถูกส่งผ่าน URL
- ต้องมีการทำลาย session อย่างถูกต้องหลัง logout, timeout

อันดับที่ 8 A08:2021-Software and Data Integrity Failures ความล้มเหลวด้านความสมบูรณ์ของซอฟต์แวร์และข้อมูล เป็นหมวดหมู่ใหม่สำหรับปี 2021 โดยมุ่งเน้นไปที่การตั้งสมมติฐานเกี่ยวกับการอัปเดตซอฟต์แวร์ ข้อมูลสำคัญ และขั้นตอน CI/CD โดยไม่ตรวจสอบความสมบูรณ์ หนึ่งในผลกระทบที่มีน้ำหนักสูงสุดจากข้อมูล Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) ที่แมปกับ CWE 10 รายการในหมวดหมู่นี้ A8:2017-Insecure Deserialization เป็นส่วนหนึ่งของหมวดหมู่ที่ใหญ่กว่านี้แล้ว

วิธีป้องกัน

- ไม่ใช้ software ที่ version ยังไม่ stable ใช้แต่ตระกูล LTS
- เลือกใช้ Linux OS ที่ Stable เช่น Debian / Centos
- checksum hashes file ที่ Download มาทุกครั้งก่อน install

อันดับที่ 9 A09:2021-Security Logging and Monitoring Failures ความล้มเหลวในการบันทึกและติดตามความปลอดภัยเดิมก็คือ A10:2017-การบันทึกและติดตามไม่เพียงพอและถูกเพิ่มจากแบบสำรวจชุมชน 10 อันดับแรก (อันดับที่ 3) โดยขยับขึ้นจากอันดับที่ 10 ก่อนหน้านี้ หมวดหมู่นี้ได้รับการขยายให้ครอบคลุมประเภทของความล้มเหลวที่หลากหลายมากขึ้น ทดสอบได้ยาก และยังไม่ปรากฏในข้อมูล CVE/CVSS อย่างชัดเจน

อย่างไรก็ตาม ความล้มเหลวในหมวดหมู่นี้อาจส่งผลกระทบโดยตรงต่อการมองเห็น การแจ้งเตือนเหตุการณ์ และการตรวจสอบทางนิติวิทยาศาสตร์

วิธีป้องกัน

ควร Log พฤติกรรมสำคัญๆ ให้ครบ และตรวจสอบให้แน่ใจว่า Log ถูก generate ใน format ที่ centralized log management เข้ามาเก็บข้อมูลไปใช้ได้ง่ายเพื่อให้สามารถรวม Log มาอ่านได้ง่าย เพราะ Log กระจายอยู่หลายเครื่องมากเกินไป และต้องเก็บ Log แบบ Append Only เพื่อเก็บทุกเหตุการณ์ที่อาจเกิดเข้าไว้ด้วยกัน พร้อมระบบแจ้งเตือนเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น เพื่อให้หากมีเหตุไม่คาดฝันเราจะรู้ตัวและหาทางแก้ไขให้เร็วที่สุด

อันดับที่ 10 A10:2021- Server-Side Request Forgery การปลอมแปลงคำขอฝั่งเซิร์ฟเวอร์ถูกเพิ่มจากแบบสำรวจชุมชน 10 อันดับแรก (#1) ข้อมูลแสดงอัตราการเกิดเหตุการณ์ที่ค่อนข้างต่ำ โดยครอบคลุมการทดสอบสูงกว่าค่าเฉลี่ย พร้อมด้วยคะแนนสูงกว่าค่าเฉลี่ยสำหรับศักยภาพในการใช้ประโยชน์และผลกระทบ หมวดหมู่นี้แสดงถึงสถานการณ์ที่สมาชิกชุมชนด้านความปลอดภัยบอกเราว่าสิ่งนี้สำคัญ แม้ว่ายังไม่ได้แสดงในข้อมูลในขณะนี้

วิธีป้องกัน

ควรแยก server ที่ต้องมีการ fetch ข้อมูลออกไปอยู่ต่าง network เพื่อป้องกันผลกระทบที่อาจเกิดขึ้น และตั้งกฎที่ Firewall ให้เป็น Deny by Default และ Validate ข้อมูลที่ Client กรอกมาก่อนทั้งหมด ไม่ให้กรอก protocol หรือ url แปลกๆ เข้ามา บังคับ URL, port ที่ใช้งานได้ผ่าน Whitelist ที่กำหนดเท่านั้น ห้ามใช้ Blacklist

3.5.2 OWASP Top 10 Mobile

ความเสี่ยงด้านมือถือ 10 อันดับแรกของ OWASP ปี 2024 OWASP Mobile Top 10 มีการเผยแพร่อย่างเป็นทางการในปี 2024 ซึ่งถือเป็นการอัปเดตครั้งใหญ่ครั้งแรกนับตั้งแต่ปี 2016 โดยรายการนี้เน้นย้ำถึงความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุดสำหรับแอปพลิเคชันมือถือ

1. M1: การใช้ข้อมูลประจำตัวที่ไม่เหมาะสม รวมถึงการใช้ข้อมูลประจำตัวที่เข้ารหัสหรือค่าเริ่มต้นอย่างไม่ถูกต้อง
2. M2: ความปลอดภัยของห่วงโซ่อุปทานที่ไม่เพียงพอ หมายถึงความเสี่ยงจากการใช้ส่วนประกอบหรือไลบรารีของบุคคลที่สามที่มีช่องโหว่
3. M3: การตรวจสอบสิทธิ์/การอนุญาตที่ไม่ปลอดภัย คล้ายกับแอปพลิเคชันเว็บ ซึ่งจะครอบคลุมถึงข้อบกพร่องในระบบการตรวจสอบสิทธิ์และการอนุญาตของแอปพลิเคชันมือถือ

4. M4: การตรวจสอบอินพุต/เอาต์พุตไม่เพียงพอ การขาดการตรวจสอบอาจนำไปสู่การโจมตีแบบฉีดยาข้อมูล และช่องโหว่อื่นๆ
5. M5: การสื่อสารที่ไม่ปลอดภัย เกี่ยวข้องกับความล้มเหลวในการเข้ารหัสหรือรักษาความปลอดภัยข้อมูล ระหว่างการส่งอย่าง ถูกต้อง
6. M6: การควบคุมความเป็นส่วนตัวที่ไม่เพียงพอ เกี่ยวข้องกับปัญหาเกี่ยวกับวิธีการรวบรวม จัดเก็บ และใช้ ข้อมูลผู้ใช้
7. M7: การป้องกันไบนารีไม่เพียงพอ หมายถึงช่องโหว่ที่ทำให้สามารถถอดรหัส ดัดแปลง หรือแก้ไขไบนารี ของแอปพลิเคชันได้
8. M8: การกำหนดค่าความปลอดภัยที่ไม่ถูกต้อง หมายความว่าครอบคลุมถึงข้อบกพร่องด้านความปลอดภัย จากการจัดการ การกำหนดค่าที่ไม่ดี
9. M9: การจัดเก็บข้อมูลที่ไม่ปลอดภัย รวมถึงการจัดเก็บข้อมูลที่ละเอียดอ่อนที่ไม่ปลอดภัยบนอุปกรณ์ นั้นเอง
10. M10: การเข้ารหัสที่ไม่เพียงพอ เกี่ยวข้องกับวิธีการเข้ารหัสที่อ่อนแอหรือใช้ไม่ถูกต้อง

Comparison Between 2016-2024		
OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

รูป 3.2 OWASP Top 10 Mobile

(ที่มา: owasp.org)

OWASP Top 10 ได้กลายเป็นมาตรฐานอุตสาหกรรมโดยพฤตินัยสำหรับการระบุและจัดอันดับความเสี่ยงด้านความปลอดภัยในแอปพลิเคชันบนเว็บ จากรายชื่อฉบับปี 2021 ที่เพิ่งเผยแพร่ไป จัดอันดับความเสี่ยงของแอปพลิเคชันเว็บ 10 อันดับ

OWASP Top 10 2021 คือรายชื่อความเสี่ยงด้านความปลอดภัยของแอปพลิเคชันเว็บที่สำคัญที่สุด 10 อันดับแรก รวมถึงการควบคุมการเข้าถึงที่เสียหายและความล้มเหลวในการเข้ารหัส ส่วน OWASP Mobile Top 10 เป็นรายการแยกต่างหากที่เน้นความเสี่ยงเฉพาะของแอปพลิเคชันมือถือ เช่น การจัดเก็บข้อมูลที่ไม่ปลอดภัย และการสื่อสารที่ไม่ปลอดภัย แม้ว่า OWASP Top 10 จะเน้นที่แอปพลิเคชันเว็บ และ Mobile Top 10 จะเน้นที่แอปพลิเคชันมือถือ แต่รายการทั้งสองนี้จัดทำโดยโครงการ Open Web Application Security Project (OWASP) เพื่อช่วยให้นักพัฒนาสร้างซอฟต์แวร์ที่ปลอดภัยยิ่งขึ้น

3.6 การจัดการความเสี่ยงจากภัยคุกคาม

การจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากช่องโหว่ตามมาตรฐาน NIST เป็นแนวทางที่มีโครงสร้างสำหรับการระบุ ประเมิน และแก้ไขจุดอ่อนด้านความปลอดภัยในระบบไอที การปฏิบัติตามแนวทางจากกรอบการทำงานต่างๆ เช่น NIST SP 800-53 และ NIST Cybersecurity Framework (CSF) จะช่วยให้องค์กรต่างๆ สามารถป้องกันระบบเชิงรุก ลดความเสี่ยง และมั่นใจได้ว่าระบบของตนเป็นไปตามกฎระเบียบ การนำ NIST Vulnerability Management มาใช้ถือเป็นสิ่งสำคัญในการรักษาความต่อเนื่องทางธุรกิจ ป้องกันการละเมิด และแสดงความพร้อมด้านความปลอดภัยทางไซเบอร์

3.6.1 การจัดการช่องโหว่ของ NIST คืออะไร?

การจัดการช่องโหว่ของ NIST คือกระบวนการจัดการช่องโหว่ด้านความปลอดภัยในสภาพแวดล้อมไอทีอย่างเป็นระบบ ตามมาตรฐาน NIST ซึ่งประกอบด้วยการระบุช่องโหว่ ประเมินความรุนแรง และดำเนินมาตรการเพื่อบรรเทาหรือกำจัดช่องโหว่เหล่านั้น

ประเด็นสำคัญ ได้แก่

คำจำกัดความ กระบวนการที่มีโครงสร้างตามมาตรฐานสำหรับการจัดการช่องโหว่ในระบบไอที

วัตถุประสงค์ เพื่อลดความเสี่ยง เพิ่มความปลอดภัย และให้เป็นไปตามกฎระเบียบด้านความปลอดภัยทางไซเบอร์

ใครต้องการ องค์กรที่จัดการข้อมูลที่ละเอียดอ่อนหรือระบบที่สำคัญ รวมถึงทั้งหน่วยงานภาครัฐ ภาคเอกชน และผู้ให้บริการด้านไอที

3.6.2 เหตุใดการจัดการช่องโหว่จึงมีความสำคัญ

การจัดการช่องโหว่เชิงรุกเป็นสิ่งสำคัญอย่างยิ่งในการรับมือกับภัยคุกคามทางไซเบอร์ เหตุผลสำคัญ ได้แก่

- **การบรรเทาความเสี่ยงเชิงรุก** ตรวจสอบช่องโหว่ก่อนที่ผู้โจมตีจะสามารถใช้ประโยชน์จากช่องโหว่เหล่านั้นได้
- **การรับรองความสอดคล้องตามกฎหมายหรือเกณฑ์มาตรฐาน** ตอบสนองข้อกำหนดด้านกฎระเบียบ เช่น HIPAA, PCI-DSS และ NIST CSF
- **ลดพื้นผิวการโจมตี** จำกัดจุดเข้าสำหรับอาชญากรทางไซเบอร์โดยการแก้ไขจุดอ่อนของระบบ
- **ความต่อเนื่องทางธุรกิจ** หลีกเลี่ยงการหยุดชะงักที่มีค่าใช้จ่ายสูงซึ่งเกิดจากเหตุการณ์ทางไซเบอร์
- **ความพร้อมในการตรวจสอบ** บำรุงรักษามันที่ความเสี่ยงโดยละเอียดสำหรับกระบวนการปฏิบัติตามข้อกำหนดและการรับรอง

3.6.3 กรอบการจัดการความเสี่ยงของ NIST

กระบวนการจัดการความเสี่ยงจากช่องโหว่ของ NIST ประกอบด้วยกิจกรรมหลัก 6 ประการ

ตาราง 3.2 กระบวนการจัดการความเสี่ยงจากช่องโหว่ของ NIST

(ที่มา: NIST Vulnerability Management Framework)

เฟส	วัตถุประสงค์	การดำเนินการที่สำคัญ
การระบุตัวตน (ID):	ค้นพบช่องโหว่ผ่านการสแกน การตรวจสอบ และการวิเคราะห์ภัยคุกคาม	ใช้เครื่องมือสแกนช่องโหว่และแพลตฟอร์มข้อมูลภัยคุกคามเพื่อระบุข้อบกพร่องด้านความปลอดภัย
การประเมิน (RA):	กำหนดความรุนแรงและผลกระทบของช่องโหว่ที่ระบุ	ใช้ระบบการให้คะแนนตามความเสี่ยง เช่น CVSS เพื่อจัดลำดับความสำคัญของช่องโหว่
การบรรเทาผลกระทบ (PR):	ลดความเสี่ยงด้วยการใช้แพตช์ความปลอดภัย การอัปเดต หรือแนวทางแก้ปัญหา	นำแพตช์ของผู้จำหน่ายและการอัปเดตที่กำหนดค่ามาใช้
การแก้ไข (IR):	แก้ไขช่องโหว่ให้ครบถ้วนเพื่อป้องกันการถูกโจมตี	เปลี่ยนหรืออัปเดตส่วนประกอบที่มีความเสี่ยง หรือปิดการใช้งานระบบที่ได้รับผลกระทบหากจำเป็น

เฟส	วัตถุประสงค์	การดำเนินการที่สำคัญ
การตรวจสอบ (AU):	ตรวจสอบให้แน่ใจว่าการแก้ไขได้รับการดำเนินการอย่างประสบความสำเร็จและรักษาเอกสารไว้	ดำเนินการสแกนติดตามและเก็บบันทึกสำหรับการตรวจสอบ
การตรวจสอบอย่างต่อเนื่อง (DE):	ตรวจสอบระบบเพื่อช่องโหว่และภัยคุกคามใหม่ๆ ที่เกิดขึ้น	ใช้เครื่องมืออัตโนมัติเพื่อการตรวจสอบแบบเรียลไทม์และการแจ้งเตือนเหตุการณ์

3.6.4 วิธีนํ้าการจัดการช่องโหว่ของ NIST ไปใช้

การนำ NIST Vulnerability Management มาใช้ต้องอาศัยแนวทางแบบเป็นระบบและเป็นขั้นตอนดังนี้

- 1) พัฒนานโยบายการจัดการช่องโหว่: กำหนดบทบาท ความรับผิดชอบ และกระบวนการสำหรับการระบุและแก้ไขช่องโหว่
- 2) ดำเนินการตรวจสอบสินทรัพย์ ระบุสินทรัพย์ IT ทั้งหมด รวมถึงเซิร์ฟเวอร์ จุดสิ้นสุด และสภาพแวดล้อมคลาวด์
- 3) ดำเนินการสแกนเป็นประจำ ใช้เครื่องมือสแกนช่องโหว่เพื่อระบุจุดอ่อนในระบบและแอปพลิเคชัน
- 4) จัดลำดับความสำคัญของช่องโหว่ ใช้แนวทางตามความเสี่ยงเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงสูงก่อน
- 5) ใช้แพตช์ความปลอดภัย ติดตั้งแพตช์และอัปเดตที่ผู้จำหน่ายแนะนำทันที
- 6.) ตรวจสอบการแก้ไข ดำเนินการสแกนติดตามเพื่อยืนยันว่าช่องโหว่ได้รับการแก้ไขสำเร็จ
- 7) การดำเนินการเอกสาร บำรุงรักษาทันทีโดยละเอียดของช่องโหว่ ขั้นตอนการแก้ไข และการประเมินความเสี่ยงสำหรับการตรวจสอบ
- 8) ตรวจสอบอย่างต่อเนื่อง ใช้เครื่องมืออัตโนมัติเพื่อตรวจจับช่องโหว่ใหม่ๆ และติดตามการปฏิบัติตามอย่างต่อเนื่อง

3.6.5 แนวทางปฏิบัติที่ดีที่สุดในการจัดการช่องโหว่

หากต้องการเพิ่มประสิทธิภาพสูงสุดของความพยายามในการจัดการช่องโหว่ พึงพิจารณาแนวทางปฏิบัติที่ดีที่สุดต่อไปนี้

- 1) การสแกนและการแพตช์อัตโนมัติ ใช้เครื่องมืออัตโนมัติเพื่อระบุช่องโหว่ จัดการแพตช์ และรายงานการปฏิบัติตามข้อกำหนด
- 2) สร้างกำหนดการจัดการแพตช์ พัฒนากำหนดการปกติสำหรับการใช้แพตช์และอัปเดตซอฟต์แวร์เพื่อลดความเสี่ยง
- 3) กำหนดแนวทางตามความเสี่ยง มุ่งเน้นทรัพยากรในการแก้ไขช่องโหว่ที่ก่อให้เกิดความเสี่ยงสูงสุดต่อระบบที่สำคัญ
- 4) จ้างผู้เชี่ยวชาญด้านความปลอดภัยจากภายนอก ดำเนินการทดสอบการเจาะระบบหรือจ้างที่ปรึกษาความปลอดภัยอิสระเพื่อการประเมินที่เป็นกลาง
- 5) รักษาความพร้อมในการตอบสนองต่อเหตุการณ์ ให้แน่ใจว่ามีแผนในการตอบสนองต่อช่องโหว่ที่สำคัญอย่างรวดเร็ว
- 6) ดำเนินการตรวจสอบและประเมินผลตามปกติ ประเมินประสิทธิภาพของโปรแกรมขององค์กรผ่านการตรวจสอบและอัปเดตเป็นระยะๆ

การนำโปรแกรมจัดการช่องโหว่ที่แข็งแกร่งตามมาตรฐาน NIST มาใช้ถือเป็นสิ่งจำเป็นสำหรับการลดความเสี่ยง การรับรองการปฏิบัติตามข้อกำหนด และการรักษาความต่อเนื่องทางธุรกิจ การปฏิบัติตามแนวปฏิบัติที่ดีที่สุดและการใช้ประโยชน์จากเครื่องมืออัตโนมัติจะช่วยให้องค์กรต่างๆ สามารถจัดการช่องโหว่ ปกป้องระบบ และปฏิบัติตามข้อกำหนดด้านกฎระเบียบได้อย่างมีประสิทธิภาพ

นอกจากนั้น การนำ NIST Vulnerability Management มาใช้แสดงให้เห็นถึงความมุ่งมั่นในการรักษาความปลอดภัยทางไซเบอร์ที่แข็งแกร่ง และสร้างข้อได้เปรียบทางการแข่งขันในภูมิทัศน์ภัยคุกคามในปัจจุบัน การจัดการความเสี่ยงที่เกิดจากช่องโหว่ที่จะส่งผลกระทบต่อทรัพย์สินดิจิทัลขององค์กร จะนำมาใช้ร่วมกันกับมาตรการอื่นๆ ได้แก่ การพิสูจน์ตัวตนจริง

บทวิเคราะห์และมุมมองเชิงวิชาการ: ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์: ช่องโหว่ ภัยคุกคาม มัลแวร์ และความเสียหาย

เนื้อหาในบทนี้ออกแบบให้เป็น “สะพาน” ระหว่างทฤษฎีคลาสสิก (เช่น security models, taxonomy ของภัยคุกคาม) กับแนวปฏิบัติร่วมสมัย เช่น CSF 2.0, SP 800-61r3, CVSS 4.0, EPSS, KEV, SBOM/VEX, และการพิสูจน์ตัวตนแบบ phishing-resistant เพื่อสนับสนุนทั้งผู้สอนและผู้เรียนในการเรียนรู้ที่ “รู้เท่าทันภัย” จริงในสภาพแวดล้อมปัจจุบัน สามารถสรุปสาระสำคัญตามหัวข้อหลักได้ดังนี้

3.1 ช่องโหว่ด้านความมั่นคงปลอดภัยทางไซเบอร์

3.1.1 ความหมายของ “ช่องโหว่”

ช่องโหว่ (vulnerability) คือจุดอ่อน/ข้อบกพร่องในตรรกะเชิงคอมพิวเตอร์/ฮาร์ดแวร์/ซอฟต์แวร์ที่เมื่อถูกบุกรุกโจมตีแล้วส่งผลกระทบต่อ **CIA triad** (Confidentiality, Integrity, Availability) ของระบบและข้อมูล เช่น bug, misconfig, design flaw ตามนิยามของ NIST/NVD และคำอธิบายในคลังศัพท์ CSRC โดยเน้นให้ผู้เรียน “แยกคำ” ให้ชัด: **ช่องโหว่ ≠ ภัยคุกคาม ≠ ความเสี่ยง** เนื่องจากกรอบแนวคิดด้านความเสี่ยงทั้งหมดผูกกับนิยามเหล่านี้อย่างเคร่งครัด (ดู 3.5.3)

3.1.2 ศัพท์ที่เกี่ยวข้องกับภัยคุกคาม

- **Threat (ภัยคุกคาม):** เหตุการณ์/สถานการณ์ที่มีศักยภาพก่อผลกระทบด้านลบต่อภารกิจ ทรัพย์สิน และบุคคล ผ่านระบบสารสนเทศ (รวม DoS, unauthorized access ฯลฯ) (csrc.nist.gov)
- **Risk (ความเสี่ยง):** ฟังก์ชันของ *ผลกระทบ* × *โอกาสเกิด* ต่อองค์กร/บุคคล/ชาติ จากเหตุการณ์ดังกล่าว (csrc.nist.gov)
- **Attack (การโจมตี):** กิจกรรมมุ่งร้ายเพื่อเก็บข้อมูล ครอบงำ ลดทอน ทำลายทรัพยากรสารสนเทศ/ข้อมูล (csrc.nist.gov)
- **Threat Intelligence:** ข้อมูลภัยคุกคามที่ผ่านการวิเคราะห์/ตีความเพื่อใช้ตัดสินใจด้านป้องกัน (csrc.nist.gov)
- **Vulnerability Scanning/Assessment:** การค้นหาและประเมินช่องโหว่เชิงระบบอย่างเป็นระบบ (csrc.nist.gov)

3.2 ภัยคุกคามที่เกิดกับคอมพิวเตอร์

3.2.1 การคุกคาม (Threat)

ภัยคุกคามที่องค์กรเผชิญมีทั้ง **คู่สงครามไซเบอร์/รัฐชาติ**, อาชญากรรมไซเบอร์, insider, และ **ซัพพลายเชน** โดยแนวโน้มร่วมสมัยชี้ว่า **credential-centric attacks**, **social engineering**, และ **exploitation** ของบริการที่เปิดสาธารณะ ยังคงครองสัดส่วนสูง

3.2.2 การโจมตี (Attack)

MITRE ATT&CK เป็นฐานความรู้ TTPs ของผู้โจมตีที่มอง “behavior-centric” ช่วยให้เรียนรู้/ออกแบบ **detection & response** ได้ตาม *tactics* → *techniques* → *procedures* และทำ **mapping** ช่องโหว่/เหตุการณ์เข้ากับ *kill chain* อย่างเป็นระบบ

3.3 พื้นฐานมัลแวร์

3.3.1 ประเภทซอฟต์แวร์อันตราย

ตาม NIST SP 800-83 (Guide to Malware Incident Prevention and Handling) จัดหมวด **ไวรัส/เวิร์ม/โทรจัน/สปายแวร์/แอดแวร์/รูกิต/บ็อตเน็ต/แบ็คดอร์/คริปโตไมเนอร์/ไฟล์เลส** ฯลฯ พร้อมวงจรชีวิต เหตุการณ์มัลแวร์และการตอบสนอง

3.3.2 ไวรัส

ไวรัสแพร่ตัวโดยการแทรกโค้ดไปยังโฮสต์/ไฟล์อื่น ต้องอาศัยการรันของโฮสต์ ต่างจากเวิร์มที่แพร่ตัวเองผ่านเครือข่าย ประเด็นที่เน้น คือ *propagation model*, *infection vector*, และ *signature vs behavior-based detection*

3.3.3 แรนซัมแวร์

ภาพรวมร่วมสมัยชี้ว่า ransomware-as-a-service, double/triple extortion, และการโจมตี supply-chain ยังคงเกิดต่อเนื่อง หน่วยงาน **CISA** บริหารศูนย์ความรู้/แนวทางรับมือ StopRansomware

3.4 การบุกรุก

3.4.1 ผู้บุกรุก

จำแนกเป็น **external, insider (malicious/negligent), third-party/supply-chain**; ศูนย์วิจัย SEI-CERT มี body of knowledge ด้าน insider indicators ที่ใช้ทำเนื้อหาวิชา *security operations & governance*

3.4.2 รูปแบบพฤติกรรมผู้บุกรุก

แนวทาง **Threat-Informed Defense** (โดย MITRE Engenuity/CTID) เน้นการปรับการป้องกันตาม TTPs จริงที่เกี่ยวข้องกับบริบทองค์กร เป็นฐานคิดสำหรับ “detection engineering” และ “continuous validation” เช่น adversary emulation/CALDERA

3.4.3 เทคนิคการบุกรุก

จาก **ATT&CK Enterprise: Initial Access** (phishing, exploit public-facing app, valid accounts), **Execution/Persistence/Defense Evasion** (LOLBins/LOLBAS, fileless), **Credential Access, Lateral Movement, Exfiltration/Impact** ฯลฯ—ใช้เป็นจุดเน้นในการเรียนรู้

3.5 การจัดการความเสี่ยงจากภัยคุกคาม

3.5.1 “การจัดการช่องโหว่ของ NIST” คืออะไร?

มุมมองของ NIST วาง **patch/vulnerability management** เป็น *preventive maintenance* ระดับองค์กร NIST SP 800-40r4 ให้หลักคิดและกระบวนการ *identify → prioritize → acquire → install → verify* ครอบคลุม IT/OT/IoT/Cloud และชี้ให้ทำแผนองค์กรไม่ใช่แค่เครื่องมือ เพื่อ *ลดความเสี่ยงเชิงระบบ*.

3.5.2 เหตุใดการจัดการช่องโหว่จึงสำคัญ

Modern prioritization ต้องให้ลึกซึ้งกว่า *severity-only*:

- **CVSS 4.0** เพิ่มกลุ่ม **Threat & Environmental & Supplemental metrics** ช่วยสะท้อนบริบทจริง มี PoC/active exploitation? reachability? ฯลฯ
- **EPSS (v4 – 2025)** ให้ “โอกาสถูกเอ็กซ์พลอยต์” เชิงสถิติราย CVE สำหรับการจัดลำดับที่ *risk-informed*
- **CISA KEV** คือแค็ตตาล็อก *vulns* ที่มีการโจมตีจริงแล้ว ควรบังคับแก้เป็นลำดับแรก หลอมรวมกับนโยบาย patch SLA

- SBOM + VEX ทำให้รู้ “อะไรอยู่ในระบบเรา” และ “ช่องโหว่นั้นกระทบบริบทการใช้งานจริงหรือไม่” เพื่อตัดงาน “false urgency” และเร่งเคสที่มี *reachability/affectedness*

3.5.3 กรอบการจัดการความเสี่ยงของ NIST

- SP 800-30r1: วิธีทำ *risk assessment* เชิงระบบ (threat-vuln-impact-likelihood)
- Risk Management Framework (SP 800-37r2): รวม *categorize* → *select/implement controls* (SP 800-53) → *assess* → *authorize* → *monitor*. (อ้างอิงใน SP 800-40r4 สำหรับ OT/IoT scope)
- CSF 2.0 (2024): เพิ่ม Function “Govern (GV)” ขั้วเคลื่อน Identify/Protect/Detect/Respond/Recover และเน้น C-SCRM
- Incident Response (SP 800-61r3, 2025): ยกระดับ IR จาก *playbook-centric* เป็น *risk-driven & continuous improvement* ที่เชื่อมกับ CSF 2.0 ตลอดวงจร

3.6 การพิสูจน์ตัวตนจริง (Authentication)

3.6.1 แบบจำลองความปลอดภัย (เพื่อปูพื้นฐานการควบคุมการเข้าถึง)

- Bell-LaPadula (Confidentiality) / Biba (Integrity) / Clark-Wilson ใช้สอน “formal properties” ของนโยบาย — แล้วเชื่อมสู่ RBAC/ABAC เชิงสมัยใหม่ (NIST SP 800-162)

3.6.2 ประเภทการพิสูจน์ตัวตนจริง & มาตรฐานร่วมสมัย

- NIST SP 800-63 (ฉบับ 63-4, 2025): แยก IAL/AAL/FAL, อธิบายชนิดตัวพิสูจน์ (Cryptography, OTP, ฯลฯ) และการจัดระดับความเชื่อมั่นตามความเสี่ยงบริการ
- Phishing-Resistant MFA (FIDO2/WebAuthn/Passkeys): แนวทางที่ CISA/หน่วยงานกลางย้ำว่าเป็นวิธีต่อต้าน *phishing/MiTM* ที่ “ใช้งานได้กว้างที่สุด” ในปัจจุบัน เหมาะเป็นมาตรฐานหลัก สำหรับระบบสำคัญ

3.6.3 แนวทางการนำระบบพิสูจน์ตัวตนจริงไปใช้งาน

1. Risk-based access: กำหนด 1) AAL ตามผลกระทบ เช่น ผู้ดูแล OT = AAL3, 2) Phased rollout: เริ่มจาก **high-value targets & apps** ที่รองรับ FIDO, 3) Federation: ใช้ OIDC/SAML เพื่อขยาย AAL ไปทุกแอป, 4) Passkey UX: จัดการ recovery/roaming ตามแนวทาง FIDO, 5) Telemetry-

driven tuning: ผสาน signals (device binding, geolocation) ปรับ **step-up** อัตโนมัติ (ทั้งหมดสอดคล้อง 800-63-B และ *playbook* ภาครัฐ)

3.2.4 สถานการณ์ภัยคุกคามปัจจุบันและแนวโน้ม

รายงาน **ENISA Threat Landscape** และ **Verizon DBIR** ชี้ต่อเนื่องถึงการยกระดับ social engineering, credential theft, และการโจมตีต่อซัพพลายเชน (supply-chain/API/CI-CD) ควบคู่การเร่ง patch ของ *known exploited* ผ่าน **KEV** ระดับประเทศ/หน่วยงาน; การบูรณาการ **CSF 2.0 + SP 800-61r3** ทำให้องค์กรขยับจาก “ตอบโต้เหตุ” เป็น “บริหารความเสี่ยงเชิงกระบวนการ” มากขึ้น

จุดเน้นที่แนะนำสำหรับการเรียนรู้

1. จาก **severity-only** → **risk-informed**: ใช้ **CVSS 4.0 + EPSS + KEV + Reachability** และ **SBOM/VEX** เป็น baseline ใหม่ของการจัดลำดับงานแก้ไข/บรรเทา
2. จาก **control-centric** → **outcome-centric**: สอน/วัดผลด้วย **CSF 2.0 outcomes** (โดยเฉพาะ *Govern* และ *C-SCRM*) ผูกกับ **IR** ของ **SP 800-61r3** เพื่อสร้าง “วงจรเรียนรู้ถาวร”
3. จาก **signature** → **behavior**: นำ **ATT&CK** และ **Threat-Informed Defense** มาออกแบบ detection engineering ที่ trace-able และทดสอบซ้ำได้
4. จาก **MFA เดิม** → **phishing-resistant**: เร่ง **FIDO2/WebAuthn/Passkeys** เป็นดีฟอลต์อย่างน้อยสำหรับแอป/บทบาทสำคัญ (AAL2/3) พร้อมสื่อสาร UX และ recovery ชัดเจน

3.8 สรุปบท

เอกสารนี้กล่าวถึงรูปแบบของการโจมตีทางคอมพิวเตอร์ทั้งแบบซ่อนเร้นและแบบเผชิญหน้า โดยอธิบายลักษณะและวิธีการของแต่ละประเภท พร้อมยกตัวอย่างเพื่อให้เข้าใจง่ายขึ้น จากนั้นได้กล่าวถึงพื้นฐานของมัลแวร์ซึ่งเป็นภัยคุกคามที่ซับซ้อนต่อระบบคอมพิวเตอร์ โดยแยกประเภทของซอฟต์แวร์ที่เป็นอันตรายและให้แนวทางจำแนกตามลักษณะการทำงานของโปรแกรม สรุปได้ว่าความเข้าใจเกี่ยวกับการโจมตีและมัลแวร์เป็นสิ่งสำคัญสำหรับการปกป้องระบบคอมพิวเตอร์จากภัยคุกคามสมัยใหม่

แนวทางการปฏิบัติเพื่อรักษาความปลอดภัยของคอมพิวเตอร์ที่ใช้ทำงาน เช่น การใช้บัญชีผู้ใช้งานมาตรฐาน และหลีกเลี่ยงการเปิดไฟล์จากแหล่งที่ไม่รู้จัก รวมถึงการเตรียมความพร้อมรับมือและกู้คืนจากการโจมตีด้วยแรนซัมแวร์ เช่น การสำรองข้อมูลและมีแผนการกู้คืนเหตุการณ์ นอกจากนี้ยังอธิบายปัญหาการบูรณาการระบบเครือข่าย

และประเภทของผู้บุกรุกที่อาจสร้างภัยคุกคามต่อความปลอดภัยของระบบ ซึ่งเน้นทั้งมาตรการป้องกันและแนวทางจัดการเมื่อเกิดเหตุการณ์ขึ้น

แนวทางปฏิบัติที่ดีที่สุดในการจัดการช่องโหว่ทางไซเบอร์ โดยเน้นการใช้เครื่องมืออัตโนมัติ กำหนดการแพตช์ และประเมินความเสี่ยง รวมถึงการนำมาตรฐาน NIST มาใช้เพื่อเสริมความมั่นคงปลอดภัยขององค์กร พร้อมทั้งอธิบายความสำคัญของการพิสูจน์ตัวจริง (Authentication) ที่เป็นขั้นตอนพื้นฐานในการควบคุมและตรวจสอบสิทธิ์การเข้าถึงระบบเครือข่าย เพื่อให้มั่นใจว่าผู้ใช้งานได้รับอนุญาตและสามารถปกป้องข้อมูลได้อย่างมีประสิทธิภาพ

ในที่สุด เอกสารนี้กล่าวถึงวิธีการพิสูจน์ตัวจริงในระบบดิจิทัล โดยเน้นการใช้ลายเซ็นดิจิทัลและวิธี zero-knowledge proofs ซึ่งแต่ละวิธีมีจุดเด่นด้านความปลอดภัยและความสามารถในการตรวจสอบการแก้ไขข้อมูล รวมถึงข้อจำกัดด้านความซับซ้อนและเวลาที่ใช้ในการประมวลผล ทั้งนี้การเลือกใช้งานขึ้นอยู่กับความต้องการด้านความปลอดภัยและประสิทธิภาพของระบบ

แบบทดสอบท้ายบท

ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง Threat, Vulnerability และ Attack พร้อมยกตัวอย่าง

แนวคำตอบ: Threat = ความเป็นไปได้ที่จะเกิดอันตราย, Vulnerability = จุดอ่อนในระบบ, Attack = การกระทำที่เจตนาละเมิด เช่น SQL Injection

ข้อ 2. อธิบายการโจมตีแบบ Passive และ Active Attack แตกต่างกันอย่างใด

แนวคำตอบ: Passive = ดักฟัง/วิเคราะห์ทราฟฟิก, Active = เปลี่ยนแปลงข้อมูล/DoS

ข้อ 3. อธิบายลักษณะและกลไกการทำงานของ Ransomware

แนวคำตอบ: เข้ารหัสไฟล์ของเหยื่อ เรียกค่าไถ่เพื่อถอดรหัส แพร่ผ่านอีเมล, ช่องโหว่, มัลแวร์

ข้อ 4. อธิบายความสำคัญของการจัดการช่องโหว่ (Vulnerability Management) ตามแนวทาง NIST

แนวคำตอบ: ลดความเสี่ยงที่ Threat ใช้โจมตีระบบ, ป้องกันการ Exploit, สอดคล้อง Risk Framework

ข้อ 5. วิเคราะห์เหตุการณ์ Phishing Email ต่อผู้ใช้ Mobile Banking ในมุมมอง CIA Triad

แนวคำตอบ: Confidentiality – ข้อมูลรั่ว, Integrity – ข้อมูลถูกแก้ไข, Availability – ระบบอาจถูกใช้ผิดวัตถุประสงค์

ข้อสอบปรนัย 4 ตัวเลือก ก. ข. ค. ง (10 ข้อ พร้อมเฉลย)

ข้อ 1. ข้อใดคือความหมายของ Vulnerability

ก. การโจมตีโดยตรง

ข. จุดอ่อนในระบบที่ถูกใช้ประโยชน์ได้

ค. การสร้างข้อมูลเท็จ

ง. การโจมตีแบบ DoS

เฉลย: ข

ข้อ 2. การเผยแพร่เนื้อหาส่วนตัวไปยังบุคคลที่สาม จัดเป็นการโจมตีใด

ก. Passive Attack

ข. Replay Attack

ค. Masquerade

ง. DoS Attack

เฉลย: ก

ข้อ 3. การทำซ้ำข้อความเก่าเพื่อเข้าถึงระบบใหม่ จัดเป็นการโจมตีแบบใด

ก. Replay Attack

ข. Modification of Message

ค. SQL Injection

ง. Sniffing

เฉลย: ก

ข้อ 4. ข้อใดจัดเป็น Malware ประเภท Trojan Horse

ก. โปรแกรมที่จำลองตัวเอง

ข. โปรแกรมที่ดูเหมือนมีประโยชน์แต่ซ่อนโค้ดอันตราย

ค. โปรแกรมที่คัดลอกไฟล์ตัวเองไปเรื่อยๆ

ง. โปรแกรมที่เข้ารหัสไฟล์เรียกค่าไถ่

เฉลย: ข

ข้อ 5. การโจมตีแบบใดทำให้ระบบหยุดการทำงานชั่วคราวหรือใช้การไม่ได้

ก. Masquerade

ข. DoS/DDoS

ค. Passive Attack

ง. Replay Attack

เฉลย: ข

ข้อ 6. ไวรัสคอมพิวเตอร์มีองค์ประกอบสำคัญข้อใดบ้าง

ก. Infection, Trigger, Payload

ข. Sniffing, DoS, Phishing

ค. Identification, Protection, Recovery

ง. Access Control, Firewall, Audit

เฉลย: ก

ข้อ 7. ข้อใดคือเป้าหมายหลักของ Ransomware

ก. ทำให้ระบบเสียหายชั่วคราว

- ข. ลักลอบขโมยรหัสผ่าน
- ค. เข้ารหัสไฟล์และเรียกค่าไถ่
- ง. ทำการ Replay ข้อความ

เฉลย: ค

ข้อ 8. IDS แตกต่างจาก IPS อย่างไร

- ก. IDS ตรวจจับ, IPS ป้องกันและบล็อก
- ข. IDS เข้ารหัส, IPS ถอดรหัส
- ค. IDS สำรองข้อมูล, IPS พื้นฟูระบบ
- ง. IDS ตรวจสอบสิทธิ์, IPS ยืนยันผู้ใช้

เฉลย: ก

ข้อ 9. ตัวอย่างใดคือการคุกคามประเภท “Interruption”

- ก. การดักฟังอีเมล
- ข. ฮาร์ดดิสก์เสียหายจนเข้าถึงข้อมูลไม่ได้
- ค. การสร้างข้อความเท็จ
- ง. การปลอมเป็นผู้ใช้อื่น

เฉลย: ข

ข้อ 10. มาตรการใดเป็นการป้องกันเบื้องต้นต่อการโจมตีด้วย Phishing

- ก. อัปเดตแพตช์ซอฟต์แวร์
- ข. ใช้การเข้ารหัสไฟล์
- ค. จัดอบรม Security Awareness
- ง. ใช้โปรแกรม Hashing

เฉลย: ค

บรรณานุกรมท้ายบท

ศิระเชษฐ์ โพธิ์ศรีบุญ, ผศ.ดร. (มปป.) เอกสารคำสอน: ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์: ช้องโหว่ ภัยคุกคาม พื้นฐานของมัลแวร์ และความเสี่ยง, รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร. รัตนบุรี.

William Stallings, (2011). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS, fourth edition.

NIST CSF 2.0 (เพิ่ม Function: *Govern*) และคู่มือใช้งาน. ([NIST Technical Series Publications](#))

NIST SP 800-61r3 (Incident Response, 2025) เชื่อม CSF 2.0 และ continuous improvement. ([csrc.nist.gov](#))

NIST SP 800-40r4 (Enterprise Patch/Vuln Mgmt). ([csrc.nist.gov](#))

CVSS 4.0 (FIRST) และการรองรับใน NVD. ([first.org](#))

EPSS v4 (2025) (FIRST) สำหรับ exploit probability. ([first.org](#))

CISA KEV (Known Exploited Vulnerabilities). ([cisa.gov](#))

SBOM/VEX (CISA/NSA joint guidance; CycloneDX/SPDX specs). ([U.S. Department of War](#))

ATT&CK & Threat-Informed Defense (MITRE/CTID). ([attack.mitre.org](#))

Digital Identity (NIST SP 800-63-4/-B) และ Phishing-Resistant MFA (CISA, FIDO Alliance). ([pages.nist.gov](#))

Threat Trends 2025. (ENISA Threat Landscape; Verizon DBIR 2025). ([GitHub](#))

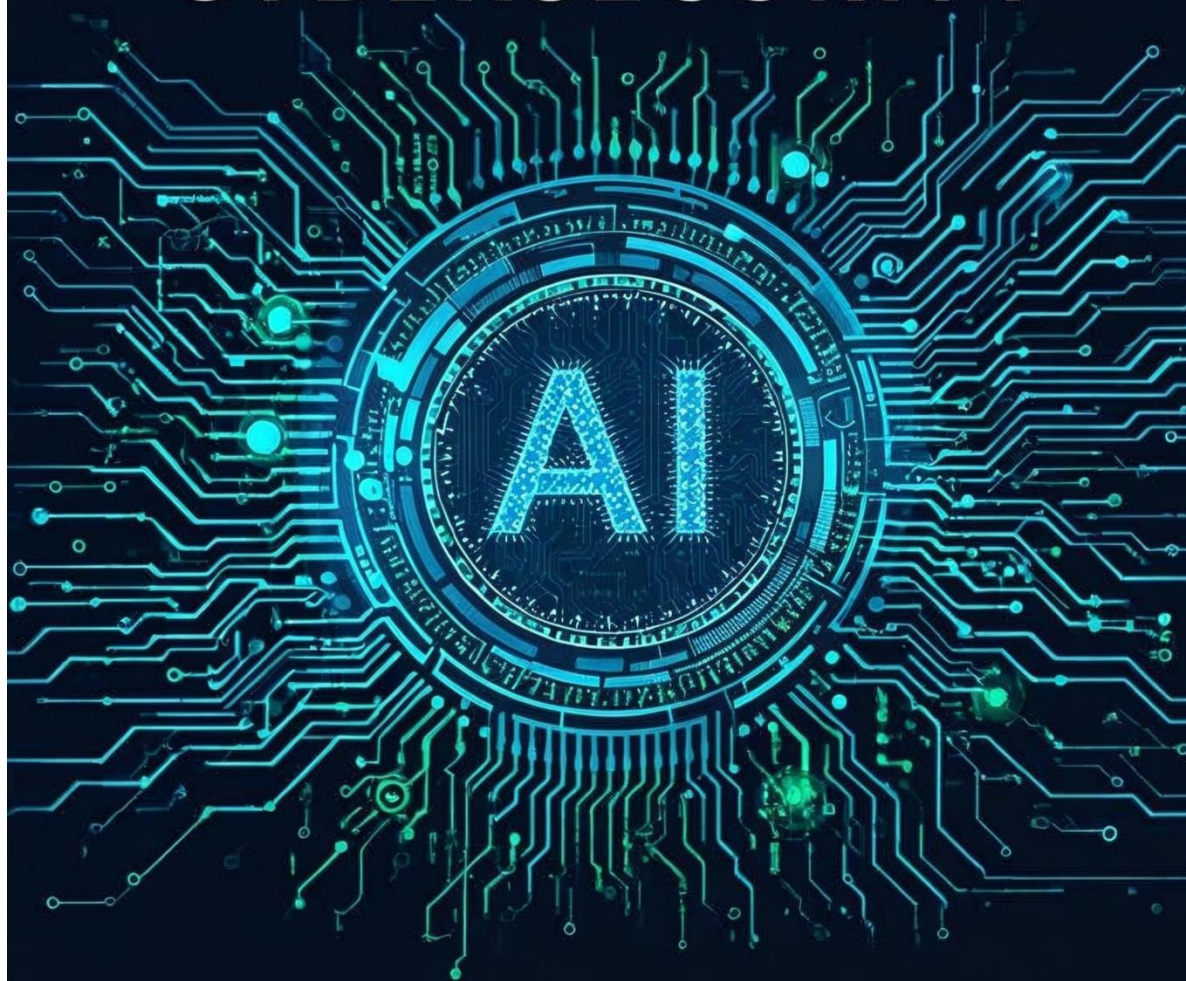
บทที่ 4

การตรวจหาการบุกรุกและการป้องกัน

Intrusion Detection and Prevention System

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์หิรัญ

บทที่ 4 การตรวจหาการบุกรุกและการป้องกัน (Intrusion Detection and Prevention System)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เพื่อให้นักศึกษา

- 1) มีความรู้ความเข้าใจเกี่ยวกับการโจมตีทางไซเบอร์และการตรวจจับการบุกรุก
- 2) เข้าใจหลักการและวิธีการทำงานของ IDS และ IPS
- 3) ออกแบบการใช้ IDS/IPS ในการป้องกันและตอบสนองต่อการโจมตีได้
4. เรียนรู้ผ่านการทำกรณีศึกษาและการปฏิบัติในห้องปฏิบัติการ

2. วัตถุประสงค์เชิงพฤติกรรม

เมื่อสิ้นสุดการเรียนรู้ในสัปดาห์นี้ นักศึกษาจะสามารถ:

- 1) อธิบายรูปแบบและเทคนิคการโจมตีทางไซเบอร์ที่พบบ่อยได้
- 2) อธิบายหลักการทำงานของระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก (IPS) ได้
- 3) แยกแยะความแตกต่างระหว่าง IDS และ IPS ได้อย่างชัดเจน
- 4) วิเคราะห์กรณีการโจมตีและเสนอแนวทางการใช้ IDS/IPS ในการตอบโต้ได้
- 5) นำความรู้ไปปรับใช้กับสถานการณ์จริงในงานด้านความมั่นคงปลอดภัยสารสนเทศได้

3. หัวข้อเนื้อหา:

- 4.1 ระบบตรวจหาการบุกรุก (IDS; Intrusion Detection Systems)
 - 4.1.1 ความหมายของระบบตรวจหาการบุกรุก
 - 4.1.2 ศัพท์ด้านการตรวจหาและป้องกันการบุกรุก
 - 4.1.3 สถาปัตยกรรมของระบบการตรวจหาการบุกรุก (IDS architecture)
 - 4.1.4 แบบจำลองระบบการตรวจหาการบุกรุก (IDS model)

- 4.1.5 เปรียบเทียบวิธีการวิเคราะห์การตรวจหาการบุกรุก
- 4.1.6 ระบบการตรวจหาการบุกรุกแบบกระจาย (dIDS; Distributed IDS)
- 4.1.7 ระบบการตรวจหาการบุกรุกที่ใช้โปรแกรมตัวแทนเคลื่อนที่ (MAIDS; Mobile Agent IDS)
- 4.1.8 โปรแกรมตัวแทนเคลื่อนที่ (Mobile Agent)
- 4.2 ระบบป้องกันการบุกรุก Intrusion Prevention System (IPS)
- 4.2.1 ความหมายของระบบป้องกันการบุกรุก
- 4.2.2 IPS ทำงานอย่างไร
- 4.2.3 ประเภทของ IPS
- 4.3 บทวิเคราะห์เปรียบเทียบระหว่าง IPS กับ IDS
- 4.3.1 วิเคราะห์ลักษณะการทำงาน
- 4.3.2 วิเคราะห์ระบบตรวจหาการบุกรุก (IDS)
- 4.3.3 วิเคราะห์การทำงานของ IPS
- 4.3.4 ข้อดีและข้อเสียของ IPS/IDS
- 4.3.5 การเลือก IPS/IDS ที่เหมาะสม
- 4.3.6 แนวโน้มในอนาคตของ IPS/IDS

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา):

บริษัท RMUTT ThaiCommerce Online ดำเนินธุรกิจ E-Commerce ถูกโจมตีด้วยเทคนิค SQL Injection ผ่านหน้าค้นหาสินค้า

- IDS ตรวจพบ Payload แปลกปลอมใน Query
- IPS พยายามบล็อก Request ที่ผิดปกติ
- Firewall Log แสดง Traffic จำนวนมากจาก IP ซ้ำๆ
- ทีม Incident Response ต้องวิเคราะห์และตอบสนอง

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

- 1) วิเคราะห์การโจมตีที่เกิดขึ้น (SQL Injection) และจัดเป็น Passive หรือ Active Attack
- 2) ระบุบทบาทของ Firewall, IDS และ IPS ในเหตุการณ์นี้
- 3) ประเมินผลกระทบต่อ CIA Triad และ AAA (Authentication, Authorization, Accounting)
- 4) เสนอขั้นตอนการตอบสนองตาม NIST Incident Response Lifecycle
- 5) สรุปเป็นรายงานและนำเสนอในชั้นเรียน

ประเด็นการเรียนรู้ที่แทรก:

- ความแตกต่างระหว่าง IDS และ IPS
- ประเภทของ IDS (Host-based, Network-based) และการตรวจจับ (Signature-based, Anomaly-based)
- หลักการทำงานของ IPS แบบ Inline
- แนวคิด NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover

5. เกณฑ์คะแนน (Rubric 4 ระดับ 100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
ความถูกต้องเชิงวิชาการ (30)	วิเคราะห์ถูกต้อง ครบคลุม IDS/IPS/Firewall	ถูกต้องส่วนใหญ่	ขาดความถูกต้องบางจุด	ขาดความถูกต้องอย่างมาก
การวิเคราะห์ผลกระทบ (25)	เชื่อมโยง CIA + AAA ครบถ้วน	ครบ 70-80%	ครบเพียงบางส่วน	ไม่ชัดเจน

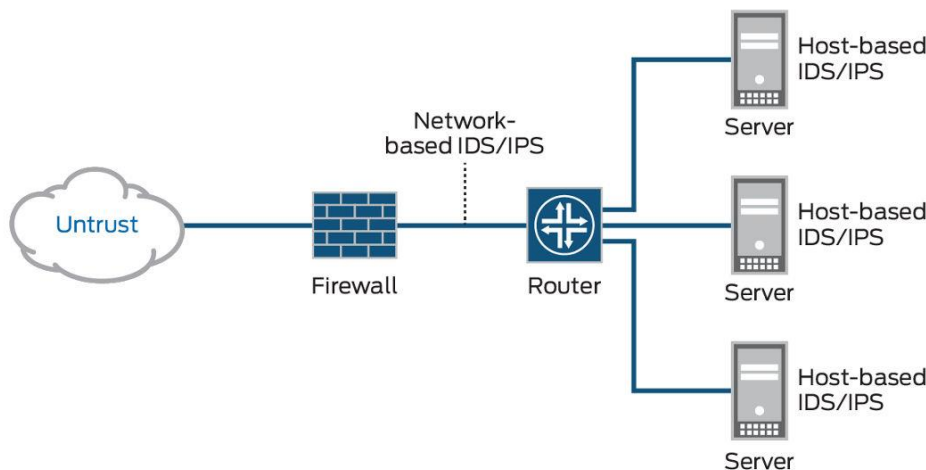
การออกแบบการ ตอบสนอง (30)	เสนอขั้นตอน IR ครอบคลุม ตาม NIST	ครอบคลุม บางส่วน	ไม่สอดคล้องบาง ประเด็น	ไม่ตรงตาม หลักการ
การนำเสนอ (15)	ชัดเจน ใช้แผนภาพ/ตาราง	ชัดเจน	พอใช้	ไม่ชัดเจน

4.1 ระบบตรวจหาการบุกรุก (IDS; Intrusion Detection Systems)

4.1.1 ความหมายของระบบตรวจหาการบุกรุก

เฮดี (Heady) และคณะ (อ้างถึงใน [22]) ได้ให้ความหมายของการบุกรุก (Intrusion) ไว้ว่า การกระทำใดๆ ที่พยายามละเมิดบูรณภาพ, ความลับ และสภาพพร้อมใช้งานของทรัพยากรคอมพิวเตอร์ นิยามนี้มีความสมนัยกับคำว่า ภัยคุกคาม (Threat) ตามนิยามของแอนเดอร์สัน (Anderson) [23] ที่ให้ความหมายไว้ว่า เป็นเจตนาของผู้ซึ่งไม่ได้รับอนุญาตที่พยายามเข้าถึงข้อมูล, แก้ไขข้อมูล หรือกระทำให้ระบบขาดความเชื่อถือได้หรือใช้งานไม่ได้ ในงานวิจัยนี้ จะใช้คำว่า การบุกรุก, ภัยคุกคาม และการโจมตี ในความหมายเดียวกัน

ระบบการตรวจหาการบุกรุก หมายถึง [24] ปัญหาของการระบุอย่างเจาะจงว่าใครคือผู้ใช้ระบบคอมพิวเตอร์โดยปราศจากสิทธิ์ รวมทั้งผู้มีสิทธิ์เข้าถึงอย่างถูกต้องแต่ใช้สิทธิ์นั้นโดยประสงค์ร้าย ระบบการตรวจหาการบุกรุกนี้จึงทำหน้าที่เสมือนยามเฝ้าประตู ทำหน้าที่ตรวจตราคนออก-คนเข้าเครือข่ายตรวจจับและกีดกันไม่ให้มีผู้บุกรุกเข้ามาได้ ดังนั้น เป้าหมายหนึ่งของระบบการตรวจหาการบุกรุกก็คือจำแนกได้อย่างถูกต้องแม่นยำว่ากิจกรรมใดเป็นการบุกรุกจริง และกิจกรรมใด (ที่คล้ายกับการบุกรุกแต่) ไม่ใช่การบุกรุก ปัจจุบัน ระบบการตรวจหาการบุกรุกถูกใช้เป็นเครื่องมือหลักในการตรวจจับและป้องกันทรัพยากรทั้งหมดของระบบคอมพิวเตอร์ในองค์กร ในหลากหลายรูปแบบ อาจจะเป็นอุปกรณ์เฉพาะหรือเป็นเพียงซอฟต์แวร์ที่ติดตั้งลงบนระบบที่ต้องการป้องกันก็ได้



รูป 4.1 IDS/IPS

(ที่มา : www.juniper.net)

แนวคิดเกี่ยวกับระบบการตรวจหาการบุกรุกนี้เกิดขึ้นครั้งแรกโดยเอนเดอร์สัน [23] ตั้งแต่ปี พ.ศ. 2523 และต่อมา ได้รับการปรับปรุงให้กระชับขึ้นโดยเดนนิง (Denning) ว่า เป็นซอฟต์แวร์ซึ่งทำหน้าที่ตรวจหา, ระบุ และโต้ตอบต่อการกระทำใดๆ ที่ไม่ได้รับอนุญาต หรือกิจกรรมที่ผิดปกติบนระบบที่เป็นเป้าหมาย [25] รูป 4.1

โดยทั่วไป เมื่อพิจารณาจากตำแหน่งที่ใช้ในการตรวจหาการบุกรุก ระบบการตรวจหาการบุกรุกแบ่งออกเป็น 2 ประเภท ได้แก่แบบโฮสต์ (host-based) และแบบเครือข่าย (network-based) [26] ระบบการตรวจหาการบุกรุกแบบโฮสต์จะเก็บรวบรวมข้อมูลจากแหล่งภายในซึ่งมักเป็นระดับระบบปฏิบัติการที่คอมพิวเตอร์เครื่องใดเครื่องหนึ่ง โดยมากมักเป็นเครื่องแม่ข่ายให้บริการ โดยจะใช้แฟ้มลงบันทึกเข้าออก (log file) เมื่อผู้ใช้แต่ละคนเริ่มลงบันทึกเข้าสู่ระบบ จากนั้นจะคอยจับตามดูผู้ใช้หรือกระบวนการที่ทำงานในนามผู้ใช้นั้นๆ แล้วรายงานลงในแฟ้มบันทึกเข้าออก วิธีการเช่นนี้ง่ายและมีค่าใช้จ่ายต่ำกว่าการตรวจจับการจราจรบนเครือข่าย แต่การตรวจหาการบุกรุกที่กระทำเฉพาะที่เครื่องใดเครื่องหนึ่งนั้นอาจมองไม่เห็นภาพโดยรวมการโจมตีที่มาจากเครือข่าย โดยเฉพาะอย่างยิ่งการโจมตีแบบการทำให้ใช้การไม่ได้ที่กระจายมาจากแหล่งต่างๆ ไม่ใช่เพียงแหล่งเดียว ประสิทธิภาพจึงด้อยกว่าระบบการตรวจหาการบุกรุกแบบเครือข่าย

ส่วนระบบการตรวจหาการบุกรุกแบบเครือข่าย จะตรวจตราแพ็กเก็ตที่วิ่งผ่านสายสื่อสารเพื่อทำการวิเคราะห์การจราจรเครือข่ายและจำแนกแพ็กเก็ตประสงคร้าย [27] ในระบบจริงมักเป็นอุปกรณ์ที่มีความสามารถในการแปลแต่ละแพ็กเก็ตที่เข้ามา อุปกรณ์นี้จะตรวจจับแพ็กเก็ตของเครือข่ายแล้วนำไปเปรียบเทียบกับแบบอย่าง (Pattern) หรือลายเซ็น (Signature) ของแพ็กเก็ตที่เก็บอยู่ฐานข้อมูลเพื่อจำแนกว่าเป็นแพ็กเก็ตของการโจมตีหรือไม่ อุปกรณ์ของระบบการตรวจหาการบุกรุกแบบเครือข่ายนี้สามารถติดตั้งลงในระบบได้ทันทีโดยไม่จำเป็นต้องปรับแก้ระบบหรือเครือข่ายใดๆ [28] แม้ว่าระบบแบบนี้จะมีประสิทธิภาพดีกว่าแบบโฮสต์ แต่มีค่าใช้จ่ายสูง ประสิทธิภาพในการตรวจหาการบุกรุกที่เกิดขึ้นเฉพาะที่เครื่องใดหนึ่งจะด้อยกว่าแบบโฮสต์

องค์กรระบบความปลอดภัยอินเทอร์เน็ต (ISS; Internet Security Systems) ได้เปรียบเทียบข้อดีและข้อด้อยของการตรวจหาการบุกรุกทั้งสองแบบไว้ใน [29] โดยระบุข้อดีของการตรวจหาการบุกรุกแบบเครือข่ายนั้นได้แก่

มีค่าใช้จ่ายในการเป็นเจ้าของโดยรวมถูกกว่าเพราะการติดตั้งระบบไว้ที่เครือข่ายทำให้การนำไปใช้งานเป็นจริงได้รวดเร็วและมีค่าใช้จ่ายต่ำกว่าการติดตั้งระบบไว้ที่โฮสต์สำคัญแต่ละตัว

สามารถตรวจจับการโจมตีที่หลุดรอดจากการตรวจหาแบบโฮสต์ เพราะระบบไม่ได้พิจารณากระแสการโจมตีที่อาจมาจากโฮสต์อื่นๆ ทั่วเครือข่าย โดยเฉพาะการโจมตีแบบการทำให้ใช้การไม่ได้ (DoS) การพิจารณาเพียงโฮสต์ใดโฮสต์หนึ่งอาจทำให้วิเคราะห์ผิดพลาดได้ง่าย

การหลบหลีกของผู้บุกรุกทำได้โดยยาก เพราะการตรวจหาแบบเครือข่ายจะตรวจจับการโจมตีแบบทันทีทันใด ถึงแม้ว่าผู้บุกรุกจะหายไปแล้ว แต่ระบบยังคงสามารถตรวจหาติดตามร่องรอยและวิธีการโจมตีของผู้บุกรุกได้ ซึ่งแตกต่างจากระบบโฮสต์ที่อาศัยข้อมูลการโจมตีจากแฟ้มลงบันทึกเข้าออก ถ้าผู้บุกรุกที่มีความชำนาญอาจลบหรือแก้ไขข้อมูลในแฟ้มดังกล่าว ก็จะไม่สามารถเห็นร่องรอยการบุกรุกได้

การตรวจหาและการโต้ตอบเป็นไปแบบทันทีทันใด เมื่อเกิดการโจมตีโดยผู้บุกรุก ระบบจะทำการแจ้งเตือนและโต้ตอบแบบทันทีทันใด การตรวจจับและตอบสนองต่อการบุกรุกโดยทันทีทันใดนี้จะช่วยให้ขอบเขตความเสียหายถูกจำกัดไปด้วย

ระบบการตรวจหาการบุกรุกแบบเครือข่ายไม่เพียงเก็บข้อมูลที่เกิดขึ้นเมื่อถูกโจมตีเท่านั้น แต่ยังเก็บข้อมูลการโจมตีที่ไม่สำเร็จและพฤติกรรมที่ไม่น่าไว้วางใจเอาไว้ได้ด้วย ซึ่งเป็นประโยชน์อย่างยิ่งต่อผู้บริหารระบบที่จะนำไปวิเคราะห์, ป้องกัน และใช้เป็นฐานในการปรับแก้นโยบายความปลอดภัยเพื่อรับมือกับการโจมตีในอนาคตได้เป็นอย่างดี

ข้อดีอีกประการหนึ่ง ระบบการตรวจหาการบุกรุกแบบเครือข่ายนั้นเป็นอิสระจากระบบปฏิบัติการ เพราะสามารถติดตั้งระบบนี้ลงบนเครือข่ายโดยปราศจากการปรับแก้ค่ากำหนดต่างๆ ได้ทันที

แม้ว่า ระบบการตรวจหาการบุกรุกแบบโฮสต์นั้นไม่สามารถตรวจจับการบุกรุกทั้งหมดทั่วเครือข่ายได้รวดเร็วกว่าแบบเครือข่าย แต่ก็มีข้อดี อันได้แก่

สามารถทวนสอบความสำเร็จและความล้มเหลวในการโจมตีได้โดยใช้แฟ้มลงบันทึกเข้าออกพิจารณาเหตุการณ์ต่างๆ ที่เกิดขึ้นจริง ซึ่งสามารถนำไปวิเคราะห์ได้ชัดเจนและรวดเร็วกว่าการแจ้งเตือนการบุกรุกของระบบแบบเครือข่าย

การเฝ้าดูกิจกรรมของระบบได้อย่างเฉพาะเจาะจง เพราะระบบนี้จะเฝ้าดูผู้ใช้และกิจกรรมการเข้าถึงแฟ้มต่างๆ รวมทั้งการเรียกใช้, เปลี่ยนแปลงสิทธิการเข้าถึงแฟ้ม, ความพยายามติดตั้งแฟ้มประเภทกระทำไม่ได้ใหม่ๆ ลงไป และ/หรือความพยายามเรียกใช้บริการพิเศษบางอย่าง

สามารถตรวจจับการโจมตีที่หลุดรอดจากระบบการตรวจหาการบุกรุกแบบเครือข่าย ระบบแบบโฮสต์สามารถตรวจจับการโจมตีที่แบบเครือข่ายมองไม่เห็นได้ ตัวอย่างเช่น การโจมตีจากแป้นพิมพ์ที่เครื่องแม่ข่ายสำคัญไม่ได้กระทำข้ามเครือข่ายจึงไม่สามารถถูกตรวจพบได้โดยระบบแบบเครือข่าย

เหมาะสมสำหรับการเข้ารหัสและสภาพแวดล้อมที่ใช้อุปกรณ์สลับสาย ในเครือข่ายขนาดใหญ่ที่ถูกแบ่งออกเป็นเครือข่ายส่วนย่อยๆ หรือเซกเมนต์ การติดตั้งระบบการตรวจหาการบุกรุกแบบเครือข่ายจะถูกติดตั้งไว้ที่แต่ละเซกเมนต์แทนที่จะอาศัยเฉพาะโฮสต์สำคัญ ดังนั้น ส่งผลให้การตรวจจับด้วยประสิทธิภาพสูงสำหรับโฮสต์ใดโฮสต์หนึ่งโดยเฉพาะ อีกทั้งการกำหนดค่าเพื่อควบคุมจะไม่สามารถกระทำได้อย่างละเอียดเพราะเป็นการ

ควบคุมทุกโฮสต์ทั้งเซกเมนต์นั้น แต่การใช้ระบบแบบโฮสต์ที่ติดตั้งลงที่โฮสต์เฉพาะที่สำคัญ ย่อมมีความเหมาะสมต่อการกำหนดค่า และมีประสิทธิภาพดีกว่าการควบคุมทั้งเซกเมนต์ นอกจากนั้น ชีตความสามารถในการตรวจจับการโจมตีที่มาพร้อมกับข้อมูลที่เข้ารหัสไว้ของระบบการตรวจหาแบบเครือข่ายจะมีประสิทธิภาพจำกัดหรือไม่สามารถตรวจหาได้เลย เนื่องจากการไหลเข้ามาที่ละเพ็กเกจของข้อมูลที่เข้ารหัสไว้จะยังไม่ครบถ้วนจนกว่าจะมาถูกถอดรหัสที่โฮสต์ปลายทาง ระบบแบบเครือข่ายจึงไม่สามารถตรวจพบการบุกรุกได้ แต่แบบโฮสต์สามารถทำได้

การตรวจหาและโต้ตอบเกือบทันทีทันใด แม้ว่าระบบแบบโฮสต์จะไม่มีคุณสมบัติของการตรวจหาและโต้ตอบแบบทันทีทันใดเหมือนกับแบบเครือข่ายก็ตาม แต่ระบบการตรวจหาแบบโฮสต์รุ่นใหม่ ๆ ในปัจจุบันก็มีคุณลักษณะใกล้เคียงกับความสามารถดังกล่าว เพราะจะรับการขัดจังหวะจากระบบปฏิบัติการได้ทันทีที่มีแฟ้มลงบันทึกเข้าออกใหม่เข้ามาซึ่งจะสามารถทำงานได้ทันที ส่งผลให้สามารถลดช่วงเวลาของการรู้จำและโต้ตอบลงได้จากเดิมที่จะต้องใช้เวลาานกว่าจะถึงกระบวนการตอบสนอง อย่างไรก็ตาม ความล่าช้าก็ยังคงมีอยู่อันเนื่องมาจากระบบปฏิบัติการต้องใช้เวลาในการบันทึกเหตุการณ์ จากนั้น ระบบการตรวจหาจึงจะเริ่มรู้จำเพื่อเทียบกับฐานข้อมูลแบบอย่าง แม้กระนั้น ในหลายกรณี ผู้บุกรุกก็ถูกตรวจจับและถูกกำจัดได้ก่อนที่จะเกิดความเสียหาย

ไม่จำเป็นต้องใช้ฮาร์ดแวร์เพิ่ม การติดตั้งระบบการตรวจหาการบุกรุกแบบโฮสต์ลงในโครงสร้างพื้นฐานเครือข่ายที่มีอยู่ รวมทั้ง แม่ข่ายแฟ้ม, แม่ข่ายเว็บ และทรัพยากรที่ใช้ร่วมกันชนิดอื่นๆ ได้อย่างอิสระโดยไม่จำเป็นต้องมีอุปกรณ์อื่นๆ เพิ่มเติม ดังนั้น พิจารณาในแง่ราคาต่อประสิทธิภาพแล้ว ระบบนี้มีความคุ้มค่าสูง อีกทั้งยังไม่ต้องการพื้นที่ การซ่อมบำรุง และการจัดการ

ประการสุดท้าย ต้นทุนต่อหน่วยต่ำกว่า ราคาต่อหน่วยของระบบการตรวจหาการบุกรุกแบบโฮสต์นั้นต่ำกว่าแบบเครือข่ายอยู่มาก

กล่าวโดยสรุปแล้ว ระบบการตรวจหาการบุกรุกทั้งแบบโฮสต์และแบบเครือข่ายต่างก็มีทั้งข้อดีและข้อด้อยที่แตกต่างกัน ดังนั้น ระบบการตรวจหาการบุกรุกจึงควรผนวกไว้ด้วยข้อดีของทั้งแบบโฮสต์และแบบเครือข่ายเข้าไว้ด้วยกัน เพื่อเพิ่มประสิทธิภาพในการตรวจหาและป้องกันการโจมตีจากผู้บุกรุก เรียกว่าระบบการตรวจหาการบุกรุกแบบลูกผสม (Hybrid IDS) ปัจจุบัน ยังไม่มีระบบการตรวจหาการบุกรุกแบบใดที่สามารถใช้ในการตรวจหาและป้องกันการโจมตีรูปแบบต่างๆ ได้อย่างสมบูรณ์แบบ การวิจัยในสาขานี้จึงเป็นสิ่งจำเป็นมากยิ่งขึ้น

นอกจากนั้น ในเมื่อระบบการตรวจหาการบุกรุกถูกใช้เป็นเครื่องมือหลักในการตรวจจับและป้องกันทรัพยากรของระบบคอมพิวเตอร์ในองค์กร ระบบการตรวจหาการบุกรุกจึงเป็นเป้าหมายแรกสำหรับผู้บุกรุกจึงมุ่งโจมตี ถ้าสามารถทำให้ระบบการตรวจหาการบุกรุกขัดข้องไปได้ ทรัพยากรทั้งหมดของระบบคอมพิวเตอร์ก็ปราศจากการป้องกัน

อย่างไรก็ตาม เมื่อเราไม่สามารถหลีกเลี่ยงการถูกโจมตีได้ ปัญหาก็คือ ทำอย่างไรเมื่อถูกโจมตีแล้วเรา จะยังสามารถอยู่รอดได้ จะเป็นเช่นนั้นได้เราจะต้องออกแบบระบบการตรวจหาการบุกรุกที่ตั้งอยู่บนพื้นฐานของ สถาปัตยกรรมที่ทนทานและอยู่รอดได้เมื่อถูกโจมตี ด้วยเหตุนี้ การวิจัยเกี่ยวกับการออกแบบสถาปัตยกรรมของ ระบบการตรวจหาการบุกรุกที่ทนทานจึงเป็นความท้าทาย

4.1.2 ศัพท์ด้านการตรวจหาและป้องกันการบุกรุก

ศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์มีศัพท์หลายศัพท์ที่ถูกใช้กันในความหมายที่ยังไม่ สอดคล้องกันนัก เพื่อความเข้าใจที่ตรงกัน ในส่วนนี้จะอธิบายความหมายซึ่งเป็นสาระสำคัญของศัพท์ที่เกี่ยวข้องที่ ปรากฏอยู่ในเอกสารเล่มนี้ ดังต่อไปนี้

ความสามารถในการอยู่รอด (Survivability)

เป็นแนวคิดในการออกแบบระบบที่มีขีดความสามารถในการดำเนินการกิจทั้งหมดต่อไปได้ แม้จะเกิด การโจมตี, ความขัดข้อง หรือเกิดอุบัติเหตุก็ตาม [72] ระบบที่มีความสามารถในการอยู่รอดได้นี้จะมีคุณลักษณะ สำคัญ 3 ประการ [79] ได้แก่ ความทนทาน (resistance) หมายถึงความสามารถในการหลีกเลี่ยงการโจมตีได้, การ รู้จำ (recognition) หมายถึง ความสามารถในการรู้จำรูปแบบการโจมตีและสามารถจำกัดขอบเขตความเสียหายได้ , และการกู้คืนได้ (recovery) หมายถึง ความสามารถในการฟื้นฟูสภาพบริการที่จำเป็นระหว่างการถูกโจมตี และ สามารถกู้คืนบริการทุกอย่างภายหลังการโจมตีได้

การบุกรุก (Intrusion)

การกระทำใดๆ ที่พยายามละเมิดความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของ ทรัพยากรคอมพิวเตอร์

การคุกคาม (Threat)

เป็นเจตนาของผู้ซึ่งไม่ได้รับอนุญาตที่พยายามเข้าถึงข้อมูล, แก้ไขข้อมูล หรือกระทำให้ระบบขาดความ เชื่อถือได้หรือใช้งานไม่ได้

การโจมตี (Attack)

เป็นการกระทำที่มีความตั้งใจให้เกิดเป็นภัยหรืออันตรายต่อระบบคอมพิวเตอร์โดยตรง การโจมตีอาจ กระทำได้ 2 ลักษณะ คือ การโจมตีแบบซ่อนเร้น (Passive attack) เป็นการโจมตีที่ไม่เปิดเผย ตรวจสอบได้ยาก ได้แก่ การเผยแพร่เนื้อหาไปยังบุคคลที่สาม และการวิเคราะห์ทราฟฟิก (Traffic analysis) และการโจมตีแบบ เชี้นำ (Active attack) เป็นการเข้าไปเปลี่ยนแปลงข้อมูลหรือกระทำให้เกิดความเสียหายโดยตรงต่อระบบ คอมพิวเตอร์ ได้แก่ การปลอมตัว (Masquerade) การทำซ้ำ (Replay) การเปลี่ยนข้อมูล และการทำให้ใช้การไม่ได้

ในเอกสารเล่มนี้ จะใช้คำว่า การบุกรุก, การคุกคาม, การโจมตี (Attack), การแฮ็ก (Hacking) การเจาะระบบ และการแคร็ก (Cracking) ในความหมายเดียวกัน

ผู้บุกรุก (Intruder)

บุคคลที่ทำการบุกรุก บางทีใช้คำว่า ผู้โจมตี (Attacker) ทั้งสองคำนี้จะถูกใช้ภายหลังจากการโจมตีเกิดขึ้น นอกจากนั้น ยังมีความหมายสมนัยกับคำว่า แฮ็กเกอร์ (Hacker) นักเจาะระบบ และแคร็กเกอร์ (Cracker) ซึ่งหมายถึงผู้บุกรุกที่เกิดขึ้นก่อนการโจมตีอีกด้วย

อุบัติการณ์ (Incident)

หน่วยรวมของข้อมูลที่ใช้แทนการโจมตีที่เกี่ยวข้องทั้งหมด เช่น โดยผู้โจมตี, ชนิดของการโจมตี, วัตถุประสงค์, ไซต์ หรือช่วงเวลา อุบัติการณ์จึงเป็นสถานการณ์ที่มีความเสี่ยงเกิดขึ้น [78]

ระบบการตรวจหาการบุกรุก (Intrusion detection systems หรือ IDS)

ปัญหาของการระบุอย่างเจาะจงว่าใครคือผู้ใช้ระบบคอมพิวเตอร์โดยปราศจากสิทธิ์ รวมทั้งผู้มีสิทธิ์เข้าถึงอย่างถูกต้องแต่ใช้สิทธิ์นั้นโดยประสงค์ร้าย ระบบการตรวจหาการบุกรุกจึงเป็นซอฟต์แวร์ซึ่งทำหน้าที่ตรวจหา, ระบุ และโต้ตอบต่อการกระทำใดๆ ที่ไม่ได้รับอนุญาต หรือกิจกรรมที่ผิดปกติบนระบบที่เป็นเป้าหมาย

วิธีการวิเคราะห์ (Analysis approach)

วิธีการวิเคราะห์เป็นวิธีที่ระบบการตรวจหาการบุกรุกใช้ในการวิเคราะห์เพื่อตัดสินใจว่ากิจกรรมที่เกิดขึ้นนั้นเป็นการบุกรุกหรือไม่ รายละเอียดเกี่ยวกับวิธีการวิเคราะห์รวมทั้งเปรียบเทียบข้อดีข้อด้อยของวิธีการทั้งสองแบบจะอธิบายไว้ในบทที่ 4 แต่แนวคิดหลักสำหรับการวิเคราะห์ดังกล่าวประกอบด้วย

การตรวจหาลายเซ็นของการโจมตี (Signature-based detection) บางครั้งเรียกว่า การตรวจหาการใช้สิทธิ์โดยมิชอบ (Misuse) โดยการเทียบเคียงแบบอย่างที่เราพบเข้ากับรูปแบบการโจมตีที่รู้จัก

วิธีการนี้รวมทั้งการวิเคราะห์โปรโตคอลแบบแพสซีฟที่ใช้สเนิฟเฟอร์ (Sniffer) ในโหมดผสม (promiscuous mode) นอกจากนั้น ยังรวมถึงการวิเคราะห์ลายเซ็นที่ใช้ตีความชุดของแพ็กเกจ (หรือชิ้นของข้อมูล) ที่บรรจุไว้ในแพ็กเกจเหล่านั้น) ที่จะใช้ตัดสินว่าเป็นการโจมตีหรือไม่

ลายเซ็นการโจมตีดังกล่าวอาจปรากฏอยู่ในรายการบันทึกการตรวจสอบ, แฟ้มลงบันทึกเข้าออก หรือการเปลี่ยนแปลงที่น่าสงสัยในระบบ

การตรวจหาค่าผิดปกติ (Anomaly-base detection) ใช้ในการจำแนกกิจกรรมที่ไม่พึงประสงค์จากพฤติกรรมที่คาดหวังไว้ซึ่งได้กำหนดเอาไว้แล้วล่วงหน้าโดยวิธีสร้างข้อมูลแสดงลักษณะเฉพาะ (Profile) ทั้งแบบอัตโนมัติและไม่อัตโนมัติ ข้อมูลแสดงลักษณะเฉพาะแบบอัตโนมัตินั้นจะถูกสร้างโดยซอฟต์แวร์ที่รวบรวมและ

ประมวลผลคุณลักษณะทั้งหมดของพฤติกรรมที่ควรจะเป็นในแต่ละช่วงเวลาและรูปแบบทั่วไปทางสถิติของพฤติกรรมกลุ่มตัวอย่าง อย่างไรก็ตาม อาจมีพฤติกรรมบางอย่างเกิดขึ้นภายหลังที่ดูอาจเหมือนกับพฤติกรรมน่าสงสัย (แต่ไม่ใช่) ก็สามารถเพิ่มเติมลงไปในรายการพฤติกรรมที่พึงประสงค์ได้ภายหลัง ระบบนี้จะใช้การวิเคราะห์ว่าพฤติกรรมใดที่ผิดไปจากพฤติกรรมที่คาดหวัง อย่างไรก็ตาม ในระบบงานขนาดใหญ่ ย่อมไม่มีทางเป็นไปได้ที่จะสามารถกำหนดพฤติกรรมที่คาดหวังไว้ล่วงหน้าได้ทั้งหมด

ช่องโหว่ (Vulnerability)

เป็นคุณลักษณะอย่างหนึ่งของระบบที่อนุญาตให้ผู้อื่นซึ่งอาจเป็นผู้ประสงค์ร้ายเข้าสู่ระบบได้ ช่องโหว่นี้มีความเสี่ยงสูงต่อการแทรกซึมเข้ามาสู่ระบบได้โดยผู้บุกรุก รู้ว่าดังกล่าวนี้อาจเกิดขึ้นเพราะความบกพร่องของตัวระบบเอง หรืออาจเกิดจากเจตนาของผู้ออกแบบ แต่เมื่อมีช่องโหว่เกิดขึ้นในระบบใดๆ อาจเพิ่มความเสี่ยงต่อการเกิดขึ้นของพฤติกรรมที่ไม่อาจคาดการณ์ได้ที่อาจเป็นอันตรายต่อระบบ

ระบบป้องกันการบุกรุก (Intrusion Prevention System หรือ IPS)

IPS คือระบบที่ทำงานแบบ **real-time** เพื่อตรวจจับ (detect) และ **ป้องกัน (prevent/block)** การโจมตีทางไซเบอร์โดยอัตโนมัติ แตกต่างจาก IDS ที่ทำหน้าที่แจ้งเตือนเพียงอย่างเดียว

การแสวงหาประโยชน์ (Exploit)

กระบวนการใช้ประโยชน์จากช่องโหว่ของระบบเพื่อละเมิดนโยบายความปลอดภัย เครื่องมือหรือวิธีการใดๆ ที่ถูกสร้างขึ้นมาเพื่อใช้ในการละเมิดนโยบายด้านความปลอดภัยมักถูกเรียกว่า บทคำสั่งแสวงหาประโยชน์ (exploit script)

การทำนายผิดเชิงลบ (False negative)

เป็นเหตุการณ์ที่ระบบการตรวจหาการบุกรุกไม่พบว่าการโจมตีต่างๆ ที่เกิดการโจมตี

การทำนายผิดเชิงบวก (False positive)

เป็นเหตุการณ์ที่ระบบการตรวจหาการบุกรุกพบว่าการโจมตีเกิดขึ้น ทั้งๆ ที่ไม่ได้มีการโจมตี (แต่อาจมีพฤติกรรมที่คล้ายการโจมตี)

การโจมตีแบบการทำให้ใช้การไม่ได้ (DoS/DDoS; denial-of-service/Distributed DoS)

โดยทั่วไป การโจมตีแบบการทำให้ใช้การไม่ได้มีพื้นฐานการโจมตีอยู่ 3 ประเภท ประกอบด้วย [8]

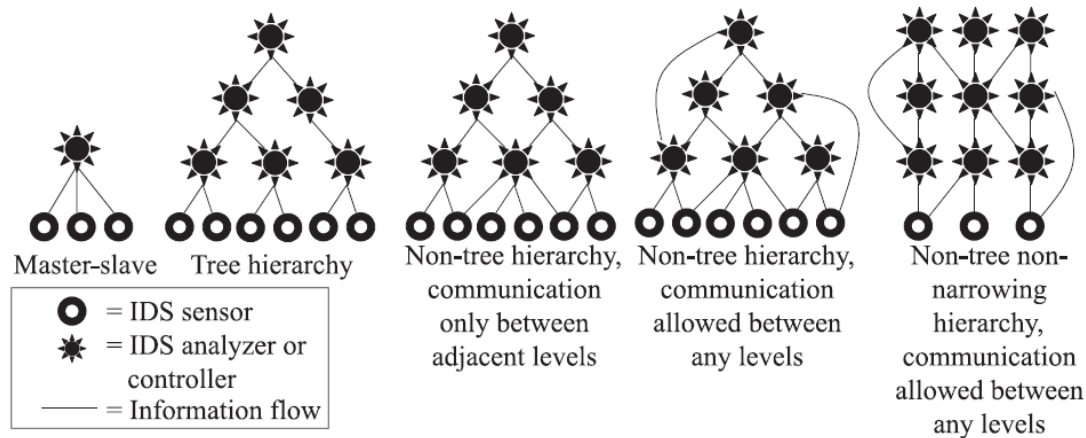
การโจมตีแบนด์วิดท์ (Bandwidth) เป็นการโจมตีเพื่อให้แบนด์วิดท์ของเหยื่อท่วมตันไปด้วย เพื่อก่อกวนประสงคร้ายของผู้โจมตีจนเหยื่อไม่เหลือแบนด์วิดท์พอที่จะรองรับการใช้งานปกติได้ เช่น การโจมตีปิง (PING attack) [9], ยูดีพีฟลัด (UDP flood) [10],

การโจมตีโพรโทคอล (Protocol attack) เป็นการโจมตีข้อบกพร่องของโพรโทคอล เช่น ซิงค์ฟลัด (SYN flood) [11], สเมอร์ฟ (Smerf) [12] และ

การโจมตีจุดอ่อนของซอฟต์แวร์ (Software attack) เช่น ปิงออฟเดธ (Ping of death) [13], เทียร์ดรอพ (Teardrop) [14] ในรายงานที่สำรวจโดยเชิร์ท [5] พบว่า ในปี พ.ศ. 2547 มีจุดอ่อนหรือช่องโหว่ของซอฟต์แวร์ที่ถูกค้นพบประมาณ 3,780 ช่องโหว่ เพิ่มขึ้นเป็น 1.7 เท่าของปี พ.ศ. 2543 ซึ่งมีเพียง 1,090 ช่องโหว่ จากสถิติดังกล่าวแสดงให้เห็นถึงอัตราการเติบโตของการโจมตีที่มีแนวโน้มเพิ่มมากขึ้นทุกปี สาเหตุหนึ่งมาจากปัจจุบันเครื่องมือที่มีประสิทธิภาพหลายชนิดที่จัดเตรียมไว้สำหรับการโจมตีแพร่หลายอยู่บนอินเทอร์เน็ตที่ทุกคนสามารถเข้าถึงโดยไม่เสียค่าใช้จ่ายและนำไปใช้ได้อย่างง่ายดาย เช่น [15], [16], [17], [18], [19] และ [20] เป็นต้น

4.1.3 สถาปัตยกรรมของระบบการตรวจหาการบุกรุก (IDS architecture)

ระบบตรวจหาการบุกรุกมีสถาปัตยกรรมอยู่หลายประเภทมีทั้งโครงสร้างแบบลำดับชั้นรูปต้นไม้ (Tree hierarchy) และแบบไม่เป็นลำดับชั้น (Non-tree hierarchy) ดังแสดงในรูป 4 [30] แต่ระบบการตรวจหาการบุกรุกที่มีอยู่ในปัจจุบันส่วนใหญ่จะมีโครงสร้างและองค์ประกอบที่คล้ายคลึงกัน โดยมีระบบการจัดการที่ใช้สำหรับเฝ้าสังเกต (Monitor), จัดการโครงแบบ (Configuration) และวิเคราะห์ข้อมูลการบุกรุก [31] โดยใช้สถาปัตยกรรมโครงสร้างแบบลำดับชั้น (Hierarchical structure) ที่มีลักษณะพื้นฐานของการแบ่งโครงสร้างออกเป็นลำดับชั้นต่างๆ ดังนี้ [32] ชั้นบนใช้สำหรับการควบคุม, ชั้นกลางเป็นหน่วยสำหรับรวบรวมข้อมูล โดยมีหน่วยตัวรับรู้ (Sensor unit) อยู่ที่บัพใบ (Leaf node) ในชั้นล่าง ชั้นล่างสุดประกอบด้วย มีการไหลของข้อมูลในรูปแบบเดียวกัน ชั้นกลาง ประกอบด้วยการเก็บรวบรวมข้อมูล, การวิเคราะห์ และตรวจหาการบุกรุก ส่วนชั้นบนสุด จะเป็นส่วนต่อประสานผู้ใช้ (User interface)



รูป 4.2 สถาปัตยกรรมชนิดต่างๆ ของระบบการตรวจหาการบุกรุก

ตัวรับรู้ จะทำหน้าที่รวบรวมข้อมูล โดยใช้ข้อมูลที่ได้จากส่วนต่างๆ ของระบบที่สามารถใช้แสดงร่องรอยของการบุกรุก ตัวอย่างเช่น เพ็กเกจเครือข่าย, แฟ้มลงบันทึกเข้าออก, และการตามรอยการเรียกระบบ (System call trace) ตัวรับรู้จะทำการรวบรวมข้อมูลดังกล่าวและส่งต่อไปยังตัววิเคราะห์อีกทอดหนึ่ง

ตัววิเคราะห์ (Analyzer) ทำหน้าที่รับข้อมูลจากตัวรับรู้เพียงตัวใดตัวหนึ่งหรือหลายตัว หรือจากตัววิเคราะห์อื่น จากนั้นจะตัดสินใจว่ามีการบุกรุกเกิดขึ้นหรือไม่ ถ้ามีผลลัพธ์เกิดขึ้นจากส่วนนี้ก็แสดงว่ามีการบุกรุก ผลลัพธ์อาจแสดงถึงรายละเอียดที่สนับสนุนการบุกรุกดังกล่าวด้วย ตัววิเคราะห์อาจกระทำการโต้ตอบการบุกรุกนั้นด้วย

ส่วนต่อประสานผู้ใช้ ส่วนนี้จะสนับสนุนให้ผู้ใช้สามารถมองเห็นผลลัพธ์จากระบบหรือใช้สำหรับควบคุมระบบ ในบางระบบอาจเรียกส่วนนี้ว่า ผู้จัดการ (Manager), ผู้อำนวยการ (Director) หรือส่วนเฝ้าคุม (Console) [61]

ข้อดีของสถาปัตยกรรมแบบนี้ช่วยให้มีประสิทธิภาพในการสื่อสารและมีความสามารถในการขยายระบบได้ แต่ข้อจำกัดก็คือ การสื่อสารระหว่างองค์ประกอบต่างๆ ที่อยู่ระดับเดียวกันนั้นมีความยุ่งยาก มีค่าใช้จ่ายมากกว่าการสื่อสารตามลำดับชั้น และอาจเป็นสาเหตุให้เกิดการท่วมตันเครือข่ายได้

แม้ว่าโดยแนวคิดแล้ว ระบบการตรวจหาการบุกรุกทั้งหมดจะถูกมองเห็นในรูปของตัวรับรู้, ตัววิเคราะห์, ส่วนต่อประสานผู้ใช้ ชนิดของข้อมูลที่ใช้ และชนิดของผลลัพธ์ที่ได้จากระบบจะถือว่ามีความสำคัญมากก็ตาม แต่ระบบการตรวจหาการบุกรุกยังสามารถแบ่งออกตามประเภทของข้อมูล [61] อันได้แก่ แบบโปรแกรมประยุกต์, โฮสต์, เครือข่าย และหลายเครือข่าย/โครงสร้างพื้นฐาน (multi-network/infrastructure)

ระบบการตรวจหาการบุกรุกแบบโปรแกรมประยุกต์ (Application-based IDS) จะใช้วิธีอธิบายพฤติกรรมของโปรแกรมประยุกต์โดยทั่วไปคืออยู่ในรูปของแฟ้มลงบันทึกเข้าออก

ระบบการตรวจหาการบุกรุกแบบโฮสต์ (Host-based IDS) จะใช้วิธีอธิบายข้อมูลอย่างเช่น แฟ้มลงบันทึกเข้าออก, ข้อมูลกระบวนการบัญชีผู้ใช้, พฤติกรรมของผู้ใช้, หรือผลลัพธ์จากระบบการตรวจหาการบุกรุกแบบโปรแกรมประยุกต์ในการทำงานบนโฮสต์นั้นๆ

ระบบการตรวจหาการบุกรุกแบบเครือข่ายจะใช้วิธีอธิบายปริมาณการใช้เครือข่าย โดยอาจเข้าถึงข้อมูลได้จากแบบโฮสต์และแบบโปรแกรมประยุกต์เพื่อทำการตรวจตราภายในสภาพแวดล้อมของเครือข่ายที่ใช้อยู่

ระบบการตรวจหาการบุกรุกแบบหลายเครือข่ายมักทำงานอยู่ในรูปของคณะโต้ตอบอุบัติการณ์ (Incident response team หรือ IRT) โดยที่ได้ข้อมูลของระบบเข้ามาจากไซต์ต่างๆ ตามที่กำหนดไว้ ดังนั้น ระบบการตรวจหาการบุกรุกของไซต์ต่างๆ เหล่านี้จำเป็นต้องมีการติดต่อสื่อสารกัน ซึ่งอาจผ่านทางโปรแกรมประยุกต์, โฮสต์, เครือข่าย หรือระบบการตรวจหาการบุกรุกของเครือข่ายต่างชนิดอื่นๆ

ประเภทของระบบการตรวจหาการบุกรุกดังกล่าว สามารถมองดูในรูปของโครงสร้างแบบลำดับขั้นก็ได้ โดยที่ส่วนบนสุดของโครงสร้างจะเริ่มจากแบบต่างเครือข่าย และส่วนล่างสุดได้แก่แบบโปรแกรมประยุกต์

แต่ละจุดของระบบการตรวจหาการบุกรุกในสถาปัตยกรรมแบบลำดับขั้นนี้ สามารถรับข้อมูลจากองค์ประกอบระดับใดๆ ที่ต่ำกว่าหรือจากระดับเดียวกันก็ได้ (ในกรณีของตัวรับรู้) ส่วนผลลัพธ์ที่ได้สามารถได้จากองค์ประกอบที่อยู่ระดับเดียวกันหรือสูงกว่าได้

4.1.4 แบบจำลองระบบการตรวจหาการบุกรุก (IDS model)

แบบจำลองของระบบการตรวจหาการบุกรุกเป็นวิธีการที่ระบบใช้ในการตรวจหาการบุกรุก โดยพื้นฐานจะมีแบบจำลองที่ใช้วิธีการอยู่ 2 วิธี ได้แก่ [33] การตรวจหาการใช้สิทธิ์โดยมิชอบ (Misuse) และการตรวจหาค่าผิดปกติ (Anomaly)

แบบจำลองการตรวจหาการใช้สิทธิ์โดยมิชอบ (Misuse detection model) เป็นวิธีการที่ใช้ในยุคเริ่มต้นของระบบการตรวจหาการบุกรุก การตรวจหาจะทำการค้นหาการใช้ประโยชน์จากช่องโหว่ที่มีอยู่ในระบบซึ่งมักมีรูปแบบที่แน่นอนโดยอาจเป็นกลุ่มของเหตุการณ์ที่เกิดขึ้นโดยลำดับหรือเป็นลายเซ็นของการบุกรุก ตัวอย่างวิธีการตรวจหาการใช้สิทธิ์โดยมิชอบได้แก่ IDES ของ ที เอฟ ลันท์ ซึ่งเป็นระบบผู้เชี่ยวชาญ (Expert system) [34], วิธีการแบบจำลองของที ดี การ์เวย์ (Model-based approach) [35], การวิเคราะห์การเปลี่ยนสถานะ (State transition analysis) ที่เรียกว่า STAT ของฟิลิป [36], Korn shell ของมอริสที่ใช้วิธีการเฝ้าสังเกตจังหวะการกดแป้นพิมพ์ (keystroke monitoring) [37] และ ASAX ที่ใช้การจับคู่แบบอย่าง (Pattern matching) [38]

ข้อดีของระบบการตรวจหาการบุกรุกที่ใช้แบบจำลองการตรวจหาการใช้สิทธิ์โดยมิชอบก็คือ สามารถตรวจหาการบุกรุกได้อย่างมีประสิทธิภาพ แต่ขาดความสามารถในการรู้จักการบุกรุกรูปแบบใหม่ๆ ในอนาคต

แบบจำลองการตรวจหาค่าผิดปกติ (Anomaly detection model) ทำงานโดยตรวจหารูปแบบหรือพฤติกรรมที่ผิดปกติในการใช้ประโยชน์จากระบบ โดยอาจใช้วิธีการทางสถิติ [39], การสร้างแบบอย่างการทำนาย [40], การใช้โครงข่ายประสาท (Neural network) [41] และการเรียนรู้อุปนิสัยหลักเกณฑ์ [42]

ข้อดีของระบบการตรวจหาการบุกรุกที่ใช้แบบจำลองการตรวจหาค่าผิดปกตินี้ก็คือ สามารถตรวจพบการบุกรุกรูปแบบใหม่ๆ ได้ แต่อย่างไรก็ตาม ข้อด้อยของวิธีนี้คือมีค่าใช้จ่ายในการคำนวณสูง และอาจเป็นไปได้ที่จะแจ้งเตือนผิดพลาดได้

อันเนื่องมาจากระบบการตรวจหาการบุกรุกแบบโฮสต์นั้นสามารถตรวจตราและรายงานพฤติกรรมที่ไม่น่าไว้วางใจเฉพาะเครื่องคอมพิวเตอร์เพียงเครื่องใดเครื่องหนึ่งเท่านั้น ในขณะที่การตรวจหาแบบเครือข่ายสามารถเฝ้าสังเกตและรายงานเฉพาะที่ในแต่ละส่วนของเครือข่าย กระนั้นก็ตาม ผู้โจมตียังคงสามารถใช้ข้อจำกัดนี้เพื่อหลบซ่อนพฤติกรรมจากการถูกตรวจจับได้หลายวิธี (เช่น การสแกนพอร์ตหรือเครือข่ายแบบไม่ต่อเนื่อง หรือการสแกนไอพีเพียงครั้งเดียว เป็นต้น) วิธีการเช่นนี้ล้วนเพิ่มความยากลำบากในการตรวจพบทั้งโดยระบบการตรวจหาและโดยผู้บริหารระบบก็ตาม

นอกจากนั้น ระบบการตรวจหาการบุกรุกส่วนใหญ่จะตรวจหาการโจมตีโดยใช้การวิเคราะห์ข้อมูลจากโฮสต์ใดโฮสต์หนึ่ง หรือส่วนหนึ่งของเครือข่ายโดยปราศจากการสื่อสารหรือแลกเปลี่ยนข้อมูลระหว่างกันกับระบบการตรวจหาอื่นๆ ดังนั้น จึงขาดความสามารถในการตรวจหาการโจมตีแบบกระจายบนระบบเครือข่ายขนาดใหญ่ได้

4.1.5 เปรียบเทียบวิธีการวิเคราะห์การตรวจหาการบุกรุก

เนื้อหาในข้อที่ 4.4 ได้อธิบายถึงวิธีการวิเคราะห์เพื่อจำแนกว่าเป็นการบุกรุกหรือไม่ รวมทั้งสรุปข้อดีข้อด้อยของวิธีการทั้งสองแบบไปแล้ว ในหัวข้อนี้จะเปรียบเทียบถึงคุณลักษณะสำคัญอื่นๆ ของวิธีการทั้งสองที่ควรพิจารณา ได้แก่ ความรู้ ความง่ายในการใช้งาน ข้อมูลรายงาน และความถูกต้องของการรายงาน

1) ความรู้ ในการตรวจหาการบุกรุกจำเป็นต้องมีความรู้ไม่ว่าจะเป็นรูปแบบที่เป็นไปได้ต่างๆ ของการบุกรุกหรือความรู้เกี่ยวกับพฤติกรรมที่คาดหวังได้ของระบบก็ตาม สำหรับวิธีการตรวจหาการโจมตีทุกชนิดแบบลายเซ็นนั้น ระบบจะต้องรู้จักการโจมตีทุกรูปแบบไว้ก่อน ระบบการตรวจหาการบุกรุกจะต้องทำการรู้จำไม่ว่าจะเป็นรายละเอียดของการโจมตีหรือแบบอย่างในระดับนามธรรมที่แสดงคุณลักษณะของการโจมตีแต่ละประเภทไว้ ส่วนระบบแบบการตรวจหาค่าผิดปกตินั้น จำเป็นต้องรู้พฤติกรรมทั้งหมดของระบบที่ทำงานอยู่เพื่อใช้ในการจำแนกการโจมตีทุกชนิด ซึ่งไม่มีทางเป็นไปได้ในความเป็นจริง

2) ความง่ายในการกำหนดค่าโครงสร้าง คุณลักษณะอีกประการหนึ่งที่พึงพิจารณา คือ ความง่ายในการใช้งานหรือการกำหนดค่าโครงสร้าง โดยทั่วไป ระบบแบบลายเซ็นต้องการความรู้ในการกำหนดค่าต่างน้อยกว่าแบบการตรวจหาค่าผิดพลาด โดยเพียงแต่รวบรวมข้อมูลเพิ่มเติมในภายหลัง, วิเคราะห์ และปรับปรุงข้อมูลให้เป็นปัจจุบันอยู่เสมอ บางระบบอนุญาตให้สามารถสร้างแฟ้มลายเซ็นเป็นของตัวเองได้ ซึ่งส่งผลให้เพิ่มความซับซ้อนในการกำหนดค่าต่างๆ ในโครงสร้างเพิ่มมากขึ้น

ส่วนระบบแบบตรวจหาค่าผิดพลาด โดยปกติมักมีความซับซ้อนและยุ่งยากในการกำหนดค่าโครงสร้างเพื่อรู้จักพฤติกรรมของการบุกรุกในรูปแบบต่างๆ มากกว่าแบบลายเซ็นอยู่แล้ว ด้วยเหตุนี้ ยิ่งทำให้ความจำเป็นในการตรวจค้นผู้ใช้, ทำความเข้าใจ, การแทนที่ และการบำรุงรักษาพฤติกรรมที่คาดหวังได้ในระบบที่ทำงานอยู่ยิ่งมีมากขึ้น ในหลายกรณีอาจมีการจัดเตรียมเครื่องมือสนับสนุนแบบอัตโนมัติไว้ แต่ก็ต้องใช้เวลาพอสมควรในการพัฒนาและข้อมูลที่มีอยู่อาจไม่ชัดเจนเพียงพอ

3) ข้อมูลรายงาน ระบบการตรวจหาการบุกรุกแบบลายเซ็นจะสร้างรายงานจากข้อมูลพื้นฐานที่ได้จากการจับคู่ลายเซ็นที่ตรวจพบกับลายเซ็นที่เก็บอยู่ในฐานข้อมูล รายงานผลลัพธ์จึงสามารถแปรผันไปตามข่าวสารแจ้งเตือนว่ามีการตรวจพบการบุกรุกเกิดขึ้น หรือแม้กระทั่งข้อมูลที่ใกล้เคียงกับลายเซ็นของการบุกรุก

ส่วนผลลัพธ์ที่ได้จากระบบการตรวจหาการบุกรุกแบบตรวจหาค่าผิดพลาดจะสร้างรายงานแบบค่าสหสัมพันธ์เชิงสถิติระหว่างพฤติกรรมที่เกิดขึ้นจริงกับพฤติกรรมที่คาดหวังของระบบ นอกจากนั้น ระบบยังคอยตรวจตราพฤติกรรมที่น่าสงสัยบางอย่างที่เกิดขึ้นนอกเหนือไปจากพฤติกรรมที่คาดหวัง และสร้างรายงานออกมา

4) ความถูกต้องของการรายงาน ทั้งแบบอย่างของลายเซ็นที่ไม่ได้กำหนดไว้และข้อมูลแสดงลักษณะเฉพาะของค่าผิดพลาดซึ่งยังไม่เพียงพอที่จะจำแนกได้ชัดเจนว่าเป็นการโจมตีของผู้ประสงค์ร้ายหรือไม่ ข้อมูลเหล่านี้จะถูกสร้างเป็นผลลัพธ์อยู่ในรายงานการแจ้งเตือน ดังนั้น ระบบการตรวจหาการบุกรุกทั้งสองแบบจึงยังคงมีโอกาที่จะสร้างผลการทำนายผิดพลาดทั้งแบบเชิงบวกและเชิงลบออกมาอยู่ในปริมาณมาก

ดังนั้น จึงขึ้นอยู่กับสภาพแวดล้อมที่ระบบการตรวจหาการบุกรุกที่ใช้อยู่เน้นว่าใช้วิธีการใด (ลายเซ็นหรือตรวจหาค่าผิดพลาด) และเป็นแบบใด (โปรแกรมประยุกต์, โฮสต์, เครือข่าย หรือแบบหลายเครือข่าย) เพื่อที่จะสามารถใช้ในการแก้ปัญหาได้อย่างเหมาะสม ระบบแบบลายเซ็นจะไม่สามารถตรวจพบการบุกรุกทุกกรณีที่เป็นไปได้ด้วยข้อจำกัดของการตรวจหาตามสภาพจริง, ความคงที่และต่อเนื่องในการปรากฏตัวของการโจมตีและการแสวงหาประโยชน์, ช่องโหว่ใหม่ๆ ที่เกิดขึ้น รวมทั้งการใช้บทคำสั่งแสวงหาประโยชน์ใหม่ๆ ย่อมเกิดขึ้นได้เสมอ

ข้อดีของระบบการตรวจหาการบุกรุกแบบตรวจหาค่าผิดพลาดก็คือ มีขีดความสามารถในการตรวจพบการโจมตีรูปแบบใหม่ที่ไม่อาจถูกตรวจจับได้โดยแบบลายเซ็น เนื่องจากการโจมตีทุกชนิดสามารถถูกวิเคราะห์ได้โดยบุคคลที่เป็นผู้บริหารระบบโดยการนิยามการโจมตีไว้ให้รัดกุม ดังนั้น การใช้การผสมผสานกันทั้งวิธีการแบบ

ลายเซ็นและแบบตรวจหาค่าผิดพลาดมีขีดความสามารถในการรับมือกับการโจมตีรูปแบบต่างๆ ได้อย่างครอบคลุมและหลากหลาย โดยต้องทำการปรับระบบฐานข้อมูลลายเซ็นให้มีความเป็นปัจจุบันอยู่เสมอ

นอกจากนั้น บริเนีย (Andrew L. Briney) [67] และคณะนักวิจัยด้านระบบความปลอดภัยหลายคน แห่งสถาบันแซนส์ (SANS Institute) ได้แก่ ซูเวอร์ (Robert Zuver) [21], วินเคเลอร์ (Robert, Winkler) [63], เยน (Ho, Swee Yenn) [64], บูรน์วาร์ (Guy Bruneau) [65] และ โกลเดนิตซ์ (Thomas Goeldenitz) [66] ซึ่ง ทำการศึกษาเกี่ยวระบบการตรวจหาการบุกรุกปัจจุบันและอนาคต ได้มีความเห็นสอดคล้องกันว่า ระบบการ ตรวจหาการบุกรุกที่มีอยู่ในปัจจุบันนั้นยังห่างไกลจากความสมบูรณ์ในความสามารถที่จะวิเคราะห์และโต้ตอบการ โจมตีที่มีอยู่ในปัจจุบันได้ ระบบการตรวจหาในอนาคตนั้นควรมีคุณลักษณะที่พึงประสงค์เพิ่มเติมได้แก่ ความ ทนทาน, ความยืดหยุ่นและการปรับขนาดได้ และความง่ายในการใช้งาน

5) ความทนทาน (Robust) ระบบการตรวจหาการบุกรุกทำงานอย่างต่อเนื่องในเบื้องหลังโดยไม่ จำเป็นต้องให้คนเข้าไปเกี่ยวข้องได้ ดังนั้น ระบบนี้จึงควรทนทานต่อภาวะผิดพลาด หมายความว่า ถ้าถ้าระบบเกิด การล้มเหลวหรือขัดข้องขึ้นมา ก็สามารถฟื้นฟูสภาพขึ้นใหม่โดยไม่จำเป็นต้องต้องสร้างหรือเริ่มปรับเปลี่ยนค่ากำหนด โครงแบบกันใหม่ ระบบควรยังคงสามารถต้านทานต่อการโจมตีได้เหมือนเดิม

6) ความยืดหยุ่นและการปรับขนาดได้ ระบบตรวจหาการบุกรุกควรสามารถปรับเปลี่ยนค่ากำหนด และมีความยืดหยุ่นพอในการตอบสนองต่อความเปลี่ยนแปลงบนสภาพแวดล้อมของเครือข่าย ระบบควรมี ความสามารถในการตรวจหาการบุกรุกได้แม้ภายใต้ปริมาณการจราจรเครือข่ายที่เติบโตมากขึ้น โดยยังคงมี ประสิทธิภาพที่ถูกต้อง เพียงตรงเหมือนเดิม

7) ความง่ายในการใช้งาน การบริหารจัดการระบบตรวจหาการบุกรุกไม่ควรใช้แบบตัววิธีอย่าง สิ้นเปลือง หรือมีค่าใช้จ่ายอื่นๆสำหรับดำเนินการ ควรมีความพอดีระหว่างความง่ายต่อการใช้งานกับประสิทธิภาพ ของระบบ ในสภาพการณ์จริง ระบบตรวจหาการบุกรุกก็ยังจำเป็นต้องพิจารณาในด้านทรัพยากรที่ใช้ในการจัดการ และการควบคุมอุปกรณ์ต่างๆ

4.1.6 ระบบการตรวจหาการบุกรุกแบบกระจาย (diIDS; Distributed IDS)

ด้วยข้อจำกัดดังกล่าวของระบบการตรวจหาการบุกรุกแบบเดิมดังที่อธิบายไว้ในหัวข้อ 4.4 และ 4.5 จึงมีแนวคิดที่จะพัฒนาระบบการตรวจหาแนวใหม่เรียกว่า ระบบการตรวจหาการบุกรุกแบบกระจาย หรือบางที เรียกว่า ระบบการตรวจหาการบุกรุกแบบเอกฉันท์ (Consensus IDS) [43] ระบบนี้จะพยายามแบ่งปันข้อมูลของ ตนแก่ระบบอื่นๆ โดยติดตั้งระบบการตรวจหากระจายไปยังหลายแห่งของเครือข่ายขนาดใหญ่ รวมทั้งระบบการ ตรวจหาที่ติดตั้งอยู่บนเครือข่ายเพื่อนบ้านอีกด้วย จากนั้น จึงส่งข้อมูลการตรวจหาของตนไปยังเครื่องแม่ข่ายกลาง ซึ่งจะสามารถมองเห็นภาพรวมของการโจมตีหรือการบุกรุกที่เกิดขึ้นจากโฮสต์ต่างๆ ได้ เนื่องจากอาจเกิดขึ้นที่โฮสต์

โดโฮสต์หนึ่งเท่านั้น วิธีการเช่นนี้จะสามารถใช้ในการตรวจตราเครือข่ายขนาดใหญ่, วิเคราะห์อุบัติการณ์ และข้อมูลการโจมตีโดยรวมได้อย่างแม่นยำ [44]

ระบบการตรวจหาการบุกรุกแบบกระจายเดิมเรียกว่า ระบบการตรวจหาเบื้องต้น (Meta-IDS) [45] ทำหน้าที่ในการรวบรวมข้อมูลจากระบบการตรวจหาตัวอื่นๆ แล้วนำมาเชื่อมโยงว่ามีการโจมตีหรือไม่และจากแหล่งใด จากนั้นนำมาวิเคราะห์รูปแบบเพื่อกำหนดวิธีการรับมือหรือบรรเทาการโจมตีบนอินเทอร์เน็ตโดยรวมได้ เพราะโดยสถิติของการโจมตีที่เคยเกิดขึ้นบนอินเทอร์เน็ตนั้น การโจมตีจะมาจากหลายแหล่งโดยมีเป้าหมายไปที่เหยื่อรายเดียวกัน การตรวจหาการโจมตีจากแหล่งใดแหล่งหนึ่งจึงยังไม่เพียงพอที่จะรับมือกับการโจมตีแบบกระจายนี้ได้ ระบบการตรวจหาการบุกรุกแบบกระจายจึงเป็นความหวังใหม่ของการป้องกันภัยที่อาจใช้เป็นเครื่องมือป้องกันการโจมตีบนอินเทอร์เน็ตได้ทั้งหมด และเป็นความท้าทายใหม่ๆ ของการวิจัยในสาขานี้

ปัจจุบัน มีผลิตภัณฑ์ระบบการตรวจหาการบุกรุกแบบกระจายออกสู่ท้องตลาด อย่างเช่น Internet Storm Center [46], DShield [47], MyNetWatchman [48], DeScan [49] และ DeepSight™ ของไซแมนเทค [50] เป็นต้น รวมทั้งเป็นแนวทางใหม่ของงานวิจัยสาขานี้

4.1.7 ระบบการตรวจหาการบุกรุกที่ใช้โปรแกรมตัวแทนเคลื่อนที่ (MAIDS; Mobile Agent IDS)

โปรแกรมตัวแทน (Agent) ถูกเรียกใช้ในหลายคำ ได้แก่ ซอฟต์แวร์อิสระ (Software agent) โปรแกรมตัวแทนอิสระ (Autonomous agent) หรือโปรแกรมตัวแทนเคลื่อนที่ (Mobile agent) หมายถึง โปรแกรมที่ดำเนินอยู่ (รวมทั้งรหัสและข้อมูล) ที่สามารถท่องเที่ยวจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งในเครือข่ายได้ สามารถกระทำการกิจในฐานะตัวแทน อย่างเช่น การรวบรวมข้อมูล จากนั้น ก็นำผลลัพธ์กลับคืนมา [51] โปรแกรมตัวแทนอาจได้รับมอบหมายให้ทำการกิจอย่างเฉพาะเจาะจงเพียงอย่างเดียวอย่างหนึ่ง หรือภารกิจที่ซับซ้อนมากก็ได้ เนื่องจากเป็นโปรแกรมที่มีความเป็นอิสระที่สามารถเคลื่อนย้ายจากโหนดหนึ่งไปยังโหนดหนึ่งในระบบกระจายได้ด้วยตัวเอง ที่มีชื่อว่าโปรแกรมตัวแทนอิสระก็ด้วยเหตุนี้เอง

โปรแกรมตัวแทนเคลื่อนที่ ประกอบด้วยส่วนสำคัญ 3 ส่วน [52] ได้แก่ **ส่วนทรัพยากร** ประกอบด้วยทรัพยากรฮาร์ดแวร์ สภาพแวดล้อมในการคำนวณ และค่าแฮชที่ถูกเข้ารหัส **ส่วนฟังก์ชัน** ประกอบด้วย มอดูลควบคุม, มอดูลสื่อสาร และเมทอด (Method) และ **ข้อมูลเกี่ยวกับหลักเกณฑ์**

การนำเทคโนโลยีของโปรแกรมตัวแทนเคลื่อนที่ไปใช้ในระบบการตรวจหาการบุกรุกถือเป็นแนวคิดใหม่สำหรับวงการ แนวคิดแรกเริ่มที่เสนอการใช้โปรแกรมตัวแทนในการสร้างระบบการตรวจหาการบุกรุกได้แก่ ครอสบี ในปี พ.ศ. 2537 [53] ในต้นฉบับที่เขาเสนอแนะนั้น โปรแกรมตัวแทนควรถูกสร้างอย่างเจาะจงเพื่อมอบหมายภารกิจโดยใช้เทคนิคของปัญญาประดิษฐ์ (การโปรแกรมเชิงพันธุกรรม) ต่อมา AAFID [54] จึงถูก

นำเสนอในปี 2541 โดยคณะนักวิจัยแห่งมหาวิทยาลัยเพอร์ดูว (Purdue university) โดยจัดโปรแกรมตัวแทนทั้งหมดให้อยู่ในโครงสร้างแบบลำดับชั้น และให้โปรแกรมตัวแทนแต่ละโปรแกรมทำงานที่แตกต่างกัน ในปี พ.ศ. 2542 เมลล์ (Peter Mell) และแม็กเลนอน (Mark McLarnon) ได้เสนอแนวคิดของระบบการตรวจหาการบุกรุกที่ทนทานในการรับมือกับการโจมตีแบบการทำให้ใช้การไม่ได้เพื่อเอาชนะการบุกรุกโดยใช้วิธีซ่อนองค์ประกอบทั้งหมดของระบบการตรวจหาการบุกรุก [55] ในบทความของพวกเขาได้เสนอสถาปัตยกรรมของระบบการตรวจหาการบุกรุกโดยการแปลงส่วนประกอบบางที่ซึ่งไม่ใช่ไปเป็นโปรแกรมตัวแทน ในปีต่อมา เมลล์และคณะ ก็ได้เสนอสถาปัตยกรรมของระบบการตรวจหาการบุกรุกที่ทนทานโดยใช้โปรแกรมตัวแทน [30] ในสถาปัตยกรรมของพวกเขาได้กำจัดผู้โจมตีโดยสร้างส่วนประกอบทั้งหมดของระบบที่ผู้โจมตีไม่สามารถมองเห็นได้ วิธีเช่นนี้จึงช่วยบรรเทาการโจมตีได้ การที่จะให้สถาปัตยกรรมของระบบการตรวจหาการบุกรุกมีขีดความสามารถดังกล่าวได้ต้องอาศัยเทคโนโลยีของโปรแกรมตัวแทนเคลื่อนที่ที่ร่วมกับการใช้ประโยชน์จากคุณลักษณะบางอย่างของโทปอโลยีของเครือข่าย

4.1.8 โปรแกรมตัวแทนเคลื่อนที่ (Mobile Agent)

เนื้อหาในหัวข้อ 4.7 ได้อธิบายถึงระบบการตรวจหาการบุกรุกแบบกระจาย และต่อมาในหัวข้อ 4.8 ได้อธิบายความหมายและสาระสำคัญของโปรแกรมตัวแทนเคลื่อนที่ไปแล้ว ในส่วนนี้จะขยายความถึงข้อดีรวมทั้งประเด็นปัญหาสำคัญของการนำโปรแกรมตัวแทนเคลื่อนที่มาใช้ในระบบการตรวจหาการบุกรุก

การพัฒนาระบบการตรวจหาการบุกรุกแบบกระจายและการใช้ซอฟต์แวร์อิสระในการทำงานด้านการตรวจหาการบุกรุกได้นำไปสู่แนวคิดของการใช้โปรแกรมตัวแทนเคลื่อนที่ ซึ่งมีจุดเด่น [68] ที่สามารถจัดข้อจำกัดที่มีอยู่ในระบบการตรวจหาในปัจจุบันได้ทั้งในแง่ความไม่ยืดหยุ่นและส่วนประกอบที่รวมศูนย์ดังต่อไปนี้

1) ช่วยลดภาระของเครือข่าย (Network load) แทนที่จะส่งข้อมูลคราวละจำนวนมาก (เช่น แฟ้มตรวจสอบ) ไปยังหน่วยประมวลผล ย่อมง่ายกว่าที่จะเคลื่อนขั้นตอนวิธีที่ใช้ประมวลผล (เช่น โปรแกรมตัวแทน) ไปยังข้อมูลเหล่านั้นแทน ซึ่งง่ายและรวดเร็วกว่า และช่วยลดภาระของปริมาณข้อมูลที่จะวิ่งไปมาบนเครือข่ายลง

2) ช่วยลดเวลาแฝงของเครือข่าย (Network latency) เมื่อโปรแกรมตัวแทนปฏิบัติงานโดยตรงอยู่บนโฮสต์นั้นๆ การติดต่อระหว่างโฮสต์และโปรแกรมตัวแทนย่อมรวดเร็วกว่าการสื่อสารผ่านชั้นต่างๆ ของส่วนประกอบของระบบตรวจหาการบุกรุกแบบลำดับชั้นไปยังศูนย์กลางที่เป็นตัวประสานงานซึ่งอยู่บนเครือข่าย จึงช่วยลดเวลาแฝงของเครือข่ายได้

3) กระทำการได้อย่างอิสระ (Autonomous execution) เมื่อส่วนประกอบบางส่วนของระบบตรวจหาการบุกรุกถูกโจมตีจนกระทั่งเสียหายไปบางส่วน หรือถูกแบ่งแยกออกไป ส่วนที่เหลือของโปรแกรมตัวแทนอิสระก็ยังคงสามารถทำงานของตนเองต่อไปได้อย่างเป็นปกติ โดยไม่จำเป็นต้องรอให้ส่วนประกอบทุกส่วนฟื้น

สภาพคืนมาก่อนเหมือนกับระบบตรวจหาการบุกรุกแบบเดิม โปรแกรมตัวแทนเคลื่อนที่จึงช่วยเพิ่มระดับความทนทานต่อความผิดพลาดในระบบโดยรวมได้

4) อิสระจากแพลตฟอร์ม (Platform independence) โดยแพลตฟอร์มของโปรแกรมตัวแทนนั้นอนุญาตให้โปรแกรมตัวแทนสามารถท่องเที่ยวไปในสภาพแวดล้อมที่แตกต่างกันและเพิ่มความเป็นอิสระจากในระดับของระบบปฏิบัติการระหว่างโฮสต์และระบบตรวจหาการบุกรุกโดยใช้โปรแกรมตัวแทน ด้วยเหตุนี้ ระบบจึงสามารถแบ่งปันข้อมูล (และสร้างฐานความรู้ร่วมกัน) กับโปรแกรมตัวแทนอื่นๆ ซึ่งเป็นส่วนประกอบหนึ่งของระบบที่เคลื่อนที่อยู่รอบๆ เครือข่ายได้ (ถ้ามีการอนุญาต)

5) สามารถปรับตัวได้อย่างพลวัต (Dynamic adaptation) ความสามารถในการเคลื่อนที่ได้ของโปรแกรมตัวแทนสามารถใช้ประโยชน์ในการปรับแต่งค่ากำหนดโครงสร้างของระบบได้ ณ เวลาดำเนินงาน (run-time) โดยกำหนดให้โปรแกรมตัวแทนเคลื่อนที่ไปยังตำแหน่งที่กำลังถูกโจมตีและปรับเปลี่ยนค่ากฎเกณฑ์เพื่อลดขอบเขตความเสียหายและยุติการโจมตีได้

6) สามารถยกระดับได้ (Upgradeability) นับเป็นเรื่องสำคัญสำหรับระบบตรวจหาการบุกรุก (โดยเฉพาะอย่างยิ่งแบบวิธีการตรวจหาการใช้สิทธิ์โดยมิชอบ) การปรับข้อมูลเกี่ยวกับลายเซ็นการโจมตีในฐานข้อมูลและขั้นตอนวิธีการตรวจหาการบุกรุกให้ทันสมัยอยู่เสมอเป็นงานที่จำเป็นอย่างยิ่ง โดยปกติ ภายหลังการปรับข้อมูลดังกล่าวจำเป็นต้องทำการเริ่มต้นระบบใหม่ทั้งหมดโดยเฉพาะตัวรับรู้ทั้งหมด แต่การใช้โปรแกรมตัวแทนนี้ทำได้ง่ายกว่าโดยการเขียนโปรแกรมตัวแทนทับลงไปใหม่ในขณะที่ระบบยังคงสามารถทำงานได้ตามปกติ

7) สามารถปรับขนาดได้ (Scalability) เมื่อหน่วยประมวลผลกลางถูกแทนที่ด้วยโปรแกรมตัวแทนเคลื่อนที่ ภาระในการคำนวณก็จะถูกกระจายไปยังเครื่องต่างๆ และภาระของเครือข่ายก็ลดลง ด้วยเหตุนี้ขีดความสามารถในการขยายระบบได้จึงเพิ่มขึ้น ระบบตรวจหาการบุกรุกแบบนี้จึงช่วยสนับสนุนพฤติกรรมที่ทนทานต่อภาวะผิดพลาดได้เป็นอย่างดี

อย่างไรก็ตาม การใช้โปรแกรมตัวแทนและแพลตฟอร์มของโปรแกรมตัวแทนนั้นอาจเป็นสาเหตุนำไปสู่ปัญหาด้านความปลอดภัย, ขนาดของรหัส และประสิทธิภาพ [69] ได้ดังนี้

8) ความปลอดภัย การใช้โปรแกรมตัวแทนเป็นส่วนประกอบในระบบตรวจหาการบุกรุกนั้นจำเป็นต้องเพิ่มความรัดกุมในกลไกการป้องกันความปลอดภัยหลายวิธี วิธีแรก โฮสต์ (และแพลตฟอร์มของโปรแกรมตัวแทน) ที่โปรแกรมตัวแทนทำงานอยู่นั้นจะต้องถูกป้องกันอย่างรัดกุมจากการโจมตีของรหัสประสงค์ร้าย (Malicious code) วิธีนี้กระทำได้โดยการใช้ลายเซ็นของรหัสโปรแกรมตัวแทนและใช้วิธีการรับรองความถูกต้องที่สามารถตรวจสอบความถูกต้องได้โดยแพลตฟอร์ม

อีกวิธีหนึ่ง โปรแกรมตัวแทนอาจถูกปลอมแปลง แก้ไข หรือถูกลอบดักฟังจากผู้โจมตีได้ขณะที่โปรแกรมตัวแทนเหล่านี้กำลังเคลื่อนที่ไปรอบๆ เครือข่าย ปัญหานี้ป้องกันได้โดยการเข้ารหัสโปรแกรมตัวแทน ในขณะที่เคลื่อนที่ไป แต่การแก้ปัญหานี้มาพร้อมกับขนาดของโปรแกรมตัวแทนที่ใหญ่กว่าปกติ และค่าใช้จ่ายที่จำเป็นต้องใช้ในการถอดรหัสที่ปลายทาง อันกระทบโดยตรงต่อประสิทธิภาพโดยรวมของระบบและภาระของเครือข่ายที่เพิ่มขึ้นอีกด้วย นอกจากนี้ โปรแกรมตัวแทนเคลื่อนที่ย่อมมีความเสี่ยงจากการถูกโจมตีแพลตฟอร์มของโปรแกรมตัวแทนด้วย การโจมตีประเภทนี้ยุ่งยากต่อการรับมือเนื่องจากโปรแกรมตัวแทนมีเงื่อนไขที่ถูกกำหนดให้ต้องเคลื่อนที่ไปรอบๆ เครือข่าย [70]

9) ขนาดของรหัส การสร้างโปรแกรมตัวแทนให้สามารถทำงานอย่างสมบูรณ์ได้อย่างอิสระด้วยตนเองนั้น จำเป็นต้องเขียนแต่ละชิ้นของซอฟต์แวร์และโปรแกรมตัวแทนที่มีความซับซ้อนและมีขนาดใหญ่ ดังนั้นการส่งผ่านรหัสโปรแกรมตัวแทนไปรอบๆ เครือข่ายจำเป็นต้องใช้เวลา โดยเฉพาะครั้งแรกเมื่อโปรแกรมตัวแทนผ่านไปถึง โดยให้แต่ละโหนดจัดเก็บโปรแกรมตัวแทนลงในโหนดนั้นๆ โปรแกรมตัวแทนที่ซับซ้อนมีขนาดใหญ่ โดยเฉพาะอย่างยิ่งเมื่อใช้ร่วมกับกลไกการเข้ารหัส เจนเซน (W. Jansen) และคณะ ได้เสนอว่า [71] ควรใส่งานประจำที่ต้องทำลงในแพลตฟอร์มของโปรแกรมตัวแทน และออกแบบให้ส่วนต่อประสานของโปรแกรมตัวแทนทุกตัวมีลักษณะแบบเดียวกัน แต่วิธีการนี้อาจเผชิญกับปัญหาเรื่องการโจมตีแพลตฟอร์มได้

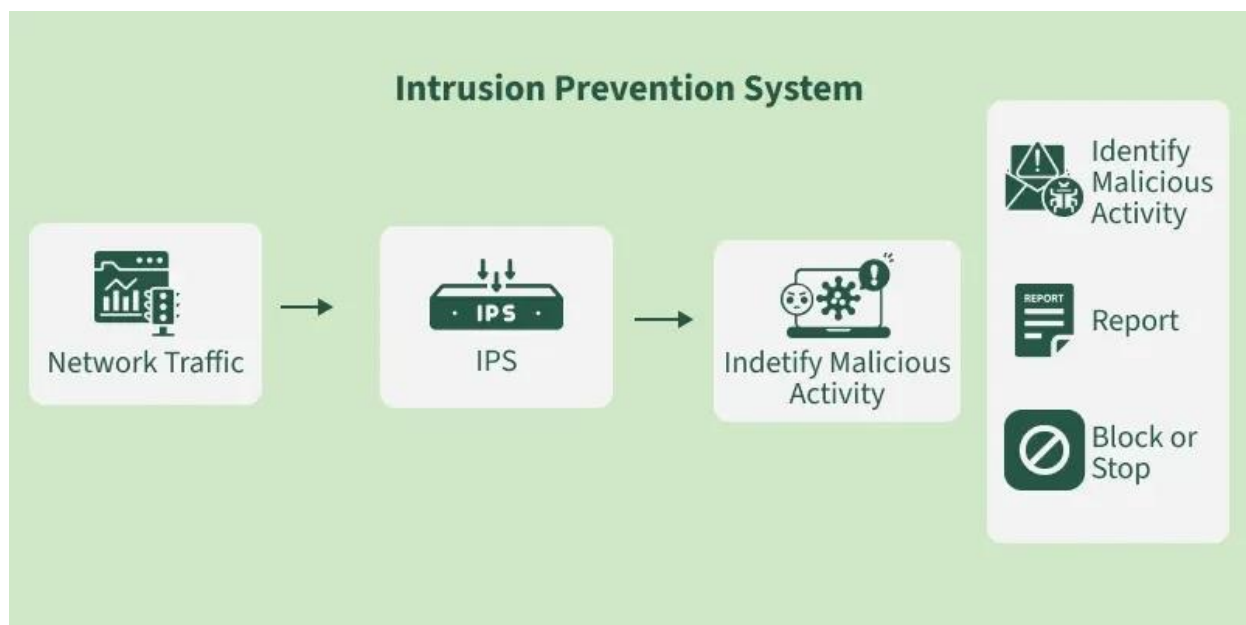
10) ประสิทธิภาพ โปรแกรมตัวแทนมักเขียนเป็นภาษาบิตคำสั่งหรือภาษาโปรแกรมแปลคำสั่งเพื่อให้่ายต่อการเคลื่อนย้ายไปยังแพลตฟอร์มที่แตกต่างกัน แต่โหมดของการกระทำนั้นจะช้ามากเมื่อเทียบกับรหัสเนทีฟ (Native code) ยิ่งไปกว่านั้น เมื่อพิจารณาว่าระบบตรวจหาการบุกรุกมีกระบวนการทำงานที่เผชิญหน้ากับข้อมูลปริมาณมหาศาลภายใต้ข้อจำกัดด้านเวลาที่ต้องการ (เกือบเท่ากับเวลาจริง) ดังนั้น การใช้เทคโนโลยีของโปรแกรมตัวแทนย่อมมีปัญหาด้านประสิทธิภาพที่ลดลง

4.2 ระบบป้องกันการบุกรุก Intrusion Prevention System (IPS)

4.2.1 ความหมายของระบบป้องกันการบุกรุก

ระบบ Intrusion Prevention System (IPS) ตามมาตรฐาน NIST คือระบบรักษาความปลอดภัยที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีเครือข่ายแบบเรียลไทม์ โดยจะวิเคราะห์ทราฟฟิก ตรวจจับกิจกรรมที่น่าสงสัย และดำเนินการหยุดยั้งการบุกรุกทันที เช่น การบล็อกแพ็กเก็ตข้อมูล หรือการปิดกั้นการเชื่อมต่อ ก่อนที่ผู้โจมตีจะสร้างความเสียหายได้ NIST เป็นหน่วยงานของสหรัฐอเมริกาที่เผยแพร่เอกสารเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์หลายฉบับที่กล่าวถึง IPS

ระบบป้องกันการบุกรุก หรือที่รู้จักกันในชื่อระบบตรวจจับและป้องกันการบุกรุก เป็นแอปพลิเคชันรักษาความปลอดภัยเครือข่ายที่คอยตรวจสอบกิจกรรมบนเครือข่ายหรือระบบเพื่อหากิจกรรมที่เป็นอันตราย หน้าที่หลักของระบบป้องกันการบุกรุกคือการระบุกิจกรรมที่เป็นอันตราย รวบรวมข้อมูลเกี่ยวกับกิจกรรมนั้น รายงาน และพยายามบล็อกหรือหยุดยั้งกิจกรรมดังกล่าว รูป 4.3 ระบบป้องกันการบุกรุก หรือ IPS



รูป 4.3 ระบบป้องกันการบุกรุก หรือ IPS

ที่มา: [geeksforgeeks.org](https://www.geeksforgeeks.org/)

ระบบป้องกันการบุกรุกถือเป็นส่วนเสริมของระบบตรวจจับการบุกรุก (IDS) เนื่องจากทั้ง IPS และ IDS ดำเนินการกับข้อมูลเครือข่ายและกิจกรรมของระบบเพื่อป้องกันการกระทำอันเป็นอันตราย โดยทั่วไป IPS จะบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่ตรวจพบ แจ้งเหตุการณ์สำคัญที่ตรวจพบให้ผู้ดูแลระบบความปลอดภัยทราบ และจัดทำรายงาน IPS จำนวนมากยังสามารถตอบสนองต่อภัยคุกคามที่ตรวจพบได้ด้วยการพยายามป้องกันไม่ให้ภัย

คุกคามนั้นเกิดขึ้นจริง พวกเขาใช้เทคนิคการตอบสนองที่หลากหลาย ซึ่งรวมถึงการหยุดการโจมตี การเปลี่ยนแปลงสภาพแวดล้อมด้านความปลอดภัย หรือการเปลี่ยนแปลงเนื้อหาของการโจมตี

4.2.2 IPS ทำงานอย่างไร

เนื่องจากหน้าที่หลักของ IPS คือตรวจจับการบุกรุกและหยุดยั้งการโจมตีบนเครือข่ายหรือระบบ จึงใช้หลักการทำงาน

- **ตรวจสอบทราฟฟิก:** IPS จะทำงานในลักษณะ "Inline" โดยวางตัวเองไว้ตรงกลางเส้นทางของข้อมูล เพื่อตรวจสอบแพ็กเก็ตข้อมูลที่ไหลผ่านเครือข่ายอย่างต่อเนื่อง.
- **วิเคราะห์รูปแบบ:** ระบบจะวิเคราะห์รูปแบบทราฟฟิกและเปรียบเทียบกับฐานข้อมูลการโจมตีหรือรูปแบบพฤติกรรมที่น่าสงสัย.
- **ดำเนินการป้องกัน:** เมื่อพบกิจกรรมที่เข้าข่ายการบุกรุก ระบบจะดำเนินการหยุดยั้งทันที เช่น ส่งสัญญาณ TCP Reset ได้ตอบกลับ, ปรับเปลี่ยนกฎของไฟร์วอลล์, บล็อกแพ็กเก็ตอันตราย หรือกักกันทราฟฟิกที่ผิดปกติ

IPS ทำงานโดยการวิเคราะห์ปริมาณการรับส่งข้อมูลเครือข่ายแบบเวลาจริง (Real-Time) และเปรียบเทียบกับรูปแบบการโจมตีและลายเซ็นที่รู้จัก เมื่อระบบตรวจพบปริมาณการรับส่งข้อมูลที่น่าสงสัย ระบบจะบล็อกไม่ให้เข้าสู่เครือข่าย IPS มีลักษณะการทำงานดังนี้

4.2.2.1 การปรับใช้แบบอินไลน์ (Inline Deployment)

IPS ถูกวางไว้ในเส้นทางการรับส่งข้อมูลเครือข่ายระหว่างเครือข่ายภายในของคุณและอินเทอร์เน็ตโดยตรง หรืออยู่ด้านหลังไฟร์วอลล์ ตำแหน่งนี้ช่วยให้สามารถตรวจสอบทุกแพ็กเก็ตที่ไหลผ่าน และบล็อกสิ่งผิดปกติใดๆ ได้ทันทีก่อนที่จะก่อให้เกิดอันตราย

4.2.2.2 การประมวลผลข้อมูลการจราจรล่วงหน้า (Traffic Preprocessing)

ก่อนที่จะเริ่มการตรวจสอบเชิงลึก IPS จะจัดระเบียบข้อมูลดิบ:

- มันทำให้รูปแบบการรับส่งข้อมูลเป็นปกติเพื่อป้องกันไม่ให้ผู้โจมตีซ่อนภัยคุกคามโดยใช้เทคนิคการเข้ารหัสอันชาญฉลาด
- ประกอบแพ็กเก็ตที่กระจัดกระจายเข้าด้วยกันใหม่เพื่อไม่ให้เกิดการพลาดข้อมูลใดๆ

4.2.2.3 การตรวจสอบแพ็กเก็ตแบบหลายชั้น (Layered Packet Inspection)

IPS ไม่ได้มองแค่ข้อมูลระดับพื้นผิวเท่านั้น “การตรวจสอบแพ็กเก็ตแบบเจาะลึก” นี้ช่วยให้ IPS เข้าใจทั้งโครงสร้างทางเทคนิคและเจตนาเบื้องหลังการรับส่งข้อมูล โดยจะเจาะลึกถึง:

- เลเยอร์เครือข่าย: ที่มาของแพ็กเก็ตและจุดหมายปลายทาง
- ชั้นการขนส่ง: ความน่าเชื่อถือหรือความน่าสงสัยของการเชื่อมต่อ
- ชั้นแอปพลิเคชัน: ข้อมูลประเภทใดที่จะถูกส่ง เช่น ข้อมูลการเข้าสู่ระบบหรือการถ่ายโอนไฟล์

4.2.2.4 กลไกการตรวจจับ (Detection Mechanisms)

เมื่อถอดแพ็กเก็ตและทำความเข้าใจแล้ว IPS จะตรวจสอบแพ็กเก็ตเหล่านั้นโดยใช้เทคนิคต่างๆ:

- **การตรวจจับตามลายเซ็น (Signature-Based Detection):** จับคู่การรับส่งข้อมูลกับรูปแบบการโจมตีที่ทราบ (เช่น ฐานข้อมูลลายนิ้วมือ)
- **การตรวจจับตามความผิดปกติ (Anomaly-Based Detection):** ทำเครื่องหมายทุกสิ่งที่เบี่ยงเบนไปจากพฤติกรรมปกติ เช่น ปริมาณการรับส่งข้อมูลที่เพิ่มขึ้นผิดปกติ
- **การตรวจจับตามพฤติกรรม (Behavior-Based Detection):** คอยติดตามการกระทำที่ผิดปกติหรือมีลักษณะน่าสงสัยในช่วงเวลาหนึ่ง เช่น การเข้าสู่ระบบที่ล้มเหลวซ้ำๆ
- **การตรวจจับตามนโยบาย (Policy-Based Detection):** ใช้กฎที่ตั้งโดยผู้ดูแลระบบ เช่น การบล็อกประเภทไฟล์หรือประเทศที่เจาะจง

4.2.2.5 การดำเนินการตอบสนองอัตโนมัติ

หาก IPS ตรวจพบภัยคุกคาม ก็สามารถดำเนินการได้ทันที:

- ทิ้งแพ็กเก็ตที่เป็นอันตราย
- บล็อก IP ต้นทาง
- ยุติเซสชัน
- การแจ้งเตือนหรือบันทึกทริกเกอร์
- อัปเดตกฎไฟร์วอลล์

4.2.2.6 การปรับแต่งและการบำรุงรักษา

IPS ที่มีประสิทธิภาพไม่ใช่ระบบแบบ "ตั้งค่าแล้วลืม" แต่จำเป็นต้องมีการอัปเดตและปรับแต่งเป็นประจำอย่างสม่ำเสมอ เพื่อ:

- ติดตามภัยคุกคามที่เปลี่ยนแปลงไป
- ลดผลบวกปลอม (ปิดกั้นการจราจรที่ปลอดภัยโดยไม่ได้ตั้งใจ)
- เพิ่มประสิทธิภาพการทำงานภายใต้ภาระหนัก

4.2.3 ประเภทของ IPS

แบ่งตามบริเวณที่ติดตั้ง IPS มีอยู่ 2 ประเภทหลักๆ ได้แก่

1) IPS ที่ใช้เครือข่าย (Network-Based): IPS ที่ใช้เครือข่ายจะถูกติดตั้งที่ขอบเขตเครือข่ายและตรวจสอบการรับส่งข้อมูลทั้งหมดที่เข้าและออกจากเครือข่าย

2) IPS แบบอิงโฮสต์ (Host-Based): IPS แบบอิงโฮสต์จะถูกติดตั้งบนโฮสต์แต่ละโฮสต์และตรวจสอบการรับส่งข้อมูลที่เข้าและออกจากโฮสต์นั้น

การจำแนกประเภท IPS ตามลักษณะการป้องกัน ระบบป้องกันการบุกรุก (IPS) แบ่งออกเป็น 4 ประเภท

1) ระบบป้องกันการบุกรุกบนเครือข่าย (Network-based intrusion prevention system: NIPS) ระบบจะตรวจสอบเครือข่ายทั้งหมดเพื่อค้นหาการรับส่งข้อมูลที่น่าสงสัยโดยวิเคราะห์กิจกรรมของโปรโตคอล

2) ระบบป้องกันการบุกรุกแบบไร้สาย (Wireless intrusion prevention system: WIPS) ตรวจสอบเครือข่ายไร้สายเพื่อค้นหาการรับส่งข้อมูลที่น่าสงสัยโดยวิเคราะห์โปรโตคอลเครือข่ายไร้สาย

3) การวิเคราะห์พฤติกรรมเครือข่าย (Network behavior analysis: NBA) ตรวจสอบปริมาณการรับส่งข้อมูลบนเครือข่ายเพื่อระบุภัยคุกคามที่ก่อให้เกิดปริมาณการรับส่งข้อมูลที่ผิดปกติ เช่น การโจมตีแบบปฏิเสธการให้บริการแบบกระจาย รูปแบบเฉพาะของมัลแวร์ และการละเมิดนโยบาย

4) ระบบป้องกันการบุกรุกบนโฮสต์ (Host-based intrusion prevention system: HIPS) เป็นแพ็คเกจซอฟต์แวร์ในตัวที่ควบคุมโฮสต์ตัวเดียวเพื่อค้นหาการกระทำที่น่าสงสัยโดยการสแกนเหตุการณ์ที่เกิดขึ้นภายในโฮสต์นั้น

4.3 บทวิเคราะห์เปรียบเทียบระหว่าง IPS กับ IDS

4.3.1 วิเคราะห์ลักษณะการทำงาน

ในสภาพแวดล้อมที่มีภัยคุกคามทางไซเบอร์เพิ่มมากขึ้น การทำความเข้าใจเกี่ยวกับระบบป้องกันความปลอดภัยเป็นสิ่งสำคัญโดยเฉพาะอย่างยิ่ง ระบบป้องกันการบุกรุกหรือ IPS (Intrusion Prevention System) และระบบตรวจหาการบุกรุก หรือ IDS (Intrusion Detection System) ซึ่งเป็นส่วนสำคัญสำหรับการปกป้องเครือข่ายขององค์กร เนื้อหาข้างต้นได้แสดงรายละเอียดของทั้งสองระบบนี้มีความแตกต่างในวิธีการทำงานและฟังก์ชันที่จำเป็นสำหรับการรักษาความปลอดภัยของข้อมูลและระบบเครือข่าย

IDS เป็นระบบที่มีหน้าที่ในการตรวจจับการเข้าถึงที่ผิดปกติและกิจกรรมที่อาจก่อให้เกิดภัยคุกคามทางไซเบอร์ โดยจะทำการสแกนและวิเคราะห์ข้อมูลที่มีการเรียกเข้ามาในเครือข่าย เป้าหมายหลักคือการแจ้งเตือนผู้ดูแลระบบเมื่อมีพฤติกรรมที่อาจเป็นอันตรายเกิดขึ้น การใช้ IDS จะช่วยให้สามารถตรวจสอบและเก็บข้อมูลที่มีความสำคัญเกี่ยวกับการบุกรุกและอื่นๆ ที่อาจเกิดขึ้นในระบบ

ในขณะที่ IPS ทำหน้าที่เป็นเครื่องมือป้องกันที่สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ทันที โดยสามารถปรับค่าของไฟร์วอลล์ให้บล็อกการบุกรุกหรือการเข้าถึงข้อมูลที่ไม่เหมาะสมที่มาจากแหล่งต้องสงสัยได้ทันที เป็นปฏิบัติการโต้ตอบแบบอัตโนมัติ แม้ว่าฟังก์ชันของ IDS จะมีความสำคัญในการแจ้งเตือน แต่ IPS จะช่วยให้ระบบป้องกันจากการทำลายหรือการขโมยข้อมูลได้อย่างมีประสิทธิภาพ ทั้งสองระบบนี้สามารถทำงานร่วมกันเพื่อเพิ่มความสามารถในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ดียิ่งขึ้น ทั้งจากการใช้ข้อมูลที่ IDS รวบรวมมาเป็นพื้นฐานในการทำงานของ IPS

การโจมตีแบบ DDoS (Distributed Denial of Service) เป็นรูปแบบอีกประเภทหนึ่งที่มีมุ่งทำให้ระบบไม่สามารถให้บริการได้ โดยการส่งปริมาณการเข้าถึงที่สูงถึงมากเกินไปไปยังโฮสต์เป้าหมาย ซึ่งทำให้ทรัพยากรของโฮสต์นั้นหมดลงและไม่สามารถตอบสนองต่อคำขอจากผู้ใช้ได้ เป็นการโจมตีต่อสภาพพร้อมใช้งาน (Availability) ของเครือข่าย

การเจาะระบบเพื่อขโมยข้อมูลจนทำให้ข้อมูลการรั่วไหล (Data Breach) เป็นอีกหนึ่งภัยคุกคามทางไซเบอร์ที่สามารถสร้างความเสียหายอย่างใหญ่หลวง โดยการเข้าถึงข้อมูลที่สำคัญและละเอียดอ่อนจากฐานข้อมูลขององค์กรทำให้ข้อมูลถูกเปิดเผย หรืออาจแก้ไขเปลี่ยนแปลงข้อมูลดังกล่าวได้ ถือเป็นการโจมตีต่อการรักษาความลับ (Confidentiality) และความถูกต้องครบถ้วนหรือบูรณภาพของข้อมูล (Integrity) ซึ่งการมีระบบการจัดการข้อมูลความปลอดภัยและเหตุการณ์ หรือ SIEM (Security Information and Event Management) และการประสานงานความมั่นคงปลอดภัย การทำงานและตอบสนองอัตโนมัติ หรือ SOAR (Security Orchestration, Automation, and Response) สามารถช่วยในการตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว และมีประสิทธิภาพ

4.3.2 วิเคราะห์ระบบตรวจหาการบุกรุก (IDS)

ระบบการตรวจหาการบุกรุก หรือ IDS เป็นเครื่องมือที่สำคัญในการป้องกันภัยคุกคามทางไซเบอร์ที่สามารถแบ่งออกเป็นสองรูปแบบหลัก ได้แก่ IDS แบบเครือข่าย (Network-Based IDS หรือ NIDS) และ IDS แบบโฮสต์ (Host-Based IDS หรือ HIDS) ซึ่งแต่ละแบบมีการทำงานและกระบวนการตรวจจับที่แตกต่างกัน

NIDS ทำงานโดยการตรวจสอบข้อมูลที่เดินทางผ่านเครือข่ายเพื่อค้นหาพฤติกรรมที่ผิดปกติหรือเป็นอันตราย มันวเคราะห์ทราฟฟิกที่เข้าสู่ระบบหรือออกไปจากระบบ ค้นหาเทคนิคการโจมตีต่าง ๆ รวมถึงการใช้ระบบ SIEM เพื่อรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งผ่านเครือข่าย โดยสามารถแจ้งเตือนได้ทันทีเมื่อพบเหตุการณ์ที่น่าสงสัย

ในขณะที่ HIDS จะทำงานโดยการตรวจสอบและวิเคราะห์ข้อมูลที่เกิดขึ้นภายในเครื่องเซิร์ฟเวอร์หรือโฮสต์ แทนที่จะมองที่ทราฟฟิกเครือข่าย การตรวจจับจะให้ความสำคัญกับเหตุการณ์ที่เกิดขึ้นในระดับระบบ โดยใช้ซอฟต์แวร์เพื่อทำการเก็บข้อมูลหรือบันทึกเหตุการณ์ที่อาจเป็นภัยคุกคามทางไซเบอร์ การตรวจจับพฤติกรรมต้องสงสัยหรือที่ผิดปกติใน HIDS สามารถช่วยให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้รวดเร็วขึ้น

ด้วยเครื่องมือ SOAR ทำให้การจัดการภัยคุกคามทางไซเบอร์มีประสิทธิภาพมากยิ่งขึ้น องค์กรสามารถใช้เทคนิคการวิเคราะห์พฤติกรรมเพื่อระบุภัยคุกคามที่อาจเกิดขึ้นและตรวจสอบขั้นตอนการตอบสนองที่เหมาะสมในเวลาอย่างรวดเร็ว ระบบ HIDS และ NIDS ทั้งสองประเภทช่วยสร้างปริมาณความปลอดภัยในการป้องกันภัยคุกคามทางไซเบอร์ที่สามารถนำมาประยุกต์ใช้ในแผนการรักษาความปลอดภัยในองค์กรได้อย่างมีประสิทธิภาพ

4.3.3 วิเคราะห์การทำงานของ IPS

ระบบป้องกันการบุกรุก หรือ IPS ทำงานโดยการตรวจสอบและวิเคราะห์ข้อมูลที่เข้ามาในเครือข่ายแบบเรียลไทม์ เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างรวดเร็ว นอกจากการตรวจจับการโจมตีแล้ว IPS ยังมีความสามารถในการบล็อกการโจมตีเหล่านั้นในระหว่างที่เกิดขึ้น ซึ่งทำให้เป็นส่วนสำคัญในกลยุทธ์การรักษาความปลอดภัยไซเบอร์ที่มีประสิทธิภาพ

การทำงานของ IPS เกิดขึ้นในสองขั้นตอนหลัก คือ การตรวจสอบข้อมูลที่เข้ามาและการตอบสนอง หากระบบตรวจพบกิจกรรมต้องสงสัยที่อาจมีโอกาasเป็นการโจมตี IPS จะทำงานโดยมีการวิเคราะห์ทราฟฟิกและพิจารณาว่ามีความเป็นไปได้ที่จะเป็นภัยคุกคามทางไซเบอร์หรือไม่ นอกจากนี้ ระบบยังสามารถใช้ข้อมูลและเหตุการณ์ที่จัดเก็บไว้ใน SIEM เพื่อหารูปแบบและแนวโน้มการโจมตีที่เกิดขึ้นในเครือข่าย

ด้วยการบล็อกการโจมตีที่อาจเป็นอันตรายอย่างอัตโนมัติ IPS สามารถเพิ่มความมั่นคงของระบบและช่วยป้องกันการรั่วไหลของข้อมูลโดยเฉพาะในองค์กรที่มีความเสี่ยงสูง การใช้ IPS ควบคู่กับ SOAR ก็เป็นอีกแนวทางหนึ่งที่ดีในการบริหารจัดการภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ SOAR สามารถเพิ่มศักยภาพใน

การตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้ทันที ดังนั้น การทำงานร่วมกันของ IPS, SIEM และ SOAR ช่วยให้การรักษาความปลอดภัยไซเบอร์มีประสิทธิภาพและคล่องตัวมากยิ่งขึ้น

4.3.4 ข้อดีและข้อเสียของ IPS/IDS

ระบบการป้องกันและตรวจสอบภัยคุกคามทางไซเบอร์ (IPS/IDS) ถือเป็นเครื่องมือสำคัญในการรักษาความมั่นคงของเครือข่าย ซึ่งมีข้อดีที่ชัดเจนในด้านการตรวจจับและป้องกันภัยคุกคามที่อาจเกิดขึ้น อย่างไรก็ตาม การใช้ IPS/IDS ยังมีข้อเสียที่ต้องพิจารณาอย่างรอบคอบ

ข้อดีที่สำคัญที่สุดของ IPS/IDS คือความสามารถในการตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว โดยจะเป็นการสแกนเครือข่ายเพื่อประเมินความเสี่ยงและป้องกันการโจมตีที่อาจเกิดขึ้นให้ทันทั่วทั้งเครือข่าย นอกจากนี้ระบบเหล่านี้ยังสามารถส่งข้อมูลเกี่ยวกับเหตุการณ์ที่ผิดปกติให้แก่ผู้ดูแลระบบได้ทันที ทำให้สามารถตอบสนองต่อสถานการณ์ได้อย่างรวดเร็ว

อย่างไรก็ตาม การใช้งาน IPS/IDS นั้นนอกจากมีค่าใช้จ่ายทั้งในการจัดหาระบบและการบำรุงรักษารายปีที่ค่อนข้างสูงมาก ยังมาพร้อมกับข้อจำกัดที่ต้องพิจารณา การติดตั้งและบำรุงรักษาระบบอาจมีความซับซ้อน ต้องการทรัพยากรที่สูงและผู้เชี่ยวชาญที่มีความรู้ในการจัดการระบบเหล่านี้ นอกจากนี้ การเกิดการทำนายผิดพลาด (false positives) ซึ่งหมายถึงการระบุเหตุการณ์ที่ไม่เป็นภัยคุกคามจริง อาจทำให้เกิดความสับสนและทำให้ผู้ดูแลระบบต้องเสียเวลาตรวจสอบเหตุการณ์เหล่านั้นเป็นจำนวนมาก ระบบ IPS/IDS ที่สร้างการแจ้งเตือนแบบการทำนายผิดพลาดนี้จำนวนมากในแต่ละช่วงเวลา ย่อมนำไปสู่การขาดการเฝ้าระวังหรือเกิดการละเลยต่อการแจ้งเตือนที่ร้ายแรงซึ่งเกิดจากการบุกรุกหรือโจมตีที่แท้จริงได้ ประเด็นนี้กลายเป็นข้อจำกัดสำคัญที่กระทบต่อความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ในองค์กร

กล่าวโดยสรุปแล้ว แม้ว่า IPS/IDS จะมีศักยภาพในการเป็นเครื่องมือที่มีประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ แต่ต้องพิจารณาข้อดีและข้อเสียอย่างรอบด้านเพื่อให้องค์กรสามารถใช้เทคโนโลยีนี้ได้อย่างเหมาะสม กับความต้องการและข้อจำกัดที่อาจเกิดขึ้นได้

4.3.5 การเลือก IPS/IDS ที่เหมาะสม

ในการเลือกระบบ IPS หรือ IDS ที่เหมาะสมสำหรับองค์กรนั้น จำเป็นต้องพิจารณาหลายปัจจัยที่มีผลต่อความปลอดภัยจากภัยคุกคามทางไซเบอร์ โดยเริ่มจากการประเมินขนาดขององค์กร ซึ่งรวมถึงจำนวนผู้ใช้งานและปริมาณข้อมูลที่จัดเก็บ ข้อมูลเหล่านี้จะช่วยให้องค์กรเข้าใจถึงความต้องการระบบที่ต้องการใช้ ในการป้องกันและตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

อีกปัจจัยที่สำคัญคือประเภทของข้อมูลที่แต่ละองค์กรดูแล หากองค์กรมีข้อมูลที่ละเอียดอ่อนหรือสำคัญ เช่น ข้อมูลการเงิน หรือข้อมูลส่วนบุคคล ระบบ IPS/IDS จะต้องสามารถรับมือกับความเสี่ยงด้านความปลอดภัยได้อย่างเพียงพอ นอกจากนี้ ความสามารถในการจัดการและตอบสนองต่อภัยคุกคามด้วยเทคโนโลยี SOAR ก็เป็นสิ่ง ที่ควรพิจารณาในกระบวนการเลือกใช้งานด้วย เนื่องจาก SOAR สามารถช่วยลดระยะเวลาในการตอบสนองต่อ เหตุการณ์ด้านความปลอดภัย ดังนั้น การวิเคราะห์ความเสี่ยงโดยพิจารณาจากระดับความร้ายแรงของผลกระทบ (Impact) และโอกาสที่ภัยคุกคามจะเกิดขึ้นจริง (Likelihood) จึงเป็นแนวปฏิบัติในการพิจารณาแนวทางในการ ตัดสินใจที่สำคัญ

การเปรียบเทียบระหว่างระบบ IPS/IDS ที่มีอยู่ในตลาดในปัจจุบันช่วยให้องค์กรมีข้อมูลในการตัดสินใจ มากขึ้น โดยจะต้องพิจารณาฟีเจอร์ที่ระบบแต่ละตัวนำเสนอ ตลอดจนความเข้ากันได้กับโครงสร้างพื้นฐานด้านไอที ขององค์กรเอง นอกจากนี้ ควรต้องคำนึงถึงการเป็นสมาชิกในระบบ SIEM ซึ่งจะช่วยให้มีการจัดการข้อมูลความ ปลอดภัยอย่างมีประสิทธิภาพมากยิ่งขึ้น สุดท้าย การเลือกใช้ IPS/IDS ที่เหมาะสมจะสามารถช่วยป้องกันและ จัดการการโจมตีจากภัยคุกคามทางไซเบอร์ได้ดีขึ้นอย่างแน่นอน การนำ IPS/IDS มาใช้ป้องกันภัยคุกคามทางไซ เบอร์ในองค์กร ถือเป็นการยกระดับการป้องกันที่สำคัญสำหรับองค์กร

4.3.6 แนวโน้มในอนาคตของ IPS/IDS

ในปัจจุบัน องค์กรต่าง ๆ เผชิญกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและหลากหลายมากขึ้น การ พัฒนาเทคโนโลยี IPS/IDS ได้กลายเป็นเรื่องจำเป็นในการป้องกันความเสี่ยงที่เกิดขึ้น การลงทุนและการมุ่งเน้นไปที่ การพัฒนาเทคโนโลยีที่ช่วยในการระบุและป้องกันภัยคุกคามทางไซเบอร์เป็นสิ่งที่ไม่สามารถมองข้ามได้ หนึ่งใน แนวโน้มที่สำคัญที่จะเห็นได้ในอนาคตคือการนำปัญญาประดิษฐ์ (AI) และแมชชีนเลิร์นนิงเข้ามาใช้ในการพัฒนา IPS/IDS อย่างเข้มข้น เทคโนโลยีดังกล่าวจะช่วยให้ระบบสามารถเรียนรู้จากข้อมูลการกระทำและพฤติกรรมที่เป็น อันตรายได้อย่างมีประสิทธิภาพมากขึ้น ทำให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ต่าง ๆ ได้อย่างรวดเร็ว และแม่นยำ

นอกจากนี้ องค์กรต่าง ๆ จะเริ่มให้ความสำคัญกับการใช้โซลูชันที่บูรณาการ SIEM และ SOAR เพื่อ เสริมสร้างความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามอย่างรวดเร็วและมีประสิทธิภาพ การบูรณาการ เชื่อมโยงข้อมูลจากหลายแหล่งจะช่วยให้องค์กรสามารถสร้างภาพรวมที่ชัดเจนเกี่ยวกับสถานการณ์ความปลอดภัย ของระบบ และทำให้การรับมือกับภัยคุกคามทางไซเบอร์สามารถทำได้ดียิ่งขึ้น การเตรียมพร้อมในด้านการป้องกัน ภัยคุกคามทางไซเบอร์จะกลายเป็นส่วนหนึ่งของกลยุทธ์ทางธุรกิจในอนาคต องค์กรจะต้องปรับตัวและพัฒนา ทิศทางใหม่ ๆ เพื่อให้สามารถจัดการกับภัยคุกคามที่เกิดขึ้นและปกป้องข้อมูลสำคัญอย่างมีประสิทธิภาพ

ข้อมูล เป็นทรัพยากรดิจิทัลที่สำคัญและมีมูลค่าอย่างยิ่งขององค์กร การปกป้องคุ้มครองทรัพยากรดิจิทัลในองค์กรจึงเป็นสิ่งสำคัญ การนำระบบตรวจหา ป้องกัน และตอบสนองต่อภัยคุกคามมาใช้นั้นเป็นเพียงมาตรการทางเทคนิค (Technical Measure) เท่านั้น องค์กรยังจำเป็นต้องพัฒนามาตรการเชิงกายภาพ (Physical Measure) และมาตรการเชิงองค์กร (Organizational Measure) ควบคู่ไปพร้อมๆ กัน เหนือสิ่งอื่นใด การยกระดับทักษะความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Skills) การสร้างการรับรู้ ความตระหนักรู้ คุกคามทางไซเบอร์ให้กับบุคลากรทุกระดับ โดยมีกิจกรรมอย่างเหมาะสมต่อเนื่องให้กลายเป็นหนึ่งในวัฒนธรรมองค์กร นับเป็นการสร้างภูมิคุ้มกันภัยไซเบอร์ที่ยั่งยืนที่สุด

4.4 สรุปบท

เนื้อหาในบทนี้กล่าวถึงความสำคัญและแนวทางในการเลือกใช้และพัฒนาเทคโนโลยี IPS/IDS เพื่อป้องกันและตรวจจับภัยคุกคามทางไซเบอร์ในองค์กร โดยเน้นการพิจารณาปัจจัยด้านขนาดองค์กร ประเภทข้อมูล และการบูรณาการกับระบบอื่น เช่น SIEM และ SOAR รวมถึงแนวโน้มการนำ AI และแมชชีนเลิร์นนิงมาใช้เพื่อเพิ่มประสิทธิภาพการป้องกันในอนาคต นอกจากนี้ยังชี้ให้เห็นว่าการสร้างวัฒนธรรมความตระหนักรู้ด้านความมั่นคงปลอดภัยในองค์กรและการพัฒนาทักษะของบุคลากรเป็นรากฐานสำคัญในการเสริมภูมิคุ้มกันภัยไซเบอร์อย่างยั่งยืน

4.5 บทวิเคราะห์และมุมมองเชิงวิชาการ

การตรวจหาการบุกรุกและการป้องกัน

เอกสารคำสอนสัปดาห์ที่ 4 หัวข้อ “การตรวจหาการบุกรุกและการป้องกัน” วางโครงสร้างแก่นความรู้ตั้งแต่นิยามการบุกรุก/ภัยคุกคาม/การโจมตี แบบจำลองการตรวจจับ (signature-based vs anomaly-based), ประเภท/สถาปัตยกรรมของ IDS (HIDS/NIDS, distributed/hybrid), บทบาทของ IPS ตลอดจนแนวโน้ม dIDS และ MAIDS—เป็นฐานที่ยอดเยี่ยมในการต่อยอดสู่สถาปัตยกรรมยุคใหม่ที่เน้นบริบท ตัวตน และหลักฐานเชิงปฏิบัติ (evidence-driven) สรุปสาระสำคัญของบทวิเคราะห์และมุมมองเชิงวิชาการดังนี้

1) สังเคราะห์แก่นความรู้จากเอกสาร (พร้อมการเชื่อมโยงเพื่อการสอน)

กรอบแนวคิด: เอกสารชี้ให้เห็นความต่างของ HIDS/NIDS, จุดแข็ง-จุดอ่อนของ signature-based และ anomaly-based, ปรากฏการณ์ false positive/false negative, สถาปัตยกรรมหลายชั้น/ลำดับชั้น, dIDS/MAIDS และความจำเป็นของ “hybrid” เพื่อลด blind spot ในสภาพเครือข่ายจริง ขณะเดียวกันขยายภาพไปถึง IPS ที่ทำงานเชิงรุกแบบ inline เพื่อลดทอนความเสียหายแบบ real-time. ส่วนคำอธิบายศัพท์ (survivability, robustness, scalability ฯลฯ) ช่วยตั้งโจทย์การประเมินคุณลักษณะระบบในห้องแล็บได้อย่างชัดเจน

นัยต่อหลักสูตร:

- วาง **learning path** จากพื้นฐาน (นิยาม/กลไก) → การเปรียบเทียบวิธี → การออกแบบสถาปัตยกรรม → แล็บ/กรณีศึกษา (เช่น SQLi+DDoS ที่โยงกับ NIST CSF)
- ใช้ชุดคำศัพท์และเมตริกจากเอกสารเป็น “ภาษากลาง” เวลาให้นักศึกษาเขียนรายงาน/อธิบายผลการทดลอง

2) จาก IDS/IPS สู่สถาปัตยกรรมตรวจจับร่วมสมัย

1. ยุคกราฟฟิกเข้ารหัส-โดย-ปริยาย (TLS 1.3, QUIC): NIDS แบบดั้งเดิมที่พึ่ง pattern ใน payload เผชิญข้อจำกัดด้านการมองเห็น จึงต้อง “ย้ายเลเยอร์ของสัญญาณ” ไปที่ **endpoint/host (EDR)**, **telemetry ระดับเคอร์เนล/eBPF**, และ **metadata-centric NDR** (เช่น SNI/JA3/เวลาหน่วง/ปริมาณ/ความถี่) แทนการแกะข้อมูลลึกทุกกรณี ซึ่งสอดคล้องแนวคิด “ความสามารถอยู่รอด/ทนทาน” ที่เอกสารวางไว้

2. **จาก dIDS → federated correlation:** แนวคิด dIDS/Consensus ที่กระจายตัวรับรู้หลายจุดในเอกสาร เป็นฐานที่ดีสำหรับ **federated learning/graph correlation** ในปัจจุบัน—แลกเปลี่ยน “สัญญาณ/คุณลักษณะ” มากกว่าข้อมูลดิบ ลดภาระเครือข่ายและเสริมความเป็นส่วนตัว
3. **MAIDS และบทเรียนสำหรับ “sensor ที่อิสระ/ยืดหยุ่น”:** จุดแข็งที่เอกสารกล่าว (ลด latency, dynamic adaptation) ยังคงร่วมสมัย—แต่ต้องดีไซน์ “trust boundary” ให้รัดกุม (รับรองความถูกต้องของเอเจนต์, จำกัดสิทธิ, ตรวจสอบรหัสก่อนวิ่ง) เพื่อไม่ให้ตัวเอเจนต์กลายเป็นพื้นผิวโจมตีใหม่
4. **บทบาท IPS ในโลก low-latency:** IPS ยังจำเป็นในจุดเชื่อมต่อสำคัญ (edge, DC gateway, east-west chokepoint) แต่ควรผสม **policy-as-code** และ **runtime context** (ผู้ใช้/อุปกรณ์/แอป/ความเสี่ยง) เพื่อเลี่ยง over-blocking และคุ้มครองผลกระทบต่อคุณภาพบริการ

3) ข้อเสนอเชิงออกแบบสำหรับสถาบันอุดมศึกษา

1. **สถาปัตยกรรมหลายชั้น:** HIDS+NIDS+NDR+IPS อย่างพอดี ไม่ “ยิ่งทุกอย่างด้วยก้อนอันเดียว”; ใช้วิธี “least-privilege telemetry”
2. **Micro-segmentation & Context:** ผูกนโยบายกับหน่วยงาน/บริการ/บริบท ไม่ยึดติดพอร์ต/ไอพีเพียงอย่างเดียว
3. **Runbook-First:** สร้าง playbook สั้น กระชับ วัดได้—ยึดภาษาเดียวกับนิยาม/ศัพท์ในเอกสาร เพื่อให้ทีมตีความตรงกัน

เอกสารต้นฉบับให้ “โครงกระดูก” ทางแนวคิดที่แข็งแรงของ IDS/IPS/dIDS/MAIDS และศัพท์สำคัญ เราจึงต่อยอดสู่หลักสูตรแบบ **evidence-driven** ที่รับมือโลกกราฟฟิกเข้ารหัสและระบบคลาวด์/คอนเทนเนอร์ ผ่านการออกแบบสัญญาณ-กฎ-เมตริก-จริยธรรมที่สมดุล พร้อมแล็บที่วัดผลได้จริง—เพื่อบ่มเพาะผู้เรียนให้คิดเป็น ออกแบบเป็น และสื่อสารเชิงหลักฐานได้อย่างมืออาชีพ

แบบทดสอบท้ายบท

ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง IDS และ IPS พร้อมยกตัวอย่าง

แนวคำตอบ: IDS = ตรวจจับ/แจ้งเตือน, IPS = ป้องกันแบบ Real-time; เช่น IDS ตรวจพบ SQL Injection, IPS บล็อก Payload

ข้อ 2. อธิบายการโจมตีแบบ Passive Attack และ Active Attack พร้อมยกตัวอย่าง

แนวคำตอบ: Passive = ดักฟัง, Traffic analysis; Active = Masquerade, Replay, DoS

ข้อ 3. อธิบายวิธีการตรวจจับการบุกรุกแบบ Signature-based และ Anomaly-based

แนวคำตอบ: Signature = เทียบกับฐานข้อมูลลายเซ็นโจมตีที่รู้จัก, Anomaly = ตรวจจับพฤติกรรมผิดปกติ, สามารถพบ Zero-day

ข้อ 4. วิเคราะห์เหตุการณ์ DoS Attack ในมุมมองของ Firewall, IDS, IPS

แนวคำตอบ: Firewall = กรอง Traffic, IDS = แจ้งเตือน Traffic ผิดปกติ, IPS = บล็อก Packet ประสงค์ร้าย

ข้อ 5. อธิบายขั้นตอนการตอบสนองต่อเหตุการณ์ตาม NIST Incident Response Lifecycle

แนวคำตอบ: Preparation, Detection/Analysis, Containment, Eradication, Recovery, Post-incident

ข้อสอบปรนัย 4 ตัวเลือก (10 ข้อ พร้อมเฉลย)

ข้อ 1. IDS มีหน้าที่หลักใด

- ก. ป้องกันการโจมตีแบบ Real-time
- ข. ตรวจจับและแจ้งเตือนการบุกรุก
- ค. สำรองข้อมูลระบบ
- ง. ฟื้นฟูหลังภัยพิบัติ

เฉลย: ข

ข้อ 2. IPS แตกต่างจาก IDS อย่างไร

- ก. IPS ป้องกัน/บล็อกได้ทันที
- ข. IPS เป็นแบบ Host-based เท่านั้น
- ค. IDS ทำงาน Inline เสมอ
- ง. IDS ไม่สามารถตรวจสอบ Log

เฉลย: ก

ข้อ 3. Passive Attack หมายถึงข้อใด

- ก. การแก้ไขข้อมูลในฐานข้อมูล
- ข. การปลอมตัวเป็นผู้ใช้
- ค. การดักฟังการสื่อสาร
- ง. การโจมตีแบบ DoS

เฉลย: ค

ข้อ 4. การโจมตีแบบ Replay Attack จัดอยู่ในกลุ่มใด

- ก. Passive
- ข. Active
- ค. IDS
- ง. IPS

เฉลย: ข

ข้อ 5. ตัวอย่างใดเป็นวิธีการตรวจจับแบบ Signature-based

- ก. เทียบ Pattern จากฐานข้อมูลลายเซ็น
- ข. วิเคราะห์ความผิดปกติทางสถิติ
- ค. ใช้ Machine Learning จัดกลุ่มพฤติกรรม
- ง. ตรวจสอบ Packet แบบสุ่ม

เฉลย: ก

ข้อ 6. ตัวอย่างใดเป็นการตรวจจับแบบ Anomaly-based

- ก. ตรวจจับ DoS ด้วย Pattern
- ข. ตรวจจับพฤติกรรมผิดไปจาก Profile ที่กำหนด
- ค. ตรวจสอบ Log ว่าเจอลายเซ็นหรือไม่
- ง. ตรวจสอบ Packet เทียบฐานข้อมูล

เฉลย: ข

ข้อ 7. ฟังก์ชันใดของ NIST CSF สอดคล้องกับการใช้ IDS แจ้งเตือน

- ก. Identify
- ข. Protect
- ค. Detect
- ง. Respond

เฉลย: ค

ข้อ 8. Firewall ทำหน้าที่หลักใด

- ก. ตรวจสอบสิทธิ์ผู้ใช้
- ข. กรอง Traffic ตาม Policy
- ค. ฟันฟุระบบหลังโจมตี
- ง. วิเคราะห์ความผิดปกติ

เฉลย: ข

ข้อ 9. ข้อใดเป็นประเภทของ DoS Attack

- ก. SYN Flood
- ข. SQL Injection
- ค. Sniffing
- ง. Masquerade

เฉลย: ก

ข้อ 10. การฝึก Incident Response Drill มีประโยชน์หลักใด

- ก. เพิ่มประสิทธิภาพการเข้ารหัส
- ข. เพิ่มความพร้อมในการตอบสนองเหตุการณ์จริง
- ค. ลดการใช้ Bandwidth
- ง. ป้องกัน False Positive

เฉลย: ข

บรรณานุกรมท้ายบท

ศิริเชษฐ์ โพธิ์ศรีบุญ, ผศ.ดร. (ม.ป.ป.) เอกสารคำสอน: การโจมตีทางไซเบอร์และการตรวจหาการบุกรุก (Cyber Attacking and Intrusion Detection), รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.

Garcia-Teodoro, P., et al. (2009). “Anomaly-based network intrusion detection: Techniques, systems and challenges.” Computers & Security.

ISO/IEC 27033-1. (2015). Network security—Part 1: Overview and concepts.

NIST. (2024). Cybersecurity Framework 2.0.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207).

Satid Vongprateep, and **Wichet Plaimart**, Survival Architecture for Distributed Intrusion Detection System (dIDS) using Mobile Agent. The Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007). 12-14 July 2007, Cambridge, Massachusetts, USA.

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94).

Sommer, R., & Paxson, V. (2010). “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.” IEEE S&P.

Wichet Plaimart and Sartid Vongpradhip (2011). A Sustainable Component of Intrusion Detection System using Survival Architecture on Mobile Agent, Intrusion Detection Systems, Pawel Skrobanek (Ed.).

William Stallings, (2011). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS, fourth edition.

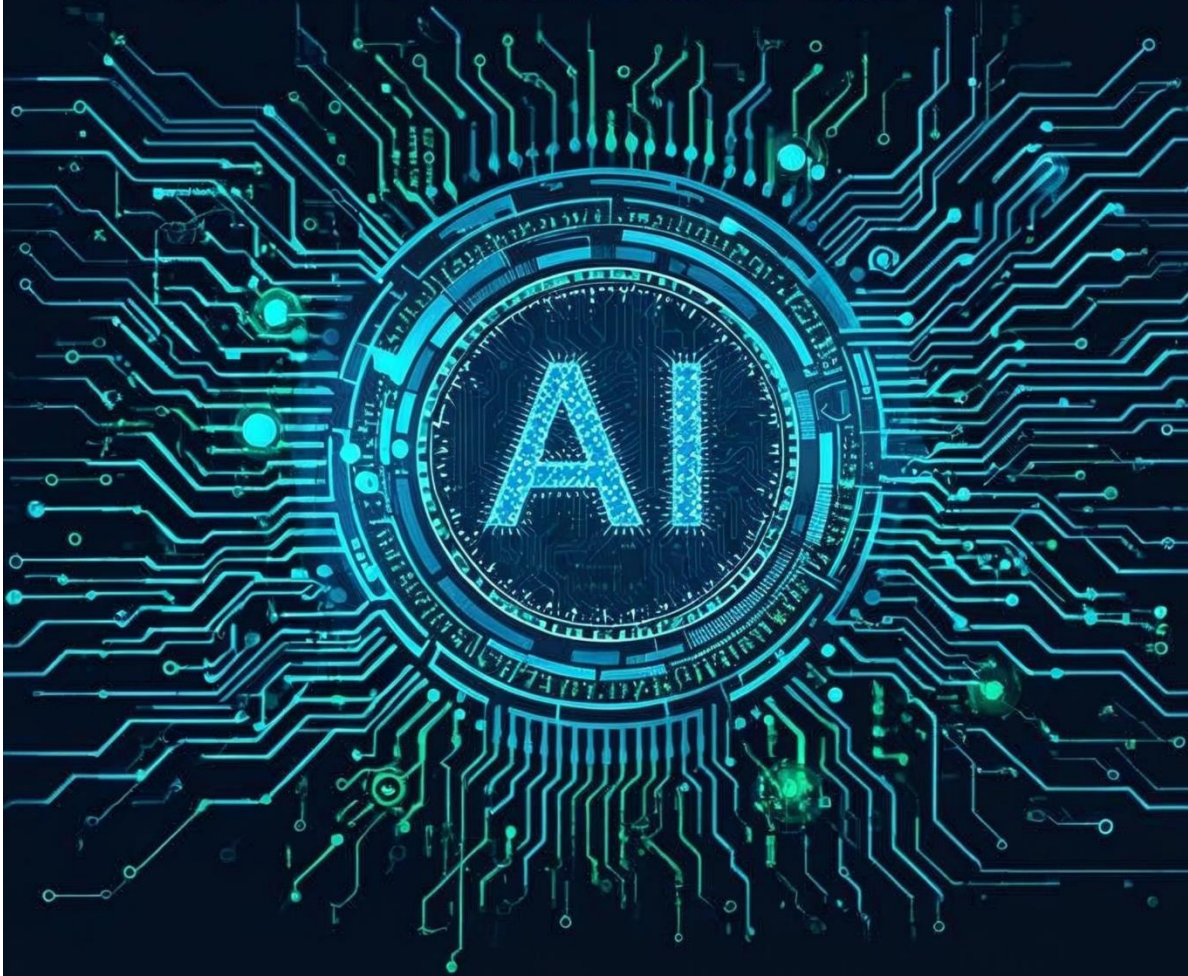
บทที่ 5

ไฟร์วอลล์และระบบอำพราง

Firewall and Anonymity Systems

**วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์**

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์หิรัญ

บทที่ 5 ไฟร์วอลล์และวิศวกรรมระบบอำพราง

(Firewall and Anonymity Systems)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

- ให้นักศึกษามีความรู้พื้นฐานเกี่ยวกับไฟร์วอลล์
- เข้าใจการทำงานของระบบอำพรางโดยใช้ NAT และ NAPT
- เข้าใจความแตกต่างระหว่าง NAT กับ NAPT ได้

2. วัตถุประสงค์เชิงพฤติกรรม

เมื่อสิ้นสุดการเรียนรู้ในสัปดาห์นี้ นักศึกษาจะสามารถ:

- อธิบายคุณลักษณะของไฟร์วอลล์, คุณสมบัติพื้นฐาน และประเภทของไฟร์วอลล์ได้อย่างถูกต้อง
- อธิบายประเภทและการทำงานของระบบอำพรางโดยใช้การแปลงเลขที่อยู่เครือข่ายเพื่อความมั่นคงปลอดภัยของเครือข่ายได้อย่างถูกต้อง
- เปรียบเทียบความแตกต่างของระบบอำพรางระหว่าง NAT กับ NAPT ได้
- วิเคราะห์การแปลงเลขที่อยู่ระหว่างเครือข่ายภายในกับเครือข่ายภายนอกได้

3. หัวข้อเนื้อหา:

ไฟร์วอลล์และวิศวกรรมระบบอำพราง

5.1 ไฟร์วอลล์ (Firewall)

- 5.1.1 ความหมายของไฟร์วอลล์
- 5.1.2 คุณลักษณะของไฟร์วอลล์
- 5.1.2 ประเภทไฟร์วอลล์
- 5.1.4 หลักการทำงานของไฟร์วอลล์

5.2 ระบบอำพรางโดยใช้การแปลงเลขที่อยู่เครือข่าย (NAT)

5.2.1 หลักการทำงานของ การแปลงเลขที่อยู่เครือข่าย

5.2.2 ประเภทของการแปลงเลขที่อยู่เครือข่าย

5.2.3 การแปลงพอร์ตที่อยู่เครือข่าย

5.2.4 ปัญหาและข้อจำกัด

5.3 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ (กรณีศึกษา)

กรณีศึกษา:

บริษัท *RMUTT ThaiE-Learning Corp.* เปิดบริการเรียนออนไลน์ให้กับนักศึกษาและบุคคลทั่วไป โดยมีระบบเซิร์ฟเวอร์อยู่ในองค์กร

- ฝ่าย IT ใช้ Firewall แบบ Stateful Inspection ในการกรองทราฟฟิก
- มีการใช้ NAT/NAPT เพื่อให้อุปกรณ์ภายในทั้งหมดแชร์ Public IP เดียว
- พบว่ามีการโจมตีจากภายนอกพยายามสแกนพอร์ตและใช้ช่องโหว่ SQL Injection ผ่าน Web Server

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

1. วิเคราะห์คุณสมบัติและข้อจำกัดของ Firewall ที่ใช้งานอยู่ (Stateful Inspection)
2. อธิบายการทำงานของ NAT/NAPT ในการปกป้องเครือข่ายภายใน
3. ประเมินผลกระทบหาก Firewall ถูกตั้งกฎไม่เหมาะสมต่อ CIA Triad
4. เสนอแนวทางเพิ่มความมั่นคงปลอดภัย เช่น ใช้ NGFW, Proxy Firewall, หรือ Load Balancer ร่วมกับ NAT
5. จัดทำรายงานสรุปผลและนำเสนอในชั้นเรียน

ประเด็นการเรียนรู้ที่แทรก:

- ความหมายและประเภทของ Firewall (Packet Filtering, Proxy, Stateful, Dynamic, Kernel Proxy)

05_ไฟร์วอลล์และระบบอำพราง

- หลักการทำงานของ NAT และ NAPT (Many-to-one, Many-to-many)
- ปัญหาและข้อจำกัดของ NAT (End-to-end, UDP, IPSec, VoIP)

- การเชื่อมโยงกับ CIA Triad และการออกแบบ Policy

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
ความถูกต้องเชิง วิชาการ (30)	วิเคราะห์ครบถ้วน อ้างอิง แนวคิด Firewall/NAT ได้ ถูกต้อง	ครบเกือบ ทั้งหมด	ครบเพียง บางส่วน	ไม่ถูกต้อง/ สับสน
การเชื่อมโยง CIA Triad (25)	วิเคราะห์ผลกระทบชัดเจน C-I- A ครบถ้วน	ครบ 2 มิติ	ครบเพียง บางส่วน	ไม่ตรงประเด็น
การเสนอแนว ทางแก้ไข (30)	เสนอวิธีแก้ไขหลายแนวทาง ครอบคลุมเชิงเทคนิค	เสนอแนวทาง 1-2 วิธี	เสนอแนวทาง แต่ยังไม่ชัด	ไม่มีข้อเสนอ
การนำเสนอ (15)	ชัดเจน ใช้ตาราง/แผนภาพ ประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

5. ไฟร์วอลล์ (Firewall)

การสื่อสารบนเครือข่ายอินเทอร์เน็ตเป็นการสื่อสารที่มีการเชื่อมโยงเครือข่ายต่างๆ ทั่วโลกเข้าไว้ด้วย แลกเปลี่ยนข้อมูลระหว่างโดยอาศัย TCP/IP เป็นโพรโทคอลมาตรฐานในการรับส่งข้อมูลจากโฮสต์ที่อยู่ในเครือข่ายหนึ่งไปส่งยังโฮสต์ปลายทางที่อยู่อีกเครือข่ายหนึ่งได้อย่างถูกต้องครบถ้วน อย่างไรก็ตาม TCP/IP นั้นยังขาดกลไกรักษาความปลอดภัยที่เพียงพอ หากอนุญาตให้โฮสต์จากเครือข่ายอื่นบนอินเทอร์เน็ตสามารถติดต่อโดยตรงกับโฮสต์ที่อยู่ในเครือข่ายภายในองค์กรของเราย่อมเสี่ยงต่อความปลอดภัยอย่างแน่นอน

5.1 ความหมายของไฟร์วอลล์

ไฟร์วอลล์ (Firewall) คือ อุปกรณ์รักษาความปลอดภัยเครือข่ายที่แยกเครือข่ายภายในที่เชื่อถือได้ (Secured Internal Network) ออกจากเครือข่ายภายนอกที่ถือว่าไม่น่าเชื่อถือ (Unsecured External Network) เช่น อินเทอร์เน็ต โดยควบคุมปริมาณการรับส่งข้อมูลเครือข่ายขาเข้าและขาออกตามกฎความปลอดภัยที่กำหนดไว้ล่วงหน้า ไฟร์วอลล์มีความสำคัญอย่างยิ่งในการป้องกันเครือข่ายจากการเข้าถึงโดยไม่ได้รับอนุญาต กิจกรรมที่เป็นอันตราย และภัยคุกคามที่อาจเกิดขึ้น ไฟร์วอลล์สามารถทำงานในรูปแบบฮาร์ดแวร์ ซอฟต์แวร์ ซอฟต์แวร์แบบบริการ (SaaS) หรือคลาวด์สาธารณะหรือส่วนตัวเสมือน

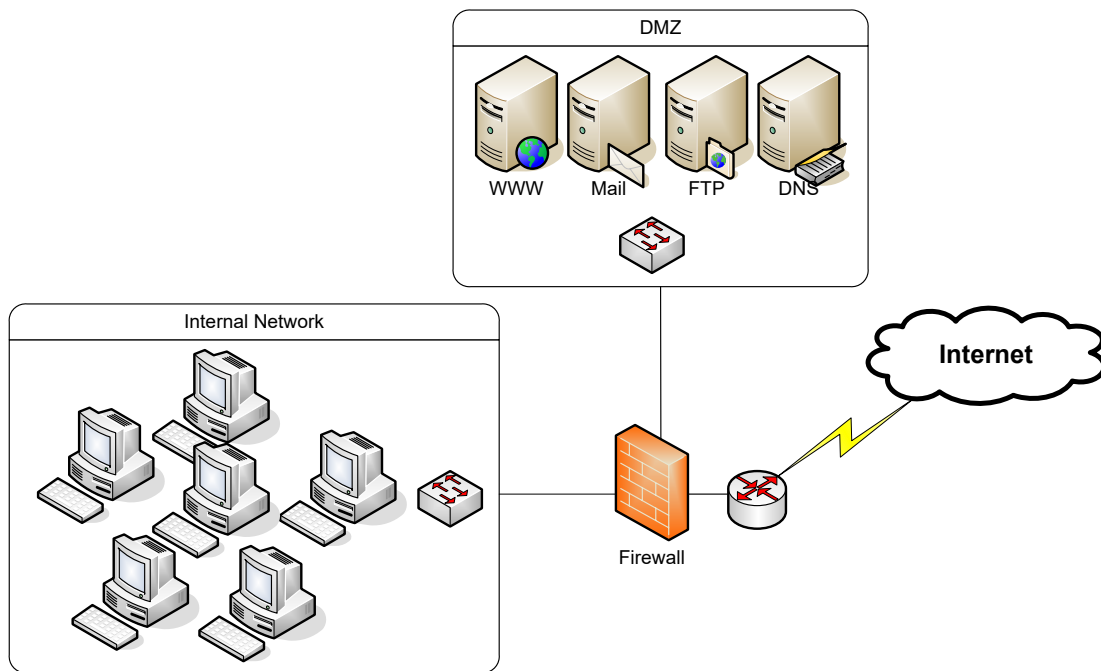
ไฟร์วอลล์ คือ ระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่ตรวจสอบและควบคุมการเข้าถึงข้อมูลระหว่างเครือข่ายภายในและเครือข่ายภายนอก เช่น อินเทอร์เน็ต โดยเปรียบเสมือนกำแพงที่คอยป้องกันข้อมูลที่ไม่ได้รับอนุญาตหรือเป็นอันตรายไม่ให้เข้าสู่เครือข่ายของเรา

ไฟร์วอลล์จะตรวจสอบแพ็กเก็ตเครือข่ายและดำเนินนโยบายความปลอดภัย ซึ่งมีประสิทธิภาพในการป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตหรือข้อมูลที่เป็นอันตรายแทรกซึมหรือออกจากเครือข่าย ไฟร์วอลล์ทำหน้าที่เป็นเกตเวย์ คอยตรวจสอบแพ็กเก็ตเครือข่ายแต่ละแพ็กเก็ตและตัดสินใจว่าจะอนุญาตหรือบล็อกแพ็กเก็ตเหล่านั้น ตามกฎที่กำหนดไว้ล่วงหน้า ซึ่งช่วยให้มั่นใจได้ว่าเฉพาะทราฟฟิกที่ปลอดภัยและถูกต้องเท่านั้นที่จะผ่านไฟร์วอลล์ได้

นอกเหนือจากฟังก์ชันหลักเหล่านี้แล้ว ไฟร์วอลล์รุ่นถัดไป (NGFW) ในปัจจุบันยังมีฟีเจอร์มากมายที่ช่วยเสริมความปลอดภัยเครือข่าย ซึ่งรวมถึงการตรวจสอบแพ็กเก็ตเชิงลึก การมองเห็นและควบคุมแอปพลิเคชัน การตรวจจับและป้องกันการบุกรุก การป้องกันมัลแวร์ การกรอง URL และอื่นๆ อีกมากมาย

องค์กรที่ตระหนักในเรื่องความปลอดภัย เมื่อต้องการให้เครือข่ายส่วนตัวขององค์กรเชื่อมต่อเข้ากับอินเทอร์เน็ตจะไม่อนุญาตให้โฮสต์ใดๆ ของเครือข่ายอื่นที่อยู่บนอินเทอร์เน็ตเชื่อมต่อเข้าโดยตรงกับโฮสต์ขององค์กร จะแบ่งการสื่อสารข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายภายนอกออกจากกันโดยอาศัยไฟร์วอลล์มา

เป็นตัวกลางควบคุมทั้งการสื่อสารจากภายในสู่ภายนอกและจากภายนอกเข้าสู่ภายใน ทราฟฟิกที่เข้ามาจากภายนอกและทราฟฟิกที่จะออกไปสู่ภายนอกจำเป็นต้องผ่านไฟร์วอลล์นี้เสมอ โดยไฟร์วอลล์จะทำหน้าที่อนุญาตหรือไม่อนุญาตโดยอาศัยกฎเกณฑ์หรือนโยบายด้านความปลอดภัยที่กำหนดไว้ล่วงหน้า [99] ดังรูป 5.1 แสดงการติดตั้งไฟร์วอลล์ซึ่งเป็นตัวกลางในการเชื่อมต่อเครือข่ายส่วนกับเครือข่ายสาธารณะ



รูป 5.1 ไฟร์วอลล์

5.2 คุณสมบัติของไฟร์วอลล์

ไฟร์วอลล์เป็นเครื่องมือรักษาความปลอดภัยที่ทำงานเชิงป้องกัน ทำหน้าที่ควบคุมการเข้าถึงเครือข่ายโดยอาศัยกฎเป็นพื้นฐาน [100] มีคุณสมบัติพื้นฐานดังนี้

- 1) การทำงานเชิงป้องกัน (Protect) ไฟร์วอลล์เป็นเครื่องมือที่ใช้ทำงานเชิงป้องกัน โดยทำหน้าที่อนุญาตหรือไม่อนุญาตแพ็กเก็ตที่เข้า-ออกเครือข่าย กลไกการอนุญาตหรือไม่อนุญาตนี้ไฟร์วอลล์จะพิจารณาจากกฎเกณฑ์ที่ตั้งไว้ ถ้าแพ็กเก็ตไม่สอดคล้องกับกฎเกณฑ์ก็จะถูกปฏิเสธจากไฟร์วอลล์ไม่ยอมให้ผ่าน ถ้าเป็นไปตามกฎเกณฑ์จึงจะยอมให้ผ่านทั้งขาเข้าและขาออก
- 2) ควบคุมการเข้าถึง (Access control) การที่โฮสต์ใดโฮสต์หนึ่งสามารถสื่อสารไปยังโฮสต์ปลายทางได้สำเร็จนั้นคือการเข้าถึงนั่นเอง การเข้าถึงในแต่ละระดับยอมทำได้ด้วยวิธีที่แตกต่างกัน

กันออกไป ไฟร์วอลล์จึงมีการทำงานที่แตกต่างกันหลายระดับเพื่อประกันว่าการเข้าถึงดังกล่าวนี้ มีความถูกต้องและปลอดภัย

- 3) อาศัยกฎเกณฑ์ (Rule based) ไฟร์วอลล์จะทำการควบคุมการเข้าถึงโดยอาศัยการเปรียบเทียบคุณสมบัติของแพ็กเก็ตที่จะผ่านไฟร์วอลล์กับกฎเกณฑ์ที่กำหนดไว้ล่วงหน้า หากพบว่าไม่มีกฎห้ามไว้ก็จะอนุญาตให้แพ็กเก็ตนั้นผ่านไปได้ แต่ถ้ามีกฎห้ามไว้ ก็จะถูกสกัดกั้นไว้ไม่ให้ผ่านไป

การที่แพ็กเก็ตใดๆ จะสามารถผ่านเข้า-ออกไฟร์วอลล์ได้หรือไม่ขึ้นอยู่กับกฎเป็นสำคัญ ไฟร์วอลล์จึงสนใจเฉพาะแพ็กเก็ตที่จะอนุญาตและแพ็กเก็ตที่จะไม่อนุญาตตามกฎที่ได้กำหนดไว้ล่วงหน้าเท่านั้น ดังนั้น หากผู้ประสงค์ร้ายทำการบุกรุกด้วยแพ็กเก็ตที่ไปเป็นตามกฎ แพ็กเก็ตนั้นก็สามารถทะลุผ่านไฟร์วอลล์ไปได้ การโจมตีประเภทนี้ก็ปราศจากการขวางกั้นโดยไฟร์วอลล์ ด้วยเหตุนี้ การป้องกันด้วยไฟร์วอลล์จึงไม่ใช่เครื่องมือพิเศษที่จะสามารถป้องกันการโจมตีทุกกรณีได้ เนื่องจากไฟร์วอลล์มีคุณสมบัติพื้นฐานอยู่ที่การควบคุมการเข้าถึงเท่านั้น หน้าที่ในการควบคุมการเข้าถึงของไฟร์วอลล์จึงเสมือนเป็นหน้าด่านสำคัญในการคัดกรองในเบื้องต้นว่าจะยอมหรือไม่ยินยอมในใครเข้า-ออกผ่านประตูไปได้บ้าง

คุณสมบัติในการคัดกรองแพ็กเก็ตของไฟร์วอลล์นั้นเป็นเรื่องสำคัญในการป้องกันความเสี่ยงที่อาจเกิดขึ้นได้ อันเนื่องมาจากการไม่สามารถจำกัดต้นทางของแพ็กเก็ตได้, การไม่สามารถจำลองทางของแพ็กเก็ตได้ [101] และการไม่สามารถจำกัดลักษณะของแพ็กเก็ตที่ต้องการได้ [102]

- 1) การไม่สามารถจำกัดต้นทางของแพ็กเก็ตได้ เมื่อโฮสต์หรือเครือข่ายของเราเชื่อมต่อเข้ากับอินเทอร์เน็ตแล้ว ก็หมายความว่าโฮสต์อื่นๆ ทั้งหมดที่อยู่บนอินเทอร์เน็ตทั่วโลกก็มีความสามารถที่จะมองเห็น, เข้าถึง และส่งแพ็กเก็ตมายังโฮสต์ของเราได้ตลอดเวลา โดยไม่สามารถปฏิเสธแหล่งที่มาของโฮสต์เหล่านั้นได้ ไม่ว่าโฮสต์เหล่านั้นจะเป็นโฮสต์ของผู้ใช้ปกติหรือเป็นผู้บุกรุกก็ตาม การมีไฟร์วอลล์จะช่วยสามารถกำหนดขอบเขตแหล่งที่มาของโฮสต์ต้นทางได้ว่าจะอนุญาตหรือไม่อนุญาตแพ็กเก็ตที่มาจากแหล่งใดได้บ้าง
- 2) การไม่สามารถจำลองทางของแพ็กเก็ตได้ เมื่อโฮสต์ใดโฮสต์หนึ่งในเครือข่ายของเราทำการเชื่อมต่อเข้ากับอินเทอร์เน็ต แม้ในความเป็นจริงจะมีเพียงโฮสต์เดียวคือแม่ข่ายที่ให้บริการเว็บเท่านั้นที่ต้องการเชื่อมต่ออินเทอร์เน็ต แต่ผลที่เกิดขึ้นก็คือทุกโฮสต์ในเครือข่ายของเราก็พลอยเชื่อมต่อกับอินเทอร์เน็ตไปด้วย จึงกลายเป็นการเพิ่มความเสี่ยงที่เกิดขึ้นจากจำนวนโฮสต์ที่เชื่อมต่ออินเทอร์เน็ตไปโดยปริยาย ความเสี่ยงที่ว่านี้อาจเกิดจากข้อที่ 1) ดังกล่าวมาแล้ว หรืออาจมีโฮสต์ใดโฮสต์หนึ่งมีช่องโหว่ที่อาจถูกโจมตีหรืออาจถูกใช้เป็นฐานในการโจมตีโฮสต์อื่นๆ ทั้งโฮสต์ภายในเครือข่ายของเราและโฮสต์ที่อยู่ภายนอกเครือข่ายของเราก็ได้ การมีไฟร์วอลล์จะ

สามารถจำกัดขอบเขตการติดต่อระหว่างโฮสต์ที่อยู่ภายในและโฮสต์ที่อยู่ภายนอกเครือข่ายของเราได้เป็นอย่างดี

- 3) การไม่สามารถจำกัดลักษณะของแพ็กเก็ตที่ต้องการได้ การใช้งานแอปพลิเคชันที่ให้บริการอยู่บนโฮสต์ต่างๆ ย่อมมีลักษณะของแพ็กเก็ตที่แตกต่างกันไปขึ้นอยู่กับลักษณะของการให้บริการ เช่น เว็บ, เมลล์, การถ่ายโอนแฟ้มต่างๆ, ICQ เป็นต้น ถ้ามีโฮสต์ที่ให้บริการเว็บอยู่ เมื่อมีผู้ร้องขอเพื่อใช้บริการอื่นๆ ที่ไม่ใช่เว็บกับโฮสต์นี้ เราก็ไม่สามารถปฏิเสธการร้องขอเหล่านั้นได้ (แม้จะไม่มีให้บริการก็ตาม) การที่โฮสต์ดังกล่าวต้องคอยตอบรับหรือปฏิเสธว่าไม่มีบริการอื่นๆ กับผู้ที่เข้ามาติดต่อนั้นถือเป็นการรบกวนการทำงานของโฮสต์นี้ได้ และนี่ถือเป็นพื้นฐานสำคัญของการถูกโจมตีประเภททำให้ใช้การไม่ได้จากผู้ไม่ประสงค์ดี การมีไฟร์วอลล์จะช่วยจำกัดประเภทของแพ็กเก็ตที่พึงประสงค์ได้

ความเสี่ยงทั้ง 3 ประการดังกล่าวล้วนเป็นความเสี่ยงที่เกิดขึ้นจากการเชื่อมต่อเครือข่ายของเราเข้ากับเครือข่ายอินเทอร์เน็ต จึงไม่สามารถควบคุมการเข้าถึงระหว่างเครือข่ายภายในกับภายนอกได้ ความเสี่ยงเหล่านี้ได้นำไปสู่ความเสียหายที่อาจเกิดขึ้นจากการโจมตีของผู้ประสงค์ร้ายในรูปแบบต่างดังที่กล่าวไว้แล้วข้างต้น ดังนั้นการมีไฟร์วอลล์จะช่วยให้หลีกเลี่ยงความเสี่ยงดังกล่าวได้โดยการกำหนดควบคุมการเข้าถึงบนพื้นฐานของกฎเกณฑ์ที่เหมาะสม

5.3 ประเภทไฟร์วอลล์

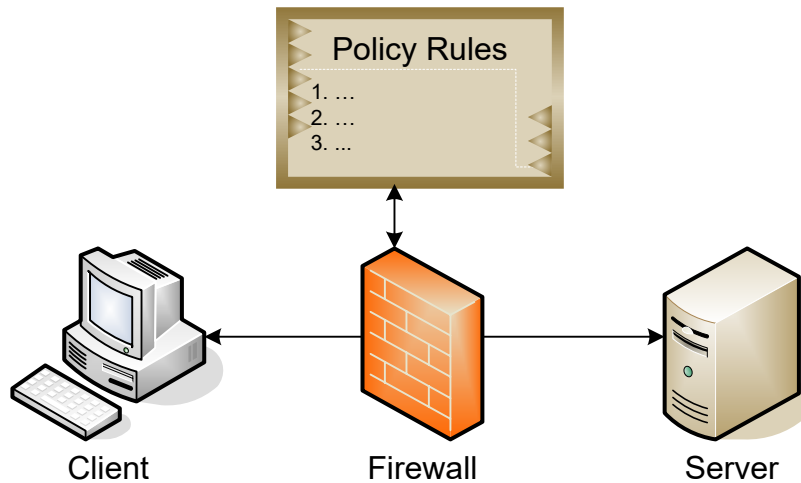
เนื่องจากไฟร์วอลล์ถูกใช้ เป็นเครื่องมือที่ใช้ควบคุมทราฟฟิกในเครือข่าย ดังนั้น ในปัจจุบันมีเครื่องมือที่ทำหน้าที่ควบคุมทราฟฟิกของเครือข่ายได้หลายลักษณะ อย่างเช่น เราเตอร์ที่สามารถคัดกรองทราฟฟิกได้ก็อาจเรียกว่าไฟร์วอลล์ได้ แต่อุปกรณ์ที่ทำหน้าที่แบบไฟร์วอลล์นั้นล้วนมีรายละเอียดการทำงานและขีดความสามารถที่แตกต่างกัน หากจำแนกไฟร์วอลล์โดยอาศัยลักษณะการทำงานเป็นเกณฑ์แล้ว เราสามารถจำแนกไฟร์วอลล์ออกเป็น 5 ประเภท ได้แก่ ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิต, ไฟร์วอลล์ระดับแอปพลิเคชันเลเยอร์ [100], ไฟร์วอลล์ระดับวงจร [102], ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบพลวัต และไฟร์วอลล์แบบพร็อกซีเคอร์เนล [103] ซึ่งมีรายละเอียดดังนี้

5.3.1 ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิต (Static packet-filtering firewall)

เป็นไฟร์วอลล์พื้นฐานที่มีความสามารถในการควบคุมทราฟฟิกโดยอาศัยการตรวจสอบข้อมูลที่ปรากฏอยู่ในส่วนเฮดเดอร์ของแพ็กเก็ต อาจเป็นได้ทั้งฮาร์ดแวร์หรือซอฟต์แวร์ หรืออาจเป็นความสามารถที่เพิ่มเข้ามาในอุปกรณ์ประเภทเราเตอร์ โดยการทำงานจะอาศัยโครงสร้างพื้นฐานของเราเตอร์ที่มีมากกว่าความสามารถในการจัดเส้นทางของแพ็กเก็ตให้ไปในทิศทางที่เหมาะสมเท่านั้น แต่ยังสามารถตรวจสอบเปรียบเทียบกับเงื่อนไขที่

กำหนดไว้ก่อนแล้วจึงส่งแพ็กเก็ตออกไป ไฟร์วอลล์ประเภทนี้จะอนุญาตให้มีการเชื่อมต่อโดยตรงระหว่างแม่ข่ายกับลูกข่ายโดยไม่จำเป็นต้องสร้างการเชื่อมต่อใหม่จึงสามารถทำงานได้รวดเร็วกว่าไฟร์วอลล์ระดับแอปพลิเคชันเลเยอร์

รูป 5.2 แสดงถึงไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ต



รูป 5.2 ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิติ

ไฟร์วอลล์ชนิดนี้บางทีเรียกว่าเราเตอร์ที่ทำหน้าที่กรอง (Screening router) เพราะเป็นการนำเอาเราเตอร์ทั่วไปที่มีความสามารถกำหนดกฎเกณฑ์การเข้าถึง (Access rule) ได้นำมาดัดแปลงเพื่อใช้ในการควบคุมทราฟฟิก ในการกำหนดกฎเกณฑ์การเข้าถึงของทราฟฟิคนั้นทำได้โดยพิจารณาจากข้อมูลแต่ละแพ็กเก็ต แต่เนื่องจากเราเตอร์เป็นอุปกรณ์ที่ทำงานในระดับอินเทอร์เน็ตเลเยอร์ ทำหน้าที่จัดเส้นทางให้แพ็กเก็ตเป็นหลักโดยพิจารณาจากเลขที่อยู่ไอพี (IP address) และจะทำการจัดเส้นทางไปที่ละแพ็กเก็ต ดังนั้น จึงสามารถควบคุมทราฟฟิกได้ดีในระดับไอพี โดยพิจารณาจากเลขที่อยู่ไอพีทั้งต้นทางและปลายทางเท่านั้น ข้อมูลในส่วนของโพรโทคอลเลเยอร์ที่สูงขึ้นไป เช่น TCP, UDP และ ICMP นั้น เนื่องจากเราเตอร์ไม่มีความสามารถในการรับรู้ข้อมูลในเลเยอร์ที่สูงกว่าคือทรานสปอร์ตเลเยอร์ (Transport layer) เราเตอร์จึงมีขีดจำกัดในการกรองทราฟฟิก โดยสามารถควบคุมทราฟฟิกได้เฉพาะเมื่อข้อมูลในทรานสปอร์ตเลเยอร์นั้นจะสามารถบรรจุได้ในแพ็กเก็ตเท่านั้น แต่ไม่สามารถรับรู้การแตกเป็นส่วนย่อยๆ ของแพ็กเก็ต (Fragment) ได้

ข้อมูลสำคัญที่บรรจุอยู่ในแต่ละแพ็กเก็ตที่สามารถนำมาใช้เป็นเงื่อนไขในการควบคุมทราฟฟิกโดยไฟร์วอลล์ประเภทนี้ ประกอบด้วย เลขที่อยู่ไอพีต้นทาง (Source IP address), เลขที่อยู่ไอพีปลายทาง (Destination IP address), โพรโทคอลที่อยู่ใน IP datagram, พอร์ตต้นทาง (Source port) สำหรับโพรโทคอลที่

ใช้พอร์ตในการติดต่อได้แก่ TCP และ UDP, พอร์ตปลายทาง (Destination port) และข้อมูลอื่นๆ ตามประเภทของโพรโทคอลที่ใช้ เช่น TCP flag, ICMP message เป็นต้น

ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิตนี้ เรียกว่า ไฟร์วอลล์ยุคที่หนึ่ง (First-generation firewall)

ข้อดีของไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบสถิตหรือเราเตอร์ที่ทำหน้าที่กรอง มีดังนี้

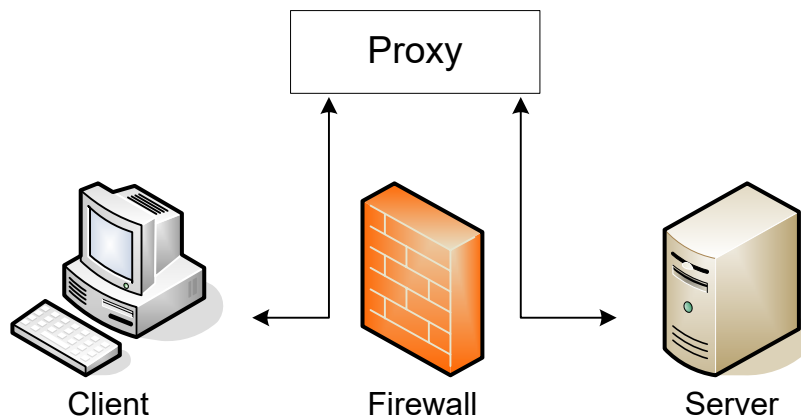
- 1) ราคาถูก เพราะเป็นคุณสมบัติที่มักมีอยู่ในเราเตอร์อยู่แล้ว ในการใช้งานเป็นไฟร์วอลล์ก็เพียงแค่กำหนดเงื่อนไขของกฎเกณฑ์การเข้าถึงให้เหมาะสม ถ้าเครือข่ายไม่มีไฟร์วอลล์ประเภทอื่นอยู่เลย ก็สามารถใช้เราเตอร์ประเภทนี้ทำหน้าที่เป็นไฟร์วอลล์ได้ในระดับหนึ่ง
- 2) หากเครือข่ายส่วนตัวขององค์กรนั้นมีจำนวนโฮสต์ในเครือข่ายจำนวนไม่มากนัก และมีการใช้งานอินเทอร์เน็ตในปริมาณไม่มากนัก ก็สามารถใช้เราเตอร์ประเภทนี้แทนไฟร์วอลล์ได้เป็นอย่างดี
- 3) การใช้เราเตอร์ทำหน้าที่กรองแพ็กเก็ตควบคู่กับไฟร์วอลล์จะช่วยแบ่งเบาภาระของไฟร์วอลล์ได้ โดยเฉพาะเมื่อมีการกำหนดกฎการเข้าถึงให้มีความสอดคล้องกันทั้งเราเตอร์และไฟร์วอลล์ จะสามารถทำหน้าที่ปกป้องเครือข่ายได้อย่างมั่นคง
- 4) การป้องกันบางประเภทไม่สามารถกระทำด้วยไฟร์วอลล์ได้ ต้องใช้เราเตอร์เท่านั้น

ส่วนข้อด้อยของเราเตอร์ที่ทำหน้าที่กรอง มีดังนี้

- 1) การกำหนดกฎเกณฑ์การเข้าถึงมีความยุ่งยากมาก ต้องการทักษะขั้นสูงของผู้ดูแลระบบ จึงมีโอกาสนี้ที่จะกำหนดเงื่อนไขผิดได้ ซึ่งส่งผลต่อความสามารถในการกรองของเราเตอร์ต้องเสียหายไป
- 2) คำสั่งในการทำงานจะผูกติดอยู่กับยี่ห้อและรุ่นของเราเตอร์ จึงไม่สามารถกำหนดคำสั่งมาตรฐานที่สามารถใช้ได้กับเราเตอร์ทุกยี่ห้อได้
- 3) ไม่สามารถกำหนดกฎที่ซับซ้อนได้ เพราะเราเตอร์จะทำการกรองทีละแพ็กเก็ตเท่านั้น
- 4) มีความสามารถที่จำกัด เช่น ไม่มีการบันทึกประวัติของแพ็กเก็ตต้องสงสัยเอาไว้ตรวจสอบภายหลัง
- 5) การใช้เราเตอร์ทำหน้าที่เป็นไฟร์วอลล์เพื่อกรองแพ็กเก็ตนั้น ย่อมส่งผลต่อประสิทธิภาพที่แท้จริงในการจัดเส้นทางของเราเตอร์ที่ต้องด้อยลง ในกรณีที่เครือข่ายมีขนาดใหญ่ การใช้เราเตอร์เพื่อการนี้ย่อมไม่คุ้มค่าต่อประสิทธิภาพที่สูญเสียไป

5.3.2 ไฟร์วอลล์ระดับแอปพลิเคชันเลเยอร์ (Application layer firewall)

บางทีเรียกว่าพร็อกซีไฟร์วอลล์ พร็อกซีเป็นกลไกที่ทำสำเนาแพ็กเก็ตจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง โดยกระบวนการสำเนานั้นจะทำการเปลี่ยนแปลงเลขที่อยู่ของต้นทางและปลายทางให้ด้วยเพื่อป้องกันโฮสต์ภายในหรือเครือข่ายส่วนตัว พร็อกซีจะเป็นตัวกลางรับคำร้องขอจากลูกข่ายแล้วทำการส่งต่อไปยังแม่ข่าย และในทำนองเดียวกันก็จะรับข้อมูลจากแม่ข่ายแล้วส่งต่อไปยังเครื่องลูกข่าย



รูป 5.3 ไฟร์วอลล์ระดับแอปพลิเคชันเลเยอร์

สำหรับไฟร์วอลล์ที่ทำงานระดับแอปพลิเคชันนั้น ทุกๆ การเชื่อมต่อจะสิ้นสุดที่ไฟร์วอลล์ ดังรูป 5.3 แสดงถึงการเชื่อมต่อจะเริ่มต้นจากลูกข่ายส่งคำร้องขอผ่านไปยังไฟร์วอลล์ จากนั้น ไฟร์วอลล์จะตรวจสอบกับนโยบายความปลอดภัยว่าจะอนุญาตให้ทราฟฟิคนั้นผ่านไปหรือไม่ ถ้าอนุญาต ไฟร์วอลล์จะสร้างการเชื่อมต่อกับแม่ข่ายแทนเครื่องลูกข่ายเอง นอกจากไฟร์วอลล์สามารถควบคุมการเชื่อมต่อจากภายในไปยังภายนอกได้แล้ว ยังสามารถควบคุมการเชื่อมต่อจากภายนอกเข้ามายังภายในได้อีกด้วย ไฟร์วอลล์จึงสามารถป้องกันการโจมตีเครือข่ายในระดับแอปพลิเคชันได้

โดยทั่วไป ไฟร์วอลล์ที่ทำงานระดับแอปพลิเคชันจะมีพร็อกซีโพรโทคอลสำหรับแอปพลิเคชันแต่ละชนิด เช่น HTTP, FTP, Telnet และ Mail เป็นต้น การใช้พร็อกซีจึงจำเป็นต้องมีโพรโทคอลแยกเฉพาะสำหรับแต่ละแอปพลิเคชัน การมีพร็อกซีจะช่วยซ่อนเลขที่อยู่ของโฮสต์ต่างๆ ภายในเครือข่ายจากการรับรู้ของผู้ที่อยู่ภายนอก ถือว่ามีส่วนช่วยป้องกันการบุกรุกได้ระดับหนึ่ง นอกจากนั้น ยังใช้พร็อกซีเป็นแคชสำหรับข้อมูลที่มีการเรียกซ้ำบ่อยๆ ซึ่งจะช่วยให้อัตราปริมาณการจราจรในเครือข่ายลงได้อีกด้วย

ไฟร์วอลล์ระดับแอปพลิเคชันนี้เรียกว่า ไฟร์วอลล์ยุคที่สอง (Second generation firewall)

ข้อดีของการใช้พร็อกซีไฟร์วอลล์ มีดังนี้

- 1) สามารถควบคุมการสื่อสารระหว่างเครือข่ายภายในกับอินเทอร์เน็ตให้อยู่ในระดับแอปพลิเคชันเท่านั้น ตัดขาดการติดต่อโดยตรงในระดับเน็ตเวิร์กเลเยอร์ทำให้ลดความเสี่ยงต่อการถูกคุกคามโดยการสแกนเครือข่าย หรือการบุกรุกที่ใช้เทคนิคในระดับเน็ตเวิร์กเลเยอร์ได้สิ้นเชิง
- 2) สามารถเพิ่มเติมหน้าที่การทำงานอย่างอื่นๆ เข้าไปในพร็อกซีได้ เช่น ป้องกันไม่ให้แม่ข่ายเว็บติดต่อกับเว็บต้องห้ามได้อีกด้วย โดยกำหนดรายชื่อเว็บต้องห้ามเหล่านั้นไว้ในรายการพร็อกซี
- 3) สามารถใช้พร็อกซีทำหน้าที่เป็นแคชได้ เพื่อเก็บข้อมูลที่มีการเรียกซ้ำอยู่บ่อยๆ ทำให้การเรียกข้อมูลจากผู้ให้บริการในเป็นการร้องขอข้อมูลที่อยู่ในพร็อกซีเท่านั้นแทนที่จะต้องร้องขอออกไปยังอินเทอร์เน็ต นอกจากนี้จะช่วยเพิ่มความเร็วแล้วยังช่วยลดปริมาณการจราจรเครือข่ายลงได้อีกทางหนึ่งด้วย
- 4) สามารถเพิ่มฟังก์ชันการพิสูจน์ตัวตนจริงของผู้ใช้ โดยกำหนดระดับสิทธิ์ของผู้ใช้ได้อย่างใกล้ชิดมากขึ้น แทนที่จะกำหนดได้แต่เพียงเลขที่อยู่ของโฮสต์เท่านั้น
- 5) สามารถกลั่นกรองเนื้อหาได้ (Content filtering) เพื่ออนุญาตให้เนื้อหาที่ไม่เหมาะสมผ่านพร็อกซีเข้าไปได้ นอกจากนี้ ยังสามารถช่วยตรวจสอบไวรัสบางชนิดที่ติดไปกับอีเมลได้อีกด้วย

ส่วนข้อจำกัดของพร็อกซีไฟร์วอลล์ มีดังนี้

- 1) ผูกติดอยู่กับแอปพลิเคชัน หากแอปพลิเคชันนั้นไม่รองรับการสื่อสารผ่านพร็อกซี ก็ไม่สามารถใช้งานได้ รวมทั้งไม่สามารถใช้งานกับแอปพลิเคชันที่ต้องการสื่อสารโดยตรงแบบ end-to-end ได้ เพราะแพ็กเก็ตจะไม่สามารถผ่านตัวกลางที่เป็นพร็อกซีได้
- 2) เสี่ยงต่อการละเมิดความเป็นส่วนตัว เนื่องจากข้อมูลที่สื่อสารกันทั้งหมดจะถูกผ่านการกลั่นกรองจากพร็อกซีก่อนเสมอ ข้อมูลเหล่านี้สามารถถูกเก็บไว้ในพร็อกซีเพื่อนำมาวิเคราะห์ตรวจตราในภายหลังได้ตลอดเวลา
- 3) จำเป็นต้องมีโปรโตคอลสำหรับแอปพลิเคชันแต่ละตัวที่ใช้พร็อกซี ไม่สามารถใช้งานร่วมกันได้ จึงทำให้เครื่องที่ทำหน้าที่พร็อกซีไฟร์วอลล์ต้องรับภาระหนัก ซึ่งย่อมต้องส่งผลต่อประสิทธิภาพของเครือข่ายอย่างแน่นอน และอาจนำไปสู่ปัญหาความขัดข้องที่จุดเดียวได้
- 4) เนื่องจากพร็อกซีเป็นแอปพลิเคชันประเภทหนึ่ง การติดต่อในระดับเน็ตเวิร์กเลเยอร์จึงจำเป็นต้องอาศัยระบบปฏิบัติการ จึงมีความสามารถในการป้องกันตัวเองต่ำกว่าไฟร์วอลล์

ประเภทอื่นๆ จึงมีความเปราะบางที่อาจบาดเจ็บได้โดยง่ายเมื่อถูกโจมตีประเภททำให้ใช้การไม่ได้

5.3.3 สเตทฟูลอินสเปกชันไฟร์วอลล์ (Stateful inspection firewall)

บางที่เรียกว่าไฟร์วอลล์ระดับวงจร (Circuit-level firewall) เรียกสั้นๆ ว่า สเตทฟูลไฟร์วอลล์ เป็นไฟร์วอลล์ที่ทำงานโดยสามารถเข้าใจสถานการณ์สื่อสารทั้งกระบวนการ ไม่ใช่แค่การกรองที่ละแพ็กเก็ตเท่านั้น แต่การกรองข้อมูลได้ทั้งสถานะ ซึ่งเป็นการมองในภาพรวมของทราฟฟิกเครือข่าย โดยสามารถเข้าใจเลขที่อยู่ต้นทางและปลายทาง, แอปพลิเคชันที่ใช้, แหล่งที่มาของต้นทาง, และความสัมพันธ์ระหว่างแพ็กเก็ตปัจจุบันกับแพ็กเก็ตก่อนหน้านี้ในเซสชันเดียวกันได้ จึงสามารถใช้ควบคุมเพื่ออนุญาตหรือไม่อนุญาตการใช้งานได้อย่างกว้างขวางครอบคลุมมากกว่าไฟร์วอลล์ประเภทที่กล่าวมา

สเตทฟูลไฟร์วอลล์ทำการควบคุมทราฟฟิกโดยอาศัยหลักการของการกรองแพ็กเก็ตและกำหนดกฎเกณฑ์การเข้าถึงเช่นเดียวกับเราเตอร์ที่ทำหน้าที่กรอง แต่มีความสามารถในการวิเคราะห์และรับรู้ความต่อเนื่องของแพ็กเก็ตของโพรโทคอลระดับสูงขึ้นไปมากกว่า เช่น TCP, FTP, HTTP เป็นต้น รวมทั้งโพรโทคอลในระดับแอปพลิเคชันที่มีลักษณะเฉพาะที่แตกต่างกัน เนื่องจาก สเตทฟูลไฟร์วอลล์เป็นเครื่องมือที่ถูกออกแบบมาเพื่อทำหน้าที่ในการควบคุมทราฟฟิกโดยเฉพาะ ไม่ใช่เป็นการดัดแปลงการทำงานของเราเตอร์ จึงมีขีดความสามารถในการควบคุมทราฟฟิก การกำหนดกฎการเข้าถึง การบริหาร ความยืดหยุ่น และมีประสิทธิภาพที่สูงกว่าไฟร์วอลล์ประเภทอื่นๆ

สเตทฟูลไฟร์วอลล์ เรียกว่าเป็นไฟร์วอลล์ยุคที่สาม (Third-generation firewall)

ข้อดีของสเตทฟูลไฟร์วอลล์ มีดังนี้

- 1) ใช้งานง่าย เพราะถูกออกแบบมาเพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ สามารถตรวจสอบแก้ไขเปลี่ยนแปลงเงื่อนไขการเข้าถึงได้ง่าย
- 2) มีประสิทธิภาพสูง ประมวลผลได้รวดเร็ว สามารถกำหนดกฎเกณฑ์การเข้าถึงที่ซับซ้อนได้โดยมีประสิทธิภาพไม่ลดลง
- 3) มีคุณสมบัติเพิ่มเติมนอกเหนือจากการควบคุมทราฟฟิก เช่น สามารถนำไปใช้ร่วมกับระบบตรวจหาการบุกรุกได้ สามารถบันทึกข้อมูลเพื่อนำไปใช้วิเคราะห์ในภายหลัง สามารถใช้งานร่วมกับซอฟต์แวร์ป้องกันไวรัสได้ เป็นต้น
- 4) สามารถเพิ่มเติมบริการอื่นๆ เช่น VPN การ Tunneling เป็นต้น
- 5) สามารถเพิ่มฟังก์ชันการพิสูจน์ตัวตนจริงของผู้ใช้ได้

- 6) การสื่อสารระหว่างไฟร์วอลล์กับโฮสต์ของผู้ดูแลระบบมีความปลอดภัยสูง มีการเข้ารหัสที่สามารถป้องกันการถูกดักอ่านข้อมูลได้

ส่วนข้อด้อยของสเตทฟูลไฟร์วอลล์ มีดังนี้

- 1) ราคาแพง เพราะเป็นเครื่องมือที่ถูกออกแบบมาเพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ มีทั้งซอฟต์แวร์และฮาร์ดแวร์โดยเฉพาะ
- 2) ในกรณีที่ไฟร์วอลล์แบบซอฟต์แวร์ที่ทำงานภายใต้ระบบปฏิบัติการ เช่น Solaris, Windows Server เป็นต้น อาจมีความเสี่ยงที่เกิดขึ้นจากข้อบกพร่องของระบบปฏิบัติการเอง ซึ่งสามารถถูกโจมตีโดยอาศัยช่องโหว่ของระบบปฏิบัติการได้ง่ายกว่าช่องโหว่ที่เกิดจากตัวไฟร์วอลล์เอง
- 3) ในกรณีที่ไฟร์วอลล์เป็นเครื่องมือเครือข่าย คือออกแบบทั้งฮาร์ดแวร์และซอฟต์แวร์ที่อยู่ในเครื่องเดียวกันเพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ ผู้ใช้จำเป็นต้องพึ่งพาผู้ผลิตเป็นหลัก

5.3.4 ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบพลวัต (Dynamic packet-filtering firewall)

ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบพลวัต สามารถแก้ไขปรับเปลี่ยนกฎเกณฑ์การเข้าถึงได้แบบทันที (Real-time) ตามสภาพแวดล้อมของเนื้อหาจราจรไฟร์วอลล์ประเภทนี้เป็นการรวมเอาคุณสมบัติของไฟร์วอลล์ประเภทแอปพลิเคชันพร็อกซีกับสเตทฟูลเข้าด้วยกัน คุณสมบัติของการกลั่นกรองแพ็กเก็ตแบบพลวัตของไฟร์วอลล์ประเภทนี้ยังสามารถใช้จัดการแพ็กเก็ตของ UDP ที่เป็นแบบไม่กำหนดการเชื่อมต่อได้ด้วย การกรองแพ็กเก็ต UDP นั้น ทำได้โดยการแคชแพ็กเก็ต UDP ไว้เป็นช่วงเวลาสั้นๆ เพื่อเก็บไว้เป็นประวัติสำหรับการวิเคราะห์เมื่อมีแพ็กเก็ตใหม่เข้ามา

ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตแบบพลวัต เรียกว่า ไฟร์วอลล์ยุคที่สี่ (Fourth-generation firewall)

5.3.5 ไฟร์วอลล์แบบพร็อกซีเคอร์เนล (Kernel proxy firewall)

เป็นการบูรณาการลงในระดับเคอร์เนลของระบบปฏิบัติการ ทำให้สามารถวิเคราะห์เซสชันและแพ็กเก็ตได้หลายระดับ ไฟร์วอลล์แบบพร็อกซีเคอร์เนลสามารถกรองแพ็กเก็ตโดยอาศัยพื้นฐานร่วมกันของนโยบายความปลอดภัยกับเงื่อนไขของสแต็กโพรโทคอล

ไฟร์วอลล์แบบพร็อกซีเคอร์เนล เรียกว่าไฟร์วอลล์ยุคที่ห้า (Fifth-generation firewall)

ไฟร์วอลล์แบบลูกผสมหรือไฟร์วอลล์เกตเวย์ที่ซับซ้อนขึ้นจะถูกสร้างจากการผสมผสานจากไฟร์วอลล์หลายประเภทหรือหลายยุคเข้าด้วยกันรวมอยู่ในไฟร์วอลล์เดียวเพื่อใช้แก้ปัญหา ส่วนใหญ่ ไฟร์วอลล์แบบหลายระดับจะมีความสามารถในการควบคุมทราฟฟิกได้ดีกว่า

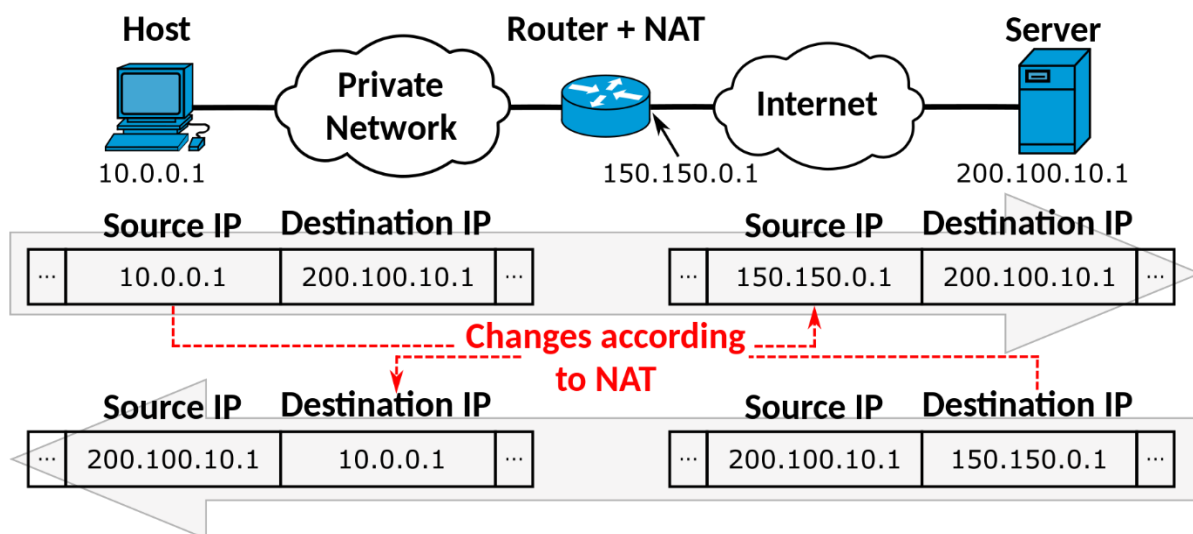
ไฟร์วอลล์เป็นเครื่องมือที่ดีสำหรับการบล็อกหรือกั้นกรองทราฟฟิก มีประสิทธิภาพที่ดีในการกีดกันทราฟฟิกที่ไม่พึงประสงค์, ความพยายามที่จะเชื่อมต่อจากภายนอกเครือข่ายส่วนตัว และใช้บล็อกข้อมูลประสงค์ร้ายที่รู้จักล่วงหน้า, ขาวสาร หรือแพ็กเก็ตเกิดตามเนื้อหา, แอปพลิเคชัน, โพรโทคอล, พอร์ต หรือแหล่งที่มา ไฟร์วอลล์ยังมีขีดความสามารถในการซ่อนโครงสร้างและเลขที่อยู่ของโฮสต์ต่างๆ ภายในเครือข่ายส่วนตัวจากสาธารณะ ส่วนใหญ่ ไฟร์วอลล์มักเพิ่มเติมการบล็อก, การตรวจสอบ และการเฝ้าดู ที่สามารถแจ้งเตือนและมีฟังก์ชันพื้นฐานเช่นเดียวกับระบบตรวจหาการบุกรุก อย่างไรก็ตาม ไฟร์วอลล์ทุกประเภท ยังไม่สามารถบล็อกไวรัสต่างๆ หรือรหัสประสงค์ร้ายที่ถูกส่งผ่านมาจากช่องที่ได้รับอนุญาต, ไม่สามารถป้องกันเจตนาร้ายของผู้ใช้จากภายใน, ไม่สามารถป้องกันการโจมตีโดยผู้ใช้ที่มีเจตนาร้ายที่อยู่ภายในไฟร์วอลล์ หรือไม่สามารถป้องกันข้อมูลที่ถูกส่งผ่านออกไปแล้วหรือผ่านเข้าไปแล้วในเครือข่ายส่วนตัวได้ การออกแบบสถาปัตยกรรมของระบบตรวจหาการบุกรุกในงานวิจัยนี้ได้ออกแบบให้มีการใช้งานร่วมกับไฟร์วอลล์ด้วย

5.4 ระบบอำพรางโดยใช้การแปลงเลขที่อยู่เครือข่าย (Network Address Translation: NAT)

5.4.1 ความหมายของ NAT

การใช้ระบบอำพรางผ่านเทคนิคการแปลงเลขที่อยู่เครือข่าย หรือเรียกว่า NAT คือกลไกสำหรับแปลงเลขที่อยู่ไอพีที่ใช้อยู่ภายในเครือข่ายส่วนตัวให้เป็นเลขที่อยู่ไอพีแบบสาธารณะเพื่อให้สามารถติดต่อสื่อสารได้บนเครือข่ายอินเทอร์เน็ต [103] เพื่อปิดบังอำพรางเลขที่อยู่ของโฮสต์ภายในเครือข่ายขององค์กรได้อย่างมีประสิทธิภาพ ช่วยลดความเสี่ยงจากการถูกโจมตีโฮสต์ได้

NAT คือบริการที่ช่วยให้เครือข่าย IP ส่วนตัวสามารถใช้อินเทอร์เน็ตและคลาวด์ได้ NAT จะแปลงที่อยู่ IP ส่วนตัวในเครือข่ายภายในเป็นที่อยู่ IP สาธารณะก่อนที่จะส่งแพ็กเก็ตไปยังเครือข่ายภายนอก รูป 5.4 แสดงหลักการทำงานของ NAT



รูป 5.4 การแปลงเลขที่อยู่ระหว่างเครือข่ายส่วนตัวต้นทางเข้ากับเลขที่อยู่เครือข่ายอินเทอร์เน็ต

(<https://commons.wikimedia.org/w/index.php?curid=86017447>)

แนวความคิดเรื่องการแปลงเลขที่อยู่เครือข่ายนี้ถูกนำเสนอโดย Kjeld Borch และ Paul Francis ใน RFC 1631 [104] เรื่อง The IP Network Address Translator (NAT) และมีข้อเสนอเพิ่มเติมโดย Pyda Srisuresh และ Matt Holdrege ใน RFC 2633 [105] เรื่อง IP Network Address Translator (NAT) Terminology and Considerations โดย NAT มีวัตถุประสงค์ในเบื้องต้นเพื่อแก้ไขความขาดแคลนของเลขที่อยู่ไอพีแบบสาธารณะ (Public IP Address) ด้วยการนำเลขที่อยู่ไอพีแบบส่วนตัว (Private IP Address) มาใช้ เพื่อเป็นการใช้งานเลขที่อยู่ไอพีได้อย่างมีประสิทธิภาพ เนื้อหาในส่วนนี้จะอธิบายถึงสาระสำคัญของการทำงานของการ

แปลงเลขที่อยู่เครือข่าย ซึ่งรวมถึงข้อดีและข้อจำกัดของการใช้ NAT และประเภทของการใช้งานการแปลงเลขที่อยู่เครือข่าย

5.4.2 หลักการทำงานของการทำงานการแปลงเลขที่อยู่เครือข่าย

การใช้ NAT จึงมีข้อดีอยู่หลายประการ เช่น สามารถเชื่อมต่อโฮสต์ทั้งหมดที่มีอยู่ภายในองค์กรเข้ากับอินเทอร์เน็ตได้โดยใช้เลขที่อยู่ไอพีแบบสาธารณะเพียงเลขเดียว (หรือจำนวนเล็กน้อย) เท่านั้น โดยสามารถใช้เลขที่อยู่ไอพีแบบส่วนตัวที่ประกาศไว้ใน RFC 1918 [106] ซึ่งแต่เดิมถูกกำหนดไว้ให้ใช้เฉพาะภายในเครือข่ายส่วนตัวเท่านั้น นอกจากนี้ NAT จะช่วยในการป้องกันเครือข่ายโดยทำการปิดบังโครงสร้างของเลขที่อยู่ไอพีและภูมิลักษณะ (Topography) ของเครือข่ายจากอินเทอร์เน็ต ซึ่งทำให้การวิเคราะห์เครือข่ายเพื่อโจมตีของผู้บุกรุกทำได้ยากยิ่งขึ้น นับเป็นการป้องกันและหลีกเลี่ยงการโจมตีที่มีประสิทธิภาพ

ปัจจุบัน การแปลงเลขที่อยู่เครือข่ายถูกนำไปใช้งานอย่างแพร่หลายทั้งในอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์โปรโทคอล รวมทั้งไฟร์วอลล์, เราเตอร์, เกตเวย์ และพร็อกซี สามารถใช้บนเครือข่ายที่ใช้ไอพีเป็นโปรโทคอลหลักและทำงานที่เน็ตเวิร์กเลเยอร์ (เลเยอร์ 3) ของ OSI

การใช้ NAT ในปัจจุบันนิยมใช้กันอย่างแพร่หลายในวัตถุประสงค์หลักเพื่อการขยายจำนวนเลขที่อยู่ไอพีแบบสาธารณะให้แก่เครือข่ายส่วนตัวขององค์กร และด้านความปลอดภัย เนื่องจากจำนวนเลขที่อยู่ไอพีสามารถมีใช้กันได้ทั้งหมด 4.3 พันล้านเลขหมาย (2^{32}) สำหรับ IPv4 ที่ใช้กันอยู่ในปัจจุบัน และความแพร่หลายของการใช้งานอินเทอร์เน็ตในอุปกรณ์ต่างๆ เพิ่มขึ้นมากขึ้นอย่างเช่นในปัจจุบันนี้ส่งผลให้เกิดการขาดแคลนเลขที่อยู่ไอพีแบบสาธารณะที่จะสามารถรองรับได้ ในขณะที่ความนิยมในการเปลี่ยนไปใช้ IPv6 ยังไม่เกิดขึ้นในอนาคตอันใกล้นี้ ดังนั้น วิธีการแก้ปัญหาที่ตรงประเด็นที่สุดในการบรรเทาปัญหาความขาดแคลนเลขที่อยู่ไอพีแบบสาธารณะก็คือการใช้ NAT เข้ามาช่วย มีเลขที่อยู่ไอพีที่เรียกว่าเลขที่อยู่ไอพีแบบส่วนตัวซึ่งถูกกำหนดไว้ใน RFC 1918 ประกอบด้วย

10.0.0.0-10.122.255.255 (จำนวน 1 คลาสสำหรับคลาส A)

172.16.0.0-172.31.255.255 (จำนวน 16 คลาสสำหรับคลาส B)

192.168.0.0-192.168.255.255 (จำนวน 255 คลาสสำหรับคลาส C)

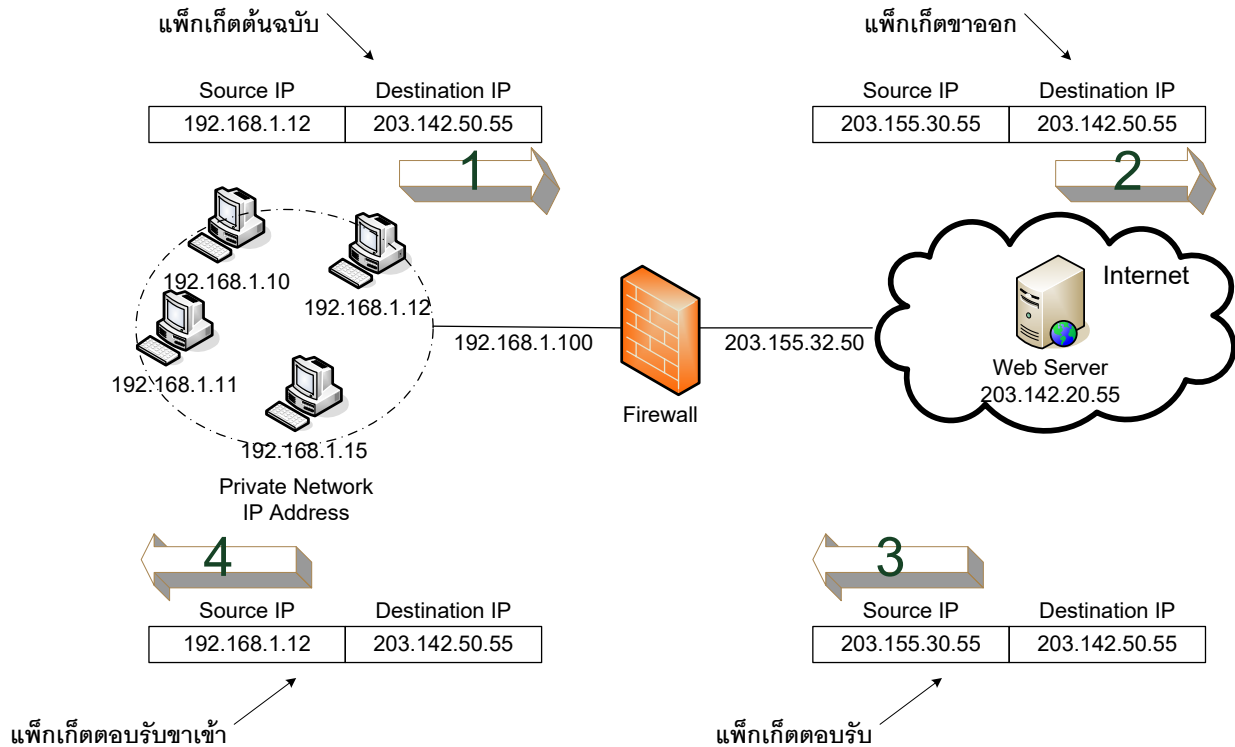
โดยปกติเลขที่อยู่ไอพีแบบส่วนตัวดังกล่าวจะถูกสงวนไว้ใช้สำหรับโฮสต์ภายในเครือข่ายส่วนตัวเท่านั้น ดังนั้น เราเตอร์ทุกตัวและอุปกรณ์ประเภทตรวจหาทราฟฟิกจะถูกกำหนดโดยค่าปริยายไม่ให้ส่งต่อทราฟฟิกจากเลขที่อยู่ไอพีเหล่านี้ออกไปสู่อินเทอร์เน็ต และหากมีทราฟฟิกที่มาจากเลขที่อยู่ไอพีประเภทดังกล่าวมาจากอินเทอร์เน็ต เราเตอร์ก็จะไม่รับทราฟฟิกเหล่านี้เข้าสู่เครือข่ายส่วนตัว นั่นหมายความว่า เลขที่อยู่ไอพีแบบส่วนตัว

จะไม่สามารถเดินทางข้ามเครือข่ายอินเทอร์เน็ตได้โดยปริยาย โฮสต์ที่ใช้เลขที่อยู่ไอพีตาม RFC 1918 นี้จะไม่สามารถเชื่อมต่อในระดับเน็ตเวิร์กเลเยอร์ได้โดยตรงกับอินเทอร์เน็ต ดังนั้น ถ้าต้องการสื่อสารกับอินเทอร์เน็ตโดยใช้เลขที่อยู่ไอพีเหล่านี้ก็จำเป็นต้องผ่านการเชื่อมต่อในระดับแอปพลิเคชัน เช่น พร็อกซี หรือแอปพลิเคชันเกตเวย์ เท่านั้น การเชื่อมต่อกับอินเทอร์เน็ตในระดับเครือข่ายโดยใช้เลขที่อยู่ไอพีแบบส่วนตัวจะสามารถทำได้โดยผ่านกระบวนการแปลงเลขที่อยู่ไอพีแบบส่วนตัว (บางทีเรียกว่า Invalid IP Address) ให้เป็นเลขที่อยู่ไอพีแบบสาธารณะ (บางทีเรียกว่า Valid IP Address หรือ Registered IP Address) เสียก่อน กระบวนการแปลงเลขที่อยู่ไอพีแบบส่วนตัวให้เป็นเลขที่อยู่ไอพีแบบสาธารณะนี้เรียกว่าการแปลงเลขที่อยู่ไอพี หรือ NAT นั่นเอง

NAT ทำงานได้โดยอาศัยการเก็บข้อมูลสำหรับแปลงส่งระหว่างคำร้องที่ถูกร้องขอโดยโฮสต์ภายใน, เลขที่อยู่ภายในของโฮสต์ที่ร้องขอ และเลขที่อยู่ไอพีของบริการอินเทอร์เน็ตที่เชื่อมต่อ เมื่อ NAT ได้รับแพ็กเก็ตที่ร้องขอจากโฮสต์หนึ่งก็จะทำการเปลี่ยนเลขที่อยู่ของโฮสต์นั้นให้เป็นเลขที่อยู่ของเครื่องแม่ข่าย NAT การเปลี่ยนเลขที่อยู่ดังกล่าวนี้จะถูกบันทึกไว้ในตารางของฐานข้อมูลการแปลงส่ง NAT (NAT mapping database) เข้ากับเลขที่อยู่ของโฮสต์ปลายทาง จากนั้น เมื่อได้รับการตอบรับจากโฮสต์ปลายทางกลับมาจากแม่ข่ายอินเทอร์เน็ตแล้ว NAT จะทำการจับคู่ระหว่างเลขที่ของต้นทางอยู่ที่ได้รับเข้าไปเก็บไว้ในฐานข้อมูล จากนั้น จะทำการเชื่อมต่อกับระหว่างเครื่องต้นทางกับปลายทางในการติดต่อสื่อสารระหว่างกัน กระบวนการนี้เรียกว่า Stateful NAT เพราะทำหน้าที่เก็บและปรับแก้ข้อมูลให้เป็นปัจจุบันเกี่ยวกับสถานะการสื่อสารของเซสชันต่างๆ ระหว่างโฮสต์ลูกข่ายกับระบบภายนอก

รูป 5.5 แสดงให้เห็นถึงขั้นตอนการทำงานในการแปลงเลขที่อยู่ไอพีแบบส่วนตัวกับแบบสาธารณะเมื่อต้องการสื่อสารข้ามเครือข่ายอินเทอร์เน็ต โดยกำหนดให้ไฟร์วอลล์ทำหน้าที่ในการแปลงเลขที่อยู่เครือข่าย โดยมีลำดับการทำงานดังต่อไปนี้

- 1) โฮสต์ 192.168.1.12 ต้องการส่งแพ็กเก็ตออกไปยังโฮสต์ 203.142.50.55
- 2) ไฟร์วอลล์จะทำการ NAT โดยเปลี่ยนเลขที่อยู่ไอพีต้นทาง (Source IP Address) จาก 192.168.1.12 ซึ่งเป็นเลขที่อยู่ไอพีแบบส่วนตัวไปเป็น 203.155.30.55 ซึ่งเป็นเลขที่อยู่ไอพีจริง (Registered IP Address) เพื่อให้โฮสต์ปลายทางบนอินเทอร์เน็ตสามารถตอบกลับมาได้
- 3) โฮสต์ 203.142.50.55 ได้รับแพ็กเก็ตจากไฟร์วอลล์ และตอบกลับไปโดยการระบุเลขที่อยู่ไอพีปลายทาง (Destination IP Address) เป็น 203.155.30.55



รูป 5.5 แสดงแพ็กเก็ตจาก Private IP Address ที่สื่อสารกับอินเทอร์เน็ตผ่าน NAT

- 4) เมื่อไฟร์วอลล์ได้รับแพ็กเก็ตปลายทางคือ 203.155.30.55 ก็จะแปลงเลขที่อยู่ให้เป็น 192.168.1.12 ซึ่งเป็นโฮสต์ที่อยู่ภายในเครือข่ายส่วนตัวแล้วส่งแพ็กเก็ตไปยังโฮสต์ดังกล่าว

ข้อดีของการใช้ NAT สำหรับเครือข่ายส่วนตัว มีดังนี้

- 1) เป็นการใช้เลขที่อยู่ไอพีแบบสาธารณะได้อย่างมีประสิทธิภาพ เนื่องจากสามารถใช้เลขที่อยู่ไอพีแบบสาธารณะเพียง 1 เลขหมายเท่านั้น แต่สามารถอนุญาตให้โฮสต์ซึ่งใช้เลขที่อยู่ไอพีแบบส่วนตัวเข้าถึงอินเทอร์เน็ตได้ทุกโฮสต์ เพราะปกติองค์กรจะได้รับการจัดสรรเลขที่อยู่ไอพีแบบสาธารณะที่จำกัดอยู่แล้ว
- 2) มีความเสี่ยงด้านความปลอดภัยต่ำกว่า ผู้บุกรุกภายนอกจะมองไม่เห็นเลขที่อยู่จริงของโฮสต์ที่อยู่เบื้องหลังไฟร์วอลล์
- 3) สามารถปิดบังโครงสร้างของเลขที่อยู่ไอพีและภูมิลักษณะของเครือข่ายจากอินเทอร์เน็ต ทำให้ยากต่อการวิเคราะห์แผนที่และจำนวนของโฮสต์ต่างๆ ที่อยู่เบื้องหลังไฟร์วอลล์, จำนวนช่วงเชื่อมต่อหรือฮอป (Hop) ที่แพ็กเก็ตเดินทางจากโฮสต์ภายในจนไปถึงไฟร์วอลล์, จำนวนเราเตอร์และเส้นทางเดินของแพ็กเก็ต เป็นต้น

- 4) สามารถใช้ในการออกแบบเครือข่ายที่ดีได้โดยการจำแนกประเภทโฮสต์ที่เชื่อถือได้ (Trusted hosts) ซึ่งอยู่ภายในเครือข่ายกับโฮสต์ที่เชื่อถือไม่ได้ (Untrusted hosts) จากอินเทอร์เน็ต ด้วยการใช้เลขที่อยู่ไอพีแบบส่วนตัวให้กับโฮสต์ภายในและเลขที่อยู่ไอพีแบบสาธารณะให้กับโฮสต์อินเทอร์เน็ต

แต่การใช้ NAT มีข้อจำกัดดังนี้

- 1) จะต้องใช้ร่วมกับไฟร์วอลล์ที่มีขีดความสามารถในการแปลงเลขที่อยู่ระหว่างเลขที่อยู่ไอพีแบบส่วนตัวกับแบบสาธารณะได้
- 2) ไฟร์วอลล์จะลดประสิทธิภาพลงเพราะจะต้องทำหน้าที่ประมวลผล NAT ไปพร้อมๆ กับการควบคุมหราชพิก
- 3) แอปพลิเคชันบางชนิดที่ทำงานในลักษณะ end-to-end จะไม่สามารถทำงานได้หากต้องผ่านกระบวนการ NAT ในกรณีเช่นนี้จำเป็นต้องใช้เลขที่อยู่ไอพีแบบสาธารณะแทน
- 4) ไม่สามารถใช้ได้กับโฮสต์ที่รอรับการติดต่อโดยตรงจากภายนอกเช่น แมชชีนให้บริการเมลล์ เป็นต้น
- 5) หากเกิดปัญหาในการสื่อสารข้อมูลกับโฮสต์ภายนอก เช่น มีผู้ใช้เจตนาร้ายใช้โฮสต์ภายในเครือข่ายส่วนตัวโจมตีไปยังภายนอก การแก้ไขปัญหาจะยุ่งยากและใช้เวลานานกว่า เนื่องจากไม่สามารถระบุเลขที่อยู่ไอพีที่แท้จริงของแพ็กเก็ตนั้นได้โดยเร็ว

5.4.3 ประเภทของการแปลงเลขที่อยู่เครือข่าย

โดยหลักการแล้ว NAT มีหลักการพื้นฐานอยู่ที่การสลับเลขที่อยู่ไอพีไปมาในแพ็กเก็ตที่ใช้สื่อสาร การนำ NAT มาใช้งานกับเครือข่ายนั้นสามารถนำไปใช้กับเราเตอร์หรือไฟร์วอลล์ก็ได้ขึ้นอยู่กับลักษณะของเครือข่าย การใช้ NAT มีรูปแบบอยู่ 3 ประการ ได้แก่ การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิต, การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบพลวัต และการแปลงพอร์ตที่อยู่เครือข่าย

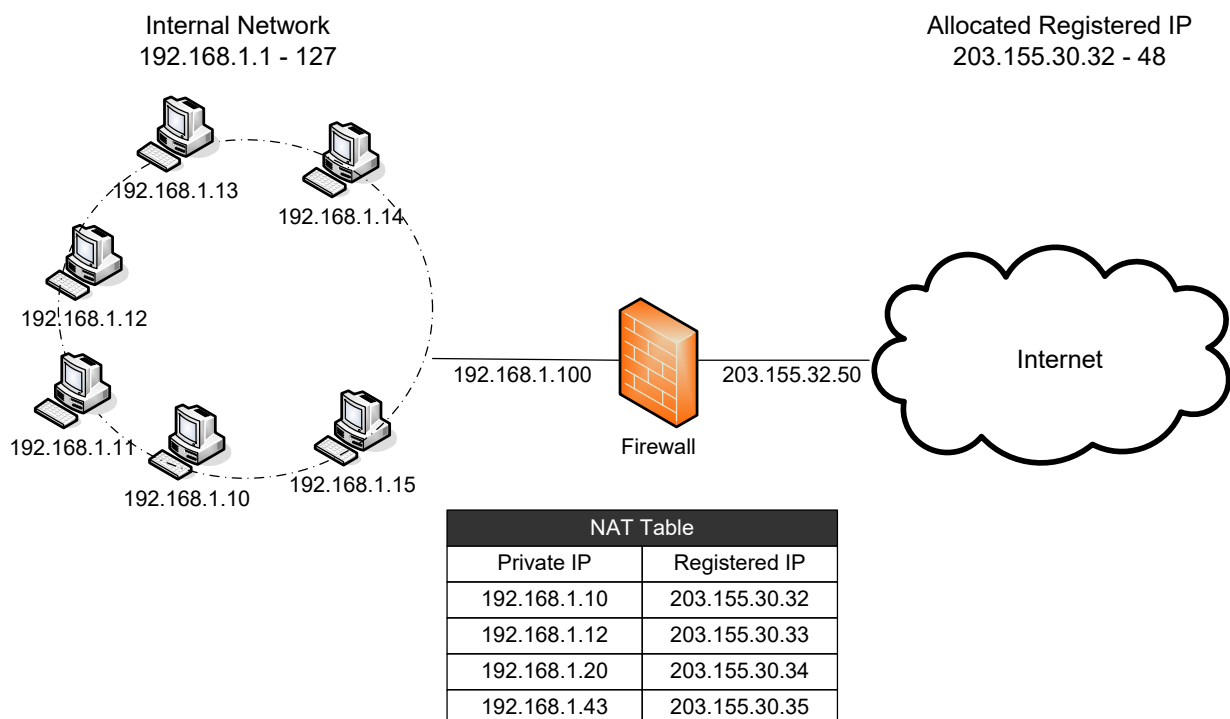
5.4.4 การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิต (Static outbound NAT)

การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิตเป็นการใช้ NAT แบบพื้นฐานที่สุด เป็นเพียงช่วยให้โฮสต์สามารถติดต่อสื่อสารกับเครือข่ายภายนอกได้เท่านั้น แต่ไม่ได้ช่วยแก้ไขปัญหาการขาดแคลนเลขที่อยู่ไอพี เนื่องจากการใช้ NAT แบบนี้จำเป็นต้องจัดหาเลขที่อยู่ไอพีจริงเท่ากับจำนวนของโฮสต์ภายในที่มีเลขที่อยู่ไอพีแบบส่วนตัวที่ต้องการเชื่อมต่อกับอินเทอร์เน็ต วิธีนี้เหมาะสำหรับในกรณีที่มีโฮสต์อยู่ภายในเครือข่ายส่วนตัวจำนวนมาก

และมีโฮสต์เพียงจำนวนหนึ่งที่ต้องการเชื่อมต่อกับอินเทอร์เน็ตเท่านั้น โฮสต์ที่ไม่เกี่ยวข้องก็ไม่จำเป็นต้องทำการ NAT

กระบวนการ NAT สำหรับวิธีนี้จำเป็นต้องจัดเตรียมการทำงานเกี่ยวกับเลขที่อยู่ไอพีจริงไว้ และการบริหารตารางแปลงเลขที่อยู่เครือข่าย โดยจะต้องจัดสรรเลขที่อยู่ไอพีจริง ในการจัดสรรเลขที่อยู่ไอพีจริงนั้น จำเป็นต้องจัดไว้เพื่อให้โฮสต์ภายในสามารถติดต่อกับภายนอกได้ และต้องจัดไว้เท่ากับจำนวนของโฮสต์ภายในที่ต้องการติดต่อกับภายนอกจึงจะสามารถทำ NAT ได้ และตารางการจัดเส้นทางของเลขที่อยู่ไอพีจริงที่ได้รับจัดสรรมานี้ต้องกำหนดให้ชี้ไปยังอินเทอร์เน็ตเฟสของไฟร์วอลล์เสมือนว่าเครือข่ายที่อยู่ด้านหลังไฟร์วอลล์นั้นมีเครือข่ายของเลขที่อยู่ไอพีจริงอยู่ด้วย

หลังจากนั้น ตาราง NAT (NAT table) จะต้องกำหนดไว้ล่วงหน้าว่า เลขที่อยู่ไอพีแบบส่วนตัวใดจะถูกเปลี่ยนให้เป็นเลขที่อยู่ไอพีแบบสาธารณะไว้เป็นคู่ๆ โดยกำหนดไว้ในตาราง NAT ไว้อย่างตายตัว ดังรูป 5.6 เครือข่ายภายในใช้เลขที่อยู่ไอพีแบบส่วนตัวตั้งแต่ 192.168.1.1-192.168.1.127 ซึ่งสามารถมีโฮสต์ภายในเครือข่ายส่วนตัวได้ทั้งสิ้น 127 โฮสต์ ในขณะที่ เลขที่อยู่ไอพีแบบสาธารณะที่ถูกจัดสรรไว้นั้นมีเพียง 16 ไอพีเท่านั้น



รูป 5.6 ตัวอย่างการใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิต

ในกรณีเช่นนี้ หากเป็นการเชื่อมต่อเครือข่ายโดยใช้เราเตอร์โดยไม่มี NAT มาช่วย โฮสต์ภายในเครือข่ายจะต้องใช้เลขที่อยู่ไอพีจริงที่ได้รับจัดสรรมาคือ 203.155.30.32-48 ซึ่งจะใช้ได้เพียง 15 โฮสต์เท่านั้น เพราะต้องจัดสรรไว้ 1 ไอพีสำหรับใช้เป็นดีฟอลต์เกตเวย์ (Default gateway) เมื่อใช้ NAT มาช่วยก็ทำให้โฮสต์ภายในทุกตัวตามที่กำหนดไว้สามารถติดต่อกับอินเทอร์เน็ตได้ โดยการระบุโฮสต์เหล่านั้นไว้ในตาราง NAT

การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบสถิตินั้นมีข้อดีดังนี้

- 1) ติดตั้งง่าย ใช้งานง่าย
- 2) เป็นการใช้ NAT ขั้นพื้นฐานที่มีวัตถุประสงค์เพื่อให้โฮสต์ภายในสามารถติดต่อได้ทั้งโฮสต์ภายในและโฮสต์ภายนอก
- 3) ตรวจสอบปัญหาได้ง่ายว่าเกิดจากโฮสต์ใด เนื่องจากการจับคู่กันแบบคงที่ระหว่างเลขที่อยู่ไอพีแบบส่วนตัวกับแบบสาธารณะ

อย่างไรก็ตาม การใช้งาน NAT ในลักษณะนี้มีข้อจำกัดดังนี้

- 1) ใช้ NAT อย่างมีประสิทธิภาพต่ำ ไม่ได้ช่วยแก้ปัญหาเรื่องการขาดแคลนเลขที่อยู่ไอพีแบบสาธารณะ เพราะในการ NAT จำเป็นต้องใช้เลขที่อยู่ไอพีจริงจับคู่กับโฮสต์ภายในแบบ 1 ต่อ 1 ดังนั้น จำนวนที่โฮสต์จะสามารถติดต่อกับภายนอกได้จริงจะมีไม่เกินจำนวนเลขที่อยู่ไอพีจริงที่ได้รับจัดสรร
- 2) ไม่ช่วยปิดบังโฮสต์ที่อยู่ภายในเครือข่ายจากภายนอกได้ เพราะการจับคู่อย่างตายตัวระหว่างโฮสต์ภายในกับเลขที่อยู่ไอพีจริง จึงไม่สามารถปกปิดการวิเคราะห์ของผู้บุกรุกได้โดยง่ายนัก

5.4.5 การใช้ NAT สำหรับแพ็กเก็ตขาออกแบบพลวัต (Dynamic outbound NAT)

การใช้งาน NAT แบบสถิตินั้นไม่เป็นไปตามวัตถุประสงค์ตามแนวคิดพื้นฐานของการใช้ NAT จึงไม่ช่วยแก้ปัญหาการขาดแคลนเลขที่อยู่ไอพีจริงและด้านความปลอดภัย จึงจำเป็นต้องกำหนดให้การใช้ NAT มีความยืดหยุ่นมากขึ้น โดยการกำหนดการจับคู่ระหว่างเลขที่อยู่ไอพีแบบส่วนตัวกับแบบสาธารณะในตาราง NAT นั้นเป็นแบบไม่ตายตัว สามารถเปลี่ยนแปลงได้ตามความเป็นจริงของสภาพการใช้งานในขณะนั้น

การใช้ NAT แบบพลวัตทำได้ดังนี้

- 1) เมื่อโฮสต์ภายในต้องการสื่อสารออกไปภายนอก ก็ทำการส่งแพ็กเก็ตไปยังดีฟอลต์เกตเวย์ซึ่งเป็นเลขที่อยู่ไอพีจริงของไฟร์วอลล์

- 2) หลังจากไฟร์วอลล์ได้รับแพ็กเก็ตดังกล่าว จะทำการตรวจสอบว่ามีเลขที่อยู่ไอพีจริงที่ว่างเพื่อมาจับคู่เข้ากับโฮสต์ดังกล่าว จากนั้นกำหนดค่าของการจับคู่ลงไปในตาราง NAT
- 3) ทำการติดต่อสื่อสารจนกว่าทั้งคู่จะสิ้นสุดเซสชัน
- 4) เมื่อการติดต่อสื่อสารระหว่างเซสชันนั้นสิ้นสุดลง ไฟร์วอลล์จึงจะคืนค่าว่างของเลขที่อยู่ไอพีกลับไปเป็นส่วนกลางเพื่อใช้ในการจับคู่กับโฮสต์ที่ต้องการใหม่

การใช้ NAT แบบนี้จึงมีความคุ้มค่า ยืดหยุ่น และสอดคล้องกับวัตถุประสงค์ในการแก้ปัญหาการขาดแคลนเลขที่อยู่ไอพีจริง และประเด็นด้านความปลอดภัยได้ แม้จำนวนโฮสต์ที่สามารถติดต่อกับภายนอก ณ เวลาเดียวกันจะมีได้ไม่เกินจำนวนเลขที่อยู่ไอพีที่มีอยู่จริงก็ตาม แต่การจับจองแบบชั่วคราวก็ทำให้โฮสต์ทั้งหมดที่อยู่ในเครือข่ายภายในมีสิทธิ์ติดต่อกับภายนอกได้ทราบเท่าที่เลขที่อยู่ไอพียังไม่ถูกจับจอง และในสภาพการใช้งานจริงนั้น การติดต่อระหว่างโฮสต์ภายในกับภายนอกนั้นอาจไม่ได้ติดต่อกันอยู่ตลอดเวลา ดังนั้น การจัดสรรด้วย NAT วิธีนี้ถือว่ามีประสิทธิภาพกว่าแบบแรก

5.4.6 การแปลงพอร์ตที่อยู่เครือข่าย (Network address port translation)

การประยุกต์ใช้ NAT ในระดับที่สูงขึ้นคือการแปลงพอร์ตที่อยู่เครือข่าย ซึ่งการ NAT จะทำการแปลงทั้งเลขที่อยู่ไอพีและแปลงพอร์ตไปด้วย เรียกว่า NAPT

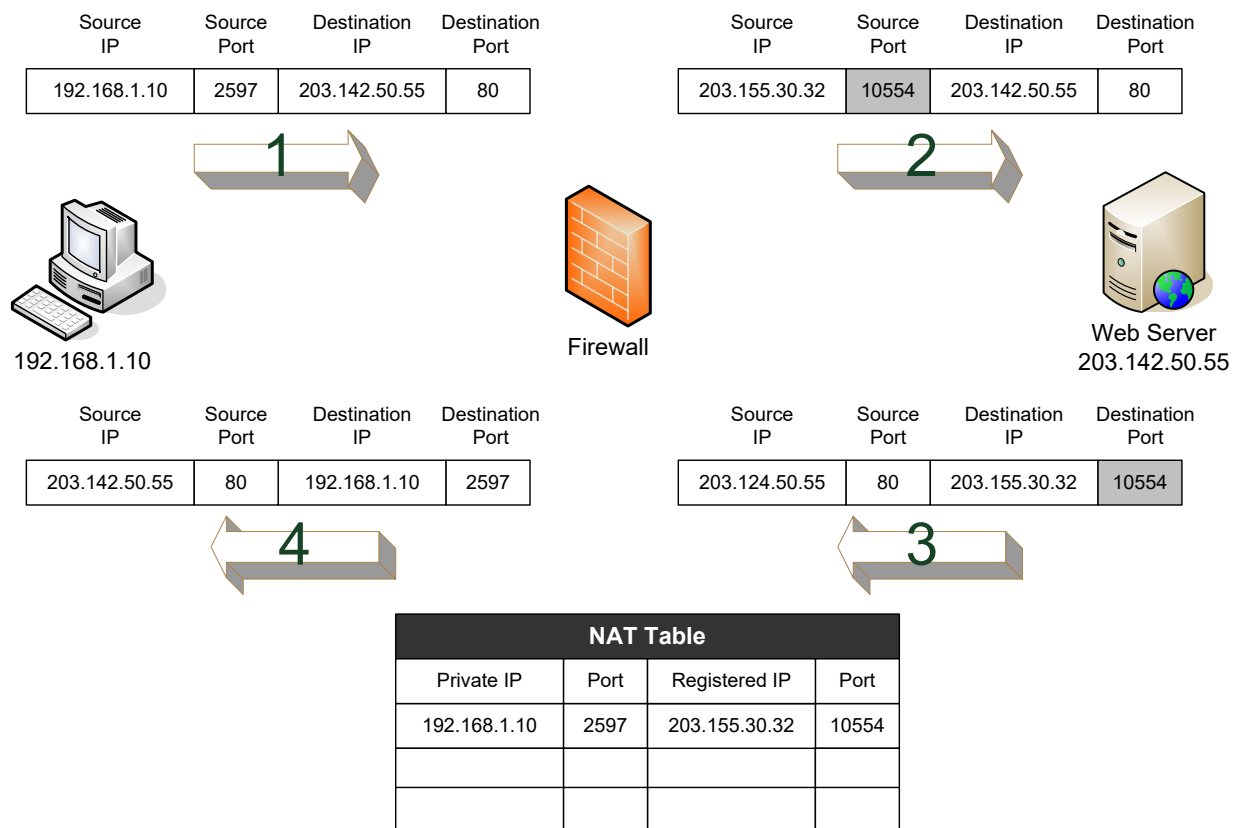
ข้อมูลสำหรับในแพ็กเก็ตสำหรับการสื่อสารนั้นประกอบด้วย เลขที่อยู่ไอพีต้นทาง, พอร์ตต้นทาง (Source port), เลขที่อยู่ไอพีปลายทาง และพอร์ตปลายทาง (Destination port) ซึ่งเรียกว่า ซ็อกเก็ต (Socket) ซึ่งเป็นตัวระบุสถานการณ์สื่อสารระหว่างโฮสต์ทั้งคู่ ทำให้ทั้งคู่สามารถสื่อสารกันได้ตลอดเซสชัน

การ NAPT นั้น จะทำการแปลงเฉพาะพอร์ตต้นทางของโฮสต์ลูกค้า (Source port หรือ Client port) โดยไม่มีการเปลี่ยนแปลงพอร์ตปลายทาง (Destination port) หรือที่เรียกว่าพอร์ตแม่ข่าย (Server port) เนื่องจากพอร์ตปลายทางจะใช้เป็นตัวระบุถึงแอปพลิเคชันที่ต้องใช้งานบนแม่ข่ายปลายทาง หากมีการเปลี่ยนแปลงพอร์ตปลายทางจะส่งผลให้ไม่สามารถเรียกใช้แอปพลิเคชันปลายทางได้ ในการ NAT ทั้งแบบสถิตและแบบพลวัตโดยปราศจากการจัดการเรื่องพอร์ตถือเป็นการ NAT แบบ 1 ต่อ 1 (One-to-One) เป็นการจับคู่กันระหว่างเลขที่อยู่ไอพีจริงกับเลขที่อยู่ไอพีแบบส่วนตัวในอัตราที่เท่ากัน เพราะในขณะใดขณะหนึ่งยังคงสามารถใช้งานโฮสต์ส่วนตัวได้เพียงโฮสต์เดียวเท่านั้น

แต่การใช้ NAPT เป็นแนวคิดที่ช่วยขยายขีดความสามารถของ NAT แบบเดิมด้วยการมัลติเพล็กซ์ (Multiplexing) เลขที่อยู่ไอพีแบบส่วนตัวจำนวนมากโดยใช้พอร์ตที่แตกต่างกันบนเลขที่อยู่ไอพีเดียวกันในเวลาเดียวกันได้ เนื่องจากการเชื่อมต่อระหว่างโฮสต์กับไฟร์วอลล์ทำให้ซ็อกเก็ต (เลขที่อยู่ไอพีและพอร์ต) ซึ่งเกิดขึ้นที่

โฮสต์ต้นทางกับโฮสต์ปลายทางจริงๆ นั้นไม่มีนัยสำคัญ และไฟร์วอลล์ที่ทำการ NAT ก็ไม่ได้ใช้หมายเลขพอร์ตต้นทางเดิมที่เกิดจากโฮสต์ภายในสื่อสารกับภายนอก ดังนั้น ไฟร์วอลล์จึงสามารถนำพอร์ตอื่นๆ ที่เหลือไปให้บริการแก่โฮสต์ภายในโฮสต์อื่นๆ ได้ ดังนั้น แม้มีเลขที่อยู่ไอพีจริงเพียงเลขหมายเดียว ไฟร์วอลล์ก็ยังสามารถทำการ NAT ให้แก่โฮสต์ภายในจำนวนมากได้ เพราะไฟร์วอลล์มีพอร์ตที่ใช้งานได้ทั้งสิ้น 65535 พอร์ต แม้จะสงวนไว้สำหรับพอร์ตแม่ข่ายประมาณ 1024 พอร์ต ก็ยังเหลือพอร์ตอยู่อีก 64511 พอร์ต ซึ่งมีจำนวนมากพอที่จะให้บริการแก่โฮสต์ภายในได้มหาศาล

นอกจากนั้น การ NAT ด้วยวิธีนี้ เป็นการปกปิดโฮสต์ภายในจากผู้สังเกตภายนอกได้เป็นอย่างดี เพราะแม่ข่ายปลายทางจะไม่สามารถล่วงรู้ว่ามีโฮสต์ใดเข้ามาใช้บริการ เนื่องจากเลขที่อยู่ไอพีที่ปรากฏแก่แม่ข่ายจะเป็นเลขที่อยู่เดิมของไฟร์วอลล์เสมอ จึงช่วยแก้ปัญหาด้านความปลอดภัยได้เป็นอย่างดี

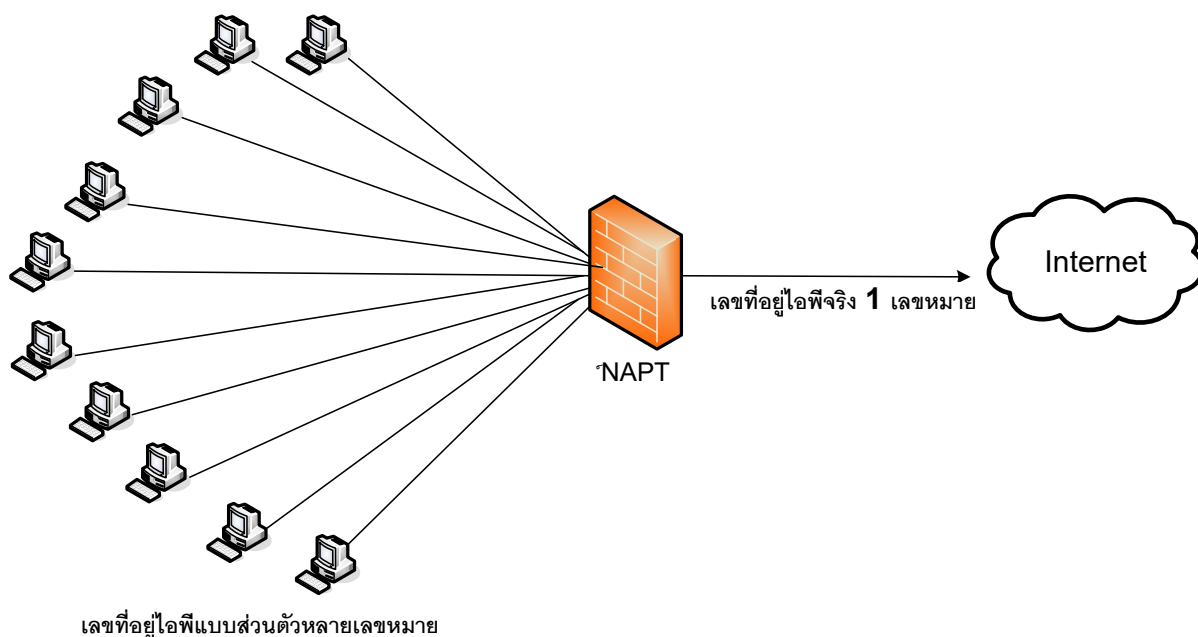


รูป 5.7 แสดงการเชื่อมต่อ TCP/IP พื้นฐานของการ NAT

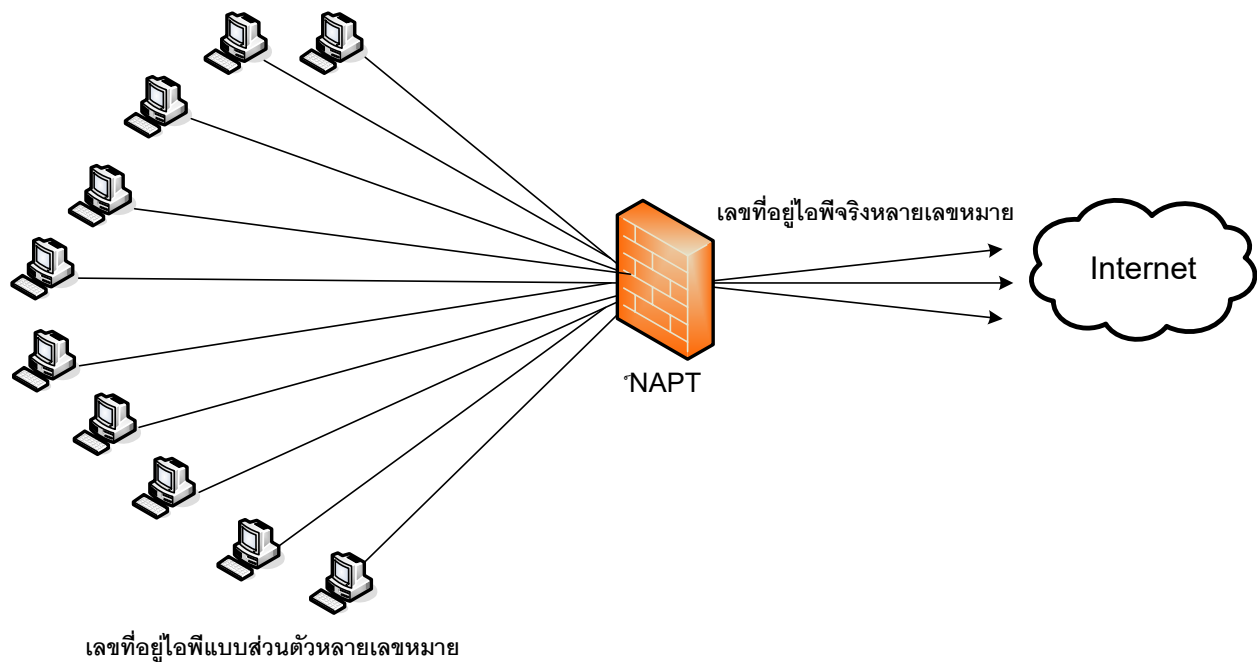
รูป 5.7 แสดงให้เห็นถึงแพ็กเก็ตที่ผ่านการ NAT ที่มีการแปลงทั้งเลขที่อยู่ไอพีและพอร์ตของต้นทางในที่นี้คือ 192.168.1.10:10554 ซึ่งแสดงให้เห็นว่าการเชื่อมต่อที่เกิดขึ้นระหว่างภายในกับภายนอกนั้นเป็นอิสระต่อกัน และสัมพันธ์โดยอาศัยตารางการ NAT เท่านั้น เมื่อตรวจสอบการเชื่อมต่อที่เกิดขึ้นจริงที่เกิดขึ้นบนโฮสต์ทั้งคู่

โดยพิจารณาจากเลขที่อยู่ไอพีก็จะไม่พบว่ามี การเชื่อมต่อที่ตรงกันแต่อย่างใด แต่โฮสต์ทั้งคู่ก็ยัง สามารถติดต่อสื่อสารกันได้ตามปกติ ในการ NAT นั้น ข้อมูลในตารางจะต้องมีค่าของพอร์ตที่ทำการแปลงรวมอยู่ด้วย เพื่อใช้ในการแปลงแพ็กเก็ตที่ตอบกลับมาจะสื่อสารกันได้อย่างถูกต้อง ในกรณีเช่นนี้ ไฟร์วอลล์จำเป็นต้องทำงาน เพิ่มขึ้นนอกเหนือจากการประมวลผลตามปกติ เพราะต้องอ่านค่าจากตารางมากขึ้น และทำการคำนวณ Checksum ที่มีขนาดใหญ่ขึ้น ซึ่งหากการสื่อสารข้อมูลมีปริมาณมากย่อมส่งผลกระทบต่อประสิทธิภาพของไฟร์วอลล์ได้

อย่างไรก็ตาม การ NAT แบบกลุ่มต่อหนึ่ง (Many-to-one) ดังแสดงในรูป 5.8 นั้น สามารถใช้ได้กับทราฟฟิกแบบขาออก (Outbound traffic) เท่านั้น ไม่สามารถใช้ได้กับทราฟฟิกแบบขาเข้า (Inbound traffic) หมายความว่าใช้ได้เฉพาะกรณีที่โฮสต์ภายในเป็นลูกข่ายเรียกใช้บริการจากแม่ข่ายที่อยู่ภายนอกบนอินเทอร์เน็ต เท่านั้น ไม่สามารถนำมาใช้ในกรณีที่โฮสต์ภายในที่ต้องการเปิดบริการให้เป็นแม่ข่ายได้ เนื่องจากการรองรับการเข้าถึงแบบขาเข้า (Inbound access) นั้นจะไม่สามารถทำการมัลติเพล็กซ์พอร์ตแม่ข่ายได้ เพราะพอร์ตของแม่ข่าย ที่ให้บริการนั้นต้องคงที่ ไม่สามารถสลับเป็นพอร์ตอื่นเหมือนกับโฮสต์ทั่วไปที่มีการใช้งานประเภทการเข้าถึงแบบขาออก (Outbound access) ได้



รูป 5.8 มุมมองเชิงตรรกะของการ NAT แบบกลุ่มต่อหนึ่ง (Many-to-one)



รูป 5.9 มุมมองเชิงตรรกะของการ NAPT แบบกลุ่มต่อกลุ่ม (Many-to-many)

การ NAPT แบบหนึ่งต่อกลุ่ม (One-to-many) สามารถพัฒนาเพิ่มความสามารถในการให้บริการ โดยที่มีเลขที่อยู่ไอพีจริงมากกว่าหนึ่งเลขหมายได้ ทำให้เป็นการ NAPT แบบกลุ่มต่อกลุ่ม (Many-to-many) ดังแสดงในภาพที่ 4-29 คือมีเลขที่อยู่ไอพีแบบส่วนตัวจำนวนมาก ในขณะเดียวกันก็มีเลขที่อยู่ไอพีสาธารณะในการใช้งานหลายเลขหมาย ได้เช่นกัน ในกรณีเช่นนี้ กระบวนการ NAPT ยิ่งเพิ่มความซับซ้อนยิ่งขึ้น วิธีการจับคู่ระหว่างเลขที่อยู่ไอพีแบบส่วนตัวกับสาธารณะและพอร์ตต่างๆ ที่ใช้จัดสรรให้แต่ละการเชื่อมต่อก็ยิ่งเพิ่มความซับซ้อนมากขึ้นด้วย ซึ่งพิจารณาในแง่ความปลอดภัยแล้ว การวิเคราะห์โครงสร้างเลขที่และภูมิสถานะของเครือข่ายโดยผู้บุกรุกภายนอกย่อมกระทำได้ยากลำบากยิ่งขึ้นด้วย

5.4.7 ปัญหาและข้อจำกัด

โฮสต์ที่อยู่เบื้องหลังเราเตอร์ที่รองรับ NAT ไม่มีการเชื่อมต่อแบบ end-to-end และไม่สามารถเข้าร่วมในโปรโตคอลอินเทอร์เน็ตบางประเภทได้ บริการที่จำเป็นต้องมีการเริ่มต้น การเชื่อมต่อ TCP จากเครือข่ายภายนอก หรือที่ใช้โปรโตคอลแบบ stateless เช่น โปรโตคอลที่ใช้ UDP อาจหยุดชะงักได้ หากเราเตอร์ NAT ไม่พยายามรองรับโปรโตคอลดังกล่าวโดยเฉพาะ แพ็กเก็ตขาเข้าจะไม่สามารถไปถึงปลายทางได้ บางโปรโตคอลสามารถรองรับ NAT หนึ่งอินสแตนซ์ระหว่างโฮสต์ที่เข้าร่วม (เช่น FTP แบบ "passive mode") บางครั้งอาจต้องใช้เกตเวย์ระดับแอปพลิเคชัน แต่จะล้มเหลวเมื่อทั้งสองระบบถูกแยกออกจากอินเทอร์เน็ตด้วย NAT การใช้ NAT

ยังทำให้โปรโตคอลแบบทันเนลเช่น IPsec มีความซับซ้อน เนื่องจาก NAT จะแก้ไขค่าในส่วนหัว ซึ่งกระบวนการตรวจสอบความสมบูรณ์ของ IPsec และโปรโตคอลแบบทันเนลอื่นๆ

การเชื่อมต่อแบบ End-to-end เป็นหลักการสำคัญของอินเทอร์เน็ต ซึ่งได้รับการสนับสนุนจากคณะกรรมการสถาปัตยกรรมอินเทอร์เน็ต (Internet Architecture Board: IAB) เอกสารสถาปัตยกรรมอินเทอร์เน็ตในปัจจุบันระบุว่า NAT ละเมิดหลักการ End-to-end แต่ NAT ก็มีบทบาทที่ถูกต้องในการออกแบบอย่างรอบคอบ

การใช้งานที่ติดตามเฉพาะพอร์ตอาจหมดลงอย่างรวดเร็วเนื่องจากแอปพลิเคชันภายในที่ใช้การเชื่อมต่อพร้อมกันหลายรายการ เช่น คำขอ HTTP สำหรับเว็บเพจที่มีวัตถุประเภทฝังตัวจำนวนมาก ปัญหานี้สามารถบรรเทาได้ด้วยการติดตามที่อยู่ IP ปลายทาง นอกเหนือจากพอร์ต ซึ่งหมายถึงการใช้พอร์ตประจำที่ (Local Port) เดียวกับโฮสต์ระยะไกล (Remote Ports) หลายเครื่อง การติดตามเพิ่มเติมนี้จะเพิ่มความซับซ้อนในการใช้งานและทรัพยากรการประมวลผลที่อุปกรณ์แปลง

เนื่องจากเลขที่อยู่ภายในทั้งหมดถูกปิดไว้ภายใต้เลขที่อยู่สาธารณะที่อยู่เดียว จึงเป็นไปได้ที่โฮสต์ภายนอกจะเริ่มต้นการเชื่อมต่อกับโฮสต์ภายในโดยตรง แอปพลิเคชันต่างๆ เช่น VoIP, การประชุมทางวิดีโอ และแอปพลิเคชันแบบเพียร์ทูเพียร์อื่นๆ ต้องใช้ เทคนิค NAT traversal จึงจะทำงานได้

NAT เป็นระบบอำพรางเครือข่ายที่ช่วยลดความเสี่ยงด้านความมั่นคงปลอดภัยขององค์กรโดยการซ่อนเครือข่ายภายในจากเครือข่ายสาธารณะ โดยค่าเริ่มต้น IP สาธารณะภายนอกจะไม่สามารถสื่อสารกับโฮสต์ IP ส่วนตัวภายในได้หากไม่มีการแปลง NAT ที่มีอยู่แล้ว ดังนั้น NAT จึงแยกเครือข่ายสาธารณะและเครือข่ายส่วนตัวออกจากกัน การปิดอำพรางเลขที่อยู่ของโฮสต์ภายในเครือข่ายขององค์กรเรา จะช่วยลดความเสี่ยงจากการถูกโจมตีจากผู้ประสงค์ร้ายได้โดยตรง นอกจากนี้ องค์กรที่ใช้ NAT สามารถติดตั้งและดูแลรักษาระบบรักษาความปลอดภัยแบบหลายชั้นเพื่อป้องกันภัยคุกคามและป้องกันกิจกรรมที่เป็นอันตราย

5.5 สรุปบท

เนื้อหาในบทนี้อธิบายหลักการและข้อจำกัดของ NAT/NAPT ที่ช่วยอำพรางเครือข่ายและลดความเสี่ยงด้านความมั่นคงปลอดภัยขององค์กร โดยการซ่อนเลขที่อยู่ IP ภายในจากเครือข่ายสาธารณะ ทั้งนี้ NAT/NAPT แม้จะเพิ่มประสิทธิภาพในการจัดการหมายเลขที่อยู่ แต่ยังมีข้อจำกัดด้านการเชื่อมต่อแบบ end-to-end และส่งผลต่อการทำงานของบางโปรโตคอล นอกจากนี้การใช้ NAT ยังเอื้อให้สามารถออกแบบระบบรักษาความปลอดภัยแบบหลายชั้นได้เพื่อป้องกันภัยคุกคามที่ซับซ้อนมากขึ้น

5.6 บทวิเคราะห์เชิงวิชาการ

เอกสารสัปดาห์ที่ 5 “ไฟร์วอลล์และระบบอำพราง (Firewall and Anonymity Systems)” วางรากฐานสำคัญเกี่ยวกับคุณลักษณะ ประเภท และข้อจำกัดของไฟร์วอลล์ ตลอดจนกลไก NAT/NAPT เพื่อการอำพรางและการแปลงที่อยู่เครือข่าย ซึ่งเป็นฐานความเข้าใจที่จำเป็นต่อการออกแบบสถาปัตยกรรมความมั่นคงยุคใหม่ในมหาวิทยาลัยและองค์กรไทย

1) วิวัฒน์ไฟร์วอลล์: จากการกรองแพ็กเก็ตสู่การควบคุมตามบริบทแอป

ประเด็นสำคัญในบทนี้: การแบ่ง “ยุค” ของไฟร์วอลล์—static packet filtering → application/proxy → stateful inspection → dynamic filtering → kernel proxy—ช่วยให้สามารถออกแบบเชิงเปรียบเทียบทั้งทางเทคนิคและยุทธศาสตร์ได้ชัดเจน (เช่น trade-off ระหว่างประสิทธิภาพกับความลึกของการตรวจสอบ)

มุมมองวิชาการร่วมสมัย:

- **NGFW (Next-Generation Firewall)** ไม่ใช่แค่ DPI/URL Filtering แต่คือ “การกำกับนโยบายตามแอป/ผู้ใช้/กลุ่ม” ที่ผสาน AAA และ Context (อุปกรณ์ สถานที่ เวลา ความเสี่ยง) เข้ากับกฎไฟร์วอลล์ ช่วยลดช่องว่างจากการยึดติดพอร์ต/โพรโทคอลแบบเดิม
- **ข้อจำกัดคลาสสิกยังคงอยู่:** หากแพ็กเก็ต “ถูกกฎ” มาตั้งแต่ต้น ไฟร์วอลล์เพียงด่านหน้าก็ปล่อยผ่าน (rule-based blind spot) การออกแบบจึงต้องพึ่ง “หลายชั้น” (defense-in-depth) และการตรวจจับ/ตอบสนอง (detect/response) ที่พึ่งกฎเกณฑ์และพฤติกรรม

2) NAT/NAPT: ประสิทธิภาพด้านหมายเลขที่อยู่ ≠ ความปลอดภัยโดยเนื้อแท้

ประเด็นสำคัญในบทนี้: NAT/NAPT อธิบายกลไก mapping, ตาราง NAT, และ multiplex พอร์ต เพื่อให้โฮสต์จำนวนมากใช้งาน IP สาธารณะจำกัดได้อย่างมีประสิทธิภาพ พร้อมย้ำทั้งข้อดี (ซ่อนโทโพโลยี ลดพื้นผิวโจมตี) และข้อจำกัด (รบกวน end-to-end, แก้ไขปัญหาซับซ้อน, แอปบางชนิดทำงานลำบาก)

มุมมองวิชาการร่วมสมัย:

- **NAT ≠ Firewall:** “การซ่อนที่อยู่” เป็นเพียงผลพลอยได้ ไม่ใช่การบังคับใช้นโยบายความปลอดภัย จำเป็นต้องจับคู่กับ stateful policy และ การตรวจจับภัยคุกคาม
- **NAT traversal** (เช่น STUN/TURN/ICE) และโพรโทคอลสมัยใหม่ (QUIC/HTTP/3, DoH/DoT) ทำให้การตรวจสอบแบบพอร์ต/โพรโทคอลยิ่งมีความท้าทาย

- **บริบท IPv6:** เมื่อองค์กรขยับสู่ IPv6 ความจำเป็นด้าน “ประหยัด IP” ของ NAT ลดลง ขณะที่ความมั่นคงควรย้ายศูนย์กลางไปที่ การยืนยันตัวตน/อุปกรณ์/บริบท มากกว่าพึ่งการอำพราง

3) แนวโน้มยุค Zero Trust, SASE และ Cloud-Native Networking

เพื่อสะท้อนความก้าวหน้าทางวิชาการในการเรียนรู้ ควรเน้นการบูรณาการไฟร์วอลล์-NAT กับสถาปัตยกรรมรุ่นใหม่ ดังนี้

- **Zero Trust Network Access (ZTNA):** นโยบาย “ไม่เชื่อใจโดยปริยาย” ตรวจสอบต่อเนื่องตามตัวตน-อุปกรณ์-บริบท-ความเสี่ยง; ใช้ **micro-segmentation** แยกโซนวิจัย/งานธุรการ/ห้องเรียน/OT; กำกับด้วย **policy-as-code** (เช่น OPA/Rego) เพื่อความตรวจสอบได้และ CI/CD
- **SASE/SSE & FWaaS:** เคลื่อนขีดความสามารถไฟร์วอลล์ไปยัง edge ของผู้ใช้และแอป คลุม BYOD/นอกสถานที่ ลดความพึ่งพา “กำแพงศูนย์กลาง” เพียงจุดเดียว
- **Kubernetes & eBPF:** ใช้ **NetworkPolicy** คุมการสื่อสารระหว่างพ็อด/เนมสเปซ พร้อมไฟร์วอลล์ระดับโฮสต์ด้วย **eBPF/XDP** (เช่นนโยบาย L3-L7 ที่ผูกกับตัวตนเซอร์วิสมากกว่าพอร์ตดิบ) สอดรับ **service mesh (mTLS)** ที่เข้ารหัสทราฟฟิกภายในโดยปริยาย
- **TLS 1.3/ความเป็นส่วนตัว:** การถอดรหัสทราฟฟิกเพื่อ DPI ต้องชั่งน้ำหนัก **PDPA** และจริยธรรม—แนวปฏิบัติที่ปลอดภัยคือ “เลือกถอดรหัสอย่างมีเหตุผล” (selective decryption) พร้อมบันทึกเหตุผล/หลักฐานเพียงพอสำหรับการตรวจสอบ

กล่าวโดยสรุป ไฟร์วอลล์และ NAT/NAPT ยังคงเป็น “ชิ้นส่วนหลัก” แต่ไม่ใช่ “คำตอบทั้งหมด” ในโลกที่ทราฟฟิกเข้ารหัสและบริการกระจายตัว การเรียนรู้ที่ดีของบทนี้คือการสร้างความตระหนักรู้ผู้เรียนจากฐานความเข้าใจทางเทคนิคในไฟล์ ไปสู่สถาปัตยกรรม **Zero Trust/SASE/Cloud-Native** ที่วัดผลได้จริงผ่านแล็บ บันทึกหลักฐาน และการสะท้อนคิด พร้อมกรอบกฎหมายไทย (PDPA) และมาตรฐานสากล

แบบทดสอบท้ายบท

ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง NAT และ NAPT

แนวคำตอบ: NAT = แปลง IP Address ระหว่าง Private ↔ Public แบบ 1:1 หรือหลายต่อหลาย; NAPT = แปลง IP + Port (Multiplexing) ทำให้หลายเครื่องใช้ Public IP เดียวได้

ข้อ 2. อธิบายคุณสมบัติของ Stateful Inspection Firewall

แนวคำตอบ: ตรวจสอบทราฟฟิกตามสถานะเซสชัน เข้าใจความสัมพันธ์ของแพ็กเก็ต สามารถควบคุม TCP/UDP และโพรโทคอลสูงขึ้น ปลอดภัยกว่า Packet Filtering ธรรมดา

ข้อ 3. ยกตัวอย่างข้อดีและข้อจำกัดของ NAT

แนวคำตอบ: ข้อดี – ซ่อนโครงสร้างเครือข่าย, ลดความเสี่ยงจากภายนอก, ใช้ Public IP น้อย; ข้อจำกัด – ไม่รองรับ end-to-end, ปัญหา VoIP/UDP/IPSec, แก้ไข Traceback ยาก

ข้อ 4. วิเคราะห์ผลกระทบหาก Firewall ตั้งกฎ Access Control ไม่เหมาะสม

แนวคำตอบ: อาจอนุญาตทราฟฟิกอันตรายผ่านเข้ามา (Loss of Confidentiality/Integrity/Availability), หรือบล็อกบริการสำคัญที่ถูกต้อง ทำให้ผู้ใช้ทำงานไม่ได้

ข้อ 5. อธิบายการทำงานของ Proxy Firewall และประโยชน์ที่ได้

แนวคำตอบ: รับ Request จาก Client, ตรวจสอบ Policy, สร้างการเชื่อมต่อใหม่กับ Server → ป้องกัน direct access; ซ่อนโครงสร้างเครือข่าย, Content Filtering, Caching

ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. Firewall ทำหน้าที่หลักใด

ก. ตรวจสอบและควบคุมการเข้าถึงเครือข่าย

ข. สแกนหาไวรัส

ค. เข้ารหัสข้อมูลทั้งหมด

ง. จัดการ Bandwidth

เฉลย: ก

ข้อ 2. NAT มีวัตถุประสงค์หลักใด

ก. เพิ่มจำนวน Public IP

ข. แปลง IP ส่วนตัวให้ใช้งานอินเทอร์เน็ตได้

ค. ทำงานแทน Firewall

ง. ทำงานแทน Proxy Server

เฉลย: ข

ข้อ 3. NATP แตกต่างจาก NAT อย่างไร

ก. NATP แปลง IP เท่านั้น

ข. NATP แปลงทั้ง IP และ Port

ค. NATP ใช้ได้เฉพาะ IPv6

ง. NATP ใช้ได้เฉพาะ UDP

เฉลย: ข

ข้อ 4. Firewall รุ่นที่สอง (Application Layer Firewall) เรียกว่าอะไร

ก. Packet-filtering Firewall

ข. Proxy Firewall

ค. Stateful Firewall

ง. Kernel Proxy Firewall

เฉลย: ข

ข้อ 5. Firewall แบบใดตรวจสอบความสัมพันธ์ของแพ็กเก็ตในเซสชันได้

ก. Packet Filtering

ข. Proxy Firewall

ค. Stateful Inspection Firewall

ง. Kernel Proxy Firewall

เฉลย: ค

ข้อ 6. การใช้ NAT ช่วยเรื่องใดมากที่สุด

ก. ป้องกัน SQL Injection

ข. ลดจำนวน Public IP ที่ต้องใช้

ค. ตรวจสอบพฤติกรรมผิดปกติ

ง. พื้นฟูระบบหลังภัยพิบัติ

เฉลย: ข

ข้อ 7. ปัญหาสำคัญของ NAT คือข้อใด

ก. ไม่รองรับ End-to-End Communication

ข. ทำให้ Firewall หายไป

ค. ใช้ได้เฉพาะกับ TCP เท่านั้น

ง. ไม่สามารถทำงานร่วมกับ Firewall

เฉลย: ก

ข้อ 8. การใช้ Proxy Firewall มีข้อดีใด

ก. เพิ่มความเร็วระบบเสมอ

ข. ป้องกัน direct access และทำ Caching ได้

ค. ใช้ IP ส่วนตัวแทน Public IP ได้

ง. ไม่ต้องตั้งค่า Security Policy

เฉลย: ข

ข้อ 9. การทำงานแบบ Many-to-one NAT ใช้กับกรณีใด

ก. Outbound Traffic

ข. Inbound Traffic

ค. VPN Tunnel

ง. Proxy Firewall

เฉลย: ก

ข้อ 10. Firewall รุ่นที่ 5 (Kernel Proxy Firewall) มีคุณสมบัติใด

ก. ตรวจสอบแค่ IP Address

ข. ตรวจสอบได้หลายเลเยอร์ที่ Kernel

ค. ทำงานได้เฉพาะ TCP

ง. ใช้ได้เฉพาะซอฟต์แวร์เท่านั้น

เฉลย: ข

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิริเชษฐ์ โพธิ์ศรีบุญ. (ม.ป.ป.). *ไฟร์วอลล์และระบบอำพราง (Firewall and Anonymity Systems)*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Egevang, K., & Francis, P. (1994). The IP Network Address Translator (NAT) (RFC 1631). IETF.

ISO/IEC. (2015). ISO/IEC 27033-1: Network security—Part 1: Overview and concepts. International Organization for Standardization.

NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., & Lear, E. (1996). Address Allocation for Private Internets (RFC 1918). IETF.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). NIST.

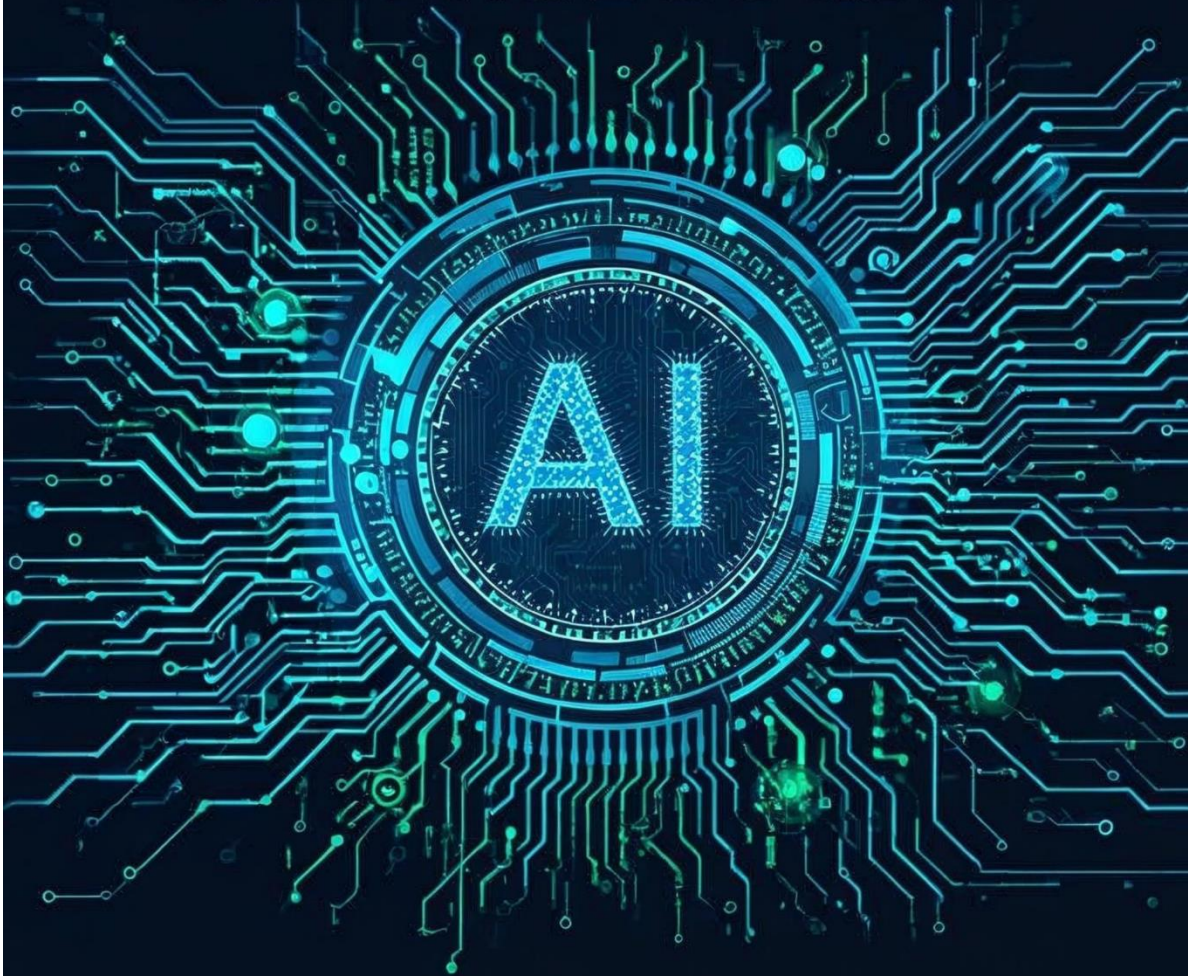
Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev. 1). NIST.

Srisuresh, P., & Holdrege, M. (1999). IP Network Address Translator (NAT) Terminology and Considerations (RFC 2663). IETF.

บทที่ 6

ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน
Virtual Private Network

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์
CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ

บทที่ 6 ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน (Virtual Private Network)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

- ให้นักศึกษามีความรู้เกี่ยวกับระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน หรือ VPN
- เข้าใจหลักการทำงานและประเภทของ VPN
- เข้าใจหลักการทำงานของโพรโทคอลที่ใช้ร่วมกับ VPN
- เข้าใจการนำ VPN ไปใช้เป็นระบบประกันความมั่นคงปลอดภัยระดับสูง

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อสิ้นสุดการเรียนรู้ในสัปดาห์นี้ นักศึกษาจะสามารถ:

- อธิบายเกี่ยวกับระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน หรือ VPN ได้อย่างถูกต้อง
- อธิบายหลักการทำงานและประเภทของ VPN ได้อย่างถูกต้อง
- อธิบายหลักการทำงานของโพรโทคอลที่ใช้ร่วมกับ VPN ได้อย่างถูกต้อง
- อธิบายการนำ VPN ไปใช้เป็นระบบประกันความมั่นคงปลอดภัยระดับสูงได้อย่างถูกต้อง

3. หัวข้อเนื้อหา:

6.1 ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน

6.1.1 ความหมายของเครือข่ายส่วนตัวเสมือน

6.1.2 คุณลักษณะของเครือข่ายส่วนตัวและเครือข่ายสาธารณะ

6.1.3 หลักการทำงานของ VPN

6.1.4 ประเภทการใช้งาน VPN

6.2 โพรโทคอลความปลอดภัยที่ใช้กับ VPN

6.2.1 PPTP (Point-to-Point tunneling protocol)

6.2.2 L2F (Layer-2 Forwarding)

6.2.3 L2TP (Layer-2 tunneling protocol)

6.2.4 IPSec (IP Security protocol)

6.2.4 ประโยชน์ของการใช้ VPN

4. กิจกรรมการเรียนรู้ในชั้นเรียน

กรณีศึกษา: บริษัท *RMUTT ThaiHealth Data Center* ต้องให้พนักงานเข้าถึงข้อมูลผู้ป่วยจากภายนอกสำนักงานผ่านอินเทอร์เน็ต

- ผู้บริหารตัดสินใจติดตั้งระบบ VPN (IPSec VPN) เพื่อความปลอดภัย
- แต่มีปัญหา: พนักงานบางคนใช้ Wi-Fi สาธารณะ, มีข้อกังวลเรื่องการจัดการกุญแจ (IKE), และมีคำถามเรื่องเลือก Remote Access VPN หรือ Site-to-Site VPN
- ผู้ดูแลระบบต้องตัดสินใจเลือกโพรโทคอลที่เหมาะสม (PPTP, L2TP, IPSec)

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4–5 คน):

- วิเคราะห์ความเสี่ยงที่เกิดจากการเข้าถึงเครือข่ายผ่าน Wi-Fi สาธารณะ
- ระบุประเภท VPN ที่เหมาะสม (Remote Access, Intranet/Extranet VPN)
- เปรียบเทียบโพรโทคอล PPTP, L2TP, IPSec ว่ามีข้อดี-ข้อจำกัดอย่างไร
- เสนอแผนการรักษาความปลอดภัย (การเข้ารหัส, การจัดการกุญแจ, การฝึกอบรมผู้ใช้)
- สรุปเป็นแผนการนำเสนอและรายงานกลุ่ม

ประเด็นการเรียนรู้ที่สำคัญ:

- ความแตกต่างระหว่างเครือข่ายส่วนตัวและสาธารณะ
- หลักการทำงานของ VPN (Tunneling, Encryption, Hide IP)

- ประเภทการใช้งาน VPN: Remote Access, Intranet, Extranet
- โพรโทคอล VPN: PPTP, L2F, L2TP, IPSec และการใช้งานจริง
- ประโยชน์และข้อจำกัดของ VPN ในองค์กร

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์เชิงวิชาการ (30)	ครบถ้วน อ้างอิง VPN/Protocol ได้ถูกต้อง	ครบ 70–80%	ครบเพียงบางส่วน	ไม่ถูกต้อง
การเชื่อมโยงกับกรณีศึกษา (25)	วิเคราะห์และเลือก VPN ได้ สอดคล้องปัญหา	เลือกได้เหมาะสมบางส่วน	ยังไม่ชัดเจน	ไม่สอดคล้อง
การออกแบบแนวทางแก้ไข (30)	เสนอแผนครอบคลุมทั้งเทคนิคและนโยบาย	เสนอแนวทางบางส่วน	แนวทางยังไม่ลึก	ไม่มีข้อเสนอ
การนำเสนอ (15)	ชัดเจน ใช้สื่อประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

6. ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน

ในบทนี้จะทำความเข้าใจเกี่ยวกับระบบประกันความมั่นคงปลอดภัยระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน หรือ VPN โดยเนื้อหาจะอธิบายถึงสาระสำคัญของคุณลักษณะของเครือข่ายส่วนตัวและเครือข่ายสาธารณะ, ประเภทของการใช้งาน VPN, ความปลอดภัยของ VPN และประโยชน์ที่ได้จาก VPN

โดยทั่วไป การสื่อสารข้อมูลผ่านเครือข่ายอินเทอร์เน็ตถือว่าการสื่อสารผ่านช่องทางที่ไม่ปลอดภัย จึงจำเป็นต้องอาศัยเทคโนโลยีของวิทยาการรหัสลับเข้ามาช่วยดังที่อธิบายไว้แล้วในหัวข้อที่ผ่านมา ความมั่นคงของระบบความปลอดภัยที่เรานำมาใช้ปกป้องข้อมูลที่มีการสื่อสารอยู่ภายในเครือข่ายของเราเพื่อป้องกันการโจมตีจากผู้บุกรุกนั้นย่อมมีขีดความสามารถในการรักษาความลับ, บุรณภาพ, การพิสูจน์ตัวจริง, การควบคุมการเข้าถึง, การไม่สามารถปฏิเสธความรับผิดชอบ และสภาพพร้อมใช้งาน ได้เป็นอย่างดีราบเท่าที่ข้อมูลยังสื่อสารเฉพาะภายในเครือข่ายของเรา

อย่างไรก็ตาม ในโลกของเครือข่ายนั้น เราจำเป็นต้องมีการติดต่อสื่อสารเพื่อเข้าถึงหรือแลกเปลี่ยนข้อมูลระหว่างเครือข่ายของเรากับคอมพิวเตอร์ที่อยู่บนเครือข่ายอื่นโดยผ่านเครือข่ายสาธารณะหรืออินเทอร์เน็ต ดังนั้น ความเสี่ยงต่อการถูกโจมตีต่อความปลอดภัยจึงมีสูงขึ้น เนื่องจากเราไม่สามารถปกป้องข้อมูลของเราที่สื่อสารไปในเครือข่ายสาธารณะได้เหมือนกับที่อยู่ภายในเครือข่ายของเรา และเราไม่สามารถหลีกเลี่ยงการใช้งานเครือข่ายสาธารณะเพื่อเข้าถึงทรัพยากรบนเครือข่ายของเราได้ เราจะอย่างไรจึงจะสามารถประกันว่า การสื่อสารข้อมูลผ่านเครือข่ายสาธารณะจะมีความมั่นคงเรื่องความปลอดภัยได้ไม่แตกต่างไปจากการสื่อสารภายในเครือข่ายของเราเอง

6.1 ความหมายของเครือข่ายส่วนตัวเสมือน

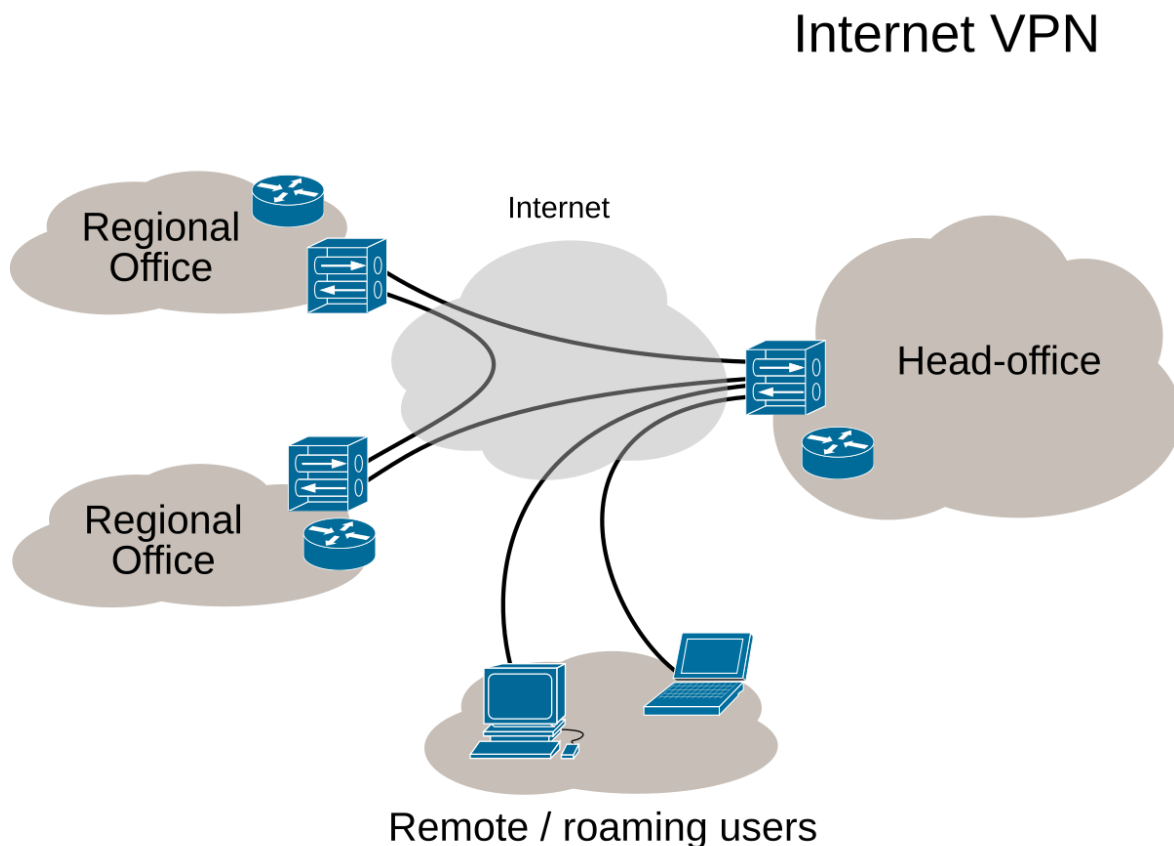
เครือข่ายส่วนตัวเสมือน (Virtual Private Network) หรือมักเรียกว่า VPN หมายถึง เครือข่ายสาธารณะ (Public network) ที่สามารถใช้งานได้และมีคุณสมบัติด้านความปลอดภัยเช่นเดียวกับการใช้เครือข่ายส่วนตัว (Private network) ที่อนุญาตให้มีการใช้งานเฉพาะภายในองค์กรเท่านั้น

VPN คือเทคโนโลยีที่สร้าง “อุโมงค์” ที่เข้ารหัสข้อมูลเพื่อการเชื่อมต่อที่ปลอดภัยผ่านเครือข่ายสาธารณะ เช่นอินเทอร์เน็ต ช่วยปกป้องความเป็นส่วนตัวโดยการซ่อน IP ของผู้ใช้ และป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

VPN คือ การเชื่อมต่ออินเทอร์เน็ตที่เข้ารหัสจากอุปกรณ์หนึ่งไปยังเครือข่าย การเชื่อมต่อที่เข้ารหัสนี้ช่วยให้มั่นใจได้ว่าข้อมูลสำคัญจะถูกส่งอย่างปลอดภัย ช่วยป้องกันบุคคลที่ไม่ได้รับอนุญาตดักฟังข้อมูล และช่วยให้ผู้ใช้สามารถทำงานจากระยะไกลได้ เทคโนโลยี VPN ถูกนำมาใช้อย่างแพร่หลายในสภาพแวดล้อมองค์กร

1. [*"virtual private network"*](#). NIST Computer Security Resource Center Glossary. [Archived](#) from the original on 2 January 2023. Retrieved 2 January 2023.
2. [*"What Is a VPN? - Virtual Private Network"*](#). Cisco. [Archived](#) from the original on 31 December 2021. Retrieved 5 September 2021.

VPN คือสถาปัตยกรรมเครือข่ายสำหรับขยายเครือข่ายส่วนตัวเสมือน (เช่นเครือข่ายคอมพิวเตอร์ใดๆ ที่ไม่ใช่อินเทอร์เน็ตสาธารณะ) ข้ามเครือข่ายอื่นหนึ่งเครือข่ายหรือหลายเครือข่ายที่ไม่น่าเชื่อถือ (เนื่องจากไม่ได้รับการควบคุมโดยหน่วยงานที่ต้องการนำ VPN มาใช้) หรือจำเป็นต้องแยกออกจากกัน (จึงทำให้เครือข่ายที่ต่ำกว่ามองไม่เห็นหรือไม่สามารถใช้งานได้โดยตรง) รูป 6.1 แสดงการเชื่อมต่อผ่านอินเทอร์เน็ตสาธารณะระหว่างโฮสต์ต่างๆ โดยใช้ VPN



รูป 6.1 เครือข่ายส่วนตัวเสมือน หรือ VPN

(ที่มา : Ludovic.ferre (talk · contribs) - Own work, CC BY-SA 4.0,
<https://commons.wikimedia.org/w/index.php?curid=10101288>)

VPN เป็นเทคโนโลยีที่ช่วยให้ผู้ใช้สามารถใช้งานอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะได้มีความปลอดภัยและระดับการป้องกันข้อมูลเช่นเดียวกับเครือข่ายองค์กรนั่นเอง โดยปกติในการใช้งานจริง VPN มักถูกใช้ร่วมกับไฟร์วอลล์ (Firewall) แต่ VPN มีคุณลักษณะการใช้งาน หน้าที และประโยชน์แตกต่างไปจากไฟร์วอลล์ ในที่นี้จะอธิบายเฉพาะ VPN เท่านั้น

VPN สร้างการเชื่อมต่อเครือข่ายส่วนตัวระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต โดยเราใช้ VPN เพื่อส่งข้อมูลอย่างปลอดภัยและไม่เปิดเผยตัวตนผ่านเครือข่ายสาธารณะ ซึ่งจะทำงานโดยปกติที่อยู่ IP ของผู้ใช้และเข้ารหัสข้อมูล เพื่อให้บุคคลที่ไม่ได้รับอนุญาตที่ได้รับข้อมูลดังกล่าวไม่สามารถอ่านได้

6.2 คุณลักษณะของเครือข่ายส่วนตัวและเครือข่ายสาธารณะ

6.2.1 เครือข่ายส่วนตัว (Private Network)

เป็นเครือข่ายที่ถูกใช้งานเฉพาะภายในองค์กรเท่านั้น ไม่อนุญาตให้บุคคลภายนอกเข้ามาใช้งาน เช่น เครือข่ายอินเทอร์เน็ตขององค์กรที่อนุญาตให้ใช้งานได้เฉพาะพนักงานขององค์กรเท่านั้น หรือเครือข่ายของมหาวิทยาลัยที่อนุญาตให้ใช้งานได้เฉพาะอาจารย์ เจ้าหน้าที่ และนักศึกษาของมหาวิทยาลัยเท่านั้น เครือข่ายส่วนตัว เช่นนี้จึงมีแพร่หลายอยู่ทั่วไป ดังนั้น เครือข่ายส่วนตัว จึงมีคุณลักษณะดังต่อไปนี้

- 1) มีอาณาบริเวณที่มีการป้องกันทางกายภาพ ถือเป็นคุณลักษณะพื้นฐานของทุกเครือข่ายที่แต่ละองค์กรมีมีข่ายการสื่อสารที่ครอบคลุมเฉพาะภายในพื้นที่ของตนเองเท่านั้น อย่างเช่น มีสายสื่อสารครอบคลุมเฉพาะภายในองค์กรหรือมหาวิทยาลัย สำหรับในกรณีที่องค์กรนั้นใช้การสื่อสารแบบไร้สาย (Wireless) ก็จะหมายถึงมีพื้นที่ทำการ (Coverage area) ครอบคลุมภายในบริเวณที่กำหนดไว้เท่านั้น ไม่อนุญาตให้บุคคลภายนอกเข้ามาใช้งาน หากบุคคลภายนอกจะเข้ามาใช้งานก็จำเป็นต้องเข้ามาขอเชื่อมต่อเข้ากับเครือข่ายส่วนตัว และอนุญาตให้สามารถเข้าใช้งานเครือข่ายส่วนตัวนี้ จึงจะสามารถใช้งานได้ ดังนั้น การสื่อสารย่อมทั้งหมดย่อมอยู่ภายใต้การควบคุมของเจ้าของเครือข่ายโดยสมบูรณ์
- 2) บุคคลที่สามารถใช้งานย่อมเป็นผู้ที่ได้รับอนุญาตให้สามารถใช้งานได้ เนื่องจาก บุคคลที่จะใช้งานภายในเครือข่ายส่วนตัวจะต้องได้รับอนุญาตจากผู้ดูแลเครือข่ายจึงจะสามารถใช้งานได้ นอกจากนั้น มีขอบเขต สิทธิ เวลา และระดับของการใช้งานเฉพาะเท่าที่ได้รับอนุญาตเท่านั้น ดังนั้น การควบคุม ติดตาม และตรวจสอบสภาพการใช้งานจึงมีความรัดกุมน่าเชื่อถือได้ จึงมีความปลอดภัยสูง

- 3) ข้อมูลและทรัพยากรที่ถูกเก็บและใช้งานอยู่ภายในเครือข่ายส่วนตัวนั้น มักเป็นข้อมูลที่เป็นความลับ มีความสำคัญสูงต่อองค์กร เพราะมีไว้เพื่อการใช้งานภายในองค์กรเท่านั้น
- 4) การสื่อสารภายในเครือข่ายส่วนตัวมีความน่าเชื่อถือได้สูง และความเสี่ยงที่ข้อมูลจะรั่วไหลออกไปสู่ภายนอกต่ำ เนื่องจากเป็นเครือข่ายที่มีอาณาบริเวณทางกายภาพที่จำกัดแน่นอน การควบคุมผู้ใช้ เส้นทางสื่อสารและการกระจายของข้อมูลสามารถทำได้อย่างรัดกุม

6.2.2 เครือข่ายสาธารณะ (Public Network)

เครือข่ายสาธารณะคือเครือข่ายที่ทุกคนมีสิทธิเข้าถึงและใช้งานได้ ในที่นี้หมายถึงเครือข่ายอินเทอร์เน็ตนั่นเอง ซึ่งมีคุณลักษณะที่ตรงข้ามกับเครือข่ายส่วนตัวดังต่อไปนี้

- 1) ไม่มีขอบเขตจำกัดทางกายภาพ สามารถเชื่อมต่อได้จากทุกที่ ทุกเวลา เมื่อผู้ใช้เชื่อมต่อได้ก็สามารถติดต่อกับเครื่องแม่ข่ายได้ทันทีไม่ว่าเครื่องแม่ข่ายนั้นจะตั้งอยู่ ณ สถานที่แห่งใดก็ตาม ในทำนองเดียวกัน ในขณะที่เรากำลังเชื่อมต่ออยู่กับเครือข่ายสาธารณะอยู่นั้น โฮสต์ทุกโฮสต์ทั่วโลกก็สามารถติดต่อสื่อสารกับโฮสต์ของเราได้ตลอดเวลาเช่นเดียวกัน
- 2) การควบคุมและจำแนกผู้ใช้เป็นไปได้อาก บุคคลที่ใช้งานอยู่บนอินเทอร์เน็ตนั้นอาจรู้จักหรือไม่รู้จักกันก็ได้ ไม่สามารถยืนยันตัวตนแท้จริงของผู้ใช้ตัวอย่างเช่น เมื่อเรามีแม่ข่ายเปิดให้บริการเว็บ เราก็ไม่สามารถระบุได้เลยว่าใคร อยู่ที่ไหนเข้ามาเปิดดูหน้าเว็บของเราบ้าง ทุกคนสามารถเข้าถึงและใช้งานได้จำนวนสูงสุดเท่าที่องค์กรจะมีไว้ให้บริการไม่ว่าจะเป็นช่องทางหรือทรัพยากรต่างๆ บนแม่ข่าย
- 3) มีความเสี่ยงด้านความปลอดภัยสูง ดังคุณลักษณะข้อ 1 และ 2 เนื่องจากผู้ดูแลเครือข่ายจะไม่มีทางทราบได้เลยว่า ผู้ที่เข้ามาเปิดดูหน้าเว็บของเรานั้นจะเป็นผู้ใช้ปกติหรือผู้ประสงค์ร้าย
- 4) ไม่สามารถควบคุมเส้นทางการสื่อสารข้อมูลได้ คุณสมบัติข้อหนึ่งของโปรโตคอล TCP/IP ที่ใช้สำหรับสื่อสารกันบนเครือข่ายอินเทอร์เน็ตนั้น คือการรับประกันว่า หากเราส่งข้อมูลไปแล้วจะได้รับการยืนยันว่าข้อมูลได้ถึงปลายทางแล้วหรือไม่ แต่โปรโตคอลดังกล่าวนี้ไม่รับประกันว่าข้อมูลที่ส่งไปนั้นจะไม่รั่วไหลไปในระหว่างทาง ข้อมูลที่ส่งผ่านไบนเครือข่ายอินเทอร์เน็ตจะถูกแบ่งออกเป็นชิ้นเล็กๆ มีกลไกในการกระจายข้อมูลทั้งหมดออกไปเป็นทอดๆ ไม่อาจกำหนดเจาะจงว่าจะให้วิ่งไปในเส้นทางใด และเส้นทางที่ข้อมูลวิ่งไปนั้นไม่อยู่ในความควบคุมของผู้ส่งและผู้รับ จึงไม่มีหลักประกันว่าข้อมูลจะไม่ถูกดักอ่านในระหว่างทาง ดังนั้น การสื่อสารข้อมูลผ่านเครือข่ายสาธารณะเช่นนี้จึงถือว่าไม่มีความปลอดภัย

จะพบว่า เครือข่ายสาธารณะหรืออินเทอร์เน็ตนั้นมีปัญหาเรื่องความมั่นคงด้านความปลอดภัยอยู่ แต่ในปัจจุบันเราไม่สามารถปฏิเสธการเชื่อมต่อเข้ากับอินเทอร์เน็ตได้ เพราะความแพร่หลายของการใช้งานและอาณานิคมที่ครอบคลุมไปทั่วโลกไม่มีขอบเขตจำกัด ดังนั้น แม้จะตระหนักถึงความเสี่ยงด้านความปลอดภัยที่มาพร้อมกับการที่เครือข่ายส่วนตัวต้องเชื่อมต่อเข้ากับอินเทอร์เน็ตก็ตาม แต่เมื่อพิจารณาในแง่ประโยชน์แล้ว เราไม่สามารถหลีกเลี่ยงได้เลย ทำอย่างไรจึงจะสามารถใช้ประโยชน์จากเครือข่ายสาธารณะในขณะที่ยังคงสามารถประกันถึงความมั่นคงด้านความปลอดภัยอยู่ได้เมื่อมีการเชื่อมต่อเข้ากับเครือข่ายส่วนตัว VPN จึงเป็นคำตอบ VPN เป็นเทคโนโลยีที่จะทำให้เราสามารถใช้งานอินเทอร์เน็ตได้เหมือนกับเป็นเครือข่ายส่วนตัว ที่ยังคงคุณสมบัติที่ดีด้านความปลอดภัยเหมือนกับใช้เครือข่ายส่วนตัว ในขณะที่ได้ขจัดข้อจำกัดของอินเทอร์เน็ตออกไปได้ด้วย

6.2.3 หลักการทำงานของ VPN

การเชื่อมต่อ VPN จะเปลี่ยนเส้นทางแพคเกจข้อมูลจากเครื่องของคุณไปยังเซิร์ฟเวอร์ระยะไกลอื่นก่อนที่จะส่งไปยังบุคคลที่สามผ่านทางอินเทอร์เน็ต โดยหลักการสำคัญที่อยู่เบื้องหลังเทคโนโลยี VPN ได้แก่

โพรโทคอลช่องทางการเชื่อมต่อ:

เครือข่ายส่วนตัวเสมือนจะสร้างช่องทางการเชื่อมต่อข้อมูลที่ปลอดภัยระหว่างเครื่องในระบบของผู้ใช้กับเซิร์ฟเวอร์ VPN อื่นในตำแหน่งที่ตั้งที่อยู่ห่างออกไปหลายพันไมล์ เมื่อผู้ใช้ออนไลน์ เซิร์ฟเวอร์ VPN นี้จะกลายเป็นต้นทางข้อมูลทั้งหมดของผู้ใช้ ผู้ให้บริการอินเทอร์เน็ต (ISP) และบริษัทภายนอกอื่นๆ จึงไม่สามารถมองเห็นรายละเอียดการใช้งานอินเทอร์เน็ตของเราได้อีกต่อไป

การเข้ารหัส:

ข้อมูลที่ส่งผ่านอุโมงค์ VPN จะถูกเข้ารหัส ทำให้บุคคลที่ไม่ได้รับอนุญาตไม่สามารถอ่านหรือเข้าใจข้อมูลได้ แม้จะดักจับได้ก็ตาม โพรโทคอล VPN ต่างๆ เช่น IPSec จะแปลงข้อมูลของเราก่อนที่จะส่งผ่านช่องทางการเชื่อมต่อข้อมูล โดย IPsec เป็นชุดโพรโทคอลในการรักษาความปลอดภัยการสื่อสารผ่านอินเทอร์เน็ตโพรโทคอล (IP) โดยการรับรองความถูกต้องและเข้ารหัสแต่ละแพคเกจ IP ของสตรีมข้อมูล ซึ่งบริการ VPN จะทำหน้าที่เป็นตัวกรอง ทำให้ข้อมูลของเราไม่สามารถอ่านได้ที่ปลายทางฝั่งหนึ่งและถอดรหัสได้เฉพาะที่ปลายอีกฝั่งหนึ่งเท่านั้น ซึ่งจะช่วยป้องกันการใช้ข้อมูลส่วนบุคคลในทางที่ผิด แม้ว่าการเชื่อมต่อเครือข่ายของเราจะถูกโจมตีก็ตาม การรับส่งข้อมูลผ่านเครือข่ายจึงไม่มีความเสี่ยงที่จะถูกโจมตีอีกต่อไป และการเชื่อมต่ออินเทอร์เน็ตของเราจะปลอดภัย

สร้างอุโมงค์ที่ปลอดภัย:

VPN สร้างการเชื่อมต่อที่ปลอดภัยระหว่างอุปกรณ์ของผู้ใช้กับเซิร์ฟเวอร์ VPN หรือเครือข่ายขององค์กร

ชื่อน IP Address:

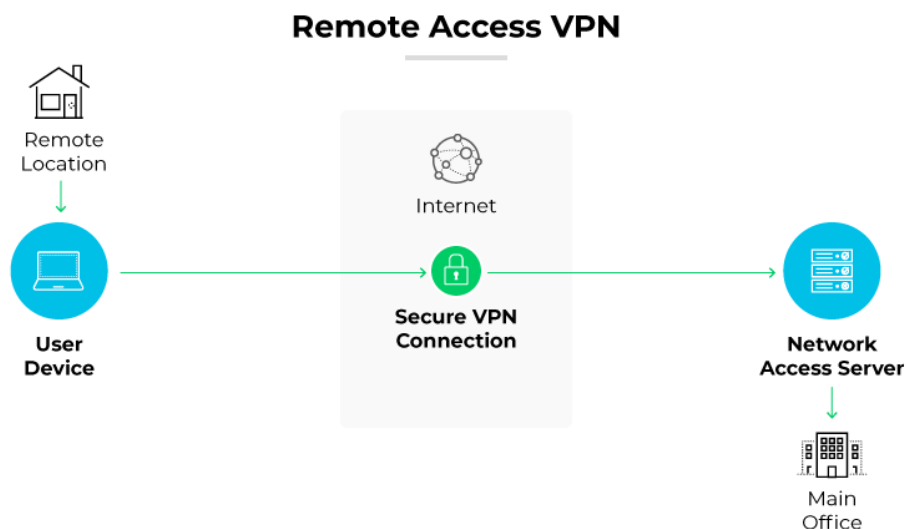
VPN จะเปลี่ยนที่อยู่ IP จริงของผู้ใช้เป็นที่อยู่ IP ของเซิร์ฟเวอร์ VPN ทำให้กิจกรรมออนไลน์ของผู้ใช้ถูกซ่อนและยากต่อการติดตาม

6.2.4 ประสิทธิภาพการใช้งาน VPN

การนำ VPN ไปใช้กับเครือข่ายองค์กรในปัจจุบันสามารถแบ่งออกได้ 3 ประเภท ได้แก่ การเข้าถึงระยะไกล, การเชื่อมต่อโฮสต์ระยะไกล และการเชื่อมต่อเครือข่ายระยะไกล

6.2.4.1 การเข้าถึงระยะไกล (Remote access VPN)

โดยปกติ เมื่อผู้ใช้ที่อยู่นอกองค์กรเช่นอยู่ที่บ้าน หากต้องการเชื่อมต่อเข้ามายังเครือข่ายของสำนักงานเพื่อใช้งานที่โฮสต์ใดโฮสต์หนึ่งจะสามารถทำได้โดยหมุนผ่านโมเด็มผ่านเครือข่ายโทรศัพท์โดยตรงไปยังหมายเลขที่สำนักงานจัดเตรียมไว้ โดยที่เครือข่ายของสำนักงานจะต้องจัดเตรียมโฮสต์ที่ทำหน้าที่เป็นแม่ข่ายให้บริการการเข้าถึงจากระยะไกล (Remote access service หรือ RAS) เพื่อรองรับการเข้าถึงจากระยะไกลได้ตลอดเวลา ดังรูป 7.2 ค่าใช้จ่ายสำหรับโทรศัพท์จึงขึ้นอยู่กับระยะทางที่ใช้งาน เช่น โทรศัพท์ภายในท้องถิ่นเดียวกันต่างจังหวัด หรือโทรศัพท์ทางไกลต่างประเทศ นอกจากนั้น ยังมีค่าใช้จ่ายที่ใช้ในการดูแลรักษาอุปกรณ์ที่ทำหน้าที่ให้บริการการเข้าถึงจากระยะไกล เช่น โมเด็มสำหรับการเข้าถึงระยะไกล (RAS modem) เครื่องแม่ข่ายที่ให้บริการระยะไกล (RAS server) เป็นต้น ซึ่งมักขึ้นอยู่กับจำนวนผู้ใช้ หากมีผู้ใช้จำนวนมากก็จะต้องเสียค่าใช้จ่ายบำรุงรักษามาก คุณภาพของการสื่อสารผ่านสายโทรศัพท์ยังต่ำและขาดเสถียรภาพ และที่สำคัญ มีความปลอดภัยต่ำ



รูป 6.2 แสดงการเข้าถึงระยะไกลโดยใช้ VPN

(ที่มา : <https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn>)

ปัจจุบัน การเข้าถึงระยะไกลมีวัตถุประสงค์เพื่อให้ผู้ใช้สามารถใช้งานโฮสต์ได้จากระยะไกล เช่น การทำงานจากระยะไกล (Remote office) นิยมเป็นการเชื่อมต่อระหว่างโฮสต์ของผู้ใช้เข้ามายังโฮสต์ในเครือข่ายส่วนตัวขององค์กรได้จากภายนอกโดยอาศัยเครือข่ายสาธารณะหรืออินเทอร์เน็ตโดยใช้ VPN เพื่อให้สามารถทำงานได้แม้จะอยู่นอกสำนักงานก็ตาม เมื่อเชื่อมต่อได้ก็เหมือนกับผู้ใช้นั้นสามารถใช้งานโฮสต์ที่อยู่ภายในเครือข่ายส่วนตัวทันที การเชื่อมต่อด้วยวิธีนี้บางทีเรียกว่า Access VPN ภาพที่ 6.3 แสดงการเข้าถึงระยะไกลโดยใช้ VPN

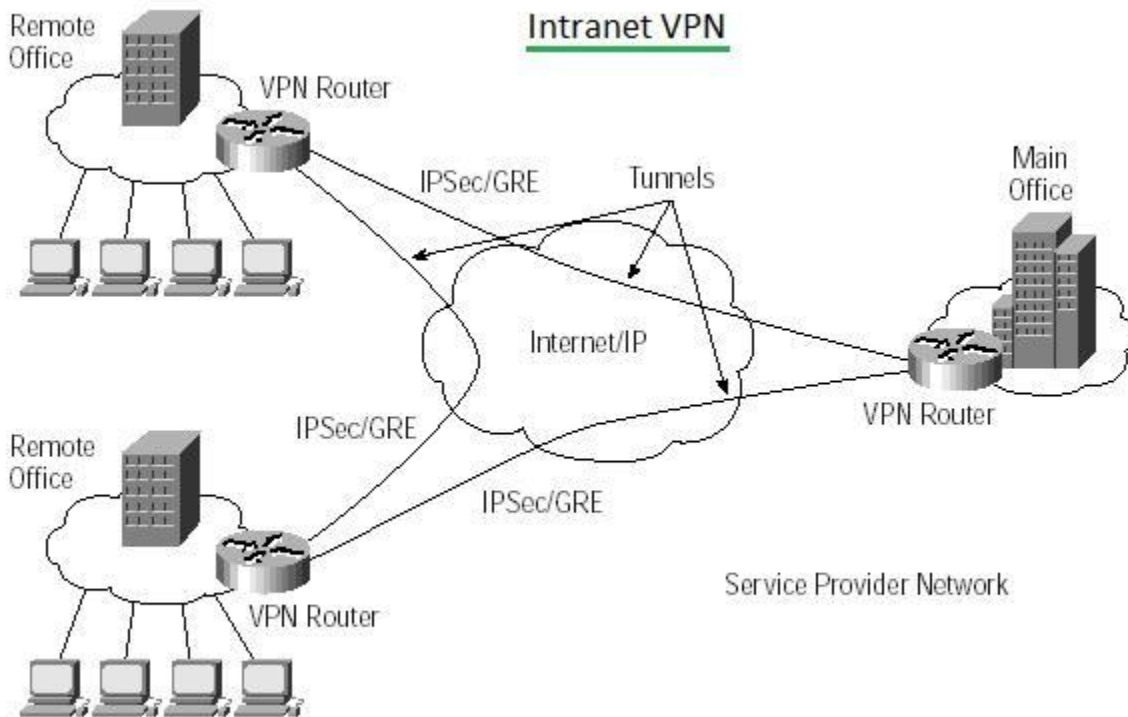
การใช้งานจากระยะไกลโดยผ่าน VPN เป็นการเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตซึ่งมีอยู่ทั่วไป มีความสะดวกกว่าการเข้าถึงระยะไกลแบบ RAS เดิม นอกจากนั้น ความสะดวก ขอบเขตการเรียกใช้บริการ และรายละเอียดในการใช้งานนั้นมีความแตกต่างจากการเข้าถึงระยะไกลแบบเดิม ได้แก่

- 1) ต้องติดตั้งซอฟต์แวร์หรืออุปกรณ์สำหรับใช้ทำ VPN เพิ่มเติมทั้งภายในเครือข่ายส่วนตัวและบนโฮสต์ภายนอกที่ต้องการใช้ VPN เข้ามา
- 2) ที่เครือข่ายส่วนตัวก็ไม่จำเป็นต้องมีโมเด็มสำหรับการเข้าถึงระยะไกลไว้รองรับเหมือนเดิม เพราะเป็นการเข้าถึงผ่านเครือข่ายอินเทอร์เน็ต
- 3) สำหรับโฮสต์ที่ต้องการเข้าถึงจากระยะไกลก็ไม่จำเป็นต้องหมุนโทรศัพท์ผ่านโมเด็มมายังหมายเลขที่จัดเตรียมไว้ที่เครือข่ายสำนักงานเหมือนเดิม เพียงหมุนผ่านไปยังผู้ให้บริการอินเทอร์เน็ต หรือ ISP รายใดก็ได้
- 4) ถ้าเครือข่ายที่โฮสต์ภายนอกทำการเชื่อมต่ออยู่กับอินเทอร์เน็ตอยู่แล้ว ผู้ใช้ก็สามารถใช้ VPN เข้ามายังเครือข่ายส่วนตัวที่ต้องการได้ทันที

6.2.3.2 การเชื่อมต่อโฮสต์ระยะไกล (Remote host connection VPN)

การเชื่อมต่อโฮสต์ระยะไกลประเภทนี้ บางทีเรียกว่า Intranet VPN ซึ่งแตกต่างจากการเข้าถึงระยะไกลที่กล่าวไว้ก่อนหน้านี้ เนื่องจาก การเข้าถึงระยะไกลนั้นจะเป็นการเชื่อมต่อจากโฮสต์หนึ่งไปยังโฮสต์ใดโฮสต์หนึ่งโดยเฉพาะ จึงสามารถใช้ทรัพยากรได้เฉพาะของโฮสต์ปลายทางนั้นเท่านั้น ไม่สามารถใช้ทรัพยากรที่มีอยู่บนโฮสต์อื่นได้ (ยกเว้นว่าจะเชื่อมต่อไปยังโฮสต์อื่นเป็นทอดๆ ไป) การใช้งานส่วนใหญ่จึงมักเป็นการควบคุมโฮสต์จากระยะไกล ซึ่งในการใช้งานจริงจะต้องมีโฮสต์หนึ่งเปิดทิ้งไว้ตลอดเวลาเพื่อทำหน้าที่รองรับการเข้าถึงจากระยะไกล

แต่การเชื่อมต่อแบบโฮสต์ระยะไกลไปยังเครือข่ายนั้น เมื่อผู้ใช้เชื่อมต่อสำเร็จแล้ว โฮสต์ของผู้ใช้เสมือนอยู่ในเครือข่ายส่วนตัวทุกประการ จะทำให้ขอบเขตการใช้งานมีมากกว่าเท่าที่ผู้ใช้นั้นได้รับสิทธิ์สามารถใช้ทรัพยากรใดๆ ที่มีอยู่บนเครือข่ายได้เสมือนกับเวลาที่เข้ามาใช้ที่สำนักงาน เพียงแต่ความเร็วในการเข้าถึงจะขึ้นอยู่กับความเร็วของโมเด็มที่ใช้ในการเชื่อมต่อ การเชื่อมต่อโฮสต์ระยะไกลดังแสดงในรูป 6.3



รูป 6.3 การเชื่อมต่อโฮสต์ระยะไกลเข้าเครือข่ายส่วนตัวโดยอาศัย VPN หรือ Intranet VPN
(ที่มา : <https://www.rfwireless-world.com/terminology/intranet-vpn-vs-extranet-vpn>)

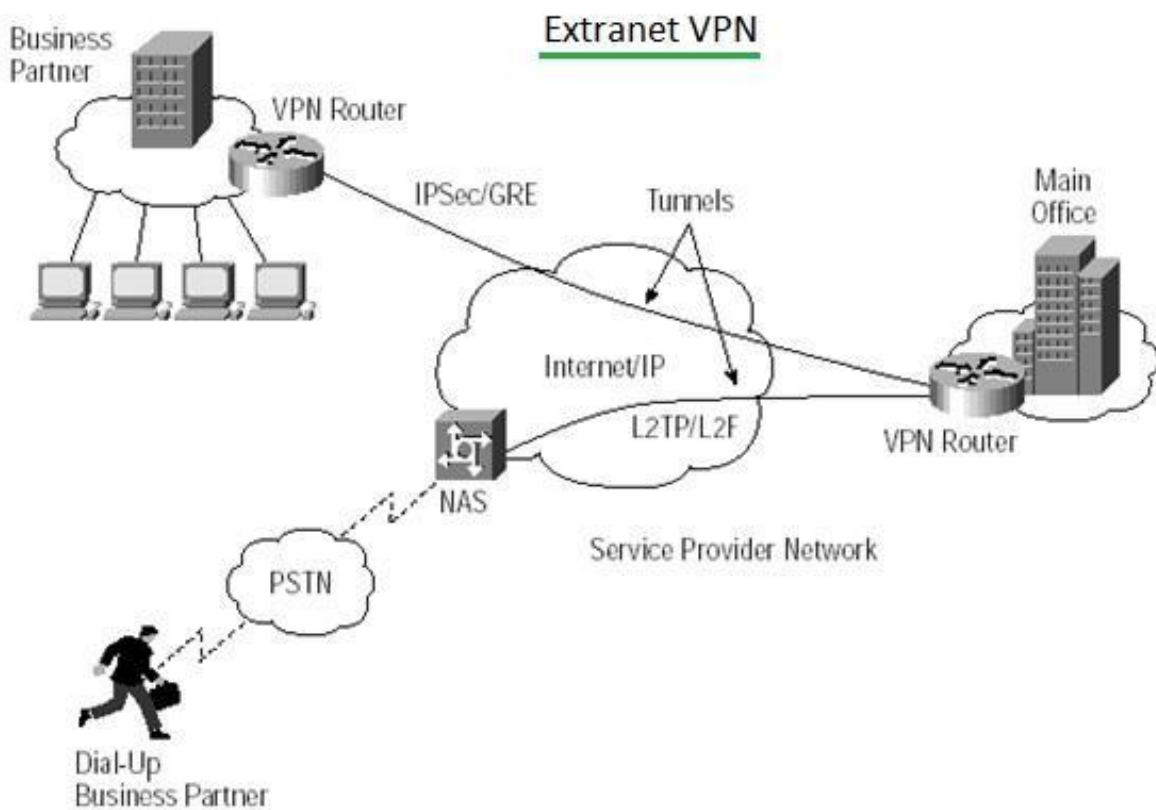
6.2.3.3 การเชื่อมต่อเครือข่ายระยะไกล (Remote network connection)

การเชื่อมต่อเครือข่ายระยะไกลด้วย VPN ประเภทนี้ บางทีเรียกว่า Extranet VPN การเชื่อมต่อโฮสต์เข้ากับเครือข่ายส่วนตัวขององค์กรโดยอาศัย VPN นั้น นอกจากจะใช้เชื่อมต่อในระดับบุคคลแล้ว เรายังสามารถใช้เชื่อมต่อระหว่างเครือข่ายกับเครือข่ายผ่าน VPN ได้อีกด้วยการเชื่อมต่อประเภทนี้จะอำนวยความสะดวกสำหรับบริษัทที่มีสำนักงานสาขากระจัดกระจายอยู่จำนวนมากในสถานที่ต่างๆ ที่ไกลกัน หรือใช้สำหรับการเชื่อมต่อเครือข่ายระหว่างมหาวิทยาลัยวิทยาเขตซึ่งอยู่ในที่ต่างๆ ได้

ในอดีต เครือข่ายคอมพิวเตอร์ขององค์กรเหล่านี้มีความจำเป็นที่จะต้องติดต่อสื่อสารระหว่างกับเครือข่ายของสำนักงานสาขาโดยการเช่าสายของการสื่อสาร เช่น สายเช่า (Leased line), X.25, Frame relay, เช่าช่องสัญญาณดาวเทียม, ไมโครเวฟ เป็นต้น ซึ่งวิธีการเช่นนี้มีข้อจำกัดหลายประการ ได้แก่ มีค่าใช้จ่ายสูง โดยที่ระยะทางจะมีผลโดยตรงต่อต้นทุนการสื่อสาร, ไม่มีช่องทางสื่อสารสำรอง ในกรณีที่ช่องสัญญาณที่เช่าใช้อยู่เกิดขัดข้อง การติดต่อก็จะมีปัญหาไปทั้งหมด, จำนวนสาขามีผลต่อต้นทุนการสื่อสาร ยังมีสาขาจำนวนมาก ย่อมต้องใช้

อุปกรณ์สื่อสารจำนวนมาก นอกจากนั้น ค่าใช้จ่ายที่ใช้ในการจัดซื้อจัดหาอุปกรณ์เหล่านี้ย่อมมีราคาแพง เทคโนโลยีเปลี่ยนแปลงเร็ว รวมทั้งมีค่าใช้จ่ายในการบำรุงรักษาและจัดหาบุคคลากรอีกด้วย

แต่ปัจจุบัน การเชื่อมต่อข้ามเครือข่ายระหว่างสำนักงานกับสาขาผ่านเครือข่ายอินเทอร์เน็ตโดยใช้ VPN ไม่เพียงอำนวยความสะดวกและมีความปลอดภัยสูงเท่านั้น ยังช่วยลดค่าใช้จ่ายที่ใช้สำหรับการเชื่อมต่อและสื่อสารระหว่างกันลงอย่างมีนัยสำคัญ การเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะจึงไม่เกิดปัญหาในเรื่องความขัดข้องของสายสื่อสาร เนื่องจากระบบโครงข่ายโทรศัพท์ที่สามารถเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ตนั้นมีอยู่ทุกหนทุกแห่ง ความจำเป็นในการจัดหาสายสื่อสารสำรองจึงหมดไป รูป 6.4 แสดงการเชื่อมต่อระหว่างเครือข่ายส่วนตัวเข้าด้วยกันผ่าน VPN



รูป 6.4 แสดงการเชื่อมต่อเครือข่ายส่วนตัวเข้าด้วยกันโดยผ่าน VPN

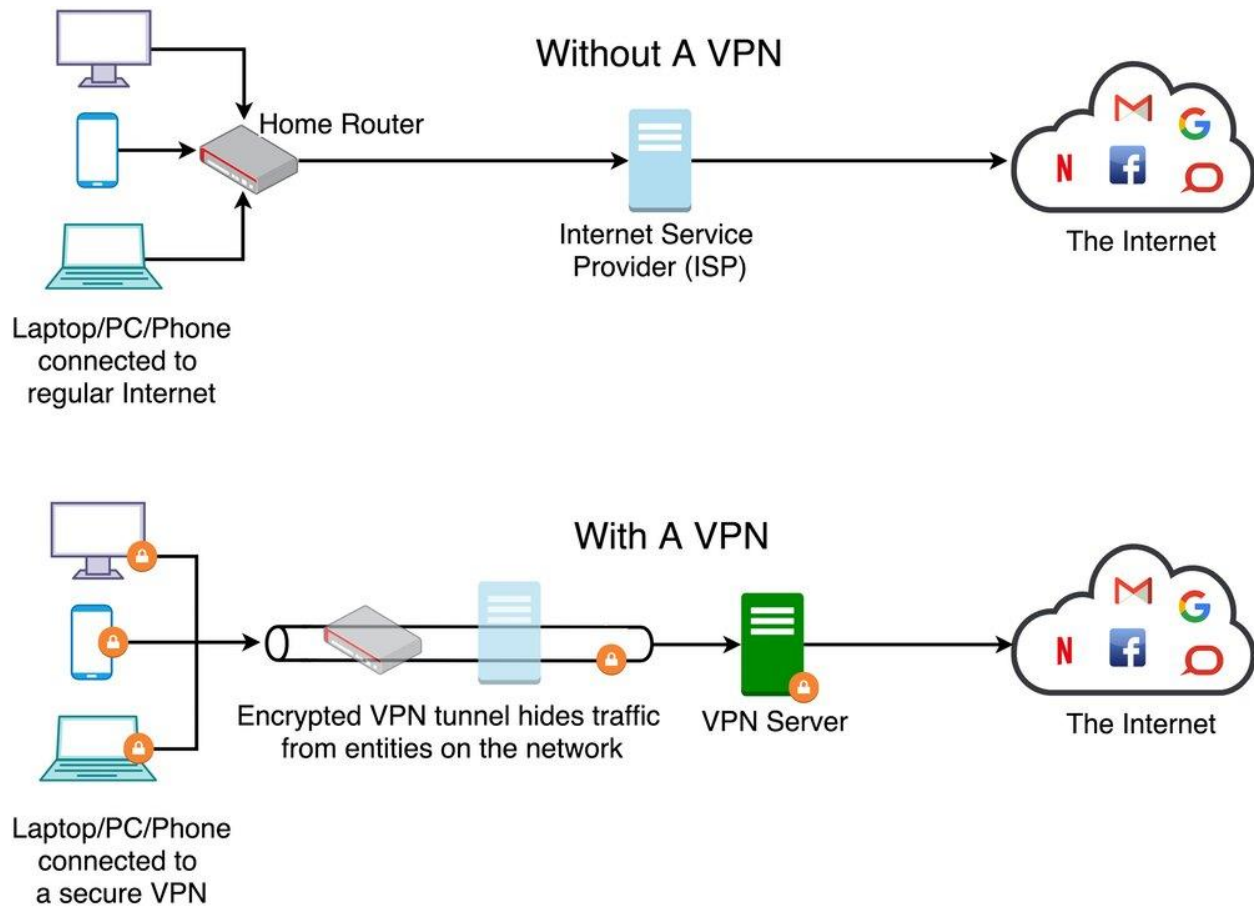
(ที่มา : <https://www.rfwireless-world.com/terminology/intranet-vpn-vs-extranet-vpn>)

จากที่กล่าวมาข้างต้น สรุปความแตกต่างที่สำคัญระหว่าง Intranet VPN กับ Extranet VPN ดังนี้

คุณสมบัติ	Intranet VPN	เอ็กซ์ทราเน็ต VPN
ขอบเขต	เชื่อมต่อผู้ใช้ภายในองค์กรอย่างปลอดภัย	เชื่อมต่อผู้ใช้นอกที่ได้รับอนุญาต (พันธมิตร ผู้ขาย ลูกค้า) เข้ากับอินทราเน็ตขององค์กรอย่างปลอดภัย
เข้าถึง	การเข้าถึงเครือข่ายภายในเท่านั้น	ให้สิทธิ์การเข้าถึงทรัพยากรอินทราเน็ตเฉพาะแบบจำกัดแก่ผู้ใช้งานนอก
ฐานผู้ใช้	พนักงาน, เจ้าหน้าที่ภายใน	พนักงาน คู่ค้า ผู้ขาย และลูกค้าที่ได้รับอนุญาต
การเชื่อมต่อ	โดยทั่วไปจะใช้โครงสร้างพื้นฐานเครือข่ายที่มีอยู่	อาจเกี่ยวข้องกับการเชื่อมต่อแบบ Dial-up ซึ่งต้องใช้ส่วนประกอบ NAS

6.3 โพรโทคอลความปลอดภัยที่ใช้งาน VPN

ปัญหาสำคัญของการนำอินเทอร์เน็ตมาใช้ร่วมกับเครือข่ายส่วนตัวก็คือความปลอดภัยโดยเฉพาะอย่างยิ่งด้านการรักษาความลับ เพราะในการรับส่งข้อมูลข้ามเครือข่ายจากต้นทางไปยังผู้รับปลายทางนั้น อินเทอร์เน็ตไม่มีกลไกใดๆ ที่จะรับประกันความลับของข้อมูลได้เลย ข้อมูลที่ส่งจากผู้รับออกจากเครือข่ายส่วนตัวผ่านไปยัง ISP เป็นทอดๆ ไปจนกระทั่งถึงผู้รับปลายทาง ช่องทางที่ข้อมูลวิ่งผ่านอยู่นี้ย่อมหนีการควบคุม เพราะไม่สามารถเจาะจงไปว่าจะต้องวิ่งไปในเส้นทางใดได้บ้าง ทุกจุดที่ข้อมูลวิ่งไปถึงผ่านเข้าและออกอุปกรณ์จัดเส้นทาง (Router) นั้นอุปกรณ์เหล่านั้นสามารถดักเก็บและอ่านข้อมูลที่วิ่งผ่านได้เสมอ (ถ้าต้องการ)



รูป 6.5 เปรียบเทียบความแตกต่างของการสื่อสารข้อมูลระหว่างไม่มี VPN กับมี VPN

(ที่มา : <https://phys.org/news/2019-02-vpn.html>)

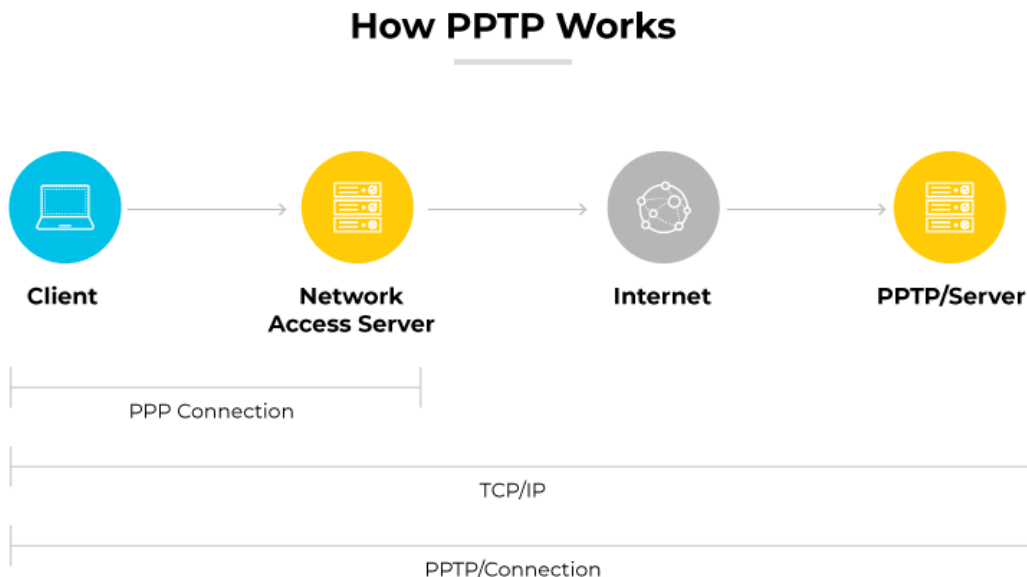
รูป 7.5 แสดงให้เห็นถึงความแตกต่างระหว่างการส่งข้อมูลระหว่างโฮสต์ A ไปยังโฮสต์ B ผ่านเครือข่ายอินเทอร์เน็ตในแต่ละครั้งนั้นจำเป็นต้องผ่านเส้นทางสื่อสารและอุปกรณ์จัดเส้นทางของ ISP จำนวนมากกว่าจะไปยังโฮสต์ปลายทาง ยิ่งต้องผ่านเส้นทางของ ISP จำนวนมากเท่าไร ความเสี่ยงต่อความลับรั่วไหลโดยการดักอ่านข้อมูลก็ยังมีมากเท่านั้น ในขณะที่การสื่อสารข้อมูลระหว่างโฮสต์บนอินเทอร์เน็ตที่ผ่านเครือข่ายส่วนตัวเสมือนหรือ VPN จะสามารถรับประกันความปลอดภัยได้สูงกว่า

ด้วยปัญหาด้านความปลอดภัยของการสื่อสารข้อมูลจากเครือข่ายส่วนตัวเสมือนข้ามไปยังเครือข่ายสาธารณะหรืออินเทอร์เน็ตนั้นสามารถแก้ไขได้โดยอาศัยการสร้างท่อ (Tunneling) ซึ่งเป็นเทคนิคที่มีวัตถุประสงค์เพื่อให้ข้อมูลที่ส่งไปในอินเทอร์เน็ตนั้นยังคงรักษาความลับไว้ได้ และประกันได้ว่าไม่มีใครสามารถลักลอบอ่านข้อมูลที่วิ่งผ่านภายในท่อได้ จึงมีการพัฒนาโปรโตคอลที่ใช้เพื่อการสร้างท่อเพื่อความปลอดภัยสำหรับ VPN ซึ่งมีอยู่ 4 ประเภท ได้แก่ PPTP, L2TP, L2TP และ IPSec การเลือกใช้โปรโตคอลใดขึ้นอยู่กับลักษณะการใช้ VPN

ขององค์กร โพรโทคอล PPTP, L2F และ L2TP เหมาะสำหรับการเชื่อมต่อผ่านสายโทรศัพท์ (Dial-up) ส่วน IPSec นิยมใช้สำหรับการเชื่อมต่อระหว่าง Intranet กับ Intranet

6.3.1 PPTP (Point-to-Point tunneling protocol)

PPTP [84] เป็นโพรโทคอลที่ใช้สร้างระบบ VPN ถูกพัฒนามาจากฟังก์ชันของโพรโทคอล PPP (Point-to-Point protocol) [85] เพื่อให้ผู้ใช้สามารถเข้าถึงโฮสต์แบบระยะไกลผ่านอินเทอร์เน็ตได้อย่างปลอดภัย มีความสามารถในการรักษาความปลอดภัย การตรวจสอบผู้ใช้และการเข้ารหัสข้อมูล แต่เป็นการสื่อสารระหว่าง 2 จุดโดยผ่านสายเฉพาะ (Dedicated link) เช่น โมเด็ม เท่านั้น โดย PPTP จะทำการห่อหุ้มแพ็กเก็ตของโพรโทคอล PPP อีกทีหนึ่ง ทำให้โพรโทคอล PPTP มีความยืดหยุ่น เนื่องจากสามารถรองรับโพรโทคอลชนิดอื่นๆ นอกเหนือจากโพรโทคอล IP เช่น IPX, NetBEUI เป็นต้น



ภาพที่ 6.6 แสดงการห่อหุ้ม IP Datagram ไปบน PPP packet

(ที่มา : <https://www.paloaltonetworks.com/cyberpedia/what-is-pptp>)

จากภาพที่ 6.6 โพรโทคอลการเชื่อมต่อแบบจุดต่อจุด (Point-to-Point Tunneling Protocol: PPTP) สร้างการเชื่อมต่อ VPN โดยการห่อหุ้มเฟรม (PPP) ในแพ็กเก็ต IP สำหรับการส่งผ่านอินเทอร์เน็ต โพรโทคอลนี้ทำงานโดยใช้ช่องควบคุม TCP และอุโมงค์ Generic Routing Encapsulation (GRE) การผสมผสานนี้ทำให้โพรโทคอลสามารถห่อหุ้มแพ็กเก็ต PPP ได้ ซึ่งทำให้สามารถใช้ VPN บนเครือข่ายที่หลากหลายได้

โพรโทคอลนี้ใช้สถาปัตยกรรมไคลเอนต์เซิร์ฟเวอร์ โดยไคลเอนต์จะเริ่มต้นการเชื่อมต่อกับเซิร์ฟเวอร์เพื่อสร้างอุโมงค์ โพรโทคอลนี้ใช้พอร์ต TCP 1723 สำหรับการตั้งค่าช่องควบคุม และ GRE สำหรับการสร้างอุโมงค์เฟรม PPP โครงสร้างแบบคู่นี้ช่วยอำนวยความสะดวกในการจัดการเซสชัน VPN และการส่งข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์อย่างปลอดภัย

ภายในการทำงานของโพรโทคอล มีโหมดการทำอุโมงค์ VPN สองโหมด ได้แก่ แบบสมัครใจและแบบบังคับ การทำอุโมงค์แบบสมัครใจเริ่มต้นโดยไคลเอนต์และเกิดขึ้นหลังจากการเชื่อมต่อเครือข่ายเสร็จสิ้น ส่วนการทำอุโมงค์แบบบังคับเริ่มต้นโดยเซิร์ฟเวอร์ ซึ่งโดยทั่วไปจะอยู่ที่ระดับผู้ให้บริการอินเทอร์เน็ต (ISP) โหมดเหล่านี้จะกำหนดจุดเริ่มต้นและการควบคุมกระบวนการทำอุโมงค์

แม้ว่า PPTP Tunneling Protocol จะเป็นเทคโนโลยีที่ก้าวล้ำสำหรับยุคนั้น แต่ข้อจำกัดด้านความปลอดภัยก็ได้รับการเน้นย้ำด้วยการถือกำเนิดของโพรโทคอลขั้นสูงมากขึ้น

PPTP ใช้กลไกในการพิสูจน์ตัวตนจริงแบบเดียวกับโพรโทคอล PPP ได้แก่ โพรโทคอล PAP, CHAP และ PPP callback control [96]

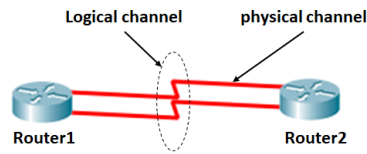
PAP (Password Authentication Protocol) เป็นการพิสูจน์ตัวตนจริงอย่างง่ายโดยที่แม่ข่ายจะทำการขอชื่อและรหัสผ่าน ซึ่งจะได้รับการตอบกลับมาด้วยข้อความที่สามารถอ่านได้ (Clear text) ซึ่งวิธีนี้มีความเสี่ยงที่อาจถูกดักอ่านข้อความการตรวจสอบนี้ได้

CHAP (Challenge Handshaking Authentication Protocol) เป็นการปรับปรุงกลไกการพิสูจน์ตัวตนจริงของ PAP ให้มีความปลอดภัยสูงขึ้นโดยการเข้ารหัสชื่อผู้ใช้และรหัสผ่านเข้ากับข้อมูลแชลแลนจ์ที่ประกอบด้วย Session ID และ Challenge string ด้วยฟังก์ชันแฮช MD5 ซึ่งทำให้ป้องกันการดักอ่านข้อมูลจากบุคคลอื่นได้

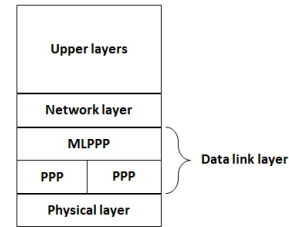
ส่วน PPP callback control ใช้สำหรับกรณีที่ต้องการความปลอดภัยสูง เพื่อความมั่นใจว่าผู้ที่โทรศัพท์เข้ามานั้นเป็นผู้ที่ได้รับอนุญาตแล้วอย่างแท้จริง โดยใช้โพรโทคอล CBCP (Callback control protocol) เมื่อผ่านการพิสูจน์ตัวตนแล้ว NAS จะทำการตัดสายออกแล้วหมุนกลับไปยังหมายเลขโทรศัพท์ที่ผู้ใช้ได้ลงทะเบียนไว้แล้วเท่านั้น เพื่อประกันว่าเป็นผู้ใช้ตัวจริงและโทรศัพท์จากเลขหมายที่ได้รับอนุญาต

PPTP เป็นการนำ PPP ซึ่งออกแบบไว้สำหรับการเชื่อมต่อประเภทไดอัลอัพให้มาใช้ IP เป็นเส้นทางในการสื่อสารแทน โดยการนำแพ็กเก็ตของ PPP มาทำการเข้ารหัสแล้วบรรจุลงโดยโพรโทคอล GRE (Generic router encapsulation) [86] แล้วนำไปบรรจุลง IP datagram อีกทีหนึ่งดังแสดงในรูป 6.7

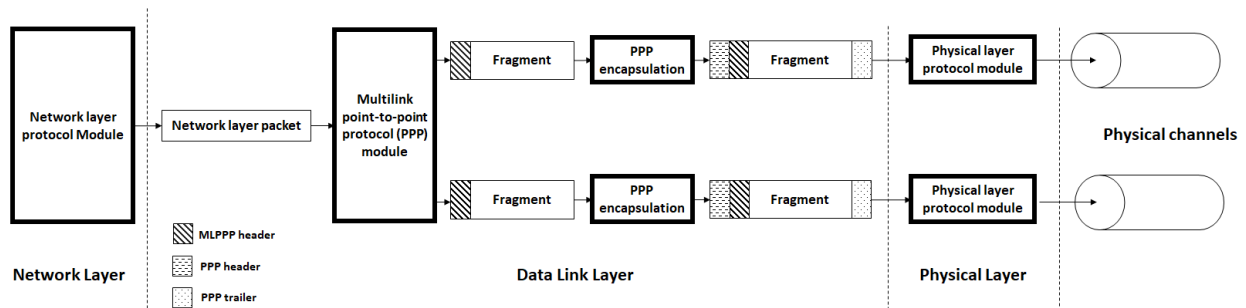
The network topology



The OSI reference model



The encapsulation process



รูป 6.7 แสดง PPP packet ที่ถูกเข้ารหัสด้วย GRE และถูกห่อหุ้มลงใน IP Datagram
(ที่มา https://en.wikipedia.org/wiki/Point-to-Point_Protocol)

ข้อดีของโปรโตคอล PPTP ได้แก่

- 1) ง่ายต่อการใช้งานของเครื่องลูกข่ายสามารถใช้งานได้อย่างกว้างขวางสำหรับระบบปฏิบัติการทุกยี่ห้อ เพียงแต่มี VPN client เท่านั้น
- 2) ใช้โอเวอร์เฮดในการทำงานน้อย
- 3) เนื่องจากเป็นโปรโตคอลที่ทำงานในเลเยอร์ 2 (Data link layer) (ในขณะที่ IPSec ทำงานที่เลเยอร์ 3) ดังนั้น จึงสามารถรองรับการทำงานของโปรโตคอลอื่นนอกจากโปรโตคอล IP ได้อีกด้วย
- 4) สามารถใช้งานผ่าน NAT [97] ได้โดยไม่มีผลกระทบ

ส่วนข้อด้อยของโปรโตคอล PPTP ได้แก่

- 1) การเข้ารหัสของ PPTP จะเริ่มต้นหลังจากขั้นตอนการพิสูจน์ตัวตนเสร็จเรียบร้อยแล้ว ในขณะที่การพิสูจน์ตัวตนนั้นข้อมูลยังอยู่ในรูปแบบที่สามารถอ่านได้ จึงมีความเสี่ยงที่อาจถูกดักอ่านได้

- 2) การพิสูจน์ตัวตนจริงของ PPTP นั้น กระทำในระดับผู้ใช้นั้น ซึ่งทำให้ระดับการตรวจสอบมีเพียงระดับเดียวจึงมีความปลอดภัยต่ำ และอาจถูกโจมตีได้

6.3.2 L2F (Layer-2 Forwarding)

เป็นโพรโทคอลที่ถูกพัฒนาขึ้นสำหรับใช้งานกับ VPN ในช่วงแรกๆ ถูกออกแบบมาใช้สำหรับสร้างการเชื่อมต่อที่ปลอดภัยระหว่างผู้ใช้งานกับเครือข่ายขององค์กร ความแตกต่างกันระหว่าง L2F กับ PPTP ก็คือเรื่องของการสร้างท่อของ L2F นั้นไม่ได้ขึ้นอยู่กับโพรโทคอล IP เท่านั้น แต่ยังรองรับการทำงานร่วมกับโพรโทคอลอื่นๆ เช่น เฟรมรีเลย์ ATM เป็นต้น L2F เป็นโพรโทคอลที่ได้รับการออกแบบมาเพื่อใช้ในการสื่อสารกันระหว่างเราเตอร์ รูป 6.8 โครงสร้าง L2F packet

Bits 0-12													13-15	16-23	24-31
F	K	P	S	0	0	0	0	0	0	0	0	C	Ver	Protocol	Sequence (opt)
Multiplex ID													Client ID		
Length													Payload offset (opt)		
Packet key (optional)															
Payload															
													L2F Checksum (opt)		

รูป 6.8 โครงสร้าง L2F packet

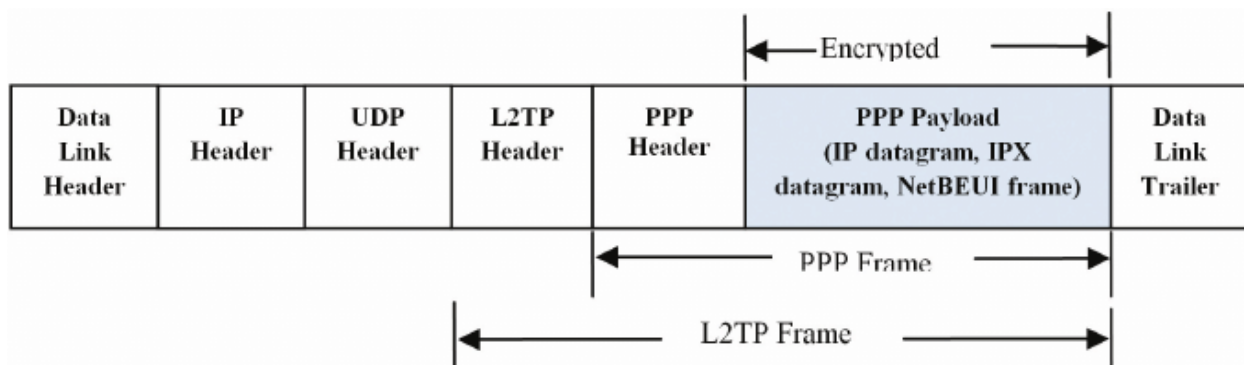
(ที่มา: https://en.wikipedia.org/wiki/Layer_2_Forwarding_Protocol)

L2F ใช้กลไกการพิสูจน์ตัวตนจริงแบบ PPP เช่นกัน และยังเพิ่ม TACACS (Terminal access controller access control protocol) และ RADIUS ด้วย นอกจากนี้ ข้อดีของ L2F ยังสามารถรองรับการเชื่อมต่อได้มากกว่าหนึ่งในแต่ละท่อที่สร้างได้ ในขณะที่ PPTP ไม่มีคุณสมบัตินี้

การพิสูจน์ตัวตนจริงของผู้ใช้ของ L2F นั้นแบ่งออกเป็น 2 ขั้นตอน ขั้นตอนแรกจะทำการตรวจสอบที่ ISP ก่อนที่จะทำการสร้างท่อสำหรับการเชื่อมต่อ ขั้นตอนถัดมา จะทำได้เมื่อสร้างการเชื่อมต่อกับเกตเวย์ของเครือข่ายขององค์กรแล้ว และเนื่องจาก L2F ทำงานบนเลเยอร์ 2 ดังนั้น จึงสามารถรองรับโพรโทคอลอื่นนอกจาก IP ได้ เช่น IPX, NetBEUI เป็นต้น

6.3.3 L2TP (Layer-2 tunneling protocol)

L2TP [87] เป็นโพรโทคอลมาตรฐานที่รับรองโดย IETF (Internet engineering task force) ออกแบบขึ้นมาเพื่อใช้ทดแทนโพรโทคอล PPTP และ L2F โดยจัดข้อบกพร่องที่มีอยู่โพรโทคอลทั้งสองซึ่งทำงานอยู่บนพื้นฐานของโพรโทคอล PPP ในการสร้างการเชื่อมต่อ แต่ L2TP ซึ่งพัฒนาต่อจาก L2F ได้ใช้วิธีการสร้างการเชื่อมต่อแบบใหม่ โดยกำหนดประเภทของแพ็กเก็ตที่สามารถส่งได้ เช่น X.25, เฟรมรีเลย์, ATM เป็นต้น ถ้ามีการใช้งานหรือการสร้างท่อนเครือข่ายประเภท IP ก็จะมีการบรรจุ L2TP frame ลงใน UDP datagram และนำไปบรรจุลงใน IP Datagram อีกทีหนึ่งเพื่อทำการสื่อสารต่อไป โครงสร้างของ L2TP บน IP datagram ดังแสดงในรูป 6.9



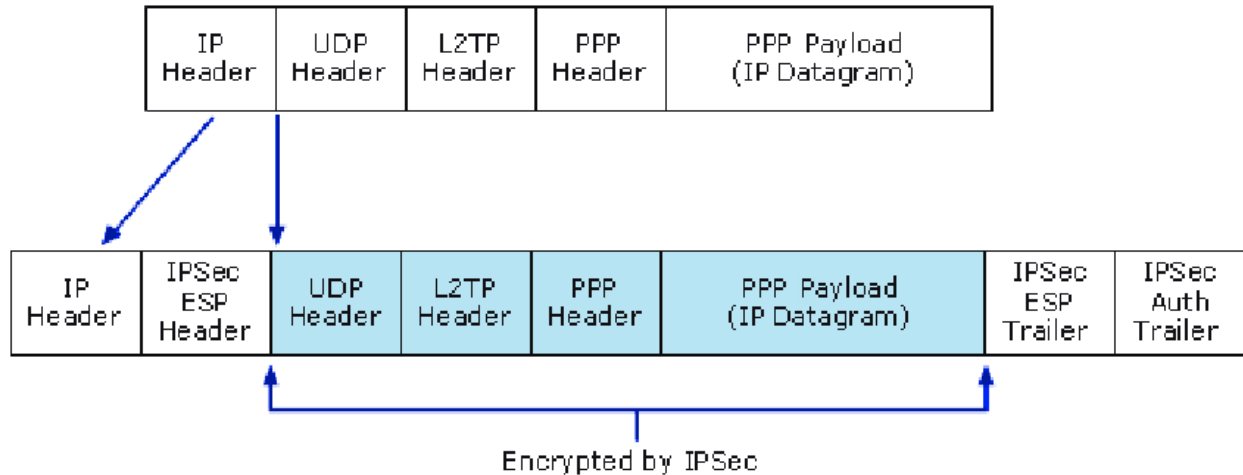
รูป 6.9 โครงสร้างของ L2TP บน IP Datagram

(ที่มา: https://www.researchgate.net/figure/L2TP-Tunnel-Data-Frame-Format_fig4_287458379)

L2TP มอง IP เสมือนเป็นโพรโทคอลในเลเยอร์ 2 อื่นๆ คือมีหน้าที่เพียงนำ L2TP frame ไปส่งยังปลายทาง ส่วนกลไกการสื่อสารอื่นๆ ก็จะเป็นหน้าที่ของโพรโทคอลที่ถูกห่อหุ้มอยู่ไปดำเนินการต่อไป

เนื่องจาก L2TP จะทำหน้าที่ห่อหุ้ม (Encapsulate) แต่ไม่ได้ทำการเข้ารหัส ดังนั้น เพื่อป้องกันไม่ให้ผู้อื่นละเมิดความลับ LTP จึงจำเป็นต้องอาศัย IPSec ในการเข้ารหัสแทน หากมีการดักอ่านข้อมูลด้วยเครื่องมือประเภทสไนฟเฟอร์ ผู้อ่านก็จะได้แต่เพียง UDP datagram เท่านั้น ซึ่งไม่สามารถนำไปใช้ประโยชน์ได้ ด้วยเหตุนี้ L2TP จึงเป็นโพรโทคอลที่มีความสมบูรณ์และปลอดภัยมากกว่าโพรโทคอลอื่นๆ

ทั้ง PPTP, L2F และ L2TP ถูกออกแบบมาให้ใช้งานกับการเชื่อมต่อประเภทไดอัลอัพซึ่งสามารถรองรับการพิสูจน์ตัวตนจริงของผู้ใช้ทั้งแบบ PAP, CHAP และ RADIUS ได้ด้วย แต่โพรโทคอลเหล่านี้ยังไม่รองรับการเข้ารหัสที่ใช้ระบบกุญแจ ในขณะที่โพรโทคอล IPSec จะรองรับกลไกนี้ ดังนั้น L2TP จึงนิยมใช้งานร่วมกับ IPSec โครงสร้างของ L2TP เมื่อใช้งานร่วมกับ IPSec ดังแสดงในรูป 6.10



(ที่มา: https://www.researchgate.net/figure/L2TP-Tunnel-Data-Frame-Format_fig4_287458379)

ข้อดีของโปรโตคอล L2TP เมื่อใช้งานร่วมกับ IPSec ได้แก่

- 1) การพิสูจน์ตัวจริงกระทำทั้งในระดับผู้ใช้และระดับโฮสต์ โดยการตรวจสอบใบรับรอง (Certificate) ของโฮสต์นั้น
- 2) IPSec สร้างความมั่นคงด้านความปลอดภัยในด้านการรักษาความลับ, บुरณาพของข้อมูล และการพิสูจน์ตัวจริง นอกจากนั้น ยังสามารถป้องกันการโจมตีแบบนำกลับมาใช้ใหม่ (Replay attack) จากผู้บุกรุกที่ดักจับแพ็กเก็ตข้อมูลแล้วนำกลับมาใช้โจมตีกระบวนการพิสูจน์ตัวจริงในภายหลังได้ กลไกการรักษาความปลอดภัยนี้ถูกนำมาใช้ในระดับแพ็กเก็ตทุกแพ็กเก็ตจึงมีความปลอดภัยสูง

ส่วนข้อดีของโปรโตคอล L2TP ได้แก่

- 1) จำเป็นต้องมีโครงสร้างพื้นฐานสำหรับใบรับรองเพื่อใช้ในการสื่อสารระหว่างแม่ข่าย VPN กับลูกข่าย
- 2) ไม่สามารถใช้งานในระบบปฏิบัติการรุ่นเก่า เช่น Windows ตั้งแต่รุ่น 98 ลงไป
- 3) ไม่สามารถใช้งานผ่าน NAT ได้

6.3.4 IPSec (IP Security protocol)

IPSec [88] เป็นโพรโทคอลให้บริการรักษาความปลอดภัยข้อมูลทำงานอยู่ในระดับเลเยอร์ 3 (เน็ตเวิร์กเลเยอร์) เป็นความพยายามที่จะบูรณาการระบบความปลอดภัยเมื่อมีการสื่อสารผ่านอินเทอร์เน็ตลงในระดับ

ไอพี IPSec ได้ถูกออกแบบสำหรับการเข้ารหัสข้อมูลแพ็กเก็ตของ IP จึงรับรองด้านการรักษาความลับ, บำรุงภาพของข้อมูล และการพิสูจน์ตัวจริง สถาปัตยกรรมของ IPSec แบ่งออกเป็น 3 ระดับ [89] ประกอบด้วย

- 1) มีความเป็นมอดูลสูง (Highly modular) โดยอนุญาตให้ผู้ใช้ (หรือผู้ดูแลระบบ) สามารถเลือกขั้นตอนวิธีการเข้ารหัสได้หลายชนิด และกำหนดโปรโตคอลความปลอดภัยได้ตามความเหมาะสม
- 2) IPSec อนุญาตให้ผู้ใช้สามารถเลือกใช้บริการความปลอดภัยได้หลายรายการ ได้แก่ การควบคุมการเข้าถึง, บำรุงภาพ, การพิสูจน์ตัวจริง, การป้องกันการนำกลับมาใช้ใหม่ และการรักษาความลับ (ความเป็นส่วนตัว)
- 3) IPSec อนุญาตให้ผู้ใช้สามารถควบคุมระดับความเข้มงวดของการใช้บริการความปลอดภัยได้หลายระดับเมื่อนำไปใช้งาน ตัวอย่างเช่น สามารถเลือกใช้ IPSec สำหรับควบคุมข้อมูลที่สื่อสารกันแบบช่วงแคบ อย่างเช่น แพ็กเก็ตที่สื่อสารกันของการเชื่อมต่อแบบ TCP ระหว่างโฮสต์กับโฮสต์ หรือการสื่อสารแบบช่วงความถี่กว้าง อย่างเช่น ทุกแพ็กเก็ตที่วิ่งผ่านระหว่างเกตเวย์กับเกตเวย์ เป็นต้น

มาตรฐานที่โปรโตคอล IPSec ใช้ในการเข้ารหัสประกอบด้วย

- 1) การแลกเปลี่ยนกุญแจลับ (Key exchange) โดยใช้ขั้นตอนวิธีของ Diffie-Hellman สำหรับแลกเปลี่ยนกุญแจลับระหว่างเครื่องผู้ส่งและผู้รับผ่านเครือข่ายสาธารณะ
- 2) ใช้วิทยาการเข้ารหัสลับแบบกุญแจสาธารณะ สำหรับเข้ารหัสแพ็กเก็ตที่ใช้แลกเปลี่ยนกุญแจลับ และเพื่อใช้ในการพิสูจน์ตัวจริงระหว่างคู่สนทนา
- 3) ใช้การเข้ารหัสข้อมูลแบบ DES
- 4) ใช้ฟังก์ชันแฮชในการตรวจสอบคุณภาพของข้อมูล เพื่อประกันว่าข้อมูลที่ถูกส่งผ่านไปบนเครือข่ายสาธารณะจะไม่ถูกแก้ไขหรือปลอมแปลง
- 5) ใช้รับรองดิจิทัล (Digital certificate) สำหรับการตรวจสอบเจ้าของกุญแจสาธารณะ

การจัดการและแลกเปลี่ยนกุญแจเมื่อใช้ IPSec นี้ สามารถทำได้ 2 แบบ [90] คือ ให้ผู้ดูแลระบบเป็นผู้จัดการเอง หรือใช้โปรโตคอล IKE (Internet key exchanging) [91] สำหรับการแลกเปลี่ยนและจัดการกุญแจโดยอัตโนมัติ ซึ่งทั้งสองแบบนี้กำหนดให้มีการใช้งานใน IPSec โดยทั่วไป การจัดการกุญแจโดยผู้ดูแลระบบเหมาะสำหรับการใช้งานจำนวนน้อย ถ้ามีการใช้ในไซต์จำนวนมาก การจัดการกุญแจโดยใช้โปรโตคอล IKE มีความเหมาะสมกว่า

ดังนั้น IPSec ถือว่าเป็นโพรโทคอลที่มีความปลอดภัยสูงและเหมาะสมที่สุดสำหรับการสร้าง VPN แต่อย่างไรก็ตาม IPSec ได้รับการออกแบบมาสำหรับเครือข่ายที่ใช้โพรโทคอล IP เป็นหลัก ถ้าองค์กรยังใช้งานโพรโทคอลอื่นๆ ร่วมอยู่ด้วย เช่น IPX (NetWare) [92], NetBUIE (Microsoft) [93], AppleTalk (Apple) [94] เป็นต้น การสร้าง VPN ก็จำเป็นต้องเลือกใช้ PPTP, L2F หรือ L2TP แทน

เมื่อในระดับสูง IPSec ประกอบด้วย 2 ส่วน ส่วนแรกเป็นคู่ของโพรโทคอลที่ใช้สำหรับให้บริการความปลอดภัย มีส่วนหัวของการพิสูจน์ตัวตนจริง (Authentication header หรือ AH) ที่ใช้ควบคุมการเข้าถึง, บารณาภาพของข่าวสารแบบไม่กำหนดการเชื่อมต่อ (Connectionless) และการป้องกันการนำกลับมาใช้ใหม่ ส่วนที่สอง เป็นการห่อหุ้ม ความปลอดภัย (Encapsulating security payload หรือ ESP) สนับสนุนบริการความปลอดภัย เช่นเดียวกับ AH แต่เพิ่มในด้านการรักษาความลับเข้ามาด้วย โพรโทคอลทั้งสองส่วนนี้ ผู้ใช้สามารถเลือกใช้ตัวใดตัวหนึ่งหรือเลือกใช้ทั้งคู่ก็ได้ นอกจากนั้น ส่วนที่สองยังสนับสนุนการจัดการกุญแจซึ่งอยู่บนพื้นฐานของโพรโทคอลที่เรียกว่า ISAKMP (Internet Security Association and Key Management Protocol)[95]

ก่อนการส่ง IP Datagram ทั้ง AH และ ESP จะสร้างการเชื่อมต่อเสมือน หรือท่อส่งข้อมูลก่อน เรียกว่า SA (Security Agreement) ซึ่งเป็นการเปลี่ยนรูปแบบการสื่อสารแบบไม่กำหนดการเชื่อมต่อของโพรโทคอลในระดับเน็ตเวิร์กเลเยอร์ไปเป็นแบบกำหนดการเชื่อมต่อ (Connection-oriented) การเชื่อมต่อเสมือน SA เป็นการเชื่อมต่อแบบทิศทางเดียว โดยการเชื่อมต่อแต่ละครั้งจะต้องมีอย่างน้อย 2 ท่อแยกขาดจากกัน จาก A ไป B และจาก B มา A เพื่อความปลอดภัย SA อาจถูกสร้างขึ้นระหว่างคู่ของโฮสต์กับโฮสต์, โฮสต์กับเกตเวย์ (เราเตอร์ที่รองรับ IPSec) หรือระหว่างเราเตอร์กับเราเตอร์ก็ได้ รูปแบบแพ็กเก็ตของ AH แสดงในภาพที่ 4- และ ESP

การเชื่อมต่อ SA จะมีหมายเลขประจำการเชื่อมต่อที่เรียกว่า SPI (Security Parameter Index) ซึ่งเมื่อนำเอา SPI และหมายเลขไอพีของโฮสต์ปลายทางรวมกันก็จะได้เลขหมายที่มีค่าไม่ซ้ำกันได้ เมื่อต้องการจะส่งแพ็กเก็ตโดยใช้ IPSec โฮสต์ฝั่งผู้ส่งจะค้นหานโยบาย SA ในฐานข้อมูล, ประยุกต์ใช้นโยบายนั้น และเพิ่มหมายเลข SPI เข้าไปในส่วนหัวของแพ็กเก็ต IPSec ในฝั่งรับ เมื่อรับก็จะทำการค้นหานโยบาย SA ในฐานข้อมูล และทำงานตามนโยบายนั้น ดังนั้น SA จึงเป็นนโยบายความปลอดภัยที่ใช้ในการเชื่อมต่อกันของ IPSec นั่นเอง

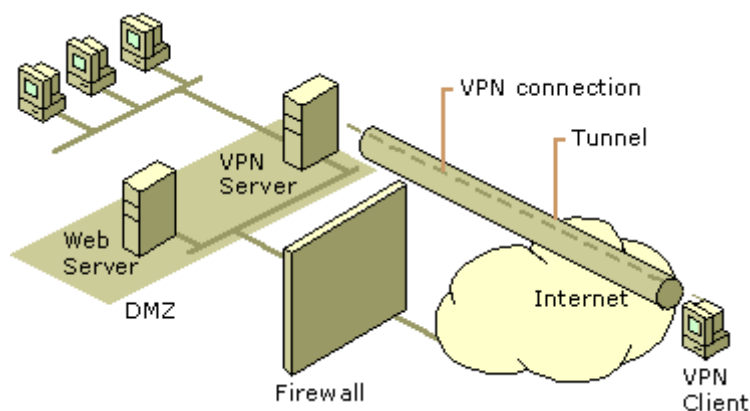
IPSec อนุญาตให้ผู้ส่งหรือเกตเวย์สามารถตรวจสอบผู้ใช้และเข้ารหัสข้อมูลของแพ็กเก็ตไอพีได้ โดยแบ่งออกเป็น 2 โหมด ได้แก่ โหมดทรานสปอร์ต (Transport mode) ใช้สำหรับเข้ารหัสเฉพาะส่วนที่เป็นข้อมูลแพ็กเก็ตไอพีเท่านั้น ส่วนหัวจะยังคงไว้เช่นเดิม และโหมดทันแนลลิง (Tunneling mode) จะทำการเข้ารหัสแพ็กเก็ตไอพีเดิมทั้งหมด และเพิ่มส่วนหัวเข้าไปใหม่

การที่โหมดทรานสปอร์ตทำการเข้ารหัสเฉพาะส่วนที่เป็นข้อมูลเท่านั้น แม้ว่าจะทำให้การสื่อสารข้อมูลมีความรวดเร็วแต่อาจไม่ปลอดภัยเพราะผู้บุกรุกสามารถวิเคราะห์การไหลเวียนของข้อมูลเพื่อใช้ในการโจมตีได้แม้จะไม่ทราบเนื้อหาข้อมูลนั้นก็ตาม ส่วนในโหมดทันแนลลิง ข้อมูลของแพ็กเก็ตไอพีเดิมจะถูกเข้ารหัสทั้งหมด โดย

IPSec จะสร้างเป็นแพ็กเก็ตใหม่ให้ ส่วนแพ็กเก็ตเดิมที่เข้ารหัสจะกลายเป็น payload ซึ่งในโหมดนี้ เราเตอร์จะทำหน้าที่เข้ารหัสแพ็กเก็ตโอพีให้แทนโฮสต์ที่ต้องการส่ง เราเตอร์ต้นทางจะเข้ารหัสแล้วส่งไปตามท่อ ส่วนเราเตอร์ปลายทางก็จะถอดรหัสแพ็กเก็ตเสร็จแล้วจึงค่อยส่งต่อไปให้โฮสต์ปลายทาง ด้วยวิธีดังกล่าว การเข้ารหัสและถอดรหัสจึงไม่เป็นภาระของโฮสต์ทั้งฝั่งรับและส่งเลย นอกจากนั้น ไม่มีความจำเป็นต้องแก้ไขค่าใดๆ ที่โฮสต์ทั้งฝั่งรับและส่งอีกด้วย ผู้บุกรุกทำได้เพียงวิเคราะห์ทางเข้าและทางออกของท่อส่งเท่านั้น แต่ไม่สามารถทราบได้ว่าข้อมูลถูกส่งและรับโดยโฮสต์ใด โหมดทันทันแนลจึงเป็นที่นิยมในการใช้งาน IPSec มากกว่าโหมดทรานสปอร์ต

การสร้างท่อที่ปลอดภัยสำหรับรับส่งแพ็กเก็ตของ IPSec นั้น ทำหน้าที่โดยโปรโตคอล IKE (Internet Key Exchange) เป็นกระบวนการที่ใช้ในการพิสูจน์ตัวตนจริงของคู่รับส่ง และใช้สร้างกุญแจที่ใช้ร่วมกันในการเข้ารหัสและถอดรหัส โดยคู่รับส่งจะทำการตรวจสอบตัวตนซึ่งกันและกันก่อนที่จะเริ่มส่งข้อมูล วิธีที่ทั้งคู่ใช้ในการตรวจสอบกันนั้นสามารถตกลงกันในขั้นตอนการเจรจา ซึ่งการตกลงนั้นจะประกอบด้วย การจัดเตรียมกุญแจร่วมกันก่อน (Pre-shared keys) ต้องมีกุญแจถูกติดตั้งอยู่บนทุกโฮสต์ที่จะใช้งาน IPSec ก่อน โดยใช้กุญแจนี้ในการเข้ารหัสแพ็กเก็ตเมื่อโฮสต์ฝั่งปลายทางสามารถถอดรหัสได้ก็แสดงว่าขั้นตอนการพิสูจน์ตัวตนจริงระหว่างผู้รับและผู้ส่งสำเร็จ จากนั้นจึงใช้ระบบการเข้ารหัสลับแบบกุญแจสาธารณะ โดยแต่ละคู่รับส่งจะสร้างเลขสุ่มขึ้นมาค่าหนึ่ง (Nonce) แล้วเข้ารหัสโดยใช้กุญแจสาธารณะของคู่รับ

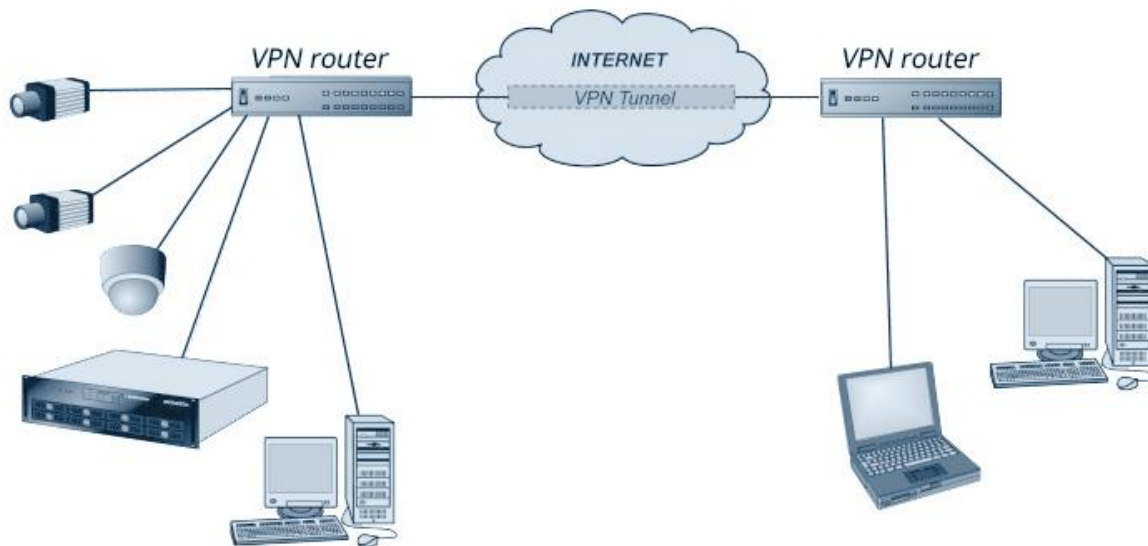
ในการใช้งานจริง เราสามารถเลือกใช้ผลิตภัณฑ์ประเภท VPN ได้หลายชนิด ได้แก่ VPN แบบไฟร์วอลล์ (Firewall based VPN) ซึ่งทำหน้าที่ควบคุมทราฟฟิกทั่วไปพร้อมทั้งทราฟฟิกแบบ VPN ด้วย ถ้าแพ็กเก็ตที่ส่งเข้ามาถูกเข้ารหัสด้วย VPN ไฟร์วอลล์ก็จะทำหน้าที่เป็นเกตเวย์ถอดรหัสให้แล้วส่งต่อไปยังเครือข่ายที่ด้านหลังต่อไป VPN แบบไฟร์วอลล์นี้ดังแสดงในรูป 6.11



รูป 6.11 VPN ประเภท Firewall Based

(ที่มา: <https://i.sstatic.net/RHDof.gif>)

บางกรณีเราอาจเลือกใช้ VPN ที่เป็นอุปกรณ์ซึ่งได้รับการออกแบบมาให้ทำหน้าที่เป็น VPN โดยเฉพาะ การประมวลผลในการเข้าและถอดรหัสจะเป็นหน้าที่โดยตรงของฮาร์ดแวร์ VPN ประเภทนี้ บางทีเรียกว่า เราเตอร์เข้ารหัส (Encrypting router) หมายถึงเราเตอร์ที่มีความสามารถในการเข้ารหัสภายในตัวเอง เป็นการสื่อสารระหว่าง VPN ด้วยกัน ซึ่ง VPN ประเภทนี้จึงมีประสิทธิภาพสูงแต่ก็มาพร้อมกับราคาที่แพงกว่าแบบอื่นๆ ดังแสดงในรูป 6.12



รูป 6.12 VPN ประเภทฮาร์ดแวร์

(ที่มา: <https://www.qsfptek.com/qt-news/vpn-router-what-is-it.html>)

ส่วนอีกประเภทหนึ่งได้แก่ซอฟต์แวร์ VPN แบบอย่างเดี่ยว (Standalone VPN application) เป็นซอฟต์แวร์ทำหน้าที่ VPN ทั้งประเภทแม่ข่ายและลูกข่าย อีกระบบปฏิบัติการและฮาร์ดแวร์ใดๆ จึงสามารถใช้สร้างการเชื่อมต่อระหว่างซอฟต์แวร์ VPN ที่มาจากองค์กรอื่นที่ได้ตกลงกัน นอกจากนั้น ยังมีการใช้ซอฟต์แวร์บางชนิดประยุกต์ใช้งานเป็น VPN ได้ทั้งแม่ข่ายและลูกข่าย เช่น SSH (Secured shell) เป็นต้น การใช้งาน VPN ประเภทซอฟต์แวร์นั้นนอกจากจะมีความคล่องตัวสูงแล้วยังมีค่าใช้จ่ายต่ำอีกด้วย

ดังนั้น จะพบว่า การสื่อสารจากเครือข่ายส่วนตัวผ่านไปยังเครือข่ายสาธารณะโดยใช้ VPN นั้นมีความปลอดภัยโดยอาศัยการสร้างท่อหรืออุโมงค์เฉพาะวิ่งผ่านไปยังอินเทอร์เน็ต โดยระดับความปลอดภัยที่ใช้ก็ขึ้นอยู่กับ การเลือกโปรโตคอลที่ใช้ในการสร้างท่อ ซึ่งจะพบว่า ท่อในการรับส่งข้อมูลที่มีความปลอดภัยสูงสุดในระบบ VPN ก็คือการสร้างท่อโดยอาศัยโปรโตคอลความปลอดภัยแบบ IPSec

6.4. ประโยชน์ของการใช้ VPN

VPN มีประโยชน์มากมายช่วยยกระดับประสบการณ์ออนไลน์และปกป้องชีวิตดิจิทัลขององค์กร สรุปได้ดังนี้

ความเป็นส่วนตัวออนไลน์: VPN เข้ารหัสการเชื่อมต่ออินเทอร์เน็ต เพื่อให้แน่ใจว่ากิจกรรมออนไลน์ของเรายังคงเป็นส่วนตัว VPN ซ่อนที่อยู่ IP และประวัติการเข้าชมของเรา ทำให้ทุกคน รวมถึงแฮกเกอร์และผู้ลงโฆษณา ไม่สามารถติดตามพฤติกรรมออนไลน์ของเราได้

ความปลอดภัยบน Wi-Fi สาธารณะ: เมื่อเราเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะ มักเสี่ยงต่อการถูกดักจับข้อมูลโดยอาชญากรไซเบอร์ VPN มอบอุโมงค์ที่ปลอดภัยสำหรับข้อมูลของเรา ปกป้องข้อมูลของเราจากภัยคุกคามที่อาจเกิดขึ้น และรับประกันว่าข้อมูลสำคัญของเรายังคงเป็นความลับ

การท่องเว็บแบบไม่ระบุตัวตน: VPN ทำให้เว็บไซต์ติดตามกิจกรรมออนไลน์ของเราได้ยาก ความไม่เปิดเผยตัวตนนี้ช่วยให้สามารถรักษาความเป็นส่วนตัวขณะท่องเว็บได้

ความปลอดภัยที่เพิ่มขึ้น: นอกเหนือจากการเข้ารหัส VPN มักมีคุณสมบัติความปลอดภัยเพิ่มเติม เช่น การบล็อกโฆษณา และการป้องกันมัลแวร์และการพยายามฟิชชิง ช่วยปกป้องประสบการณ์ออนไลน์ของเราให้ดียิ่งขึ้น

การเข้าถึงระยะไกล: สำหรับธุรกิจ VPN ช่วยให้สามารถเข้าถึงเครือข่ายและข้อมูลของบริษัทจากระยะไกลได้อย่างปลอดภัย ซึ่งมีประโยชน์อย่างยิ่งในโลกที่การทำงานระยะไกลและการทำงานจากที่บ้านกำลังได้รับความนิยมเพิ่มมากขึ้น

ความสามารถในการปรับขนาดเครือข่าย: แม้แต่ VPN ช่วยให้นักงานหลายคนและพนักงานระยะไกลเข้าถึงได้พร้อมกัน นอกจากนี้ยังรองรับแอปพลิเคชันบนคลาวด์ ให้การเข้าถึงที่ปลอดภัยผ่านอุโมงค์ VPN ความสามารถในการปรับขนาดนี้ช่วยให้ธุรกิจสามารถรองรับผู้ใช้จำนวนมากขึ้นได้อย่างง่ายดาย และให้สิทธิ์เข้าถึงทรัพยากรที่จำเป็น

ความเป็นส่วนตัวจาก ISP: VPN ป้องกันไม่ให้ผู้ให้บริการอินเทอร์เน็ต (ISP) ของเราตรวจสอบและขายข้อมูลออนไลน์ของเราให้กับผู้โฆษณา จึงรักษาความเป็นส่วนตัวออนไลน์ของเราได้

หลีกเลี่ยงการจำกัดแบนด์วิดท์: ผู้ให้บริการอินเทอร์เน็ตบางรายจำกัดความเร็วของกิจกรรมออนไลน์บางอย่าง เช่น การสตรีมมิ่งและการเล่นเกม VPN สามารถช่วยหลีกเลี่ยงข้อจำกัดเหล่านี้ได้ รับรองประสบการณ์ออนไลน์ที่ราบรื่น

ลดต้นทุน: ในการติดตั้งระบบแบบ onsite แบบดั้งเดิมที่บริษัทต่างๆ มีเซิร์ฟเวอร์เป็นของตนเอง การดูแลรักษาและแก้ไขปัญหาด้านประสิทธิภาพหรือความปลอดภัยนั้นต้องใช้เวลาและทรัพยากรภายในองค์กร VPN จะช่วยโอนความรับผิดชอบเหล่านี้ไปยังผู้ให้บริการ ซึ่งสามารถจัดการโครงสร้างพื้นฐานได้อย่างมีประสิทธิภาพมากขึ้นและมีต้นทุนที่ลดลง

6.5 สรุปบท

เทคโนโลยีเครือข่ายส่วนตัวเสมือน (VPN) เป็นสิ่งจำเป็นสำหรับการสร้างความมั่นใจในความปลอดภัยระดับสูงในการสื่อสารข้อมูลผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต โดยสร้างอุโมงค์เข้ารหัสที่ปกป้องความเป็นส่วนตัว ความสมบูรณ์ของข้อมูล และการตรวจสอบสิทธิ์ผู้ใช้ ช่วยให้สามารถเข้าถึงและเชื่อมต่อเครือข่ายจากระยะไกลได้อย่างปลอดภัย พร้อมทั้งลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานเครือข่ายสาธารณะ เนื้อหาในบทนี้กล่าวถึง

- **นิยามและวัตถุประสงค์ของ VPN:** VPN มอบฟังก์ชันการทำงานของเครือข่ายส่วนตัวผ่านเครือข่ายสาธารณะ โดยการสร้างอุโมงค์เข้ารหัส เพื่อให้มั่นใจถึงความปลอดภัยในการส่งข้อมูลและการไม่เปิดเผยตัวตนของผู้ใช้ ช่วยให้สามารถเข้าถึงและสื่อสารระหว่างเครือข่ายต่างๆ ได้อย่างปลอดภัย

- **เครือข่ายส่วนตัวและเครือข่ายสาธารณะ:** เครือข่ายส่วนตัวถูกจำกัดเฉพาะผู้ใช้ที่ได้รับอนุญาตภายในองค์กรที่มีขอบเขตทางกายภาพที่ควบคุมได้และมีความปลอดภัยสูง ในขณะที่เครือข่ายสาธารณะ เช่น อินเทอร์เน็ต ทุกคนสามารถเข้าถึงได้ ไม่มีขอบเขตทางกายภาพ และมีความเสี่ยงด้านความปลอดภัยที่สูงกว่า VPN ช่วยลดความแตกต่างเหล่านี้ด้วยการรักษาความปลอดภัยการสื่อสารผ่านเครือข่ายสาธารณะ

- **กลไกการทำงานของ VPN:** VPN เปลี่ยนเส้นทางข้อมูลผู้ใช้ผ่านเซิร์ฟเวอร์ระยะไกล เข้ารหัสข้อมูลเพื่อซ่อนที่อยู่ IP และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต กลไกสำคัญประกอบด้วยโปรโตคอลการเชื่อมต่อที่ปลอดภัย การเข้ารหัส การสร้างอุโมงค์ และการปกปิดที่อยู่ IP

- **ประเภทการใช้งาน VPN:** VPN แบ่งออกเป็น VPN สำหรับการเข้าถึงระยะไกล (การเข้าถึงของผู้ใช้แต่ละราย), VPN สำหรับการเชื่อมต่อโฮสต์ระยะไกล (VPN สำหรับอินทราเน็ตสำหรับการเข้าถึงทรัพยากรเครือข่ายที่กว้างขึ้น) และ VPN สำหรับการเชื่อมต่อเครือข่ายระยะไกล (VPN สำหรับเอ็กซ์ทราเน็ตที่เชื่อมต่อหลายเครือข่ายอย่างปลอดภัย) แต่ละประเภทรองรับความต้องการขององค์กรที่แตกต่างกัน

- **โพรโทคอลความปลอดภัย VPN:** โพรโทคอลหลัก 4 โพรโทคอล ได้แก่ PPTP, L2F, L2TP และ IPSec ช่วยอำนวยความสะดวกด้านความปลอดภัยของ VPN PPTP และ L2F รองรับการเชื่อมต่อแบบ dial-up โดย L2TP พัฒนาต่อยอดจากโพรโทคอลเหล่านี้และมักใช้ร่วมกับ IPSec ซึ่งให้การเข้ารหัสและการตรวจสอบสิทธิ์ที่แข็งแกร่งที่ขึ้น IP ทำให้ IPSec เป็นโพรโทคอลที่ปลอดภัยที่สุดสำหรับ VPN

- **สถาปัตยกรรม IPSec:** IPSec ทำงานที่ชั้นเครือข่าย ให้การรักษาความลับ ความถูกต้องครบถ้วน สมบูรณ์ การตรวจสอบสิทธิ์ และการป้องกันการปลอมแปลงผ่านโพรโทคอลแบบโมดูลาร์ AH และ ESP พร้อมการจัดการคีย์ผ่าน IKE รองรับโหมดการขนส่งและโหมดอุโมงค์ โดยโหมดอุโมงค์จะเหมาะสมสำหรับ VPN เนื่องจากมีความปลอดภัยสูง

- **ประเภทการใช้งาน VPN:** VPN อาจเป็นแบบไฟร์วอลล์ แบบฮาร์ดแวร์ (เราเตอร์เข้ารหัส) หรือแบบซอฟต์แวร์เดี่ยว ซึ่งแต่ละแบบมีประสิทธิภาพ ต้นทุน และความยืดหยุ่นในการใช้งานที่แตกต่างกัน VPN แบบซอฟต์แวร์นำเสนอโซลูชันที่คุ้มค่าและยืดหยุ่น ในขณะที่ VPN แบบฮาร์ดแวร์ให้ประสิทธิภาพสูงในราคาที่สูงกว่า

- **ประโยชน์ของ VPN:** VPN ช่วยเพิ่มความเป็นส่วนตัวทางออนไลน์ด้วยการเข้ารหัสการเชื่อมต่อ อินเทอร์เน็ต รักษาความปลอดภัยการใช้งาน Wi-Fi สาธารณะ เปิดใช้งานการท่องเว็บแบบไม่ระบุตัวตน รองรับการทำงานระยะไกล ปรับขนาดการเข้าถึงเครือข่ายอย่างมีประสิทธิภาพ ป้องกันการติดตามและควบคุมปริมาณการใช้งานของ ISP และลดต้นทุนด้วยการจ้างผู้ให้บริการจัดการโครงสร้างพื้นฐานภายนอก

เครือข่ายส่วนตัวเสมือน หรือ VPN มีบทบาทสำคัญในการปกป้องความเป็นส่วนตัวและความปลอดภัยออนไลน์ ทั้งสำหรับบุคคลและองค์กร โดยช่วยเข้ารหัสข้อมูล ป้องกันการติดตาม เข้าถึงเครือข่ายจากระยะไกล ลดความเสี่ยงจากภัยคุกคามออนไลน์ และยังช่วยลดต้นทุนให้กับธุรกิจอีกด้วย เครือข่ายส่วนตัวเสมือนนั้นใช้โพรโทคอลการสร้างอุโมงค์ และอาจรวมเข้ากับโพรโทคอลเครือข่ายหรือแอปพลิเคชันอื่น ๆ เพื่อเพิ่มความสามารถและการครอบคลุมรูปแบบความปลอดภัยที่แตกต่างกัน

เทคโนโลยีเครือข่ายส่วนตัวเสมือน (VPN) มีความสำคัญต่อการรักษาความปลอดภัยการสื่อสารข้อมูลผ่านเครือข่ายสาธารณะ โดยการสร้างอุโมงค์เข้ารหัสที่ปกป้องความเป็นส่วนตัว รับประกันความสมบูรณ์ของข้อมูล และเปิดใช้งานการเข้าถึงระยะไกลที่ปลอดภัย โดยใช้โพรโทคอลเช่น PPTP, L2F, L2TP และ IPSec เพื่อรักษามาตรฐานความปลอดภัยสูงและรองรับความต้องการเครือข่ายขององค์กรต่างๆ พร้อมทั้งมอบประโยชน์ต่างๆ เช่น ความเป็นส่วนตัวออนไลน์ที่เพิ่มขึ้น การใช้งาน Wi-Fi ที่ปลอดภัย และการปรับขนาดเครือข่ายที่คุ้มค่าต้นทุน

6.4 บทวิเคราะห์และมุมมองเชิงวิชาการ: ระบบประกันระดับสูงด้วยเครือข่ายส่วนตัวเสมือน (VPN) ในยุค Zero Trust, Cloud-Native และการเรียนการสอนเชิงหลักฐาน

เอกสารคำสอนสัปดาห์ที่ 6 เรื่อง “ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน (VPN)” ได้วางฐานความเข้าใจเรื่องนิยาม/คุณลักษณะของเครือข่ายส่วนตัว-สาธารณะ หลักการทำงานของ VPN ประเภทการใช้งาน (Remote Access, Intranet/Remote Host, Extranet/Remote Network) ตลอดจนโพรโทคอลสำคัญ (PPTP, L2F, L2TP, IPSec) และประโยชน์ด้านความเป็นส่วนตัว/ความมั่นคงปลอดภัย ซึ่งเป็นจุดตั้งต้นที่เป็นรากฐานสำคัญสำหรับยกระดับการออกแบบระบบจริงและการสอนระดับอุดมศึกษาในบริบทปัจจุบันที่ทราฟฟิกถูกเข้ารหัสโดยปริยาย อุปกรณ์หลากหลาย และระบบคลาวด์ครองพื้นที่การทำงาน มีบทวิเคราะห์และมุมมองเชิงวิชาการที่สรุปสาระสำคัญแต่ละหัวข้อได้ดังนี้

1) สังเคราะห์แก่นความรู้จากบทเรียน

โครงแนวคิดในต้นฉบับ

- VPN = “อุโมงค์เข้ารหัส” บนเครือข่ายสาธารณะเพื่อให้ประสบการณ์เหมือนอยู่ในเครือข่ายส่วนตัว: ปกป้องความลับ บุคลากร การยืนยันตัวตน และเอื้อการเข้าถึงระยะไกล (work-from-anywhere)
- ประเภทการใช้งาน 3 กลุ่ม: Remote Access (user ↔ org), Intranet/Remote Host (โฮสต์หนึ่งเชื่อมเข้า intranet), Extranet/Remote Network (site-to-site) พร้อมกรณีใช้จริงขององค์กร/มหาวิทยาลัยหลายวิทยาเขต
- โพรโทคอลหลัก: PPTP, L2F, L2TP (+IPSec), และ IPSec (AH/ESP, โหมด Transport/Tunnel, IKE) รวมถึงประเด็นการจัดการกุญแจและใบรับรอง

นัยต่อการสอน:

ใช้บทนี้เป็น “สะพาน” เชื่อมจากหลักการ (tunneling, crypto, authn/authz) ไปสู่สถาปัตยกรรมร่วมสมัย: Zero Trust, per-app access, policy-as-code, และ VPN-less/identity-aware approach เพื่อให้ผู้เรียนเห็นข้อจำกัด/สมมติฐานของ VPN แบบเดิมและทางเลือกที่เหมาะสมกับงาน

2) วิพากษ์และอัปเดตเชิงวิชาการ: จาก “VPN แบบท่อ” สู่ “การเข้าถึงตามบริบท”

1. **โพรโทคอลและคริปโทสมัยใหม่.** ในทางปฏิบัติการใช้งานปัจจุบันพึ่ง IKEv2/IPSec (รองรับ MOBIKE, NAT-T/UDP 4500, เสถียรเมื่อเปลี่ยนเครือข่าย), TLS-VPN (เช่น OpenVPN ที่วางบน TLS 1.2/1.3), และ WireGuard (Noise-based, codebase เล็ก, UDP, roaming ดี, เลือกใช้ AEAD เช่น ChaCha20-Poly1305/AES-GCM). ส่วน PPTP/L2F ถือว่า **ล้าสมัย** และควรถอดออกจากแผนใช้งานจริง/ลับเพื่อหลีกเลี่ยงการส่งสัญญาณผิดเชิงจริยธรรมด้านความปลอดภัยให้ผู้เรียน
2. **NAT & IPv6.** ต้นฉบับซีซีจำกัด L2TP ไว้เพื่อให้เข้าใจภาพรวม แต่ในงานจริง L2TP/IPSec รองรับ NAT-Traversal (NAT-T) หากอุปกรณ์รองรับ; เมื่อเดินสู่ IPv6-first ประเด็น “ซ่อนที่อยู่” แบบ NAT มีน้ำหนักลดลง—การคุมเข้าถึงจึงควรย้ายศูนย์ถ่วงไปที่ **ตัวตน/อุปกรณ์/บริบท** มากกว่าพึ่งการอำพรางเครือข่าย
3. **Zero Trust / ZTNA / SSE.** VPN ให้สิทธิแบบ “กว้าง” ระดับเครือข่าย (network-level trust). แนวทางร่วมสมัยคือ ZTNA (per-app/identity-aware), micro-segmentation, policy-as-code (เช่นกำกับด้วยกฎประกาศและทดสอบได้) และ continuous verification (ผู้ใช้-อุปกรณ์-สถานที่-ความเสี่ยง) แทน “เชื่อใจเมื่อเข้าโมเมนต์แล้ว”
4. **ยุคกราฟฟิกเข้ารหัส-โดย-ปริยาย.** TLS 1.3/QUIC ทำให้การตรวจแบบ payload-centric ยากขึ้น เฟรมเวิร์กการสังเกตการณ์ควรเน้น **metadata-centric** (DNS, SNI, JA3/JA4, timing, flow) ผนวก EDR/eBPF telemetry ที่ปลายทาง เพื่อให้ทั้งความเป็นส่วนตัวและความสามารถตรวจจับคงอยู่พร้อมกัน
5. **ประสิทธิภาพและเสถียรภาพ.** ควรสอนเรื่อง MTU/MSS clamping, UDP vs TCP-over-TCP meltdown, DSCP/QoS, และผลของ cipher suite/AEAD ต่อ latency/throughput

3) แบบแผนสถาปัตยกรรม (Design Patterns) และข้อควรเลี่ยง (Anti-patterns)

สิ่งที่ควรทำ (Patterns)

- **Per-app VPN / Split-include (ไม่ใช่ split-tunnel แบบเปิดโล่ง):** อนุมัติเฉพาะกราฟฟิกที่จำเป็น ลด blast radius และลดภาระแบนด์วิดท์
- **MFA + Device Posture + Short-lived Credentials:** รวมการยืนยันหลายปัจจัย ตรวจสอบสภาพเครื่อง (OS patch/EDR/ดิสก์เข้ารหัส) และใช้ใบรับรอง/โทเคนอายุสั้น

- NAT-T/NAT64/DNS64/Happy-Eyeballs สำหรับสภาพแวดล้อมผสม IPv4/IPv6 และ mobile/roaming
- Logging ที่เคารพ PDPA: เก็บ “เท่าที่จำเป็น” (minimization), ทำบัญชีเหตุการณ์การถอดรหัสแบบ selective decryption, กำกับ retention/role-based access
สิ่งที่ควรหลีกเลี่ยง (Anti-patterns)
- Full-tunnel ทั้งหมดเสมอ โดยไม่มี control list → เสี่ยง exfiltration/latency สูง
- PPTP/L2F และ DES/MD5 ในสภาพแวดล้อมการผลิตหรือแล็บโดยไม่ป้องกัน → ขัดกับมาตรฐานร่วมสมัย
- Certificate/Key อายุยาวโดยไม่มีการหมุนเวียน และ CRL/OCSP ไม่พร้อม → เพิ่มความเสี่ยง lateral movement
- “อุโมงค์แล้วเชื่อใจทั้งหมด” (Implicit trust) โดยไม่ตรวจสอบต่อเนื่อง → ขัดหลัก Zero Trust

4) ภัยคุกคามต่อ VPN และการควบคุม

- Credential stuffing / MFA fatigue: บังคับ FIDO2 หรือ push-MFA พร้อม number matching; ตรวจจับ login ผิดปกติ/เวลา-สถานที่
- Split-tunnel Exfiltration: ใช้ per-app routing + DNS policy (DNS-over-TLS/HTTPS ภายนอก) และ data-aware egress control
- Endpoint compromise: บังคับ EDR + local firewall + disk encryption, block access เมื่อ posture ไม่ผ่าน
- Server/PKI compromise: ทำ key rotation อัตโนมัติ, short-lived certs, HSM/TPM สำหรับ key material
- Misconfiguration/Shadow IT: Detection-as-Code (lint/test rule ก่อน deploy), Inventory สม่ำเสมอ, least-privilege for admin

บทเรียน VPN ในไฟล์แนบให้ “โครงการดูแลสุขภาพ” ที่ครบถ้วนสำหรับนิยาม ประเภท และโปรโตคอล เราต่อยอดด้วยสถาปัตยกรรมร่วมสมัย (Zero Trust/per-app, NAT-T/roaming, AEAD-first) พร้อมกรอบการ

สอนเชิงหลักฐานที่เน้นผลทดลอง-วิเคราะห์-สรุปเชิงระบบ เพื่อผลิตบัณฑิตที่ออกแบบ/ประเมิน/ปรับปรุงระบบได้
จริงภายใต้ข้อกำหนดด้านกฎหมายและจริยธรรมของไทย

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความหมายและหลักการทำงานของ VPN

แนวคำตอบ: VPN = อุโมงค์เข้ารหัสบนเครือข่ายสาธารณะ ทำให้การสื่อสารปลอดภัยเทียบเท่าเครือข่ายส่วนตัว มีคุณสมบัติ: Encryption, Tunneling, Hide IP

ข้อ 2. เปรียบเทียบความแตกต่างของ Private Network และ Public Network

แนวคำตอบ: Private = จำกัดการเข้าถึง, ควบคุมได้, ปลอดภัยสูง; Public = ทุกคนเข้าถึงได้, เสี่ยงสูง, ไม่สามารถควบคุมเส้นทางข้อมูล

ข้อ 3. อธิบายประเภทการใช้งาน VPN และยกตัวอย่าง

แนวคำตอบ: Remote Access VPN (พนักงานเชื่อมต่อจากบ้าน), Intranet VPN (โฮสต์ภายใน), Extranet VPN (บริษัท-คู่ค้า)

ข้อ 4. วิเคราะห์ข้อดี-ข้อเสียของโปรโตคอล PPTP และ IPSec

แนวคำตอบ: PPTP = ใช้งานง่าย, overhead ต่ำ แต่ความปลอดภัยต่ำ; IPSec = ปลอดภัยสูง, รองรับ Encryption/Authentication, overhead สูง

ข้อ 5. อธิบายประโยชน์ของการใช้ VPN ในองค์กร

แนวคำตอบ: ปกป้องข้อมูลบนเครือข่ายสาธารณะ, ทำงานจากระยะไกลได้, ป้องกันการดักฟัง, ลดต้นทุนโครงสร้างพื้นฐาน

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. VPN ย่อมาจากข้อใด

- ก. Virtual Private Network
- ข. Virtual Public Network
- ค. Verified Private Network
- ง. Virtual Protected Network

เฉลย: ก

ข้อ 2. คุณสมบัติสำคัญของ VPN คือข้อใด

- ก. การเข้ารหัสและการสร้างอุโมงค์
- ข. การเพิ่ม Bandwidth
- ค. การแทนที่ Firewall
- ง. การจัดการ DNS

เฉลย: ก

ข้อ 3. การเชื่อมต่อ Remote Access VPN มีประโยชน์อย่างไร

- ก. ทำให้ผู้ใช้เข้าถึงเครือข่ายภายในจากภายนอกได้
- ข. เพิ่มความเร็วอินเทอร์เน็ต
- ค. ใช้แทน Proxy Server
- ง. ลดการใช้ CPU ของเครื่องลูกข่าย

เฉลย: ก

ข้อ 4. PPTP ทำงานบนเลเยอร์ใดเป็นหลัก

- ก. Application Layer

ข. Data Link Layer

ค. Transport Layer

ง. Physical Layer

เฉลย: ข

ข้อ 5. โพรโทคอล VPN ไตปลอดภัยที่สุด

ก. PPTP

ข. L2F

ค. L2TP

ง. IPSec

เฉลย: ง

ข้อ 6. การใช้ VPN ร่วมกับ Wi-Fi สาธารณะมีข้อดีใด

ก. เพิ่มความปลอดภัยในการสื่อสาร

ข. ลดค่าใช้จ่ายอินเทอร์เน็ต

ค. ทำงานได้เร็วขึ้นเสมอ

ง. ใช้แทนการเข้ารหัส HTTPS

เฉลย: ก

ข้อ 7. การเชื่อมต่อ Intranet VPN มีวัตถุประสงค์หลักใด

ก. เชื่อมต่อผู้ใช้ภายในองค์กรเข้ากับทรัพยากรเครือข่าย

ข. ให้สิทธิ์เข้าถึงเว็บสาธารณะ

ค. ใช้สำหรับบริการ DNS

ง. ใช้สำหรับการเข้ารหัสอีเมล

เฉลย: ก

ข้อ 8. องค์ประกอบใดเป็นส่วนหนึ่งของ IPSec

ก. AH และ ESP

ข. PPTP และ L2F

ค. GRE และ NAT

ง. SSL และ TLS

เฉลย: ก

ข้อ 9. การใช้ VPN แบบ Extranet เหมาะกับกรณีใด

ก. เชื่อมต่อพนักงานในองค์กร

ข. เชื่อมต่อคู่ค้าและลูกค้าที่ได้รับสิทธิ์เข้ากับเครือข่าย

ค. เชื่อมต่อเครื่องภายในบ้านเข้ากับเครือข่าย

ง. ใช้แทนการเข้าถึงฐานข้อมูล

เฉลย: ข

ข้อ 10. ข้อใดคือประโยชน์สำคัญของ VPN สำหรับธุรกิจ

ก. เข้าถึงเครือข่ายระยะไกลอย่างปลอดภัย

ข. ทำให้ระบบรวดเร็วขึ้นเสมอ

ค. ลดจำนวนเซิร์ฟเวอร์ที่ต้องใช้

ง. ยกเลิกความจำเป็นของ Firewall

เฉลย: ก

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ. (ม.ป.ป.). : ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน (Virtual Private Network). เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Donenfeld, J. (2018). WireGuard: Next Generation Kernel Network Tunnel. (whitepaper).

Huttunen, A., et al. (2005). UDP Encapsulation of IPsec ESP Packets (NAT-T) (RFC 3948) & Negotiation (RFC 3947). IETF.

Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296). IETF.

Kent, S., & Seo, K. (2005). Security Architecture for the Internet Protocol (RFC 4301). IETF.

NIST. (2020). Zero Trust Architecture (SP 800-207).

NIST. (2021). Guide to IPsec VPNs (SP 800-77, Rev. 1).

NIST. (2024). Cybersecurity Framework 2.0.

OpenVPN Project. (2020). OpenVPN Protocol and TLS 1.3 Hardening Guide.

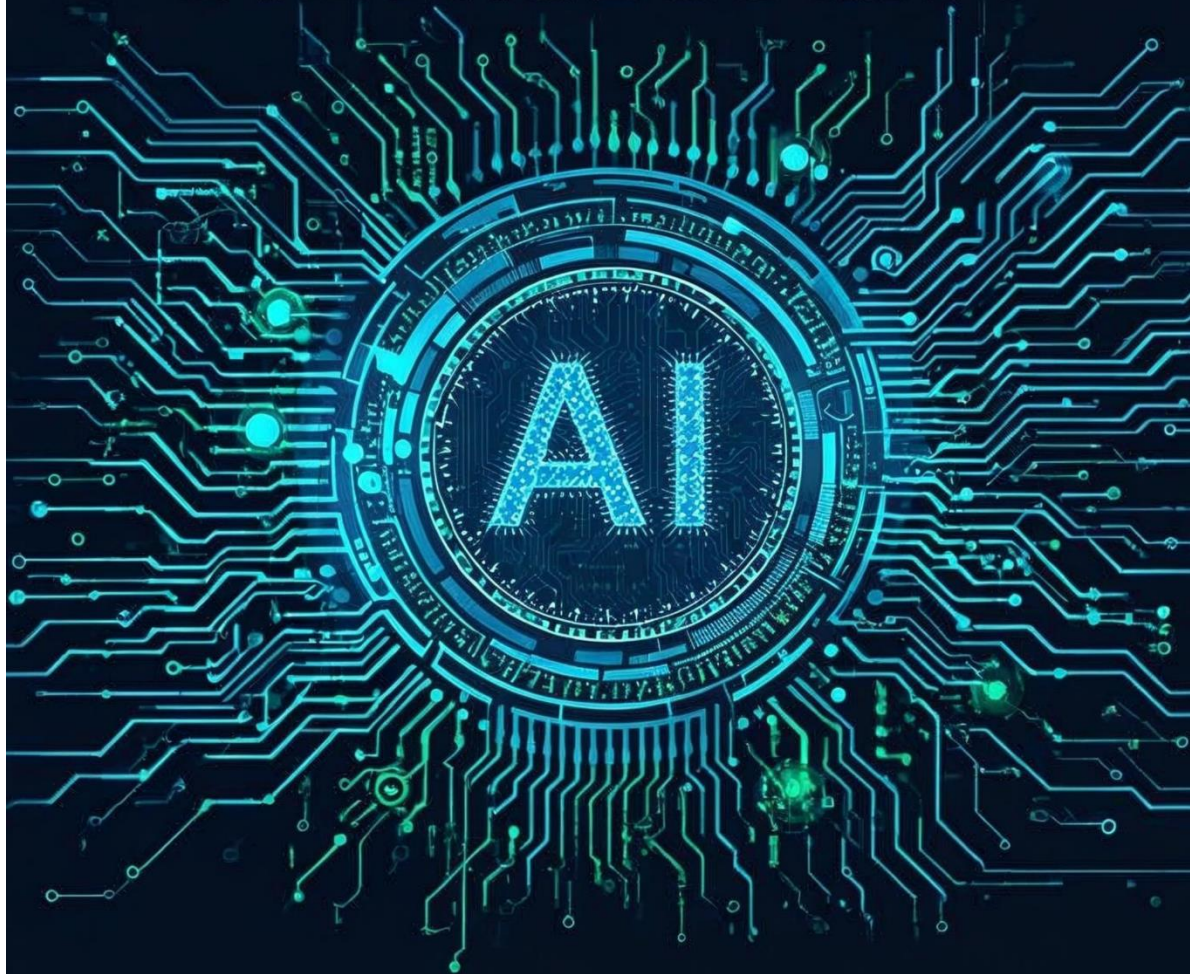
"virtual private network". NIST Computer Security Resource Center Glossary. Archived from the original on 2 January 2023. Retrieved 2 January 2023.

บทที่ 7

พื้นฐานวิทยาการรหัสลับ

Cryptography Overview

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์
CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์ศรีบุญ

สัปดาห์ที่ 7 พื้นฐานวิทยาการรหัสลับ (Cryptography Overview)

รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์
(Cyber Security Principles)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบบทนี้ นักศึกษาจะสามารถ:

- อธิบายความหมาย องค์ประกอบ และประเภทของระบบรหัสลับได้อย่างถูกต้อง
- วิเคราะห์ความแตกต่างระหว่างการเข้ารหัสแบบกุญแจสมมาตรและกุญแจอสมมาตรได้
- อธิบายหลักการทำงานของขั้นตอนวิธีการเข้ารหัสที่สำคัญ เช่น DES, 3DES, AES, RSA ได้
- ประเมินความมั่นคงปลอดภัยและความเสี่ยงจากการโจมตีทางรหัสลับ (Brute-force, Cryptanalysis) ได้
- ประยุกต์ใช้ความรู้ทางวิทยาการรหัสลับเพื่อแก้ไขปัญหาด้านความมั่นคงปลอดภัยสารสนเทศในสถานการณ์จริงได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบบทนี้ นักศึกษาจะสามารถ:

- ระบุและอธิบายองค์ประกอบพื้นฐานของระบบรหัสลับได้
- เปรียบเทียบข้อดี-ข้อจำกัดของการเข้ารหัสแบบสมมาตรและอสมมาตรได้
- อธิบายการทำงานของขั้นตอนวิธี DES, AES, RSA และลายมือชื่อดิจิทัลได้
- วิเคราะห์การโจมตีระบบรหัสลับและเสนอวิธีการป้องกันได้
- ใช้ความรู้รหัสลับในการเสนอแนวทางรักษาความปลอดภัยข้อมูลในกรณีศึกษาได้

3. หัวข้อเนื้อหา:

พื้นฐานวิศวกรรมการเข้ารหัสดิจิทัล

7.1 วิทยาการรหัสลับ

7.1.1 ความหมายของวิทยาการรหัสลับ

7.1.2 องค์ประกอบของระบบรหัสลับ

7.1.3 ประเภทของระบบรหัสลับ

7.2 การเข้ารหัสลับแบบกุญแจสมมาตร

7.2.1 การเข้ารหัสข้อมูลแบบ DES

7.2.2 การเข้ารหัสข้อมูลแบบ 2DES

7.2.3 การเข้ารหัสข้อมูลแบบ 3DES

7.2.4 การเข้ารหัสแบบ AES

7.3 การเข้ารหัสลับแบบกุญแจแอสสมมาตร

7.3.1 Diffie-Hellman

7.3.2 โพรโทคอล Oakley

7.3.3 RSA

7.3.4 ลายมือชื่อดิจิทัล

7.4 การโจมตีระบบรหัสลับ

7.4.1 การวิเคราะห์รหัสลับ

7.4.2 การโจมตีแบบ Brute-force

7.4.3 ความมั่นคงของขั้นตอนวิธีการเข้ารหัสลับ

7.4.4 ขั้นตอนวิธีที่ปลอดภัยโดยปราศจากเงื่อนไข

7.4.5 ขั้นตอนวิธีที่ปลอดภัยเชิงคำนวณ

7.5. บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา:

ธนาคาร *RMUTT ThaiSecure Bank* ต้องการให้ลูกค้าสามารถทำธุรกรรมออนไลน์ได้อย่างปลอดภัย ปัจจุบันยังใช้การเข้ารหัสแบบ DES ซึ่งถูกมองว่าไม่ปลอดภัยแล้ว ทีม IT ต้องตัดสินใจว่าจะเปลี่ยนไปใช้ AES หรือ RSA ในการรักษาความปลอดภัยของข้อมูลการทำธุรกรรม

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

- วิเคราะห์ข้อดี-ข้อเสียของ DES, AES, และ RSA ในบริบทการทำธุรกรรมออนไลน์
- ระบุประเภทของการเข้ารหัส (สมมาตร/อสมมาตร) และผลต่อการจัดการกุญแจ
- เสนอทางเลือกที่เหมาะสมที่สุดสำหรับธนาคาร พร้อมเหตุผลเชิงเทคนิคและการประยุกต์ใช้งานจริง
- จัดทำสรุปและนำเสนอผลในชั้นเรียน

ประเด็นการเรียนรู้ที่สำคัญ:

- ความแตกต่างระหว่างการเข้ารหัสสมมาตรและอสมมาตร
- ขั้นตอนวิธี DES, 3DES, AES, RSA
- ปัญหาการจัดการกุญแจและความมั่นคงปลอดภัยของระบบรหัสลับ
- การโจมตีรหัสลับแบบ Brute-force และ Meet-in-the-middle

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์เชิง วิชาการ (30)	ถูกต้อง ครอบคลุม DES/AES/RSA	ถูกต้องเกือบ ทั้งหมด	ขาดบางส่วน	ไม่ถูกต้อง
การเชื่อมโยงกรณีศึกษา (25)	เหมาะสมและ สมเหตุสมผล	เชื่อมโยงได้ บางส่วน	ไม่ชัดเจน	ไม่สอดคล้อง
การเสนอแนวทางแก้ไข (30)	มีเหตุผล ครอบคลุมทั้ง เทคนิคและนโยบาย	มีบางเหตุผล	ยังไม่ชัดเจน	ไม่มีข้อเสนอ
การนำเสนอ (15)	ชัดเจน ใช้สื่อประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

7. พื้นฐานวิทยาการรหัสลับ

ในบทนี้จะทำความเข้าใจเกี่ยวกับสาระสำคัญของวิทยาการรหัสลับ ซึ่งถือเป็นกลไกสำคัญที่ใช้ในการรับมือกับภัยคุกคามบนระบบคอมพิวเตอร์และเครือข่าย วิทยาการรหัสลับที่มักนิยมเรียกว่า การเข้ารหัสลับ มักเป็นวิธีการพื้นฐานที่ถูกนำไปใช้ในการป้องกันภัยคุกคามบนระบบคอมพิวเตอร์ ซึ่งไม่เพียงถูกนำไปใช้ในการเข้ารหัสและถอดรหัสข้อมูลโดยตรงเท่านั้น แต่ยังสามารถใช้ผสมผสานร่วมกับระบบความปลอดภัยอื่นๆ ได้อีกด้วย เนื้อหาในบทนี้จะเริ่มจากการอธิบายพื้นฐานของวิทยาการรหัสลับ เนื้อหาในส่วนนี้ จะอธิบายถึงเทคโนโลยีที่สำคัญของการเข้ารหัสลับ หัวข้อที่อธิบายประกอบด้วย องค์ประกอบของระบบรหัสลับ, ประเภทของระบบรหัสลับ, การเข้ารหัสลับทั้งแบบกุญแจสมมาตรและแบบกุญแจอสมมาตร, การโจมตีระบบรหัสลับ และความมั่นคงของขั้นตอนวิธีการเข้ารหัสลับ

7.1 ความหมายของวิทยาการรหัสลับ (Cryptography)

โดยทั่วไป ข้อมูลที่ถูกส่งผ่านไปบนเครือข่ายจะอยู่ในรูปแบบข้อมูลปกติ (Clear text) ซึ่งสามารถถูกดักอ่านหรือคัดลอกได้ด้วยเทคนิคที่เรียกว่า สนิฟฟิง (Sniffing) โดยอาศัยเครื่องมือต่างๆ เช่น การวิเคราะห์โพรโทคอล (Protocol analyzer), โปรแกรมสำหรับเฝ้าสังเกตเครือข่าย (Network monitor) ซึ่งมีอยู่อย่างแพร่หลาย เนื่องจากช่องทางดังกล่าวถือว่าเป็นช่องสัญญาณที่ไม่ปลอดภัย (Insecure channel) ดังนั้น การเข้ารหัสข้อมูลก่อนการส่งผ่านเครือข่ายจึงช่วยรักษาความปลอดภัยได้เป็นอย่างดี

การเข้ารหัสข้อมูล (Data encryption) คือวิธีการแปลงข้อมูลปกติให้กลายเป็นข้อมูลเข้ารหัส หรือข้อความไซเฟอร์ (Cipher text) แล้วจึงส่งผ่านเครือข่ายไปยังผู้รับ จากนั้นจะทำการถอดรหัสข้อมูล (Decryption) เพื่อให้ได้ข้อมูลเดิม กระบวนการเข้ารหัสและถอดรหัสข้อมูลนี้เรียกว่า วิทยาการรหัสลับ (Cryptography) ซึ่งมีมาตั้งแต่อดีตส่วนใหญ่ถูกใช้สำหรับการส่งข่าวสารของทหารในสงคราม คำว่า cryptography นี้มาจากภาษากรีกซึ่งมีความหมาย 2 อย่าง ได้แก่ การเขียนความลับ (Secret writing) และศาสตร์และศิลป์ในการปิดบังความหมาย [62] ส่วนการวิเคราะห์รหัสลับ (Cryptanalysis) คือการวิเคราะห์เพื่อแกะหรือถอดข้อความที่เข้ารหัสลับด้วยวิธีการต่างๆ เพื่อให้การเข้ารหัสลับนั้นปราศจากความหมาย งานด้านวิทยาการรหัสลับจะประกอบด้วยบุคคล 2 ประเภทที่ทำงานตรงข้ามกัน ได้แก่ นักสร้างรหัสลับ (Cryptographer) ซึ่งทำหน้าที่ออกแบบขั้นตอนวิธีในการเข้าและถอดรหัสลับ ส่วนอีกบุคคลหนึ่งเรียกว่า นักวิเคราะห์รหัสลับ (Cryptanalyst) ซึ่งทำหน้าที่วิเคราะห์หาจุดอ่อนของขั้นตอนวิธีของการเข้าและถอดรหัสลับเพื่อโจมตี

วิทยาการเข้ารหัสลับได้มีการพัฒนาเทคนิคสำหรับการเข้ารหัสลับอยู่หลายวิธี เทคนิคพื้นฐานของการเข้ารหัสลับแบบฉบับ (Classical cryptography) ได้แก่ วิธีการแทนที่และวิธีการสลับตำแหน่งภายในชุดข้อความ นอกจากนี้ อาจใช้เทคนิคการเข้ารหัสลับที่ตัวข้อความต้นฉบับ ได้แก่ การแบ่งข้อความต้นฉบับออกเป็นบล็อกๆ

แล้วทำการเข้ารหัสลับข้อความต้นฉบับที่ละบล็อก วิธีนี้เรียกว่า ไซเฟอร์แบบบล็อก ส่วนอีกแบบหนึ่งเรียกว่าไซเฟอร์แบบสตรีม เป็นการเข้ารหัสข้อความต้นฉบับทีละบิต แต่วิธีการเข้ารหัสทีละบิตต้องใช้เวลาในการเข้าและถอดรหัส นานกว่าแบบบล็อกมาก ปัจจุบัน จึงนิยมการเข้ารหัสแบบบล็อกมากกว่า อีกวิธีหนึ่งจะใช้กุญแจเป็นหลักในการเข้าและถอดรหัส ได้แก่ การเข้ารหัสลับแบบกุญแจสมมาตร และแบบกุญแจอสมมาตร

7.2 องค์ประกอบของระบบรหัสลับ

ส่วนประกอบพื้นฐานของวิทยาการรหัสลับ เรียกว่า ระบบรหัสลับ (Cryptosystem) ระบบรหัสลับใดๆ ก็ตาม จะมีองค์ประกอบสำคัญอยู่ 5 ส่วน ได้แก่ [81] ข้อความต้นฉบับ, ขั้นตอนวิธีการเข้ารหัส, กุญแจลับ, ข้อความไซเฟอร์ และขั้นตอนวิธีการถอดรหัสลับ

7.2.1 ข้อความต้นฉบับ (Plaintext) หมายถึงข้อมูลต้นฉบับซึ่งอาจอยู่ในรูปแฟ้มข้อมูลหรือแฟ้มโปรแกรมก็ได้ ที่เราต้องการนำไปเข้ารหัสลับ

7.2.2 ขั้นตอนวิธีการเข้ารหัสลับ (Encryption algorithm) หมายถึงกระบวนการที่ใช้ในการเปลี่ยนแปลงข้อความต้นฉบับให้อยู่ในรูปแบบที่เปลี่ยนไปจากเดิม โดยที่ผู้อื่นไม่สามารถเข้าใจข้อความต้นฉบับได้

7.2.3 กุญแจลับ (Key) เป็นองค์ประกอบที่ใช้ร่วมกันกับขั้นตอนวิธีการเข้ารหัสลับเพื่อแปลงข้อความต้นฉบับให้เป็นข้อความเข้ารหัสและ/หรือใช้ร่วมกันในขั้นตอนของการถอดข้อความเข้ารหัสให้กลับไปเป็นข้อความต้นฉบับดั้งเดิม กุญแจลับที่ใช้ในกระบวนการดังกล่าวนี้ไม่ขึ้นอยู่กับข้อความต้นฉบับ

7.2.4 ข้อความเข้ารหัสหรือข้อความไซเฟอร์ (Ciphertext) เป็นผลลัพธ์ที่ได้จากการนำข้อความต้นฉบับไปผ่านกระบวนการเข้ารหัสด้วยกุญแจลับ ข้อความไซเฟอร์จะอยู่ในรูปแบบที่ผู้อื่นไม่สามารถอ่านเข้าใจข้อความเดิมได้

7.2.5 ขั้นตอนวิธีการถอดรหัส (Decryption algorithm) กระบวนการในการแปลงข้อความไซเฟอร์ให้กลับไปอยู่ในรูปแบบของข้อความต้นฉบับ โดยอาศัยกุญแจลับที่สัมพันธ์กับขั้นตอนในการเข้ารหัสข้อความ

7.3 ประเภทของระบบรหัสลับ

ดังที่กล่าวไว้แล้วในหัวข้อก่อนหน้านี้ว่า ระบบรหัสลับนั้นสามารถจำแนกออกเป็นประเภทต่างๆ ได้มากมาย ในที่นี้จะขอพิจารณาเกณฑ์ที่ใช้แบ่ง 3 รูปแบบ ได้แก่ การแปลงจากข้อความต้นฉบับไปเป็นข้อความไซเฟอร์ จำนวนกุญแจที่ใช้ และวิธีการเข้ารหัสข้อความต้นฉบับ

7.3.1 การแปลงจากข้อความต้นฉบับไปเป็นข้อความไซเฟอร์

สามารถทำได้ 2 แบบ ได้แก่ การแทนที่ (Substitution cipher) ซึ่งเป็นการเปลี่ยนแปลงส่วนประกอบในข้อความต้นฉบับไปเป็นรูปแบบที่แตกต่างไปจากข้อความไซเฟอร์ และการสลับตำแหน่ง (Transposition หรือ permutation cipher) ซึ่งเป็นวิธีการสลับตำแหน่งของส่วนประกอบในข้อความต้นฉบับเท่านั้น โดยที่เนื้อหาที่ปรากฏในข้อความต้นฉบับยังเหมือนเดิม ทั้งสองวิธีดังกล่าว จะต้องคงไว้ซึ่งข้อมูลเดิมภายหลังการถอดรหัส ข้อมูลเดิมต้องไม่สูญหายเมื่อกระทำแบบย้อนกลับ การเข้ารหัสด้วยวิธีนี้ในทางปฏิบัติอาจเลือกใช้เพียงวิธีใดวิธีหนึ่งหรือใช้ทั้งสองวิธีควบคู่กันก็ได้

7.3.2 จำนวนกุญแจที่ใช้

ในการเข้าและถอดรหัสระหว่างผู้รับและผู้ส่งข้อมูล ถ้าใช้กุญแจดอกเดียวกันในการเข้าและถอดรหัสเรียกว่า การเข้ารหัสแบบสมมาตร หรือการเข้ารหัสแบบกุญแจลับ ถ้าผู้ส่งและผู้รับต่างใช้กุญแจในการเข้าและถอดรหัสคนละดอก เราเรียกวินี้ว่า การเข้ารหัสแบบอสมมาตร หรือการเข้ารหัสแบบกุญแจสาธารณะ ซึ่งจะขยายความในหัวข้อถัดไปเนื่องจากมีความสำคัญกับงานวิจัยนี้

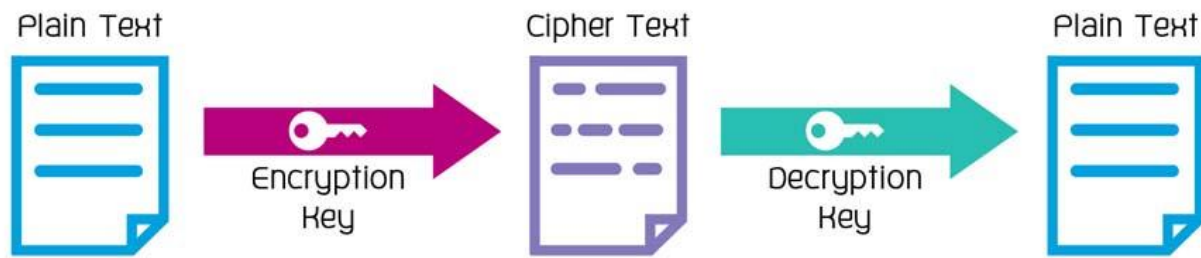
7.3.3 การเข้ารหัสข้อความต้นฉบับ

เราสามารถเข้ารหัสข้อความต้นฉบับได้ 2 วิธี วิธีแรก ได้แก่ ไซเฟอร์แบบบล็อก (Block cipher) เป็นการแบ่งข้อความต้นฉบับออกเป็นส่วนๆ แต่ละส่วนเรียกว่าบล็อก จากนั้น ทำการเข้ารหัสข้อความต้นฉบับทีละบล็อกไปจนครบ อีกวิธีหนึ่งได้แก่ไซเฟอร์แบบสตรีม (Stream cipher) เป็นการเข้ารหัสข้อความต้นฉบับทีละบิตแบบหลังนี้จะใช้เวลานานกว่าแบบแรกอยู่มาก ดังนั้น การเข้ารหัสข้อความต้นฉบับส่วนใหญ่จึงนิยมใช้ไซเฟอร์แบบบล็อก

7.4 การเข้ารหัสลับแบบกุญแจสมมาตร (Symmetric key encryption scheme)

การเข้ารหัสลับแบบกุญแจสมมาตร บางทีเรียกว่า การเข้ารหัสแบบกุญแจเดียว (Single key encryption scheme) เป็นวิธีการเข้ารหัสและถอดรหัสโดยใช้กุญแจลับ (Secret key หรือ shared key) ตัวเดียวกัน กุญแจลับหรือบางทีเรียกสั้นๆ ว่า กุญแจ ที่ใช้จะมีความยาวคงที่ ความยาวของกุญแจมีผลโดยตรงต่อความมั่นคงของความปลอดภัย มีลักษณะการทำงานดังแสดงในรูป 7.1

ประสิทธิภาพที่โดดเด่นของวิธีการเข้ารหัสลับแบบสมมาตรคือความเร็วในการเข้าและถอดรหัส จึงได้รับความนิยมเป็นอย่างมากในเวลาต่อมา มีผู้พัฒนาขั้นตอนวิธีสำหรับการเข้าและถอดรหัสข้อมูลประเภทนี้อยู่มากมาย เช่น RC-4, DES, Triple-DES เป็นต้น



รูป 7.1 การทำงานของระบบการเข้ารหัสลับแบบกุญแจสมมาตร

(ที่มา: etda.or.th)

เนื่องจาก การเข้ารหัสลับแบบกุญแจสมมาตรนี้ ขั้นตอนวิธีในการเข้าและถอดรหัสข้อมูลนั้นล้วนเป็นมาตรฐานที่เปิดเผยทั่วไปต่อสาธารณะ ดังนั้น ความมั่นคงปลอดภัยของข้อมูลจึงอยู่ที่กุญแจเป็นสำคัญ กุญแจจึงไม่เป็นที่เปิดเผยต้องเก็บเป็นความลับเสมอ ใครก็ตามที่ได้กุญแจไปก็สามารถถอดรหัสข้อมูลได้ หากกุญแจตกอยู่ในความครอบครองของผู้บุกรุก ระบบทั้งหมดก็ปราศจากความปลอดภัย ดังนั้น การส่งมอบกุญแจจากผู้ส่งข้อมูลไปยังผู้รับจึงจำเป็นต้องมั่นใจได้ว่าถูกส่งไปในช่องทางที่ปลอดภัยอย่างเพียงพอ การกระจายกุญแจไปยังผู้รับที่เกี่ยวข้องถือเป็นปัญหาสำคัญของวิธีการเข้ารหัสแบบสมมาตร และเนื่องจากความมั่นคงของกุญแจขึ้นอยู่กับความยาวของกุญแจ หมายความว่าหากมีการออกแบบให้กุญแจมีความยาวมากขึ้น ความปลอดภัยก็ย่อมเพิ่มมากขึ้น เพราะผู้บุกรุกต้องใช้เวลานานมากขึ้นในการถอดรหัสของกุญแจ แต่นั่น ก็จะได้มาพร้อมกับกระบวนการที่ใช้ในการคำนวณสำหรับการเข้าและถอดรหัสลับย่อมใช้เวลานานเพิ่มขึ้นไปด้วย และมีค่าใช้จ่ายในการคำนวณเพิ่มมากขึ้น ส่งผลโดยตรงต่อประสิทธิภาพซึ่งเป็นข้อโดดเด่นของวิธีการแบบนี้

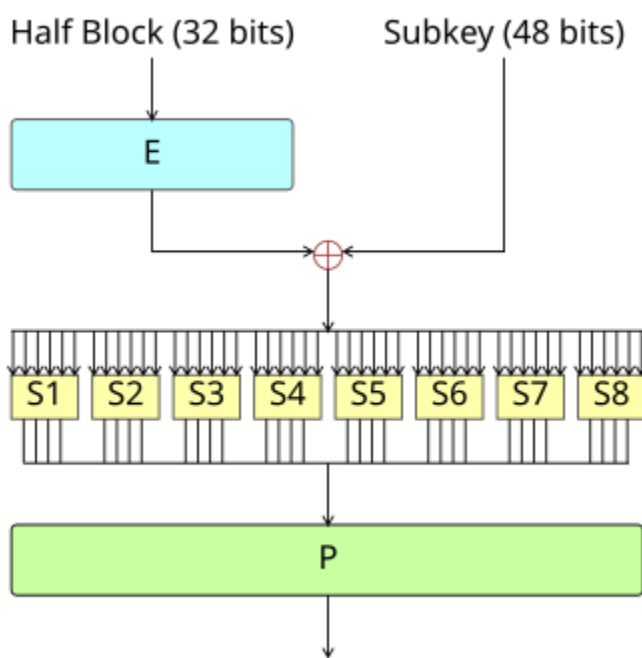
เพื่อให้เห็นหลักการทำงานของวิธีการเข้ารหัสลับแบบสมมาตร จะอธิบายโดยสรุปถึงขั้นตอนวิธีของการเข้ารหัสลับแบบสมมาตรที่มีความปลอดภัยสูงและได้รับความนิยมเป็นเวลานาน ได้แก่ DES, 2DES และ 3DES ซึ่งมีพื้นฐานมาจากแนวคิดเดียวกัน และ AES ซึ่งมีหลักการพื้นฐานมาจากขั้นตอนวิธี DES เช่นเดียวกัน

7.4.1 การเข้ารหัสข้อมูลแบบ DES (Data Encryption Standard)

มาตรฐานการเข้ารหัสข้อมูลแบบ DES มีพื้นฐานการเข้ารหัสที่ได้รับการพัฒนาจากบริษัทไอบีเอ็ม โดยเรียกว่า ลูซิเฟอร์ (Lucifer ใช้กุญแจขนาด 128 บิต) จนกระทั่งในปี พ.ศ. 2520 รัฐบาลสหรัฐได้กำหนดให้ใช้ DES ในการเข้ารหัสข้อมูลที่มีชั้นความลับน้อย DES เป็นขั้นตอนวิธีที่ได้รับความนิยมกันอย่างแพร่หลายในธุรกิจอุตสาหกรรมทั่วไป แต่ปัจจุบันถือว่าไม่ปลอดภัยแล้ว เนื่องจากการโจมตี DES ด้วยการถอดรหัสนั้นสามารถกระทำได้อย่างง่ายดายและรวดเร็ว

การเข้ารหัสแบบ DES ประกอบด้วย 2 ส่วน ได้แก่ การจัดเตรียมกุญแจ (Key scheduled) และการเข้ารหัสลับ (Enciphered) โดยกุญแจมีความยาว 56 บิต โดยกรรมวิธีทำงานล้วนแต่อาศัยกล่องอยู่ 2 กล่อง ได้แก่ กล่องสลับลำดับ หรือเรียกว่า P-box (Permutation box) และกล่องสลับลำดับ หรือเรียกสั้นๆ ว่า S-box (Substitution box) มีขั้นตอนการทำงานดังแสดงในรูป 8.2

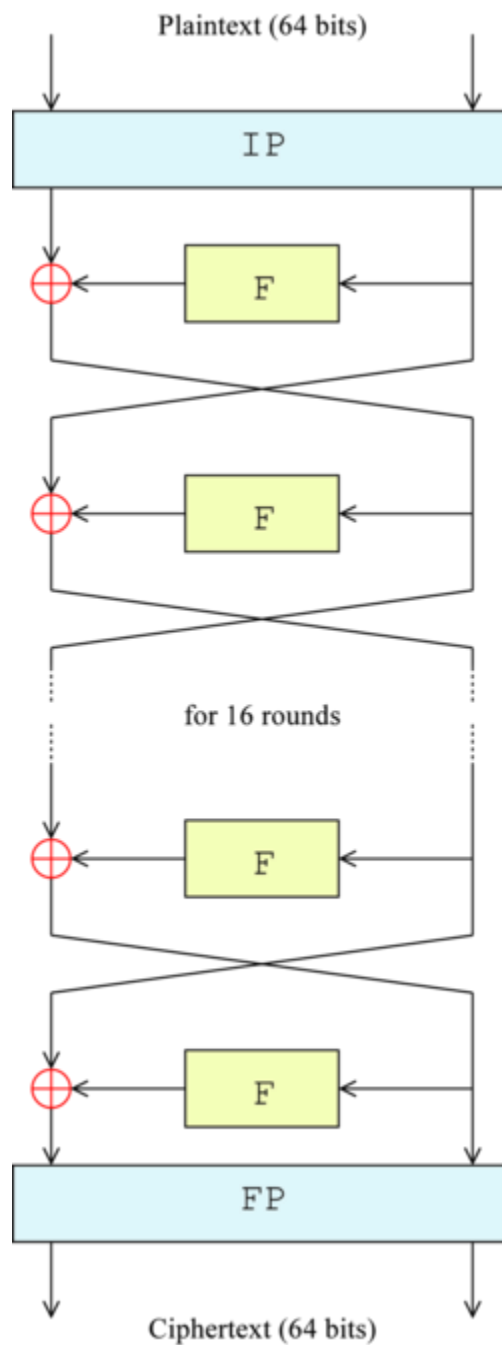
ข่าวสารจะถูกแบ่งออกเป็นบล็อกขนาด 64 บิต และใช้บิตที่เหลือจำนวน 8 บิตสำหรับเป็นบิตตรวจสอบ (Parity bit) มีขั้นตอนการเข้ารหัสทั้งหมดจำนวน 18 ขั้นตอน แต่ขั้นตอนการเข้ารหัสจริงมีเพียง 16 ขั้นตอน เพราะขั้นตอนแรกและสุดท้ายคือการสลับบิต (Permutation) เท่านั้นโดยไม่ใช้กุญแจเข้าไปร่วมด้วย ส่วนขั้นตอนการเข้ารหัสจะใช้วิธีการเดียวกันทั้ง 16 ขั้นตอน โดยใช้ผลลัพธ์ที่ได้จากขั้นตอนก่อนหน้านี้ไปเป็นข้อมูลนำเข้าของขั้นตอนถัดไป ข้อมูลนำเข้าจะถูกแบ่งออกเป็น 2 ส่วน ส่วนทางซ้ายขนาด 32 บิต (L_i) และส่วนทางขวา (R_i) ส่วนทางขวาจะถูกนำไปเป็นส่วนทางซ้ายของผลลัพธ์ ส่วนทางซ้ายและส่วนทางขวาพร้อมด้วยกุญแจ 48 บิต ที่ได้จากการคำนวณกุญแจหลัก 56 บิต นั้นจะเป็นข้อมูลนำเข้าของฟังก์ชันการเข้ารหัส ซึ่งเป็นการทำ XOR ในระดับบิต จากนั้น ผลลัพธ์ที่ได้ก็จะถูกนำไปเป็นส่วนทางขวาของผลลัพธ์ต่อไป ส่วนการถอดรหัสนั้นจะใช้วิธีการเช่นเดียวกันกับการเข้ารหัส และใช้กุญแจตัวเดียวกัน แต่กระทำการย้อนกลับขั้นตอนการเข้ารหัสนั่นเอง



รูป 7.2 ฟังก์ชัน Feistel (ฟังก์ชัน F) ของ DES ทั้งหมด (wikipedia.org)

สำหรับประเด็นเรื่องความปลอดภัยของมาตรฐาน DES นั้น เนื่องจากกุญแจที่ใช้ในกระบวนการเข้ารหัสและถอดรหัสแบบ DES มีขนาดเพียง 56 บิต ซึ่งทำให้จำนวนกุญแจทั้งหมดที่เป็นไปได้คือ 2^{56} หรือ 7.2×10^{16} ดังนั้น การโจมตีกุญแจโดยการค้นหาค่าทุกค่าที่เป็นไปได้ของระบบ DES นั้นจึงความเป็นไปได้สูง ซึ่งต่อมาภายหลัง

พบว่า การถอดรหัสข้อมูลแบบ DES โดยไม่ทราบกุญแจจะถูกถอดได้โดยใช้เวลาไม่นานนักด้วยประสิทธิภาพของคอมพิวเตอร์ในปัจจุบัน ดังนั้น การเข้ารหัสแบบ DES จึงถือว่าไม่มีความปลอดภัยอีกในปัจจุบัน



รูป 7.3 แผนภาพแสดงการเข้ารหัสลับของขั้นตอนวิธีแบบ DES (wikipedia.org)

อย่างไรก็ตาม แม้ระบบ DES จะมีจุดอ่อนอยู่ที่กุญแจซึ่งมีขนาดเล็กก็ตาม แต่พบว่าโดยพื้นฐานแล้ว ขั้นตอนวิธีที่ใช้ในการเข้ารหัสและถอดรหัสของ DES นั้นกลับไม่มีจุดอ่อนรุนแรงพอที่จะโจมตีได้ง่าย ต่อมาภายหลัง จึงมี

ผู้พัฒนาขั้นตอนวิธีที่มีความปลอดภัยสูงขึ้นโดยอยู่บนพื้นฐานของขั้นตอนวิธีแบบ DES เรียกว่า ขั้นตอนวิธีแบบ AES อีกวิธีหนึ่งคือการพัฒนาการใช้ขั้นตอนวิธีของ DES ให้มีความแข็งแกร่งขึ้นโดยทำการเข้ารหัสลับมากกว่า 1 ครั้ง โดยไม่จำเป็นต้องพัฒนาขั้นตอนวิธีขึ้นมาใหม่ เนื่องจาก DES ได้รับการพัฒนามานานและใช้งานกันอย่างแพร่หลาย การเปลี่ยนไปใช้การเข้ารหัสลับแบบใหม่ย่อมมีค่าใช้จ่ายสูงในการเปลี่ยนย้ายระบบ จึงใช้วิธีการเข้ารหัสลับโดยใช้ขั้นตอนวิธีแบบ DES มากกว่า 1 ครั้ง เรียกว่า การเข้ารหัสโดยใช้ DES 2 ครั้ง และการเข้ารหัสโดยใช้ DES 3 ครั้ง

7.4.2 การเข้ารหัสข้อมูลแบบ DES 2 ครั้ง (Double DES หรือ 2DES)

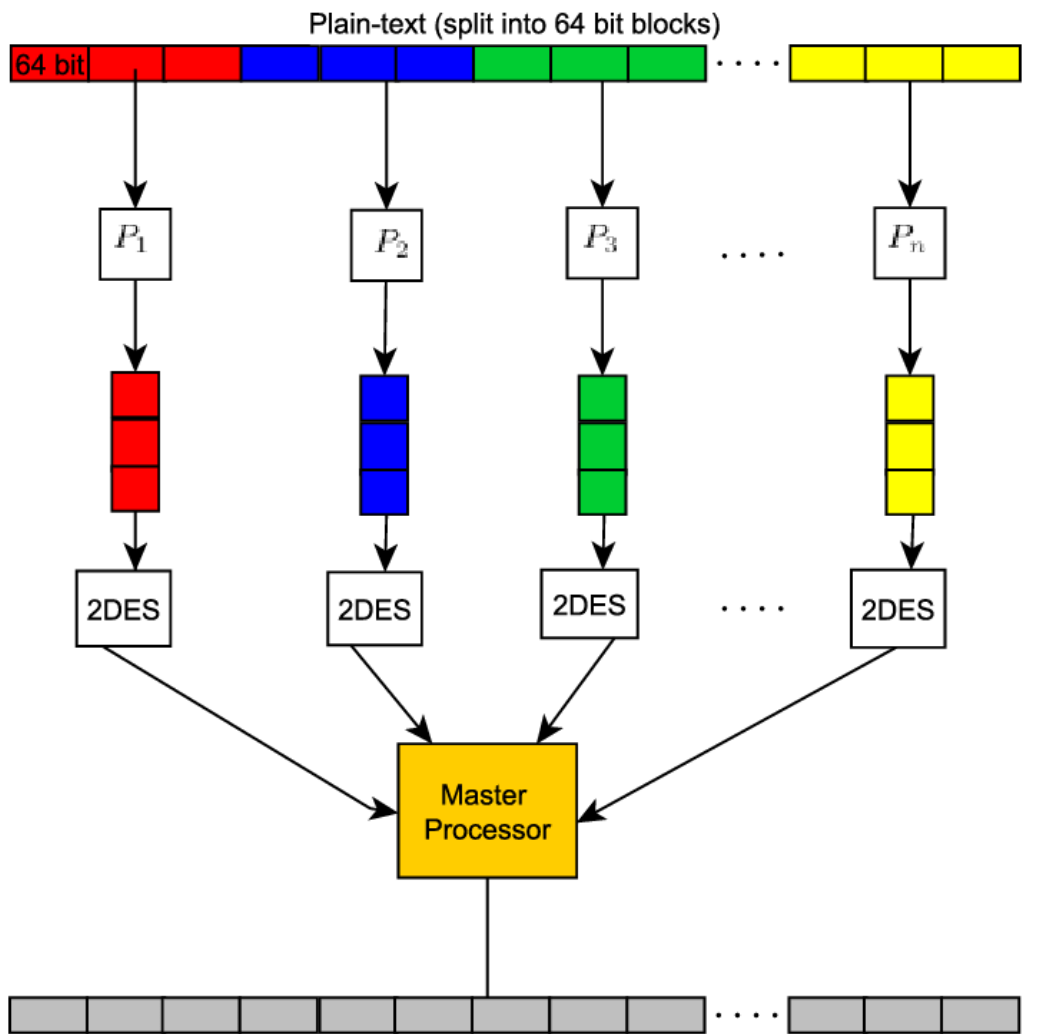
การเข้ารหัสโดยใช้ DES 2 ครั้ง ขั้นแรกข้อความต้นฉบับ P ไปเข้ารหัสลับด้วยขั้นตอนวิธี DES โดยใช้กุญแจดอกแรก k_1 ผลลัพธ์ที่ได้คือข้อความไซเฟอร์แรก คือ X จากนั้น เข้ารหัสลับข้อความไซเฟอร์ X โดยใช้ขั้นตอนวิธี DES อีกครั้งด้วยกุญแจดอกที่สอง k_2 จะได้ข้อความไซเฟอร์ C ดังนิยามทางคณิตศาสตร์ได้ว่า

$$C = E_{k_2} [E_{k_1} [P]]$$

ส่วนการถอดรหัสลับนั้น ให้ทำแบบย้อนกลับได้โดยนำข้อความไซเฟอร์ C มาถอดรหัสโดยใช้กุญแจ k_2 ก่อน เพื่อให้ได้ข้อความไซเฟอร์ X ออกมา จากนั้น ทำการถอดรหัสข้อความไซเฟอร์ X โดยใช้กุญแจ k_1 จะได้ข้อความต้นฉบับ P กลับมาเหมือนเดิม ซึ่งสามารถแสดงนิยามการถอดรหัส DES 2 ครั้งได้ดังนี้

$$P = D_{k_1} [D_{k_2} [C]]$$

ขั้นตอนการเข้ารหัสและถอดรหัสลับ DES 2 ครั้ง ดังแสดงในรูป 8.3 ความปลอดภัยของการเข้ารหัสลับแบบ DES 2 ครั้งนั้น เนื่องจากใช้กุญแจขนาด $56 \times 2 = 112$ บิต ดังนั้น จำนวนค่าที่เป็นไปได้ทั้งหมดของกุญแจแบบ DES 2 ครั้งนั้นมีขนาดเพิ่มขึ้นเป็นหนึ่งเท่าของ DES จึงทำให้ทนทานต่อการโจมตีแบบค้นหาทุกค่าที่เป็นไปได้ได้ดีกว่า



รูป 7.4 การเข้ารหัสลับของ 2DES (researchgate.net)

อย่างไรก็ตาม ต่อมา เมอร์เคิลและเฮลล์แมน (Merkle and Hellman) ได้เสนอการโจมตีที่เรียกว่า “พบกันครึ่งทาง” (meet-in-the-middle attack) ซึ่งมีหลักการคือ เข้ารหัสด้านหนึ่ง และถอดรหัสอีกด้านหนึ่ง จากนั้น นำผลลัพธ์ที่ได้จากการกระทำทั้งสองด้านมาเปรียบเทียบค่ากัน ซึ่งพบว่าสามารถโจมตี DES 2 ครั้งได้ การค้นหาค่ากุญแจทั้งหมดของการเข้ารหัส DES 2 ครั้ง โดยการโจมตีแบบพบกันครึ่งทางนั้น สามารถค้นหาคุญแจทั้งสิ้นเพียง $2 \times 2^{56} = 2^{57}$ ค่าเท่านั้น แทนที่จะเป็น 2^{112} ค่า แม้ว่า การโจมตีแบบนี้โดยอาศัยเทคโนโลยีในปัจจุบันยังมีความเป็นไปได้ยากเพราะต้องสร้างตารางที่ใช้ในการเก็บผลลัพธ์และค่ากุญแจขนาดใหญ่มหาศาล

7.4.3 การเข้ารหัสแบบ DES 3 ครั้ง (Triple-DES หรือ 3DES)

ความไม่ปลอดภัยของการเข้ารหัสแบบ DES นั้นเกิดจากกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสมีขนาดสั้นเกินไป แต่กระบวนการทำงานถือว่ามีความมั่นคง ดังนั้น จึงได้มีการปรับปรุงเพื่อแก้จุดอ่อนของ DES ในเวลาต่อมา โดยการเพิ่มขนาดกุญแจให้มีความยาวเพิ่มมากขึ้นด้วยการเข้ารหัสจำนวน 3 ครั้ง ส่วนขั้นตอนการเข้ารหัสจะเหมือนกับ DES ความยาวของกุญแจที่ใช้มี 2 ขนาดคือ แบบ 112 บิต เป็นการเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 2 ค่า และแบบ 168 บิต เป็นการเข้ารหัส DES 3 ครั้งด้วยกุญแจ 3 ค่า

7.4.4 การเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่า

การเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่าจะมีขั้นตอนคล้ายคลึงกับการเข้ารหัสโดยใช้ DES 2 ครั้ง โดยการนำข้อความต้นฉบับ P ผ่านเข้าสู่ขั้นตอนวิธีเข้ารหัส DES 3 ครั้ง แต่แต่ละครั้งใช้ค่ากุญแจที่แตกต่างกันคือ k_1 , k_2 และ k_3 กุญแจแต่ละตัว (k_1 , k_2 , k_3) มีขนาด 56 บิตรวมเป็น 168 บิต

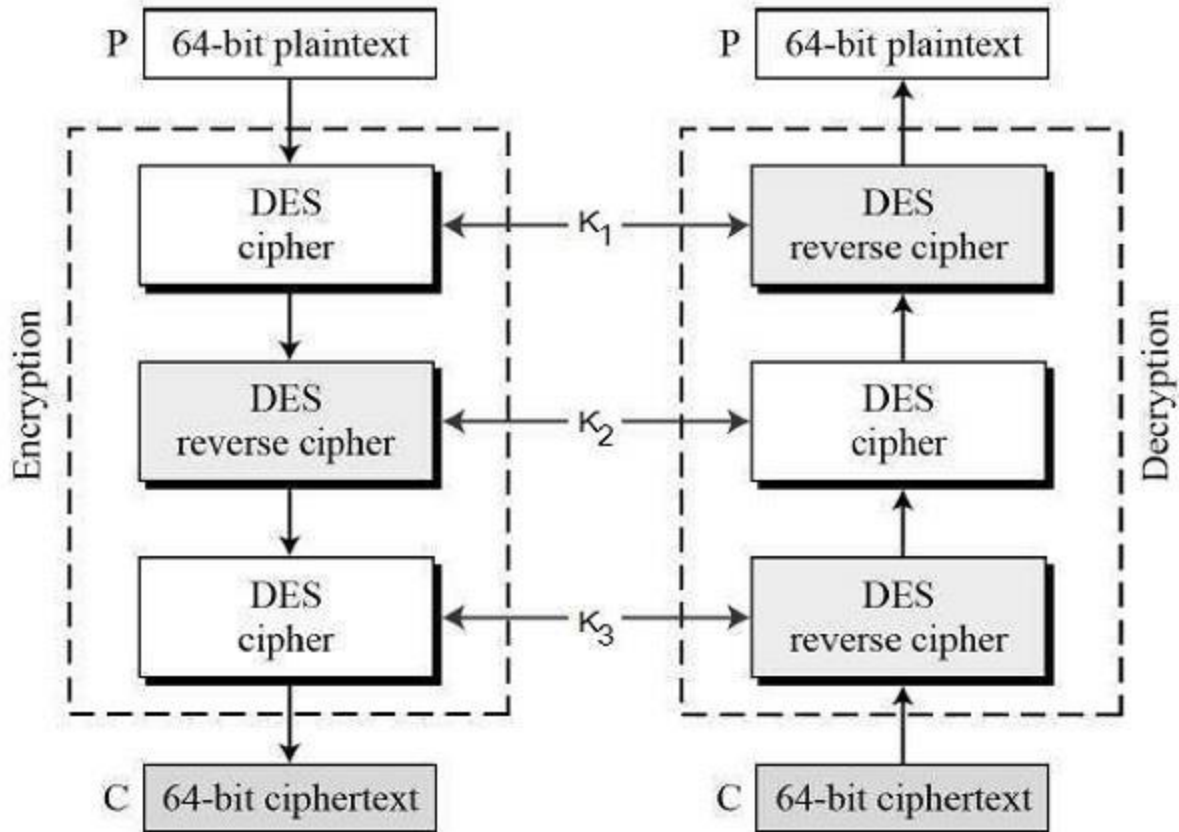
เราสามารถแสดงนิยามการเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่า ได้ว่า

$$C = E_{k_3} [E_{k_2} [E_{k_1} [P]]]$$

ส่วนการถอดรหัสก็กระทำแบบย้อนกลับ โดยถอดรหัสด้วยค่ากุญแจ k_3 , k_2 และ k_1 ตามลำดับ

เราสามารถแสดงนิยามการถอดรหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่าได้ดังนี้

$$P = D_{k_1} [D_{k_2} [D_{k_3} [C]]]$$



รูป 7.5 3-KEY Triple DES

(https://www.tutorialspoint.com/cryptography/triple_des.htm)

7.4.5 การเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 2 ค่า

แม้ว่าการเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่า จัดเป็นวิธีที่ปลอดภัยมากที่สุดในปัจจุบัน เนื่องจากกุญแจขนาด 168 บิตทำให้การโจมตีแบบค้นหาค่าที่เป็นไปได้ทั้งหมดของกุญแจแบบนี้ยังไม่สามารถทำได้ด้วยเทคโนโลยีในปัจจุบัน อย่างไรก็ตาม ขนาดกุญแจ 168 บิตนั้นมีจุดอ่อนในเรื่องเวลาที่ใช้ในกระบวนการเข้ารหัสและถอดรหัสซึ่งนานมาก จึงมีผู้พัฒนารูปแบบการเข้ารหัสโดยใช้ DES 3 ครั้งแต่ใช้กุญแจเพียง 2 ค่าแทน ทำให้ขนาดของกุญแจ $56 \times 2 = 112$ บิต เท่ากับการใช้ DES 2 ครั้งแต่มีความปลอดภัยสูงกว่า

เราสามารถนิยามการเข้ารหัส DES 3 ครั้งด้วยกุญแจ 2 ค่าได้ดังนี้

$$C = E_{k1} [D_{k2} [E_{k1} [P]]]$$

ส่วนการถอดรหัส DES 3 ครั้งด้วยกุญแจ 2 ค่าสามารถนิยามได้ดังนี้

$$P = D_{k1} [E_{k2} [D_{k1} [C]]]$$

ส่วนการถอดรหัส DES 3 ครั้งด้วยกุญแจ 2 ค่าแบบนี้เรียกว่า การทำงานแบบการเข้ารหัส-ถอดรหัส-เข้ารหัส (encrypt-decrypt-encrypt) หรือเรียกสั้นๆ ว่า EDE ส่วนการเข้ารหัสโดยใช้ DES 3 ครั้งด้วยกุญแจ 3 ค่าเรียกว่า การทำงานแบบเข้ารหัส-เข้ารหัส-เข้ารหัส (encrypt-encrypt-encrypt) หรือ EEE การทำงานแบบ EDE มีจุดประสงค์เพื่อให้สามารถนำไปใช้กับ DES แบบดั้งเดิมที่ใช้กุญแจค่าเดียวได้ เพราะถ้ากำหนดให้กุญแจ $k1 = k2$ เราสามารถนิยามได้ดังนี้

$$C = E_{k1} [D_{k1} [E_{k1} [P]]] = E_{k1} [P]$$

ดังนั้น $C = E_{k1} [P]$ ก็คือการเข้ารหัสแบบปกตินั่นเอง การทำงานแบบ EDE จึงมีจุดประสงค์เพื่อสามารถนำไปใช้กับ DES เดิมที่มีอยู่แล้ว การเข้ารหัส DES 3 ครั้งด้วยกุญแจ 2 ค่า จึงเป็นระบบการเข้ารหัสลับแบบกุญแจสมมาตรที่ได้รับความนิยมแพร่หลายในปัจจุบัน

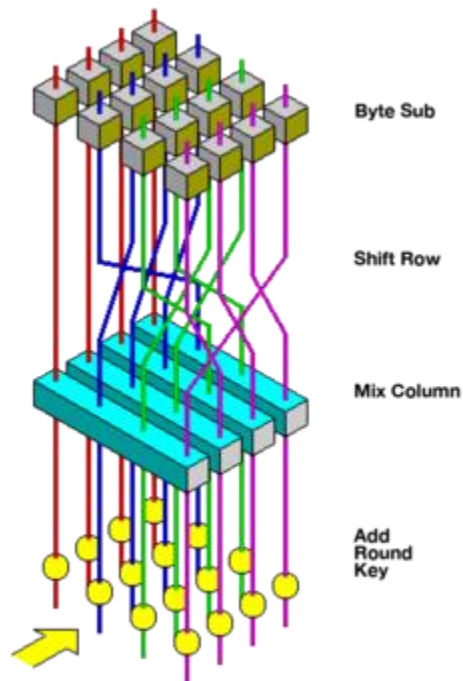
7.4.6 การเข้ารหัสแบบ AES (Rijndael)

ในปี พ.ศ. 2544 สถาบันมาตรฐานและเทคโนโลยีแห่งชาติได้พัฒนามาตรฐานการเข้ารหัสลับแบบใหม่ขึ้น เรียกว่า Advance Encryption Standard (AES) [82] การเข้ารหัสแบบ AES นี้เป็นกระบวนการเข้ารหัสบนหลักการของ DES แต่ใช้กุญแจ 3 แบบ ได้แก่ 128 บิต, 192 บิต และ 256 บิต ซึ่งเรียกขั้นตอนวิธีเหล่านี้ว่า AES-128, AES-192 และ AES-256 ตามลำดับ มาตรฐานใหม่นี้มีขีดความสามารถในประกันความมั่นคงด้านความปลอดภัยแก่ข้อมูลอย่างดี มีประสิทธิภาพและสอดคล้องกับสมรรถนะของคอมพิวเตอร์ที่นิยมใช้กันในปัจจุบัน

AES พัฒนาโดยชาวเบลเยียม 2 คน คือ Vincent Rijmen และ Joan Daemen ปรากฏสู่สาธารณชนเมื่อปี 1998 ขนาด Block 128 bit ขนาด Key 128, 192, 256 bit จำนวนรอบเข้ารหัส 10, 12, 14 รอบ ขึ้นอยู่กับขนาด Key โครงสร้าง Substitution-Permutation Network

กระบวนการเข้ารหัสแบบ AES มีโครงสร้างการทำงานคล้ายคลึงกับมาตรฐาน DES มีการแบ่งกระบวนการทำงานออกเป็น 2 ด้าน ได้แก่ ด้านข้อความต้นฉบับที่จะเข้ารหัส และด้านกุญแจที่ใช้ในการเข้ารหัส ใน

ขั้นตอนการเข้ารหัสจะแบ่งข้อความต้นฉบับออกเป็นบล็อกๆ ละ 128 บิต เพื่อนำไปสู่กระบวนการเข้ารหัสที่มีการทำงานเป็นรอบๆ เหมือนกับ DES จำนวนรอบจะขึ้นอยู่กับขนาดของกุญแจที่ใช้ในการเข้ารหัส ตามมาตรฐานได้กำหนดจำนวนรอบในการเข้ารหัสเป็น 10, 12 และ 14 รอบ สำหรับกุญแจขนาด 128 บิต, ขนาด 192 บิต และขนาด 256 บิต ตามลำดับ รูป 7.6 มาตรฐานการเข้ารหัสขั้นสูง (AES Rijndael)



รูป 7.6 มาตรฐานการเข้ารหัสขั้นสูง AES (Rijndael)

([https://en.wikipedia.org/wiki/File:AES_\(Rijndael\)_Round_Function.png](https://en.wikipedia.org/wiki/File:AES_(Rijndael)_Round_Function.png))

ในวงการ Cryptography นั้น Advanced Encryption Standard (AES) จะรู้จักกันในอีกชื่อหนึ่งว่า Rijndael ซึ่งเป็น Algorithm การเข้ารหัสข้อมูลที่ได้รับเลือกให้เป็นมาตรฐานโดยรัฐบาลสหรัฐ จึงถูกคาดหวังว่าจะถูกนำมาใช้กันอย่างแพร่หลายทั่วโลก และการทดสอบก็จะเป็นไปอย่างเข้มข้นด้วยเช่นกัน เหมือนเช่นมาตรฐานรุ่นก่อน คือ Data Encryption Standard (DES) ซึ่ง AES โดย National Institute of Standards and Technology (NIST) ได้นำมาเป็น US FIPS PUB 197 ในเดือนพฤศจิกายน 2001 หลังจาก 5 ปีของการกำหนดมาตรฐาน

Rijndael คือผู้ชนะในการแข่งขัน AES คำว่า Rijndael มาจากการผสมชื่อผู้พัฒนาทั้ง 2 คน ในการแข่งขัน AES ซึ่งมีคู่แข่งทั้งหมด 15 ราย คือ CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, Twofish รอบสุดท้ายคัดเหลือ 5 ราย คือ MARS, RC6,

Rijndael, Serpent, Twofish ซึ่ง Rijndael คือผู้ชนะในที่สุด และได้รับเลือกให้เป็น AES ซึ่งเป็นมาตรฐานใหม่เพื่อมาแทนที่ DES

คะแนนโหวต Rijndael ได้ 86 Serpent ได้ 59 Twofish ได้ 31 RC6 ได้ 23 และ MARS ได้ 13

การเข้ารหัสของ Rijndael ในแต่ละรอบนั้น จะใช้เทคนิค 4 ขั้นตอน คือ AddRoundKey, SubBytes, ShiftRows และ MixColumns โดยในรอบสุดท้ายจะใช้ AddRoundKey แทน MixColumns

ในปี 2006 การโจมตี AES ที่ได้ผลเพียงอย่างเดียว คือ Side Channel Attack ดังนั้น National Security Agency (NSA) ได้ตรวจสอบ Algorithm ที่เข้ารอบสุดท้ายทั้งหมด รวมทั้ง Rijndael ได้กล่าวว่า ทุก Algorithm มีความปลอดภัยเพียงพอสำหรับ Non-Classified Data ของรัฐบาลสหรัฐ ในเดือนมิถุนายน 2003 รัฐบาลสหรัฐประกาศว่า อาจจะนำ AES มาใช้เข้ารหัส Classified Information

"การออกแบบและความแข็งแกร่งของทุกๆ ขนาด Key (128, 192, 256 bit) เพียงพอต่อการป้องกัน Classified Information จนถึงระดับ SECRET level ส่วน TOP SECRET Information จะใช้ Key ที่ขนาด 192, 256 bit การนำ AES มาใช้ในผลิตภัณฑ์จะมุ่งเน้นเพื่อการปกป้อง National Security System และ/หรือ Information จะต้องถูกตรวจสอบและรับรองโดย NSA ก่อนที่จะนำไปใช้"

นี่เป็นครั้งแรกที่ Algorithm ที่ใช้กันโดยทั่วไปได้รับการอนุมัติโดย NSA สำหรับข้อมูลระดับ TOP SECRET Information จุดที่น่าสนใจที่ต้องกล่าวไว้คือ ในหลายผลิตภัณฑ์ในตลาดจะใช้ Key ขนาด 128 bit มันเป็นไปได้ที่ NSA จะสงสัยในจุดอ่อนของการที่ Key มีขนาดเล็ก หรือเขาอาจจะต้องการความปลอดภัยที่มากกว่าสำหรับ Top Secret Document (ซึ่งต้องการความปลอดภัยนานนับทศวรรษ)

การโจมตีที่นิยมที่สุดคือการลองใช้หลายๆ วิธี ในการโจมตีเพื่อลดจำนวนรอบลง AES มี 10 รอบ ใน Key ขนาด 128 bit 12 รอบ ใน Key ขนาด 192 bit และ 14 รอบ ใน Key ขนาด 256 bit ในปี 2006 การโจมตีที่ดีที่สุดในรอบที่ 7 ของ Key ขนาด 128 bit รอบที่ 8 ของ Key ขนาด 192 bit และ รอบที่ 9 ของ Key ขนาด 256 bit

Cryptographer บางคนกังวลต่อความปลอดภัยของ AES เขารู้สึกว่าช่องว่างระหว่างจำนวนรอบที่ถูกโจมตีมันน้อยเกินไปจนจะสบายใจได้ ความเสี่ยงมันอยู่ตรงที่ บางครั้งหนทางที่จะเพิ่มประสิทธิภาพการโจมตีอาจถูกค้นพบ และถ้าเป็นเช่นนั้น ข้อมูลก็จะถูกเจาะ ในทาง Cryptographic คำว่า "Break" คืออะไรก็ตามที่เร็วกว่า Exhaustive Search ฉะนั้น การโจมตี AES 128 bit ซึ่งต้องการแค่ 2120 Operation จึงถูกพิจารณาว่าเป็นการ Break แม้จะเป็นเพียงแค่มโนทัศน์ก็ตาม ในตอนนี้ มันยังคงเป็นไปได้ในทางปฏิบัติ การ Break AES ที่ได้เพียงขั้น "ดี" นั้นอาจจะไม่ใช่ประเด็น สำหรับตอนนี้ ในเรื่องนี้ควรจะเลิกกังวลได้ การโจมตีแบบ Brute-Force ที่

รู้จักกันดีที่สุดคือการโจมตีต่อ RC5 ใน Key ขนาด 64 bit โดย distributed.net (สำเร็จในปี 2002 : กฎของมัวร์ บอกเป็นนัยว่า มันยากลำบากมากที่จะทำในแบบเดียวกันบน Key ขนาด 66 bit ในตอนนี้)

เรื่องอื่นที่น่ากังวลคือ โครงสร้างทางคณิตศาสตร์ของ AES ซึ่งไม่เหมือน Algorithm อื่นๆ ส่วนใหญ่ AES มีรายละเอียดทางคณิตศาสตร์ที่เรียบง่ายมาก แม้จะยังไม่ถูกโจมตี แต่นักวิจัยบางคนก็เป็นกังวลต่อการโจมตีในอนาคต ซึ่งจะใช้ประโยชน์จากโครงสร้างดังกล่าว

ในปี 2002 การโจมตีในทางทฤษฎี เรียกว่า "XSL Attack" ได้ถูกประกาศให้รับทราบกัน โดย Nicolas Courtois และ Josef Pieprzyk แสดงให้เห็นถึงจุดที่อ่อนที่สุดใน Algorithm ของ AES ผู้เชี่ยวชาญด้าน Cryptography หลายคนได้พบปัญหาภายใต้คณิตศาสตร์ของการโจมตี โดยได้เสนอแนะว่า อาจจะเป็นการทำผิดพลาดในการประมาณการของคนทั้งสอง แม้ว่าจะสามารถโจมตีต่อ AES จนเกิดคำถามขึ้นมาได้ แต่ถึงตอนนี้ XSL Attack ต่อ AES นั้น ก็ยังไม่สามารถทะลุผ่านความแข็งแกร่งของ AES ได้

Side Channel Attacks ไม่ได้โจมตี Cipher แต่โจมตีการ Implementations ของ Cipher บนระบบที่ข้อมูลรั่วไหลโดยไม่ได้ตั้งใจ

เมษายน 2005 D.J. Bernstein ได้ประกาศถึงการโจมตีแบบ Cache Timing Attack ซึ่งเขาได้ใช้ Break เครื่อง Server ที่ใช้ OpenSSL ที่ใช้การเข้ารหัสด้วย AES เครื่อง Server ถูกออกแบบให้หยุดการทำงานตามปริมาณความถี่ของข้อมูลเท่าที่จะเป็นไปได้ และการโจมตีต้องการ Chosen Plaintexts มากกว่า 200 ล้าน บางคนกล่าวว่า การโจมตีนำไปใช้ในทางปฏิบัติจริงไม่ได้ บน Internet Bruce Schneier เรียกการวิจัยนี้ว่า "Nice Timing Attack"

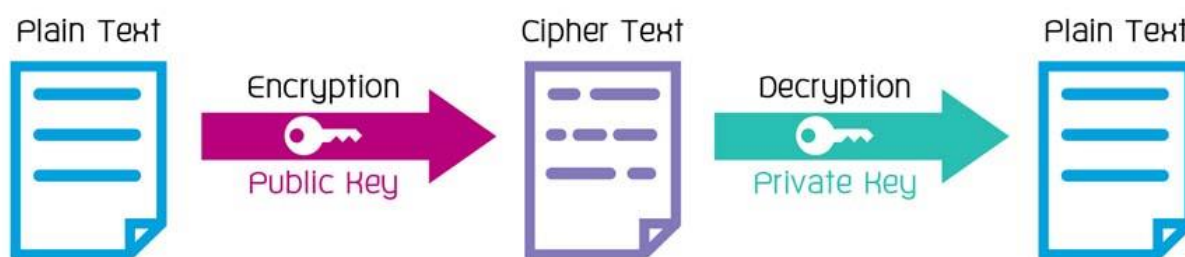
ตุลาคม 2005 Adi Shamir และนักวิจัยอีก 2 คน ได้เสนอรายงานที่แสดงให้เห็นถึงการโจมตีแบบ Cache Timing Attacks ในหลายๆ แบบ ในการโจมตี AES ในการโจมตีครั้งหนึ่งสามารถเจาะ Key ทั้งหมดได้หลังจาก 800 Writes ในเวลาเพียง 65 Milliseconds เท่านั้น แต่การโจมตีนี้ ผู้โจมตีต้องสามารถ Run โปรแกรมบนระบบเดียวกันกับระบบที่เข้ารหัส AES

หมายเหตุ : Rijndael ได้รับเลือกให้เป็น AES ไม่ใช่เพราะว่ามันเป็น Algorithm ที่แข็งแกร่งปลอดภัยที่สุด แต่เป็นเพราะมันเป็น Algorithm ที่โดยรวมแล้วดีที่สุด นั่นหมายถึง ความเร็ว เป็นปัจจัยหนึ่งที่ทำให้ Rijndael ได้รับเลือก อย่างไรก็ตาม Rijndael มีความเร็วสู้กับ Twofish ในแทบทุก Platform และใน Key ขนาด 192, 256 bit แล้ว Rijndael จะทำงานช้ากว่า Twofish อย่างเห็นได้ชัด (Rijndael จะช้าลง 20% ใน Key ขนาด 192 bit 40% ใน Key ขนาด 256 bit) ส่วนในด้านความปลอดภัยนั้น MARS, Serpent, Twofish ถูกจัดว่ามีความปลอดภัยสูงกว่า Rijndael

7.5 การเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric key encryption scheme)

ปัญหาหลักของการเข้ารหัสลับแบบกุญแจอสมมาตรก็คือ ปัญหาเรื่องการจัดการกุญแจ (Key management) ได้แก่การสร้างกุญแจ (Generation of keys), การเก็บรักษากุญแจ (Storage of keys) และการส่งผ่านกุญแจ (Transmission of keys) ทั้งฝ่ายผู้ส่งและผู้รับจำเป็นต้องตกลงกันก่อนว่าจะใช้กุญแจใดในการเข้ารหัส เนื่องจากกุญแจที่ทั้งคู่ใช้นั้นเรียกว่า กุญแจร่วม (Key shared) ที่ใช้สำหรับการเข้ารหัสและถอดรหัสข้อมูล ทั้งสองฝ่ายจะต้องหาช่องทางที่ปลอดภัยในการส่งมอบกุญแจลับ ซึ่งอาจไม่สะดวกและปลอดภัยพอเมื่อทั้งสองอยู่ในสถานที่ห่างไกลกัน ปัญหาการเก็บรักษากุญแจทั้งหมดให้เป็นความลับตลอดเวลาถือเป็นความยุ่งยากในระบบการเข้ารหัสลับแบบกุญแจอสมมาตร

ในปี พ.ศ. 2519 ดิฟฟี และ เฮลล์แมน (Whitfield Diffie and Martin Hellman) ได้เสนอวิทยาการรหัสลับชนิดใหม่ที่ใช้กุญแจที่แตกต่างกันระหว่างการเข้ารหัสและถอดรหัสลับ ที่รู้จักกันในชื่อว่า กุญแจสาธารณะและกุญแจส่วนตัวของเจ้าของนั่นเอง [83] ซึ่งแนวคิดนี้สามารถนำมาใช้แก้ปัญหาเรื่องการจัดการกุญแจได้เป็นอย่างดีและยังคงใช้กันอยู่ในปัจจุบัน เทคนิคนี้อาศัยหลักการของการใช้กุญแจคนละดอกสำหรับการเข้ารหัสและถอดรหัสข้อมูล กุญแจดอกแรกที่มีชื่อว่า กุญแจสาธารณะ (Public key) สำหรับใช้ในการเข้ารหัสลับข้อความ และกุญแจดอกที่สองซึ่งเรียกว่า กุญแจส่วนตัว (Private key) มีไว้สำหรับใช้ในกระบวนการถอดรหัสลับข้อความที่ถูกเข้ารหัสไว้ เรียกเทคนิคดังกล่าวนี้ว่า การเข้ารหัสลับแบบอสมมาตร หรือบางทีเรียกว่า การเข้ารหัสลับแบบกุญแจ 2 ดอก (Two keys encryption scheme) หรือ การเข้ารหัสลับแบบกุญแจสาธารณะ (Public key encryption)



รูป 7.7 การทำงานของระบบการเข้ารหัสลับแบบกุญแจอสมมาตร

(ที่มา: etda.or.th)

การเข้ารหัสลับแบบอสมมาตรจะใช้กุญแจ 2 ดอก เรียกว่า กุญแจสาธารณะ/กุญแจส่วนตัว (Public/private key) โดยใช้กุญแจดอกหนึ่งสำหรับการเข้ารหัสและใช้กุญแจอีกดอกหนึ่งสำหรับการถอดรหัส โดยที่กุญแจทั้งคู่จะมีความสัมพันธ์กันในทางคณิตศาสตร์ กุญแจสาธารณะนั้นประกาศให้เป็นที่รับรู้กันทั่วไป ในขณะที่กุญแจส่วนตัว จะมีเอกลักษณ์ รู้และใช้ได้เฉพาะเจ้าของกุญแจเท่านั้น เมื่อผู้ส่งจะทำการส่งข้อมูลจะใช้กุญแจส่วนตัว

ของผู้ส่งในการเข้ารหัสข้อมูลแล้วส่งข้อมูลที่ผ่านการเข้ารหัสไปยังผู้รับ จากนั้น ผู้รับจะสามารถเปิดข้อมูลเหล่านั้นได้โดยอาศัยกุญแจสาธารณะของผู้ส่งในการถอดรหัสข้อมูล ดังแสดงในรูป 7.7

ระบบรหัสแบบอสมมาตรเป็นระบบรหัสที่ใช้กุญแจคู่ (Key Pair) ซึ่งประกอบด้วยกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) กล่าวคือ ผู้ใช้ 1 คนหรือที่เรียกว่าเจ้าของกุญแจจะใช้กุญแจคู่นี้ในการติดต่อสื่อสารกับบุคคลอื่นโดยไม่จำเป็นต้องมีกุญแจเป็นจำนวนมากเช่นเดียวกับกรณีของระบบรหัสแบบสมมาตร ทั้งนี้ในการเก็บรักษากุญแจนั้น กุญแจส่วนตัวจะต้องเก็บรักษาไว้กับเจ้าของกุญแจและห้ามไม่ให้ผู้อื่นล่วงรู้ ส่วนกุญแจสาธารณะนั้นต้องมีการประกาศให้ผู้อื่นรับรู้หรือเก็บไว้ในที่ซึ่งบุคคลอื่นสามารถเข้ามาสืบค้นได้

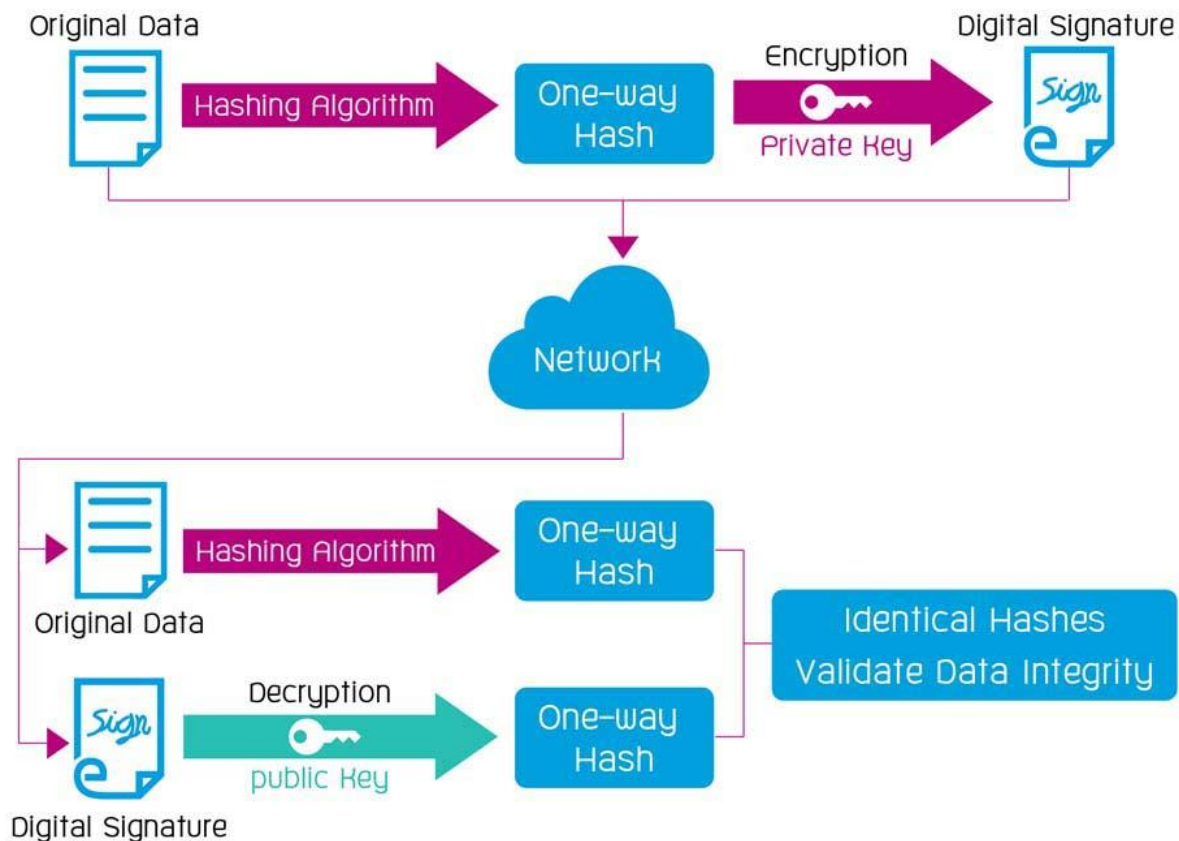
ในการเข้ารหัสลับข้อมูลจะต้องใช้กุญแจดอกหนึ่งในการเข้ารหัสลับและใช้กุญแจอีกดอกหนึ่งที่เป็นคู่กันในการถอดรหัสลับ เช่น หากใช้กุญแจสาธารณะในการเข้ารหัสลับก็จะต้องใช้กุญแจส่วนตัวในการถอดรหัสลับในทางกลับกัน หากใช้กุญแจส่วนตัวในการเข้ารหัสลับก็จะต้องใช้กุญแจสาธารณะในการถอดรหัสลับ ซึ่งวิธีการเลือกใช้กุญแจจะขึ้นอยู่กับวัตถุประสงค์ของการใช้งาน เช่น นำไปใช้ในการเข้ารหัสลับ (Encryption) เพื่อรักษาความลับของข้อมูลหรือใช้งานในลักษณะลายมือชื่อดิจิทัล (Digital Signature) ดังรูป 7.8

เนื้อหาต่อไปนี้จะสรุปสาระสำคัญของการขั้นตอนวิธีเข้ารหัสลับแบบอสมมาตรเฉพาะเทคนิคที่ได้รับ ความนิยม โดยเริ่มจากแนวคิดของขั้นตอนวิธีแบบ Diffie-Hellman นอกจากนั้น จะกล่าวถึงการใช้โปรโตคอล Oakley เพื่อแก้ปัญหาข้อจำกัดของ Diffie-Hellman, ขั้นตอนวิธี RSA และลายมือชื่อดิจิทัล

7.4.7.1 Diffie-Hellman

ปัญหาสำคัญประการหนึ่งในวิทยาการรหัสลับก็คือ การกระจายกุญแจ เพราะไม่ว่าขั้นตอนวิธีในการเข้าและถอดรหัสรวมทั้งกุญแจที่ใช้จะมีความมั่นคงเพียงใดก็ตาม แต่ในการแจกจ่ายกุญแจไปยังผู้รับที่เกี่ยวข้อง อาจมีช่องโหว่ที่ทำให้ผู้บุกรุกสามารถเข้าถึงกุญแจที่ใช้ ระบบการเข้ารหัสก็ปราศจากประโยชน์ โดยเฉพาะการโจมตีที่เรียกว่า “บุคคลที่อยู่ระหว่างกลาง (man-in-the-middle attack)” ซึ่งอยู่ระหว่างทางที่ข้อมูลถูกส่งผ่านไปยังผู้รับปลายทาง ซึ่งอาจใช้เครื่องมืออย่างเช่นสแนฟเฟอร์ในการดักอ่านข้อมูลได้

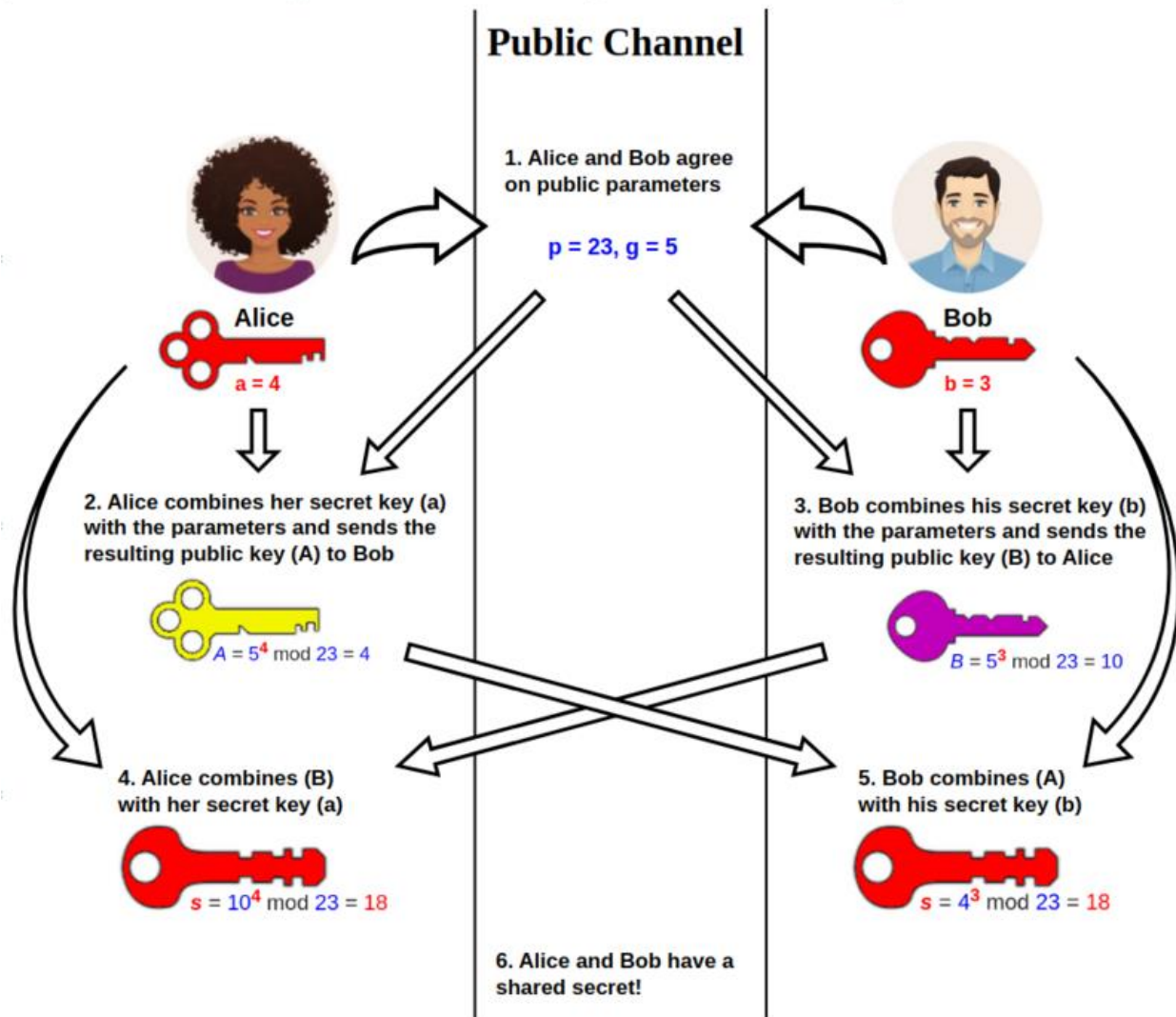
วิธีหนึ่งที่ใช้เพื่อความปลอดภัยในการแจกจ่ายกุญแจก็คือ การใช้ขั้นตอนวิธีของ Diffie-Hellman ขั้นตอนวิธีนี้มีการใช้พารามิเตอร์ 2 ตัว ได้แก่ p และ g โดยค่าทั้งสองสามารถเปิดเผยต่อสาธารณะได้ และผู้ใช้ทุกคนในระบบสามารถนำมาใช้ได้ พารามิเตอร์ p เป็นจำนวนเฉพาะขนาดใหญ่ค่าหนึ่ง ส่วนพารามิเตอร์ g เป็นเลขจำนวนเต็มที่มีค่าน้อยกว่า p และสามารถให้กำเนิดเลขทุกตัวตั้งแต่ 0 ถึง $p-1$ เมื่อนำไปคูณกับตัวเองซ้ำๆ กัน ภายใต้ทอดูล p เรียกตัวเลขนี้ว่า ตัวกำเนิด (Generator) ในทางคณิตศาสตร์ g เป็นรากพริมีทีฟ (primitive root) ของ p



รูป 7.8 การใช้งานลายเซ็นดิจิทัล (Digital Signature) ด้วยระบบรหัสแบบอสมมาตร

(ที่มา: etad.or.th)

ขั้นตอนวิธีของ Diffie-Hellman มีหลักการทำงานดังแสดงในรูป 7.9 ซึ่งแสดงการสื่อสารระหว่างอลิสกับบ๊อบ แสดงขั้นตอนการเข้ารหัสและถอดรหัสโดยใช้เทคนิคของ Diffie-Hellman ขั้นตอนแรก บ๊อบและอลิสจะต้องแลกเปลี่ยนกุญแจสาธารณะของกันและกันก่อน จากนั้น เมื่อทั้งคู่ได้รับกุญแจสาธารณะของอีกฝ่ายหนึ่งแล้วก็สามารถคำนวณกุญแจลับโดยใช้กุญแจส่วนตัวของตนเองกับกุญแจสาธารณะของอีกฝ่ายหนึ่ง ผลที่ได้คือทั้งคู่จะได้กุญแจลับดอกเดียวกันเพื่อใช้สำหรับการเข้ารหัสและถอดรหัสข้อมูลที่รับส่งระหว่างกันได้ เนื่องจากผลลัพธ์ของการเข้ารหัสโดยใช้กุญแจส่วนตัวของอลิสกับกุญแจสาธารณะของบ๊อบจะต้องเท่ากับผลลัพธ์ที่ได้จากการคำนวณโดยใช้กุญแจสาธารณะของอลิสร่วมกับกุญแจส่วนตัวของบ๊อบ ดังนั้น ทั้งคู่จึงสามารถสร้างกุญแจลับที่ใช้ในการเข้ารหัสและถอดรหัสระหว่างกันได้โดยไม่ต้องกังวลถึงการแลกเปลี่ยนกุญแจ เฉพาะทั้งคู่เท่านั้นที่รู้จักกุญแจลับของกันและกันสำหรับเข้ารหัสและถอดรหัส



รูป 7.9 การแลกเปลี่ยนข้อมูลที่เข้ารหัสลับโดยใช้ขั้นตอนวิธีของ Diffie-Hellman

(By Epachamo - Own work, CC BY-SA 4.0,

<https://commons.wikimedia.org/w/index.php?curid=142206661>)

สมมติว่า บ๊อบกับอลิสต้องการตกลงกุญแจลับเพื่อการสื่อสารระหว่างกันโดยอาศัยขั้นตอนวิธีของดิฟฟี-เฮลล์แมน สามารถทำได้ดังนี้ ขั้นแรก อลิสสุ่มค่าตัวเลขจำนวนเต็ม A ขึ้นมาค่าหนึ่ง ซึ่งค่าดังกล่าวนี้อลิสจะเก็บไว้เองโดยไม่เปิดเผย ส่วนบ๊อบก็ทำการสุ่มค่าตัวเลขจำนวนเต็ม B ขึ้นมาค่าหนึ่งเช่นเดียวกันโดยเก็บไว้เป็นความลับ อลิสจะนำค่า A ไปผ่านกระบวนการคำนวณกับพารามิเตอร์ของระบบคือ ค่า p และ g เพื่อให้ได้ค่าที่เปิดเผยต่อสาธารณะโดยใช้สมการความสัมพันธ์ดังนี้ คือ

$$g^A \bmod p$$

ในทำนองเดียวกัน บ๊อบก็สามารถคำนวณค่าที่จะทำการเปิดเผยต่อสาธารณะโดยการนำค่า B ไปคำนวณดังนี้

$$g^B \bmod p$$

จากนั้น อลิสกับบ๊อบทำการแลกเปลี่ยนตัวเลขที่คำนวณได้ระหว่างกัน ดังนั้น อลิสจะนำค่าที่ได้ไปคำนวณต่อดังนี้

$$K_{AB} = (g^B)^A \bmod p$$

ส่วนบ๊อบจะคำนวณด้วยค่าดังนี้

$$K_{BA} = (g^A)^B \bmod p$$

ค่าที่ทั้งคู่คำนวณได้จะได้ผลลัพธ์ที่เป็นค่าเดียวกัน ดังนี้

$$K = K_{AB} = (g^B)^A \bmod p = g^{(AB)} \bmod p = (g^A)^B \bmod p = K_{BA}$$

ดังนั้น ทั้งอลิสและบ๊อบสามารถกำหนดให้ K เป็นกุญแจลับร่วมกันได้

อย่างไรก็ตาม ปัญหาอีกประการหนึ่งที่พบตามหลักการของขั้นตอนวิธีแบบ Diffie-Hellman ก็คือ ทั้งคู่จะแน่ใจได้อย่างไรทั้งคู่ได้รับกุญแจสาธารณะของอีกฝ่ายหนึ่งจริง เนื่องจากในขั้นตอนที่ทั้งคู่กำลังแลกเปลี่ยนกุญแจสาธารณะระหว่างกันผ่านช่องทางสื่อสารสาธารณะที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต อยู่ นั่นอาจมี

บุคคลที่สามเช่นชื่ออีฟแอบเปลี่ยนเป็นกุญแจสาธารณะของตัวเองส่งไปให้แทน ดังนั้น กุญแจที่อลิสกับบ๊อบได้จึงกลายเป็นของอีฟแทน ปัญหานี้เรียกว่าปัญหา “บุคคลที่อยู่ระหว่างกลาง” ดังที่กล่าวแล้วข้างต้น เมื่อเป็นเช่นนี้ ข้อมูลของทั้งอลิสและบ๊อบย่อมจะถูกมองเห็นและอ่านได้โดยอีฟเช่นเดียวกัน ปัญหานี้เรียกว่าปัญหาการแลกเปลี่ยนกุญแจ วิธีการแก้ปัญหานี้สามารถทำได้โดยใช้โปรโตคอล Oakley และการใช้ขั้นตอนวิธีแบบ RSA ร่วมกับลายมือชื่อดิจิทัล ซึ่งจะกล่าวในหัวข้อถัดไป

7.4.7.2 โปรโตคอล Oakley

เนื่องจากขั้นตอนวิธี Diffie-Hellman ยังมีข้อจำกัดที่สำคัญ ได้แก่

- 1) ไม่มีข้อมูลที่สามารถใช้ระบุตัวตนผู้ที่ติดต่อกันได้
- 2) ยังไม่สามารถแก้ปัญหาจากการโจมตีแบบที่เรียกว่า “บุคคลที่อยู่ระหว่างกลาง” ได้อันเนื่องจากระบบนี้ไม่มีกลไกที่ใช้ในการพิสูจน์ตัวจริง
- 3) ขั้นตอนการหากุญแจกลับใช้เวลาในการคำนวณทางคณิตศาสตร์มาก ทำให้ถูกใช้จุดอ่อนข้อนี้ในการโจมตีได้ โดยส่งกุญแจสาธารณะไปยังเครื่องของเหยื่อเพื่อขอติดต่อ ส่งผลให้เหยื่อต้องใช้เวลาในการคำนวณกุญแจกลับ ถ้าผู้โจมตีจงใจส่งข้อความในลักษณะดังกล่าวต่อเนื่องเป็นจำนวนมากย่อมส่งผลให้เครื่องของเหยื่อไม่สามารถใช้งานได้ การโจมตีด้วยวิธีนี้คล้ายกับการโจมตีที่เรียกว่าทำให้ใช้การไม่ได้ แต่เรียกการโจมตีชนิดนี้ว่า Congestion attack หรือ Clogging attack

โปรโตคอล Oakley เป็นโปรโตคอลการแลกเปลี่ยนกุญแจ (Key exchange protocol) ที่มีพื้นฐานการทำงานตามแบบขั้นตอนวิธี Diffie-Hellman แต่มีการปรับปรุงเพิ่มเติมกลไกเพื่อให้ระบบมีความปลอดภัยมากขึ้น โดยเพิ่มกลไกเพื่อแก้ปัญหาจุดอ่อนดังกล่าว และยังคงรักษาคุณสมบัติที่ดีของขั้นตอนวิธีแบบ Diffie-Hellman ไว้เหมือนเดิม กลไกที่เพิ่มเข้ามาประกอบด้วย

- 1) ใช้คุกกี้ (Cookies) เพื่อป้องกันการโจมตีแบบ Congestion
- 2) ป้องกันการส่งแพ็กเก็ตซ้ำได้โดยใช้ nonces
- 3) สามารถเปลี่ยนค่ากุญแจสาธารณะที่ใช้ในขั้นตอนวิธี Diffie-Hellman ได้
- 4) สามารถพิสูจน์ตัวจริงของเจ้าของเอกสารได้ เพื่อป้องกันผู้อื่นมาอ่านหรือแก้ไขข้อมูล

คุกกี้ เป็นเลขสุ่มที่แต่ละฝ่ายที่ติดต่อกันจะต้องใช้ในการแลกเปลี่ยนกันในช่วงเริ่มต้นติดต่อกัน เพื่อให้แต่ละฝ่ายต่างทราบคุกกี้ของอีกฝ่ายหนึ่ง และในขั้นตอนการแลกกุญแจ แต่ละฝ่ายก็ต้องส่งคุกกี้ของตนไป

พร้อมกับกุญแจสาธารณะ หากมีบุคคลที่สามทำการโจมตีแบบ Congestion โดยการปลอมเลขที่อยู่ของอีกฝ่ายหนึ่ง ผู้โจมตีจะไม่สามารถทราบค่าคีย์ของฝ่ายที่ตนปลอมตัวได้ จึงไม่สามารถทำการแลกกุญแจกับอีกฝ่ายหนึ่งได้ การคำนวณเพื่อหากุญแจรับก็ย่อมไม่เกิดขึ้น

7.4.7.3 RSA

เป็นวิธีการเข้ารหัสแบบสมมาตรวิธีหนึ่งที่ได้รับการยกย่องว่าเป็นขั้นตอนวิธีที่มั่นคงยากต่อการโจมตี RSA มาจากอักษรตัวแรกของชื่อผู้คิดค้นวิธีการนี้ ได้แก่ รีเวสต์ (Rivest), แชเมียร์ (Shamir) และแอดเลแมน (Adleman) แห่งมหาวิทยาลัยเอ็มไอที RSA ใช้วิธีการเข้ารหัสโดยอาศัยพื้นฐานของทฤษฎีตัวเลข สามารถใช้ได้ทั้งกับการเข้ารหัสข้อมูลและลายมือชื่อดิจิทัล ข้อความต้นฉบับที่จะเข้ารหัสจะอยู่ในรูปของบล็อกตัวเลขไบนารีที่มีค่าจำกัดไม่เกิน n กล่าวคือ มีความยาวไม่เกิน $\log_2(n)$ บิต ข้อมูลที่ถูกเข้ารหัสไว้ด้วยกุญแจส่วนตัวจะถูกถอดรหัสได้ด้วยกุญแจสาธารณะที่เป็นคู่กันเท่านั้น ถ้าผู้ส่งใช้กุญแจส่วนตัวในการเข้ารหัสข้อมูล ใครก็ตามที่มีกุญแจสาธารณะของผู้ส่งย่อมสามารถถอดรหัสข้อมูลนั้นได้ การเข้ารหัสแบบ RSA จึงสามารถใช้ได้ทั้งในการเข้ารหัสข้อมูลและในการแจกจ่ายกุญแจลับ

การเข้ารหัสแบบ RSA มีขั้นตอนของการเลือกกุญแจสาธารณะและกุญแจส่วนตัว สรุปได้ดังนี้

- 1) เลือกตัวเลขเฉพาะ (Prime number) สำหรับ p และ q ยิ่งเลขจำนวนมากยิ่งทำให้ยากต่อการถอดรหัส แต่จะทำให้การถอดรหัสใช้เวลานานขึ้น โดยปกติ เลขที่ใช้จะมีค่ามากกว่าหรือเท่ากับ 10^{100}
- 2) คำนวณหาค่า n โดยที่ $n = p \cdot q$ และ $z = (p-1)(q-1)$
- 3) เลือกจำนวนเฉพาะ e ซึ่งมีค่าน้อยกว่า n และ e ไม่มีตัวหารร่วมกับ z ยกเว้น 1 ผลที่ได้คือทั้ง e และ z จึงเป็นจำนวนเฉพาะซึ่งกันและกัน และ e จะถูกใช้เป็นกุญแจส่วนตัวในการถอดรหัส
- 4) คำนวณหาค่า d โดยเมื่อ d คูณกับ e แล้วหารด้วย z เหลือเศษ 1 ($ed \bmod z = 1$)
- 5) กุญแจสาธารณะที่ได้คือ จำนวน (n, e) ส่วนกุญแจส่วนตัวคือ (n, d)

ขั้นตอนในการเข้าและถอดรหัสจะเป็นดังนี้ ถ้าผู้ส่งต้องการส่งข้อมูล m โดยที่ $m < n$ ในการเข้ารหัสนั้น จะใช้กุญแจสาธารณะ (n, e) ซึ่งมีสูตรในการเข้ารหัส ดังนี้

$$c = m^e \bmod n$$

โดยที่ c คือข้อมูลที่ถูกเข้ารหัสแล้ว ส่วนในการถอดรหัสนั้นจะใช้กุญแจส่วนตัว (n, d) ซึ่งมีสูตรดังนี้

$$m = c^d \bmod n$$

ในการเข้ารหัสและถอดรหัสที่นั่นจึงทำงานโดยอาศัยทฤษฎีทางคณิตศาสตร์ ได้แก่ เลขยกกำลัง (Exponentiation) และเศษจากการหาร (Modulo)

ความปลอดภัยของการเข้ารหัสแบบ RSA นี้จึงขึ้นอยู่กับความยากในการหาตัวประกอบของตัวเลขที่มีค่ามากๆ p และ q ดังกล่าว ถ้าผู้โจมตีสามารถหาตัวประกอบของเลขสำหรับเข้ารหัส n ได้ ก็อาจหาค่าของ p และ q ได้เช่นกัน และนำไปสู่การหาค่าของ z ได้ในที่สุด เมื่อรู้ค่าของ z แล้ว ก็สามารถเชื่อมโยงไปหาค่า e ได้เช่นกัน ปกติในการคำนวณหาค่า d นั้นจะใช้ขั้นตอนวิธีของยูคลิด (Euclid's algorithm) ริเวสต์และคเนะ ได้พิสูจน์ให้เห็นว่า การคำนวณหาตัวประกอบของเลข 200 หลัก จะใช้เวลาจนถึงสี่พันปี ในการคำนวณหาตัวประกอบสำหรับเลข 500 หลัก ต้องใช้เวลาประมาณ 10^{25} ปี นอกจากนั้น พวกเขายังได้ใช้ขั้นตอนวิธีที่ดีที่สุดในขณะนั้น และใช้คอมพิวเตอร์ที่มีความเร็ว 1 MIPS (Million Instruction per Second-ล้านคำสั่งต่อวินาที) ก็ยังไม่สามารถคำนวณหาตัวประกอบของเลข 500 หลักได้ แสดงให้เห็นว่า แม้จะหาตัวประกอบ p และ q ที่มีขนาดใหญ่ได้ แต่ต้องใช้เวลาเนิ่นนานเกินไป

ยกตัวอย่างเช่น บ๊อบเลือก $p=5$ และ $q=7$ เพราะฉะนั้น $n=35$, $z=24$ และเลือก $e=5$ เพราะ 5 ไม่มีตัวหารร่วมกับ 24, $d=29$ เพราะ $e*d \bmod n=1$ กฎแจกสาธารณะของเขาขณะนี้คือ (35, 5) และกฎแจกส่วนตัวคือ (35, 29) สมมุติว่า อลิสต้องการส่งข้อความ “love” ไปหาบ๊อบ โดยแปลงตัวอักษรให้เป็นตัวเลขระหว่าง 1-26 ($a \Rightarrow 1$, $b \Rightarrow 2$, ..., $z \Rightarrow 26$) ทั้งคู่จะต้องเข้ารหัสและถอดรหัสดังตารางที่ 7.1 และ 7.2 ตามลำดับ

ตาราง 7.1 การเข้ารหัสด้วยขั้นตอนวิธีแบบ RSA โดยที่ $n=35$ และ $e=5$

Plaintext	m	m^e	Ciphertext ($m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

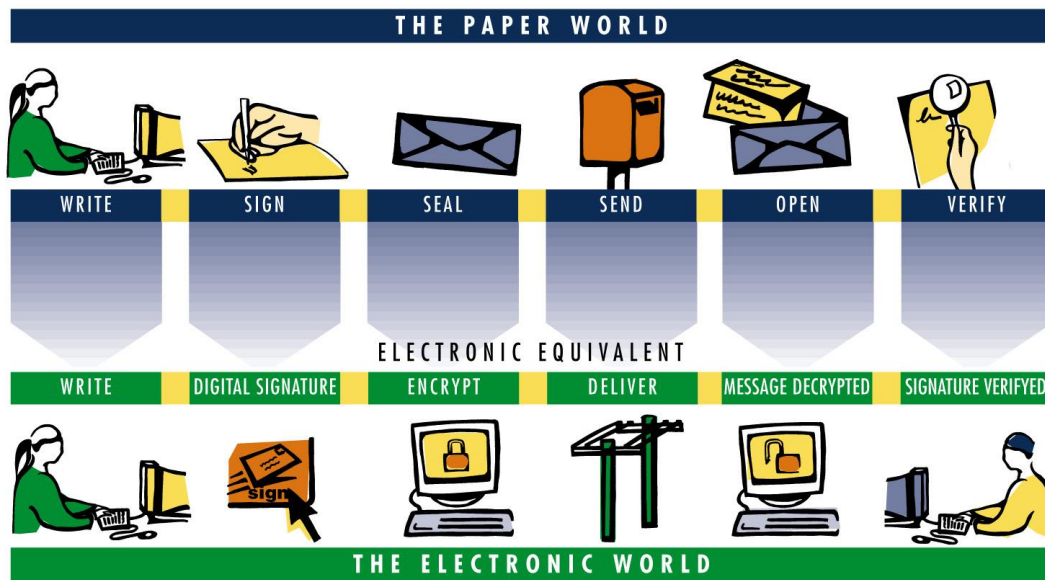
ตาราง 7.2 การถอดรหัสด้วยขั้นตอนวิธีแบบ RSA โดยที่ $n=35$ และ $d=29$

Ciphertext	c^d	$m=c^d \bmod n$	Plaintext
17	4.8196857210675091509141182522307e+35	12	l
15	1.2783403948858939111232757568359e+34	15	o
22	8.5164331908653770195619449972111e+38	22	v
10	10000000000000000000000000000000	5	e

จากตัวอย่างข้างบนนี้ จะพบว่า แม้จะเลือกกุญแจที่เป็นตัวเลขน้อยๆ แต่จำนวนที่ได้จากการยกกำลังตามขั้นตอนวิธีแบบ RSA นั้นมีค่ามากๆ ค่าที่ได้สำหรับการเข้ารหัสและถอดรหัสจึงมีความยาวมากๆ ไปด้วย การถอดรหัสตามขั้นตอนวิธีแบบ RSA จึงมีความยากอย่างยิ่ง โดยทั่วไป กุญแจที่ใช้บนอินเทอร์เน็ตนั้นมีขนาด 1024 บิต จึงทำให้การถอดรหัสของผู้โจมตีจำเป็นต้องใช้เวลานานมากเกินไป อย่างไรก็ตาม การเลือกกุญแจที่มีขนาดยาวๆ ก็ส่งผลทำให้ขั้นตอนในการเข้ารหัสและถอดรหัสตามขั้นตอนวิธีดังกล่าวต้องใช้เวลานานขึ้นอีกด้วยเมื่อเทียบกับการใช้กุญแจแบบบล็อกเดียวของขั้นตอนวิธีแบบสมมาตรเช่น DES, 2DES, 3DES และ AES เป็นต้น ในทางปฏิบัติ เราสามารถใช้ RSA ควบคู่กับ DES เพื่อลดเวลาในกระบวนการทั้งการเข้ารหัสและถอดรหัส โดยครั้งแรกจะใช้ RSA สำหรับแจกจ่ายกุญแจลับของ DES ไปยังผู้รับที่เกี่ยวข้องเพื่อใช้ในการเข้ารหัสและถอดรหัส ซึ่งกุญแจดังกล่าวนี้เรียกว่า เซสชันคีย์ (Session key)

7.6 ลายมือชื่อดิจิทัล (Digital signature)

การใช้กุญแจ 2 ดอกของการเข้ารหัสแบบสมมาตรช่วยให้การเข้ารหัสและถอดรหัสมีความปลอดภัยมากยิ่งขึ้น อย่างไรก็ตาม เราจะมั่นใจได้อย่างไรว่าเรากำลังสื่อสารอยู่กับผู้ส่งหรือผู้รับตัวจริง และในฐานะผู้รับเอกสารที่เราได้รับมาจากผู้ส่งเราจะมั่นใจได้อย่างไรว่าเอกสารถูกส่งมาจากผู้ส่งตัวจริง หากผู้ส่งปฏิเสธความรับผิดชอบว่าเอกสารที่เราได้รับนั้นไม่ได้ถูกส่งมาจากเขา (แต่ถูกลักลอบส่งมาในชื่อของเขาแทน)



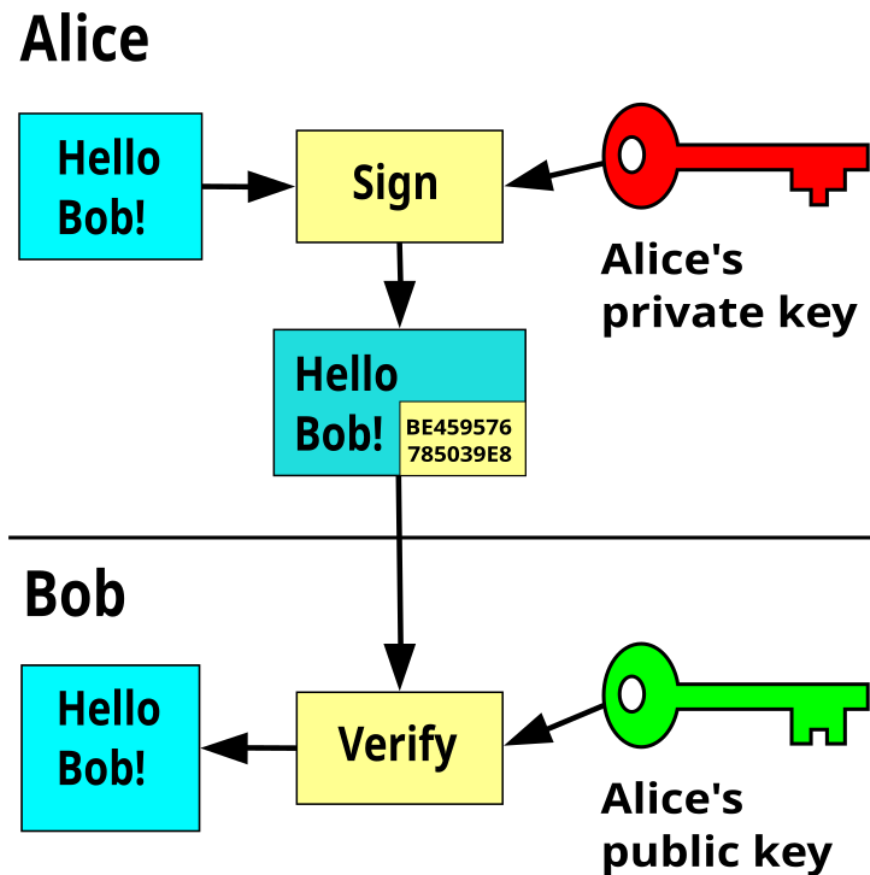
รูป 7.10 แสดงการเปรียบเทียบการลงลายมือชื่อแบบปกติและแบบที่ใช้งานในโลกดิจิทัล

การเซ็นชื่อท้ายเอกสารทั่วไบนั้นเป็นการระบุความเป็นเจ้าของเอกสารฉบับนั้นว่าเป็นของผู้เซ็น หรือผู้เซ็นเห็นด้วยกับเนื้อหาในเอกสารนั้น ในโลกของข้อมูลแบบดิจิทัล ลายมือชื่อดิจิทัลได้ถูกนำมาเป็นเทคนิค เพื่อให้บรรลุจุดมุ่งหมายดังกล่าว รูป 8.9 เปรียบเทียบให้เห็นถึงการลงลายมือชื่อแบบธรรมดา กับแบบดิจิทัล เราจึงใช้ลายมือชื่อดิจิทัลเพื่อจุดมุ่งหมายสำคัญ 3 ประการ

- 1) เพื่อพิสูจน์ว่าเอกสารที่ได้รับนั้นมาจากผู้ส่งตัวจริง และไม่ได้ถูกปลอมแปลงขึ้น ซึ่งเรียกคุณสมบัตินี้ว่า การพิสูจน์ตัวจริง (Authentication)
- 2) เจ้าของเอกสารไม่สามารถบอกปัดหรือปฏิเสธความรับผิดชอบในความเป็นเจ้าของเอกสารนั้นได้ เรียกคุณสมบัตินี้ว่า การไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-repudiation)
- 3) พิสูจน์ได้ว่า เนื้อหาในเอกสารได้ถูกเปลี่ยนแปลงหรือไม่ เรียกคุณสมบัตินี้ว่า บูรณภาพของข้อมูล (Data Integrity)

แม้ว่า การเข้ารหัสแบบอสมมาตรนั้น สามารถใช้เป็นลายมือชื่อดิจิทัลได้เช่นกัน เพราะเทคนิคดังกล่าวสามารถตรวจสอบผู้เซ็นได้จากกุญแจส่วนตัว/สาธารณะที่ใช้ และข้อมูลนั้นไม่สามารถถูกเปลี่ยนแปลงแก้ไขได้อย่างแน่นอน ซึ่งเป็นการระบุตัวตนของผู้เป็นเจ้าของได้เป็นอย่างดี อย่างไรก็ตาม การเข้าและถอดรหัสโดยใช้กุญแจสาธารณะ/ส่วนตัวนั้นใช้เวลานานเกินไป โดยเฉพาะอย่างยิ่งในกรณีที่เอกสารมีขนาดใหญ่ เนื่องจากในขั้นตอนการเข้าและถอดรหัสนั้นจะมีการคำนวณเลขยกกำลังจำนวนมาก นอกจากใช้เวลานานแล้วยังใช้กำลังจาก

หน่วยประมวลผลมากอีกด้วย นอกจากนั้น จุดประสงค์หลักของลายมือชื่อดิจิทัลนั้นแตกต่างไปจากการเข้ารหัสแบบอสมมาตร กล่าวคือ การเข้ารหัสแบบอสมมาตรนั้นมีจุดประสงค์หลักเพื่อปกปิดข้อความที่ต้องการส่ง ซึ่งเน้นคุณสมบัติด้านการรักษาความลับข้อมูล (Confidentiality) ในขณะที่ลายมือชื่อดิจิทัลถูกใช้เพื่อเป็นการรับรองว่าเอกสารฉบับนั้นเป็นของผู้ส่งหรือผู้ลงลายเซ็นนั้นเห็นด้วยกับข้อความดังกล่าวโดยที่มั่นใจได้ว่าเนื้อหาในเอกสารนั้นจะไม่ได้ถูกแก้ไขไปโดยบุคคลที่สาม ดังนั้น เนื้อหาในเอกสารนั้นสามารถอาจถูกเปิดเผยได้



รูป 7.11 หลักการทำงานของลายมือชื่อดิจิทัล

(By FlippyFlink - Combined changed the image

https://en.wikipedia.org/wiki/File:Public_key_encryption.svg from encryption to signing., CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=78867393>)

ดังนั้น การพัฒนาลายมือชื่อดิจิทัลจึงเกิดขึ้นเพื่อจุดมุ่งหมายดังกล่าว หลักการทำงานของลายมือชื่อดิจิทัลมีขั้นตอนดังแสดงในรูป 7.11 ซึ่งสามารถสรุปขั้นตอนได้ดังนี้

- 1) ข้อมูลที่ต้องการส่งจะถูกนำไปคำนวณเพื่อให้ได้ข้อความที่สั้นลง โดยใช้ฟังก์ชันแฮช (Hash function) เพื่อให้ได้ข้อมูลสั้นๆ มีความยาวคงที่ เรียกว่า แฮชเสกไดเจสต์ (Message digest)
- 2) ผู้ส่งจะเซ็นชื่อในเอกสารโดยการเข้ารหัสแฮชเสกไดเจสต์ ด้วยการใช้กุญแจส่วนตัวของตนเอง ผลลัพธ์ที่ได้จะเรียกว่า ลายมือชื่อดิจิทัล ของเอกสารนั้น
- 3) ข้อความเดิมจะถูกส่งไปพร้อมกับลายมือชื่อดิจิทัลไปยังผู้รับ
- 4) ผู้รับสามารถตรวจสอบข้อความที่ได้รับโดย
 - a) คำนวณย้อนกลับแฮชเสกไดเจสต์โดยใช้ฟังก์ชันแฮชเดียวกัน
 - b) ใช้กุญแจสาธารณะของผู้ส่งในการถอดรหัสลายมือชื่อดิจิทัลที่ถูกส่งมาพร้อมกับแฮชเสกไดเจสต์อีกชุดหนึ่ง
 - c) เปรียบเทียบแฮชเสกไดเจสต์ที่คำนวณได้กับข้อความที่ถอดได้ ถ้าเหมือนกันแสดงว่าข้อความไม่ได้ถูกเปลี่ยนแปลงไปจากข้อความเดิม

ฟังก์ชันแฮชที่นิยมใช้มีมากมาย ได้แก่ MD4, MD5, SHA-1, CBC-DES-MAC, HMAC และ RIPEMD-160 ซึ่งมีความแตกต่างกันตามความยาวของกุญแจที่ใช้ และความยาวของแฮชเสกไดเจสต์ที่ได้

ฟังก์ชันแฮชทางเดียว (One-way hash function) คือขั้นตอนวิธีที่รับข้อความ M ที่มีขนาดความยาวแปรเปลี่ยนได้ไปประมวลผลเพื่อให้ได้เป็นรหัสแฮช $H(M)$ ที่มีขนาดคงที่ ฟังก์ชันแฮชทางเดียวมีชื่อเรียกได้ชื่อ ได้แก่ message digest, digital fingerprint และ compression function คุณสมบัติสำคัญของฟังก์ชันแฮช คือ การคำนวณเพื่อหาค่าของรหัสแฮช $H(M)$ จากข้อความ M มีขั้นตอนที่ชัดเจนไม่ซับซ้อน แต่ในทางกลับกัน หากกำหนดรหัสแฮช $H(M)$ มาให้ค่าหนึ่ง การคำนวณย้อนกลับเพื่อหาข้อความ M ที่ทำให้เกิดรหัสแฮชดังกล่าวนั้นทำได้ยากอย่างยิ่ง นอกจากนั้น การหาข้อความ M จำนวน 2 ชุด ที่ให้รหัสแฮชค่าเดียวกันก็เป็นเรื่องที่ยากเช่นเดียวกัน เราเรียกคุณสมบัติแบบทางเดียวของฟังก์ชันแฮชข้อนี้ว่า คุณสมบัติปลอดการชน (Collision-free)

HMAC (Hashed Message Authentication Code) เป็นขั้นตอนวิธีที่ถูกนำไปใช้เป็นส่วนหนึ่งของลายเซ็นดิจิทัลเพื่อประกันบูรณภาพของข่าวสารในขณะส่งถูกส่งผ่าน แต่ HMAC ไม่มีฟังก์ชันด้านการปฏิเสธความรับผิดชอบ (Repudiation) [103] เราจึงสามารถประยุกต์ใช้ฟังก์ชันแฮชเข้ากับการลงลายมือชื่อดิจิทัลเพื่อการตรวจสอบบูรณภาพของข้อมูล ซึ่งสามารถกระทำกับเอกสารหรือข้อความต้นฉบับโดยตรงก็ได้ หรือกระทำกับค่าแฮชที่ได้จากเอกสารต้นฉบับแทนก็ได้ การเลือกทำกับค่าแฮชของเอกสารต้นฉบับนั้นจะทำให้การประมวลผลเร็วกว่าเนื่องจากค่าแฮชจะมีขนาดเล็กกว่าเอกสารต้นฉบับ นอกจากนั้น เรายังสามารถนำเอกสารต้นฉบับไปผ่านการ

ประทับเวลา (Timestamping) ก็ได้โดยไม่จำเป็นต้องเปิดเผยเอกสารต้นฉบับ ในกรณีเช่นนี้ การใช้ค่าแฮชแทนเอกสารต้นฉบับย่อมมีความเหมาะสมกว่า

ขั้นตอนวิธีของฟังก์ชันแฮชแบบ MD-4 ได้รับการพัฒนาโดย ริเวสต์ (Ron Rivest) ในปี พ.ศ. 2533 และปรับปรุงเป็น MD-5 ในปีต่อมา ใช้ค่าแฮชขนาด 128 บิต ส่วน SHA-1 ได้รับการพัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติในปี พ.ศ. 2535 และจัดว่าเป็นฟังก์ชันแฮชที่มีความมั่นคงกว่าแบบ MD-4 และ MD-5 เพราะให้ค่าแฮชขนาด 160 บิต เพราะการโจมตีค่าแฮชขนาด 160 บิตด้วยวิธีค้นหาทุกค่าที่เป็นไปได้นั้น ต้องทดสอบค่ามากถึง $2^{160} = 1.5 \times 10^{48}$ กรณี ซึ่งถือว่าเป็นค่าที่ใหญ่มาก

7.7 การโจมตีระบบรหัสลับ

การโจมตีรหัสลับเพื่อต้องการรู้ถึงข้อความต้นฉบับหรือกุญแจที่ใช้ในการเข้ารหัสและถอดรหัส สามารถทำได้ 2 วิธี ได้แก่ การวิเคราะห์รหัสลับ และการโจมตีแบบ Brute-force

7.7.1 การวิเคราะห์รหัสลับ

ในการโจมตีระบบรหัสลับนั้น นักวิเคราะห์รหัสลับจำเป็นต้องรู้จักโครงสร้างของรหัสลับที่ต้องการโจมตี ดังนั้น ผู้สร้างรหัสลับจะออกแบบภายใต้สมมุติฐานที่ว่าผู้โจมตีสามารถรู้ถึงระบบรหัสลับที่ใช้ ตามหลักการที่เรียกว่า Kerckhoff's principle

การวิเคราะห์รหัสลับเพื่อทำการโจมตีนั้น สามารถกระทำได้หลายวิธีขึ้นอยู่กับขีดความสามารถของผู้โจมตีและข้อมูลที่สามารถเข้าถึงได้ ประกอบด้วย

- 1) ข้อความไซเฟอร์อย่างเดียว เป็นสถานการณ์ที่ผู้โจมตีสามารถเข้าถึงข้อความไซเฟอร์ y และต้องการทราบกุญแจหรือข้อความต้นฉบับ วิธีนี้เป็นวิธีที่ผู้โจมตีมีข้อมูลน้อยที่สุด
- 2) รู้ข้อความต้นฉบับ ผู้โจมตีสามารถรู้ข้อความต้นฉบับ x และข้อความไซเฟอร์ y ที่สัมพันธ์กัน โดยผู้โจมตีอาจรู้จักรูปแบบของข้อความต้นฉบับที่ปรากฏอยู่ในข้อความ ตัวอย่างเช่น แฟ้มภาษาโพสต์สคริปต์ที่มีรูปแบบมาตรฐานที่ต้นแฟ้มเสมอ หรือเอกสารทางธุรกิจที่มีปรากฏข้อความมาตรฐานตามที่ใช้กันอยู่ในบริเวณที่แน่นอน เมื่อผู้โจมตีมีทั้งข้อความต้นฉบับและข้อความไซเฟอร์ที่คู่กันนั้น ย่อมสามารถวิเคราะห์หาความสัมพันธ์ระหว่างข้อความต้นฉบับและข้อความไซเฟอร์เพื่อหากุญแจได้
- 3) เลือกข้อความต้นฉบับ เป็นสถานการณ์ที่ผู้โจมตีสามารถเข้าถึงเครื่องที่ใช้ในการเข้ารหัสลับได้ชั่วคราว จึงสามารถเลือกข้อความต้นฉบับ x ได้ตามความต้องการ และยังได้ข้อความไซเฟอร์

y ที่คู่กันอีกด้วย ในสถานการณ์นี้ผู้โจมตีสามารถเลือกรูปแบบข้อความที่ต้องการเข้ารหัสเพื่อศึกษาแบบอย่างของข้อความไซเฟอร์ที่สัมพันธ์กันเพื่อใช้ในการวิเคราะห์หาค่ากุญแจได้

- 4) เลือกข้อความไซเฟอร์ เป็นสถานการณ์ที่ตรงข้ามกับวิธีที่ผ่านมา โดยผู้โจมตีสามารถเข้าถึงเครื่องที่ใช้ในการเข้ารหัสลับได้ชั่วคราว จึงสามารถเลือกข้อความไซเฟอร์ y ได้ จากนั้นทำการถอดรหัสเพื่อให้ได้เป็นข้อความต้นฉบับแทน
- 5) การวิเคราะห์ความแตกต่าง เป็นวิธีการโจมตีแบบเลือกข้อความอีกวิธีหนึ่ง โดยผู้โจมตีทำการเข้ารหัสข้อความหลายๆ ฉบับที่แตกต่างกันเล็กน้อย จากนั้น นำมาเปรียบเทียบข้อความไซเฟอร์ที่ได้ ก็สามารถค้นพบรูปแบบการเข้ารหัสได้

ในการโจมตีระบบรหัสลับนั้น ความรุนแรงหรือความสำเร็จจะขึ้นอยู่กับวิธีการที่ใช้ในการโจมตี ถ้าผู้โจมตีที่รู้เพียงข้อความไซเฟอร์เท่านั้น ความสำเร็จก็ยากอย่างยิ่ง โดยทั่วไป ขั้นตอนวิธีการเข้ารหัสย่อมทนทานต่อการโจมตีประเภทนี้อยู่แล้ว นอกจากนั้น ขั้นตอนวิธีการเข้ารหัสส่วนใหญ่ในปัจจุบันมีความทนทานต่อการโจมตีที่รู้ข้อความต้นฉบับได้เป็นอย่างดี

7.7.2 การโจมตีแบบ Brute-force

การโจมตีแบบ Brute-force เป็นการโจมตีที่ผู้โจมตีทำการเดาค่ากุญแจทุกค่าที่เป็นไปได้แล้วนำค่ากุญแจที่ได้มาถอดรหัสข้อความไซเฟอร์ จนกระทั่งสามารถถอดข้อความออกมาได้เป็นข้อความต้นฉบับ การโจมตีประเภทนี้เป็นการโจมตีที่ไม่สามารถป้องกันได้ เพราะผู้โจมตีสามารถออกแรงเดาค่ากุญแจไปเรื่อยๆ จนกว่าจะพบนั่นเอง ดังนั้น การรับมือกับการโจมตีประเภทนี้จึงขึ้นอยู่กับขนาดของกุญแจที่ใช้เป็นสำคัญ การกำหนดค่ากุญแจขนาดยาวจะทำให้การโจมตีประเภทนี้มีความยากลำบากในการโจมตี

ขนาดของกุญแจ 2 บิต จะมีค่าที่เป็นไปได้อยู่ 4 ค่า หรือ 2^2 ได้แก่ 00, 01, 10 และ 11 ถ้าขั้นตอนวิธีที่มีกุญแจขนาด n บิต จำนวนค่าทั้งหมดของกุญแจที่จะเป็นไปได้จะเท่ากับ 2^n ถ้ากำหนดให้กุญแจที่ใช้ในขั้นตอนวิธีมีจำนวนบิตสูงขึ้น ย่อมทำให้การโจมตีด้วยวิธี Brute-force มีความยากลำบากมากยิ่งขึ้นเพราะต้องใช้เวลาในการเดาค่านานมากขึ้น ตารางที่ 7.3 แสดงให้เห็นถึงขนาดกุญแจและจำนวนกุญแจที่มีขนาดแตกต่างกัน รวมทั้งเวลาที่ใช้ในการเดาค่ากุญแจ

ตาราง 7.3 ขนาดกุญแจและเวลาที่ใช้ในการเดารหัสกุญแจ โดยคิดเวลา 1 ล้านล้านครั้งต่อวินาที

ขนาดกุญแจ (บิต)	จำนวนกุญแจทั้งหมด	เวลาที่ใช้ในการถอดรหัส
32	$2^{32} = 4.3 \times 10^9$	1.25 มิลลิวินาที

ขนาดกุญแจ (บิต)	จำนวนกุญแจทั้งหมด	เวลาที่ใช้ในการถอดรหัส
56	$2^{56} = 7.2 \times 10^{16}$	10.01 ชั่วโมง
112	$2^{112} = 5.2 \times 10^{33}$	8.2×10^{13} ปี
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} ปี
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} ปี
256	$2^{256} = 5.8 \times 10^{64}$	1.8×10^{57} ปี

จากตารางด้านบนจะพบว่า ถ้ากุญแจมีขนาดเล็ก ผู้โจมตีสามารถค้นหาค่ากุญแจเพื่อถอดข้อความไซเฟอร์ออกมาได้ด้วยเวลาไม่นาน บนพื้นฐานของเทคโนโลยีคอมพิวเตอร์ในปัจจุบัน ยิ่งไปกว่านั้น เทคโนโลยีคอมพิวเตอร์แบบขนาน (Parallel computer) หรือควอนตัมคอมพิวเตอร์ (Quantum computer) [98] จะยิ่งทำให้เวลาในการถอดรหัสลดน้อยลงอย่างมาก ถ้าขนาดของกุญแจเพิ่มขึ้นเป็น 112 บิต 128 บิต 168 บิต หรือ 256 บิต การถอดรหัสจะต้องใช้เวลานานยาวนานเกินไป นอกจากนั้น จะพบว่า กุญแจขนาด 128 บิต ยังคงสามารถทนทานต่อการถูกโจมตีแบบ Brute-force ได้โดยอาศัยเทคโนโลยีคอมพิวเตอร์ในปัจจุบัน อย่างไรก็ตาม ต้องตระหนักว่า กุญแจที่มีขนาดใหญ่ย่อมทนทานต่อการโจมตีได้ยาวนานกว่ากุญแจขนาดเล็กก็จริง แต่ก็มาพร้อมกับการประมวลผลที่ยาวนานขึ้นในการเข้ารหัสและถอดรหัสอีกด้วย

7.7.3 ความมั่นคงของขั้นตอนวิธีการเข้ารหัสลับ

ดังที่ได้อธิบายไว้ในหัวข้อก่อนหน้านี้แล้วว่า ความมั่นคงของระบบรหัสลับอยู่ที่ขนาดของกุญแจที่ใช้ในขั้นตอนวิธีการเข้ารหัสลับเป็นสำคัญ นั่นหมายความว่า การเลือกใช้ขั้นตอนวิธี RSA ด้วยกุญแจขนาด 128 บิต ย่อมมีความปลอดภัยสูงกว่าแบบ DES ด้วยกุญแจขนาด 56 บิต (บวกด้วยอีก 8 บิตสำหรับบิตตรวจสอบ) อย่างไรก็ตาม หากพิจารณาในด้านความเร็วแล้ว DES ย่อมใช้เวลาในการประมวลผลในกระบวนการเข้ารหัสและถอดรหัสน้อยกว่าแบบ RSA รวมทั้งความสิ้นเปลืองในการใช้พลังงานหลังจากการประมวลผลของระบบคอมพิวเตอร์ต่ำกว่าอีกด้วย

ในบางสถานการณ์การเลือกใช้ขั้นตอนวิธีแบบ DES (หรือแบบอื่นๆ) ในการเข้ารหัสเพื่อปกป้องข้อมูลที่มีระดับลับน้อย อาจเหมาะสมกว่าการเลือกใช้ขั้นตอนวิธีที่มีความปลอดภัยสูงแต่ต้องการพลังจากการประมวลผลมากกว่า ดังนั้น เราควรทราบว่าขั้นตอนวิธีเข้ารหัสที่เราจะใช้นั้นมีความมั่นคงปลอดภัยอยู่ในระดับใด โดยทั่วไป เราสามารถแบ่งความปลอดภัยของขั้นตอนวิธีได้ 2 ประเภท ดังนี้

7.7.4 ขั้นตอนวิธีที่ปลอดภัยโดยปราศจากเงื่อนไข (Unconditional secure algorithm)

จัดว่าเป็นขั้นตอนวิธีที่มีความมั่นคงปลอดภัยสูงสุด เพราะผู้โจมตีจะไม่สามารถถอดรหัสข้อความไซเฟอร์กลับไปเป็นข้อความต้นฉบับได้ไม่ว่าในกรณีใดๆ ไม่ว่าจะใช้ระบบคอมพิวเตอร์ที่มีพลังของการประมวลผลสูงเพียงใดก็ตาม เพราะข้อมูลที่ผู้โจมตีได้จากข้อความที่ผ่านการเข้ารหัสแล้วนั้นไม่มีข้อมูลมากพอที่จะนำไปใช้ในการถอดรหัสเพื่อย้อนกลับไปเป็นข้อความต้นฉบับได้ โดยหลักการแล้ว ขั้นตอนวิธีที่ปลอดภัยโดยปราศจากเงื่อนไขคือรหัสผ่านแบบใช้ครั้งเดียว (One-time pad)

7.7.5 ขั้นตอนวิธีที่ปลอดภัยเชิงคำนวณ (Computationally secure algorithm)

เป็นขั้นตอนวิธีที่ผู้โจมตีต้องใช้เวลานานมากจึงจะสามารถถอดข้อความที่ผ่านการเข้ารหัสกลับไปเป็นข้อความต้นฉบับได้อย่างสมบูรณ์ อาจต้องใช้เวลานานชั่วอายุขัยหรือมีค่าใช้จ่ายในการถอดรหัสอย่างมหาศาล โดยทฤษฎีแล้ว ผู้โจมตีสามารถถอดรหัสข้อความเข้ารหัสได้เสมอถ้ามีเวลาและพลังในการประมวลผลที่เพียงพอ ดังนั้นในทางปฏิบัติในการใช้งานในระบบความปลอดภัย เราจึงไม่จำเป็นต้องใช้ขั้นตอนวิธีที่ปลอดภัยโดยปราศจากเงื่อนไขสำหรับปกป้องความลับข้อมูลก็ได้ เราสามารถเลือกใช้ขั้นตอนวิธีที่มีความมั่นคงเชิงคำนวณก็เพียงพอ

ขั้นตอนวิธีการเข้ารหัสลับที่ใช้อยู่ในปัจจุบัน เช่น AES และ RSA นั้น จัดว่าเป็นขั้นตอนวิธีที่มีความมั่นคงสูงตรงเท่าที่สมมติฐานของสมรรถนะของระบบคอมพิวเตอร์ยังคงใช้กันอยู่ในเทคโนโลยีปัจจุบัน

นอกจากนั้น ระบบความปลอดภัยที่มีการผสมผสานระหว่างระบบการเข้ารหัสร่วมกับระบบความปลอดภัยประเภทอื่นๆ เช่น ลายมือชื่อดิจิทัล การใช้เครือข่ายส่วนตัวเสมือน รวมทั้งการออกแบบเครือข่ายที่ใช้การแปลงเลขที่อยู่เครือข่ายเพื่อซ่อนองค์ประกอบสำคัญของทรัพยากรเครือข่ายไว้ไม่ให้ผู้บุกรุกสามารถมองเห็นเพื่อวิเคราะห์และโจมตีได้โดยง่าย ถือเป็นทางเลือกที่สามารถประกันถึงความมั่นคงของระบบความปลอดภัยที่รัดกุม ถือเป็นแนวทางที่น่าสนใจ

7.8 สรุปบท

เนื้อหาในบทนี้นำเสนอภาพรวมเกี่ยวกับวิทยาการรหัสลับ โดยอธิบายหลักการ ความมั่นคงของขั้นตอนวิธีการเข้ารหัสลับ การแบ่งประเภทขั้นตอนวิธีตามระดับความปลอดภัย และการนำไปประยุกต์ใช้ในระบบความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ยังชี้ให้เห็นความสำคัญของการพัฒนาทักษะทั้งภาคทฤษฎีและปฏิบัติ เพื่อให้การปกป้องข้อมูลมีประสิทธิภาพและสอดคล้องกับมาตรฐานสากลในยุคปัจจุบัน

บทวิเคราะห์และมุมมองเชิงวิชาการ: “พื้นฐานวิทยาการรหัสลับ (Cryptography Overview)”

เอกสาร “พื้นฐานวิทยาการรหัสลับ” วางรากฐานที่จำเป็นต่อรายวิชา หลักการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Principles) ตั้งแต่นิยามวิทยาการรหัสลับ องค์ประกอบของระบบรหัส (plaintext/algorithm/key/ciphertext/decryption), การจำแนกแบบสมมาตร-อสมมาตร, DES-2DES-3DES-AES, Diffie-Hellman-Oakley, RSA, และลายมือชื่อดิจิทัล ตลอดจนภาพรวมการโจมตี (brute force, cryptanalysis, meet-in-the-middle) ซึ่งเป็น “กระดูกสันหลัง” ในการออกแบบระบบความมั่นคงสมัยใหม่และหลักสูตรเชิงหลักฐานสำหรับวิชาชีพด้าน Cybersecurity สรุปสาระสำคัญแต่ละหัวข้อได้ดังนี้

1) สังเคราะห์จากต้นฉบับ: จุดแข็งที่ใช้ต่อยอดการเรียนรู้

- **กรอบแนวคิดและคำจำกัดความครบถ้วน:** ตั้งแต่ความหมายของ cryptography/cryptanalysis, โครงสร้าง cryptosystem 5 องค์ประกอบ, ไปจนถึงการจำแนก substitution vs transposition, block vs stream ใช้เป็น “ภาษากลาง” ของห้องเรียนและกรอบอ้างอิงในรายงาน
- **สายอัลกอริทึมคลาสสิกสู่มาตรฐานปัจจุบัน:** บรรยาย DES-2DES-3DES-AES (กลไก Feistel, S-box, P-box, key schedule, รอบการเข้ารหัส) พร้อมข้อจำกัดด้านความยาวกุญแจและการโจมตีพบกันครึ่งทางใน 2DES เพื่อเป็นฐานให้ผู้เรียนเข้าใจเหตุผลเชิงวิศวกรรมที่ทำให้ AES กลายเป็น baseline
- **อสมมาตรและการกระจายกุญแจ:** อธิบาย DH, ปัญหา man-in-the-middle, แนวทาง Oakley (cookie, nonce, anti-clogging) และ RSA (คณิตศาสตร์เบื้องต้น, กุญแจคู่, ขั้นตอนยกกำลังโมดูลาร์) รวมถึงการใช้ลายมือชื่อดิจิทัลเพื่อ authentication/integrity/non-repudiation

นัยต่อการเรียนรู้: โครงสร้างดังกล่าวเหมาะจะ “เชื่อมสะพาน” จาก ปรัชญาเชิงแนวคิด → การก่อสร้าง (construction) → การใช้งานในโปรโตคอลจริง ให้ผู้เรียนเห็นเส้นทางเหตุผลครบวงจร ไม่ใช่ท่องจำสูตรล้วน ๆ

2) ข้อเสนอแนะในการต่อยอด จากภาคทฤษฎีสู่ภาคปฏิบัติ: จาก “เข้ารหัสได้” สู่ “ใช้ถูกต้องและพิสูจน์ได้”

เนื่องจากสภาพรายวิชานี้เป็นทฤษฎีล้วนไม่มีปฏิบัติ แต่ผู้สอนก็ได้การออกแบบการเรียนรู้ที่พยายามปูรากฐานทฤษฎีหรือหลักการที่เป็นที่ยอมรับอย่างเป็นทางการเป็นมาตรฐานสากล เช่น NIST Cybersecurity framework เพื่อให้สามารถให้ผู้เรียนไปประยุกต์ต่อยอดในภาคปฏิบัติได้ ข้อเสนอแนะก็คือ ควรมียาวิชาต่อยอดจากรายวิชานี้เป็นรายวิชาภาคปฏิบัติที่มีแลปให้นักศึกษาได้ฝึกฝนได้จริง โดยต่อยอดดังนี้

1. **Authenticated Encryption** เป็นค่าตั้งต้น แม้ต้นฉบับเน้นบล็อกไซเฟอร์ระดับ primitive (DES/3DES/AES) การสอนสมัยใหม่ควรยกระดับไปที่ AEAD เช่น AES-GCM และ ChaCha20-Poly1305 เพื่อให้ได้ *confidentiality+integrity* ในคราวเดียว ลดโอกาสโจมตีแบบ padding-oracle/bit-flipping ที่มักเกิดจากการประกอบ primitive ผิดวิธี
2. โหมดการทำงานสำคัญกว่าตัวไซเฟอร์ แยกให้ชัดระหว่าง CBC/CTR/CFB/OFB/GCM/XTS และประเด็น *nonce/IV reuse* ที่ “ผิดครั้งเดียวพังทั้งระบบ” เป็นหัวใจของการออกแบบแลบ *misuse resistance* ที่สะท้อนการใช้งานจริงใน TLS, IPsec, SSH ฯลฯ
3. **Side-Channel & Constant-Time** ต้นฉบับในเอกสารนี้อธิบายถึงการโจมตีเชิงคณิตศาสตร์/แรงดันเชิงกระประมวลผลได้ชัดเจนแล้ว ควรเติม *side-channel* (timing/cache/power/fault) และหลัก *constant-time coding, blinding, masking* เพื่อฝึก “คิดให้พ้นแบบจำลองช่องสื่อสารสมบูรณ์แบบ”
4. **Key Management คือแกนกลาง** จากข้อสังเกตเรื่อง *key length* ในต้นฉบับ สามารถต่อยอดไป วงจรชีวิตกุญแจ (generation-storage-rotation-revocation), KDF (HKDF), HSM/KMS/TPM, threshold cryptography และ forward secrecy (X25519/ffdhe) เพื่อให้ผู้เรียนออกแบบระบบครบวงจร ไม่หยุดที่อัลกอริทึม
5. **Hash & Password Hardening** เติม SHA-2/SHA-3 (Keccak)/HMAC และ password hashing ที่ทันสมัย (Argon2id แทน PBKDF2/bcrypt ในบริบทใหม่) เพื่อเชื่อมกับลอจิกยืนยันตัวตน, การเก็บรหัสผ่าน, และเหตุการณ์รั่วข้อมูล
6. **คริปโตในโปรโตคอลจริง** ผูกกับ TLS 1.3/QUIC (AEAD-only, forward secrecy by default), IPsec/IKEv2 และ WireGuard (design-minimalism, roaming, modern primitives) เพื่อให้ผู้เรียนเห็น “ระบบ” ไม่ใช่แค่ “จำสูตร”

7. **Post-Quantum Readiness** ปิดท้ายด้วยแนวคิด KEM/DSA หลังควอนตัม และ ไฮบริด-แฮนด์เชก (คลาสสิก+PQC) เพื่อ “คิดยาว” —โยงนโยบาย crypto-agility และการประเมินความเสี่ยงเชิงเวลา (ข้อมูลที่ต้องปกป้องนานหลายปี)

จุดเน้นของแก่นความคิดคือ *Primitives* → *Modes* → *Protocols* → *Systems* → *Governance* : สอนให้เห็นทุกชั้น และวัดผลด้วยหลักฐาน ซึ่งควรลงมือปฏิบัติจริงในแลป

3) แบบแผนสำหรับออกแบบ/ประเมินระบบ (Design Patterns & Anti-patterns)

ควรทำ (Patterns):

- AEAD-first (AES-GCM/ChaCha20-Poly1305), unique nonce, HKDF-based key schedule
- Forward secrecy + short-lived keys/tokens; key rotation และ crypto-agility
- Deterministic builds/constant-time libs; ใช้ verified libraries มากกว่า “เขียนเอง”
- Logging ที่เคารพ PDPA: เก็บเฉพาะเมตาเดตาที่จำเป็น, พิสัยเหตุการณ์การถอดรหัสแบบ *selective decryption* ในกรณีเสี่ยงสูง

ควรเลี่ยง (Anti-patterns):

- ฟังก์ชัน DES/2DES/3DES หรือ ECB/CBC-no-MAC ในงานใหม่ (สาคิตได้ในแล็บแต่ต้องตีกรอบ)
- Nonce reuse กับ CTR/GCM, TCP-over-TCP สำหรับชั้นเข้ารหัส, และการปะติดปะต่อ primitive ด้วยตนเองโดยไม่มี *proof/standard guidance*

เอกสารคำสอนบท “พื้นฐานวิทยาการรหัสลับ” เนื้อหาทั้งหมดได้ให้ฐานความรู้ที่แข็งแกร่งด้านนิยามองค์ประกอบ ประเภท และอัลกอริทึมหลัก และได้ต่อยอดด้วยแนวคิดร่วมสมัย AEAD-first, mode-aware, constant-time, key-lifecycle, protocol-integration และ crypto-agility/PQC-ready เพื่อยกระดับจาก “รู้จักสูตร” สู่ “ออกแบบ-พัฒนา-ตรวจสอบ-พิสูจน์” อย่างเป็นระบบในบริบทของวิชาชีพด้าน Cybersecurity

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่างการเข้ารหัสแบบกุญแจสมมาตรและกุญแจอสมมาตร

แนวคำตอบ: สมมาตรใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส (เช่น DES, AES) เร็วแต่มีปัญหาการกระจายกุญแจ อสมมาตรใช้กุญแจคู่ (Public/Private) เช่น RSA ปลอดภัยแต่ช้ากว่า

ข้อ 2. อธิบายหลักการทำงานของ AES และเหตุผลที่นิยมใช้แทน DES

แนวคำตอบ: AES ใช้ขนาดกุญแจ 128/192/256 บิต ปลอดภัยสูงกว่าการใช้ DES (56 บิต) ซึ่งถูกโจมตี Brute-force ได้ง่าย AES มีโครงสร้าง Substitution-Permutation ทำงานเป็นรอบ

ข้อ 3. อธิบายการทำงานของ Diffie-Hellman และปัญหา Man-in-the-Middle

แนวคำตอบ: Diffie-Hellman ใช้เลขเฉพาะ p และ g แลกเปลี่ยนกุญแจเพื่อสร้าง shared key ร่วมกัน ปัญหาคือ หากผู้โจมตีแทรกกลางการแลกเปลี่ยน จะทำให้กุญแจถูกดักได้

ข้อ 4. วิเคราะห์การโจมตีแบบ Brute-force ต่อ DES และเหตุผลที่ทำให้ DES ไม่ปลอดภัยแล้ว

แนวคำตอบ: DES ใช้กุญแจ 56 บิต ทำให้จำนวนความเป็นไปได้ 2^{56} ($\sim 7.2 \times 10^{16}$) ปัจจุบันคอมพิวเตอร์สามารถถอดได้ในเวลาไม่นาน $\rightarrow$ DES ล้าสมัย

ข้อ 5. อธิบายการทำงานของลายมือชื่อดิจิทัลและประโยชน์

แนวคำตอบ: ใช้ Hash function สร้าง message digest $\rightarrow$ เข้ารหัสด้วย Private Key ของผู้ส่ง $\rightarrow$ ผู้รับตรวจสอบด้วย Public Key $\rightarrow$ ประโยชน์: Authentication, Integrity, Non-repudiation

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. วิทยาการรหัสลับ (Cryptography) มีความหมายตรงกับข้อใด

- ก. การเขียนความลับ
- ข. การส่งข้อมูลแบบไร้สาย
- ค. การจัดการฐานข้อมูล

ง. การป้องกันไวรัส

เฉลย: ก

ข้อ 2. องค์ประกอบใดไม่ใช่ส่วนหนึ่งของระบบรหัสลับ (Cryptosystem)

ก. Plaintext

ข. Encryption Algorithm

ค. Firewall Policy

ง. Key

เฉลย: ค

ข้อ 3. การเข้ารหัสแบบ Stream Cipher คืออะไร

ก. การเข้ารหัสทีละบล็อก

ข. การเข้ารหัสทีละบิต

ค. การเข้ารหัสด้วย Public Key

ง. การเข้ารหัสแบบ Hashing

เฉลย: ข

ข้อ 4. ข้อใดเป็นตัวอย่างของ Symmetric Key Encryption

ก. RSA

ข. DES

ค. Diffie-Hellman

ง. Digital Signature

เฉลย: ข

ข้อ 5. ขั้นตอนวิธีเข้ารหัสลับใดเป็นมาตรฐานที่แทน DES

ก. AES

ข. L2TP

ค. SHA-1

ง. PPTP

เฉลย: ก

ข้อ 6. การเข้ารหัสแบบอสมมาตรใช้กุญแจอย่างไร

ก. ใช้กุญแจเดียวกันทั้งเข้ารหัสและถอดรหัส

ข. ใช้กุญแจคู่ Public/Private

ค. ใช้กุญแจสลับทุกครั้ง

ง. ใช้กุญแจ Hash แทนที่

เฉลย: ข

ข้อ 7. Diffie-Hellman มีปัญหาหลักใด

ก. การโจมตีแบบ Man-in-the-Middle

ข. การเข้ารหัสซ้ำ

ค. ใช้กุญแจมากเกินไป

ง. ไม่สามารถใช้บนอินเทอร์เน็ต

เฉลย: ก

ข้อ 8. การใช้ RSA ต้องอาศัยพื้นฐานทางคณิตศาสตร์ใด

ก. การแยกตัวประกอบจำนวนเฉพาะ

ข. การแทนที่อักขร

ค. การทำ Hash

ง. การสลับตำแหน่งข้อความ

เฉลย: ก

ข้อ 9. ลายมือชื่อดิจิทัลให้คุณสมบัติใด

ก. Authentication, Integrity, Non-repudiation

ข. Confidentiality, Availability, Accountability

ค. Confidentiality, Authorization, Integrity

ง. Availability, Hashing, Non-repudiation

เฉลย: ก

ข้อ 10. ฟังก์ชันใดเป็นตัวอย่างของ Hash Function

ก. AES

ข. MD5

ค. RSA

ง. DES

เฉลย: ข

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิริเชษฐ์ โพธิ์ศรีบุญ. (ม.ป.ป.). *พื้นฐานวิทยาการรหัสลับ (Cryptography Overview)*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Bernstein, D. J. (2005). Cache-timing attacks on AES. (manuscript).

IETF. (2018). RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3.

IETF. (2020). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.

Krawczyk, H., Eronen, P. (2010). HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869.

NIST. (2001). FIPS 197: Advanced Encryption Standard (AES).

NIST. (2007). SP 800-57: Recommendation for Key Management.

NIST. (2017). SP 800-38D: Recommendation for GCM and GMAC.

NIST. (2018). FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

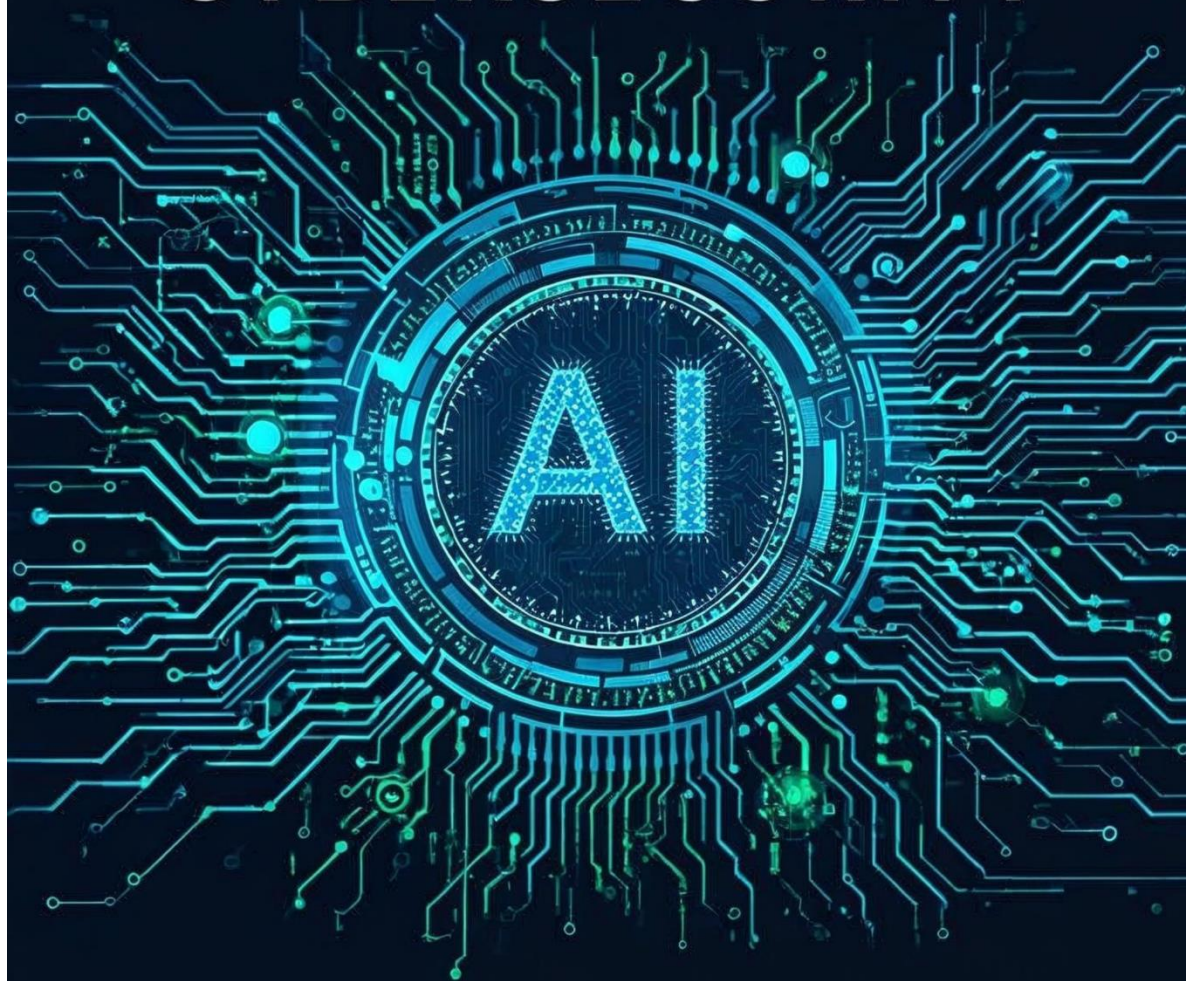
NIST. (2018). SP 800-56A Rev.3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.

NIST. (2024). Post-Quantum Cryptography (e.g., ML-KEM, ML-DSA) — standards and migration guidance.

บทที่ 8

วิศวกรรมเครือข่ายการสื่อสาร
Communications Networks

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์
CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์ศรีบุญ

บทที่ 8 วิศวกรรมเครือข่ายการสื่อสาร (Communications Networks Engineering)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบ นักศึกษาจะสามารถ:

- 1) รู้จักประเภทเครือข่ายทั้ง WAN, MAN, LAN, โสตต์และโหนด, เซิร์ฟเวอร์และไคลเอ็นต์
- 2) เข้าใจเครือข่ายเฉพาะที่และโทโปโลยีแต่ละชนิดของเครือข่าย
- 3) เข้าใจมาตรการรักษาความมั่นคงปลอดภัยเครือข่าย

2. วัตถุประสงค์เชิงพฤติกรรม

เมื่อสิ้นสุดการเรียนในสัปดาห์นี้ นักศึกษาจะสามารถ:

- 1) อธิบายความหมาย ประเภทเครือข่ายทั้ง WAN, MAN และ LAN ได้อย่างถูกต้อง
- 2) อธิบายประเภท ส่วนประกอบ และโทโปโลยีของแลนได้อย่างถูกต้อง
- 3) ประยุกต์ใช้มาตรการรักษาความมั่นคงปลอดภัยเครือข่ายทั้งด้านเทคนิค ด้านองค์กร และด้านกายภาพได้

3. หัวข้อเนื้อหา:

8.1 ประเภทเครือข่าย

- 8.1.1 เครือข่ายบริเวณกว้าง หรือแวน
- 8.1.2 เครือข่ายนครหลวง หรือแมน
- 8.1.3 เครือข่ายเฉพาะที่ หรือแลน
- 8.1.4 โสตต์และโหนด, เซิร์ฟเวอร์และไคลเอ็นต์

8.2 เครือข่ายเฉพาะที่ หรือแลน

8.2.1 ประเภทของแลน

8.2.2 ส่วนประกอบของแลน

8.2.3 โทโปโลยีของแลน

8.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย

8.3.1 มาตรการด้านเทคนิค

8.3.2 มาตรการด้านองค์กร

8.3.3 มาตรการด้านกายภาพ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา:

บริษัท RMUTT ThaiLogistics Corp. มีสาขาในหลายจังหวัดและต้องการเชื่อมต่อระบบคลังสินค้าเข้ากับสำนักงานใหญ่ผ่านเครือข่าย WAN ขณะเดียวกัน แต่ละสาขาก็มี LAN ภายใน และบางพื้นที่ในเขตเมืองใช้ MAN เพื่อเชื่อมต่อระหว่างศูนย์บริการ ลูกค้าย้องเรียนว่าบางครั้งการเข้าถึงระบบล่าช้าและเสี่ยงต่อการถูกบุกรุกจากเครือข่าย Wi-Fi ที่ไม่มีการป้องกัน

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

- วิเคราะห์ประเภทเครือข่ายที่บริษัทใช้งาน (WAN, MAN, LAN) และการทำงานร่วมกัน
- ระบุข้อดี-ข้อจำกัดของโทโปโลยี LAN ที่เลือกใช้ (Star, Ring, Bus, Mesh)
- เสนอแนวทางการปรับปรุงประสิทธิภาพและความปลอดภัย (เช่น Firewall, IDS/IPS, SD-WAN, Network Segmentation)
- สรุปผลการวิเคราะห์และนำเสนอในชั้นเรียน

ประเด็นการเรียนรู้ที่สำคัญ:

- ประเภทเครือข่าย WAN, MAN, LAN
- องค์ประกอบและโทโปโลยีของ LAN

- มาตรการรักษาความมั่นคงปลอดภัยเครือข่ายทั้งด้านเทคนิค องค์กร และกายภาพ
- แนวคิด Security by Design และการประยุกต์ใช้ SD-WAN

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ เครือข่าย (30)	ครอบคลุม WAN, MAN, LAN อย่างถูกต้อง	ครบเกือบทั้งหมด	ครอบคลุม บางส่วน	ไม่ถูกต้อง
การประเมินโทโปโลยี (20)	อธิบายข้อดี-ข้อเสียเชื่อมโยง กรณีศึกษา	ครอบคลุมแต่ยังไม่เชื่อมโยง	กล่าวบางส่วน	ไม่สอดคล้อง
การเสนอแนะ ทางแก้ไข (30)	เสนอหลายวิธี ครอบคลุมทั้ง เทคนิค/องค์กร	เสนอวิธีบางส่วน	เสนอไม่ชัดเจน	ไม่มีข้อเสนอ
การนำเสนอ (20)	ชัดเจน ใช้สื่อ/ผังเครือข่าย ประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

8. เครือข่ายการสื่อสาร (Communications Networks)

การสื่อสารทั้งมีสายและไร้สายอาจใช้ช่องทางสื่อสารแบบชนิดเดี่ยวๆ หรือผสมผสานในรูปของเครือข่าย (network) หรือเครือข่ายสื่อสาร (communication network) คือระบบของการเชื่อมต่อกันของคอมพิวเตอร์, โทรศัพท์ หรืออุปกรณ์สื่อสารอื่นๆ ที่สามารถติดต่อสื่อสารกับเครื่องอื่นๆ และสามารถแบ่งปันแอปพลิเคชันและข้อมูลร่วมกันได้ โดยมีการเชื่อมต่อเข้าด้วยกันของอุปกรณ์สื่อสารหลายชนิด

8.1 ประเภทเครือข่าย: เครือข่ายบริเวณกว้าง (WAN) และ เครือข่ายเฉพาะที่ (LAN)

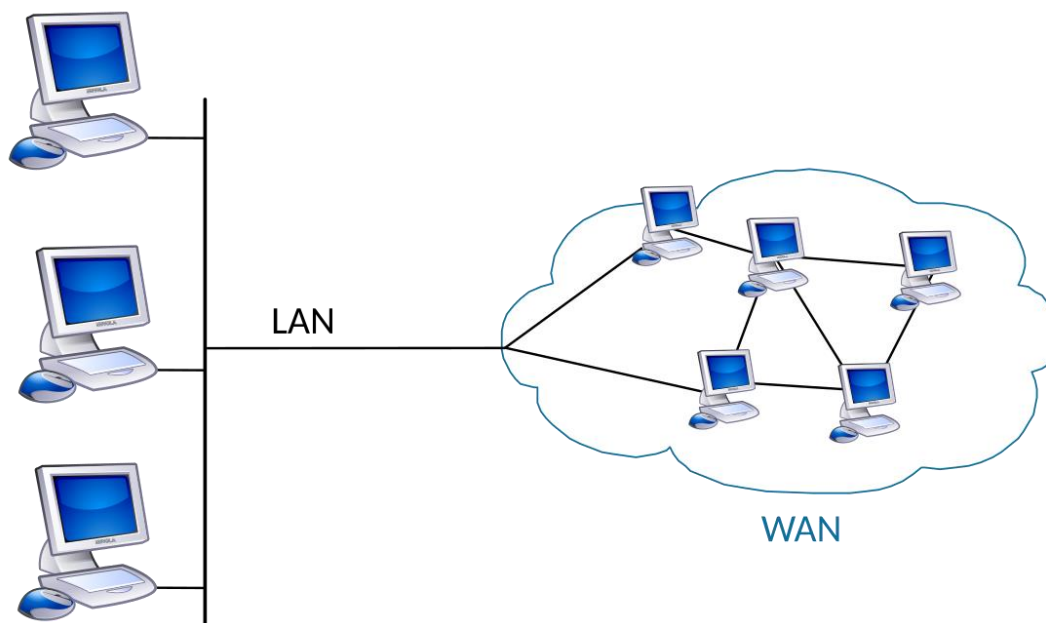
โดยทฤษฎีเครือข่าย เมื่อพิจารณาตามขนาด เครือข่ายแบ่งออกเป็น 3 ประเภท ประกอบด้วย เครือข่ายบริเวณกว้าง (WAN: Wide Area Network) เครือข่ายนครหลวง (MAN: Metropolitan Area Network) และ เครือข่ายเฉพาะที่ (LAN: Local Area Network) ในที่นี้จะมุ่งอธิบายเฉพาะ WAN และ LAN เป็นหลัก ซึ่งมีการประยุกต์ใช้งานจริงในประเทศไทย

8.1.1 เครือข่ายบริเวณกว้างหรือแวน (Wide Area Network: WAN)

8.1.1.1 WAN คืออะไร

ระบบเครือข่ายขนาดใหญ่เชื่อมต่อภายในและภายนอกองค์กร เครือข่ายคอมพิวเตอร์ที่ใช้สำหรับเชื่อมโยงกันในระยะทางที่ห่างไกลมากเป็นหลายๆ กิโลเมตร ซึ่งอาจใช้เชื่อมโยงระหว่างเมือง หรือระหว่างประเทศ ดังนั้น ความเร็วในการเชื่อมโยงระหว่างกันอาจไม่สูงมากนัก เพราะระยะทางไกลทำให้มีสัญญาณรบกวนได้สูง ความเร็วจึงอยู่ในระดับช่วง 9.6-64 Kbps และ 1.5-2 Mbps ขึ้นอยู่กับแอปพลิเคชันและขนาดของข้อมูล ผ่านสื่อที่เป็นตัวกลางรับ-ส่งข้อมูลเช่น สายเคเบิล หรือ ดาวเทียม เป็นต้น

เทคโนโลยีที่เชื่อมต่อสำนักงาน ศูนย์ข้อมูล แอปพลิเคชันบนระบบคลาวด์ และพื้นที่เก็บข้อมูลบนระบบคลาวด์เข้าด้วยกัน เราเรียกว่าเครือข่ายบริเวณกว้างเนื่องจากเครือข่ายนี้กินพื้นที่มากกว่าอาคารหนึ่งหลังหรือวิทยาเขตขนาดใหญ่ โดยครอบคลุมสถานที่หลายแห่งที่กระจายอยู่ทั่วพื้นที่ทางภูมิศาสตร์ที่เฉพาะเจาะจงหรือแม้แต่ทั่วโลก เช่น ธุรกิจที่มีสำนักงานในหลายประเทศจะใช้ WAN เพื่อเชื่อมต่อเครือข่ายของสำนักงานต่างๆ เข้าด้วยกัน WAN ที่ใหญ่ที่สุดในโลกคืออินเทอร์เน็ต เนื่องจากการรวบรวมเครือข่ายของนานาประเทศที่เชื่อมต่อถึงกัน เนื้อหาในบทนี้มุ่งเน้นไปที่ WAN ขององค์กร รวมถึงการใช้งานและประโยชน์ เพื่อจะนำไปสู่การประยุกต์ใช้งานในองค์กรและความตระหนักด้านความมั่นคงปลอดภัยของเครือข่าย รูป 8.1



รูป 8.1 เครือข่ายเฉพาะที่ (LAN) ที่มีการเชื่อมต่อกับเครือข่ายบริเวณกว้าง (WAN)

(ที่มา: https://en.wikipedia.org/wiki/Wide_area_network)

8.1.1.2 ประเภทของ WAN

WAN ต่างกับ LAN ตรงที่สามารถเชื่อมโยงได้ในระยะทางที่ไกลมากกว่า เครือข่าย WAN สามารถแบ่งเป็นประเภทใหญ่ๆ คือ

1) **เครือข่ายส่วนตัว** (Private Network: PN) เป็นการจัดตั้งระบบเครือข่ายซึ่งมีการใช้งานเฉพาะองค์กร เช่น องค์กรที่มีสาขาอาจทำการสร้างระบบเครือข่าย เพื่อเชื่อมต่อระหว่างสำนักงานใหญ่กับสาขาที่มีอยู่ เป็นต้น การจัดตั้งระบบเครือข่ายส่วนตัวมีจุดเด่นในเรื่องของการรักษาความลับของข้อมูล สามารถควบคุมดูแลเครือข่ายและขยายเครือข่ายไปยังจุดที่ต้องการ ส่วนข้อเสียคือในกรณีที่ไม่ได้มีการส่งข้อมูลต่อเนื่องตลอดเวลา จะเสียค่าใช้จ่ายสูงมากเมื่อเทียบกับการส่งข้อมูลผ่านเครือข่ายสาธารณะ และหากมีการส่งข้อมูลระหว่างสาขาต่างๆ จะต้องมีการจัดหาช่องทางสื่อสารเชื่อมโยงระหว่างแต่ละสาขาด้วย ซึ่งอาจจะไม่สามารถจัดช่องทางสื่อสารไปยังพื้นที่ที่ต้องการได้

2) **เครือข่ายสาธารณะ** (PDN: Public Data Network) หรือบางครั้งเรียกว่า**เครือข่ายมูลค่าเพิ่ม** (VAN: Value Added Network) เป็นเครือข่าย WAN ที่จะมียุติการภายนอก (Third Party) เป็นผู้ทำหน้าที่ในการเดินระบบเครือข่าย และให้เข้าช่องทางสื่อสารให้กับบริษัทต่างๆ ที่ต้องการสร้างระบบเครือข่าย

ซึ่งบริษัทจะลดค่าใช้จ่ายของตนลงได้ เนื่องจากมีบุคคลอื่นมาช่วยแบ่งปันค่าใช้จ่ายไป ซึ่งจะนิยมใช้กันมากเนื่องจากมีค่าใช้จ่ายต่ำกว่าการจัดตั้งเครือข่ายส่วนตัว สามารถใช้งานได้ทันทีโดยไม่ต้องเสียเวลาในการจัดตั้งเครือข่ายใหม่ รวมทั้งมีบริการให้เลือกอย่าง หลากหลาย ซึ่งแตกต่างกันไปทั้งในส่วนของราคา ความเร็ว ขอบเขตพื้นที่บริการ และความเหมาะสมกับงานแบบต่าง ๆ

8.1.1.3 โพรโทคอลและเทคโนโลยี WAN

โพรโทคอลเครือข่ายพื้นที่กว้างกำหนดโครงสร้างและกฎเกณฑ์ของการสื่อสาร โพรโทคอลเหล่านี้ช่วยให้แน่ใจว่าเครือข่ายถ่ายทอดข้อมูลอย่างมีประสิทธิภาพในพื้นที่ขนาดใหญ่ ตัวอย่างบางส่วนของโพรโทคอล WAN ได้แก่:

- **Multi-Protocol Label Switching (MPLS):** คือเทคโนโลยี WAN ที่ช่วยปรับปรุงความเร็วและประสิทธิภาพในการส่งข้อมูลผ่านเครือข่าย โดยจะเพิ่มป้ายกำกับที่กำหนดไว้ล่วงหน้าให้กับแต่ละแพ็กเก็ตข้อมูลที่ส่งผ่านเครือข่าย ซึ่งช่วยให้กำหนดเส้นทางข้อมูลได้เร็วขึ้นโดยไม่ต้องเสียเวลาในการค้นหา IP address แบบเดิมสำหรับแต่ละแพ็กเก็ต
- **Point-to-Point Protocol (PPP):** เป็นโพรโทคอลการเชื่อมต่อข้อมูลที่ใช้สร้างการเชื่อมต่อโดยตรงระหว่างโหนดเครือข่ายสองโหนด โดยทั่วไปจะใช้เพื่อเชื่อมต่อคอมพิวเตอร์กับอินเทอร์เน็ตผ่านการเชื่อมต่อแบบ dial-up แต่ยังสามารถใช้สำหรับการเชื่อมต่อแบบจุดต่อจุดประเภทอื่นได้ด้วย เช่น การเชื่อมต่อระหว่างเราเตอร์สองตัว
- **Frame Relay:** โพรโทคอลการสลับแพ็กเก็ตนี้ทำงานบนเลเยอร์ 1 และ 2 ของโมเดล OSI และใช้ในการเชื่อมต่อสถานที่ห่างไกลกับเครือข่ายส่วนกลาง เฟรมรีเลย์เป็นเทคโนโลยี WAN แบบเก่าที่รวมข้อมูลลงในเฟรมเพื่อส่งผ่านเครือข่ายเฟรมรีเลย์ที่ใช้ร่วมกัน
- **Integrated Services Digital Network (ISDN):** ISDN ใช้ในการส่งข้อมูลเสียง, ข้อมูล และวิดีโอผ่านเครือข่ายโทรศัพท์ดิจิทัล ซึ่งเป็นเทคโนโลยี WAN แบบเก่าที่ใช้กันทั่วไปสำหรับการประชุมทางวิดีโอความเร็วสูง, การประชุมทางโทรศัพท์ และการถ่ายโอนข้อมูลแบบเรียลไทม์
- **Packet over SONET/SDH (POS):** SONET (Synchronous Optical Network) และ SDH (Synchronous Digital Hierarchy) เป็นโพรโทคอลการสื่อสารความเร็วสูงที่พัฒนาขึ้นเพื่อรองรับการส่งสัญญาณเสียง, ข้อมูล และวิดีโอแบบดิจิทัลผ่านเครือข่ายใยแก้วนำแสง POS ช่วยให้สามารถสื่อสารผ่านลิงก์แบบจุดต่อจุดได้เมื่อใช้ใยแก้วนำแสง
- **Asynchronous Transfer Mode (ATM):** เป็นเทคนิคการสลับเซลล์แบบเก่าที่ช่วยส่งข้อมูลจำนวนมากด้วยความเร็วสูง และมักใช้โดยผู้ให้บริการอินเทอร์เน็ต (ISP) สำหรับเครือข่ายหลัก

เทคโนโลยีที่ซับซ้อนนี้ใช้การแบ่งเวลาแบบมัลติเพล็กซ์ที่แปลงสัญญาณดิจิทัลเป็นเซลล์ขนาดคงที่ 53 ไบต์ จากนั้นส่งและประกอบใหม่อีกครั้งที่ปลายทาง

- **Transmission Control Protocol/Internet Protocol (TCP/IP):** เทคโนโลยีนี้ประกอบด้วย Transmission Control Protocol (TCP) และ Internet Protocol (IP) ซึ่งทำงานร่วมกันเพื่อสร้างรากฐานของอินเทอร์เน็ต ถือเป็นโพรโทคอลสำคัญที่กำหนดการสื่อสารแบบครบวงจรโดยระบุว่าข้อมูลควรถูกแบ่งแพ็กเก็ต ระบุที่อยู่ ส่ง กำหนดเส้นทาง และรับสัญญาณอย่างไร
- **Packet Switching:** การสลับแพ็กเก็ตจะแบ่งข้อความออกเป็นแพ็กเก็ตที่ส่งโดยอิสระผ่านเส้นทางที่มีประสิทธิภาพ แพ็กเก็ตแต่ละแพ็กเก็ตจะประกอบด้วยข้อมูล (payload) และส่วนหัว (header) ที่ใช้ระบุตัวต้นแพ็กเก็ตจะถูกส่งเป็นสามชุดเพื่อตรวจสอบข้อผิดพลาด และแจ้งให้ส่งซ้ำเมื่อการตรวจสอบล้มเหลว

8.1.1.4 ประเภทการเชื่อมต่อ WAN

- **สายแบบเช่าใช้ (Leased Line)** สายแบบเช่าใช้คือการเชื่อมต่อเครือข่ายโดยตรงที่คุณสามารถเช่าจากผู้ให้บริการเครือข่ายขนาดใหญ่ เช่น ISP เพื่อเชื่อมต่อตำแหน่งข้อมูล LAN สองจุดเข้าด้วยกัน สายแบบเช่าใช้ไม่จำเป็นต้องเป็นสายจริงๆ โดยอาจเป็นการเชื่อมต่อแบบเสมือนจริงที่ผู้ให้บริการใช้กับโครงสร้างพื้นฐานเครือข่ายอื่นๆ
- **การสร้างอุโมงค์ส่วนตัวเสมือน** การสร้างอุโมงค์เป็นวิธีเข้ารหัสแพ็กเก็ตข้อมูลขณะที่ข้อมูลเดินทางผ่านอินเทอร์เน็ตสาธารณะ ในการสร้างอุโมงค์ จะใช้การเชื่อมต่ออินเทอร์เน็ตเพื่อเข้าถึงเซิร์ฟเวอร์ขององค์กรที่อยู่ในประเทศอื่น แต่จะส่งเป็นแพ็กเก็ตที่มีการห่อหุ้ม เป็นการสร้าง Virtual Private Network (VPN) ของเราเอง
- **Multiprotocol Label Switching Multiprotocol Label Switching (MPLS)** เป็นเทคนิคที่กำหนดเส้นทางการรับส่งข้อมูลตามป้ายกำกับที่กำหนดไว้ล่วงหน้า โดยจะพยายามกำหนดเส้นทางการรับส่งข้อมูลทั่วทั้งเส้นทางเครือข่ายที่สั้นกว่าหรือเร็วกว่า ซึ่งจะช่วยปรับปรุงประสิทธิภาพของเครือข่าย รูปแบบนี้จะทำงานอยู่ระหว่าง Open Systems Interconnection (OSI) เลเยอร์ที่ 2 และ 3 สามารถใช้เพื่อสร้างเครือข่ายแบบรวมในโครงสร้างพื้นฐานที่มีอยู่ เช่น IPv6, เฟรมรีเลย์, ATM หรืออีเธอร์เน็ต สามารถใช้สายแบบเช่าใช้ MPLS หรือใช้ MPLS กับ VPN เพื่อสร้างเครือข่ายที่มีประสิทธิภาพและปลอดภัย
- **WAN ที่กำหนดโดยซอฟต์แวร์** เครือข่ายบริเวณกว้างที่กำหนดโดยซอฟต์แวร์ (Software-Defined Wide-Area Network: SD-WAN) คือเทคโนโลยี MPLS ที่พัฒนาขึ้นมาอีกขั้น โดยจะ

แยกฟังก์ชัน MPLS ออกเป็นเลเยอร์ซอฟต์แวร์ เนื่องจาก SD-WAN ทำงานผ่านการเชื่อมต่ออินเทอร์เน็ตบรอดแบนด์ทั่วไป จึงมักช่วยลดค่าใช้จ่ายของเครือข่ายและให้ความยืดหยุ่นมากกว่าการเชื่อมต่อแบบคงที่

- **MPLS เทียบกับ SD-WAN** MPLS ทำให้การผสมผสานการทำงานกับระบบคลาวด์เข้าถึงได้ เนื่องจากมีการกำหนดเส้นทางรับส่งข้อมูลผ่านสำนักงานใหญ่ของบริษัท ซึ่งทำหน้าที่เป็นจุดควบคุมส่วนกลาง ในขณะที่ SD-WAN นั้นรับรู้ถึงระบบคลาวด์และผสมผสานการทำงานกับโครงสร้างพื้นฐานของระบบคลาวด์ที่ทันสมัยได้ดีกว่ามาก SD-WAN ยังประหยัดกว่าด้วย และมีประสิทธิภาพเหนือกว่า MPLS จึงสามารถใช้แบนวิธที่ได้มีประสิทธิภาพมากกว่าสายแบบเช่าใช้ MPLS ที่มีราคาแพง

8.1.1.5 การประยุกต์ใช้งาน WAN อย่างมีประสิทธิภาพและความปลอดภัย

แนวทางปฏิบัติที่สำคัญสำหรับการนำ WAN ไปใช้งานที่สามารถจัดการภายในองค์กรได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัย เป็นการรวบรวมเทคนิคที่จะปรับปรุงเมตริกประสิทธิภาพการทำงานของ WAN เช่น อัตราการโอนถ่ายข้อมูล ความหนาแน่น และเวลาแฝง การออกแบบของ WAN ตัวเลือกเทคโนโลยี และการจัดการทิศทางการรับส่งข้อมูลล้วนมีผลต่อประสิทธิภาพการทำงานของ WAN ตัวอย่างเทคนิคทั่วไปสำหรับการเพิ่มประสิทธิภาพ WAN ที่องค์กรยังสามารถธำรงไว้ซึ่งการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของเครือข่าย มีดังนี้

- **การจัดการทิศทางการรับส่งข้อมูล** การจัดการทิศทางการรับส่งข้อมูลรวมถึงเทคนิคที่ลดปริมาณข้อมูลที่ส่งผ่านเครือข่าย ตัวอย่างเช่น การแคชมักจะเก็บข้อมูลไว้ในเซิร์ฟเวอร์ท้องถิ่น การระบุและกำจัดสำเนาข้อมูลซ้ำซ้อนสำหรับการสำรองข้อมูลและกระบวนการกู้คืนจากความเสียหาย การบีบอัดหรือการชิปไฟล์ข้อมูล เป็นต้น
- **การเร่งโปรโตคอล** โปรโตคอล WAN บางอย่างมีการรับส่งข้อมูลจำนวนมาก กล่าวคือต้องใช้การสื่อสารข้อมูลกลับไปกลับมาจำนวนมากสำหรับคำขอเดียว ตัวอย่างเช่น ทั้งเซิร์ฟเวอร์และไคลเอนต์อาจส่งข้อมูลตอบรับกลับไปเพื่อยืนยันว่าได้รับข้อมูลแล้ว การเร่งโปรโตคอลจะรวมการสื่อสารของโปรโตคอลที่มีการรับส่งข้อมูลจำนวนมาก เพื่อลดจำนวนแพ็กเก็ตข้อมูลบนเครือข่าย
- **อัตราและขีดจำกัดการเชื่อมต่อ** ผู้ดูแลเครือข่ายสามารถจำกัดจำนวนลิงก์การเข้าถึงอินเทอร์เน็ตที่เปิดอยู่ จำนวนผู้ใช้ และจำนวนแบนวิธที่ผู้ใช้แต่ละคนสามารถเข้าถึงได้ในแต่ละครั้ง ตัวอย่างเช่น สามารถตั้งกฎเพื่อป้องกันไม่ให้พนักงานสตรีมวิดีโอบน WAN ขององค์กรได้

- **การแบ่งเซกเมนต์เครือข่าย** การกำหนดรูปแบบการรับส่งข้อมูลจะควบคุมทิศทางของข้อมูลสำหรับแอปพลิเคชันเฉพาะ ซึ่งจะแบ่งแบนด์วิธเครือข่ายระหว่างแอปพลิเคชันต่างๆ อย่างเหมาะสม ผู้ให้บริการเครือข่ายสามารถเลือกจัดลำดับความสำคัญของแอปพลิเคชันที่สำคัญเพื่อปรับปรุงประสิทธิภาพได้
- **การเชื่อมต่อแบบไร้สาย** รองรับระบบไร้สายสำหรับงานไฮบริดและ IoT ด้วยจุดเชื่อมต่อเชิงกลยุทธ์และการจัดการบนคลาวด์
- **สถาปัตยกรรม "Hardware-lite"** เลือกใช้ส่วนประกอบที่ใช้ซอฟต์แวร์เพื่อลดความซับซ้อนของฮาร์ดแวร์และเพิ่มความยืดหยุ่น
- **เลือกผู้ให้บริการ WAN อย่างชาญฉลาด** ประเมินตัวเลือกเช่นซัพพลายเออร์ฮาร์ดแวร์ ผู้ให้บริการที่มีการจัดการเครือข่าย และผู้ให้บริการโทรคมนาคมตามทรัพยากรและความต้องการ
- **นำกลไกการป้องกันความล้มเหลวมาใช้** ตั้งค่าโครงสร้างพื้นฐานการสำรองข้อมูลด้วยเทคโนโลยีที่หลากหลายเพื่อลดระยะเวลาหยุดทำงานให้น้อยที่สุด
- **SD-WAN สำหรับเครือข่ายที่ไม่ขึ้นอยู่กับผู้ให้บริการ** ลดการพึ่งพาผู้ให้บริการลงอย่างค่อยเป็นค่อยไปด้วยเทคโนโลยี SD-WAN
- **กลยุทธ์ด้านความปลอดภัยที่ครอบคลุม** เสริมสร้างมาตรการรักษาความปลอดภัยและการควบคุมการเข้าถึงสำหรับสภาพแวดล้อม WAN
- **เทคโนโลยีการเพิ่มประสิทธิภาพ WAN** ใช้การบีบอัดข้อมูล, การจัดข้อมูลซ้ำซ้อน และเครื่องมือวิเคราะห์ Wi-Fi เพื่อประสิทธิภาพที่เพิ่มขึ้น
- **รองรับสภาพแวดล้อมแบบมัลติคลาวด์** จัดสรรแบนด์วิธอย่างมีประสิทธิภาพสำหรับแอปพลิเคชันคลาวด์ต่างๆ
- **สร้างความสมดุลระหว่าง Leased Lines และ SD-WAN** ใช้งาน Leased lines สำหรับแอปพลิเคชันที่สำคัญ และใช้ SD-WAN สำหรับแอปพลิเคชันอื่นๆ
- **ตรวจสอบและอัปเดตอย่างสม่ำเสมอ** อัปเดตโซลูชันและเทคโนโลยีเครือข่ายพื้นที่กว้างที่เกิดขึ้นใหม่ เพื่อการนำไปใช้ในการปรับปรุงประสิทธิภาพ

8.1.2 เครือข่ายนครหลวงหรือแมน (MAN: Metropolitan Area Network)

เครือข่ายนครหลวง หรือแมน (MAN: metropolitan area network) คือเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อผู้ใช้กับทรัพยากรคอมพิวเตอร์ในพื้นที่ทางภูมิศาสตร์ที่มีขนาดเท่ากับเขตเมืองคำว่า MAN หมายถึงการเชื่อมต่อเครือข่ายท้องถิ่น (LAN) ในเมืองหนึ่งเข้าด้วยกันเป็นเครือข่ายขนาดใหญ่ ซึ่งอาจเชื่อมต่อไปยังเครือข่ายพื้นที่กว้าง ได้อย่างมีประสิทธิภาพ คำนี้ยังใช้เพื่ออธิบายการเชื่อมต่อ LAN หลายเครือข่ายในเขตเมืองโดยใช้การเชื่อมต่อแบบจุดต่อจุดระหว่างเครือข่ายเหล่านั้น แมนเป็นเครือข่ายสื่อสารที่ครอบคลุมพื้นที่เชิงภูมิศาสตร์ในระดับเมืองหรือเมืองขนาดเล็กรอบนอก วัตถุประสงค์ของแมนมักมีไว้เพื่อหลีกเลี่ยงบริษัทโทรศัพท์ท้องถิ่นเมื่อมีการเข้าถึงบริการในระยะไกล เช่น เครือข่ายมหาวิทยาลัยที่เชื่อมโยงเครือข่ายของมหาวิทยาลัยเข้ากับวิทยาเขตต่างๆ ระบบโทรศัพท์แบบเซลลูลาร์ส่วนใหญ่มักใช้แมน

ระบบโครงสร้างพื้นฐานโดยปกติแล้วจะเป็นระบบไร้สายเช่นการใช้คลื่นไมโครเวฟหรือใช้ใยแก้วนำแสงเป็นตัวเชื่อมต่อระหว่างสถานที่ต่างๆเข้าด้วยกัน ตัวอย่างการใช้งานจริง เช่น ภายในมหาวิทยาลัยหรือในสถานศึกษา จะมีระบบแมนเพื่อเชื่อมต่อระบบแลนของแต่ละคณะวิชาเข้าด้วยกันเป็นเครือข่ายเดียวกันในวงกว้าง เทคโนโลยีที่ใช้ในเครือข่ายแมนได้แก่ ATM, FDDI และ SMDS ระบบเครือข่ายแมนที่จะเกิดในอนาคตอันใกล้ คือระบบที่จะเชื่อมต่อคอมพิวเตอร์ภายในเมืองเข้าด้วยกันโดยผ่านเทคโนโลยี Wi-MAX

8.1.3 เครือข่ายเฉพาะที่ หรือแลน (LAN: Local Area Network)

เป็นเครือข่ายสื่อสารระยะใกล้เฉพาะบริเวณที่ใช้ครอบคลุมเฉพาะพื้นที่ภายในบริเวณเดียวกัน มีระยะทางไม่เกินหนึ่งไมล์ โดยอาจเชื่อมต่อภายในสำนักงาน, ตึกเดียวกัน, หรือหลายอาคารในกลุ่มเดียวกัน อย่างเช่นเครือข่ายของแต่ละวิทยาเขต มี 2 ชนิด ได้แก่ การแลกเปลี่ยนสาขาส่วนตัว (PBXs: private branch exchanges) และเครือข่ายเฉพาะที่ (LANs: local area network)

เครือข่ายเหล่านั้น ล้วนมีส่วนประกอบที่ผสมผสานกันของคอมพิวเตอร์, อุปกรณ์หน่วยเก็บ และอุปกรณ์สื่อสารประเภทต่างๆ หลากหลายชนิด

8.1.4 โฮสต์และโหนด, เซิร์ฟเวอร์และไคลเอ็นต์ (Hosts & Nodes, Servers & Clients)

หลายเครือข่ายโดยเฉพาะเครือข่ายขนาดใหญ่จะมีสนับสนุนโดยโฮสต์ โฮสต์คอมพิวเตอร์ (host computer) มักเรียกสั้นๆว่า โฮสต์ (host) หมายถึงเครื่องแม่ข่าย เป็นคอมพิวเตอร์หลักหรือศูนย์กลางคอยควบคุมเครือข่าย ส่วนโหนด (node) คืออุปกรณ์ใดๆ ที่เชื่อมต่อเข้ากับเครือข่าย

บนเครือข่ายเฉพาะที่หน้าที่บางอย่างจะถูกกระทำโดยเครื่องเซิร์ฟเวอร์ เซิร์ฟเวอร์ (server) หรือ เซิร์ฟเวอร์ของเครือข่าย (network server) บางทีเรียกว่าเครื่องแม่ข่ายหรือเครื่องผู้ให้บริการ เป็นคอมพิวเตอร์ ศูนย์กลางที่ทำหน้าที่เก็บฐานข้อมูลและโปรแกรมไว้สนับสนุนเครื่องพีซี, สถานีงานหรือเทอร์มินัลทั้งหมดที่เรียกว่า ไคลเอ็นต์ (clients) หรือเครื่องผู้ขอใช้บริการ บรรดาเครื่องไคลเอ็นต์เหล่านี้คือโหนดถูกเชื่อมต่อเข้ากับเครือข่าย ผ่านสายสื่อสารหรือไร้สายก็ได้ และเครือข่ายทั้งหมดนี้เรียกว่า เครือข่ายแบบไคลเอ็นต์/เซิร์ฟเวอร์ (client/server) โปรแกรมประยุกต์และแฟ้มที่ถูกเก็บไว้ที่เครื่องเซิร์ฟเวอร์จะถูกประจุไปยังหน่วยความจำของเครื่องไคลเอ็นต์เมื่อต้องการใช้งาน

ขนาดของเครือข่ายมีหลายขนาด โดยอาจประกอบด้วยเครื่องพีซีราคาสองหมื่นบาทไปจนถึงเครื่อง เมนเฟรมหรือระดับซูเปอร์คอมพิวเตอร์ราคาหลายร้อยล้านบาท

8.1.5 ข้อดีของเครือข่าย

เครือข่ายคอมพิวเตอร์ทุกประเภทไม่ว่าจะเป็นแวน, แมน หรือแลน มีข้อดีมากมาย โดยเฉพาะอย่างยิ่ง เครือข่ายแบบแลน ในด้านต่างๆ เช่น การแบ่งปันการใช้ทรัพยากรชนิดต่างๆ ร่วมกัน, ระบบการสื่อสารที่ดี, ความปลอดภัยที่รัดกุมของสารสนเทศ และการเข้าฐานข้อมูล ข้อดีต่างๆ สามารถสรุปได้ดังนี้

- การใช้อุปกรณ์รอบข้างร่วมกัน (sharing of peripheral devices) เครื่องพิมพ์ชนิดเลเซอร์สี, ดิสก์ไดรฟ์, สแกนเนอร์ ล้วนเป็นตัวอย่างของอุปกรณ์รอบข้างซึ่งเป็นฮาร์ดแวร์ที่ใช้พ่วงต่อเข้ากับคอมพิวเตอร์ อุปกรณ์เหล่านี้ มีราคาแพง เมื่อพ่วงต่อเข้ากับเครือข่ายคอมพิวเตอร์ย่อมสามารถถูกแบ่งปันการเรียกใช้งานจากเครื่องใดๆ ณ จุดใดๆ ก็ได้จากผู้ใช้งานจำนวนมากในเครือข่าย
- การใช้โปรแกรมและข้อมูลร่วมกัน (sharing of programs and data) ในองค์กรทุกระดับโดยเฉพาะขนาดใหญ่ จะมีผู้ใช้งานจำนวนมากที่มีความจำเป็นต้องใช้ซอฟต์แวร์และสารสนเทศอย่างเดียวกัน อย่างเช่น ซอฟต์แวร์ประยุกต์ ด้านเอกสาร, ตารางคำนวณ, การนำเสนองาน เป็นต้น การจัดซื้อซอฟต์แวร์เหล่านั้นสำหรับผู้ใช้งานคนย่อมมี ค่าใช้จ่ายสูง มีความสิ้นเปลืองทั้งค่าใช้จ่ายในการจัดหาซอฟต์แวร์และอุปกรณ์หน่วยเก็บ

ในองค์กรที่มีนโยบายให้พนักงานสามารถจัดเก็บและเรียกใช้ข้อมูลจากหน่วยเก็บเดียวกัน สามารถจัดซื้อ ซอฟต์แวร์เหล่านั้นในรุ่นสำหรับเครือข่าย นอกจากจะมีข้อดีด้านค่าใช้จ่ายต่ำกว่าซื้อทั้งชุดแบบปกติแล้ว ยัง สะดวกต่อการจัดการด้านความสอดคล้องกันของรุ่นของซอฟต์แวร์ที่ใช้สำหรับผู้ใช้งานทั้งหมด, สะดวกต่อการติดตั้ง, และสะดวกต่อการแก้ไขปัญหาหรือข้อบกพร่องที่เกิดจากซอฟต์แวร์ของเครื่องใดๆ

ประการสุดท้าย พนักงานที่เชื่อมโยงเข้ากับเครือข่าย ยังสะดวกต่อการทำงานร่วมกันแบบออนไลน์เกี่ยวกับ โครงการขนาดใหญ่ โดยอาศัยซอฟต์แวร์ประเภทกรุปแวร์ (groupware) เข้ามาช่วย

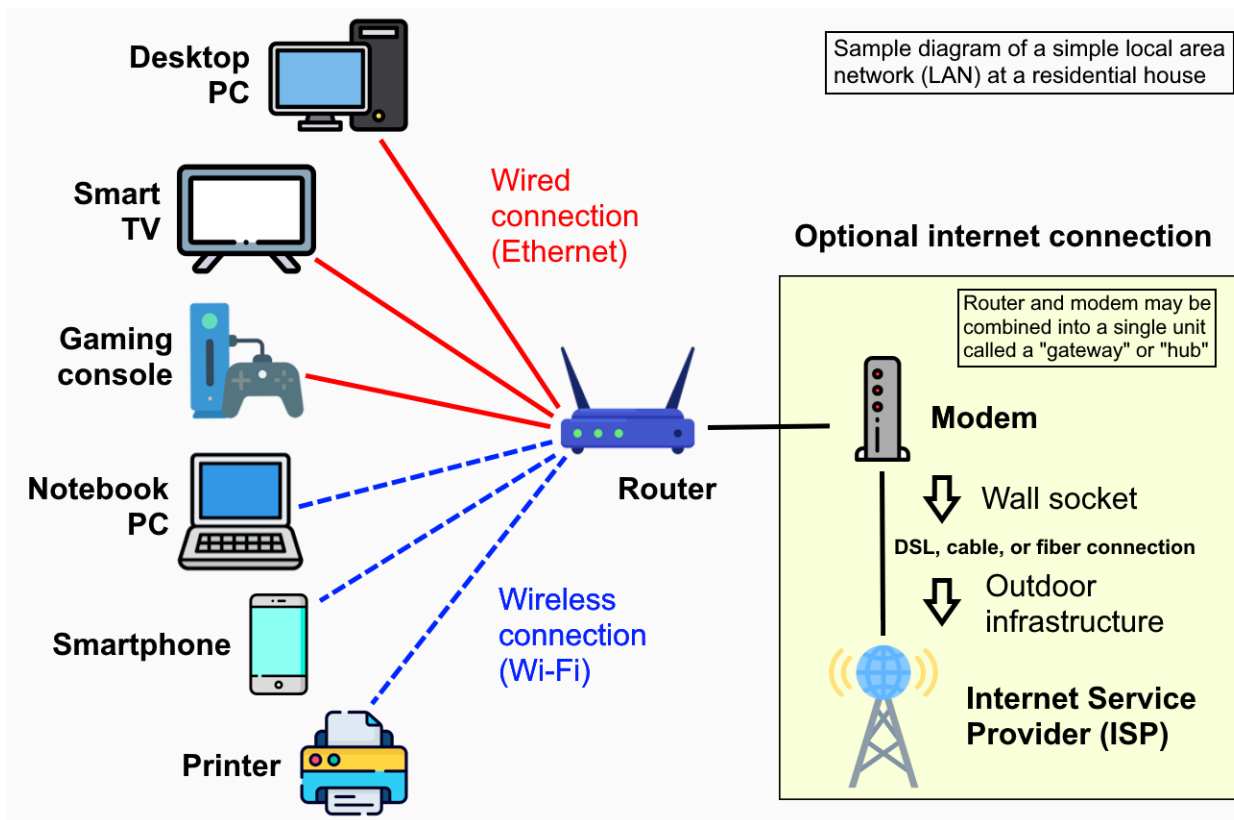
- การสื่อสารที่ดี (better communication) คุณสมบัติที่ดีอีกประการหนึ่งของเครือข่ายคืออิเล็กทรอนิกส์เมลล์หรืออีเมล ด้วยอีเมล ทำให้ทุกคนบนเครือข่ายสามารถแลกเปลี่ยนสื่อสาร, เก็บรักษา และแสดงเกี่ยวกับสารสนเทศที่มีความสำคัญได้โดยสะดวก ดังนั้น บริษัทจึงสามารถลดปัญหาเกี่ยวกับความล่าช้าที่อาจเกิดจากขั้นตอนการทำงานแบบปกติ, รูปแบบจดหมายมาตรฐานในการติดต่อกันกับหน่วยงานภายนอก และโทรศัพท์ไม่ว่าจะหมดไป
- ความปลอดภัยของสารสนเทศ (security of information) ก่อนที่เครือข่ายจะเข้ามาแทนที่การทำงานแบบเดิม พนักงานคนหนึ่งๆ จะทำการเก็บรักษาข้อมูลที่สำคัญไว้เอง เช่นอาจในตู้หรือโต๊ะแล้วติดกุญแจ หากเกิดกรณีที่พนักงานคนนั้นไม่อยู่, อุบัติเหตุไฟไหม้, น้ำท่วมสำนักงาน อาจไม่มีใครสามารถรู้ข้อมูลสำคัญนั้น แต่ปัจจุบันที่เครือข่ายเข้ามาแทนที่ ข้อมูลสำคัญของบริษัทจะถูกเก็บรักษาและสำรองไว้ตลอดเวลา การเรียกคืนข้อมูลที่เสียหายจากอุบัติเหตุเหล่านั้นสามารถทำได้โดยง่าย
- การเข้าถึงฐานข้อมูล (access to database) เครือข่ายยังอำนวยความสะดวกให้ผู้ใช้งานเข้าถึงข้อมูลหรือสารสนเทศที่มีอยู่อย่างมากมายและหลากหลายจากแหล่งของฐานข้อมูลทั้งภายในบริษัทและภายนอกอย่างเช่นอินเทอร์เน็ต

8.2 เครือข่ายเฉพาะที่ หรือแลน (LAN: Local Area Network)

แลน เครือข่ายเฉพาะที่ คือ เครือข่ายคอมพิวเตอร์ที่เชื่อมต่อคอมพิวเตอร์เข้าด้วยกันภายในพื้นที่จำกัด เช่น ที่อยู่อาศัย วิทยาเขต หรืออาคารและมีอุปกรณ์เครือข่ายและการเชื่อมต่อภายในที่บริหารจัดการภายใน แลนอำนวยความสะดวกในการกระจายข้อมูลและการแบ่งปันอุปกรณ์เครือข่าย เช่น เครื่องพิมพ์

แลนแตกต่างจากเครือข่ายบริเวณกว้าง (WAN) ซึ่งไม่เพียงแต่ครอบคลุมระยะทางทางภูมิศาสตร์ที่กว้างกว่าเท่านั้น แต่ยังเกี่ยวข้องกับวงจรโทรคมนาคมเช่าหรือ ลิงก์ อินเทอร์เน็ต อีก ด้วย ความแตกต่างที่เด่นชัดกว่านั้นคืออินเทอร์เน็ตซึ่งเป็นระบบคอมพิวเตอร์ธุรกิจและคอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกันทั่วโลก

อินเทอร์เน็ตและWi-Fi เป็นสองเทคโนโลยีที่นิยมใช้มากที่สุดสำหรับเครือข่ายเฉพาะที่ เทคโนโลยีเครือข่ายในอดีต ได้แก่ ARCNET, Token Ring และ LocalTalk รูป 8.2



รูป 8.2 แผนภาพแนวคิดของ LAN ในบ้านพักอาศัย

(ที่มา: https://en.wikipedia.org/wiki/Local_area_network)

จากรูป 9.2 แผนภาพแนวคิดของ LAN ในบ้านพักอาศัย โดยในกรณีนี้ เราเตอร์จะทำหน้าที่เป็นจุดเชื่อมต่อไร้สายด้วย นอกจากนี้ ในตัวอย่างนี้ แรเงาด้วยสีเหลือง ยังแสดงการเชื่อมต่อเครือข่ายกับอินเทอร์เน็ตผ่านสายโทรศัพท์พื้นฐาน

เครือข่ายเหล่านั้น ล้วนมีส่วนประกอบที่ผสมผสานกันของคอมพิวเตอร์, อุปกรณ์หน่วยเก็บ และอุปกรณ์สื่อสารประเภทต่างๆ หลากหลายชนิด แม้เครือข่ายขนาดใหญ่จะมีประโยชน์มาก แต่หลายองค์กรก็ยังจำเป็นที่จะใช้เครือข่ายท้องถิ่นซึ่งอาจเป็นภายในบ้าน บริษัทเล็กๆ ที่เชื่อมโยงอุปกรณ์ต่างๆ เข้าด้วยกัน

8.2.1 ประเภทของแลน: ไคลเอ็นท์/เซิร์ฟเวอร์ และเพียร์-ทู-เพียร์

เครือข่ายเฉพาะที่มี 2 ประเภทหลักๆ ได้แก่ ไคลเอ็นท์/เซิร์ฟเวอร์ (client/server) และเพียร์-ทู-เพียร์ (peer-to-peer) มีลักษณะสำคัญดังนี้

1) แลนแบบไคลเอ็นท์/เซิร์ฟเวอร์ (client/server LANs) ประกอบด้วยเครื่องไมโครคอมพิวเตอร์ซึ่งทำหน้าที่เป็นผู้ร้องขอ เรียกว่า ไคลเอ็นท์ (client) หรือผู้ขอใช้บริการ หรือลูกข่าย และเครื่องที่ทำหน้าที่เป็นผู้

ให้บริการ เรียกว่าเซิร์ฟเวอร์ (server) หรือแม่ข่าย เครื่องแม่ข่ายจะเป็นคอมพิวเตอร์ที่มีสมรรถนะสูงทำหน้าที่จัดการอุปกรณ์ที่ใช้ร่วมกัน เช่น เครื่องพิมพ์ แฟ้ม เป็นต้น

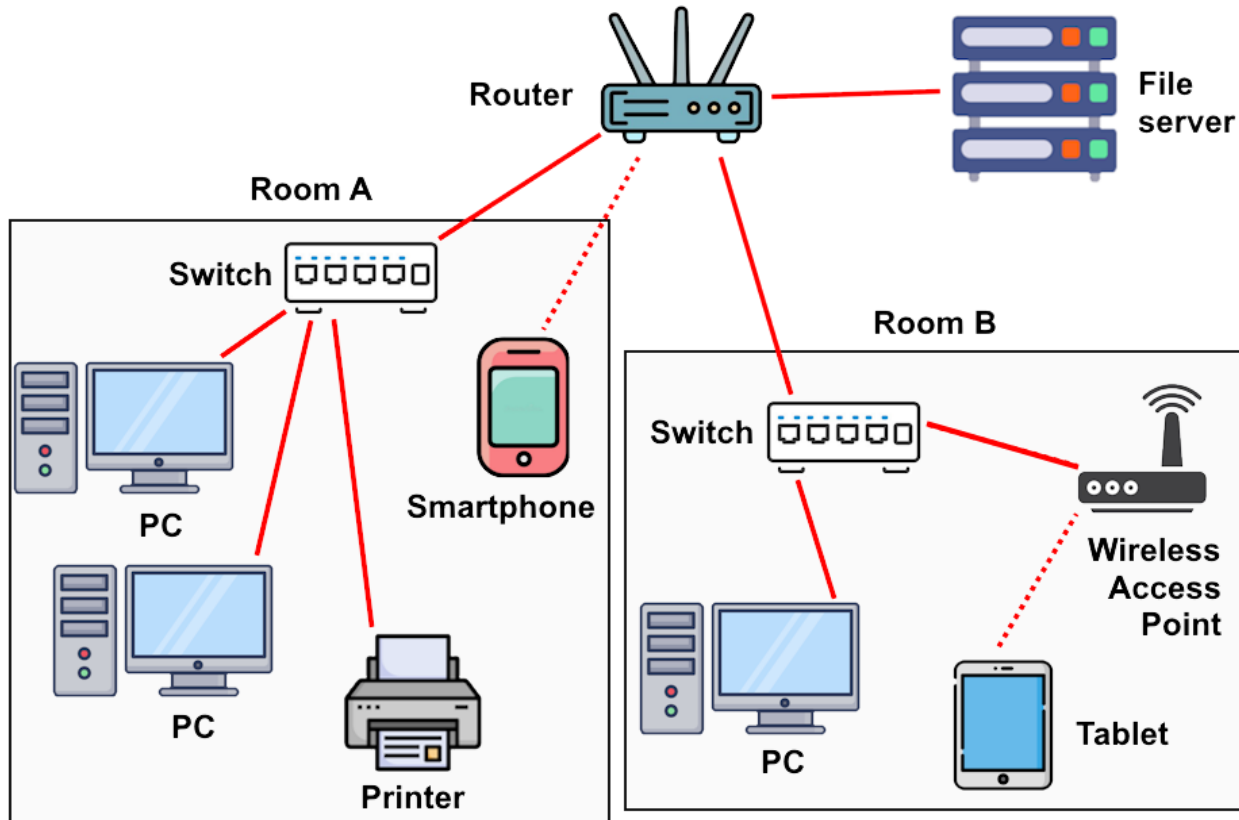
เครือข่ายแบบไคลเอ็นท์/เซิร์ฟเวอร์จะดำเนินภายใต้ระบบปฏิบัติการเครือข่าย เช่น เน็ตแวร์ (Novell's NetWare) วินโดวส์เอ็นที (Windows NT) หรือวินโดวส์เซิร์ฟเวอร์ (Windows Server) บางส่วนของระบบปฏิบัติการเครือข่ายจะถูกฝังที่เครื่องไคลเอ็นท์ บางส่วนจะฝังไว้ที่เซิร์ฟเวอร์ ระบบปฏิบัติการเครือข่ายจะอนุญาตให้ฮาร์ดดิสก์ไดรฟ์บนเซิร์ฟเวอร์สามารถถูกเข้าถึงได้จากเครื่องไคลเอ็นท์

แม่ข่ายมีหลายชนิดขึ้นอยู่กับภารกิจที่ให้บริการ เช่น แฟ้มและโปรแกรม, ฐานข้อมูล, เครื่องพิมพ์, แอปพลิเคชัน เป็นต้น ไฟล์เซิร์ฟเวอร์ (file server) คือคอมพิวเตอร์ที่เก็บโปรแกรมและแฟ้มข้อมูลที่ถูกใช้ร่วมกันโดยผู้ใช้งานแลน โดยจะทำหน้าที่เสมือนเป็นหน่วยเก็บหรือดิสก์ไดรฟ์แต่อยู่ในระยะไกล

ดาตาเบสเซิร์ฟเวอร์ (database server) คือคอมพิวเตอร์ในแลนที่จัดเก็บข้อมูล แต่ไม่เหมือนไฟล์เซิร์ฟเวอร์เพราะไม่ได้เก็บโปรแกรม, พรินท์เซิร์ฟเวอร์ (print server) คือคอมพิวเตอร์ที่ควบคุมเครื่องพิมพ์เครื่องเดียวหรือหลายเครื่อง ทำหน้าที่เก็บผลลัพธ์ที่ถูกส่งพิมพ์จากไคลเอ็นท์ในเครือข่ายแล้วจึงพิมพ์ผลออกมาทางเครื่องพิมพ์อีกทอดหนึ่งตามลำดับของงาน, แฟกซ์เซิร์ฟเวอร์ (fax server) ทำหน้าที่จัดการเกี่ยวกับการรับส่งแฟกซ์, และเมลเซิร์ฟเวอร์ (mail server) ทำหน้าที่จัดการอีเมล

2) **เพียร์-ทู-เพียร์ (peer-to-peer)** คำว่าเพียร์ (peer) แสดงถึงของสิ่งหนึ่งที่มีฐานะเท่าเทียมกับของสิ่งอื่น แลนแบบเพียร์-ทู-เพียร์ (peer-to-peer LAN) คือไมโครคอมพิวเตอร์เครื่องหนึ่งๆ สามารถติดต่อโดยตรงไปยังเครื่องอื่นๆ ได้ทุกเครื่องโดยไม่จำเป็นต้องอาศัยเซิร์ฟเวอร์ มีค่าใช้จ่ายต่ำกว่าแบบไคลเอ็นท์/เซิร์ฟเวอร์ แต่เหมาะสำหรับเครือข่ายขนาดเล็กที่สามารถทำงานได้อย่างมีประสิทธิภาพถ้าจำนวนเครื่องในเครือข่ายไม่เกิน 25 เครื่อง ถ้าเกินกว่านั้นจะทำให้เกิดความล่าช้าทั้งระบบ

แลนหลายแห่งอาจมีส่วนประกอบที่ผสมผสานได้ทั้งไคลเอ็นท์/เซิร์ฟเวอร์กับแบบเพียร์-ทู-เพียร์โมเดล



รูป 8.3 แผนภาพแนวคิดของระบบ LAN ในสำนักงานธุรกิจขนาดเล็ก

(ที่มา: https://en.wikipedia.org/wiki/Local_area_network)

จากรูป 9.3 ตัวอย่างนี้ประกอบด้วยห้องสองห้อง แต่ละห้องมีสวิตช์เซิร์ฟเวอร์ไฟล์และการเชื่อมต่อแบบมีสายและไร้สายแบบผสม นี่คือโทโพโลยีแบบดาว

8.2.2 ส่วนประกอบของแลน

เครือข่ายเฉพาะที่ถูกพัฒนามาจากส่วนประกอบมาตรฐานหลายชนิด ดังนี้

1) การเชื่อมต่อหรือระบบการติดตั้งสาย (connection or cabling) แลนไม่ใช่เครือข่ายสายโทรศัพท์ แต่ใช้ระบบการเชื่อมต่อหรือการติดตั้งสายสัญญาณอย่างอื่นแทน ซึ่งได้ทั้งระบบสายและไร้สาย ด้วยระบบสาย, แลนอาจใช้สายคู่ตีเกลียว, สายโคแอก หรือสายใยแก้วนำแสง ส่วนระบบไร้สาย, อาจใช้การส่งสัญญาณแบบอินฟราเรดหรือคลื่นวิทยุ เครือข่ายไร้สายจะเอื้อประโยชน์ถ้าการใช้งานคอมพิวเตอร์ที่มีการเคลื่อนย้ายบ่อยๆ เช่น เครื่องแบบพกพา

2) ไมโครคอมพิวเตอร์พร้อมการ์ดเครือข่าย (microcomputer with interface card) มีไมโครคอมพิวเตอร์มากกว่าสองเครื่องขึ้นไปซึ่งมีการ์ดเครือข่าย (NIC: network interface card) เสียบบลงในช่องสล็อตขยายเพื่อให้เครื่องเหล่านั้นสามารถรับและส่งข่าวสารระหว่างกันได้

3) ระบบปฏิบัติการเครือข่าย (NOS: network operating system) เป็นซอฟต์แวร์ระบบปฏิบัติการเครือข่ายทำหน้าที่บริหารจัดการกิจกรรมทั้งหมดที่เกิดในเครือข่าย ซอฟต์แวร์ดังกล่าวนั้นขึ้นอยู่กับชนิดของเครือข่าย บางชนิดจะถูกติดตั้งไว้ที่เครื่องโพล์เซิร์ฟเวอร์ บางชนิดติดตั้งไว้ที่เครื่องไมโครคอมพิวเตอร์บนเครือข่ายแต่ละเครื่อง หรือติดตั้งไว้ที่ทั้งคู่ ตัวอย่างของระบบปฏิบัติการเครือข่ายได้แก่ โนวอลล์เน็ตแวร์ (Novell's NetWare), ไมโครซอฟต์วินโดวส์เซิร์ฟเวอร์ (Microsoft Windows Server), และไอบีเอ็มแลนเมนเนเจอร์ (IBM's LAN Manager) ส่วนเครือข่ายแบบเพียร์-ทู-เพียร์ อย่างเช่นแอปเปิ้ลทอล์ค (AppleTalk), ไมโครซอฟต์วินโดวส์ (MS Windows) เป็นต้น

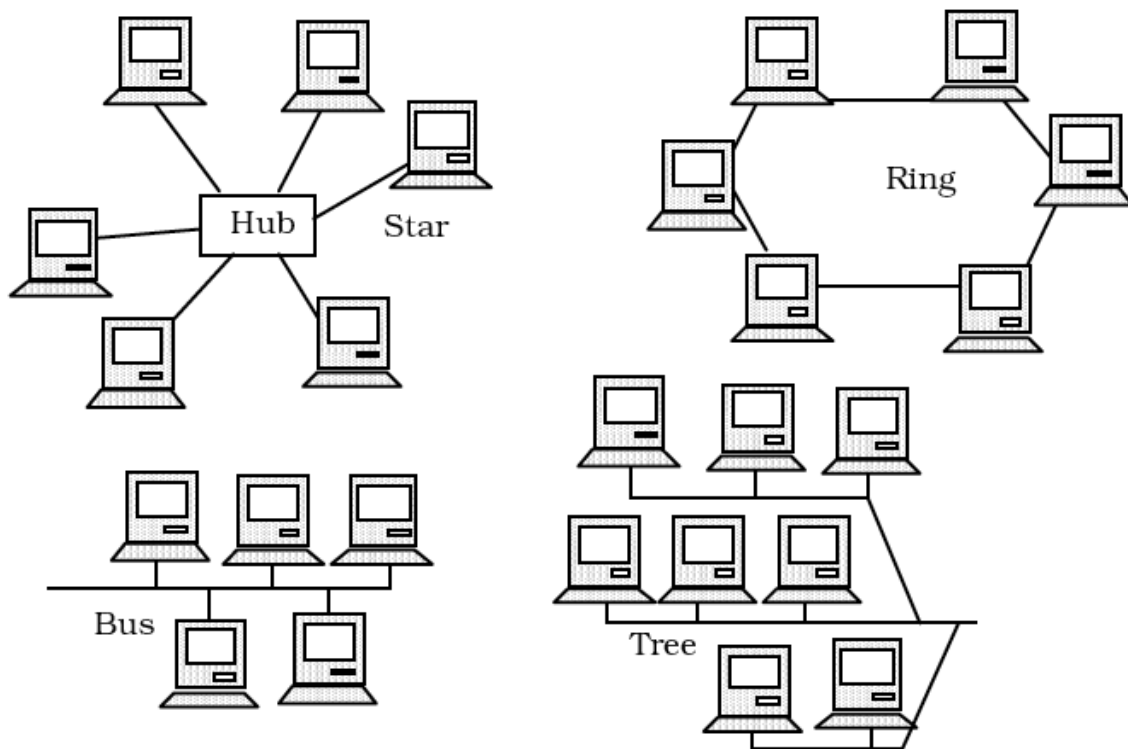
4) อุปกรณ์ที่ใช้ร่วมกันชนิดอื่นๆ (other shared devices) เครื่องพิมพ์, สแกนเนอร์, เครื่องแฟกซ์, อุปกรณ์หน่วยเก็บ, และอุปกรณ์อื่นๆ ที่จำเป็นต้องใช้จากผู้ใช้งานหลายคนในเครือข่าย

5) บริดจ์, เราเตอร์ และเกตเวย์ (bridges, routers and gateways) แล่นอาจอยู่เป็นวงเดี่ยวๆ หรืออาจเชื่อมต่อเข้ากับเครือข่ายวงอื่นอีกก็ได้ โดยที่เครือข่ายที่เชื่อมต่อนั้นอาจใช้เทคโนโลยีอย่างเดียวกันหรือต่างชนิดกันก็ได้ ดังนั้น ผู้ออกแบบเครือข่ายจำเป็นต้องพิจารณาทั้งซอฟต์แวร์, ฮาร์ดแวร์และอุปกรณ์ที่จำเป็นในการเชื่อมต่อเครือข่ายเข้าด้วยกัน ได้แก่ บริดจ์, เราเตอร์ และเกตเวย์

- บริดจ์ (bridges) เป็นได้ทั้งส่วนของฮาร์ดแวร์และซอฟต์แวร์ที่ใช้เชื่อมต่อเครือข่ายประเภทเดียวกันเข้าด้วยกัน
- เราเตอร์ (routers) อุปกรณ์จัดเส้นทาง เป็นอุปกรณ์คอมพิวเตอร์ชนิดพิเศษที่จัดการด้านข่าวสารที่สื่อสารกันโดยตรงจากเครือข่ายทุกชนิดเมื่อเครือข่ายเหล่านี้เชื่อมต่อกัน เราเตอร์ความเร็วสูงสามารถใช้สนับสนุนเส้นทางในเครือข่ายกระดูกสันหลังอินเทอร์เน็ต (the Internet backbone), คำนวณเส้นทาง, และควบคุมความแออัดของการจราจรในเครือข่าย
- เกตเวย์ (gateways) เป็นทั้งฮาร์ดแวร์และซอฟต์แวร์ที่ใช้ในการเชื่อมต่อกันของเครือข่ายหลายชนิดที่แตกต่างกันทั้งระบบปฏิบัติการเครือข่าย, โทโพลยีและโพรโทคอล เช่น การเชื่อมต่อระหว่าง แวน, แมน และแลน

8.2.3 โทโปโลยีของแลน (Topology of LAN)

โทโปโลยีแลนอธิบายถึงวิธีการจัดเรียงและสื่อสารอุปกรณ์ในเครือข่ายพื้นที่ท้องถิ่น (LAN) ครอบคลุมทั้งรูปแบบทางกายภาพ (เช่น สายเคเบิล) และการไหลของข้อมูลเชิงตรรกะ โทโปโลยีทั่วไปประกอบด้วยบัส (สายหลักเส้นเดียว), สตาร์ (อุปกรณ์เชื่อมต่อกับฮับกลาง), รিং (อุปกรณ์ในวงวนวงกลม) และเมช (อุปกรณ์ทั้งหมดเชื่อมต่อถึงกัน) การเลือกโทโปโลยีมีผลต่อประสิทธิภาพ ต้นทุน และความน่าเชื่อถือของเครือข่าย รูป 8.4 แสดงโทโปโลยีต่างๆ ของแลน



รูป 8.4 โทโปโลยีต่างๆ ที่อาจใช้ใน LAN แบบมีสายแบบรวมศูนย์: ดาว วงแหวน บัส และต้นไม้

(ที่มา: https://en.wikipedia.org/wiki/Local_area_network)

เราสามารถติดตั้งเครือข่ายได้หลายทาง โครงสร้างเชิงตรรกะหรือรูปทรงของเครือข่ายเรียกว่า โทโปโลยี (topology) ซึ่งมีโทโปโลยีพื้นฐานอยู่ 5 ชนิด ประกอบด้วย ดาว, วงแหวน, บัส, ผสม และ FDDI

- **เครือข่ายแบบดาว (star network)** จะมีไมโครคอมพิวเตอร์เครื่องหนึ่งทำหน้าที่เป็นเครื่องศูนย์กลางแม่ข่าย ไมโครคอมพิวเตอร์ที่เหลือและอุปกรณ์สื่อสารอื่นๆ ทั้งหมดจะเชื่อมต่อไปยังเครื่องแม่ข่ายโดยมีฮับ (hub) เป็นอุปกรณ์คอยจัดการรับส่งข่าวสารจากเครื่องหนึ่งๆ ไปสู่เครื่องอื่นๆ สายสื่อสารจะเชื่อมต่อจากไมโครคอมพิวเตอร์เข้าสู่ฮับแยกไปแต่ละเครื่อง สัญญาณอิเล็กทรอนิกส์จะถูกส่งผ่านจากเครื่องหนึ่งผ่านฮับไปยังเครื่องปลายทาง ฮับจะคอยตรวจสอบลำดับการจราจรที่วิ่งไปมาในเครือข่าย

เครือข่ายแบบดาว อ้างอิงมาตรฐาน IEEE 802.3 อีเธอร์เน็ต (Ethernet) เป็นกลุ่มงานและชุดมาตรฐานที่กำหนดการควบคุมการเข้าถึงสื่อ (MAC) ของเลเยอร์ทางกายภาพและเลเยอร์ลิงก์ข้อมูลของอีเธอร์เน็ต แบบใช้สายมาตรฐานเหล่านี้จัดทำโดยกลุ่มงานของสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) โดยทั่วไปชุดมาตรฐานนี้ใช้กับเครือข่ายท้องถิ่น (LAN) และมี แอปพลิเคชัน เครือข่ายพื้นที่กว้าง (WAN) การเชื่อมต่อทางกายภาพเกิดขึ้นระหว่างโหนดเครือข่ายและโดยปกติแล้วอุปกรณ์โครงสร้างพื้นฐานเครือข่ายต่างๆ (ฮับสวิตช์เราเตอร์) โดยใช้สายเคเบิลทองแดงหรือใยแก้วนำแสงหลายประเภท มาตรฐาน 802.3 รองรับสถาปัตยกรรมเครือข่าย IEEE 802.1 802.3 ยังกำหนดวิธีการเข้าถึง LAN โดยใช้การเข้าถึงหลายช่องทางแบบตรวจจับการชนกัน (CSMA/CD)

ข้อดีของเครือข่ายแบบดาวคือ ฮับจะทำหน้าที่คอยปกป้องการชนกันของข่าวสาร เมื่อเครื่องใดเครื่องหนึ่งเสียหายก็จะมีผลกระทบต่อเครื่องอื่นๆ ทั้งระบบ แต่ถ้าฮับเสียหายจะทำให้ทั้งระบบต้องหยุดชะงัก นอกจากนั้น โทโปโลยีแบบดาวนี้มีความสิ้นเปลืองสายสัญญาณมากกว่าโทโปโลยีแบบอื่นๆ

- **เครือข่ายแบบวงแหวน (ring network)** ไมโครคอมพิวเตอร์ทุกเครื่องจะสื่อสารกันภายในเครือข่ายผ่านสายสัญญาณที่มีลักษณะเป็นวงแหวน สัญญาณอิเล็กทรอนิกส์จะถูกส่งวิ่งไปรอบวงแหวนจนกระทั่งไปถึงยังเครื่องปลายทางโดยไม่จำเป็นต้องมีเครื่องเซิร์ฟเวอร์เป็นศูนย์กลาง ตัวอย่างของโทโปโลยีแบบวงแหวนที่ขึ้นชื่อที่สุดได้แก่ เครือข่ายโทเคนริงของไอบีเอ็ม (IBM's Token Ring) โดยมีโทเคนซึ่งเป็นบิตแบบมีแบบแผนจะวิ่งไปรอบๆ วงแหวนทำหน้าที่พิจารณาว่าเครื่องใดในเครือข่ายจะเป็นผู้ส่งสารเสนอ

มาตรฐาน IEEE 802.5 กำหนดเครือข่ายโทเคนริง เทคโนโลยี LAN ที่พัฒนาโดย IBM ซึ่งใช้โปรโทคอลการส่งโทเคนเพื่อให้การส่งข้อมูลมีความแน่นอนและยุติธรรม ในโทโปโลยีวงแหวนเชิงตรรกะนี้ สถานีต่างๆ จะได้รับ "โทเคน" หมุนเวียนเพื่อส่งข้อมูล ป้องกันการชนกันและรับรองว่าทุกโหนดมีโอกาสรับส่งข้อมูลเดิมที่เครือข่ายโทเคนริงใช้โทโปโลยีแบบดาวทางกายภาพพร้อมหน่วยการเข้าถึงหลายสถานี (Multistation Access Unit: MAU) ซึ่งรองรับความเร็ว 4 Mbps และ 16 Mbps

ลักษณะสำคัญ:

การส่งโทเคน: เฟรมสามไบต์พิเศษที่เรียกว่า "โทเคน" จะหมุนเวียนในวงแหวนลอจิก

ปราศจากการชนกัน: เฉพาะสถานีที่ถือโทเค็นเท่านั้นที่สามารถส่งข้อมูลได้ ซึ่งจะช่วยขจัดปัญหาการชนกันของข้อมูลที่เกิดขึ้นในเครือข่ายอีเทอร์เน็ต

การเข้าถึงแบบกำหนดแน่นอน: แต่ละสถานีรับประกันโอกาสในการส่งสัญญาณภายในระยะเวลาสูงสุดป้องกัน "การขาดสัญญาณ"

วงแหวนตรรกะ ดาวทางกายภาพ: ในขณะที่ข้อมูลไหลตามตรรกะในวงแหวน สถานีต่างๆ จะเชื่อมต่อทางกายภาพกับ MAU ส่วนกลาง ซึ่งมีลักษณะคล้ายกับโทโพโลยีแบบดาว

การกำหนดลำดับความสำคัญ: Token Ring มีคุณสมบัติสำหรับการกำหนดลำดับความสำคัญของสถานี ช่วยให้เซิร์ฟเวอร์ที่มีความต้องการลำดับความสำคัญสูงกว่าสามารถส่งข้อมูลได้บ่อยขึ้น

การไหลของข้อมูลแบบทิศทางเดียว: ข้อมูลและโทเค็นจะเคลื่อนที่ไปในทิศทางเดียวเท่านั้นรอบวงแหวน

ข้อดีของแบบวงแหวนก็คือ ข่าวสารจะเคลื่อนที่เป็นลำดับไปในทิศทางเดียว ขจัดปัญหาการชนกันของสัญญาณ แต่ข้อจำกัดของเครือข่ายวงแหวนก็คือ ถ้าเครื่องใดเครื่องหนึ่งในเครือข่ายเสียหาย อาจทำให้ทั้งระบบหยุดทำงานได้

แม้ว่า จะมีการใช้งานอย่างแพร่หลายในสภาพแวดล้อมองค์กร แต่โทเค็นริงก็ค่อยๆ ถูกแทนที่ด้วยอีเทอร์เน็ตเวอร์ชันใหม่ ซึ่งในที่สุดก็ให้ความเร็วที่สูงขึ้นมาตรฐานสุดท้ายที่เป็นทางการคือกิกะบิตโทเค็นริง (IEEE 802.5z)

- **เครือข่ายแบบบัส (bus network)** จะทำงานเหมือนกับรถบัสโดยสารประจำทางคอยวิ่งรับส่งผู้โดยสารจากจุดหนึ่งๆ ไปยังจุดหมายปลายทาง ในเครือข่ายแบบบัส จะไม่มีเครื่องเซิร์ฟเวอร์ศูนย์กลางคอยควบคุมจัดการ ทุกเครื่องในเครือข่ายจะเชื่อมต่อเข้ากับช่องสื่อสารเส้นเดียวกัน อุปกรณ์สื่อสารทั้งหมดในเครือข่ายสามารถสื่อสารส่งข่าวสารอิเล็กทรอนิกส์ถึงกันได้โดยไม่จำเป็นต้องมีเครื่องเซิร์ฟเวอร์ศูนย์กลาง ถ้ามีบางข่าวสารชนกัน อุปกรณ์ตัวนั้นจะหยุดชั่วขณะแล้วพยายามส่งใหม่ ตัวอย่างของเครือข่ายแบบบัสได้แก่อีเทอร์เน็ตของซีรอกซ์ (Xerox's Ethernet สามารถกำหนดให้ใช้โทโพโลยีแบบดาวได้)

ข้อดีของเครือข่ายแบบบัสก็คือ สามารถจัดการได้ทั้งเครือข่ายแบบโคลเอ็นท์/เซิร์ฟเวอร์ และแบบเพียร์-ทู-เพียร์ แต่มีข้อจำกัดคือจำเป็นต้องใช้วงจรสื่อสารและซอฟต์แวร์เข้ามาช่วยเพื่อหลีกเลี่ยงการชนกันของสัญญาณข้อมูล และถ้ามีอุปกรณ์เชื่อมต่อตัวใดตัวหนึ่งเสียหาย เช่นเมื่อเคลื่อนย้ายโต๊ะแล้วทำให้อุปกรณ์เชื่อมต่อเสียหายอาจส่งผลให้ทั้งระบบหยุดทำงานได้

โทเค็นบัสได้รับการกำหนดมาตรฐานโดยมาตรฐาน IEEE 802.4 โดยส่วนใหญ่ใช้สำหรับการใช้งานในภาคอุตสาหกรรม เจเนอรัลมอเตอร์ส์ ใช้โทเค็นบัส เพื่อรับประกันการหน่วงเวลาและการส่งข้อมูลของแพ็กเก็ตใน

โปรโตคอลโทเค็นบัส จึงมีการเสนอโทเค็นบัสที่ปรับเปลี่ยนแล้วในระบบอัตโนมัติการผลิตและระบบการผลิตแบบยืดหยุ่น (FMS) เพื่อเพิ่มประสิทธิภาพการเข้าถึงแบบกำหนดได้ที่จำเป็นสำหรับการสื่อสาร IoT แบบเรียลไทม์ในโรงงานผลิตแบบกระจายหรือ IIoT วิธีโทเค็นบัสยังสามารถนำไปใช้ตามมาตรฐาน IEEE 802.15.4 ได้อีกด้วย มีการพัฒนาวิธีการในการส่งโปรโตคอลอินเทอร์เน็ตผ่าน เครือข่าย IEEE 802 รวมถึงเครือข่ายโทเค็นบัส อย่างไรก็ตาม กลุ่มการทำงาน IEEE 802.4 ถูกยุบและมาตรฐานดังกล่าวถูกถอนออกโดย IEEE

- **เครือข่ายแบบผสม (hybrid network)** เป็นเครือข่ายที่ผสมผสานกันทั้งแบบดาว, วงแหวน และบัส ตัวอย่างเช่น ในวิทยาเขตขนาดเล็กที่มีหลายอาคาร เครือข่ายของแต่ละอาคารอาจใช้แบบบัสเชื่อมต่อกับอาคารอื่นๆ ที่ใช้แบบดาว และแบบวงแหวน
- **เครือข่ายแบบ FDDI (FDDI network)** เครือข่ายความเร็วสูงรุ่นใหม่เรียกว่า FDDI มาจากคำว่า Fiber Distributed Data Interface การเชื่อมต่อจะมีความเร็วประมาณ 100 – 200 เมกะบิตต่อวินาที เครือข่าย FDDI จะใช้สายใยแก้วนำแสงโดยแปลงจากโทโพโลยีแบบวงแหวน เพียงแต่มีวงแหวน 2 วง นิยมใช้สำหรับงานด้านที่ต้องการเทคโนโลยีสูงอย่างเช่นระบบภาพอิเล็กทรอนิกส์ (electronics imaging) กราฟิกความละเอียดสูง และวิดิทัศน์แบบดิจิทัล

ข้อดีประการหนึ่งของเครือข่าย FDDI คือความเร็วสูง มีเสถียรภาพ และความน่าเชื่อถือสูง เนื่องจากวงแหวนสื่อสารมีจำนวน 2 วงหากวงใดวงหนึ่งเสียหาย การสื่อสารยังสามารถดำเนินต่อไปได้ในวงแหวนที่เหลือ แต่ข้อจำกัดประการสำคัญคือ ค่าใช้จ่ายสูงอันเนื่องมาจากใช้วัสดุที่เป็นใยแก้วนำแสง, อุปกรณ์และการจัดการ เครือข่ายจะมีต้นทุนสูงกว่าโทโพโลยีแบบอื่นๆ โดยปกตินิยมใช้ FDDI เป็นกระดูกสันหลังของเครือข่ายหลัก ส่วนเครือข่ายที่เข้ามาเชื่อมต่ออาจผสมผสานได้ทั้งแบบดาว, วงแหวน และบัสได้

8.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย (Network Security)

คือ ระบบ มาตรการ และเทคนิคต่างๆ ที่ใช้ในการรักษาความปลอดภัยที่ครอบคลุมทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ เพื่อปกป้องโครงสร้างเครือข่าย และข้อมูลสำคัญขององค์กรจากการโจมตีทางไซเบอร์ทุกรูปแบบ ไม่ว่าจะเป็นการโจรกรรมข้อมูล เรียกค่าไถ่ หรือแทรกซึมเข้าสู่เครือข่ายคอมพิวเตอร์ เปรียบเสมือนเป็นเกราะป้องกันองค์กรและบุคคลจากภัยคุกคามทางไซเบอร์ ที่ยิ่งนับวัน ยังมีจำนวนและความรุนแรงมากขึ้น

หลักการพื้นฐานความมั่นคงปลอดภัยไซเบอร์ (The CIA Triad)

- การรักษาความลับ (Confidentiality):

ป้องกันการเข้าถึงและการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลสำคัญขององค์กรหรือข้อมูลส่วนบุคคลจะถูกเก็บเป็นความลับ

- **ความสมบูรณ์ (Integrity):**

ทำให้มั่นใจว่าข้อมูลจะไม่ถูกเปลี่ยนแปลง แก้ไข หรือทำลายโดยผู้ไม่ได้รับอนุญาต ซึ่งรวมถึงข้อมูลระหว่างการโอนย้ายและข้อมูลที่จัดเก็บ

- **ความพร้อมใช้งาน (Availability):**

รับประกันว่าผู้ใช้งานที่ได้รับอนุญาตจะสามารถเข้าถึงข้อมูลและบริการได้ตลอดเวลาที่ต้องการ



มาตรการและเทคนิคที่ใช้

- **การยืนยันตัวตน (Authentication) และการกำหนดสิทธิ์ (Authorization):**

กระบวนการตรวจสอบตัวตนของผู้ใช้งานก่อนให้สิทธิ์เข้าถึงระบบ และกำหนดสิทธิ์การใช้งานตามความจำเป็นเท่านั้น (Principle of Least Privilege)

- **การป้องกันการบุกรุก (Intrusion Prevention):**

การติดตั้งระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection/Prevention Systems - IDS/IPS) เพื่อระบุและหยุดยั้งกิจกรรมที่เป็นอันตราย

- **การเข้ารหัส (Encryption):**

การแปลงข้อมูลให้อยู่ในรูปแบบที่อ่านไม่ออก เพื่อปกป้องข้อมูลทั้งในขณะที่กำลังถูกส่งและในขณะจัดเก็บ

- **ไฟร์วอลล์ (Firewalls):**

ระบบที่ทำหน้าที่เป็นกำแพงกัน ระหว่างเครือข่ายภายในและภายนอก เพื่อควบคุมการเข้าออกของข้อมูลตามนโยบายที่กำหนด

- **การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ:**

การอัปเดตระบบปฏิบัติการและแอปพลิเคชันให้เป็นเวอร์ชันล่าสุด ช่วยปิดช่องโหว่ด้านความปลอดภัยที่อาจถูกใช้ในการโจมตี

- **การสำรองข้อมูล (Backup):**

การสำเนาข้อมูลอย่างสม่ำเสมอไปยังระบบอื่นหรือคลาวด์ เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่เกิดการสูญหายหรือถูกโจมตี

- **การแบ่งเครือข่าย (Network Segmentation):**

การแบ่งเครือข่ายออกเป็นส่วนย่อยๆ เพื่อจำกัดวงการแพร่กระจายของมัลแวร์หรือการโจมตีหากส่วนใดส่วนหนึ่งถูกบุกรุก

- **การสร้างตระหนักรู้ (Security Awareness):**

การให้ความรู้แก่ผู้ใช้งานเกี่ยวกับความเสี่ยงทางไซเบอร์และแนวทางปฏิบัติที่ปลอดภัย เช่น การใช้รหัสผ่านที่คาดเดายาก การไม่ดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ

มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย LAN

มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย LAN รวมถึงการติดตั้งและตั้งค่า ไฟร์วอลล์ (Firewall), ระบบตรวจจับการบุกรุก (IDPS), ซอฟต์แวร์ป้องกันมัลแวร์ (Anti-Malware), การบริหารจัดการ บัญชีผู้ใช้และรหัสผ่าน อย่างปลอดภัย, การอัปเดต ซอฟต์แวร์ให้ทันสมัย, การ จำกัดสิทธิ์การเข้าถึง, การสำรองข้อมูล, การตรวจสอบบันทึกการใช้งาน (Log) และการให้ความรู้แก่ผู้ใช้งานเกี่ยวกับภัยคุกคาม ประกอบด้วย มาตรการด้านเทคนิค มาตรการด้านองค์กร มาตรการด้านกายภาพ

มาตรการด้านเทคนิค

- **ติดตั้งและตั้งค่าอุปกรณ์รักษาความปลอดภัย:**

- **ไฟร์วอลล์ (Firewall):** ตั้งค่าให้เป็นด่านหน้าเพื่อควบคุมการเข้าถึงข้อมูลและทรัพยากรในเครือข่าย.
- **ระบบตรวจจับและป้องกันการบุกรุก (IDPS):** ติดตั้งเพื่อตรวจจับและป้องกันการโจมตีในเครือข่าย.
- **ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์:** ติดตั้งบนเครื่องคอมพิวเตอร์และเซิร์ฟเวอร์ทุกเครื่อง และอัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ.
- **บริหารจัดการการเข้าถึง:**
 - **ตั้งค่าบัญชีผู้ใช้และรหัสผ่าน:** กำหนดให้ผู้ใช้แต่ละคนมีบัญชีและรหัสผ่านที่แตกต่างกัน และเปลี่ยนแปลงรหัสผ่านอย่างสม่ำเสมอ รวมถึงบังคับใช้นโยบายรหัสผ่านที่ซับซ้อน.
 - **จำกัดสิทธิ์การเข้าถึง (Access Control):** กำหนดสิทธิ์การเข้าถึงข้อมูลและทรัพยากรต่างๆ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของแต่ละบุคคล.
- **การรักษาความปลอดภัยซอฟต์แวร์:**
 - **อัปเดตซอฟต์แวร์:** อัปเดตระบบปฏิบัติการ โปรแกรม และเว็บเบราว์เซอร์อย่างสม่ำเสมอเพื่อปิดช่องโหว่ที่อาจถูกโจมตีได้.
- **การตรวจสอบและบันทึก:**
 - **ตรวจสอบบันทึก (Log):** ตรวจสอบบันทึกการใช้งานระบบเครือข่ายเพื่อหากิจกรรมที่น่าสงสัย หรือการเข้าถึงโดยไม่ได้รับอนุญาต.

มาตรการด้านองค์กร

- **นโยบายความมั่นคงปลอดภัย:**

กำหนดนโยบายและแนวปฏิบัติที่ชัดเจนเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และสื่อสารให้ผู้ใช้งานทุกคนทราบและปฏิบัติตาม.
- **การจัดการภัยคุกคาม:**

มีแผนการตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น เช่น การติดไวรัส เพื่อให้ทีมงานสามารถดำเนินการได้อย่างรวดเร็ว.
- **การฝึกอบรมและให้ความรู้:**

จัดอบรมผู้ใช้งานเกี่ยวกับภัยคุกคามทางไซเบอร์ เช่น ฟิชซิง (Phishing) การเปิดไฟล์แนบที่น่าสงสัย หรือ การคลิกลิงก์ที่ไม่ควรไว้วางใจ.

- **การป้องกันการแพร่กระจายมัลแวร์:**

ผู้ใช้ควรระมัดระวังและแจ้งผู้ดูแลระบบทันที หากพบความผิดปกติที่อาจเกิดจากมัลแวร์ หรือหากพบว่า เครื่องคอมพิวเตอร์ติดไวรัส

มาตรการด้านกายภาพ

- **การควบคุมการเข้าถึงพื้นที่:**

- **จัดวางอุปกรณ์เครือข่ายในห้องที่ปลอดภัย:** ควรสอดแทรกในสถานที่ที่เข้าถึงได้ยาก และมีระบบรักษาความปลอดภัย เช่น กุญแจ หรือการล็อกอย่างแน่นหนา
- **ติดตั้งระบบกล้องวงจรปิด (CCTV):** เพื่อเฝ้าระวังและบันทึกเหตุการณ์บริเวณที่ตั้งของอุปกรณ์เครือข่าย
- **ใช้ระบบควบคุมการเข้า-ออก:** ติดตั้งระบบที่สามารถควบคุมการเข้าถึงพื้นที่ได้ เช่น ระบบสแกนใบหน้า (Face Recognition) หรือระบบอ่านแผ่นป้ายทะเบียน (LPR)
- **จำกัดการเข้าถึงของบุคลากร:** กำหนดเฉพาะบุคลากรที่ได้รับอนุญาตให้เข้าถึงพื้นที่อุปกรณ์เครือข่ายได้

- **การรักษาความปลอดภัยของอุปกรณ์:**

- **วางแผนผังเครือข่าย:** จัดทำผังเครือข่าย (Network Diagram) ที่แสดงรายละเอียดของอุปกรณ์ต่างๆ เพื่อให้ทราบตำแหน่งและข้อมูลการเชื่อมต่อ
- **ติดตั้งสัญญาณเตือนภัย:** อาจมีการติดตั้งอุปกรณ์เตือนภัยเมื่อมีการจัดแจงหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- **ตรวจสอบและซ่อมบำรุงอุปกรณ์สม่ำเสมอ:** เพื่อให้แน่ใจว่าอุปกรณ์ทำงานได้อย่างมีประสิทธิภาพ และไม่มีการชำรุดที่อาจนำไปสู่ความเสี่ยง

- **การเฝ้าระวัง:**

- **หมั่นตรวจสอบบริเวณที่ตั้งอุปกรณ์:** เพื่อให้มั่นใจว่าไม่มีการบุกรุกหรือการกระทำที่ผิดปกติใดๆ
- **สร้างความตระหนักรู้:** อบรมให้บุคลากรทราบถึงความเสี่ยงที่อาจเกิดขึ้น และให้ความสำคัญกับการรักษาความปลอดภัยทางกายภาพของอุปกรณ์

อย่างไรก็ตาม มาตรการรักษาความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์แบบแลนดังกล่าวข้างต้นเป็นเพียงมาตรการขั้นต้นที่ทุกองค์กรพึงปฏิบัติ ส่วนมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งระบบสายและระบบไร้สายจำเป็นต้องได้รับการกำหนดมาตรการมาตั้งแต่ขั้นตอนการออกแบบ เรียกว่า ความมั่นคงปลอดภัยโดยการออกแบบ (Security by Design) ความมั่นคงปลอดภัยโดยค่าปริยาย (Security by Default) ซึ่งจำเป็นต้องพิจารณาทั้งเครือข่ายมีสายและไร้สาย รวมทั้งการเชื่อมต่อเครือข่ายทั้งสองประเภทเข้าด้วยกัน ซึ่งจะมีรายละเอียดอยู่ในบทที่ว่าด้วย ความมั่นคงปลอดภัยของเครือข่ายไร้สาย และการออกแบบเครือข่ายเพื่อความมั่นคงปลอดภัย

8.4 สรุปบท

เนื้อหาในบทนี้กล่าวถึงมาตรการพื้นฐานในการรักษาความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์แบบแลนทั้งด้านการควบคุมการเข้าถึง การเฝ้าระวัง และการซ่อมบำรุงอุปกรณ์ พร้อมเน้นความสำคัญของการออกแบบระบบให้มีความมั่นคงปลอดภัยตั้งแต่ต้น ครอบคลุมทั้งเครือข่ายมีสายและไร้สาย โดยเชื่อมโยงองค์ความรู้ด้านวิศวกรรมเครือข่ายกับหลักการไซเบอร์ซีเคียวริตี้อย่างเป็นระบบ เพื่อให้เกิดการปกป้องข้อมูลและโครงสร้างพื้นฐานขององค์กรอย่างมีประสิทธิภาพ

8.5 บทวิเคราะห์และมุมมองเชิงวิชาการ: “วิศวกรรมเครือข่ายการสื่อสาร (Communications Networks Engineering)”

เอกสารคำสอนสัปดาห์ที่ 8 บทเรียน “วิศวกรรมเครือข่ายการสื่อสาร” เป็นหัวข้อสำคัญในรายวิชา *หลักการความมั่นคงปลอดภัยทางไซเบอร์* ที่มุ่งเน้นให้ผู้เรียนเข้าใจโครงสร้างพื้นฐานของเครือข่ายสื่อสาร ทั้ง WAN, MAN, LAN ตลอดจนมาตรฐานการด้านความมั่นคงปลอดภัยเชิงเทคนิค องค์กร และกายภาพ โดยมีเป้าหมายเพื่อเชื่อมโยงแนวคิดวิศวกรรมเครือข่ายกับหลักการไซเบอร์ซีเคียวริตี้ได้อย่างเป็นระบบ ซึ่งถือเป็นจุดเชื่อมต่อที่สำคัญระหว่างความรู้เชิงเทคนิคและการออกแบบสถาปัตยกรรมการรักษาความปลอดภัยสมัยใหม่ สรุปสาระสำคัญและมุมมองเชิงวิชาการได้ดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

- **การจำแนกประเภทเครือข่าย:** บทเรียนให้ภาพรวมชัดเจนของ WAN, MAN และ LAN ซึ่งช่วยให้ผู้เรียนเข้าใจขอบเขตการใช้งานในเชิงภูมิศาสตร์และเทคโนโลยีรองรับ
- **องค์ประกอบของเครือข่าย LAN:** เช่น สายสัญญาณ, NIC, NOS, อุปกรณ์เครือข่าย, bridges, routers และ gateways ซึ่งเป็นพื้นฐานสู่การวิเคราะห์ความเสี่ยงและการเลือกมาตรการป้องกันที่เหมาะสม
- **โทโปโลยีเครือข่าย:** เช่น star, ring, bus, mesh, hybrid และ FDDI ที่แต่ละแบบมีข้อดีข้อเสียต่อทั้งประสิทธิภาพและความมั่นคงปลอดภัย
- **มาตรการความมั่นคงปลอดภัย:** ครอบคลุม 3 ด้าน ได้แก่
 - ด้านเทคนิค (firewall, IDS/IPS, encryption, access control)
 - ด้านองค์กร (นโยบาย, incident response plan, security awareness)
 - ด้านกายภาพ (CCTV, access control, secure facility design)

2) มุมมองเชิงวิชาการและการอัปเดตสู่ความก้าวหน้าปัจจุบัน

1. **จากเครือข่ายแบบดั้งเดิมสู่ SDN และ SD-WAN** แนวโน้มสำคัญคือการเปลี่ยนผ่านจากการจัดการเครือข่ายแบบ static ไปสู่ Software-Defined Networking (SDN) และ Software-Defined WAN (SD-WAN) ซึ่งให้ความยืดหยุ่นและการควบคุมเชิงนโยบายที่ละเอียดขึ้น สามารถบังคับใช้ security policy แบบ *zero trust* ได้ที่ระดับ edge
2. **ความมั่นคงปลอดภัยโดยการออกแบบ (Security by Design)** บทเรียนได้กล่าวถึงมาตรการพื้นฐานแต่ในระดับวิชาการควรต่อยอดด้วยการสอน *secure network design patterns* เช่น micro-segmentation, zero trust network access (ZTNA) และ secure service edge (SSE) เพื่อสอดคล้องกับมาตรฐานสากลอย่าง NIST CSF 2.0
3. **การบูรณาการระบบคลาวด์และ IoT MAN และ WAN** ในปัจจุบันไม่เพียงรองรับ data center แต่ต้องสามารถ integrate กับ multi-cloud และ edge/IoT การเรียนการสอนควรเน้นความท้าทาย เช่น latency-sensitive workload, IoT trust, และ multi-cloud security posture
4. **การฝึกปฏิบัติและ Incident Response Drill** สิ่งที่น่าสนใจคือการฝึก DDoS Attack response โดยเชื่อมกับ NIST Cybersecurity Framework (CSF) ซึ่งสะท้อนการสอนแบบ evidence-driven เหมาะกับการยกระดับการประเมินผลผู้เรียนในรูปแบบ Outcome-based Education (OBE)

บท “วิศวกรรมเครือข่ายการสื่อสาร” ให้ฐานความรู้ที่ชัดเจนด้าน WAN, MAN, LAN และมาตรการความมั่นคงปลอดภัยพื้นฐาน จุดแข็งคือการออกแบบกิจกรรมเชิงปฏิบัติและ rubric ที่เชื่อมโยงกับ cybersecurity framework แต่เพื่อความทันสมัยและสะท้อนความก้าวหน้าทางวิชาการ การสอนควรยกระดับไปสู่ SD-WAN, Zero Trust, virtualization, และ multi-cloud integration ซึ่งจะทำให้ นักศึกษามีทั้งทักษะเชิงทฤษฎีและการปฏิบัติที่ตอบโจทย์อุตสาหกรรมจริง

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ พร้อมแนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง WAN, MAN และ LAN พร้อมยกตัวอย่างการใช้งาน

แนวคำตอบ: WAN ครอบคลุมพื้นที่กว้าง เช่น เชื่อมสำนักงานใหญ่กับสาขาต่างประเทศ; MAN เชื่อมเครือข่ายระดับเมือง เช่น มหาวิทยาลัยหลายวิทยาเขต; LAN ครอบคลุมพื้นที่จำกัด เช่น สำนักงานเดียว

ข้อ 2. อธิบายโทโปโลยีของ LAN ที่นิยมใช้ พร้อมข้อดีและข้อจำกัด

แนวคำตอบ: เช่น Star ใช้งานง่าย แก้ปัญหาเฉพาะจุด แต่ขึ้นกับ Hub/Switch; Ring ลดการชนกันแต่เครื่องเดียวเสียอาจล่ม; Bus ติดตั้งง่ายแต่เสี่ยงต่อความเสียหายจากสาย; Mesh มีความน่าเชื่อถือสูงแต่ต้นทุนสูง

ข้อ 3. วิเคราะห์ผลกระทบหากองค์กรละเลยมาตรการด้านเทคนิค เช่น Firewall และ IDS

แนวคำตอบ: เสี่ยงถูกบุกรุกจากภายนอก, การรั่วไหลของข้อมูล, การโจมตี DDoS ส่งผลต่อ Availability ของระบบ

ข้อ 4. อธิบายแนวคิด Security by Design และยกตัวอย่างในเครือข่าย LAN

แนวคำตอบ: ออกแบบความปลอดภัยตั้งแต่ต้น เช่น แบ่ง VLAN แยกเซิร์ฟเวอร์กับผู้ใช้, บังคับใช้ Access Control

ข้อ 5. อธิบายความสำคัญของมาตรการด้านกายภาพ เช่น CCTV และการควบคุมการเข้าถึงห้องเซิร์ฟเวอร์

แนวคำตอบ: ป้องกันการบุกรุกทางกายภาพ, ลดความเสี่ยงจากบุคคลที่ไม่ได้รับอนุญาต, เพิ่มความมั่นใจในการเก็บรักษาข้อมูล

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. เครือข่ายใดครอบคลุมพื้นที่กว้างที่สุด

ก. LAN

ข. MAN

ค. WAN

ง. WLAN

เฉลย: ค

ข้อ 2. ตัวอย่างของเครือข่าย MAN คือข้อใด

- ก. เครือข่ายอินเทอร์เน็ตทั่วโลก
- ข. เครือข่ายเชื่อมโยงคณะภายในมหาวิทยาลัยเดียวกัน
- ค. เครือข่ายเชื่อมโยงสำนักงานหลายประเทศ
- ง. เครือข่ายในบ้านพักอาศัย

เฉลย: ข

ข้อ 3. โทโปโลยี LAN แบบใดที่หาก Hub เสียหายจะกระทบทั้งระบบ

- ก. Bus
- ข. Star
- ค. Ring
- ง. Mesh

เฉลย: ข

ข้อ 4. โทโปโลยีใดมีความน่าเชื่อถือสูงสุดแต่มีต้นทุนสูง

- ก. Star
- ข. Bus
- ค. Ring
- ง. Mesh

เฉลย: ง

ข้อ 5. Firewall จัดเป็นมาตรการด้านใด

- ก. กายภาพ
- ข. องค์กร
- ค. เทคนิค

ง. การจัดการบุคคล

เฉลย: ค

ข้อ 6. หลักการพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ (CIA Triad) **ไม่รวม**ข้อใด

ก. Confidentiality

ข. Availability

ค. Authentication

ง. Integrity

เฉลย: ค

ข้อ 7. อุปกรณ์ใดใช้ในการกำหนดเส้นทางข้อมูลในเครือข่าย

ก. Switch

ข. Router

ค. Hub

ง. Bridge

เฉลย: ข

ข้อ 8. การแบ่ง VLAN ภายในองค์กรจัดเป็นมาตรการใด

ก. Intrusion Detection

ข. Network Segmentation

ค. Data Encryption

ง. Access Control

เฉลย: ข

ข้อ 9. มาตรการด้านองค์การที่สำคัญต่อ Network Security คือข้อใด

ก. การติดตั้ง CCTV

ข. การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ

ค. การเข้ารหัสข้อมูล

ง. การใช้รหัสผ่านซับซ้อน

เฉลย: ข

ข้อ 10. SD-WAN มีข้อดีสำคัญข้อใดเมื่อเทียบกับ MPLS

ก. ใช้ Bandwidth ได้คุ้มค่าและยืดหยุ่นกว่า

ข. ไม่ต้องใช้ Firewall

ค. ใช้ต้นทุนสูงกว่าเสมอ

ง. ไม่รองรับระบบคลาวด์

เฉลย: ก

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์ศรีบุญ. (ม.ป.ป.). *วิศวกรรมเครือข่ายการสื่อสาร (Communications Networks Engineering)*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Cisco Systems. (2022). SD-WAN Design Guide.

Gartner. (2021). Market Guide for Zero Trust Network Access (ZTNA).

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015).

Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE.

MITRE. (2023). ATT&CK Framework for Enterprise.

NIST. (2020). Zero Trust Architecture (SP 800-207).

NIST. (2024). Cybersecurity Framework (CSF) 2.0.

Stallings, W. (2020). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud.

Pearson.

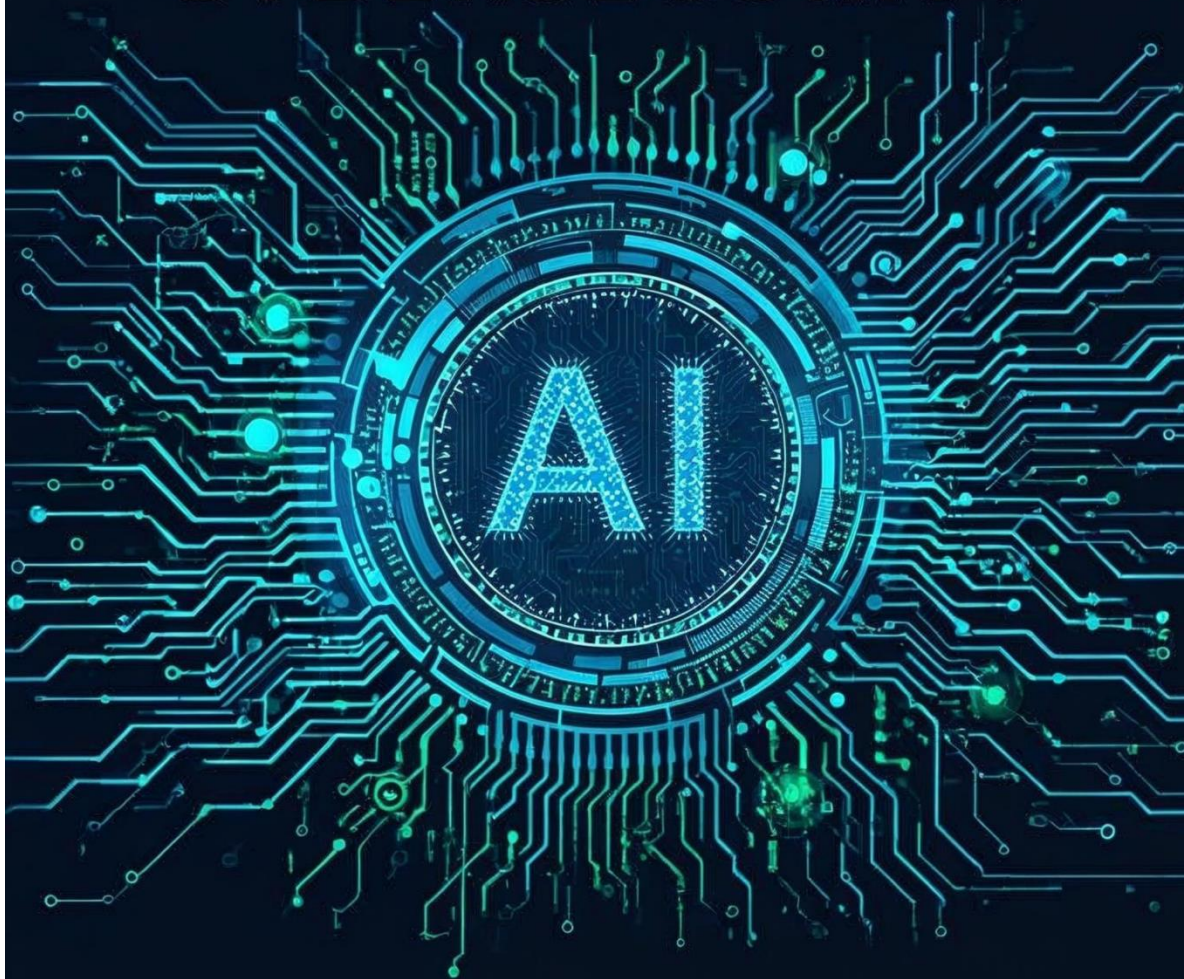
บทที่ 9

การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย

Secured Network Design

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพธิ์ศรีบุญ

บทที่ 9 การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (Secured Network Design)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบบทนี้ นักศึกษาจะสามารถ:

- 1) อธิบายหลักการออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (CIA Triad, Firewall, IDS/IPS) ได้
- 2) วิเคราะห์ภัยคุกคามและแบบจำลองการโจมตี (Threat Model & Phases of Compromise) ได้
- 3) ออกแบบการแบ่งโซนเครือข่าย (Internal, External, DMZ, Wireless) และโซนเฝ้าระวังได้
- 4) ประเมินบทบาทของอุปกรณ์และเทคนิค (Firewall, NAT, VPN) ในการเพิ่มความมั่นคงปลอดภัยได้
- 5) ประยุกต์ใช้แนวคิด Defense-in-Depth และ Zero Trust ในการออกแบบเครือข่ายได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบบทนี้ นักศึกษาจะสามารถ:

- 1) ระบุและอธิบายองค์ประกอบของการออกแบบเครือข่ายที่มั่นคงปลอดภัยได้
- 2) วิเคราะห์ขั้นตอนการบุกรุกเครือข่าย 5 ขั้น (Reconnaissance → Exploitation → Reinforcement → Consolidation → Pillage) ได้
- 3) ออกแบบเครือข่ายโดยการแบ่งโซนและกำหนดนโยบายควบคุมทราฟฟิกได้
- 4) ประเมินข้อดี-ข้อจำกัดของการใช้ Firewall, IDS/IPS และ NAT ในการป้องกันการบุกรุกได้
- 5) เสนอแนวทางการออกแบบเครือข่ายเชิงรุกโดยอ้างอิง Zero Trust และ Defense-in-Depth ได้

3. หัวข้อเนื้อหา:

9.1 การประยุกต์ใช้หลักการออกแบบเครือข่ายที่เหมาะสม

9.1.1 เครือข่ายต้องมีอาณาบริเวณที่ชัดเจน

9.1.2 ทราฟฟิกต้องเข้าออกผ่านไฟร์วอลล์เท่านั้น

9.1.3 แยกโฮสต์ที่มีการใช้งานเครือข่ายต่างกันออกจากกัน

9.1.4 ช่องทางพิเศษที่ไม่ได้ผ่านไฟร์วอลล์จำเป็นต้องควบคุมอย่างเข้มงวด

9.1.5 หลีกเลี่ยงการสื่อสารที่เชื่อมต่อโดยตรงระหว่างโฮสต์ภายในกับโฮสต์ภายนอก

9.2 การวิเคราะห์การบุกรุกเครือข่ายจนทำให้เหยื่อสยยอม

9.2.1 แบบจำลองภัยคุกคาม

9.2.2 โฮสต์ในเครือข่าย

9.2.3 การแบ่งโซนเครือข่าย

9.2.4 การจัดโซนเฝ้าระวัง

4. กิจกรรมการเรียนรู้ (กรณีศึกษา)

กรณีศึกษา:

มหาวิทยาลัย *RMUTT ThaiTech University* ต้องการปรับปรุงเครือข่ายของตนให้มั่นคงปลอดภัยยิ่งขึ้น ปัจจุบันใช้ Firewall เพียงชั้นเดียวเชื่อมต่อกับอินเทอร์เน็ต และมีเซิร์ฟเวอร์เว็บกับเมลล์อยู่ใน LAN เดียวกับผู้ใช้ภายใน ทำให้เกิดความเสี่ยงจากการโจมตี นักศึกษาต้องช่วยวิเคราะห์และออกแบบโครงสร้างเครือข่ายใหม่

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

- วิเคราะห์ความเสี่ยงจากโครงสร้างเครือข่ายปัจจุบัน
- เสนอการแบ่งโซนเครือข่าย (Internal, External, DMZ, Wireless)
- กำหนดมาตรการควบคุม (Firewall Rules, IDS/IPS, VPN สำหรับ Remote Access)
- สรุปผลการออกแบบและนำเสนอในรูปแบบ Diagram

ประเด็นการเรียนรู้:

- CIA Triad และการออกแบบเครือข่ายที่สอดคล้อง
- Threat Model และ Phases of Compromise
- Network Zoning และ Monitoring Zoning

- Defense-in-Depth และ Zero Trust Architecture

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ความเสี่ยง (25)	ครอบคลุมและลึกซึ้ง	ครบถ้วนแต่ยังไม่ลึก	กล่าวบางส่วน	ไม่ถูกต้อง
การออกแบบโซนเครือข่าย (30)	มี Diagram + เหตุผลชัดเจน	ออกแบบครบแต่ไม่ละเอียด	มีข้อเสนอแต่ไม่สมบูรณ์	ขาดการออกแบบ
มาตรการควบคุม (30)	ครอบคลุม Firewall, IDS, VPN, NAT	มีบางมาตรการ	ยังไม่ชัดเจน	ไม่มีข้อเสนอ
การนำเสนอ (15)	ชัดเจน ใช้สื่อ/ผังประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

9. การออกแบบความปลอดภัยเครือข่าย

แม้ระบบเครือข่ายภายในองค์กรจะมีกลไกการรับมือกับภัยคุกคามประเภทต่างๆ เช่น ระบบตรวจหา/ป้องกันการบุกรุก วิทยาการรหัสลับ ไฟร์วอลล์ เครือข่ายส่วนตัวเสมือน รวมทั้งอุปกรณ์อื่นๆ อย่างเต็มรูปแบบแล้วก็ตาม แต่ระบบความปลอดภัยในปัจจุบันจะอาศัยเพียงเครื่องมือป้องกันและกลไกการรับมือกับการโจมตีเครือข่ายเพียงประการเดียวย่อมไม่สามารถรับมือกับภัยคุกคามได้อย่างสมบูรณ์แบบถ้าปราศจากการออกแบบเครือข่ายที่เหมาะสม

การออกแบบเครือข่ายที่เหมาะสมจะมีส่วนช่วยเหลืออย่างสำคัญต่อการความยั่งยืนและอยู่รอดได้ของกลไกความปลอดภัยทั้งหมดที่กล่าวมาได้เป็นอย่างดี การออกแบบเครือข่ายโดยการจัดแบ่งทรัพยากรของเครือข่ายออกเป็นโซนโดยอาศัยไฟร์วอลล์ มีการออกแบบโดยจัดแบ่งทรัพยากรสำคัญออกเป็นส่วนๆ แต่ละส่วนจะวางตัวตรวจจับเพื่อเฝ้าระวังไว้ในตำแหน่งที่เหมาะสมจะช่วยให้การกำหนดกฎการเข้าถึง (Access rules) ในอุปกรณ์ที่ทำหน้าที่เฝ้าระวังและตรวจจับ เช่น ไฟร์วอลล์ ทำได้โดยง่าย สามารถกรองและวิเคราะห์การบุกรุกได้อย่างถูกต้องและแม่นยำ

การออกแบบในหนังสือเล่มนี้จะยึดหลักการออกแบบโดยแบ่งแยก (Separate design) ที่อาศัยหลักการสำคัญว่า “อย่าวางไข่ทุกฟองไว้ในตะกร้าใบเดียว” แนวคิดนี้มีวัตถุประสงค์เพื่อหลีกเลี่ยงไม่ให้เครือข่ายของเราตกเป็นเป้าหมายของการถูกโจมตีได้โดยง่าย และช่วยกระจายความเสี่ยงต่อการถูกโจมตี หลีกเลี่ยงความเสียหายรวมทั้งช่วยบรรเทาและจำกัดขอบเขตความเสียหายเมื่อถูกโจมตี

เนื้อหาในบทนี้จะอธิบายถึงการประยุกต์ใช้มาตรการด้านความมั่นคงปลอดภัย การออกแบบเครือข่ายที่เหมาะสม, แบบจำลองภัยคุกคาม (Threat model), โฮสต์ที่ไว้วางใจได้ (Trusted host) โฮสต์ที่ไว้วางใจไม่ได้ (Untrusted host) การแบ่งโซนเครือข่าย (Network zoning) และการจัดโซนเฝ้าระวัง (Monitoring zoning)

9.1 การประยุกต์ใช้หลักการออกแบบเครือข่ายที่เหมาะสม

การออกแบบเครือข่ายขององค์กรให้สอดคล้องกับหลักการสามเสาของ C-I-A Triad กล่าวคือ เป็นการออกแบบเครือข่ายเพื่อให้สามารถธำรงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้ (Availability) จากบริการต่างๆ ของเครือข่ายองค์กร

สมมุติฐานในเบื้องต้นของเนื้อหาในบทนี้ คือการให้ระบบตรวจหาการบุกรุกทำงานร่วมกับการใช้ไฟร์วอลล์ในควบคุมการจราจรของเครือข่าย การกำหนดนโยบายในไฟร์วอลล์และระบบตรวจหาการบุกรุกสำหรับใช้ในการป้องกันและตรวจจับการบุกรุกที่เหมาะสมนั้นจะทำให้ระบบรักษาความปลอดภัยภายใต้สถาปัตยกรรมนี้ทำงานได้เต็มประสิทธิภาพ และเพื่อให้บรรลุตามวัตถุประสงค์ดังกล่าว ตำแหน่งของการติดตั้งไฟร์วอลล์และระบบ

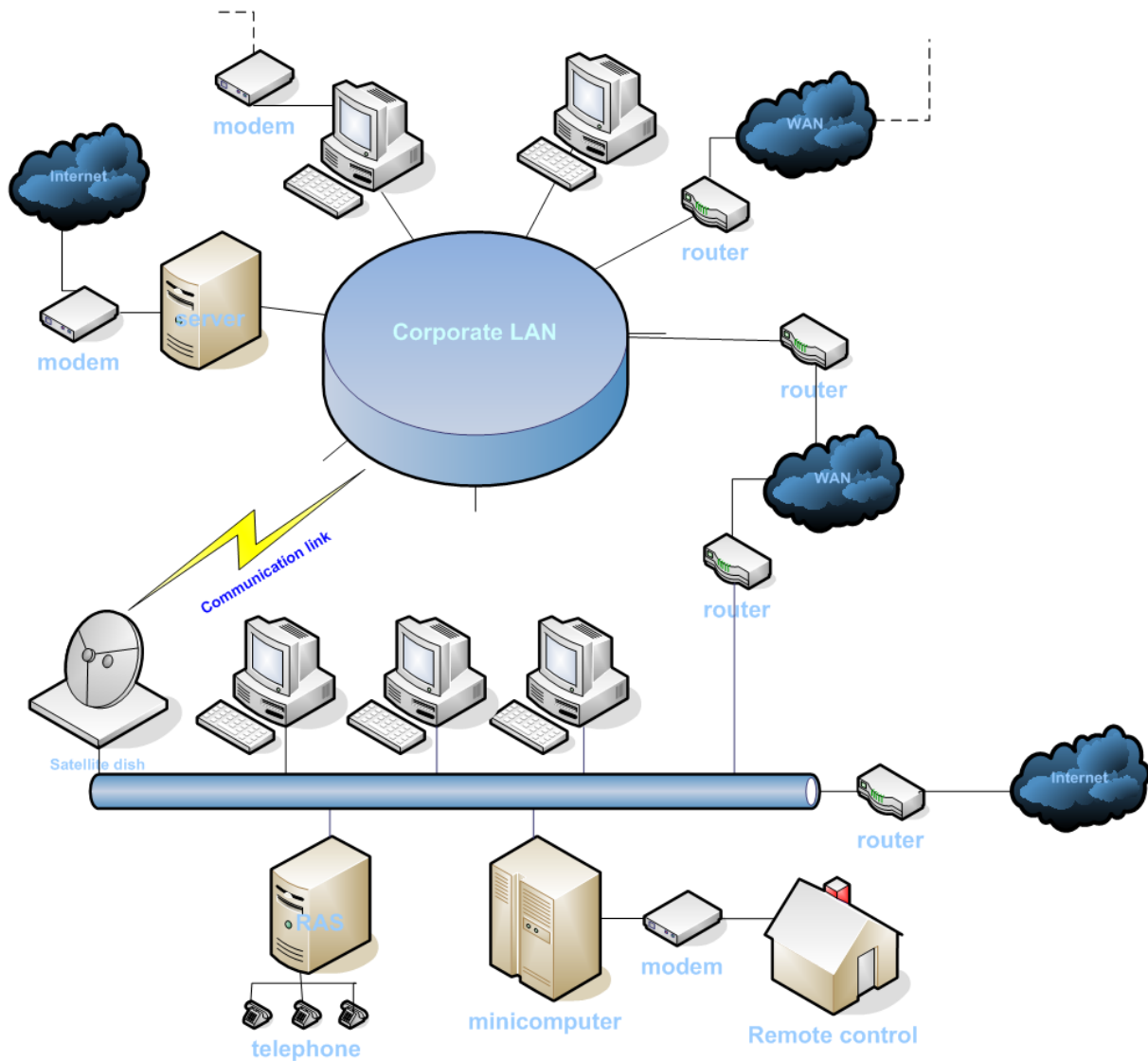
ตรวจหาการบุกรุกจะต้องได้รับการออกแบบที่เหมาะสมและเอื้อต่อการทำงานของระบบตรวจหาการบุกรุกที่ได้รับการออกแบบภายใต้สถาปัตยกรรมนี้ เนื้อหาในบทนี้จึงกล่าวถึงหลักการสำคัญของออกแบบเครือข่ายคอมพิวเตอร์เพื่อติดตั้งไฟร์วอลล์และ IDS/IPS ไว้ในตำแหน่งที่เหมาะสม

การมีระบบตรวจหาการบุกรุกที่ดีไม่ได้เป็นหลักประกันว่าระบบเครือข่ายจะปลอดภัยจากการบุกรุกหรือถูกโจมตีจากผู้ประสงค์ร้าย ระบบตรวจหาการบุกรุกจะสามารถทำงานได้อย่างมีประสิทธิภาพบนพื้นฐานของเครือข่ายที่ถูกออกแบบมาดีเท่านั้น เครือข่ายที่ดีจะต้องจำกัดให้ทราฟฟิกทั้งหมดที่สื่อสารกันระหว่างภายในกับภายนอกนั้นวิ่งผ่านช่องทางที่ถูกควบคุมไว้ด้วยไฟร์วอลล์ และสามารถถูกมองเห็นได้โดยระบบตรวจหาการบุกรุก หากมีช่องทางใดที่ทราฟฟิกจะสามารถเข้าออกได้โดยไม่ผ่านการควบคุมของไฟร์วอลล์และระบบตรวจหาการบุกรุก แม้เพียงช่องทางเดียว การทำงานของระบบตรวจหาการบุกรุกบนเครือข่ายนั้นก็ปราศจากความหมาย

ดังนั้น ก่อนที่จะพิจารณาระบบตรวจหาการบุกรุกไปติดตั้งไว้ ณ บริเวณใดในเครือข่าย เครือข่ายนั้นจำเป็นต้องได้รับการออกแบบให้รัดกุมและรองรับการทำงานของระบบตรวจหาการบุกรุกเสียก่อน โดยการออกแบบเครือข่ายนั้นต้องอยู่บนพื้นฐานสำคัญดังต่อไปนี้ เครือข่ายต้องมีอาณาบริเวณที่ชัดเจน, ทราฟฟิกต้องเข้าออกผ่านไฟร์วอลล์เท่านั้น, แยกโฮสต์ที่มีลักษณะการใช้งานเครือข่ายต่างกันออกจากกัน, ช่องทางพิเศษที่ไม่ได้ผ่านไฟร์วอลล์จำเป็นต้องควบคุมอย่างเข้มงวด และหลีกเลี่ยงการสื่อสารที่เชื่อมต่อโดยตรงระหว่างโฮสต์ภายในกับโฮสต์ภายนอก

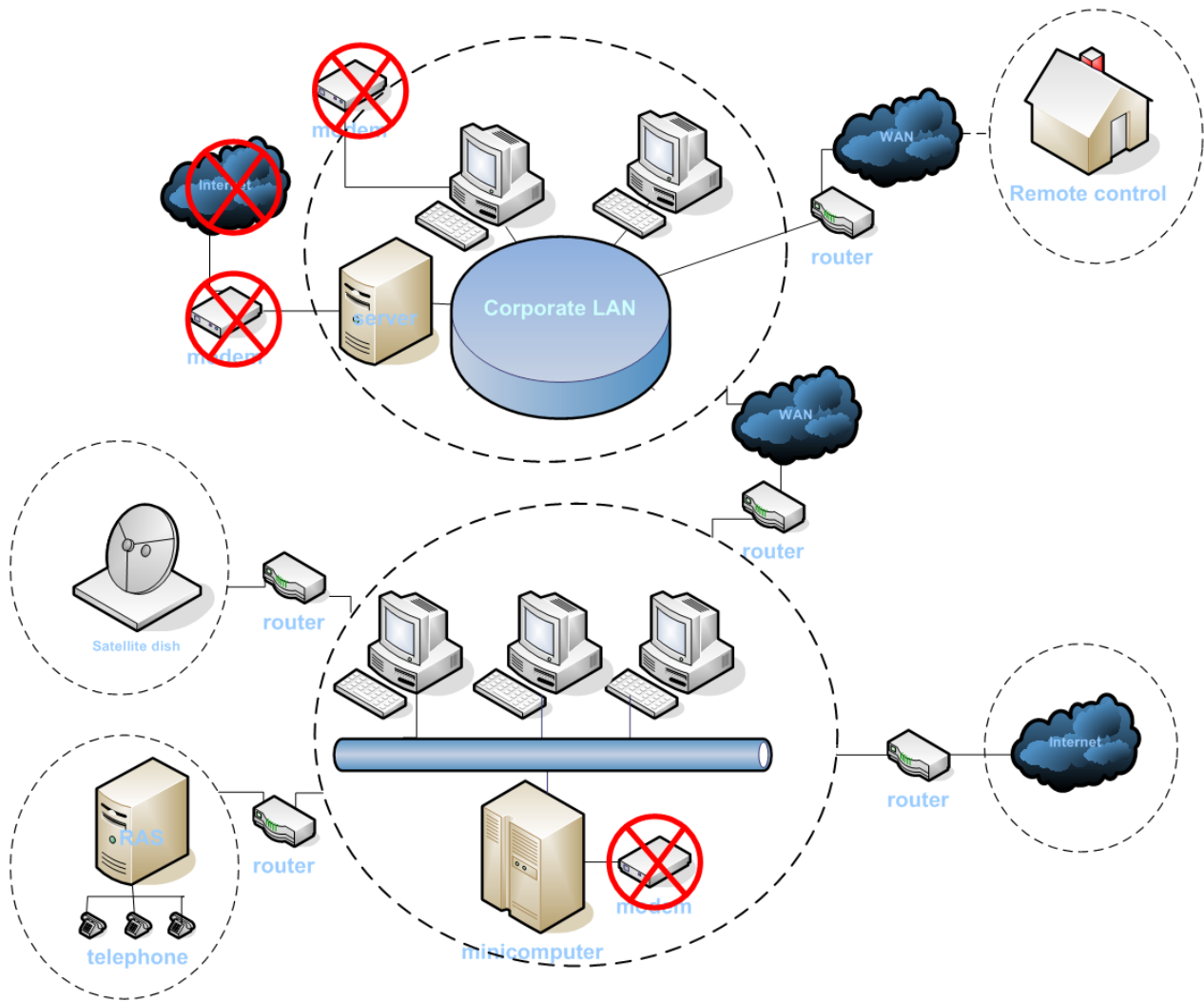
9.1.1 เครือข่ายต้องมีอาณาบริเวณที่ชัดเจน

ในการจัดการเครือข่าย เราจะใช้ไฟร์วอลล์เป็นเครื่องที่สร้างแนวป้องกันการบุกรุก ทำงานในลักษณะปกป้องอาณาเขต (Perimeter defense) ไฟร์วอลล์จะไม่สามารถทำงานได้อย่างถูกต้องบนเครือข่ายที่ไม่มีการกำหนดขอบเขตให้ชัดเจนก่อน ดังนั้น ถ้าจะนำไฟร์วอลล์ไปใช้จะต้องออกแบบให้เครือข่ายมีอาณาบริเวณที่ชัดเจน กล่าวคือจะต้องระบุให้ชัดเจนว่าเครือข่ายนั้นครอบคลุมโฮสต์ใดบ้าง ใช้เลขที่อยู่ไอพีช่วงใดถึงช่วงใด สามารถระบุได้ชัดเจนว่าจะอนุญาตให้ทราฟฟิกผ่านเข้าออกจากจุดใดบ้าง รูป 9.1 แสดงให้เห็นถึงเครือข่ายที่ไม่มีอาณาบริเวณที่ชัดเจน (non-perimeter network) มีการขยายขอบเขตของการเชื่อมต่อออกไปอย่างไม่ที่สิ้นสุด บางส่วนไม่มีการควบคุมโฮสต์ที่เข้ามาเชื่อมต่อด้วยได้เช่นแม่ข่ายให้บริการจากระยะไกล (RAS: Remote access server) มีช่องทางเข้าออกจำนวนมาก สามารถเชื่อมต่อกับอินเทอร์เน็ตได้หลายจุด ทำให้ความเสี่ยงที่จะถูกบุกรุกสามารถเกิดขึ้นได้จากหลายช่องทาง



รูป 9.1 เครือข่ายที่ไม่มีอาณาบริเวณ (Non-perimeter network)

เครือข่ายที่กำหนดอาณาบริเวณที่แน่นอนแล้ว การออกแบบที่ดีจะพยายามลดช่องทางการสื่อสารกับภายนอกเครือข่ายให้เหลือน้อยที่สุด โดยอาจกำหนดเป็นช่องทางหลัก ช่องทางรอง และช่องทางสำรองเพื่อไว้ในกรณีช่องทางหลักและรองมีปัญหา การมีช่องทางจำกัดจะช่วยให้การควบคุมทราฟฟิกและการตรวจสอบการบุกรุกทำได้ง่ายขึ้น ในกรณีที่เกิดการละเมิดความปลอดภัยก็จะสามารถตรวจพบได้ง่ายและสามารถแก้ไขได้รวดเร็ว



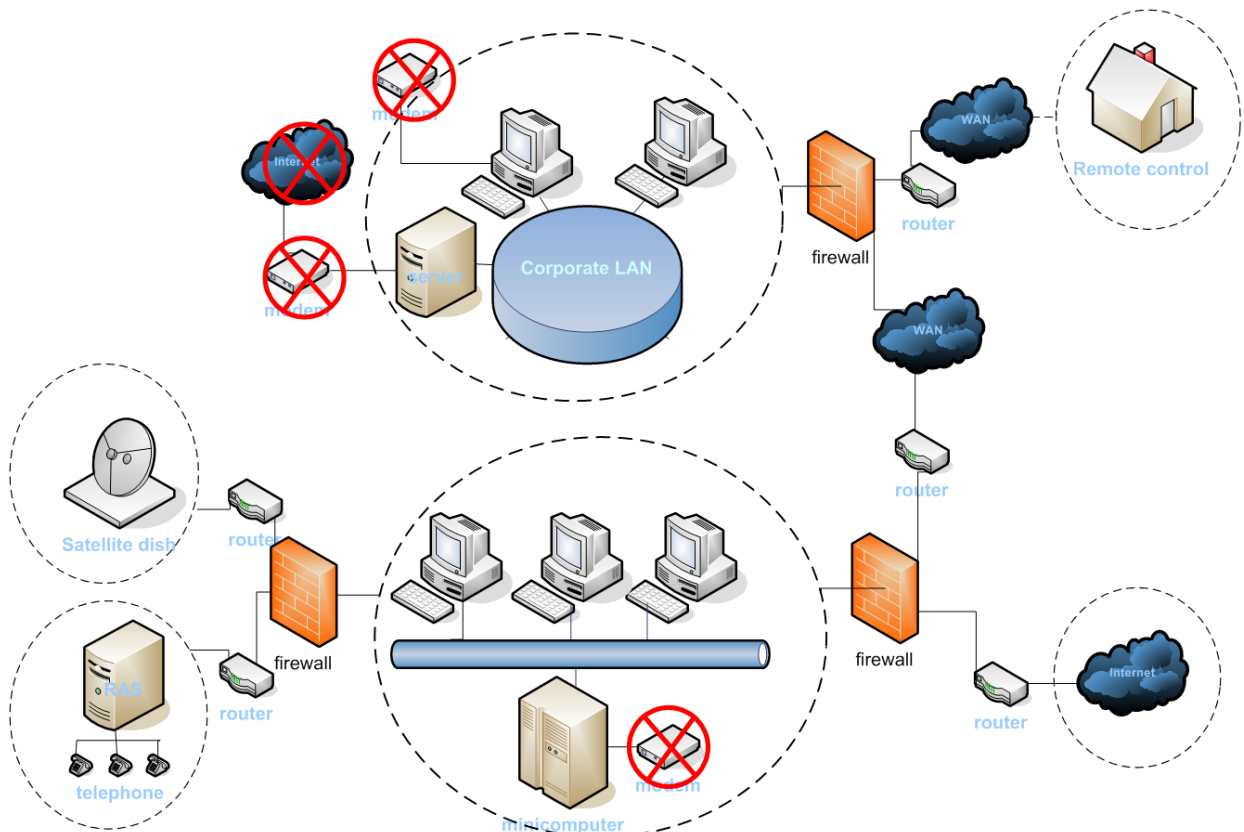
รูป 9.2 การแบ่งส่วนเครือข่ายออกเป็นส่วนย่อยๆ แต่ละส่วนมีอาณาบริเวณที่แน่นอน

รูป 9.2 แสดงการจัดทรัพยากรเครือข่ายที่ได้จากภาพที่ 5-1 มาจัดให้เป็นเครือข่ายย่อยๆ แต่ละเครือข่ายมีอาณาบริเวณที่ชัดเจน จำกัดช่องทางผ่านเข้าออกกราฟฟิก ครอบคลุมโฮสต์จำนวนที่แน่นอน อย่างไรก็ตาม ภายใต้วงจรที่ 5-2 ยังมีบางช่องทางที่ไม่สามารถควบคุมกราฟฟิกได้อย่างรัดกุม เช่น การเชื่อมต่ออินเทอร์เน็ตผ่านโมเด็มโดยผู้ใช้ การเชื่อมต่อระยะไกลจากที่บ้าน การสื่อสารประเภทนี้จำเป็นต้องถูกตัดออกไป จากนั้น อนุญาตให้ใช้ช่องทางอื่นที่ปลอดภัยเข้ามาทดแทน เมื่อเครือข่ายมีขอบเขตที่ชัดเจนแล้ว การวางตำแหน่งของไฟร์วอลล์เพื่อควบคุมกราฟฟิกและระบบตรวจหาการบุกรุกเพื่อเฝ้าระวังไว้ในแต่ละส่วน ก็ถือเป็นการออกแบบเครือข่ายที่มีการควบคุมที่ดี

9.1.2 ทราฟฟิกต้องเข้าออกผ่านไฟร์วอลล์เท่านั้น

โดยทั่วไปแล้ว ไฟร์วอลล์จะสามารถทำหน้าที่ควบคุมและรักษาความปลอดภัยไว้ได้อย่างสมบูรณ์ก็ต่อเมื่อทราฟฟิกทั้งหมดของเครือข่ายที่เข้าออกระหว่างเครือข่ายภายในกับภายนอกนั้นผ่านช่องทางของไฟร์วอลล์เท่านั้น หากมีการเข้าออกได้โดยไม่ผ่านไฟร์วอลล์จะถือว่าระดับความปลอดภัยของเครือข่ายนั้นถูกลดต่ำลงและอาจสูญเสียการควบคุมได้ ตัวอย่างเช่น มีไฟร์วอลล์ควบคุมทราฟฟิกทุกจุดแต่ยังอนุญาตให้บางโฮสต์สามารถเชื่อมต่ออินเทอร์เน็ตผ่านโมเด็ม ซึ่งการเชื่อมต่อดังกล่าวนี้ไม่ได้ผ่านการควบคุมของไฟร์วอลล์ จึงเป็นช่องโหว่สำคัญที่อาจถูกบุกรุกผ่านทางโมเด็มได้ ดังนั้น การออกแบบเครือข่ายที่จะต้องประกันว่าทุกจุดที่ทำการเชื่อมต่อกับเครือข่ายภายนอกจะต้องมีไฟร์วอลล์ควบคุมทราฟฟิกไว้ด้วยเสมอ

รูป 10.3 แสดงตัวอย่างการนำไฟร์วอลล์ไปติดตั้งที่จุดเชื่อมต่อของเครือข่ายแต่ละส่วนที่ถูกแบ่งออกเป็นส่วนย่อยๆ แล้วเพื่อควบคุมทราฟฟิกที่เข้าออกระหว่างเครือข่ายเหล่านั้น การออกแบบดังรูป 9.3 นี้แสดงให้เห็นว่ามาตรการควบคุมทราฟฟิกได้ถูกกำหนดไว้อย่างเหมาะสม สามารถรับมือกับการบุกรุกได้อย่างมีประสิทธิภาพ ทั้งนี้ ขึ้นอยู่กับค่า Access rule ได้ถูกกำหนดไว้อย่างเหมาะสมอีกด้วย



รูป 9.3 แสดงการนำไฟร์วอลล์มาควบคุมทราฟฟิกเข้าออกแต่ละเครือข่าย

9.1.3 แยกโฮสต์ที่มีการใช้งานเครือข่ายต่างกันออกจากกัน

โฮสต์ที่อยู่ภายในเครือข่ายย่อมมีการใช้งานแตกต่างกัน บางโฮสต์อาจเป็นไคลเอนต์ที่มีผู้ใช้ใช้งานอยู่ภายในองค์กร ไม่เปิดให้บริการแก่ผู้ใช้งานนอก ในขณะที่บางโฮสต์อาจจำเป็นต้องเปิดให้บริการผู้ใช้งานนอกโดยตรงเช่นเครื่องแม่ข่ายให้บริการไปรษณีย์, เครื่องแม่ข่ายให้บริการเว็บ เป็นต้น ระดับการเข้าถึงโฮสต์ทั้งสองประเภทเหล่านี้นย่อมแตกต่างกัน โดยปกติ โฮสต์ที่สามารถเข้าถึงได้โดยบุคคลภายนอกย่อมมีความเสี่ยงที่จะถูกบุกรุกสูงกว่าโฮสต์ที่เป็นของผู้ใช้ทั่วไป เพื่อป้องกันในกรณีนี้โฮสต์ที่เป็นเครื่องให้บริการเหล่านั้นถูกบุกรุกสำเร็จแล้วใช้เป็นช่องทางในการบุกรุกโฮสต์อื่นๆ ที่อยู่ภายในเครือข่ายขององค์กร ดังนั้น เราจึงไม่ควรออกแบบให้โฮสต์ทั้งสองประเภทเหล่านี้อยู่ในเครือข่ายเดียวกัน

เพื่อแก้ปัญหานี้ เราจะออกแบบให้เครือข่ายจำแนกโฮสต์เหล่านั้นออกเป็นโซน (Zone) เพื่อให้การกำหนดค่า Access rule สำหรับควบคุม ป้องกัน และเฝ้าระวังทำได้โดยง่าย การแบ่งเครือข่ายออกเป็นโซนจะอธิบายในหัวข้อถัดไป

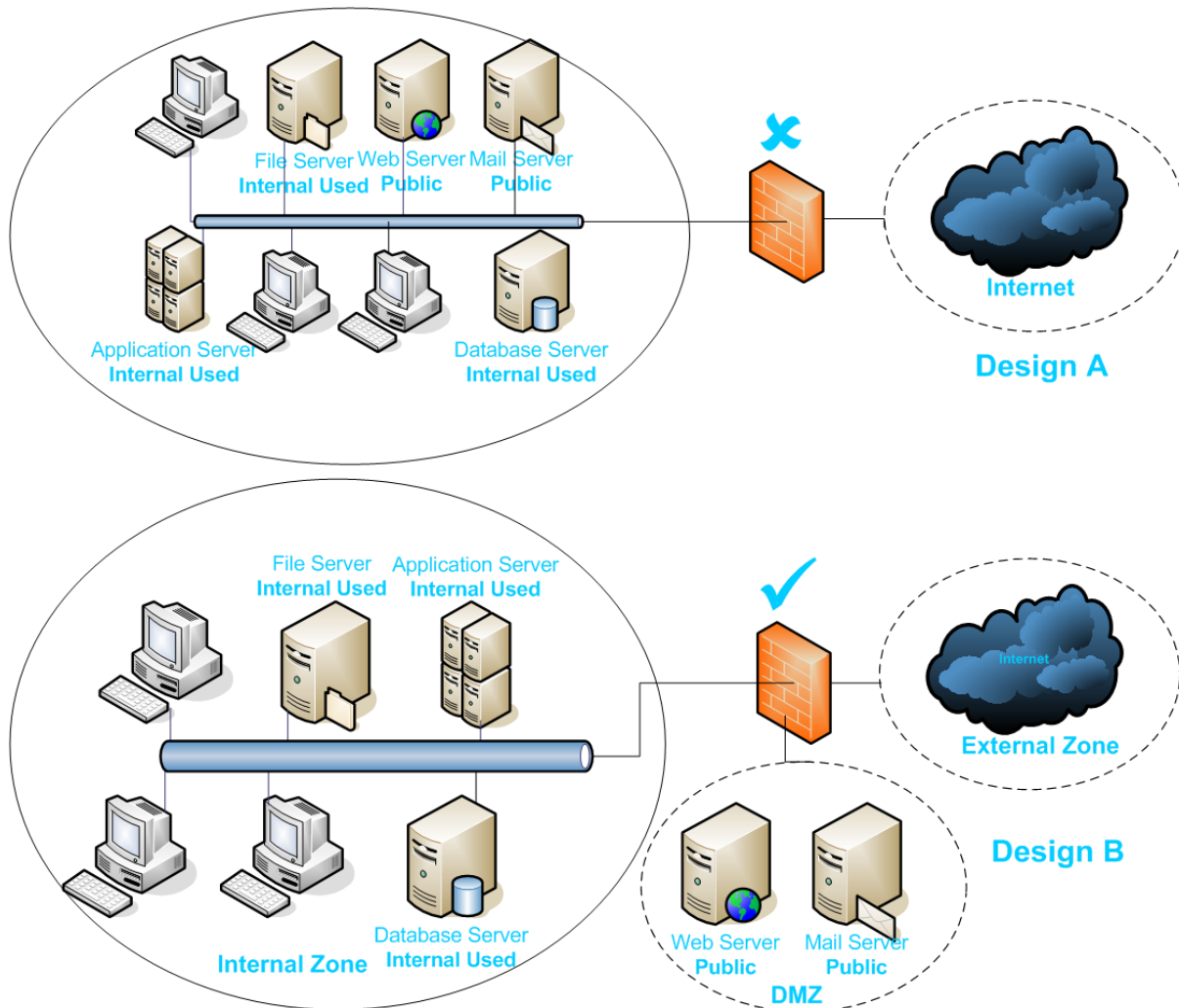
รูป 9.4 แสดงการออกแบบเครือข่ายออกเป็นโซน ด้วยการแยกโฮสต์ภายในออกจากโฮสต์ภายนอก โดยอาศัยไฟร์วอลล์มาช่วยควบคุมทราฟฟิกที่ผ่านเข้าออกทั้งสองโซน แต่ Design A แสดงให้เห็นถึงตัวอย่างของการนำเอาโฮสต์ที่สามารถเข้าถึงได้โดยบุคคลภายนอกได้แก่แม่ข่ายให้บริการไปรษณีย์และแม่ข่ายให้บริการเว็บรวมอยู่กับโซนเครือข่ายภายใน แม้ว่าทราฟฟิกทั้งหมดจะถูกควบคุมโดยไฟร์วอลล์ แต่ออกแบบเช่นนี้มีความเสี่ยงต่อการถูกบุกรุกจากภายนอกได้โดยง่าย เนื่องจากการกำหนด access rule ในการเข้าถึงเครื่องให้บริการสาธารณะเหล่านั้นจะใช้ค่าเดียวกับโฮสต์ภายในทั้งหมด แต่ระดับความเสี่ยงของโฮสต์ที่ใช้งานภายในกับโฮสต์ที่ทำหน้าที่เป็นแม่ข่ายต่อบุคคลภายนอกนั้นย่อมแตกต่างกัน โฮสต์ที่ติดต่อกับภายนอกโดยตรงย่อมมีโอกาที่จะถูกบุกรุกได้สูงกว่า

ดังนั้น การออกแบบ Design A จึงถือว่ายังไม่เหมาะสม ในขณะที่ Design B ได้แยกเครื่องแม่ข่ายให้บริการสาธารณะทั้งสองออกไปอยู่อีกโซน (DMZ) และทราฟฟิกที่ผ่านเข้าออกแต่ละโซนจะต้องผ่านไฟร์วอลล์ทั้งสิ้น การออกแบบ Design B จึงมีความเหมาะสม สามารถกำหนดค่า access rule แต่ละโซนให้เหมาะสมแตกต่างกันตามระดับความเสี่ยงของเครือข่ายแต่ละโซน เมื่อเกิดการโจมตีขึ้นที่โซนใดก็สามารถจำกัดขอบเขตความเสียหายให้อยู่ในโซนนั้นได้ไม่ส่งผลกระทบต่อโฮสต์ทั้งหมดที่อยู่ในโซนที่เหลือ

9.1.4 ช่องทางพิเศษที่ไม่ได้ผ่านไฟร์วอลล์จำเป็นต้องควบคุมอย่างเข้มงวด

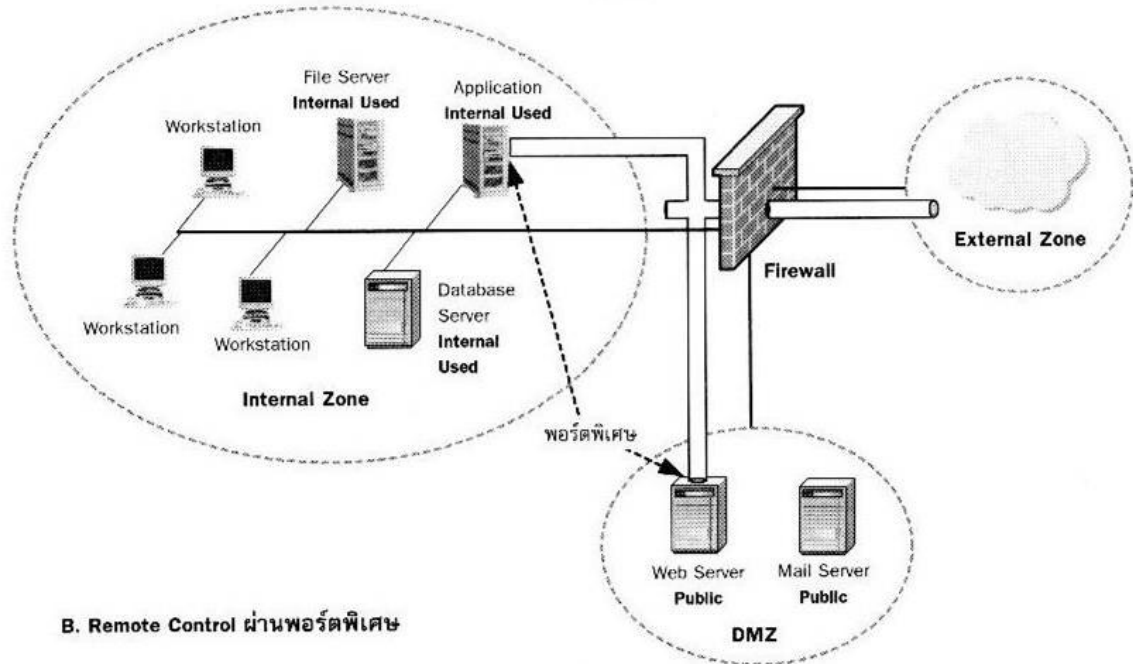
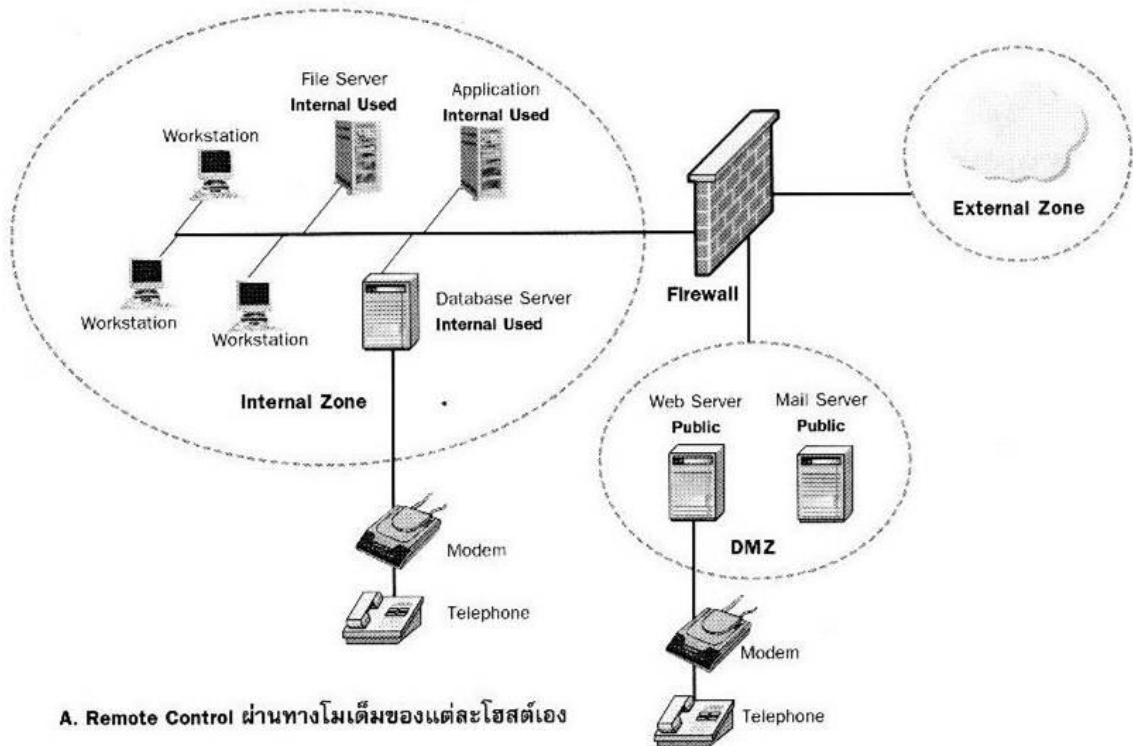
แม้ว่าเครือข่ายจะถูกออกแบบให้มีช่องทางที่จำกัดในการเชื่อมต่อกับภายนอกเพื่อประกันว่าทุกทราฟฟิกจะต้องเข้าออกผ่านไฟร์วอลล์เท่านั้น แต่บางองค์กรก็จำเป็นต้องยอมให้มีช่องทางพิเศษไว้โดยสามารถผ่านไฟร์วอลล์ได้โดยไม่มีการควบคุม ในกรณีเช่นนี้จำเป็นที่จะต้องมีการรักษาความปลอดภัยอย่างอื่นร่วมด้วย โดย

ปกติไฟร์วอลล์จะให้ความสำคัญกับการเข้าถึงจากภายนอก (Inbound access) มากกว่าทราฟฟิกขาออก (Outbound access) ทั้งนี้ ทราฟฟิกขาเข้าจะเป็นแหล่งนำมาซึ่งการบุกรุกจากผู้ประสงค์ร้ายได้มากกว่าทราฟฟิกขาออกนั่นเอง ดังนั้น การอนุญาตให้มีทราฟฟิกขาเข้าจึงเป็นไปอย่างจำกัดเท่าที่จำเป็นเท่านั้น



รูป 9.4 แสดงการออกแบบเครือข่ายออกเป็นโซน

อย่างไรก็ตาม มีหลายกรณีที่ต้องครั้นยอมให้มีการเข้าถึงจากระยะไกลโดยการเชื่อมต่อเข้าสู่เครือข่ายขององค์กรจากจากผู้ใช้ที่มีโฮสต์อยู่บนอินเทอร์เน็ต เช่น เอกซ์ทราเน็ต (Extranet) ในกรณีเช่นนี้ ไฟร์วอลล์จะต้องมีการเปิดช่องทางพิเศษไว้เพื่ออนุญาตให้ทราฟฟิกประเภทนี้สามารถผ่านเข้ามาภายในเครือข่ายได้โดยที่ไฟร์วอลล์จะไม่สามารถควบคุมการสื่อสารในช่องทางพิเศษนี้ได้เลย



รูป 9.5 แสดงการมีช่องทางพิเศษสำหรับการควบคุมจากระยะไกล

โดยปกติ ช่องทางพิเศษนี้จะถูกออกแบบไว้สำหรับการเข้าถึงจากระยะไกลโดยผู้บริหารระบบ (System administrator) อาจเพื่อเข้ามาช่วยแก้ปัญหาบางประการโดยอาศัยโปรแกรมประเภทควบคุมจากระยะไกล (Remote control) เช่น Telnet, Secure Shell, XWindow, Microsoft Terminal Server,

Anywhere เป็นต้น โดยอาศัยโปรแกรมดังกล่าว จะทำให้บุคคลนั้นสามารถควบคุมเครื่องแม่ข่ายจากระยะไกลได้ โดยสมบูรณ์ อย่างไรก็ตาม การเข้าถึงช่องทางพิเศษด้วยวิธีดังกล่าวไม่เพียงแต่อนุญาตให้ผู้บริหารระบบเข้าควบคุมเครื่องแม่ข่ายจากระยะไกลเท่านั้น แต่อาจเป็นช่องทางที่ผู้บุกรุกสามารถเข้าควบคุมเครื่องแม่ข่ายจากระยะไกลได้อีกด้วย หากระบบปราศจากมาตรการรักษาความปลอดภัยที่ดีพอ

รูป 9.5.A เป็นการต่อโมเด็มไว้ที่เครื่องแม่ข่ายทั้งสองเครื่อง มีวัตถุประสงค์เพื่อให้ผู้บริหารระบบสามารถหมุนโมเด็มเพื่อทำการเชื่อมต่อจากระยะไกล วิธีเช่นนี้อาจเป็นช่องโหว่ที่ผู้บุกรุกสามารถเจาะระบบผ่านได้ โดยอาศัยโปรแกรมประเภท war dialer หรือในกรณีตรงกันข้าม ผู้บุกรุกอาจเป็นเจ้าของหน้าที่บริหารระบบก็ได้

รูป 9.5.B แสดงตัวอย่างของการเข้าถึงจากระยะไกลโดยไม่อาศัยโมเด็มแต่จะวิธีผ่านพอร์ต TCP หรือ UDP ที่ถูกกำหนดไว้ล่วงหน้าด้วยวัตถุประสงค์เดียวกัน หมายเลขของพอร์ตทั้ง TCP และ UDP มีจำนวนเท่ากับ 65,534x2 ดังนั้น หมายเลขพอร์ตที่ใช้ควรเป็นความลับเช่นเดียวกับหมายเลขโทรศัพท์สำหรับการควบคุมจากระยะไกล หากไม่มีการเปิดเผยก็ย่อมยากที่จะคาดเดาได้โดยผู้บุกรุก อย่างไรก็ตาม ผู้บุกรุกสามารถใช้เครื่องมือในการสแกนพอร์ตเข้ามาช่วยเพื่อค้นหาพอร์ตที่ใช้สำหรับการควบคุมจากระยะไกล

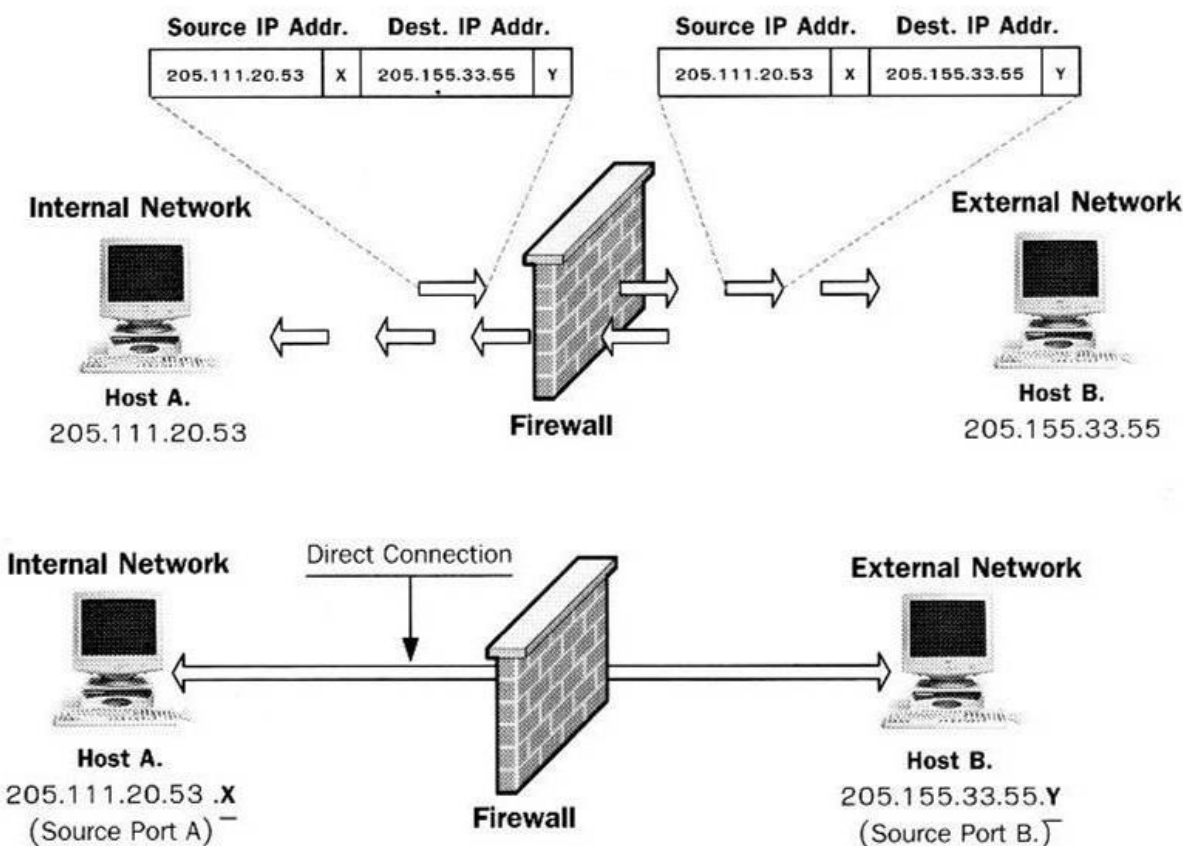
ดังนั้น จะเห็นว่า การที่องค์กรอนุญาตให้มีการใช้ช่องทางพิเศษผ่านเข้ามาทำการควบคุมจากระยะไกลเพื่อวัตถุประสงค์สำหรับผู้บริหารระบบนั้นแม้มีประโยชน์ต่อการทำงานก็ตาม แต่ก็อาจเป็นช่องโหว่ที่มีความเสี่ยงต่อการบุกรุกสำหรับผู้ประสงค์ร้ายได้เช่นกัน

หากเครือข่ายขององค์กรมีการอนุญาตให้ใช้งานในลักษณะนี้ได้ เราเสนอให้ใช้ VPN เป็นกระบวนการรักษาความปลอดภัยสำหรับช่องทางพิเศษดังกล่าวนี้ เพื่อประกันว่า โฮสต์หรือผู้ใช้ที่สามารถใช้งานผ่านช่องทางพิเศษนี้ได้จะต้องเป็นผู้ที่ได้รับสิทธิ์นี้เท่านั้น โดย VPN จะมีกระบวนการตั้งแต่การเข้ารหัสแบบอสมมาตร, การพิสูจน์ตัวจริง, การตรวจสอบรหัสผ่าน และกระบวนการตรวจสอบระดับสิทธิ์ในการใช้งาน รายละเอียดเกี่ยวกับ VPN ได้อธิบายไว้แล้วในหัวข้อที่ผ่านมา

9.1.5 หลีกเลี่ยงการสื่อสารที่เชื่อมต่อโดยตรงระหว่างโฮสต์ภายในกับโฮสต์ภายนอก

การสื่อสารของ TCP/IP นั้นจะต้องอาศัยการสถาปนาการเชื่อมต่อโดยตรงระหว่างโฮสต์ต้นทางกับโฮสต์ปลายทางโดยอาศัยเลขที่อยู่ไอพีและเลขหมายพอร์ตเป็นสิ่งที่ระบุการเชื่อมต่อที่เกิดขึ้นในขณะนั้น โดยทั่วไปการกำหนดเลขที่อยู่ไอพีของโฮสต์ภายในเครือข่ายนั้นจะถูกกำหนดให้ใช้เลขที่อยู่ไอพีสาธารณะ (Public IP หรือ Registered IP address) แต่องค์กรสามารถกำหนดให้ใช้เลขที่อยู่ไอพีส่วนตัว (Private IP หรือ Invalid IP address) โดยอาศัยการแปลงเลขที่อยู่ไอพี (NAT) ก็ได้ รายละเอียดการใช้ NAT ได้อธิบายไว้แล้วในบทก่อนหน้านี้ หากกำหนดให้ใช้เลขที่อยู่ไอพีส่วนตัวจำเป็นต้องอาศัยไฟร์วอลล์เข้ามาเป็นอุปกรณ์ในการทำหน้าที่แปลงเลขที่อยู่

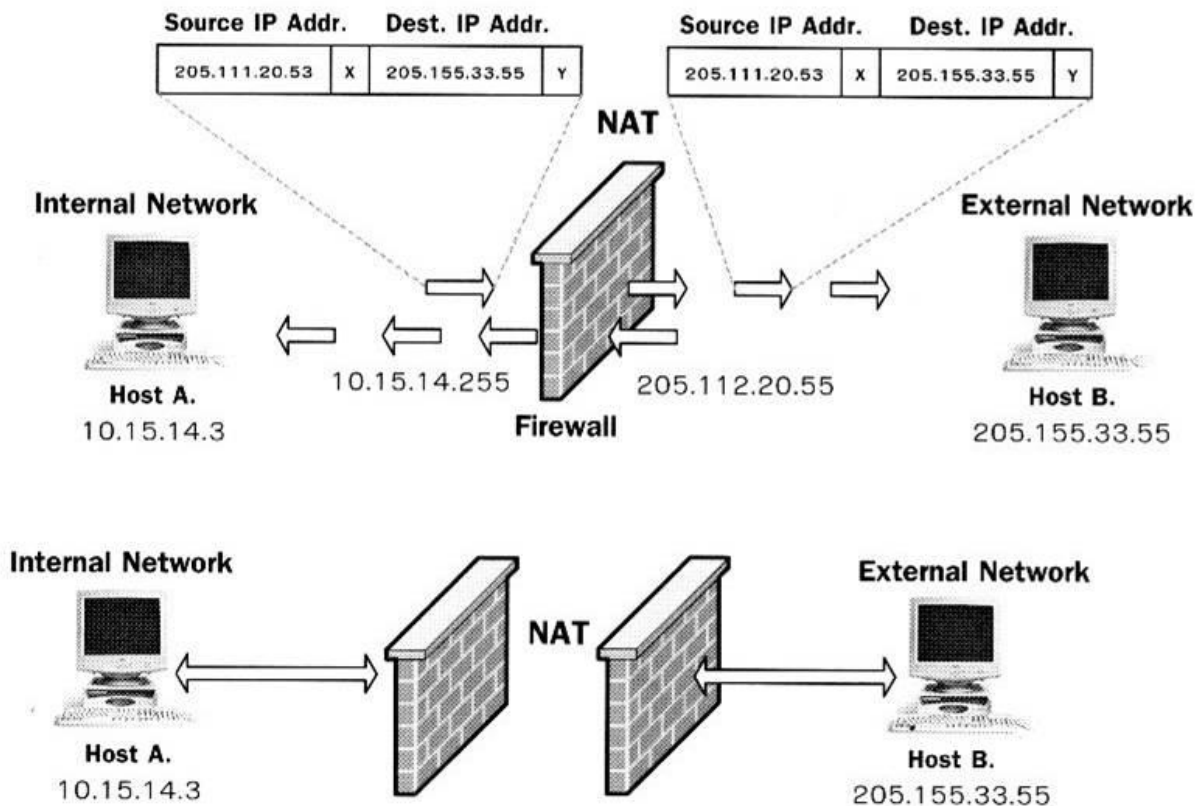
ในกรณีเช่นนี้ ไฟร์วอลล์นอกเหนือจากทำหน้าที่ควบคุมทราฟฟิกแล้วยังถูกใช้ในการซ่อนโฮสต์ทั้งหลายที่อยู่เบื้องไฟร์วอลล์จากการติดต่อโดยตรงจากภายนอก ทำการซ่อนหรือปิดบังไม่ให้โฮสต์ปลายทางที่กำลังสื่อสารอยู่ด้วยนั้นไม่สามารถรู้ว่าโฮสต์ที่ตนเองกำลังติดต่อกับด้วยขณะนี้ใช้เลขที่อยู่ไอพีใด เมื่อนำไฟร์วอลล์และกระบวนการแปลงเลขที่อยู่ไอพีมาใช้ร่วมกัน จะก่อให้เกิดการเชื่อมต่อจำลองขึ้นระหว่างโฮสต์ต้นทางที่อยู่ภายในเครือข่ายกับโฮสต์ปลายทางที่อยู่บนอินเทอร์เน็ต แม้ว่าโฮสต์ทั้งคู่จะมีความทำงานและโต้ตอบสื่อสารกันเสมือนกำลังมีการเชื่อมต่อระหว่างทั้งคู่โดยตรงตามปกติ แต่แท้จริงนั้น เมื่อพิจารณาเลขที่อยู่ไอพีและพอร์ตที่กำลังใช้งานอยู่จะพบว่า โฮสต์ทั้งคู่กำลังสื่อสารผ่านเลขที่อยู่ไอพีและพอร์ตของไฟร์วอลล์อยู่ต่างหาก



รูป 9.6 การเชื่อมต่อโดยตรงระหว่างโฮสต์ภายในกับภายนอกแม้จะมีไฟร์วอลล์

รูป 10.6 แสดงให้เห็นถึงการเชื่อมต่อโดยตรงระหว่าง Host A (205.111.20.53) โดยใช้พอร์ต X (Client's port) ซึ่งอยู่ภายในเครือข่ายหลังไฟร์วอลล์กับ Host B (205.155.33.55) ซึ่งใช้พอร์ต Y (server's port) ซึ่งอยู่ภายนอกเครือข่าย ในกรณีเช่นนี้ ไฟร์วอลล์ยอมอนุญาตให้ทั้งคู่ทำการสื่อสารกันได้โดยตรงเพราะพิจารณาว่าเป็นทราฟฟิกปกติที่สอดคล้องกับค่าที่กำหนดไว้ใน Access rule ไฟร์วอลล์ไม่ได้ทำหน้าที่อำพรางทรัพยากรที่อยู่

ภายในเครือข่าย จึงไม่สามารถช่วยลดความเสี่ยงที่โฮสต์ภายนอกจะทำการบุกรุกโดยอาศัยข้อมูลจากโฮสต์ภายในที่กำลังติดต่อกันอยู่ได้ หรือมุ่งโจมตีไปยังโฮสต์ดังกล่าวได้ ตัวอย่างเช่น โฮสต์ภายในกำลังสนทนากับโฮสต์ของผู้ประสงค์ร้ายภายนอกผ่านโปรแกรมประเภท IRC (Internet Relay Chat) เช่น ICQ, MSN เป็นต้น โดยอาศัยข้อมูลที่โฮสต์ภายนอกมีอยู่อาจทำการโจมตีคู่สนทนาซึ่งเป็นโฮสต์ภายในเครือข่ายด้วยโปรแกรมประเภท Winnuke, Winfreeze, ICQBomb เป็นต้น จนเป็นเหตุให้โฮสต์ภายในบาดเจ็บหรือหยุดการทำงานได้



รูป 9.7 การแยกจากกันของโฮสต์โดยกระบวนการ NAT

รูป 9.7 แสดงให้เห็นถึงการใช้กระบวนการแปลงเลขที่อยู่ไอพีเข้ามาช่วยในการแปลงเลขที่อยู่ไอพีและพอร์ตต้นทางของ Host A (จาก 10.15.14.3 พอร์ต X) ไปเป็นเลขที่อยู่ไอพีและพอร์ตของไฟร์วอลล์เอง (205.112.20.55 พอร์ต T) ดังนั้น แพ็กเก็ตที่รับส่งระหว่างไฟร์วอลล์กับ Host A กับแพ็กเก็ตระหว่างไฟร์วอลล์กับ Host B จึงแตกต่างกันโดยทั้งคู่ยังสามารถสื่อสารกันได้ตามปกติ เนื่องจากการเชื่อมต่อระหว่างโฮสต์ทั้งคู่ไม่ได้ใช้เลขที่อยู่ไอพีและพอร์ตที่แท้จริง ดังนั้น โฮสต์ A จึงไม่สามารถนำข้อมูลของ Host B เพื่อย้อนกลับมาโจมตีมายังโฮสต์ B ในภายหลังได้ ลักษณะการใช้กระบวนการแปลงเลขที่อยู่ไอพีเข้ามาช่วยเช่นนี้ จะทำให้โฮสต์ปลายทางบน

อินเทอร์เน็ตไม่สามารถล่วงรู้สถานะที่แท้จริงของโฮสต์ต้นทางที่อยู่ภายในเครือข่ายได้ ถ้าโฮสต์บนอินเทอร์เน็ตเป็นโฮสต์ของผู้ประสงค์ร้าย โอกาสที่จะใช้ประโยชน์จากวิธีการเช่นนี้เพื่อนำไปใช้ในการบุกรุกภายหลังย่อมมีน้อยลง

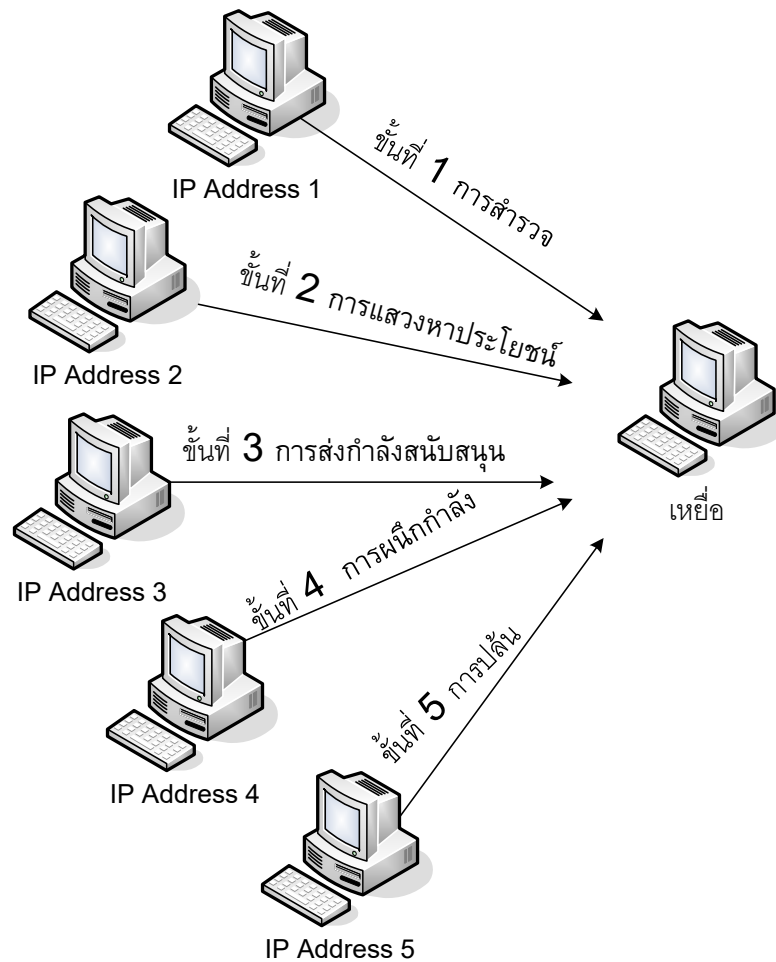
การออกแบบให้โฮสต์ภายในกับโฮสต์ภายนอกไม่สามารถติดต่อกันได้โดยตรงโดยอาศัยกระบวนการแปลงเลขที่อยู่ไอพีนี้ นอกเหนือจากจะช่วยอำพรางทรัพยากรที่อยู่ภายในเครือข่ายไม่ให้ตกเป็นเป้าหมายจากการโจมตีโดยตรงแล้ว ยังช่วยลดความเสี่ยงที่จะถูกบุกรุกหรือโจมตีจากผู้ประสงค์ร้ายภายนอกได้เป็นอย่างดี นอกจากนั้น ยังช่วยจำกัดขอบเขตความเสียหายที่เกิดขึ้นไม่ให้ลุกลามไปยังโฮสต์อื่นๆ ได้โดยง่าย ในงานวิจัยของเราจึงถือว่าการออกแบบเครือข่ายในลักษณะนี้เป็นส่วนหนึ่งของสถาปัตยกรรมของเรา

9.2 การวิเคราะห์การบุกรุกเครือข่ายจนทำให้เหยื่อสมยอม (Phases of compromise)

ถ้าเราต้องการตรวจจับการบุกรุกให้ได้ เราก็จำเป็นต้องทำความเข้าใจวิธีการที่จะทำให้เหยื่อสมยอม เพื่อจะได้เรียนรู้กระบวนการตั้งแต่ขั้นตอนเริ่มต้นสำรวจ แทรกซึม ไปจนกระทั่งสามารถทำให้เหยื่อตกอยู่ในอาณัติ เช่นเดียวกับถ้าตำรวจต้องการจับโจรปล้นทรัพย์ ตำรวจก็จำเป็นต้องทำความเข้าใจถึงขั้นตอนการปล้นทรัพย์ของโจร เพื่อวิเคราะห์ให้ทะลุถึงวิธีการคิดของโจร จากนั้นจึงวางแผนและออกแบบวิธีการจับโจร การทำความเข้าใจกระบวนการโจมตีในเรื่องนี้ก็เช่นกัน วิธีการที่ผู้บุกรุกจะเข้าถึงจนกระทั่งสามารถให้เหยื่อสมยอมแบ่งออกเป็น 5 ขั้นตอน ประกอบด้วย การสำรวจ (Reconnaissance), การแสวงหาประโยชน์ (Exploitation), การส่งกำลังสนับสนุน (Reinforcement), การผนึกกำลัง (Consolidation) และการปล้น (Pillage) รูป 10.8 แสดงให้เห็นถึงเวลาและโอกาสที่เราสามารถตรวจพบผู้บุกรุกในระหว่างที่ผู้บุกรุกกำลังโจมตีเหยื่อ ขั้นตอนทั้ง 5 สามารถสรุปได้ดังนี้

ขั้นตอนที่ 1 การสำรวจ

เป็นกระบวนการตรวจตราการเชื่อมต่อและจำนวนของโฮสต์, จำนวนและประเภทของบริการ และตรวจสอบเพื่อหาช่องโหว่ของแอปพลิเคชัน ในขั้นตอนนี้ ผู้บุกรุกจะพยายามสำรวจเหยื่อเป้าหมายเพื่อจะรู้ว่าโฮสต์อยู่จำนวนเท่าใด, ใช้เลขไอพีใด, เป็นโฮสต์ที่มีเจ้าของ (เครื่องคอมพิวเตอร์ของผู้ใช้) หรือเป็นเครื่องที่ไม่มีใครเป็นเจ้าของ (เครื่องแม่ข่ายให้บริการต่างๆ), เปิดใช้ตลอดเวลาหรือชั่วคราว, ใช้ซอฟต์แวร์ระบบปฏิบัติการรุ่นใด, ดำเนินงานแอปพลิเคชันใดบ้าง, เปิดพอร์ตสำหรับบริการใดบ้าง เป็นต้น วิธีการสำรวจในขั้นนี้ผู้บุกรุกอาจใช้เครื่องมือประเภทสแกนพอร์ตหรือสแกนเครือข่าย เมื่อผู้บุกรุกรวบรวมข้อมูลที่สามารถได้จากนั้นจะได้ใช้เครื่องมือในการโจมตีช่องโหว่หรือจุดอ่อนได้สอดคล้องกับระบบที่เหยื่อมีอยู่



รูป 9.8 ขั้นตอนการบุกรุกจนทำให้เหยื่อสมยอม

ขั้นตอนที่ 2 การแสวงหาประโยชน์

เป็นกระบวนการใช้ช่องโหว่ในทางที่ผิด, การปรับเปลี่ยน หรือทำให้บริการของเหยื่อใช้การไม่ได้ ขั้นตอนนี้ถือเป็นการแทรกซึมไปยังเครื่องของเหยื่อ การใช้ประโยชน์จากช่องโหว่หมายถึงการใช้ประโยชน์ในทางที่ผิดจากบริการที่เกี่ยวข้องเสมือนกับการใช้งานอย่างถูกขั้นตอน อย่างเช่นการบันทึกเข้า (Log on) เครื่องแม่ข่าย ให้บริการของเหยื่อเป้าหมายผ่านทาง TelNet, Secure Shell หรือ Microsoft Terminal Service โดยใช้ชื่อบัญชีผู้ใช้และรหัสผ่านที่ขโมยมาจากระบบอื่น ส่วนการปรับเปลี่ยน หมายถึง การเข้าไปปรับเปลี่ยนสิทธิ์ กฎเกณฑ์ หรือ แก๊ซรหัสในโปรแกรมเพื่อให้ตนเองมีสิทธิ์ใช้อย่างสมบูรณ์ ส่วนการหยุดบริการหมายถึง การทำให้บริการที่เหยื่อ

กำลังดำเนินอยู่หยุดไป ปรับเปลี่ยนลำดับ จนส่งผลให้บริการดังกล่าวของเหยื่อใช้การไม่ได้ เช่น อาจเข้าไปปิดบริการการตรวจหาหนอนหรือไวรัสของเครื่อง

ขั้นตอนที่ 3 การส่งกำลังสนับสนุน

เป็นขั้นตอนที่จะพยายามสร้างความแข็งแกร่งให้กับผู้บุกรุก โดยการเพิ่มขีดความสามารถของตนในขณะที่แฝงตัวอยู่บนเหยื่อ เช่น เพิ่มสิทธิ์ในการเข้าถึงทรัพยากรสำคัญ เลื่อนระดับสิทธิ์ในโหมดที่สูงขึ้น ใช้เหยื่อปิดบังอำพรางตัวผู้บุกรุก รวมทั้งทำให้เหยื่อกลายเป็นแหล่งช่องสุ่มโปรแกรมประสงค์ร้ายโดยการสร้างประตูลับ (Back door) ไว้ที่เครื่องของเหยื่อ เพื่อจะใช้ประโยชน์ในภายหลัง

ขั้นตอนที่ 4 การฉีกกำลัง

เป็นขั้นตอนที่เกิดขึ้นเมื่อผู้บุกรุกสื่อสารกับเครื่องแม่ข่ายของเหยื่อผ่านทางประตูลับ แล้วใช้เหยื่อเป็นฐานในการดักฟังทราฟฟิกของการติดต่อระหว่างเครื่องข่ายกับเครื่องอื่นๆ หรือใช้เหยื่อเป็นฐานในการแพร่รหัสประสงค์ร้าย รวมทั้งใช้เป็นฐานในการโจมตีเครื่องอื่นๆ ได้ ทำให้เหยื่อกลายเป็นเครื่องผีดิบ (Zombie machine) ผู้บุกรุกจะพยายามสื่อสารกับเครื่องผีดิบเครื่องอื่นๆ ที่อยู่บริเวณเดียวกันหรืออาจอยู่ต่างเครือข่ายเพื่อประเมินกำลังว่าจะสามารถรวบรวมให้เครื่องเหล่านี้เป็นฐานในการโจมตีอย่างประสงค์ร้ายกับเหยื่อที่เป็นเป้าหมายได้เพียงพอหรือไม่ การสื่อสารระหว่างเครื่องผีดิบเหล่านี้อาจถูกปกปิดหรือตรวจสอบไม่ได้ด้วยระบบการป้องกันที่เหยื่อมีอยู่ เนื่องจากผู้บุกรุกจะใช้ช่องทางสื่อสารผ่านประตูลับ

ขั้นตอนที่ 5 การปล้น

คือการกระทำในขั้นสุดท้ายตามความประสงค์ของผู้บุกรุก อาจเป็นการขโมยข้อมูลสำคัญ, ทำการโจมตีเหยื่อ หรือสั่งการให้โจมตีเครื่องเป้าหมายอื่นตามที่กำหนดไว้โดยใช้เหยื่อเป็นฐานในการโจมตี, หยุดการทำงานของเหยื่อ, ทำลายทรัพยากรสำคัญของเหยื่อ หรืออาจทำให้องค์กรทั้งหมดของเหยื่อได้รับความเสียหาย เป็นต้น

เมื่อทำความเข้าใจขั้นตอนและกิจกรรมต่างๆ ของการโจมตีได้แล้ว จะทำให้เราสามารถออกแบบระบบตรวจหาการบุกรุกให้สามารถรับมือ, ตรวจพบ, วิเคราะห์, และทำการโต้ตอบการบุกรุกในแต่ละขั้นตอนเหล่านี้ได้โดยง่าย

9.3 แบบจำลองภัยคุกคาม

แบบจำลองภัยคุกคาม (Threat model) หรือรูปแบบการโจมตี (attack model) คือรูปแบบหรือคุณลักษณะของภัยคุกคามแบบต่างๆ ที่สามารถสร้างความเสียหายต่อทรัพยากรของระบบ เราจะสามารถรับมือกับการโจมตีเหล่านี้ได้ก็ต่อเมื่อเรารู้จักรูปแบบของการโจมตีประเภทต่างๆ ได้ เพื่อทำความเข้าใจต่อธรรมชาติของผู้โจมตีและคุณลักษณะของเป้าหมายที่ตกเป็นเหยื่อของการโจมตี เพื่อที่จะได้ออกแบบให้ระบบตรวจหาการบุกรุกสามารถทำการตรวจตราเพื่อเฝ้าระวังการโจมตีได้อย่างถูกต้องและครบถ้วน เราสามารถจัดหมวดหมู่ของผู้โจมตีออกเป็น 4 ประเภท (Class) ได้แก่

10.3.1 ผู้โจมตีภายนอกที่ทำการบุกรุกจากอินเทอร์เน็ต (class 1)

10.3.2 ผู้โจมตีภายนอกที่ทำการบุกรุกจาก Wireless segment (class 2)

10.3.3 ผู้โจมตีภายในที่ทำการบุกรุกจาก Wired LAN (class 3)

10.3.4 ผู้โจมตีภายในที่ทำการบุกรุกจาก Wireless segment (class 4)

เมื่อสามารถจัดหมวดหมู่ของผู้โจมตีได้ดังกล่าวแล้ว ก็ง่ายต่อการแบ่งเครือข่ายออกเป็นสองส่วนโดยอาศัยไฟร์วอลล์ และจัดวางตัวตรวจจับไว้ในตำแหน่งที่เหมาะสมเพื่อทำหน้าที่กรอง ตรวจสอบ และวิเคราะห์การบุกรุกของผู้โจมตีประเภทต่างๆ ได้ง่าย

9.3.1 โฮสต์ในเครือข่าย

โฮสต์ภายในเครือข่ายสามารถแบ่งออกเป็น 2 ประเภท ได้แก่ โฮสต์ที่ไว้วางใจได้ (Trusted host) และโฮสต์ที่ไว้วางใจไม่ได้ (Untrusted host)

9.3.1.2 โฮสต์ที่ไว้วางใจได้

หมายถึง โฮสต์ที่เราสามารถไว้วางใจได้ สามารถรู้ได้ว่า ผู้ใช้เป็นใคร เป็นโฮสต์ที่มีการควบคุมและป้องกันการใช้งานเป็นอย่างดี โดยส่วนใหญ่หมายถึงคอมพิวเตอร์ที่อยู่ภายในองค์กร ซึ่งเครื่องคอมพิวเตอร์เหล่านี้จะมีเฉพาะผู้ใช้ภายในองค์กรเท่านั้นเท่านั้นที่มีสิทธิ์ใช้ มีการป้องกันเชิงกายภาพตามสมควร เช่น ติดตั้งอยู่ในบริเวณที่อนุญาตให้เฉพาะพนักงานที่มีสิทธิ์เท่านั้น แม้ว่าโฮสต์เหล่านี้อาจมีความเสี่ยงที่จะถูกใช้งานโดยบุคคลอื่น แต่ก็จัดได้ว่ามีความเสี่ยงอยู่ในระดับต่ำ เนื่องจากมีการควบคุมในระดับกายภาพ (Physical control) อยู่แล้วในระดับหนึ่ง และหากเกิดเหตุการณ์ใดขึ้นมา ก็สามารถติดตามผู้ที่ใช้งานโฮสต์ประเภทนี้ได้ไม่ยาก

9.3.1.3 โฮสต์ที่ไว้วางใจไม่ได้

หมายถึง โฮสต์ที่เราไม่สามารถไว้วางใจได้ โดยไม่สามารถล่วงรู้ได้ว่าผู้ใช้โฮสต์ประเภทนี้เป็นใคร อยู่ที่ไหน มีวัตถุประสงค์ใด ไม่สามารถล่วงรู้ได้ว่าใครเป็นเจ้าของโฮสต์นี้ และโฮสต์เหล่านี้มีการป้องกันความเสี่ยงในระดับใด โดยทั่วไปหมายถึงโฮสต์ใดๆ ที่อยู่บนอินเทอร์เน็ต ซึ่งอาจเป็นโฮสต์ที่อยู่ตามบริเวณมหาวิทยาลัย ผู้ใช้ตามบ้าน ผู้ใช้จากร้านให้บริการอินเทอร์เน็ตสาธารณะ อาจเป็นโฮสต์ของผู้ประสงค์ร้ายหรือไม่ก็ได้ เมื่อเกิดเหตุการณ์ขึ้น ก็มีความยากลำบากหรือไม่สามารถติดตามหาว่าใครเป็นเจ้าของโฮสต์ หรือใครคือผู้ก่อเหตุการณ์โดยอาศัยโฮสต์ดังกล่าวได้

หากบุกรุกได้อาศัยโฮสต์ประเภทที่ไว้วางใจไม่ได้เหล่านี้เป็นฐานในการโจมตีเหยื่อที่ตกเป็นเป้าหมาย แม้จะสามารถค้นหาได้ว่าการโจมตีดังกล่าวมาจากโฮสต์ใด แต่ก็ยากที่จะสืบสาวติดตามว่าใครเป็นผู้บุกรุกตัวจริง

การที่เราสามารถล่วงรู้ได้ว่าผู้ใช้เป็นใครนี้เองทำให้โฮสต์เหล่านี้จัดอยู่ในประเภทโฮสต์ที่ไว้วางใจไม่ได้ ซึ่งยากต่อการคาดเดาว่าผู้ที่จะกระทำการการใดต่อเครือข่ายของเรา อาจเข้ามาใช้งานตามปกติ หรืออาจเข้ามาด้วยวัตถุประสงค์ร้ายก็ได้

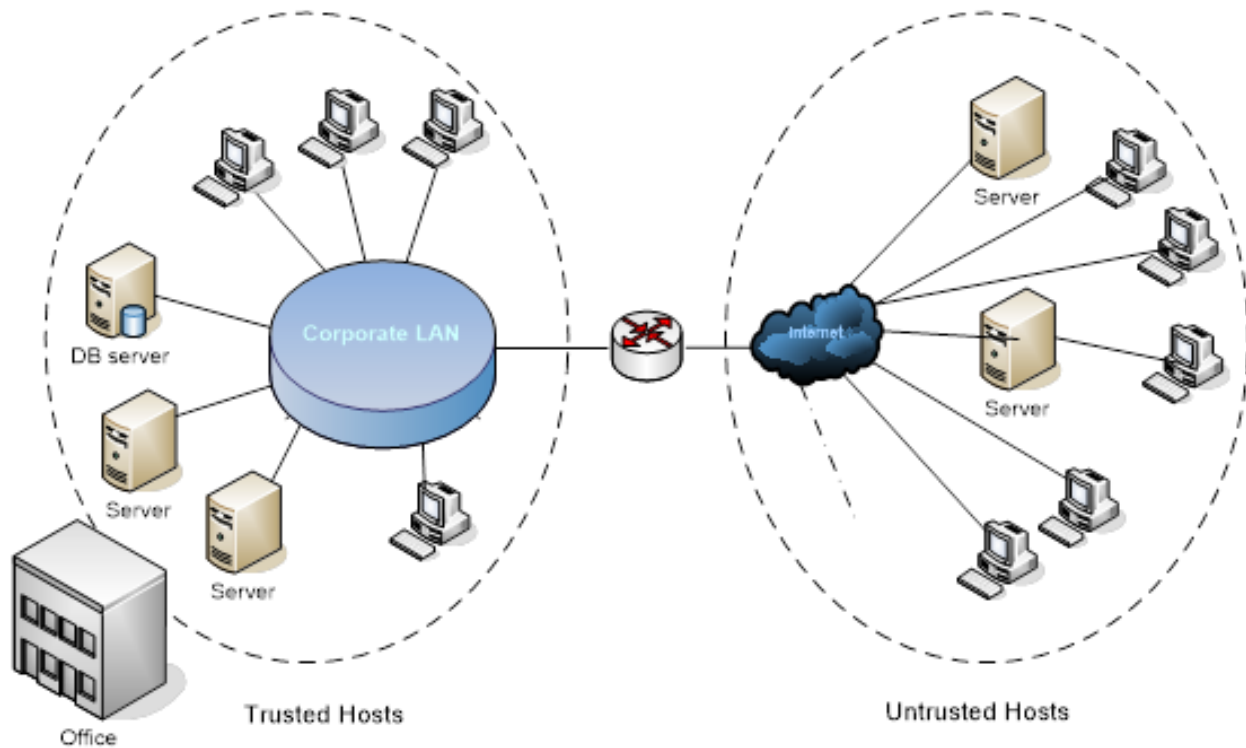
หลักเบื้องต้นของการรักษาความปลอดภัยคือ ให้ทำการประเมินว่า สถานการณ์ที่เลวร้ายที่สุดที่จะเกิดขึ้นจากโฮสต์เหล่านี้ที่มีผลกระทบต่อเครือข่ายของเรามีอะไรบ้าง มีความรุนแรงมากน้อยแค่ไหน เกิดขึ้นได้ยากง่ายเพียงใด เพื่อใช้เป็นฐานในการสร้างระดับการป้องกันให้เหมาะสม วิธีการเช่นนี้จะช่วยให้โอกาสหรือความเสี่ยงที่จะเกิดปัญหาได้ถูกทำให้ลดน้อยลงไปด้วยมาตรการเชิงป้องกันดังกล่าว

แม้พบว่า โฮสต์ที่ไว้วางใจไม่ได้ถือเป็นโฮสต์ประเภทที่เครือข่ายของเราไม่ควรติดต่อด้วย และไม่ควรอนุญาตให้มีการเชื่อมต่อเข้าโฮสต์ประเภทที่ไว้วางใจได้ก็ตาม แต่ในสภาพการใช้งานจริง เราไม่อาจตัดขาดจากการติดต่อกับเครือข่ายภายนอก ปัจจุบันองค์กรส่วนใหญ่ที่เครือข่ายก็ย่อมมีความจำเป็นที่จะต้องเชื่อมต่อกับอินเทอร์เน็ตทั้งแบบตลอดเวลาและแบบครั้งคราวเพื่ออนุญาตให้พนักงานเข้าถึงข้อมูลบนอินเทอร์เน็ต หรือองค์กรอาจมีเว็บไซต์เพื่อเผยแพร่ข่าวสาร, ให้บริการไปรษณีย์อิเล็กทรอนิกส์ หรือบริการธุรกรรมทางแบบพาณิชย์อิเล็กทรอนิกส์ ซึ่งเป็นการเปิดรับการติดต่อจากโฮสต์ภายนอกโดยตรง จึงเป็นไปได้ที่เครือข่ายของเราจะปฏิเสธการเชื่อมต่อกับโฮสต์ที่ไว้วางใจไม่ได้โดยสิ้นเชิง นอกจากนั้น โฮสต์ที่ไว้วางใจไม่ได้เหล่านั้น ย่อมไม่ใช่โฮสต์ของผู้บุกรุกด้วยประสงค์ร้ายทุกกรณีไป

ด้วยเหตุนี้ จึงมีความจำเป็นที่ต้องยอมให้มีการเชื่อมต่อระหว่างโฮสต์ที่ไว้วางใจได้เข้ากับโฮสต์ที่ไว้วางใจไม่ได้ โดยมีวิธีเฝ้าระวังและควบคุมความปลอดภัยในระดับและตำแหน่งที่เหมาะสม

เมื่อจำแนกโฮสต์ออกเป็น 2 ประเภทดังกล่าวแล้วแล้วในเบื้องต้น เราจะใช้ไฟร์วอลล์ในการแยกโฮสต์ทั้งสองประเภทออกจากกัน และเราสามารถออกแบบเครือข่ายให้แยกโฮสต์ทั้งสองประเภทออกจากกันได้ดังรูป 10.9 โดยอาศัยเราเตอร์เป็นอุปกรณ์ที่ยอมให้โฮสต์ทั้งสองส่วนสามารถติดต่อกันได้เสมือนอยู่บนเครือข่ายเดียวกัน

เพื่อความปลอดภัย เราจะออกแบบให้แบ่งแยกกลุ่มของโฮสต์ที่ไว้วางใจได้เป็นเครือข่ายภายในออกจากกลุ่มของโฮสต์ที่ไว้วางใจไม่ได้เป็นเครือข่ายภายนอกออกจากกัน โดยอาศัยอุปกรณ์ประเภทไฟร์วอลล์ เพื่อควบคุมการสื่อสารระหว่างเครือข่ายทั้งภายในกับภายนอกให้อยู่ภายใต้กฎเกณฑ์ความปลอดภัย ในขณะที่เครือข่ายทั้งภายในและภายนอกยังคงสามารถติดต่อสื่อสารกันได้ตามวัตถุประสงค์เดิมดังแสดงในรูป 9.9



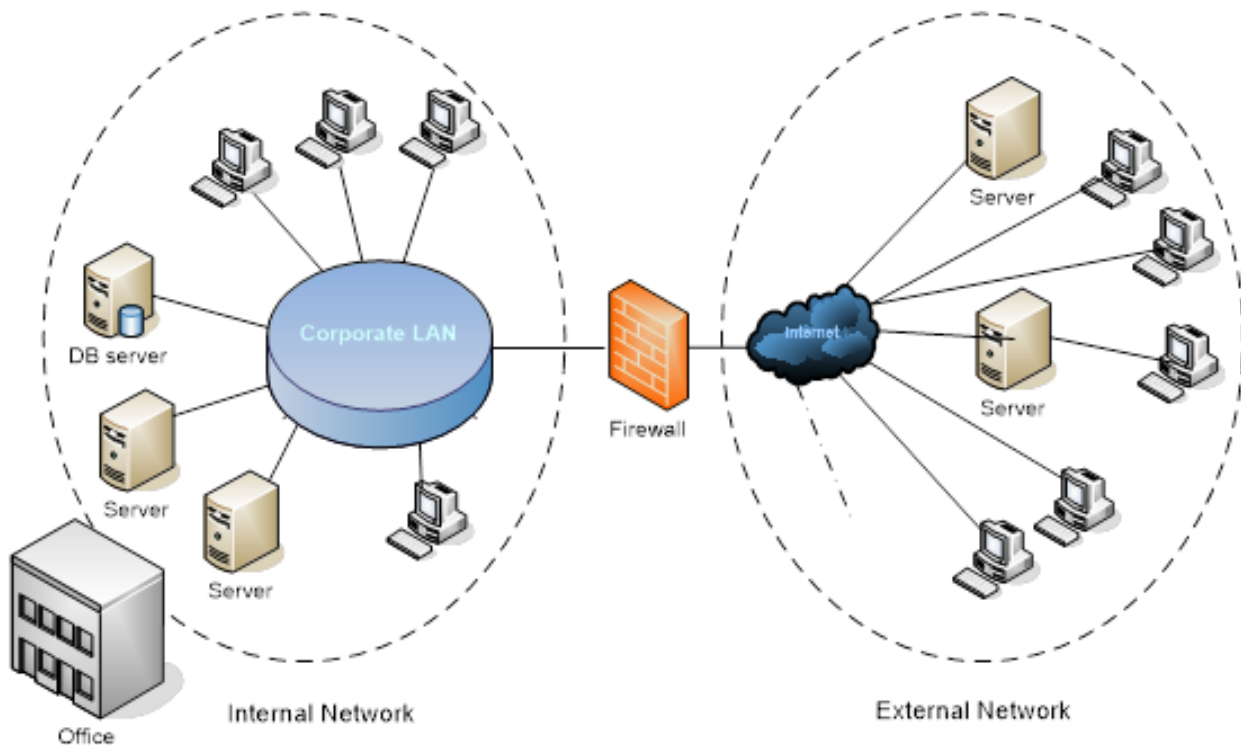
รูป 9.9 โฮสต์ที่ไว้วางใจได้กับโฮสต์ที่ไว้วางใจไม่ได้จำเป็นต้องเชื่อมต่อเข้าด้วยกัน

9.4 การแบ่งโซนเครือข่าย (Network zoning)

ในเบื้องต้น เราจะออกแบบโดยการแบ่งเครือข่ายออกเป็น 2 โซน ตามประเภทของโฮสต์ที่ไว้วางใจได้และโฮสต์ที่ไว้วางใจไม่ได้ ประกอบด้วย โซนเครือข่ายภายในและเครือข่ายภายนอก อย่างไรก็ตาม ยังมีโฮสต์อีก 2 ประเภทที่มีลักษณะแตกต่างไปจากโฮสต์ทั้งสองประเภทดังกล่าวข้างต้น ได้แก่ โฮสต์ประเภทที่มีความคล่องตัวไม่สามารถเจาะจงตายตัวว่าเป็นโฮสต์ภายในหรือโฮสต์ภายนอก และโฮสต์ที่เชื่อมต่ออยู่กับเครือข่ายไร้สาย ดังนั้น ในการออกแบบเครือข่าย เราจะแบ่งโซนของเครือข่ายออกเป็น 4 โซน รูป 10.10 ประกอบด้วย โซนเครือข่ายภายใน, โซนเครือข่ายภายนอก, DMZ และโซนไร้สาย

โซนเครือข่ายภายใน (Internal network zone) กำหนดให้มีเฉพาะโฮสต์ที่ไว้วางใจได้เท่านั้น เพราะการใช้งานภายในเครือข่ายนี้จะมีเฉพาะการใช้งานภายในองค์กรโดยบุคลากรภายในองค์กร และโฮสต์ทั้งหมดก็เป็นขององค์กร โซนนี้รองรับการใช้งานของเครือข่ายภายในองค์กรที่เรียกว่าอินทราเน็ต (Intranet)

โซนเครือข่ายภายนอก (External network zone) ประกอบด้วยโฮสต์อื่นๆ ที่ไม่ได้อยู่ภายในโซนเครือข่ายภายใน อาจเป็นโฮสต์ใดๆ ขององค์กรภายนอกที่เราติดต่อกับ หรือโฮสต์ต่างๆ ที่อยู่บนอินเทอร์เน็ต โซนนี้รองรับการใช้งานของอินเทอร์เน็ต



รูป 9.10 การแบ่งเครือข่ายภายในออกจากเครือข่ายภายนอกโดยใช้ไฟร์วอลล์

DMZ (Demilitarized Zone) หรือเขตปลอดทหาร หมายถึง โซนอีกประเภทหนึ่งที่ไม่ใช่ทั้งโซนเครือข่ายภายในและภายนอก แต่มีความจำเป็นต้องติดต่อและเชื่อมต่อเข้ากับทั้งเครือข่ายภายในและภายนอก โฮสต์ที่อยู่ในโซนนี้ต้องติดต่อโดยตรงทั้งกับโฮสต์ที่ไว้วางใจได้และโฮสต์ไว้วางใจไม่ได้ เช่น แม่ข่ายให้บริการไปรษณีย์ (Mail server), แม่ข่ายให้บริการเว็บ (Web server), แม่ข่ายให้บริการเอฟทีพี (FTP server) เป็นต้น ซึ่งโฮสต์เหล่านี้จำเป็นต้องให้บริการและติดต่อกับทั้งโฮสต์ภายนอกที่ไม่น่าไว้วางใจและโฮสต์ภายในที่ไว้วางใจได้ ดังนั้น เพื่อให้การแบ่งแยกโซนนั้นชัดเจนไม่คลุมเครือ โดยยังคงความปลอดภัยไว้ดังเดิมจึงจำเป็นต้องกำหนดเป็น DMZ ขึ้นมาเพื่อ

รองรับทั้งโฮสต์ที่ต้องสื่อสารโดยตรงกับทั้งเครือข่ายภายในและภายนอก เพื่อใช้เป็นแนวกันชนระหว่างโฮสต์ที่ไว้วางใจได้กับโฮสต์ที่ไว้วางใจไม่ได้

โซนไร้สาย (Wireless zone) โฮสต์ที่อยู่ภายในโซนไร้สายย่อมสามารถติดต่อสื่อสารกับโฮสต์ในเครือข่ายแบบมีสายได้ สามารถติดต่อกับทั้งโฮสต์ทั้งภายในเครือข่าย (อินทราเน็ต) และภายนอกเครือข่าย (อินเทอร์เน็ต) รวมทั้งโฮสต์ที่อยู่ภายใน DMZ ได้อีกด้วย การใช้มาตรการความปลอดภัยจึงจำเป็นต้องแตกต่างไปจากโฮสต์ที่อยู่ในโซนอื่นๆ โดยทั่วไป เราจะออกแบบมาตรการความปลอดภัยสำหรับโฮสต์ในโซนไร้สายนี้เช่นเดียวกับ โฮสต์ที่ไว้วางใจไม่ได้เช่นเดียวกับโฮสต์จากอินเทอร์เน็ต

การออกแบบโดยการแบ่งโฮสต์ที่ไว้วางใจได้ที่อยู่ในโซนของเครือข่ายภายในแยกออกจากโฮสต์ที่ไว้วางใจไม่ได้ในโซนเครือข่ายภายนอก แยกโฮสต์ที่คลุมเครือไปอยู่ในโซน DMZ และแยกโฮสต์ส่วนที่ไร้สายไปอยู่ในโซนไร้สาย ย่อมทำให้การกำหนดมาตรการเกี่ยวกับการรักษาความปลอดภัยเป็นได้โดยง่าย รัดกุม และมีประสิทธิภาพ

9.5 การจัดโซนเฝ้าระวัง (Monitoring zoning)

เพื่อให้มีความสามารถในการมองเห็นการโจมตีและเหยื่อเป้าหมายผู้ถูกโจมตี ในสถาปัตยกรรมนี้เราจะใช้แนวคิดของแบบอย่างของการเฝ้าระวัง (Monitoring platform) มาช่วยในการออกแบบเพื่อจัดวางการตรวจจับไว้ประจำแต่ละโซนโดยอาศัยตัวตรวจจับ โดยที่ตัวแทนตรวจจับ (Sensor agent) หรือเรียกสั้นๆ ว่า ตัวตรวจจับนั้นเป็นส่วนที่ใช้ในการรวบรวมและวิเคราะห์กราฟฟิคของเครือข่ายโดยมีวัตถุประสงค์เพื่อระบุถึงเหตุการณ์ที่น่าสงสัย

จากรูป 9.11 เป็นภาพแสดงเครือข่ายอย่างง่ายที่ใช้อยู่ในองค์กรขนาดกลาง ซึ่งมีทรัพยากรที่ครอบคลุมทั้ง 4 โซน เครือข่ายประกอบด้วยโซนเฝ้าระวัง 4 โซน โซนเฝ้าระวังจะเป็นตำแหน่งที่จะจัดวางตัวตรวจจับไว้ในบริเวณที่กราฟฟิคจะวิ่งผ่านเข้าและออกรวมกัน ในการจัดทรัพยากรของเครือข่ายไม่ว่าจะเป็นเครื่องแม่ข่าย โฮสต์ และอุปกรณ์ใดๆ ขององค์กรเข้าอยู่ในโซนใดจะขึ้นอยู่กับระดับของความไว้วางใจตามประเภทของโฮสต์เป็นสำคัญ โซนเฝ้าระวังจะแบ่งออกเป็น 4 โซนให้สอดคล้องกับการแบ่งโซนเครือข่ายที่อธิบายในหัวข้อก่อนหน้านี้ ซึ่งสามารถแบ่งขอบเขตหรืออาณาบริเวณของแต่ละโซนได้ดังนี้

9.5.1 โซนเครือข่ายภายนอก มีอาณาเขตตั้งแต่ external firewall interface ผ่านไปยัง boundary router ไปจนถึง Internet

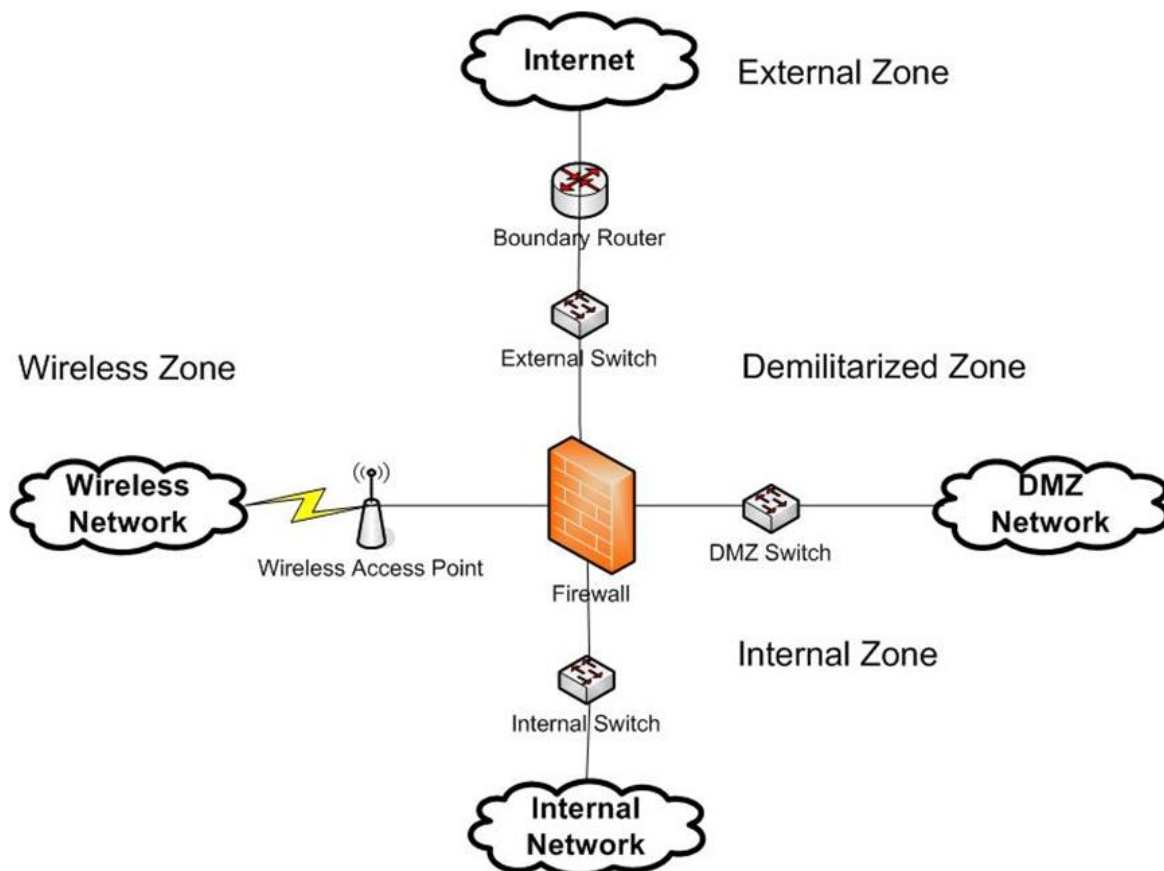
9.5.2 DMZ มีขอบเขตตั้งแต่ firewall DMZ interface รวมทั้งทุกโฮสต์ที่เชื่อมต่ออยู่กับ DMZ switch

9.5.3 โซนไร้สาย ประกอบด้วยอุปกรณ์และโฮสต์ทั้งหมดที่เชื่อมต่อเข้ากับ wireless

9.5.4 โซนเครือข่ายภายใน มีอาณาเขตครอบคลุมตั้งแต่ internal firewall interface รวมทั้งทุกโฮสต์ที่เชื่อมต่ออยู่ลงมาถึง internal switch

แต่ละโซนจะประกอบด้วยมาตรการที่สามารถรับมือกับผู้บุกรุกได้ทั้งภายในและจากภายนอก โดยปกติการกำหนดค่าที่เหมาะสมในอุปกรณ์ไฟร์วอลล์จะสามารถช่วยจำกัดขอบเขตความเสียหายที่เกิดขึ้นให้อยู่ภายในแต่ละโซนไม่ให้ส่งผลกระทบไปยังโซนอื่นๆ ได้โดยการจำกัดทราฟฟิกทั้งขาเข้า (Inbound traffic) ได้เช่นเดียวกับทราฟฟิกขาออก (outbound traffic) นอกจากนั้น ไฟร์วอลล์ยังสามารถควบคุมการบุกรุกทั้งจากภายนอกและภายใน (egress and ingress control)

การแบ่งเครือข่ายออกเป็นโซนดังกล่าวนี้ จะทำให้สามารถเฝ้าระวังและตรวจจับการบุกรุกจากผู้โจมตีทั้ง 4 ประเภท (Class 1-4) ดังที่กล่าวไว้ในหัวข้อแบบจำลองภัยคุกคาม นอกจากนั้น จะช่วยสนับสนุน security framework ที่ดี ช่วยให้การกำหนดค่าเกี่ยวกับ rule and security policy ให้สอดคล้องกับ traffic แต่ละโซนได้อย่างชัดเจนและรัดกุม ทำให้สามารถเฝ้าระวัง ตรวจสอบ และตรวจจับการบุกรุกได้อย่างไม่คลุมเครือ รูป 9.11



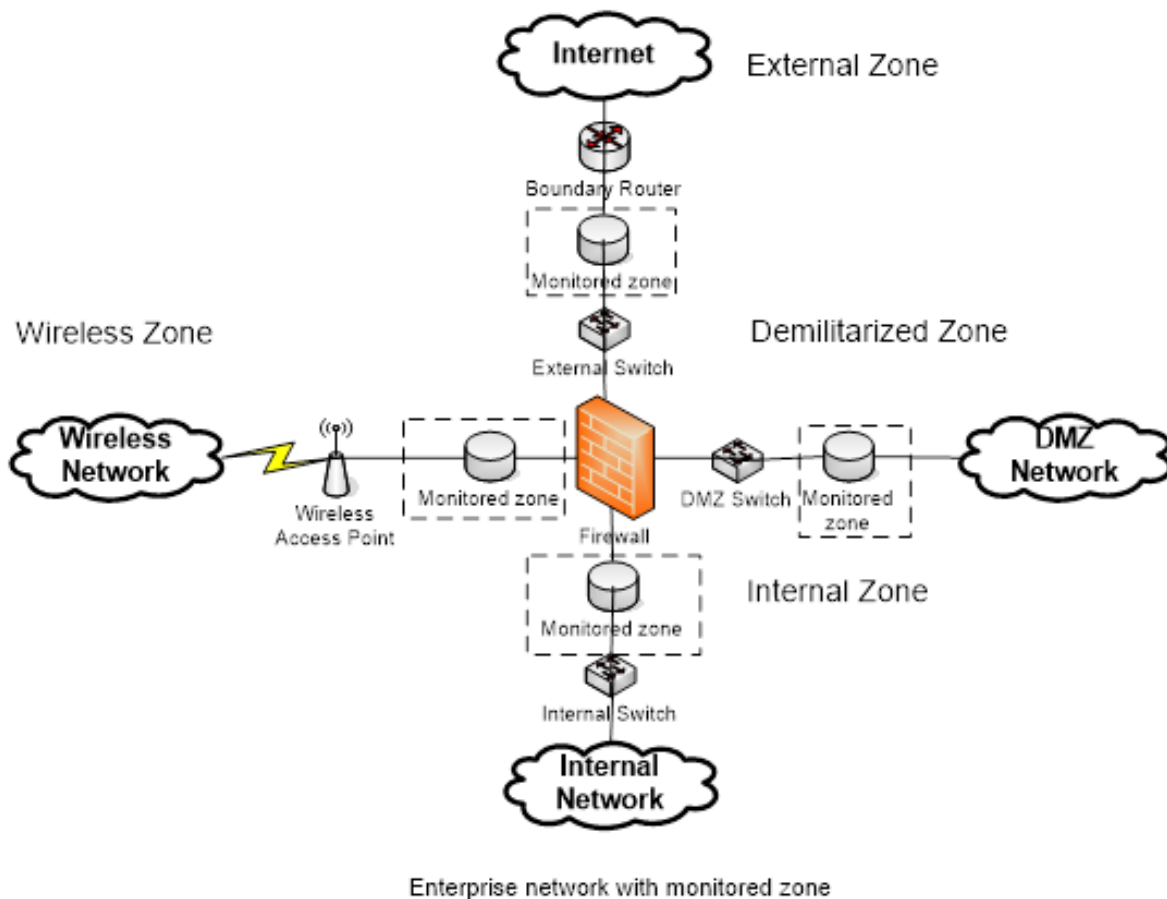
รูป 9.11 การแบ่งโซนเครือข่ายองค์กร

ตัวตรวจจับจะถูกติดตั้งไว้ในแต่ละโซนเพื่อรับมือกับการบุกรุกทั้ง 4 ประเภทดังแสดงในรูป 9.12 ได้ดังนี้

โซนเครือข่ายภายนอก

การวางตัวตรวจจับเพื่อเฝ้าระวังไว้ ณ โซนนี้ถือว่าเป็นตำแหน่งที่ดีที่สุดที่จะช่วยให้สามารถมองเห็นและรับมือกับผู้โจมตีภายนอกที่ทำการบุกรุกจากอินเทอร์เน็ต (Class 1) ที่มาจากอินเทอร์เน็ต เนื่องจากเป็นจุดเชื่อมต่อระหว่างภายในกับภายนอกที่ทราฟฟิกจะผ่านเข้าและออก ดังนั้น ตัวตรวจจับจะรับภาระที่หนักกว่าบริเวณอื่น

นอกจากนั้น การเฝ้าระวังในโซนนี้จะช่วยให้สามารถมองเห็นการโจมตีใดๆ ที่กระทำจากผู้บุกรุกภายนอกไปยังโซนไร้สาย, ไปยัง DMZ และไปยังโซนเครือข่ายภายในอีกด้วย แต่การเฝ้าระวังในโซนนี้จะไม่สามารถมองเห็นการโจมตีที่เกิดขึ้นจากผู้บุกรุกภายในของแต่ละโซน ได้แก่ การโจมตีที่เกิดขึ้นภายในโซนไร้สาย, การโจมตีที่เกิดขึ้นภายในโซน DMZ และการโจมตีที่เกิดขึ้นภายในโซนเครือข่ายภายใน ดังรูป 9.12



รูป 9.12 การแบ่งโซนเครือข่ายพร้อมกับตำแหน่งที่เฝ้าระวัง

การออกแบบเครือข่ายในโซนนี้ กำหนดให้ทราฟฟิกเข้าและออกต้องผ่านทางไฟร์วอลล์เท่านั้น จะไม่ยอมให้มีการติดต่อโดยตรงระหว่างโฮสต์ที่มาจากภายนอกเข้ากับโฮสต์ที่อยู่ภายในเครือข่ายได้โดยตรง และไม่สามารถมองเห็นเลขที่อยู่ที่แท้จริงของโฮสต์ภายในเครือข่ายขององค์กรด้วยการใช้ NAT เข้ามาช่วยกำหนดเลขที่อยู่ให้แยกกันระหว่างเลขที่อยู่ไอพีแบบสาธารณะ (Public IP address) กับเลขที่อยู่ไอพีแบบส่วนตัว (Private IP address) ส่วนการเชื่อมต่อระยะไกลด้วยวิธีการใดๆ ผ่านทาง RAS (Remote access service) จำเป็นต้องกำหนดให้ใช้ช่องทาง VPN เท่านั้น

DMZ

การเฝ้าระวังใน DMZ นี้จะสามารถมองเห็นผู้โจมตีภายนอกที่ทำการบุกรุกจากอินเทอร์เน็ต (class 1) ปกติภายใน DMZ จะประกอบไปด้วย แมชชีนให้บริการเมลล์, แมชชีนให้บริการระบบชื่อโดเมน (DNS server), เวย์บีพี, และแมชชีนอื่นๆ ตัวตรวจจับที่ถูกลงไว้ในโซนนี้จะรับภาระน้อยกว่าในโซนเครือข่ายภายนอก ดังนั้น การเฝ้าระวังในบริเวณนี้จึงทำให้สามารถตรวจพบกิจกรรมที่ผิดปกติที่เกิดขึ้นกับโฮสต์ที่อยู่ใน DMZ ได้โดยง่าย

โซนไร้สาย

โดยปกติ องค์กรอนุญาตให้มีการเชื่อมต่อกันระหว่างส่วนของเครือข่ายไร้สายเข้ากับส่วนของเครือข่ายมีสายภายในองค์กร ดังนั้น มาตรการความปลอดภัยที่จะนำมาใช้กับโฮสต์ภายในเครือข่ายไร้สายจะต้องใช้กฎเกณฑ์เดียวกับโฮสต์ที่อยู่บนอินเทอร์เน็ต เนื่องจากโฮสต์ที่อยู่ในโซนไร้สายจัดเป็นโฮสต์ที่ไว้วางใจไม่ได้ การใช้งานจากผู้ใช้อินเทอร์เน็ต ไม่ว่าจะเป็นพนักงานที่ใช้งานแบบระยะไกล (Remote connect) จากบ้าน หรืออาจเป็นลูกค้าทางธุรกิจ จะต้องถูกกำหนดให้มีการห่อหุ้มทราฟฟิกไว้ด้วยเครือข่ายส่วนเสมือน (VPN) ร่วมกับการพิสูจน์ตัวตนจริงด้วยระบบกุญแจสาธารณะ

ผู้บุกรุกจากภายนอกที่ทำการโจมตีโซนไร้สาย (Class 2) โดยอาศัยช่องโหว่ของการกำหนดค่าที่ไม่รัดกุมบนอุปกรณ์ไร้สาย ผวนกับระบบความปลอดภัยบนระบบไร้สายยังคงมีจุดอ่อนในปัจจุบัน ผู้บุกรุกภายนอกสามารถเข้าถึงหรือมองเห็นโฮสต์ภายในโซนไร้สายเสมือนกับเป็นโฮสต์ที่อยู่ในอินเทอร์เน็ต การเฝ้าระวังในบริเวณนี้จึงมีความจำเป็น

โซนเครือข่ายภายใน

อินเทอร์เน็ตประกอบไปด้วยทรัพยากรที่ไว้วางใจได้ทั้งหมดขององค์กร ดังนั้น ผู้ใช้จากอินเทอร์เน็ตจึงไม่ควรได้รับสิทธิ์ให้สามารถเข้าถึงทรัพยากรเหล่านี้ได้โดยตรงถ้ายังไม่ได้ผ่านระบบการพิสูจน์ตัวตนจริงก่อนเริ่มติดต่อ การเฝ้าระวังในโซนนี้ถือเป็นงานที่ยากอย่างยิ่งสำหรับตัวตรวจจับ เนื่องจากเป็นความพยายามในการรับมือกับผู้โจมตีภายในที่ทำการบุกรุกจาก Wired LAN (class 3) และผู้โจมตีภายในที่ทำการบุกรุกจาก Wireless segment (class 4)

การเฝ้าระวังในโซนนี้ สามารถทำได้ 2 วิธี วิธีแรก แบ่งทรัพยากรที่สำคัญของเครือข่ายจัดให้อยู่ในประเภททรัพยากรวิกฤติ (Critical asset) ซึ่งมักประกอบด้วย แม่ข่ายของระบบเงินเดือนและการเงิน ที่มีการป้องกันโดยใช้ไฟร์วอลล์ภายในที่จำเพาะเจาะจง โดยไฟร์วอลล์นี้จะกำหนดเงื่อนไขที่จำกัดการเข้าถึงโฮสต์ของงานการเงินอย่างเข้มงวด และมีตัวตรวจจับจะถูกวางไว้บริเวณนี้ด้วย ส่วนวิธีที่สอง ติดตั้งตัวตรวจจับแบบลูกผสม (Hybrid sensor) ที่สามารถตรวจตราได้ทั้งแบบเครือข่ายและแบบประจำโฮสต์

จากที่อธิบายไว้ในบทก่อนหน้านี้ เราสามารถสรุปรูปแบบการโจมตีทุกประเภทได้จากแบบจำลองการโจมตีออกเป็น 4 ประเภท ได้แก่ ผู้โจมตีภายนอกที่ทำการบุกรุกจากอินเทอร์เน็ต (class 1), ผู้โจมตีภายนอกที่ทำการบุกรุกจากส่วนเครือข่ายไร้สาย (class 2), ผู้โจมตีภายในที่ทำการบุกรุกจากเครือข่ายเฉพาะบริเวณแบบมีสาย (class 3) และผู้โจมตีภายในที่ทำการบุกรุกจากส่วนของเครือข่ายไร้สาย (class 4) ดังนั้น เราจึงสรุปรูปแบบการบุกรุกออกเป็น 2 กลุ่ม กลุ่มแรก คือการบุกรุกจากผู้บุกรุกภายนอกผ่านทางอินเทอร์เน็ตและเครือข่ายไร้สาย กลุ่มที่สองคือการบุกรุกจากผู้บุกรุกภายในผ่านเครือข่ายองค์กรและเครือข่ายไร้สาย ทั้งสองกลุ่มล้วนมีความประสงค์ร้ายต่อทรัพยากรขององค์กร

อย่างไรก็ตาม ด้วยการออกแบบเครือข่ายที่เหมาะสมและจัดวางอุปกรณ์ของระบบความปลอดภัยที่เหมาะสมตามข้อเสนอของหนังสือเล่มนี้ แม้ว่าเราจะสามารถมองเห็นช่องทาง (ว่ามาจากช่องทางใด), ทิศทาง (ในการโจมตี) และประเภทของผู้บุกรุกได้ (ใคร-ภายในหรือภายนอก) แต่เราไม่สามารถปิดช่องทางเหล่านี้ลงเพื่อไม่อนุญาตให้ผู้บุกรุกใช้ประโยชน์ได้ เนื่องจากเป็นช่องทางที่ผู้ใช้ปกติสามารถใช้งานได้ด้วย และเป็นไปไม่ได้ที่องค์กรจะไม่อนุญาตให้พนักงานภายในองค์กรใช้งานอินเทอร์เน็ตจากเครื่องภายในองค์กร

ดังนั้น การออกแบบเครือข่ายที่ปลอดภัย เราต้องกำหนดให้ช่องทางในการเข้าสู่เครือข่ายเพื่อเข้าถึงทรัพยากรเหล่านั้นถูกกำหนดไว้อย่างแน่นอนและจำกัด โดยแบ่งทรัพยากรเครือข่ายออกเป็น 4 โซน ประกอบด้วย โซนเครือข่ายภายใน, โซนเครือข่ายภายนอก, โซนไร้สาย และ DMZ แต่ละโซนมีการควบคุมช่องทางเข้าออกที่แน่นอนโดยอาศัยไฟร์วอลล์ควบคุมการไหลผ่านของทราฟฟิกทั้งขาเข้าและขาออก และกำหนดให้ทั้ง 4 โซนเป็นโซนเฝ้าระวัง และออกแบบให้ติดตั้งโฮสต์เฝ้าระวังไว้ในแต่ละโซนด้วย

ด้วยการออกแบบเครือข่ายที่เหมาะสมเช่นนี้ เราจึงตั้งสมมุติฐานว่า ไม่มีการบุกรุกประเภทใด ผ่านช่องทางใด และโดยใคร จะรอดพ้นสายตาเราไปได้ ระบบของเราสามารถ “มองเห็น” การบุกรุกที่เกิดขึ้นทุกช่องทางและ

ทุกเวลาได้อย่างแน่นอน โดยสมมุติฐานนี้ จึงอาจประกันได้ว่า ระบบเครือข่ายคอมพิวเตอร์ของคุณจะสามารถต้านทานจากการบุกรุกและสามารถอยู่รอดได้เมื่อถูกโจมตีได้เป็นอย่างดี

9.6 สรุปบท

เนื้อหาในบทนี้กล่าวถึงการออกแบบเครือข่ายที่มั่นคงปลอดภัย โดยแบ่งเครือข่ายออกเป็น 4 โซนหลัก และใช้มาตรการควบคุมผ่านไฟร์วอลล์ร่วมกับการติดตั้งโฮสต์เฝ้าระวังในแต่ละโซน เพื่อให้สามารถตรวจจับการโจมตีได้ทุกช่องทาง ทั้งนี้ ยังเน้นความสำคัญของการใช้แนวคิด Zero Trust และ Defense-in-Depth เพื่อรับมือกับภัยคุกคามสมัยใหม่และสร้างความปลอดภัยให้กับโครงสร้างพื้นฐานขององค์กร

9.7 บทวิเคราะห์และมุมมองเชิงวิชาการ: “การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (Secured Network Design)”

เอกสารคำสอนบทเรียน “การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย” ในรายวิชา **หลักการความมั่นคงทางไซเบอร์ (Cyber Security Principles)** ถือเป็นหัวใจของการเรียนการสอนด้าน Cybersecurity เพราะเป็นการผานองค์ความรู้ทางวิศวกรรมเครือข่ายเข้ากับการออกแบบเชิงสถาปัตยกรรมความมั่นคงปลอดภัยที่ตอบสนองต่อภัยคุกคามยุคใหม่ การออกแบบที่ดีไม่เพียงแค่ใช้เครื่องมือป้องกัน (firewall, IDS/IPS, VPN) เท่านั้น แต่ยังเป็นการจัดโครงสร้างเครือข่าย (network zoning, monitoring zoning) ให้สอดคล้องกับหลัก *CIA Triad* และสถาปัตยกรรมสมัยใหม่ เช่น Zero Trust และ Defense-in-Depth สรุปสาระสำคัญของการวิเคราะห์และมุมมอง ดังนี้

1) สังเคราะห์องค์ความรู้จากบทเรียน

เนื้อหาในบทเรียนนำเสนอองค์ประกอบสำคัญของการออกแบบเครือข่าย ได้แก่:

- **หลักการเบื้องต้น:** กำหนดอาณาเขตเครือข่าย, ให้ทราฟฟิกทั้งหมดผ่าน firewall, แยกโฮสต์ภายในกับโฮสต์ที่ให้บริการสาธารณะ (DMZ), และหลีกเลี่ยงการสื่อสารโดยตรงภายใน-ภายนอก
- **Threat Model & Phases of Compromise:** อธิบายขั้นตอนของการบุกรุกตั้งแต่ reconnaissance → exploitation → reinforcement → consolidation → pillage ทำให้นักศึกษาเข้าใจวงจรการโจมตี
- **Network & Monitoring Zoning:** การแบ่งเครือข่ายเป็นโซน (internal, external, DMZ, wireless) และจัดวางตัวตรวจจับ (sensors) เพื่อให้เห็นการโจมตีทั้งจากภายในและภายนอก
- **กิจกรรมการสอน:** Incident Response Drill (DDoS Attack), Case Study (SQL Injection), การเชื่อมโยงกับ Cybersecurity Framework

2) มุมมองเชิงวิชาการและความก้าวหน้าปัจจุบัน

1. จาก Perimeter Defense → Zero Trust แนวคิด perimeter firewall ที่ปรากฏในบทเรียนยังมีคุณค่า แต่ไม่เพียงพอในยุคที่มี cloud, SaaS, และ remote work แนวทาง Zero Trust Architecture

(ZTA) จึงเข้ามาเสริม โดยเน้น *identity-based access, continuous verification, least privilege* แทนการพึ่งพา “เขตแดนเดียว”

2. **Network Segmentation สู่ Micro-segmentation** การแบ่งโซน (DMZ, internal, external, wireless) ในบทเรียนคือรากฐานที่ดี แต่ปัจจุบันควรขยายสู่ micro-segmentation โดยใช้ SDN และ policy-based access control ที่ละเอียดถึงระดับ workload และ application
3. **Monitoring → Threat Hunting & AI-driven SOC** การวาง sensor ในแต่ละโซนช่วยให้มองเห็นทราฟฟิก แต่โลกปัจจุบันต้องเสริมด้วย behavioral analytics, AI-driven anomaly detection และ MITRE ATT&CK mapping เพื่อยกระดับจากการ “ตรวจจับ” ไปสู่การ “ล่าเชิงรุก” (threat hunting)
4. **Secure Remote Access & VPN Evolution** เนื้อหาเดิมเสนอให้ใช้ VPN ปกป้องช่องทางพิเศษ ซึ่งยังสำคัญ แต่ควรอัปเดตด้วย ZTNA (Zero Trust Network Access) และ SASE (Secure Access Service Edge) ที่ใช้ cloud-based security controls ผนวก SD-WAN

3) ประสบการณ์และการสอดแทรกเชิงการสอน

จากประสบการณ์ในวิชาชีพและวิจัย ผู้สอนเห็นว่า **การออกแบบเครือข่ายที่ดี คือการออกแบบเพื่อการตรวจจับ (Design for Visibility)** ไม่ใช่แค่การป้องกัน จึงเน้นการเรียนรู้ให้ผู้เรียนถูกฝึกให้คิดเชิงสถาปัตยกรรมตั้งแต่ต้น โดยสมมติว่า “ระบบถูกเจาะได้เสมอ” และเป้าหมายคือ **จำกัดความเสียหาย (Containment) และตรวจจับเร็วที่สุด (Early Detection)** วิธีคิดเช่นนี้ช่วยให้ผู้เรียนไม่เพียงแค่ท่องจำ แต่ยังเข้าใจวิธีวางระบบในโลกจริง

บท “การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย” เป็นรากฐานสำคัญที่ครอบคลุมทั้ง **principle, threat model, network zoning และ monitoring zoning** จุดแข็งคือการฝึกปฏิบัติและการเชื่อมโยงกับ cybersecurity framework อย่างไรก็ตาม เพื่อตอบโจทย์ยุค **Cloud, Zero Trust, และ AI-driven SOC** การสอนควรปรับไปสู่ **micro-segmentation, ZTNA/SASE, และ threat hunting** สิ่งเหล่านี้จะช่วยให้ผู้เรียนก้าวจาก “นักศึกษา” ไปสู่ “วิศวกรความมั่นคงปลอดภัย” ที่พร้อมทำงานในโลกจริง

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายหลักการออกแบบเครือข่ายที่สอดคล้องกับ CIA Triad

แนวคำตอบ: Confidentiality = ใช้ Firewall/VPN, Integrity = IDS/IPS ตรวจสอบการโจมตี, Availability = Network redundancy และการควบคุมทราฟฟิก

ข้อ 2. วิเคราะห์ขั้นตอนการบุกรุกเครือข่าย 5 ขั้นตอน

แนวคำตอบ: Reconnaissance, Exploitation, Reinforcement, Consolidation, Pillage

ข้อ 3. อธิบายความสำคัญของการแบ่งเครือข่ายเป็นโซน (Network Zoning)

แนวคำตอบ: ลดความเสี่ยง, ควบคุม Access Rule ได้ง่าย, จำกัดความเสียหายเมื่อเกิดการโจมตี

ข้อ 4. อธิบายบทบาทของ Firewall และ NAT ในการออกแบบเครือข่าย

แนวคำตอบ: Firewall = ควบคุมการเข้าออก, NAT = ซ่อน IP ภายใน, ลดโอกาสถูกโจมตีตรงๆ

ข้อ 5. เปรียบเทียบแนวคิด Perimeter Defense กับ Zero Trust Architecture

แนวคำตอบ: Perimeter Defense = เน้น Firewall รอบนอก, Zero Trust = identity-based access, continuous verification, least privilege

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. หลักการ “อย่าวางไข่ทุกฟองไว้ในตะกร้าใบเดียว” ใช้กับแนวคิดใด

ก. Defense-in-Depth

ข. Zero Trust

ค. Separate Design

ง. Threat Hunting

เฉลย: ค

ข้อ 2. ข้อใดคือขั้นตอนแรกของการบุกรุกเครือข่าย

ก. Exploitation

ข. Reconnaissance

ค. Reinforcement

ง. Pillage

เฉลย: ข

ข้อ 3. โซน DMZ มีหน้าที่ใด

ก. แยกโฮสต์ภายในออกจากภายนอก

ข. เป็นแนวกันชนระหว่างเครือข่ายภายในกับภายนอก

ค. ใช้เก็บข้อมูลลับ

ง. ใช้เข้ารหัสข้อมูลทั้งหมด

เฉลย: ข

ข้อ 4. การใช้ NAT มีประโยชน์อย่างไร

ก. เพิ่ม Bandwidth

ข. ปกปิดที่อยู่จริงของโฮสต์ภายใน

ค. ทำให้การโจมตีง่ายขึ้น

ง. ใช้แทน Firewall ได้

เฉลย: ข

ข้อ 5. Firewall จะทำงานได้มีประสิทธิภาพเมื่อใด

ก. เมื่อทราฟฟิกทั้งหมดผ่าน Firewall

ข. เมื่อมี IDS เพียงอย่างเดียว

ค. เมื่อใช้ NAT ร่วมด้วย

ง. เมื่อใช้ VPN เท่านั้น

เฉลย: ก

ข้อ 6. Threat Model แบ่งผู้โจมตีออกเป็นกี่ประเภทหลัก

ก. 2

ข. 3

ค. 4

ง. 5

เฉลย: ค

ข้อ 7. ข้อใดไม่ใช่โซนหลักในการออกแบบเครือข่ายที่ปลอดภัย

ก. DMZ

ข. Wireless Zone

ค. Public Zone

ง. Internal Zone

เฉลย: ค

ข้อ 8. IDS/IPS มีบทบาทหลักในเครือข่ายอย่างไร

ก. ป้องกันการบุกรุกเชิงกายภาพ

ข. ตรวจจับและป้องกันการโจมตีในเครือข่าย

ค. เข้ารหัสข้อมูลก่อนส่ง

ง. จัดการ Bandwidth

เฉลย: ข

ข้อ 9. Zero Trust Architecture เน้นหลักการใด

ก. เชื่อถือทุกสิ่งภายในระบบ

ข. การตรวจสอบอย่างต่อเนื่องและ least privilege

ค. ใช้ Firewall ภายนอกเพียงอย่างเดียว

ง. การแบ่ง VLAN

เฉลย: ข

ข้อ 10. Defense-in-Depth หมายถึงอะไร

ก. ใช้เครื่องมือป้องกันเพียงชั้นเดียว

ข. การใช้มาตรการหลายชั้นเพื่อเพิ่มความปลอดภัย

ค. การใช้ NAT เพื่อป้องกันการบุกรุก

ง. การใช้ DMZ ในการออกแบบเครือข่าย

เฉลย: ข

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ. (ม.ป.ป.). *การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (Secured Network Design)*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Cisco Systems. (2021). *Network Security Design Guide*.

Gartner. (2021). *Market Guide for Secure Access Service Edge (SASE)*.

Kindervag, J. (2010). *No More Chewy Centers: Introducing Zero Trust*. Forrester Research.

NIST. (2020). *Zero Trust Architecture (SP 800-207)*.

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*.

MITRE. (2023). *ATT&CK Framework for Enterprise*.

Stallings, W. (2021). *Foundations of Security Architecture*. Pearson.

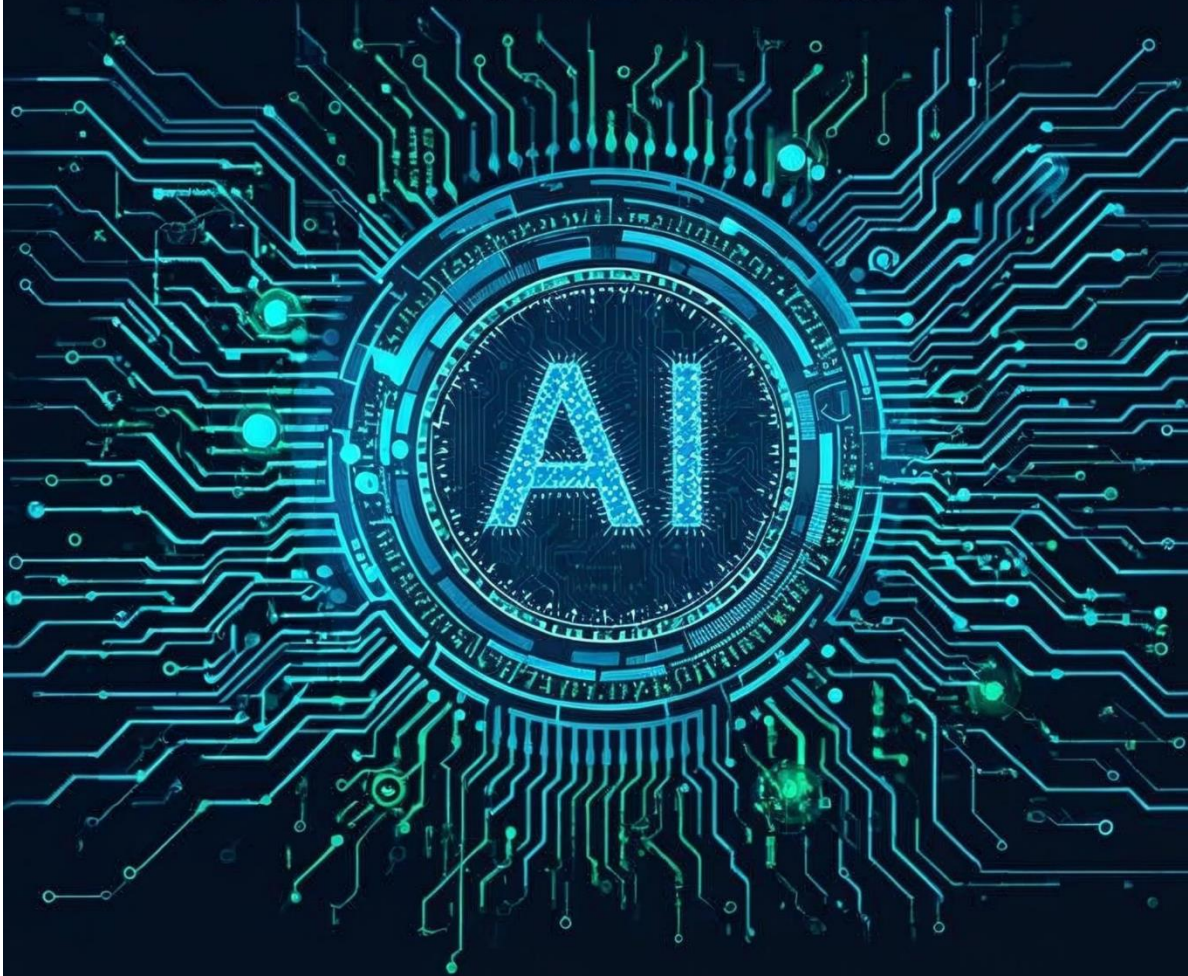
บทที่ 10

เครือข่ายไร้สาย

Wireless Network

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพรธีรัตน์

บทที่ 10 เครือข่ายไร้สาย (Wireless Network)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบบทนี้ นักศึกษาจะสามารถ:

- 1) อธิบายประเภทของเครือข่ายไร้สาย (WPAN, WLAN, WMESH, WMAN, WWAN, Cellular) ได้
- 2) อธิบายมาตรฐาน IEEE 802.11 และวิวัฒนาการของ Wi-Fi (4-7) ได้
- 3) วิเคราะห์ข้อดี-ข้อจำกัดของเครือข่ายไร้สายเทียบกับเครือข่ายแบบใช้สายได้
- 4) ประเมินความมั่นคงปลอดภัยของการเชื่อมต่อไร้สายและมาตรการป้องกันได้
- 5) ประยุกต์ใช้ความรู้ในการออกแบบการเชื่อมต่อไร้สายที่มีประสิทธิภาพและปลอดภัยในสถานการณ์จริงได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบบทนี้ นักศึกษาจะสามารถ:

- 1) ระบุและอธิบายองค์ประกอบและกระบวนการสื่อสารไร้สายได้
- 2) จำแนกและเปรียบเทียบประเภทเครือข่ายไร้สายและมาตรฐาน IEEE 802.11 ได้
- 3) อธิบายโหมดการเชื่อมต่อ WLAN (Infrastructure vs Ad-Hoc) ได้
- 4) วิเคราะห์ความเสี่ยงด้านความปลอดภัยของ WLAN และ Wi-Fi Hotspot ได้
- 5) เสนอแนวทางการออกแบบ WLAN สำหรับองค์กรโดยคำนึงถึงประสิทธิภาพและความปลอดภัยได้

3. หัวข้อเนื้อหา:

10.1 ประเภทของเครือข่ายไร้สาย

10.1.1 แพนไร้สาย (WPAN)

10.1.2 เครือข่ายเฉพาะกิจแบบไร้สาย (WMESH)

10.1.3 แมนไร้สาย (WMAN)

10.1.4 แวนไร้สาย (WWAN)

10.1.5 เครือข่ายเซลลูลาร์ (Cellular Network)

10.1.6 เครือข่ายเฉพาะบริเวณไร้สาย (WLAN)

10.1.7 เปรียบเทียบมีสายกับไร้สาย (Wired vs Wireless)

10.2 การเชื่อมต่อเครือข่ายและมาตรฐาน IEEE 802.11 WLAN

10.2.1 โหมดโครงสร้างพื้นฐาน

10.2.2 โหมด Ad-Hoc หรือ Peer-to-Peer

10.2.3 เทคโนโลยี Wi-Fi มาตรฐาน IEEE 802.11

10.2.4 วิวัฒนาการของมาตรฐาน IEEE 802.11

10.2.5 สรุปมาตรฐาน IEEE 802.11

4. กิจกรรมการเรียนรู้ (กรณีศึกษา)

กรณีศึกษา:

บริษัท *RMUTT SmartOffice Solutions* ให้บริการพื้นที่ทำงานร่วม (Co-working Space) ซึ่งมีผู้ใช้บริการจำนวนมาก เชื่อมต่อ Wi-Fi ผ่าน Access Point เดียวโดยไม่มีการเข้ารหัส WPA2/3 ส่งผลให้มีความเสี่ยงต่อการถูกดักฟังข้อมูล (Sniffing) และการโจมตี Man-in-the-Middle นักศึกษาต้องช่วยวิเคราะห์และออกแบบ WLAN ใหม่ที่มีความปลอดภัยมากขึ้น

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

1. วิเคราะห์ปัญหาและความเสี่ยงจากการออกแบบ WLAN ปัจจุบัน
2. ศึกษาและเสนอการใช้มาตรฐาน IEEE 802.11 รุ่นใหม่ (เช่น Wi-Fi 6/7)
3. เสนอวิธีการป้องกัน เช่น WPA3, การแบ่ง VLAN, Captive Portal, Firewall
4. จัดทำผังเครือข่ายและนำเสนอแนวทางแก้ไข

ประเด็นการเรียนรู้:

- ประเภทเครือข่ายไร้สาย (WPAN, WLAN, WWAN ฯลฯ)
- มาตรฐาน IEEE 802.11 และวิวัฒนาการ Wi-Fi
- โหมด Infrastructure vs Ad-Hoc
- มาตรการด้านความปลอดภัยของ Wi-Fi (WEP → WPA2 → WPA3)

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ปัญหา (25)	ครอบคลุมทุกความเสี่ยง	ครบเกือบทั้งหมด	ครอบคลุมบางส่วน	ไม่ถูกต้อง
การเสนอการใช้มาตรฐาน/เทคโนโลยี (25)	นำเสนอ Wi-Fi รุ่นใหม่ + WPA3 ครบถ้วน	นำเสนอเพียงบางส่วน	มีข้อมูลแต่ไม่ครบถ้วน	ขาดการเสนอ
การเสนอแนวทางป้องกัน (30)	ครอบคลุม WPA3, VLAN, Firewall, Captive Portal	ครอบคลุมบางส่วน	มีข้อเสนอแต่ไม่ชัดเจน	ไม่มีข้อเสนอ
การนำเสนอ (20)	ชัดเจน มีผังเครือข่ายประกอบ	ชัดเจน	พอใช้	ไม่ชัดเจน

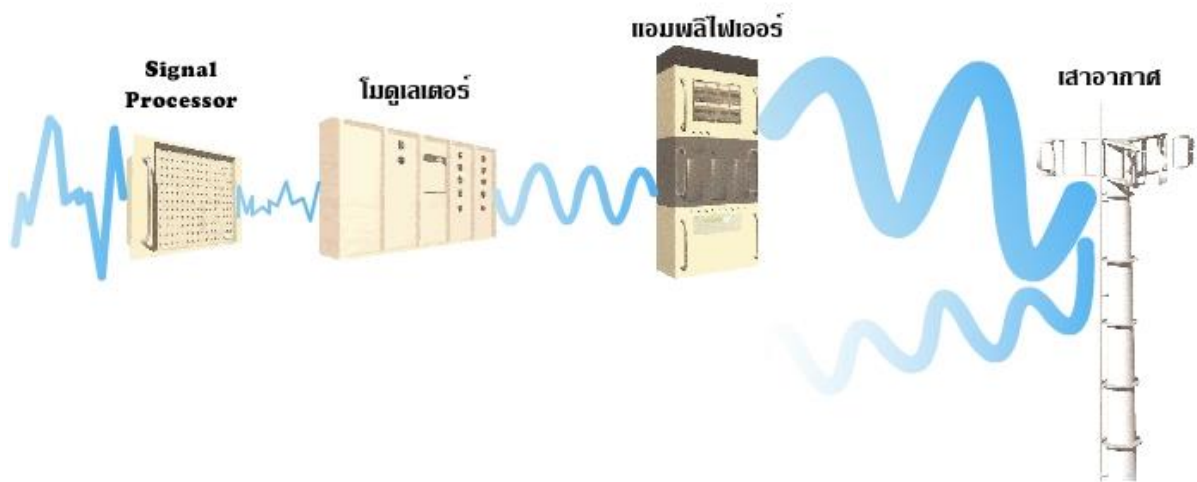
10. เครือข่ายไร้สาย

เครือข่ายไร้สาย (Wireless Network) คือเครือข่ายคอมพิวเตอร์ที่ใช้การเชื่อมต่อข้อมูลไร้สายระหว่าง โหนดเครือข่าย เครือข่ายไร้สายช่วยให้บ้านเรือนเครือข่ายโทรคมนาคมและธุรกิจต่างๆ หลีกเลียงกระบวนการที่มี ค่าใช้จ่ายสูงในการเดินสายเคเบิลเข้าไปในอาคาร หรือการเชื่อมต่อระหว่างตำแหน่งอุปกรณ์ต่างๆ โดยทั่วไป เครือข่ายโทรคมนาคมของผู้ดูแลระบบจะถูกนำไปใช้และบริหารจัดการโดยใช้การสื่อสารทางวิทยุการใช้งานนี้ เกิดขึ้นที่ระดับกายภาพ (เลเยอร์) ของโครงสร้างเครือข่ายแบบจำลอง OSI ตัวอย่างของเครือข่ายไร้สาย ได้แก่ เครือข่ายโทรศัพท์มือถือ เครือข่ายพื้นที่ไร้สาย (WLAN) เครือข่าย เซ็นเซอร์ไร้สาย เครือข่ายการสื่อสารผ่านดาวเทียม และเครือข่ายไมโครเวฟภาคพื้นดิน

ข้อมูลหลายชนิดสามารถส่งแบบไร้สายได้ เช่น ข้อมูลจากคอมพิวเตอร์ เสียงจากโทรศัพท์ สัญญาณ โทรศัพท์และวิทยุ ในการส่งข้อมูลเหล่านั้น ขั้นตอนแรกข้อมูลที่ถูกส่งจะถูกสร้างจากอุปกรณ์ที่สร้างข้อมูล เช่น คอมพิวเตอร์ มือถือ สถานีวิทยุ หรือโทรศัพท์มือถือ เป็นต้น แล้วนำไปผสมกับคลื่นความถี่วิทยุ ซึ่งเรียกว่า สัญญาณ โดยอาศัยกระบวนการมอดูเลชัน สัญญาณที่จะเป็นตัวส่งข้อมูลเรียกว่าคลื่นพาห์ (Carrier Wave) ข้อมูล จะถูกผสมไปกับคลื่นตัวนำ โดยอุปกรณ์ที่เรียกว่ามอดูเลเตอร์ ซึ่งอาจรวมอยู่ในอุปกรณ์ที่สร้างข้อมูลอย่างเช่น โทรศัพท์มือถือ สมาร์ทโฟน คอมพิวเตอร์แบบพกพา พีดีเอ

จากนั้น สัญญาณจะถูกส่งโดยอุปกรณ์ส่งสัญญาณส่งออกไปโดยผ่านทางอากาศ อุปกรณ์ส่งสัญญาณนั้นมี หลายแบบโดยขึ้นอยู่กับชนิดข้อมูลที่ส่ง ระยะทาง และความแรงของสัญญาณ ขนาดของเสาอากาศนั้นอาจเล็ก มากเหมือนที่อยู่โทรศัพท์มือถือ หรืออาจจะใหญ่มากเหมือนเสาอากาศส่งสัญญาณของโทรทัศน์ ก็ได้ ในฝั่งของ อุปกรณ์รับสัญญาณสามารถรับสัญญาณได้โดยตรง หรืออาจผ่านทางระบบเครือข่ายโดยขึ้นกับชนิดของข้อมูลที่ส่ง ในกรณีของโทรศัพท์มือถือ หรือคอมพิวเตอร์แบบพกพา เมื่อจะติดต่อกับอินเทอร์เน็ตมันจะส่งสัญญาณไปที่ เครือข่ายและส่งต่อไปยังผู้รับโดยใช้อุปกรณ์ส่งสัญญาณ (Transmitters)

เมื่อสัญญาณถูกส่งไปถึงจุดรับสัญญาณ เสาอากาศหรือสายอากาศรับสัญญาณที่ส่งมาให้อุปกรณ์รับ สัญญาณ โดยจะรับเฉพาะคลื่นวิทยุที่ต้องการและไม่รับคลื่นที่เหลือ อุปกรณ์รับสัญญาณจะใช้ตัวขยาย สัญญาณ (Amplifier) เพื่อเพิ่มความเข้มของสัญญาณ จากนั้น มอดูเลเตอร์ (หรืออาจเรียกว่าดีมอดูเลเตอร์) จะทำ การแปลงสัญญาณและแยกคลื่นตัวนำออกจากข้อมูลที่ถูส่งมาพร้อมกัน เพื่อที่จะเปลี่ยนกลับไปเป็นข้อมูลดั้งเดิมที่ ส่งมาแสดงผลที่อุปกรณ์รับสัญญาณ เช่น โทรศัพท์มือถือ เครื่องรับโทรทัศน์ คอมพิวเตอร์แบบพกพา รูป 10.1 แสดงกระบวนการส่งข้อมูลไปพร้อมกับคลื่น



รูป 10.1 กระบวนการส่งข้อมูลไปพร้อมกับคลื่น

ที่มา http://www.rmutphysics.com/CHARUD/oldnews/265/wireless/cp1_1.html

10.1 ประเภทของเครือข่ายไร้สาย

10.1.1 แพนไร้สาย (WPAN: Wireless Personal Area Network)

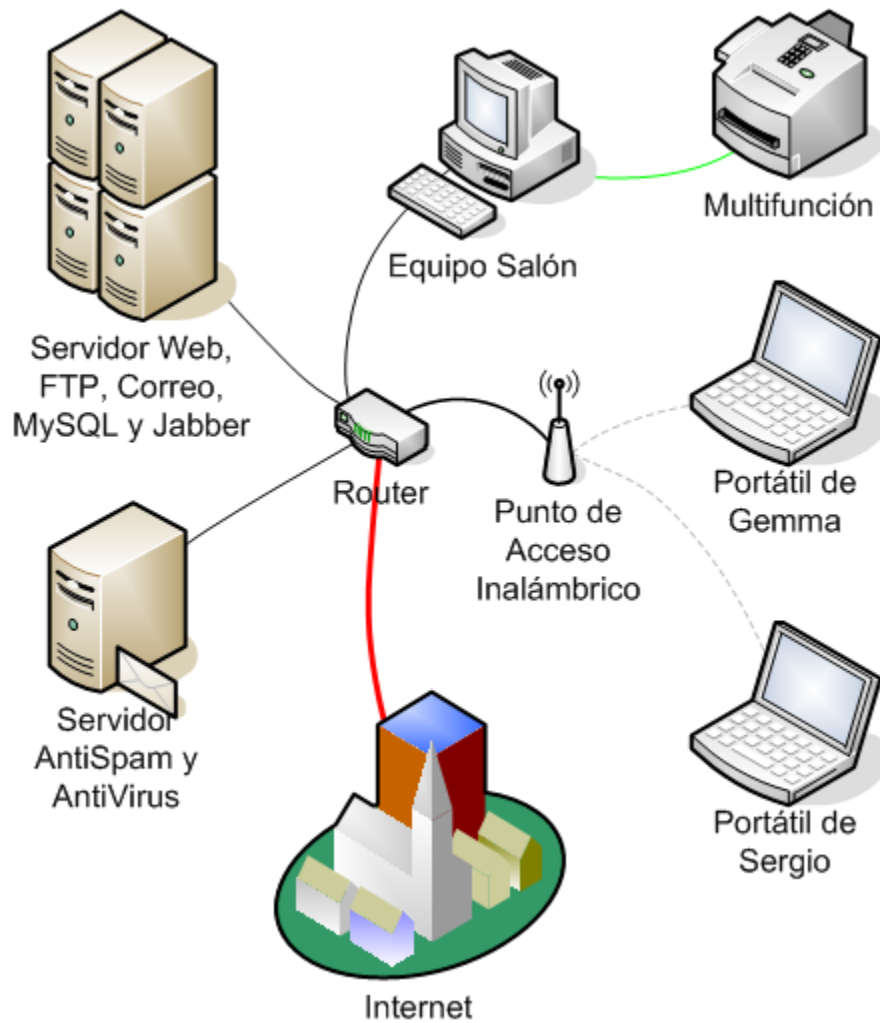
เครือข่ายพื้นที่ส่วนบุคคลแบบไร้สาย (WPAN) เชื่อมต่ออุปกรณ์ต่างๆ ภายในพื้นที่ที่ค่อนข้างเล็ก ซึ่งโดยทั่วไปแล้วอยู่ในระยะที่บุคคลสามารถเข้าถึงได้ ตัวอย่างเช่น ทั้งวิทยุบลูทูธ และแสง อินฟราเรด ที่มองไม่เห็นเป็น WPAN สำหรับเชื่อมต่อชุดหูฟังเข้ากับแล็ปท็อปยังรองรับแอปพลิเคชัน WPAN ด้วย Wi-Fi PAN กำลังกลายเป็นเรื่องธรรมดา เนื่องจากนักออกแบบอุปกรณ์เริ่มผสมผสาน Wi-Fi เข้ากับอุปกรณ์อิเล็กทรอนิกส์สำหรับผู้บริโภคหลากหลายประเภท ความสามารถ "My WiFi" ของ Intel และ "virtual Wi-Fi" ของ Windows 7 ทำให้ Wi-Fi PAN ง่ายและสะดวกต่อการตั้งค่าและกำหนดค่า

10.1.2 ระบบแลนไร้สาย (WLAN: Wireless Local Area Network)

เครือข่ายเฉพาะบริเวณไร้สาย (WLAN) เชื่อมโยงอุปกรณ์ตั้งแต่สองเครื่องขึ้นไปในระยะทางสั้นๆ โดยใช้วิธีการกระจายสัญญาณไร้สาย ซึ่งโดยปกติจะเชื่อมต่อผ่านจุดเชื่อมต่ออินเทอร์เน็ต การใช้เทคโนโลยีสเปกตรัม หรือ OFDM อาจช่วยให้ผู้ใช้สามารถเคลื่อนที่ไปมาภายในพื้นที่ครอบคลุมท้องถิ่น และยังคงเชื่อมต่อกับเครือข่ายได้

ผลิตภัณฑ์ที่ใช้ มาตรฐาน IEEE 802.11 WLAN วางตลาดภายใต้ชื่อแบรนด์ Wi-Fi เทคโนโลยี ไร้สายแบบประจำที่ (Fixed Wireless) เชื่อมโยงคอมพิวเตอร์หรือเครือข่ายจากระยะไกลสองจุด โดยมักใช้ไมโครเวฟเฉพาะหรือลำแสงเลเซอร์แบบปรับแสงบนเส้นทางที่มองเห็นมักใช้ในเมืองเพื่อเชื่อมต่อเครือข่ายในอาคารสองหลังหรือ

มากกว่าโดยไม่ต้องติดตั้งการเชื่อมต่อแบบใช้สาย หากต้องการเชื่อมต่อ Wi-Fi โดยใช้อุปกรณ์พกพา สามารถใช้อุปกรณ์อย่างเช่นเราเตอร์ไร้สายหรือสวิตช์ส่วนตัวของอุปกรณ์พกพาเครื่องอื่นได้ ดังรูป 10.2



รูป 10.2 WLAN มักเชื่อมต่อเข้ากับอินเทอร์เน็ต

(https://en.wikipedia.org/wiki/Wireless_network#/media/File:LAN.png)

10.1.3 เครือข่ายเฉพาะกิจแบบไร้สาย

เครือข่ายไร้สายเฉพาะกิจ หรือที่รู้จักกันในชื่อเครือข่ายไร้สายแบบตาข่าย (wireless mesh network) หรือเครือข่ายเคลื่อนที่เฉพาะกิจ (mobile ad hoc network หรือ MANET) เป็นเครือข่ายไร้สายที่ประกอบด้วย โหนดวิทยุที่จัดอยู่ในโครงสร้างแบบตาข่าย แต่ละโหนดจะส่งต่อข้อความแทนโหนดอื่นๆ และแต่ละโหนดจะกำหนดเส้นทาง เครือข่ายเฉพาะกิจสามารถ "ซ่อมแซมตัวเอง (self-heal)" ได้ โดยกำหนดเส้นทางใหม่โดยอัตโนมัติรอบโหนดที่ไพล่ดับ จำเป็นต้องใช้โปรโตคอลชั้นเครือข่ายต่างๆ เพื่อสร้างเครือข่ายเคลื่อนที่เฉพาะกิจ เช่น การกำหนด

เส้นทางแบบเวกเตอร์ระยะทางแบบเรียงลำดับ, การกำหนดเส้นทางแบบอิงการเชื่อมโยง, การกำหนดเส้นทางแบบเวกเตอร์ระยะทางแบบตามความต้องการเฉพาะกิจและการกำหนดเส้นทางแบบต้นทางแบบไดนามิก

รูปแบบเครือข่ายไร้สาย การส่งผ่านข้อมูลผ่านทางเครือข่ายไร้สายจำเป็นต้องมีอุปกรณ์ที่เป็นตัวกลางในการรับข้อมูลจาก node หนึ่ง ส่งไปอีก node หนึ่ง โดยอุปกรณ์นี้เรียกว่า AP (Access Point) ซึ่งทำหน้าที่เหมือน switch ใน Wired Network เราสามารถจำแนกประเภทของ APs ได้ ดังนี้

Software APs เป็น AP ที่ใช้เครื่องคอมพิวเตอร์ที่มี NIC (Network Interface Card) ทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูล

Hardware APs เป็น AP ที่เป็นลักษณะ appliance ถูกผลิตออกมาเพื่อใช้งานเป็น AP โดยเฉพาะ โดย Hardware APs จะมีรูปแบบการปรับแต่งค่าการใช้งานได้หลากหลายกว่าแบบ Software APs

10.1.4 แมนไร้สาย (WMAN: Wireless Metropolitan Area Networks)

เครือข่ายพื้นที่มหานคร ไร้สายเป็นเครือข่ายไร้สายประเภทหนึ่งที่เชื่อมต่อเครือข่าย LAN ไร้สายหลายเครือข่ายเข้าด้วยกัน WiMAX เป็นประเภทหนึ่งของ Wireless MAN และได้รับการอธิบายโดยมาตรฐาน IEEE 802.16

10.1.5 แวนไร้สาย (WWAN: Wireless WAN)

เครือข่ายไร้สายบริเวณกว้าง (Wireless Wide Area Network) คือเครือข่ายไร้สายที่โดยทั่วไปครอบคลุมพื้นที่ขนาดใหญ่ เช่น ระหว่างเมืองใกล้เคียง หรือระหว่างเมืองและชนเมือง เครือข่ายเหล่านี้สามารถใช้เชื่อมต่อสำนักงานสาขาของธุรกิจ หรือใช้เป็นระบบอินเทอร์เน็ตสาธารณะ การเชื่อมต่อไร้สายระหว่างจุดเชื่อมต่อมักจะเป็นการเชื่อมต่อไมโครเวฟแบบจุดต่อจุด โดยใช้จานพาราโบลาบนยานความถี่ 2.4 GHz และ 5.8 GHz แทนที่จะใช้เสาอากาศรอบทิศทางแบบเดียวกับเครือข่ายขนาดเล็ก ระบบทั่วไปประกอบด้วยเกตเวย์สถานีฐาน จุดเชื่อมต่อและรีเลย์บริดจ์ไร้สาย การกำหนดค่าอื่นๆ เป็นระบบเมช ซึ่งจุดเชื่อมต่อแต่ละจุดจะทำหน้าที่เป็นรีเลย์เช่นกัน เมื่อใช้ร่วมกับระบบพลังงานหมุนเวียน เช่น แผงโซลาร์เซลล์แบบโฟโตโวลตาอิก หรือระบบพลังงานลม ก็สามารถเป็นระบบแบบสแตนด์อโลนได้

10.1.6 เครือข่ายเซลลูลาร์ (Cellular Network)

เครือข่ายมือถือ หรือ เครือข่ายเซลลูลาร์ หรือเครือข่ายโมบาย (cellular network/mobile network) เครือข่ายเซลลูลาร์ (Cellular Network) คือระบบการสื่อสารแบบไร้สายที่แบ่งพื้นที่ทางภูมิศาสตร์ออกเป็น "เซลล์" โดยแต่ละเซลล์จะมี "สถานีฐาน" (เสาสัญญาณ) คอยให้บริการสัญญาณวิทยุ ทำให้โทรศัพท์มือถือและอุปกรณ์อื่นๆ สามารถสื่อสารกันได้ทั่วถึง แม้จะมีการเคลื่อนที่ไปมาระหว่างเซลล์ต่างๆ โดยมีการส่งต่อการเชื่อมต่ออย่างราบรื่น เครือข่ายนี้ใช้ในการโทรออก ส่งข้อความ และเชื่อมต่ออินเทอร์เน็ตผ่านเทคโนโลยีต่างๆ เช่น GSM, LTE และ 5G

องค์ประกอบหลักของเครือข่ายเซลลูลาร์

- 1) เซลล์ (Cell): พื้นที่ทางภูมิศาสตร์ที่กำหนดซึ่งแต่ละส่วนมีสถานีฐาน
- 2) สถานีฐาน (Base Station): อุปกรณ์รับส่งสัญญาณที่ให้บริการในแต่ละเซลล์
- 3) ศูนย์กลางควบคุม (Central Control/Mobile Switching Center): ระบบที่บริหารจัดการสถานีฐานทั้งหมดเพื่อเชื่อมต่อเครือข่ายเข้าด้วยกัน

หลักการทำงาน

- 1) การแบ่งพื้นที่: พื้นที่ครอบคลุมถูกแบ่งออกเป็นเซลล์เล็กๆ เพื่อให้ใช้ทรัพยากรคลื่นวิทยุได้อย่างมีประสิทธิภาพ
- 2) การส่งสัญญาณ: สถานีฐานในแต่ละเซลล์จะกระจายสัญญาณวิทยุ เพื่อให้อุปกรณ์เคลื่อนที่สามารถเชื่อมต่อได้
- 3) การส่งต่อ (Handover): เมื่อผู้ใช้เคลื่อนที่จากเซลล์หนึ่งไปยังอีกเซลล์หนึ่ง เครือข่ายจะส่งต่อการเชื่อมต่อโดยอัตโนมัติ เพื่อให้การสื่อสารไม่ขาดตอน
- 4) การจัดการทรัพยากร: เทคโนโลยีอย่าง GSM, LTE หรือ 5G ถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพการสื่อสาร รองรับผู้ใช้งานจำนวนมาก และรักษาความปลอดภัย

ข้อดีและประโยชน์

- **การครอบคลุมพื้นที่กว้าง:**
การรวมเซลล์จำนวนมากเข้าด้วยกันทำให้เกิดการครอบคลุมสัญญาณในพื้นที่กว้าง
- **การสื่อสารที่ราบรื่น:**
การส่งต่อการเชื่อมต่อระหว่างเซลล์ทำให้การสื่อสารไม่หยุดชะงักขณะเคลื่อนที่
- **รองรับอุปกรณ์หลากหลาย:**
ใช้ได้กับสมาร์ทโฟน แท็บเล็ต ไปจนถึงอุปกรณ์ IoT
- **การเชื่อมต่อข้อมูล:**
ทำให้สามารถเข้าถึงอินเทอร์เน็ตและใช้งานแอปพลิเคชันต่างๆ ได้ทุกที่ทุกเวลา

10.1.7 เครือข่ายเฉพาะบริเวณไร้สาย: แลนไร้สาย

เครือข่ายเฉพาะบริเวณไร้สาย หรือ แลนไร้สาย (Wireless LAN หรือ WLAN) คือเครือข่ายคอมพิวเตอร์สำหรับองค์กรที่ใช้มาตรฐานอีเธอร์เน็ต (Ethernet IEEE 802.3) สามารถเชื่อมโยงสื่อสารกันระหว่างเครื่องลูกข่ายในเครือข่ายเดียวกันโดยไม่ใช้สายสัญญาณ แต่ใช้คลื่นวิทยุสื่อสารผ่านอากาศ WLAN ยังสามารถเชื่อมโยงเข้ากับ

เครือข่ายแบบใช้สายในองค์กรเดียวกันที่ไม่เพียงใช้แลกเปลี่ยนข้อมูลเฉพาะภายในองค์กรเท่านั้นแต่ยังอนุญาตให้เข้าถึงทรัพยากรต่างๆ บนอินเทอร์เน็ตได้อีกด้วย รูป 10.3 แสดงการทำงานร่วมกันของ WLAN กับเครือข่ายมีสาย



รูป 10.3 การทำงานร่วมกันของ WLAN กับเครือข่ายมีสายรวมทั้งการเชื่อมต่ออินเทอร์เน็ต
ที่มา http://www.pchelplosangeles.com/home_networking.htm

จึงสามารถสรุปข้อดีของ WLAN ได้ดังนี้

ความยืดหยุ่น (Flexibility)

ความมีเสถียรภาพของแลนไร้สายที่ได้รับการพัฒนาบนมาตรฐาน IEEE 802.11 มาอย่างต่อเนื่องจนถึงปัจจุบัน จึงทำให้ผู้ใช้ไม่ต้องกังวลว่าจะต้องใช้อุปกรณ์ไร้สายที่ผูกติดกับผลิตภัณฑ์ของยี่ห้อใดยี่ห้อหนึ่ง ด้วยมาตรฐานดังกล่าว ทำให้ผู้ใช้สามารถเลือกใช้อุปกรณ์ของบริษัทใดก็ได้ที่รองรับมาตรฐานก็มั่นใจถึงความเข้ากันได้ของอุปกรณ์เหล่านั้น

ความสามารถในการขยายระบบได้ง่าย (Scalability)

หากต้องการโยกย้ายโต๊ะทำงาน ปรับเปลี่ยนห้องทำงาน หรือมีคอมพิวเตอร์เครื่องใหม่เข้ามา ในเครือข่ายแบบใช้สายจะมีงานตามมาอีกมากมาย เช่น ต้องคำนึงถึงแลนพอร์ตบนฮับหรือสวิตช์ว่าว่างหรือไม่ สาย UTP เดินไปถึงหรือไม่ ช่องเสียบ (UTP Outlet) เหลือพอหรือไม่ เป็นต้น ปัญหาเหล่านี้จะถูกขจัดไปเมื่อใช้แลนไร้สาย ข้อจำกัดด้านสถานที่ เช่น การใช้งานในสถานที่โล่งแจ้ง กลางสนาม ก็จะไม่ต้องกังวลอีกต่อไป นอกจากนั้น องค์กรอาจใช้แลนไร้สายขยายไปยังจุดที่แลนแบบใช้สายไปไม่ถึงก็จะช่วยประหยัดต้นทุนได้มากกว่าที่จะติดตั้งระบบแลนแบบใช้สาย

คummค่าในระยะยาว (TCO-Total Cost of Ownership)

แม้ราคาต่อหน่วยของอุปกรณ์ไร้สายในปัจจุบัน เช่น การ์ดเครือข่าย ฮับหรือสวิตช์ เป็นต้น ต้นทุนอาจสูงกว่าเมื่อเทียบกับแลนแบบใช้สาย ทั้งนี้เพราะแลนแบบใช้สายได้มีการใช้งานกันมายาวนานกว่า มีความแพร่หลายกว่า แต่การนำระบบแลนมาใช้ในองค์กรไม่ควรคำนึงเพียงราคาต่อหน่วยของอุปกรณ์แต่ขึ้นที่ซื้อเท่านั้น หากยังต้องคำนึงถึงค่าใช้จ่ายในการติดตั้ง การฝึกอบรม ค่าบุคลากร ค่าดูแลรักษา สายสัญญาณ อุปกรณ์อื่นๆ เช่น RJ45 อุปกรณ์เข้าหัว เป็นต้น เรียกว่า ต้นทุนในการเป็นเจ้าของ (TCO) ซึ่งในระยะยาวแล้วต้นทุน TCO ของแลนไร้สายจะต่ำกว่าแลนใช้สาย

ต้องการความรู้ทางเทคนิคน้อยกว่า

การติดตั้งอุปกรณ์รับและกระจายสัญญาณแบบไร้สาย (WAP: Wireless Access Point) เช่น ฮับไร้สาย สวิตช์ไร้สาย ไม่จำเป็นต้องมีความรู้ระดับผู้เชี่ยวชาญ การสนับสนุนภายหลังการใช้งาน การติดตั้งอุปกรณ์ การดูแลรักษาระบบแลนไร้สายนั้น ยังต้องการบุคลากรที่มีความชำนาญทางเทคนิคน้อยกว่าในระบบแลนแบบใช้สาย

ต้นทุนในการบำรุงรักษาต่ำ (maintenance cost)

เมื่อพิจารณาจากเหตุผลทุกข้อดังกล่าวมา ค่าใช้จ่ายในการดูแลระบบแลนไร้สายโดยรวมย่อมต่ำกว่าองค์กรขนาดเล็กที่ใช้แลนไร้สาย ไม่จำเป็นต้องมีพนักงานด้านไอทีก็ได้

ด้วยเหตุผลเหล่านี้ทำให้แลนไร้สายได้รับความนิยมอย่างแพร่หลายในปัจจุบัน

10.1.7 เปรียบเทียบมีสายกับไร้สาย (Wired vs Wireless)

คำถามที่น่าสนใจว่า ในที่สุดแล้ว อนาคตจะเหลือแต่เพียงโลกไร้สาย หรือไม่?

แม้กระแสของเทคโนโลยีกำลังก้าวไปในทิศทางของโลกไร้สายก็ตาม แต่ก็ไม่ได้หมายความว่า จะเข้ามาทดแทนเทคโนโลยีแบบมีสายโดยสิ้นเชิง แท้จริงแล้ว เทคโนโลยีทั้งสองแบบต่างก็มีข้อเด่นข้อด้อยแตกต่างกัน การ

ผสมผสานของเทคโนโลยีทั้งสองแบบย่อมสามารถช่วยเติมเต็มซึ่งกันและกันและกันที่จะช่วยส่งมอบบริการที่ดีไม่ขาดตอนแก่ผู้รับบริการขององค์กรได้

ดังนั้น ในทางปฏิบัติ เราจึงพบว่าบริษัทผู้ให้บริการโทรคมนาคมแบบไร้สาย เช่น ระบบเซลลูลาร์ มีการดาวเทียม แม้เป็นธุรกิจประเภทไร้สายต่างก็ต้องอาศัยระบบสายสัญญาณเช่นใยแก้วนำแสงมาช่วยทั้งในแง่เป็นช่องทางสำรองและช่วยในการรวบรวมและอพยพข้อมูลปริมาณมากๆ จากระบบไร้สายที่มีความเร็วต่ำกว่า ตัวอย่างเช่น การสร้างโครงข่ายโทรคมนาคมในพื้นที่กันดารห่างไกล มีจำนวนหมู่บ้านอยู่อย่างกระจัดกระจาย อาจไม่คุ้มค่าในเชิงผลตอบแทนทางธุรกิจถ้าจะต้องใช้ระบบสาย ในอดีตจะพบว่า หมู่บ้านในชนบทเหล่านั้นกว่าจะได้รับ การติดตั้งโทรศัพท์ตามบ้านต้องใช้เวลารอคอยนานหลายปี แต่ในปัจจุบัน โทรศัพท์ระบบเซลลูลาร์ได้เข้ามาช่วยให้ทุกคนสามารถติดต่อสื่อสารถึงกันได้ไม่ว่าจะในพื้นที่ใดๆ ก็ตาม แม้แต่การพัฒนาโครงข่ายโทรศัพท์ในพื้นที่ชนบทของหน่วยงานภาครัฐ เช่น องค์กรโทรศัพท์แห่งประเทศไทยในปัจจุบันก็ยังเลือกใช้ทั้งระบบมีสายและไร้สายควบคู่กันไป ตารางที่ 10.1 แสดงเปรียบเทียบข้อเด่นข้อด้อยระหว่างระบบใช้สายกับไร้สาย ซึ่งจะช่วยเป็นคำตอบว่าอนาคต โลกจะเหลือเพียงระบบไร้สายเท่านั้น หรือไม่

ตาราง 10.1 เปรียบเทียบข้อเด่นข้อด้อยระหว่างเทคโนโลยีใช้สายกับไร้สาย

เทคโนโลยี	ข้อเด่น	ข้อด้อย
มีสาย	- ความเร็วสูงกว่า - มีเสถียรภาพกว่า - ความปลอดภัยกว่า - ไม่ถูกรบกวนด้วยคลื่นแม่เหล็กไฟฟ้า - พัฒนาและแพร่หลายมานาน - ต้นทุนต่ำกว่า - สามารถควบคุมตรวจสอบได้ด้วยสายตา (visible control) - สามารถใช้เป็นโครงสร้างพื้นฐานของระบบใช้สายของกิจการโทรคมนาคมได้หลายประเภท	- ต้องลงทุนด้านสายสัญญาณ - สามารถให้บริการได้เฉพาะพื้นที่ที่สายไปถึง - ขาดความคล่องตัวยืดหยุ่น - ค่าใช้จ่ายในการบำรุงรักษาสูง - ต้องการบุคลากรที่มีความชำนาญและจำนวนมาก - อาจถูกจำกัดด้วยสถานที่
ไร้สาย	- ไม่จำเป็นต้องใช้สายสัญญาณ - ครอบคลุมพื้นที่ในวงกว้าง - ไม่ถูกจำกัดด้วยพื้นที่และสิ่งกีดขวาง - มีความยืดหยุ่น	- ความเร็วต่ำกว่า - เสถียรภาพของระบบต่ำกว่า - ความปลอดภัยต่ำกว่า

เทคโนโลยี	ข้อเด่น	ข้อด้อย
	สามารถขยายระบบได้ง่าย	- ถูกรบกวนด้วยคลื่นแม่เหล็กไฟฟ้าในธรรมชาติ เช่น ฝนตก ฟ้าคะนอง - สัญญาณถูกรบกวนด้วยระบบไร้สายด้วยกัน - อาจมีผลกระทบต่อสุขอนามัยของมนุษย์และสิ่งมีชีวิตอื่นๆ

10.2 การเชื่อมต่อเครือข่ายและมาตรฐาน IEEE 802.11 WLAN

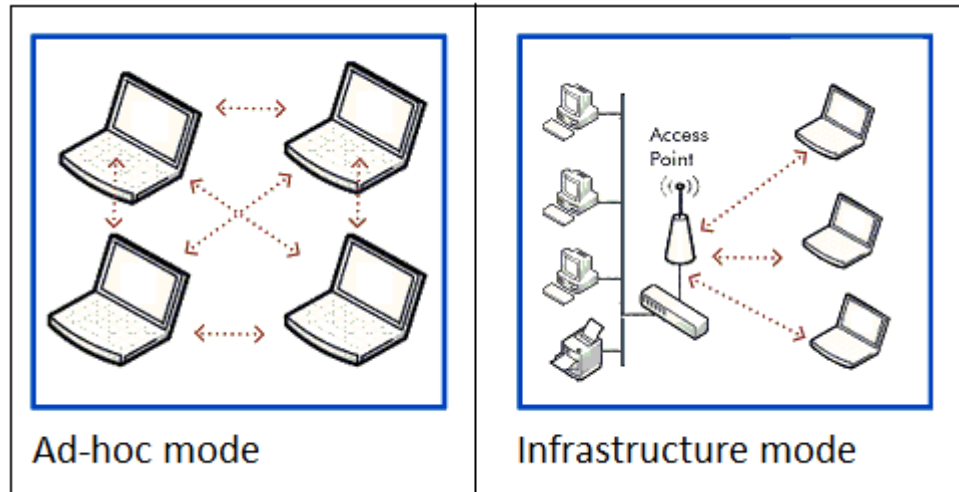
มาตรฐาน IEEE 802.11 ได้กำหนดลักษณะการเชื่อมต่อของอุปกรณ์ภายในเครือข่ายของแลนไร้สายไว้ 2 ลักษณะคือโหมดโครงสร้างพื้นฐาน และโหมด Ad-Hoc หรือ Peer-to-Peer

10.2.1 โหมดโครงสร้างพื้นฐาน (Infrastructure mode)

การเชื่อมต่ออุปกรณ์ในเครือข่ายแลนไร้สายจะเชื่อมต่อกันในโหมด ซึ่งเป็นโหมดที่อนุญาตให้อุปกรณ์ภายในแลนไร้สายสามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมดโครงสร้างพื้นฐานนี้ เครือข่ายแลนไร้สายจะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่ สถานีลูกข่าย (Client Station) ได้แก่ อุปกรณ์คอมพิวเตอร์ (Desktop, Laptop, หรือ PDA ต่างๆ) ที่มีอุปกรณ์ประเภทการ์ดเครือข่ายไร้สาย (Wireless NIC) เพื่อใช้รับส่งข้อมูลผ่าน IEEE 802.11 WLAN และแอ็กเซสพอยน์ท์ ซึ่งทำหน้าที่เชื่อมต่อลูกข่ายเข้ากับเครือข่ายมีสาย การทำงานในโหมดนี้มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ กล่าวคือเครื่องลูกข่ายจะสามารถรับส่งข้อมูลโดยตรงกับเครื่องแม่ข่ายที่ให้บริการแก่ลูกข่ายนั้นอยู่เท่านั้น ส่วนแม่ข่ายจะทำหน้าที่ส่งต่อ (forward) ข้อมูลที่ได้รับจากสถานีผู้ใช้ไปยังจุดหมายปลายทางหรือส่งต่อข้อมูลที่ได้รับจากเครือข่ายอื่นมายังลูกข่ายของผู้ใช้ ภาพที่ 10.4 แสดงการเชื่อมต่อแลนไร้สายในโหมดโครงสร้างพื้นฐาน

10.2.2 โหมด Ad-Hoc หรือ Peer-to-Peer

ad hoc ถือเป็นเครือข่ายไร้สายแบบกระจาย (Decentralized) เครือข่ายเป็น ad hoc เพราะไม่จำเป็นต้องพึ่งพาอุปกรณ์ประเภทโครงสร้างพื้นฐาน เช่น เราเตอร์ (ในเครือข่ายแบบมีสาย) หรือแอ็กเซสพอยน์ท์ (ที่ใช้ในโหมดโครงสร้างพื้นฐาน) เพื่อจัดการการสื่อสารภายในเครือข่าย แต่ละโหนดมีส่วนร่วมในการกำหนดเส้นทางโดยข้อมูลส่งต่อสำหรับโหนดอื่นๆ และเพื่อการตัดสินใจของที่ nodes ส่งข้อมูลทำตามแบบไดนามิกในการเชื่อมต่อเครือข่าย ซึ่งเครื่องลูกข่ายสามารถติดต่อสื่อสารข้อมูลกับลูกข่ายของผู้ใช้อื่นๆ ที่อยู่ภายในอาณาบริเวณเดียวกันโดยตรงโดยไม่ต้องผ่านแม่ข่าย แต่ผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่นๆ ได้ รูป 10.4 แสดงการเชื่อมต่อระหว่างอุปกรณ์ของแลนไร้สายในโหมด Ad-Hoc



รูป 10.4 การเชื่อมต่อแลนไร้สายในโหมด Ad-Hoc และโครงสร้างพื้นฐาน

(https://www.researchgate.net/figure/Ad-hoc-mode-vs-Infrastructure-mode-IEEE80211-introduced-many-types-of-the-Wi-Fi_fig1_316175326)

10.2.3 เทคโนโลยี Wi-Fi มาตรฐาน IEEE 802.11

Wi-Fi มาจาก Wireless Fidelity หมายถึงชุดผลิตภัณฑ์ต่างๆ ที่สามารถใช้ได้กับมาตรฐานแลนไร้สาย (WLAN) ซึ่งอยู่บนมาตรฐาน IEEE 802.11 เดิมที Wi-Fi ถูกออกแบบมาใช้สำหรับอุปกรณ์พกพาต่างๆ และใช้กับแลนเท่านั้น แต่ปัจจุบันนิยมใช้ Wi-Fi เพื่อต่อกับอินเทอร์เน็ต โดยอุปกรณ์พกพาต่างๆ สามารถเชื่อมต่อกับอินเทอร์เน็ตได้ผ่านอุปกรณ์ที่เรียกว่าแอคเซสพอยต์ (AP: Access Point หรือ WAP: Wireless Access Point) และบริเวณที่ระยะทำการของแอคเซสพอยต์ครอบคลุมเรียกว่า ฮอตสปอต (Hotspot) หรือ Wi-Fi Zone ซึ่งหมายถึง สถานที่ที่ผู้ใช้สามารถเข้าถึงอินเทอร์เน็ตโดยใช้แล็ปท็อป Wi-Fi และอื่นๆ Wi-Fi เปิดการใช้งานอุปกรณ์เพื่อการเชื่อมต่อผ่านระบบไร้สายเข้าสู่อินเทอร์เน็ต อาจจะให้ฟรีหรือเก็บค่าธรรมเนียม จุดที่มักจะพบคือที่ร้านกาแฟ, โรงแรม, ห้องนั่งเล่นสนามบิน, สถานีรถไฟ, ศูนย์ประชุม, สถานีบริการน้ำมัน, ที่จอดรถและพื้นที่สาธารณะอื่นๆ, ที่ประชุม สถาบันและวิทยาเขต ปัจจุบัน ฮอตสปอตมักเป็นบริการอินเทอร์เน็ตไร้สายสำหรับสาธารณะ

แต่เดิมคำว่า Wi-Fi เป็นชื่อที่ตั้งแทนตัวเลข IEEE 802.11 ซึ่งง่ายกว่าในการจดจำ โดยนำมาจากเครื่องขยายเสียง Hi-Fi อย่างไรก็ตามในปัจจุบันใช้เป็นคำย่อของ Wireless-Fidelity โดยมีแสดงในเว็บไซต์ของ Wi-Fi Alliance โดยใช้ชื่อ Wi-Fi เป็นเครื่องหมายการค้าผลิตภัณฑ์หลายอย่างเข้ากันได้กับ 802.11a, 802.11b, 802.11g หรือ 802.11n มาตรฐานไร้สายจึงเรียกรวมเป็นเทคโนโลยี Wi-Fi

Wi-Fi ออกเสียงว่า วายฟาย เป็นเทคโนโลยีเครือข่ายไร้สายมาตรฐาน IEEE 802.11 ถือกำเนิดขึ้นในปี พ.ศ. 2540 จัดตั้งโดยองค์การ Institute of Electrical and Electronics Engineers หรือ IEEE (สถาบัน

วิศวกรรมทางด้านไฟฟ้าและอิเล็กทรอนิกส์) มีความเร็ว 1 Mbps ในยุคเริ่มแรกนั้นให้ประสิทธิภาพการทำงานที่ค่อนข้างต่ำ ทั้งไม่มีการรับรองคุณภาพของการให้บริการที่เรียกว่า QoS (Quality of Service) และมาตรฐานความปลอดภัยต่ำ จากนั้นทาง IEEE จึงจัดตั้งคณะกรรมการขึ้นมาปรับปรุงหลายกลุ่มด้วยกัน โดยที่กลุ่มที่มีผลงานเป็นที่น่าพอใจและได้รับการยอมรับอย่างเป็นทางการว่า ได้มาตรฐานได้แก่กลุ่ม 802.11a , 802.11b และ 802.11g แต่ละมาตรฐานนั้นมีความแตกต่างกันหลักๆ ในด้านย่านความถี่ที่ใช้ ความเร็ว ระยะทำการ และกรรมวิธีในการเข้ารหัสสัญญาณหรือมอดูเลชัน

IEEE 802.11เป็นส่วนหนึ่งของ ชุด มาตรฐานทางเทคนิคของเครือข่ายท้องถิ่น (LAN) ของ IEEE 802และกำหนดชุดโปรโตคอลการควบคุมการเข้าถึงสื่อกลาง (MAC) และชั้นกายภาพ (PHY) สำหรับการสื่อสารคอมพิวเตอร์ ในเครือข่ายท้องถิ่นไร้สาย (WLAN) มาตรฐานและฉบับแก้ไขนี้เป็นพื้นฐานสำหรับผลิตภัณฑ์เครือข่ายไร้สายที่ใช้ แบรนต์ Wi-Fiและเป็นมาตรฐานเครือข่ายคอมพิวเตอร์ไร้สายที่ใช้กันอย่างแพร่หลายที่สุดในโลก IEEE 802.11 ใช้ในเครือข่ายภายในบ้านและสำนักงานส่วนใหญ่เพื่อให้แล็ปท็อป เครื่องพิมพ์ สมาร์ทโฟน และอุปกรณ์อื่นๆ สามารถสื่อสารและเข้าถึงอินเทอร์เน็ตได้โดยไม่ต้องเชื่อมต่อสาย IEEE 802.11 ยังเป็นพื้นฐานสำหรับเครือข่ายการสื่อสารในยานพาหนะที่ใช้ IEEE 802.11p อีกด้วย

มาตรฐานเหล่านี้สร้างขึ้นและดูแลโดย คณะกรรมการมาตรฐาน LAN/ MAN ของสถาบันวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) (IEEE 802) มาตรฐานเวอร์ชันพื้นฐานเผยแพร่ในปี พ.ศ. 2540 และมีการแก้ไขเพิ่มเติมในภายหลัง แม้ว่าการแก้ไขเพิ่มเติมแต่ละครั้งจะถูกยกเลิกอย่างเป็นทางการเมื่อรวมอยู่ในมาตรฐานเวอร์ชันล่าสุด แต่องค์กรธุรกิจต่างๆ มักจะนำการแก้ไขเพิ่มเติมไปใช้ในตลาด เนื่องจากการแก้ไขเพิ่มเติมเหล่านี้แสดงถึงความสามารถของผลิตภัณฑ์ของตนได้อย่างชัดเจน ดังนั้น การแก้ไขเพิ่มเติมแต่ละครั้งจึงมีแนวโน้มที่จะกลายเป็นมาตรฐานเฉพาะตัวในตลาด 802.11x เป็นคำย่อของ "802.11 เวอร์ชันใดก็ได้" เพื่อหลีกเลี่ยงความสับสนกับ "802.11" ซึ่งใช้สำหรับเวอร์ชันดั้งเดิมปี พ.ศ. 2540 โดยเฉพาะ

IEEE 802.11 ใช้คลื่นความถี่ที่หลากหลาย ซึ่งรวมถึงแต่ไม่จำกัดเพียงย่านความถี่ 2.4 GHz, 5 GHz, 6 GHz และ 60 GHz แม้ว่าข้อกำหนดของ IEEE 802.11 จะระบุช่องสัญญาณที่อาจนำมาใช้ แต่ความพร้อมใช้งานของสเปกตรัมความถี่วิทยุที่อนุญาตนั้นแตกต่างกันอย่างมากตามขอบเขตของกฎระเบียบ

โดยทั่วไปโปรโตคอลจะใช้ร่วมกับ IEEE 802.2 และได้รับการออกแบบมาให้ทำงานร่วมกับอีเทอร์เน็ต (Ethernet) ได้อย่างราบรื่น และมักใช้ในการรับส่งข้อมูลโปรโตคอลอินเทอร์เน็ต

มาตรฐาน IEEE 802.11b เสร็จสมบูรณ์เมื่อปี พ.ศ. 2542 ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ผสมกับ DSSS (Direct Sequence Spread Spectrum) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps ผ่านคลื่นวิทยุความถี่ 2.4 GHz (เป็นย่านความถี่ที่เรียกว่า ISM (Industrial Scientific and Medical) ซึ่งถูกจัดสรรไว้อย่างสากลสำหรับการใช้งานอย่างสาธารณะด้านวิทยาศาสตร์ อุตสาหกรรม และการแพทย์ โดยอุปกรณ์ที่ใช้ความถี่ย่านนี้ก็เช่น IEEE 802.11, Bluetooth,

โทรศัพท์ไร้สาย, และเดาโมโครเวฟ มีระยะการส่งสัญญาณได้ไกลมาก ถึง 100 เมตร ปัจจุบันผลิตภัณฑ์อุปกรณ์เครือข่ายไร้สายภายใต้มาตรฐานนี้ถูกผลิตออกมาเป็นจำนวนมาก และที่สำคัญแต่ละผลิตภัณฑ์มีความสามารถทำงานร่วมกันได้ อุปกรณ์ของผู้ผลิตทุกยี่ห้อต้องผ่านการตรวจสอบจากสถาบัน Wi-Fi Alliance เพื่อตรวจสอบมาตรฐานของอุปกรณ์และความเข้ากันได้ของแต่ละผู้ผลิต ปัจจุบันนี้ยมนำอุปกรณ์ WLAN ที่มาตรฐาน 802.11b ไปใช้ในองค์กรธุรกิจ สถาบันการศึกษา สถานที่สาธารณะ และกำลังแพร่เข้าสู่สถานที่พักอาศัยมากขึ้น มาตรฐานนี้มีระบบเข้ารหัสข้อมูลแบบ WEP ที่ 128 บิต

มาตรฐาน IEEE 802.11a เสร็จสมบูรณ์เมื่อปี พ.ศ. 2542 โดยออกเผยแพร่ช้ากว่าของมาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความเร็วในการส่งข้อมูลให้วิ่งได้สูงถึง 54 Mbps บนความถี่ 5GHz เป็นย่านความถี่ประเภท U-NII (Unlicensed National Information Infrastructure) ซึ่งจะมีคลื่นรบกวนน้อยกว่าความถี่ 2.4 GHz ที่มาตรฐานอื่นใช้กัน ที่ความเร็วนี้สามารถทำการแพร่ภาพและข่าวสารที่ต้องการความละเอียดสูงได้ อัตราความเร็วในการรับส่งข้อมูลสามารถปรับระดับให้ช้าลงได้ เพื่อเพิ่มระยะทางการเชื่อมต่อให้มากขึ้น แต่ทว่าข้อเสียก็คือ ความถี่ 5 GHz นั้นหลายๆประเทศไม่อนุญาตให้ใช้ เช่นประเทศไทย เพราะได้จัดสรรให้อุปกรณ์ประเภทอื่นไปแล้ว และยิ่งไปกว่านั้นระยะการส่งข้อมูลของ IEEE 802.11a ยังสั้นเพียง 30 เมตรเท่านั้น อีกทั้งอุปกรณ์ของ IEEE 802.11a ยังมีราคาสูงกว่า IEEE 802.11b ด้วย ดังนั้นอุปกรณ์ IEEE 802.11a จึงได้รับความนิยมน้อยกว่า IEEE 802.11b มาก จึงทำให้ไม่ค่อยเป็นที่ได้รับความนิยมเท่าที่ควร

มาตรฐาน IEEE 802.11g เสร็จสมบูรณ์ในปี พ.ศ. 2546 ทางคณะกรรมการ IEEE 802.11g ได้นำเอาเทคโนโลยี OFDM ของ 802.11a มาพัฒนาบนความถี่ 2.4 GHz จึงทำให้ใช้ความเร็ว 36-54 Mbps ซึ่งเป็นความเร็วที่สูงกว่ามาตรฐาน 802.11b ซึ่ง 802.11g สามารถปรับระดับความเร็วในการสื่อสารลงเหลือ 2 Mbps ได้ตามสภาพแวดล้อมของเครือข่ายที่ใช้งาน มาตรฐานนี้เป็นที่ยอมรับจากผู้ใช้เป็นจำนวนมากและเข้ามาแทนที่ 802.11b ในเวลาต่อมา

นอกจากที่กล่าวมาข้างต้นนี้ยังมีบางผลิตภัณฑ์ใช้เทคโนโลยีเฉพาะตัวเข้ามาเสริม ทำให้ความเร็วเพิ่มขึ้นจาก 54 Mbps เป็น 108 Mbps แต่ต้องทำงานร่วมกันเฉพาะอุปกรณ์ที่ผลิตจากบริษัทเดียวกันเท่านั้น ซึ่งความสามารถนี้เกิดจากชิป (Chip) กระจายสัญญาณของตัวอุปกรณ์ที่ผู้ผลิตบางรายสามารถเพิ่มประสิทธิภาพการรับส่ง สัญญาณเป็น 2 เท่าของการรับส่งสัญญาณได้แต่ปัญหาของการกระจายสัญญาณนี้จะมีผลทำให้อุปกรณ์ ไร้สายในมาตรฐาน 802.11b มีประสิทธิภาพลดลงด้วยเช่นกัน

มาตรฐาน IEEE 802.11e คณะทำงานชุดนี้ได้รับมอบหมายให้ปรับปรุง MAC Layer ของ IEEE 802.11 เพื่อให้สามารถรองรับการใช้งานหลักการ Quality of Service สำหรับ application เกี่ยวกับมัลติมีเดีย (Multimedia) เนื่องจาก IEEE 802.11e เป็นการปรับปรุง MAC Layer ดังนั้นมาตรฐานเพิ่มเติมนี้จึงสามารถ

นำไปใช้กับอุปกรณ์ IEEE 802.11 WLAN ทุกเวอร์ชันได้ แต่อย่างไรก็ตามการทำงานของคณะทำงานชุดนี้ยังไม่แล้วเสร็จในขณะนี้

มาตรฐาน IEEE 802.11i คณะทำงานชุดนี้ได้รับมอบหมายให้ปรับปรุง MAC Layer ของ IEEE 802.11 ในด้านความปลอดภัย เนื่องจากเครือข่าย IEEE 802.11 WLAN มีช่องโหว่อยู่มากโดยเฉพาะอย่างยิ่งการเข้ารหัสข้อมูล (Encryption) ด้วย key ที่ไม่มีการเปลี่ยนแปลง คณะทำงานชุด IEEE 802.11i จะนำเอาเทคนิคขั้นสูงมาใช้ในการเข้ารหัสข้อมูลด้วย key ที่มีการเปลี่ยนค่าอยู่เสมอและการตรวจสอบผู้ใช้ที่มีความปลอดภัยสูง มาตรฐานเพิ่มเติมนี้จึงสามารถนำไปใช้กับอุปกรณ์ IEEE 802.11 WLAN ทุกเวอร์ชันได้ แต่อย่างไรก็ตามการทำงานของคณะทำงานชุดนี้ยังไม่แล้วเสร็จในขณะนี้

มาตรฐาน IEEE 802.11n เป็นมาตรฐานที่ทาง Wi-Fi Alliance มีความเร็วในการถ่ายโอนข้อมูลอยู่ที่ 74 Mbps และสูงสุดที่ 248 Mbps ซึ่งหมายความว่าความเร็วเร็วกว่ารุ่นก่อนถึงประมาณ 5 เท่า นอกจากนี้ก็ยังมีรัศมีทำการภายในอาคารที่ 70 เมตร และนอกอาคารที่ 160 เมตร เพิ่มความสามารถในการกันสัญญาณรบกวนจากอุปกรณ์อื่นๆ ที่ใช้ความถี่ 2.4GHz เหมือนกัน และสามารถรองรับอุปกรณ์มาตรฐาน IEEE 802.11b และ IEEE 802.11g ได้ มาตรฐาน IEEE 802.11n นี้ได้เสร็จสมบูรณ์ในปี พ.ศ. 2552 แล้ว รวมทั้งมีคุณสมบัติ MIMO

MIMO เป็นคำย่อของ Multiple-Input Multiple-Output เป็นเทคโนโลยีการประมวลผลสัญญาณขั้นสูงที่ใช้เสารับและส่งสัญญาณ (receiver/transmitter) หลายชุดทั้งที่อยู่ในเครื่องลูกข่ายและแอ็กเซสพอยน์ ทำให้สัญญาณมีความคมชัดและมีประสิทธิภาพสูงขึ้น

10.2.4 วิวัฒนาการของมาตรฐาน IEEE 802.11

Wi-Fi ซึ่งเป็นเทคโนโลยีเครือข่ายท้องถิ่นไร้สาย (WLAN) ที่ช่วยให้อุปกรณ์ดิจิทัลภายในพื้นที่หนึ่งสามารถสื่อสารกันผ่านคลื่นวิทยุถูกนำมาใช้อย่างแพร่หลายและแพร่หลายในปัจจุบัน จนแทบจำไม่ได้ว่าเคยมียุคใดที่ยังไม่มี Wi-Fi แต่ในความเป็นจริงแล้วช่วงเวลานั้นไม่ได้ยาวนานนัก

Wi-Fi เข้าสู่ตลาดครั้งแรกในปี พ.ศ. 2540 เมื่อมีการประกาศมาตรฐานทางเทคนิค IEEE 802.11 อันเป็นมาตรฐานแรก ซึ่งทำให้สามารถส่งข้อมูลแบบไร้สายได้ความเร็วสูงสุด 2 เมกะบิตต่อวินาที โดยใช้คลื่นความถี่วิทยุ 2.4 GHz โดยไม่ต้องมีใบอนุญาต ความก้าวหน้าทางการค้าครั้งสำคัญเกิดขึ้นในปี พ.ศ. 2542 เมื่อ Apple เปิดตัวผลิตภัณฑ์สำหรับผู้บริโภคครั้งแรกที่วางจำหน่ายในตลาดมวลชน ซึ่งประกอบด้วยเครื่องเชื่อมต่อ Wi-Fi มาตรฐานไร้สาย AirPort และ iBook ด้วยการแก้ไขมาตรฐาน Wi-Fi เดิมของ IEEE 802.11b™ ในขณะนั้น ทำให้สามารถส่งข้อมูลทางทฤษฎีได้สูงถึง 11 เมกะบิตต่อวินาที

หลังจากนั้นไม่นาน Apple ก็ได้เปิดตัว AirPort ที่ใช้มาตรฐาน IEEE 802.11b ซึ่งเป็นจุดเริ่มต้นของการปฏิวัติระบบไร้สายแม้ว่าจะเป็นความจริง แต่สิ่งที่ทำให้การปฏิวัตินี้เกิดขึ้นได้ตั้งแต่แรกก็คือมาตรฐาน IEEE 802.11

นับตั้งแต่นั้นมา วิวัฒนาการอย่างต่อเนื่องของ มาตรฐาน Wi-Fi IEEE 802.11ได้นำไปสู่อัตราการส่งข้อมูลที่รวดเร็วขึ้นมาก ระยะการเชื่อมต่อที่ไกลขึ้น และการเชื่อมต่อที่เชื่อถือได้และปลอดภัยยิ่งขึ้น มาตรฐาน IEEE 802.11 ฉบับแก้ไขทั้งหมดได้รับการออกแบบในลักษณะที่อุปกรณ์ที่ทำงานตามข้อกำหนดจะสามารถใช้งานร่วมกับเวอร์ชันก่อนหน้าได้ เพื่อให้อุปกรณ์ที่ใช้ IEEE 802.11 รุ่นใหม่สามารถสื่อสารกับผลิตภัณฑ์รุ่นเก่าได้ รูป 10.5 แสดงวิวัฒนาการของ Wi-Fi



รูป 10.5 แสดงวิวัฒนาการของมาตรฐาน Wi-Fi

(ที่มา: <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>)

มาตรฐาน IEEE สำหรับ Wi-Fi

ระหว่างทางนั้น Wi-Fi Alliance (“Wi-Fi #”) ได้พัฒนารูปแบบการตั้งชื่อเพื่อช่วยให้ประชาชนทั่วไปสามารถแยกแยะระหว่างการใช้งาน IEEE 802.11 ต่างๆ ได้ดีขึ้น ประกอบด้วย:

- **IEEE 802.11™** เป็นมาตรฐาน Wi-Fi ความถี่ 2.4 GHz รุ่นแรกที่ถูกกล่าวถึงข้างต้นตั้งแต่ปี 1997 และยังคงใช้ชื่อเรียกนี้อยู่ มาตรฐานนี้และการแก้ไขเพิ่มเติมที่ตามมาเป็นพื้นฐานสำหรับเครือข่ายไร้สาย Wi-Fi และเป็นตัวแทนของโปรโตคอลเครือข่ายคอมพิวเตอร์ไร้สายที่ใช้กันอย่างแพร่หลายที่สุดในโลก
- **IEEE 802.11b™** เปิดตัวสู่ตลาดในปี พ.ศ. 2542 พร้อมกับการประกาศของ Apple มาตรฐานนี้ยังทำงานที่ความถี่ 2.4 GHz แต่เพื่อลดสัญญาณรบกวนจากเตาไมโครเวฟ โทรศัพท์ไร้สาย จอภาพเด็ก และแหล่งสัญญาณอื่นๆ และเพื่อให้ได้อัตราข้อมูลที่สูงขึ้น จึงได้รวมรูปแบบการมอดูเลตที่เรียกว่า direct-sequence spread spectrum/complementary code keying (DSSS/CCK) ไว้ด้วย IEEE 802.11b ช่วยให้สามารถสื่อสารไร้สายได้ในระยะทางประมาณ 38 เมตรภายในอาคาร และประมาณ 140 เมตรภายนอกอาคาร
- **IEEE 802.11a™** ซึ่งเปิดตัวในปี พ.ศ. 2542 ถือเป็นมาตรฐานต่อยอดจาก IEEE 802.11b นับเป็นมาตรฐาน Wi-Fi แรกที่มีระบบมัลติแครีเออร์มอดูเลชัน (OFDM) เพื่อรองรับอัตราข้อมูลสูง รองรับการทำงานที่ความถี่ 5 GHz และแบนด์วิดท์ 20 MHz รองรับอัตราข้อมูลหลายอัตรา
- **IEEE 802.11g™** เปิดตัวในปี พ.ศ. 2546 รองรับอัตราข้อมูลสูงสุด 54 Mbps ในย่านความถี่ 2.4 GHz เดียวกับ IEEE 802.11b ด้วยรูปแบบการมอดูเลตแบบหลายคลื่นพาหะ OFDM และการปรับปรุงอื่นๆ ซึ่งทำให้ผู้ใช้ในตลาดทั่วไปสนใจ เนื่องจากอุปกรณ์ 2.4 GHz มีราคาถูกกว่าอุปกรณ์ 5 GHz

- **IEEE 802.11n™ หรือ Wi-Fi 4** เปิดตัวในปี พ.ศ. 2552 เพื่อรองรับย่านความถี่ 2.4 GHz และ 5 GHz ด้วยอัตราข้อมูลสูงสุด 600 Mbps รองรับหลายช่องสัญญาณในแต่ละย่านความถี่ และคุณสมบัติอื่นๆ ทรูพุดข้อมูลของ IEEE 802.11n ช่วยให้สามารถใช้เครือข่าย WLAN แทนเครือข่ายแบบใช้สาย ซึ่งเป็นคุณสมบัติสำคัญที่นำไปสู่การใช้งานรูปแบบใหม่ๆ และลดต้นทุนการดำเนินงานสำหรับผู้ให้บริการและองค์กรไอที

ตาราง 10.2 สรุปเปรียบเทียบคุณสมบัติสำคัญของ IEEE 802.11b/a/g/n

มาตรฐาน	คุณสมบัติเด่น	ข้อดี-ข้อด้อย
802.11b	ประเภทคลื่นความถี่ (Band) ISM (Industrial Scientific and Medical) ย่านความถี่ (Frequency) 2.4 GHz ความเร็ว (Throughput) สูงสุด 11 Mbps ระยะทำการ (Coverage area) 100 เมตร	ข้อดี • ต้นทุนต่ำสุด • ช่วงสัญญาณดีและไม่บดบังได้ง่าย • ระยะทางไกลเทียบเท่าแลนใช้สาย ข้อด้อย • ความเร็วต่ำ • ความเร็วยังแปรผันตามระยะทาง สิ่งกีดขวางจำนวนผู้ใช้ สัญญาณรบกวน • ถูกรบกวนได้ง่ายจาก เตาไมโครเวฟ โทรศัพท์ไร้สาย บลูทูธ
802.11a	ประเภทคลื่นความถี่ (Band) U-NII (Unlicensed National Information Infrastructure) ย่านความถี่ (Frequency) 5 GHz ความเร็ว (Throughput) สูงสุด 54 Mbps ระยะทำการ (Coverage area) 10 เมตร	ข้อดี • ความเร็วสูง • ความถี่ควบคุมป้องกันการรบกวนสัญญาณจากอุปกรณ์อื่น ข้อด้อย • ต้นทุนสูงทั้งอุปกรณ์และความถี่ • ระยะทำการต่ำ
802.11g	ประเภทคลื่นความถี่ (Band) ISM (Industrial Scientific and Medical)	ข้อดี • พัฒนาจากพื้นฐานของ 802.11b

มาตรฐาน	คุณสมบัติเด่น	ข้อดี-ข้อด้อย
	ย่านความถี่ (Frequency) 2.4 GHz ความเร็ว (Throughput) สูงสุด 54 Mbps ระยะทำการ (Coverage area) 100 เมตร	● ความเร็วสูง ● ข้อด้อย ● ต้นทุนสูงกว่า 802.11b
802.11n	ประเภทคลื่นความถี่ (Band) ISM (Industrial Scientific and Medical) ย่านความถี่ (Frequency) 2.4 GHz ความเร็ว (Throughput) ระยะหวังผล 100 Mbps ระยะทำการ (Coverage area) 100-160 เมตร	ข้อดี ● มีคุณสมบัติ MIMO ● ความเร็วสูง ● ย่านความถี่ทนทานต่อสิ่งรบกวน ข้อด้อย ● ต้นทุนสูง ● หลายผลิตภัณฑ์ยังไม่รองรับมาตรฐาน ● สัญญาณอาจรบกวนบริเวณใกล้เคียง

- IEEE 802.11ac™ หรือ Wi-Fi 5 เปิดตัวในปี 2013 เพื่อรองรับอัตราข้อมูลสูงสุด 3.5 Gbit/s พร้อมแบนด์วิดท์ที่มากขึ้น ช่องสัญญาณที่เพิ่มขึ้น การมอดูเลตที่ดีขึ้น และคุณสมบัติอื่นๆ นับเป็นมาตรฐาน Wi-Fi แรกที่รองรับเทคโนโลยี MIMO (Multiple Input/Multiple Output) เพื่อให้สามารถใช้เสาอากาศหลายเสาได้ทั้งบนอุปกรณ์ส่งและรับสัญญาณ เพื่อลดข้อผิดพลาดและเพิ่มความเร็ว
- Wi-Fi 6 ระบุความหนาแน่นของเครือข่ายและให้ประสิทธิภาพสเปกตรัม

IEEE 802.11ax™ หรือ Wi-Fi 6 คือมาตรฐานล่าสุดในซีรีส์นี้ ซึ่งเผยแพร่ในปี 2021 และปัจจุบันมีการนำอุปกรณ์ที่ใช้มาตรฐานดังกล่าวไปปรับใช้ในอุปกรณ์หลายพันล้านเครื่องต่อปี

แม้ว่าอัตราข้อมูลเชิงทฤษฎีจะอยู่ที่ 9.6 กิกะบิตต่อวินาที แต่มาตรฐานนี้ไม่ได้มุ่งเน้นที่การเพิ่มความเร็ว Wi-Fi เพียงอย่างเดียว แต่มุ่งแก้ไขปัญหการใช้งาน Wi-Fi ที่แพร่หลายในปัจจุบัน จนทำให้ประสิทธิภาพของเครือข่ายลดลงในพื้นที่ที่มีการใช้งาน Wi-Fi หนาแน่น เช่น สนามกีฬา หอแสดงคอนเสิร์ต และศูนย์กลางการขนส่ง

สาธารณะ และยังแย่งลงไปอีก แม้แต่ในบ้านของเราที่เราเตอร์ต้องสื่อสารกับอุปกรณ์ดิจิทัลจำนวนมากขึ้นเรื่อยๆ พร้อมกัน

IEEE 802.11ax นำเสนอการปรับปรุงมากมาย โดยมีการใช้กลไกแบบหลายผู้ใช้ (multi-user) ที่ทำให้สามารถแบ่งอัตราข้อมูล 9.6 Gbit/s ให้กับอุปกรณ์ต่างๆ ได้ นอกจากนี้ยังรองรับเราเตอร์ที่ส่งข้อมูลไปยังอุปกรณ์หลายเครื่องในเฟรมเดียวแบบออกอากาศผ่านอากาศ และช่วยให้อุปกรณ์ Wi-Fi สามารถกำหนดเวลาการส่งข้อมูลไปยังเราเตอร์ได้ นอกจากนี้ยังมีการเพิ่มกลไกเพื่อรองรับการใช้งานกลางแจ้งระยะไกลอีกด้วย

เมื่อพิจารณาโดยรวมแล้ว คุณสมบัติเหล่านี้จะช่วยปรับปรุงปริมาณงานโดยรวมและรองรับการใช้งาน Wi-Fi ที่เพิ่มมากขึ้นในสถานการณ์ที่มีข้อมูลจำนวนมาก และในแอปพลิเคชันต่างๆ เช่น วิดีโอและการเข้าถึงระบบคลาวด์ ซึ่งต้องการประสิทธิภาพแบบเรียลไทม์และการใช้พลังงานต่ำสำหรับอุปกรณ์ที่ใช้พลังงานแบตเตอรี่ โดยเฉพาะอย่างยิ่ง วิดีโอความละเอียดสูงคาดว่าจะจะเป็นประเภทการรับส่งข้อมูลหลักในการใช้งาน Wi-Fi ที่กำลังจะเกิดขึ้นในอนาคต

Wi-Fi 7: ก้าวต่อไปของวิวัฒนาการ Wi-Fi

ปัจจุบัน IEEE P802.11be™ หรือ Wi-Fi 7 เป็นการพัฒนาที่ IEEE Standards Association (IEEE SA) โดยกลุ่มผู้เชี่ยวชาญด้านเทคนิคและอุตสาหกรรมแล้วเสร็จภายในปี 2024

มาตรฐานนี้ถือเป็นก้าวสำคัญด้านวิวัฒนาการของเทคโนโลยี Wi-Fi ด้วยอัตราการส่งข้อมูลที่เร็วขึ้น 4 เท่า (~40 กิกะบิต/วินาที) และแบนด์วิดท์ที่เพิ่มขึ้นสองเท่า (ช่องสัญญาณ 320 MHz เทียบกับช่องสัญญาณ 160 MHz สำหรับ Wi-Fi 6) นอกจากนี้ยังรองรับการใช้งานคลื่นความถี่ที่มีอยู่และต่อเนื่องได้อย่างมีประสิทธิภาพและเชื่อถือได้มากขึ้น ผ่านการรวมคลื่นความถี่หลายย่านความถี่/หลายช่องสัญญาณและวิธีการอื่นๆ มาตรฐานนี้มีการปรับปรุงโปรโตคอล MIMO มากมาย รวมถึงความก้าวหน้าและการปรับปรุงความสามารถของ Wi-Fi ที่มีอยู่ในปัจจุบันอีกมากมาย

ผลลัพธ์ของการปรับปรุงทางเทคนิคทั้งหมดนี้ทำให้ผู้ใช้ได้รับเทคโนโลยี Wi-Fi 7 ที่รวดเร็วยิ่งขึ้น มีเวลาแฝงต่ำกว่ามาก รองรับอุปกรณ์ได้มากขึ้น และทำงานได้ดีขึ้นมากในพื้นที่ Wi-Fi ที่มีการใช้งานหนาแน่นและที่เครือข่าย Wi-Fi ทับซ้อนกัน

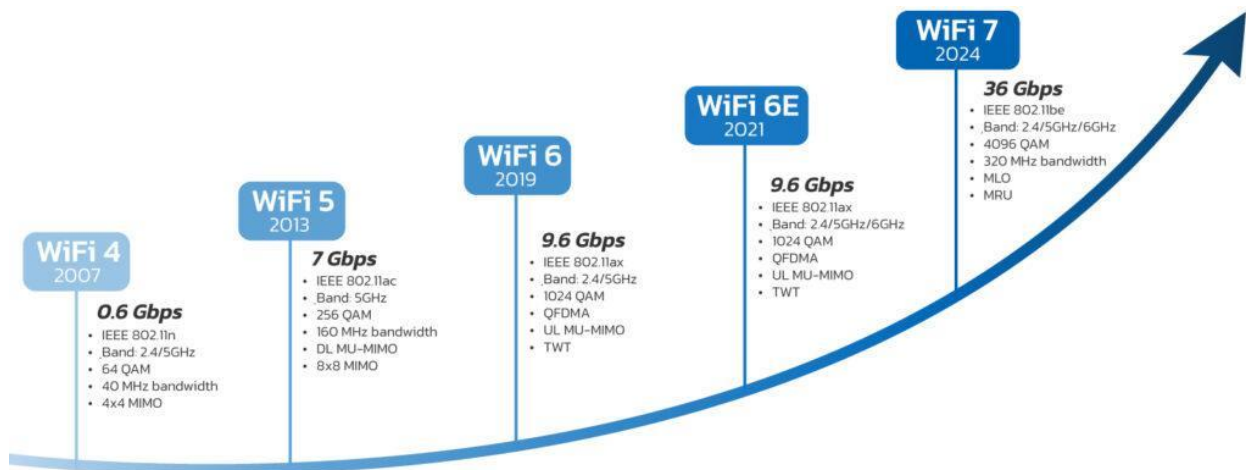
มาตรฐาน IEEE 802.11 ที่พัฒนาขึ้นสำหรับกรณีการใช้งาน Wi-Fi ใหม่และที่เกิดขึ้นใหม่

IEEE P802.11be ควบคู่ไปกับ IEEE 802.11ax และมาตรฐาน IEEE 802.11 ในอนาคต สามารถรองรับแอปพลิเคชัน Wi-Fi รุ่นต่อไปได้อีกมากมายคณะทำงาน IEEE 802.11 ได้จัดตั้งกลุ่มเฉพาะทางขึ้นหลายกลุ่มเพื่อศึกษาแอปพลิเคชันเหล่านี้ ต่อไปนี้คือตัวอย่างบางส่วน:

- **เครือข่ายอินเทอร์เน็ตออฟริงส์ (IoT) ที่ใช้พลังงานจากสภาพแวดล้อมและไม่ต้องใช้แบตเตอรี่** – พลังงานจากสภาพแวดล้อม หมายถึงพลังงานที่เก็บเกี่ยวได้จากสิ่งแวดล้อม เช่น ความร้อน ซึ่งจะถูกลดแปลงเป็นพลังงานไฟฟ้า พลังงานนี้สามารถนำไปใช้จ่ายพลังงานให้กับอุปกรณ์ IoT แบบกระจาย นำไปสู่ระบบ

IoT ที่ไม่ต้องใช้แบตเตอรี่และเป็นมิตรต่อสิ่งแวดล้อมมากขึ้น โดยไม่จำเป็นต้องบำรุงรักษามากนัก เครือข่าย IoT ที่ไม่ต้องใช้แบตเตอรี่อาจเป็นประโยชน์ต่อหลายอุตสาหกรรม เช่น เกษตรกรรม โครงข่ายไฟฟ้าอัจฉริยะ เหมืองแร่ การผลิต โลจิสติกส์ บ้านอัจฉริยะ การขนส่ง และอื่นๆ ขณะนี้กำลังมีการศึกษาเพื่อศึกษากรณีการใช้งาน ข้อกำหนดด้านฟังก์ชันการทำงาน และความเป็นไปได้ทางเทคนิคของการเพิ่มคุณสมบัติต่างๆ ลงในมาตรฐาน IEEE 802.11 เพื่อรองรับอุปกรณ์ IoT ที่ใช้พลังงานจากสภาพแวดล้อม

- **เทคโนโลยี Augmented/Virtual Reality (AR/VR) และ Metaverse** – แอปพลิเคชันเหล่านี้ต้องการปริมาณข้อมูลสูงมากและความหน่วงต่ำมาก ผู้ใช้เทคโนโลยีสำหรับผู้บริโภคที่กำลังเติบโตอย่างรวดเร็วเหล่านี้ต้องการเครือข่าย Wi-Fi ที่เร็วขึ้น ราบรื่นขึ้น และเชื่อถือได้มากขึ้น กลุ่มศึกษา IEEE 802.11 Extremely High Throughput Study Group ก่อตั้งขึ้นเพื่อศึกษาคุณสมบัติใหม่ๆ ของ IEEE 802.11 สำหรับย่านความถี่ระหว่าง 1 ถึง 7.125 GHz ซึ่งจะช่วยให้เพิ่มปริมาณข้อมูลสูงสุดเพื่อรองรับแอปพลิเคชันที่ต้องการประสิทธิภาพสูงเหล่านี้
- **ปัญญาประดิษฐ์/การเรียนรู้ของเครื่อง (AI/ML)** – การใช้เทคนิค AI/ML เติบโตอย่างรวดเร็วในช่วงไม่กี่ปีที่ผ่านมา และครอบคลุมแทบทุกด้านของความพยายามของมนุษย์ อัลกอริทึม AI/ML จำเป็นต้องใช้ข้อมูลจำนวนมากในการถ่ายโอนระหว่างแหล่งข้อมูลแบบกระจาย เช่น กล้อง สมาร์ทโฟน และอุปกรณ์เล่นเกม และเซิร์ฟเวอร์ส่วนกลางที่ใช้วิเคราะห์ข้อมูล เพื่อตอบสนองความต้องการนี้ อัลกอริทึม AI/ML ใหม่ ๆ จึงได้รับการพัฒนาขึ้น ซึ่งช่วยให้สามารถวิเคราะห์ข้อมูลได้มากขึ้น ณ แหล่งที่มา ช่วยลดปริมาณข้อมูลที่เครือข่ายต้องรับส่ง เครือข่าย Wi-Fi ที่ใช้มาตรฐาน IEEE 802.11 มีข้อมูลจำนวนมากและเพิ่มขึ้นเรื่อยๆ ทำให้สามารถใช้ประโยชน์จากอัลกอริทึม AI/ML ใหม่ ๆ เช่น การเรียนรู้แบบรวมศูนย์ เพื่อปรับปรุงประสิทธิภาพของ Wi-Fi และประสบการณ์ผู้ใช้ ขณะนี้กลุ่มผู้สนใจพิเศษภายใน IEEE 802.11 WG กำลังศึกษาแนวคิดนี้อยู่



รูป 10.6 วิวัฒนาการ WiFi4-WiFi7

(ที่มา: <https://ifocusshop.com/wi-fi-7-technology-network/>)

10.2.5 สรุปมาตรฐาน IEEE 802.11

สรุปมาตรฐานตามอนุกรมของ IEEE 802.11 ได้ประกาศออกมาอย่างเป็นทางการมีมากกว่าที่ระบุไว้ข้างต้น ดังแสดงในตาราง 10.3

ตาราง 10.3 สรุปมาตรฐาน IEEE 802.11

มาตรฐาน	ความหมาย
802.11a	มาตรฐาน IEEE สำหรับเครือข่ายไร้สายที่ทำงานที่ 5 GHz มีอัตราข้อมูลสูงสุด 54Mbps
802.11b	มาตรฐาน IEEE สำหรับเครือข่ายไร้สายที่ทำงานที่ 2.4 GHz มีอัตราข้อมูลสูงสุด 11Mbps
802.11d	IEEE คุณสมบัติที่ช่วยให้การเปลี่ยนแปลงการกำหนดค่าที่ชั้น Media Access Control (MAC layer) ระดับการปฏิบัติตามกฎของประเทศที่เป็นเครือข่ายที่จะใช้ (ดู MAC)
802.11e	มาตรฐาน IEEE ที่เพิ่มคุณภาพของบริการ (QoS) คุณสมบัติและการสนับสนุนมัลติมีเดียที่มีอยู่ 802.11b, 802.11g และ 802.11a เครือข่ายไร้สาย
802.11f	รู้จักกันในอีกชื่อว่า IAPP (Inter Access Point Protocol) เป็นมาตรฐานที่ออกแบบมาให้ Access Point คุยกันโดยใช้ Layer 2 เพื่อจัดการกับผู้ใช้ที่เคลื่อนที่ข้ามขอบข่ายการให้บริการจาก Access Point ตัวหนึ่งไปหา Access Point อีกตัวหนึ่ง (Roaming)
802.11g	มาตรฐาน IEEE สำหรับเครือข่ายไร้สายที่ทำงานที่ 2.4 GHz Wi-Fi ที่มีอัตราข้อมูลสูงสุด 54Mbps
802.11h	802.11h สนับสนุน Dynamic Frequency Selection (DFS) และส่ง Power Control (TPC) ข้อกำหนดเพื่อให้อยู่ร่วมกันระหว่าง Wi-Fi และประเภทอื่นๆ อุปกรณ์ความถี่ใน 5 วง GHz เป็นมาตรฐานที่ออกแบบมาให้ระบบ WLAN ที่ทำงานในความถี่ 5GHz สามารถทำงานได้ถูกต้องตามข้อกำหนดการใช้ความถี่ของค่ายยุโรป ซึ่งมาตรฐานนี้จะถูกรองรับโดย EU
802.11i	มาตรฐาน IEEE กำหนดกลไกการรักษาความปลอดภัยสำหรับเครือข่าย 802.11 802.11i ทำให้การใช้ Advanced Encryption Standard (AES) ตัวเลขบล็อก มาตรฐานรวมถึงการปรับปรุงในการจัดการคีย์ตรวจสอบผู้ใช้งาน 802.1X และความสมบูรณ์ของข้อมูลของส่วนหัว

มาตรฐาน	ความหมาย
802.11j	คุณสมบัติ IEEE สำหรับเครือข่ายไร้สายที่ประกอบด้วยข้อกำหนดเกี่ยวกับญี่ปุ่นส่งไฟฟ้าไร้สาย output, โหมดการดำเนินงานการจัดช่องและระดับการปล่อยมารยา
802.11k	เป็นมาตรฐานที่ทำให้ระบบ WLAN สามารถจัดการได้ง่ายขึ้น โดยให้ข้อมูลด้านการจัดการ เช่น ข้อมูลการใช้ความถี่ หรือข้อมูลเกี่ยวกับเครือข่ายสามารถส่งไปมาบนเน็ตเวิร์คเพื่อให้ระบบจัดการสามารถทำงานจากศูนย์กลางได้
802.11n	รุ่นล่าสุดของเทคโนโลยี Wi-Fi สนับสนุน 802.11n Multiple-Input/Multiple-Output (MIMO) อุปกรณ์เทคโนโลยีการรับและส่งสัญญาณหลายหลายทั้งลูกค้าและจุดเชื่อมต่อเพื่อให้เกิดประสิทธิภาพดีขึ้นผลิตภัณฑ์ designated เป็น Wi-Fi n CERTIFIED สามารถทำงานได้ทั้งใน 2.4 หรือ 5 GHz ความถี่และเข้ากันได้กับ 802.11 a / b / g เครือข่าย 802.11n เทคโนโลยีสามารถส่งอัตราข้อมูลได้ถึง 600 Mbps
802.1X	มาตรฐานในการตรวจสอบ port-based ใช้ครั้งแรกในเครือข่ายสายที่ถูกดัดแปลงเพื่อใช้ใน WLANs องค์กรที่อยู่ผิดพลาดความปลอดภัยใน WEP, คุณสมบัติการรักษาความปลอดภัยเดิม 802.11 เครือข่าย 802.1X ให้กรอบสำหรับผู้ใช้ในการตรวจสอบและการควบคุมการเข้าถึงเครือข่ายเพื่อป้องกันและคีย์การเข้ารหัสแบบไดนามิกเพื่อปกป้องข้อมูลส่วนตัว

ตาราง 10.3 เปรียบเทียบคุณสมบัติสำคัญของมาตรฐานปัจจุบัน Wi-Fi4/5/6/7



เปรียบเทียบ WiFi แต่ละรุ่น

	WiFi 4	WiFi 5	WiFi 6	WiFi 6E	WiFi 7
วันที่เปิดตัว	2007	2013	2019	2021	2024
มาตรฐาน IEEE	802.11n	802.11ac	802.11ax		802.11be
ส่งข้อมูลสูงสุด	0.6 Gbps	7 Gbps	9.6 Gbps		36 Gbps
คลื่นความถี่	2.4 GHz, 5 GHz	5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz, 6 GHz	
ความปลอดภัย	WPA 2		WPA 3		WPA4 (TBD)
ช่องสัญญาณความถี่	20, 40 MHz	20, 40, 80, 80+80, 160 MHz		20, 40, 80, 80+80, 160, 320 MHz	
การแปลงสัญญาณ	64 QAM OFDM	256 QAM OFDM	1024 QAM OFDMA		4096 QAM OFDMA (with extensions)
เสาอากาศ	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 DL+ UL MU-MIMO		16x16 MLO MRU

รูป 10.7 เปรียบเทียบไวไฟแต่ละรุ่น

(ที่มา: <https://ifocusshop.com/wi-fi-7-technology-network/>)

มาตรฐานใหม่ WiFi 7 จะรองรับคลื่นความถี่ 2.4GHz, 5GHz, 6GHz โดยที่มีการปรับปรุงเสถียรภาพที่ดียิ่งขึ้น การเชื่อมต่อที่เร็วขึ้น มีความน่าเชื่อถือที่มั่นคง ความปลอดภัยที่สูงขึ้น ส่งข้อมูลได้เร็วขึ้นอย่างไม่มีปัญหา รองรับการใช้งานบริการ สตรีมมิง 8K A/V, AR/VR, การเล่นเกมบนคลาวด์, แอปพลิเคชันแบบโต้ตอบ, IoT ด้านอุตสาหกรรมและอุตสาหกรรม 4.0, การวินิจฉัยระยะไกลและการผ่าตัดระยะไกลได้เป็นอย่างดี

10.3 สรุปบท

เนื้อหาในบทนี้กล่าวถึงวิวัฒนาการของมาตรฐาน Wi-Fi ตั้งแต่ 802.11n ที่เน้นประสิทธิภาพและความเข้ากันได้ ไปจนถึง WiFi 7 ซึ่งพัฒนาให้รองรับความถี่หลากหลายและความเร็วสูง ตลอดจนมาตรฐาน 802.1X ที่เน้นการรักษาความปลอดภัยเครือข่าย นอกจากนี้ ยังชี้ให้เห็นถึงแนวคิดและหลักการออกแบบเครือข่ายที่มุ่งเน้นความมั่นคงปลอดภัย เช่น การใช้ไฟร์วอลล์, DMZ, การแบ่งโซนเครือข่าย และมาตรการป้องกันภัยคุกคาม เพื่อให้เครือข่ายมีประสิทธิภาพและปลอดภัยสูงสุด

10.4 บทวิเคราะห์และมุมมองเชิงวิชาการ: “การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (Secured Network Design)”

เอกสารคำสอน บทเรียน การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (สัปดาห์ที่ 9) ของรายวิชา หลักการความมั่นคงทางไซเบอร์ มุ่งเน้นให้ผู้เรียนเข้าใจหลักการออกแบบเครือข่ายคอมพิวเตอร์ที่สามารถต้านทานต่อภัยคุกคามสมัยใหม่ได้อย่างมีประสิทธิภาพ เนื้อหาครอบคลุมตั้งแต่การกำหนดขอบเขตเครือข่าย การบังคับใช้ firewall และ IDS/IPS การใช้ NAT, VPN, DMZ ไปจนถึงการแบ่งโซนเครือข่าย (Network zoning) และโซนเฝ้าระวัง (Monitoring zoning) ทั้งหมดนี้สะท้อนถึงการเรียนการสอนที่มุ่งเน้นการเชื่อมโยงทฤษฎีเข้ากับการปฏิบัติ และการออกแบบที่ใช้ได้จริง สรุปสาระสำคัญของการวิเคราะห์และมุมมองเชิงวิชาการได้ดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

1. หลักการ Perimeter Defense – ไฟร์วอลล์ถูกนำมาใช้เป็น “แนวป้องกันแรก” เพื่อควบคุมให้ทราฟฟิกทั้งหมดผ่านจุดตรวจสอบที่ชัดเจน
2. การแยกโฮสต์และการใช้ DMZ – แบ่งแยกโฮสต์ภายใน (trusted) กับโฮสต์ภายนอก (untrusted) โดยโฮสต์ที่ต้องให้บริการสาธารณะ เช่น mail server, web server ถูกจัดให้อยู่ใน DMZ เพื่อลดผลกระทบเมื่อถูกโจมตี
3. การควบคุมช่องทางพิเศษ – เช่น remote access หรือ extranet ต้องใช้ VPN และการพิสูจน์ตัวตนที่เข้มงวด
4. NAT และการอำพราง IP – ใช้เพื่อป้องกันการโจมตีโดยตรงและจำกัดการเข้าถึงจากภายนอก
5. Threat Model & Phases of Compromise – อธิบายขั้นตอนการบุกรุกตั้งแต่ reconnaissance → exploitation → reinforcement → consolidation → pillage ช่วยให้นักศึกษามองเห็นวงจรการโจมตีและสามารถวางมาตรการตอบสนองได้อย่างมีเหตุผล
6. การแบ่งโซนเครือข่ายและโซนเฝ้าระวัง – ใช้ firewall และ sensors เพื่อจำกัดและตรวจสอบทราฟฟิกทั้งภายใน ภายนอก DMZ และ wireless zone

2) มุมมองเชิงวิชาการและความก้าวหน้าปัจจุบัน

1. **จาก Perimeter Defense → Zero Trust** แม้ firewall และ DMZ จะยังสำคัญ แต่ปัจจุบันเครือข่ายองค์กรมีการเชื่อมต่อกับ cloud, SaaS และ IoT ทำให้ perimeter-based model ไม่เพียงพอ แนวทาง Zero Trust Architecture (ZTA) จึงกลายเป็นมาตรฐานใหม่ เน้น *identity, least privilege, continuous verification*
2. **Network Segmentation → Micro-Segmentation** การแบ่งโซนเครือข่ายในบทเรียนถือเป็นรากฐาน แต่สถาปัตยกรรมสมัยใหม่ใช้ micro-segmentation ด้วย SDN/SD-WAN ทำให้การควบคุมละเอียดถึงระดับ workload และ application
3. **Monitoring → AI-driven SOC** จากการติดตั้ง sensors ในทุกโซน ปัจจุบัน SOC (Security Operations Center) ใช้ AI/ML-driven anomaly detection และ MITRE ATT&CK-based threat hunting ทำให้การเฝ้าระวังมีประสิทธิภาพและ proactive มากขึ้น
4. **VPN → ZTNA/SASE VPN** แบบเดิมถูกแทนที่ด้วย Zero Trust Network Access (ZTNA) และ Secure Access Service Edge (SASE) ที่รวม SD-WAN + Cloud Security Controls เช่น CASB, SWG, FWaaS

3) ประสบการณ์และการสอดแทรกเชิงการสอน

จากประสบการณ์การสอนและทำงานในสายวิชาชีพและสายวิชาการ ผู้สอนพบว่าการฝึกให้ผู้เรียนมีทักษะ “Design for Visibility” มีความสำคัญมากกว่าการป้องกันเพียงอย่างเดียว กล่าวคือต้องออกแบบระบบให้ “มองเห็นการบุกรุก” ได้เสมอ แนวคิดนี้สอดคล้องกับแนวทางของ NIST CSF และ Zero Trust ซึ่งจะช่วยให้ผู้เรียนเข้าใจว่าเป้าหมายของ cybersecurity ไม่ใช่การป้องกันที่สมบูรณ์แบบ แต่คือการ *จำกัดความเสียหาย ตรวจจับเร็ว และตอบสนองได้ทันเวลา*

บทเรียน “การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย” สร้างพื้นฐานการคิดเชิงสถาปัตยกรรมที่สำคัญ โดยเน้น firewall, DMZ, NAT, VPN, Threat Model และ Monitoring Zoning อย่างไรก็ดี เพื่อสะท้อนความก้าวหน้าทางวิชาการและอุตสาหกรรม สามารถปรับให้เชื่อมโยงกับ Zero Trust, Micro-segmentation, Cloud-native security และ AI-driven SOC สิ่งเหล่านี้จะทำให้ผู้เรียนไม่เพียงแต่เข้าใจหลักการ แต่สามารถออกแบบเครือข่ายให้ทันสมัยและสอดคล้องกับโลกจริง

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง WPAN, WLAN และ WWAN พร้อมยกตัวอย่าง

แนวคำตอบ: WPAN = Bluetooth/Infrared; WLAN = Wi-Fi IEEE 802.11; WWAN = Cellular (LTE/5G)

ข้อ 2. อธิบายโหมดการเชื่อมต่อ WLAN แบบ Infrastructure และ Ad-Hoc

แนวคำตอบ: Infrastructure = มี Access Point เชื่อมต่อเครือข่าย; Ad-Hoc = อุปกรณ์เชื่อมตรงกัน ไม่มี AP

ข้อ 3. วิเคราะห์ข้อดี-ข้อจำกัดของ WLAN เทียบกับเครือข่ายแบบใช้สาย

แนวคำตอบ: WLAN = ยืดหยุ่น ขยายง่าย แต่เสถียรภาพต่ำกว่า ความเร็วต่ำกว่า ถูกดักฟังได้ง่าย

ข้อ 4. อธิบายวิวัฒนาการของมาตรฐาน IEEE 802.11 จาก Wi-Fi 4 ถึง Wi-Fi 7

แนวคำตอบ: Wi-Fi 4 = 802.11n, Wi-Fi 5 = 802.11ac, Wi-Fi 6 = 802.11ax, Wi-Fi 7 = 802.11be → เพิ่มความเร็ว, ลด latency, รองรับอุปกรณ์มากขึ้น

ข้อ 5. เสนอแนวทางป้องกันการโจมตี Sniffing และ Man-in-the-Middle บน WLAN

แนวคำตอบ: ใช้ WPA3, VPN, Captive Portal, การเข้ารหัส End-to-End

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. เทคโนโลยีใดเป็นตัวอย่างของ WPAN

ก. Bluetooth

ข. Wi-Fi

ค. LTE

ง. Fiber Optic

เฉลย: ก

ข้อ 2. WLAN ใช้มาตรฐานใด

ก. IEEE 802.3

ข. IEEE 802.11

ค. IEEE 802.16

ง. IEEE 802.15

เฉลย: ข

ข้อ 3. โหมด Infrastructure WLAN ต้องมีอุปกรณ์ใด

ก. Router

ข. Access Point

ค. Switch

ง. Bridge

เฉลย: ข

ข้อ 4. ข้อใดคือข้อดีของเครือข่ายไร้สาย

ก. เสถียรภาพสูงสุด

ข. ความเร็วสูงกว่าใยแก้วนำแสง

ค. ความยืดหยุ่นและขยายง่าย

ง.ปลอดภัยกว่ามีสาย

เฉลย: ค

ข้อ 5. ข้อใดคือข้อจำกัดของเครือข่ายไร้สาย

ก. ความเร็วต่ำกว่าและถูกรบกวนง่าย

ข. ความยืดหยุ่นสูง

ค. ต้นทุนการติดตั้งต่ำ

ง. ครอบคลุมพื้นที่กว้าง

เฉลย: ก

ข้อ 6. มาตรฐาน IEEE 802.11n ถูกเรียกว่า Wi-Fi รุ่นใด

ก. Wi-Fi 3

ข. Wi-Fi 4

ค. Wi-Fi 5

ง. Wi-Fi 6

เฉลย: ข

ข้อ 7. มาตรฐานใดมีความเร็วสูงสุดและรองรับการใช้งาน AR/VR ได้ดี

ก. Wi-Fi 4

ข. Wi-Fi 5

ค. Wi-Fi 6

ง. Wi-Fi 7

เฉลย: ง

ข้อ 8. การโจมตีแบบ Sniffing มีผลกระทบอย่างไร

ก. ทำให้เครือข่ายล่มทันที

ข. ดักจับข้อมูลที่ส่งผ่านเครือข่าย

ค. ทำให้สัญญาณอ่อนลง

ง. เพิ่มความเร็วในการส่งข้อมูล

เฉลย: ข

ข้อ 9. มาตรฐานความปลอดภัยใดแทนที่ WEP และ WPA2

ก. WPA3

ข. VPN

ค. HTTPS

ง. DMZ

เฉลย: ก

ข้อ 10. ข้อใดคือการใช้ Zero Trust บนเครือข่ายไร้สาย

ก. เปิดให้ทุกคนเข้าถึงโดยไม่ตรวจสอบ

ข. ตรวจสอบตัวตนและกำหนดสิทธิ์อย่างต่อเนื่อง

ค. ใช้เพียง Firewall ภายนอก

ง. ใช้เพียงการเข้ารหัส WEP

เฉลย: ข

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิริเชษฐ์ โพธิ์hirัญ. (ม.ป.ป.). เครือข่ายไร้สาย (Wireless Network). เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Cisco Systems. (2021). *Network Security Design Guide*.

Gartner. (2021). *Market Guide for Secure Access Service Edge (SASE)*.

Kindervag, J. (2010). *No More Chewy Centers: Introducing Zero Trust*. Forrester Research.

MITRE. (2023). *ATT&CK Framework for Enterprise*.

NIST. (2020). *Zero Trust Architecture (SP 800-207)*.

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*.

Stallings, W. (2021). *Foundations of Security Architecture*. Pearson.

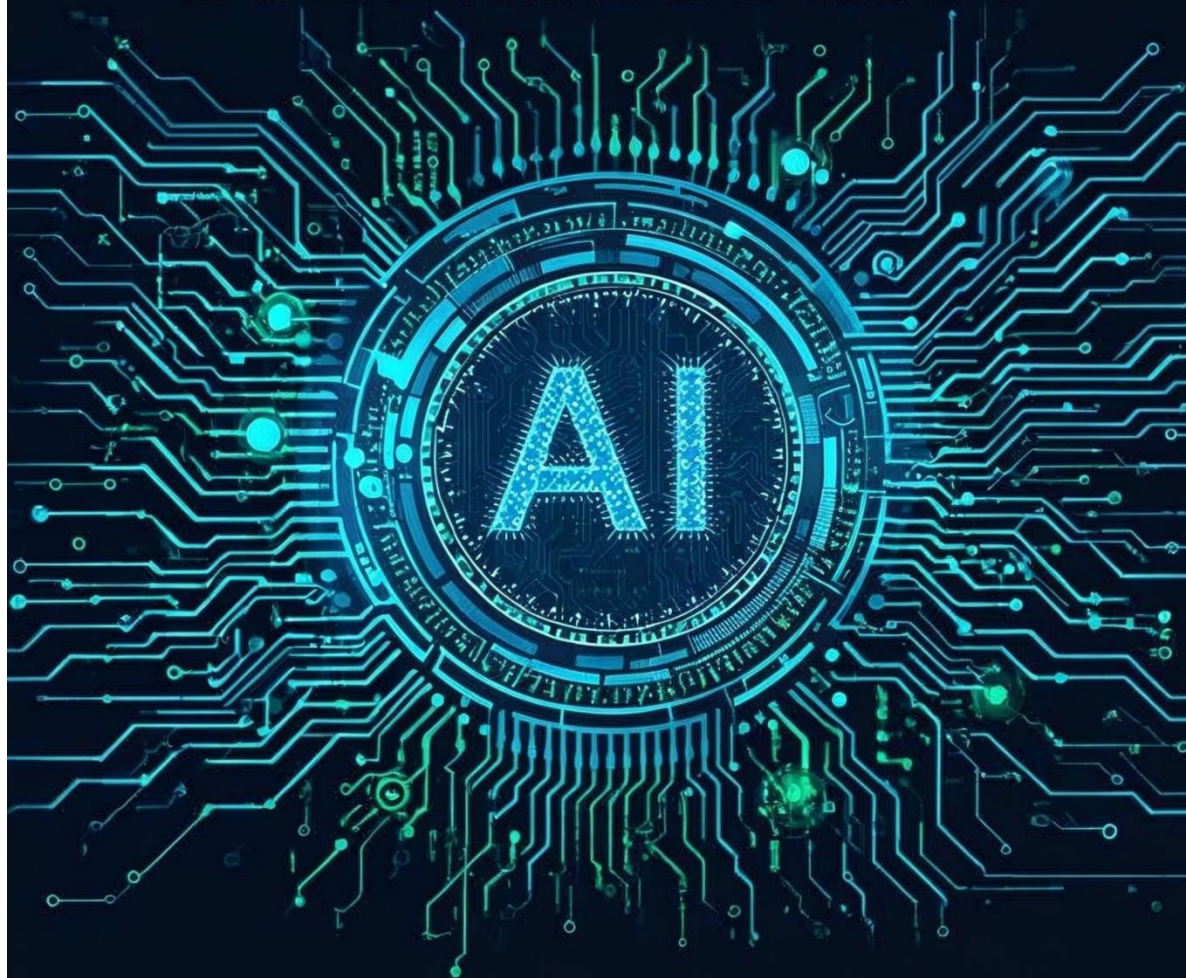
บทที่ 11

ความมั่นคงปลอดภัยเครือข่ายไร้สาย

Wireless Network Security

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ โพรธีรัตน์

บทที่ 11 ความมั่นคงปลอดภัยเครือข่ายไร้สาย (Wireless Network Security)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบบทนี้ นักศึกษาจะสามารถ:

- 1) อธิบายประเภทของการโจมตีเครือข่ายไร้สายและช่องโหว่ของมาตรฐาน IEEE 802.11 ได้
- 2) อธิบายวิวัฒนาการของกลไกความปลอดภัยไร้สาย (WEP, WPA, WPA2, WPA3, IEEE 802.11i, 802.1X) ได้
- 3) วิเคราะห์ภัยคุกคาม (เช่น MiTM, Rogue AP, Jamming, Brute Force, Confidentiality /Integrity /Access Control Attacks) ได้
- 4) ประเมินมาตรการป้องกันเครือข่ายไร้สาย (Firewall, VPN, Captive Portal, MFA, SSO) ได้
- 5) ประยุกต์ใช้มาตรฐานความปลอดภัยไร้สายกับสถานการณ์จริง เช่น Wi-Fi องค์กร/สาธารณะ ได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบบทนี้ นักศึกษาจะสามารถ:

- 1) ระบุและอธิบายรูปแบบการโจมตีไร้สาย 8 ประเภท (insertion, interception, jamming, client-to-client, brute force, encryption, misconfiguration, MITM) ได้
- 2) อธิบายกลไกและมาตรฐานด้านความปลอดภัยไร้สาย (WEP, WPA, WPA2, WPA3, IEEE 802.11i, IEEE 802.1X) ได้
- 3) วิเคราะห์ภัยคุกคามและผลกระทบต่อองค์กร เช่น WarDriving, Rogue AP, Evil Twin ได้
- 4) ประเมินแนวทางและมาตรการป้องกัน เช่น การเข้ารหัส WPA3, VPN, Firewall, การปิด SSID ได้
- 5) ประยุกต์ใช้ความรู้ในการออกแบบ WLAN ที่ปลอดภัยสำหรับองค์กรหรือเครือข่ายสาธารณะได้

3. หัวข้อเนื้อหา:

11.1 การโจมตีและการป้องกันเครือข่ายไร้สาย

11.1.1 ประเภทของการโจมตีเครือข่ายไร้สาย

11.1.2 แนวคิดการป้องกันการบุกรุกแบบไร้สาย

11.2 วิศวกรรมความมั่นคงปลอดภัยในมาตรฐาน IEEE 802.11

11.2.1 WEP (Wired Equivalent Privacy)

11.2.2 มาตรฐาน IEEE 802.11i-2004

11.2.3 มาตรฐาน IEEE 802.1X

11.2.4 Wi-Fi Protected Access (WPA และ WPA2)

11.2.5 WPA3

11.2.6 เปรียบเทียบโพรโทคอลความปลอดภัยเครือข่ายไร้สาย 4 ประเภท

11.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi

11.3.1 แนวทางรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi

11.3.2 ความปลอดภัยแบบไร้สายในสภาพแวดล้อมเฉพาะ

11.3.3 กลไกการตรวจสอบสิทธิ์ 4 ประการสำหรับการรักษาความปลอดภัยเครือข่ายไร้สาย

11.4 ภัยคุกคามเครือข่ายไร้สายและผลกระทบต่อองค์กร

11.4.1 ภัยคุกคามเครือข่ายไร้สาย Wi-Fi Chalking

11.4.2 ภัยคุกคามเครือข่ายไร้สาย Access control attacks

11.4.3 ภัยคุกคามเครือข่ายไร้สาย Integrity attacks

11.4.4 ภัยคุกคามเครือข่ายไร้สาย Confidentiality attacks

11.4.5 วิธีการสร้างความปลอดภัยสำหรับเครือข่ายไร้สาย

11.5 มาตรการป้องกันการโจมตีทางเครือข่ายไร้สาย

11.5.1 แนวปฏิบัติที่ดีสำหรับป้องกันความปลอดภัยเครือข่ายไร้สาย

11.5.2 มาตรการความปลอดภัยของเครือข่ายแบบไร้สายสำหรับองค์กร

11.5.3 การป้องกันการปฏิเสธการให้บริการ

11.6 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา:

บริษัท *RMUTT CityCafe* เปิดให้บริการ Wi-Fi ฟรีสำหรับลูกค้า แต่พบว่าการโจมตี **Evil Twin AP** ทำให้ผู้ใช้ถูกหลอกให้เชื่อมต่อกับ AP ปลอม ส่งผลให้ข้อมูลบัตรเครดิตถูกขโมย นักศึกษาต้องวิเคราะห์และเสนอแนวทางแก้ไข

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4–5 คน):

1. วิเคราะห์ลักษณะการโจมตี Evil Twin และผลกระทบต่อผู้ใช้/องค์กร
2. ศึกษามาตรฐานการรักษาความปลอดภัย (WPA3, IEEE 802.1X, Captive Portal, VPN)
3. เสนอแนวทางแก้ไข เช่น การบังคับใช้ WPA3-Personal/Enterprise, VPN, Firewall, SSID Management
4. นำเสนอ Diagram ของ WLAN ใหม่ที่ปลอดภัยกว่า

ประเด็นการเรียนรู้:

- ประเภทการโจมตีเครือข่ายไร้สาย 8 ประเภท
- กลไกการป้องกันมาตรฐาน IEEE 802.11 และ WPA3
- ภัยคุกคามไร้สาย (Evil Twin, MITM, Rogue AP, WarDriving)
- มาตรการรักษาความปลอดภัย Wi-Fi ในองค์กรและสาธารณะ

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์การโจมตี (25)	ครอบคลุม Evil Twin + ผลกระทบชัดเจน	ครบแต่ยังไม่ลึก	กล่าวบางส่วน	ไม่ถูกต้อง
การอ้างอิงมาตรฐาน (25)	ระบุ WPA3, 802.1X, Captive Portal, VPN ครบ	กล่าวถึงบางส่วน	กล่าวไม่ครบ	ขาดการอ้างอิง

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
แนวทางแก้ไข (30)	ครอบคลุมหลายมาตรการ ปฏิบัติได้จริง	ครอบคลุม บางส่วน	ไม่ชัดเจน	ขาดข้อเสนอ
การนำเสนอ (20)	ชัดเจน + Diagram	ชัดเจน	พอใช้	ไม่ชัดเจน

11. ความมั่นคงปลอดภัยเครือข่ายไร้สาย

ความปลอดภัยแบบไร้สายเป็นอีกแง่มุมหนึ่งของความปลอดภัยทางคอมพิวเตอร์ องค์กรต่างๆ อาจมีความเสี่ยงเป็นพิเศษต่อการละเมิดความปลอดภัยที่เกิดจากจุดเชื่อมต่อที่ไม่น่าเชื่อถือ หากพนักงานเพิ่มอินเทอร์เน็ตไร้สายลงในพอร์ตที่ไม่มีการรักษาความปลอดภัยของระบบ พวกเขาอาจสร้างช่องโหว่ด้านความปลอดภัยของเครือข่ายที่ทำให้สามารถเข้าถึงข้อมูลลับได้ มาตรการป้องกันเช่น การปิดใช้งานพอร์ตสวิตช์ที่เปิดอยู่ระหว่างการกำหนดค่าสวิตช์ และการกำหนดค่า VLAN เพื่อจำกัดการเข้าถึงเครือข่าย เป็นสิ่งที่สามารถทำได้เพื่อปกป้องเครือข่ายและข้อมูลที่อยู่ในเครือข่าย แต่มาตรการป้องกันดังกล่าวต้องบังคับใช้กับอุปกรณ์เครือข่ายทั้งหมดอย่างเท่าเทียมกัน

11.1 การโจมตีและการป้องกันเครือข่ายไร้สาย

ช่องโหว่ด้านความปลอดภัยของเครือข่าย IEEE 802.11 โดยทั่วไปแล้วระบบแลนไร้สายมีความเสี่ยงต่อการถูกโจมตีมากกว่าระบบเครือข่ายที่ใช้สาย เนื่องจากสัญญาณข้อมูลแพร่กระจายอยู่ในอากาศ และไม่จำกัดขอบเขตอยู่เพียงแต่ในห้องๆ เดียวหรือบริเวณแคบๆ เท่านั้น แต่สัญญาณอาจจะแพร่ไปถึงบริเวณภายนอกเขตความดูแลขององค์กรได้ อาจทำให้ผู้บุกรุกสามารถดักฟัง ปลอมแปลงสัญญาณข้อมูล หรือบุกรุกระบบของท่านได้โดยไม่ต้องปรากฏตัวให้เห็น ยิ่งไปกว่านั้นผู้โจมตีอาจใช้อุปกรณ์สายอากาศพิเศษที่ทำให้สามารถรับส่งสัญญาณจากบริเวณภายนอกที่ไกลออกไปได้มาก อีกทั้งเทคโนโลยีสำหรับการรักษาความปลอดภัยที่ใช้ในมาตรฐาน IEEE 802.11 ที่ใช้กันอยู่มีช่องโหว่อยู่มากดังได้กล่าวแล้วข้างต้น สามารถสรุปประเภทของการโจมตีเครือข่ายไร้สายได้ดังนี้

11.1.1 ประเภทของการโจมตีเครือข่ายไร้สาย

- การปลอมขึ้น (insertion/fabrication attack)
- การดักฟังและการเฝ้าดูทราฟฟิกของระบบไร้สายโดยไม่ได้รับอนุญาต (Interception and unauthorized monitoring of wireless traffic)
- การรบกวน (Jamming)
- การโจมตีจากลูกข่าย (Client-to-Client attacks)
- Brute force attacks against access point passwords การโจมตีแบบ Brute-force เป็นการโจมตีที่ผู้โจมตีทำการเดาคำกุญแจทุกค่าที่เป็นไปได้แล้วนำคำกุญแจที่ได้มาถอดรหัสข้อความ
- การโจมตีการเข้ารหัส (Encryption attacks)
- การกำหนดค่าติดตั้งที่ผิดพลาด (Misconfigurations)

- การโจมตีแบบ Man-in-Middle (MiM) หรือ Man-In-The-Middle (MITM)

การโจมตีทั้ง 8 ประเภทดังกล่าวเป็นวิธีการโจมตีที่ไม่ได้เกิดขึ้นเฉพาะแลนไร้สาย 802.11 เท่านั้น แต่เป็นพื้นฐานของการโจมตีเครือข่ายไร้สายทุกประเภท จึงควรทำความเข้าใจไว้เพื่อเป็นข้อมูลในการเตรียมการป้องกันระบบไร้สาย มีรายละเอียดดังนี้

การปลอมขึ้น (insertion/fabrication attack)

การรูปแบบการโจมตีด้านการพิสูจน์ตัวจริง (Authentication attack) การโจมตีอาจทำได้โดยสร้างบัญชีรายชื่อผู้ใช้ปลอมขึ้นมาใหม่ การติดตั้ง/ปรับใช้อุปกรณ์ที่ไม่ได้รับอนุญาต สร้างเครือข่ายไร้สายขึ้นมาใหม่ได้ไม่ได้รับอนุญาตหรือไม่ผ่านกระบวนการด้านความปลอดภัย มีรูปแบบดังนี้

ลูกข่ายที่ไม่ได้รับอนุญาต (Unauthorized Clients)

ผู้บุกรุกพยายามเชื่อมต่อเครื่องลูกข่ายไร้สาย เช่น คอมพิวเตอร์แบบพกพา PDA เพื่อทะลุผ่านเข้าไปยังแอ็กเซสพอยน์ ซึ่งโดยปกติจะต้องกำหนดการป้อนรหัสผ่าน แต่ถ้าแอ็กเซสพอยน์นั้นไม่ได้มีการกำหนดรหัสผ่านไว้ ผู้บุกรุกก็จะสามารถเชื่อมต่อเข้าสู่เครือข่ายไร้สายได้อย่างง่ายดาย และมีอิสระที่จะเข้าทรัพยากรภายในเครือข่ายได้เท่าเทียมกับลูกข่ายเครื่องอื่นๆ เช่นเดียวกันกับแอ็กเซสพอยน์บางตัวที่ใช้รหัสผ่านชุดเดียวกันสำหรับลูกข่ายทุกเครื่อง (default password) จำเป็นที่ลูกข่ายต้องเปลี่ยนรหัสผ่านใหม่ก่อนใช้งานจริง

แอ็กเซสพอยน์เถื่อนหรือที่ไม่ได้รับอนุญาต (Unauthorized or Renegade Access Points)

บางองค์กรอาจมิได้ตระหนักถึงระบบรักษาความปลอดภัยในการใช้เครือข่ายไร้สายมากพอ จึงอาจมีพนักงานนำแอ็กเซสพอยน์เข้ามาติดตั้งเองเพื่อเข้าถึงทรัพยากรเครือข่ายขององค์กรผ่านแอ็กเซสพอยน์เถื่อน (rogue access point) ดังนั้น องค์กรจึงควรติดตั้งนโยบายความปลอดภัย (security policy) สำหรับทุกการเข้าถึงเครือข่ายเพื่อประกันความปลอดภัย อีกทั้งควรใช้เครื่องมือในการสแกนการเข้าถึงเครือข่ายไร้สายที่ไม่ได้อนุญาตอย่างสม่ำเสมอ

การดักฟังและการเฝ้าดูการจราจรของระบบไร้สายโดยไม่ได้รับอนุญาต (Interception and unauthorized monitoring of wireless traffic)

ในเครือข่ายแลนแบบใช้สาย ผู้บุกรุกจำเป็นต้องเข้ามาในบริเวณที่มีสายสัญญาณครอบคลุมไปถึง เช่น ในห้องแม่ข่าย บริเวณเครื่องลูกข่าย จุดเชื่อมจากอุปกรณ์ประเภทสวิตช์หรือฮับ ซึ่งโดยปกติแล้วยากที่บุคคลภายนอกจะเข้ามาได้เพราะถูกป้องกันโดยกายภาพอยู่แล้ว แต่สำหรับเครือข่ายไร้สาย เป็นไปไม่ได้ที่เราจะกำหนดบังคับให้สัญญาณจากแอ็กเซสพอยน์แพร่ไปเฉพาะขอบเขตที่กำหนด เมื่อผู้บุกรุกเพียงแต่นำอุปกรณ์รับสัญญาณเข้าอยู่ภายในรัศมีของสัญญาณ เช่น ประมาณ 100 เมตรจากแอ็กเซสพอยน์สำหรับ 802.11b ก็สามารถเชื่อมต่อเข้าสู่เครือข่ายของเราได้ทันที ถ้าเครือข่ายไม่ได้กำหนดระบบความปลอดภัยไว้ ทรัพยากรทั้งหมดภายในเครือข่ายของ

เราก็ปราศจากการป้องกัน เมื่อผู้บุกรุกเข้ามาอยู่ภายในเครือข่ายของเรา ก็สามารถใช้เครื่องมือในการดักฟังสัญญาณที่ส่งไปมาภายในเครือข่ายได้อย่างง่ายดาย การบุกรุกแบ่งออกเป็น 3 แบบ

การวิเคราะห์แพ็คเกจไร้สาย (wireless packet analysis)

ผู้บุกรุกที่มีความเชี่ยวชาญสามารถใช้เทคนิคและเครื่องมือสำหรับการวิเคราะห์แพ็คเกจไร้สาย เช่นเดียวกับที่ใช้สำหรับเครือข่ายแบบใช้สาย เครื่องมือเหล่านี้จะสามารถจับส่วนแรกของการเชื่อมต่อซึ่งข้อมูลมักรวมถึงชื่อผู้ใช้และรหัสผ่าน ผู้บุกรุกสามารถปลอมแปลงเป็นผู้ใช้ที่ถูกต้องโดยใช้บันทึกข้อมูลนี้เพื่อปล้นเซสชัน (session) ของผู้ใช้ เข้าปลอมตัวเป็นผู้ใช้ทำการแทนผู้ใช้ ทำให้ผู้ใช้ตัวจริงใช้งานไม่ได้

การเฝ้าดูการแพร่สัญญาณ (broadcast monitoring)

ถ้าแอกเซสพอยน์ต์เชื่อมต่อกับฮับแทนที่จะเปลี่ยนสวิตช์ ทุกการจราจรระหว่างลูกข่ายภายในเครือข่ายทั้งหมดจะเป็นการสื่อสารแบบแพร่สัญญาณ หมายความว่า ผู้บุกรุกจะสามารถมองเห็นและดักฟังทุกสัญญาณที่สื่อสารกันภายในเครือข่าย

การติดตั้งแอกเซสพอยน์ต์เชื่อมต่อลง (คูโง) เพื่อดักฟังการจราจร (Access Point Clone (Evil Twin) Traffic Interception)

ผู้บุกรุกพยายามติดตั้งแอกเซสพอยน์ต์ลงที่กำลังส่งแรงกว่าไว้คู่กับแอกเซสพอยน์ต์ตัวจริงขององค์กรเพื่อให้เครื่องลูกข่ายเชื่อมต่อผ่านแอกเซสพอยน์ต์ลงนี้แทนตัวจริง เมื่อลูกข่ายพยายามเชื่อมต่อผ่านอุปกรณ์นี้ สัญญาณการจราจร ชื่อผู้ใช้ รหัสผ่าน รวมทั้งข้อมูลลับก็จะถูกดักฟังได้ทั้งสิ้น

สัญญาณรบกวน (Jamming)

สัญญาณรบกวนเป็นปัญหาที่สำคัญอีกปัญหาหนึ่งที่หลีกเลี่ยงได้สำหรับแลนไร้สาย เนื่องจากเป็นธรรมชาติของการสื่อสารแบบไร้สายที่ใช้ความถี่ย่านสาธารณะ 2.4GHz. (ISM) ซึ่งมีอุปกรณ์ไร้สายหลากหลายชนิดใช้งานความถี่ร่วมกัน เช่น เตาไมโครเวฟ โทรศัพท์ไร้สาย บลูทูธ อุปกรณ์แลนไร้สายอื่นๆ สัญญาณรบกวนอาจเกิดจากคลื่นแม่ไฟฟ้าตามธรรมชาติเมื่อเกิดฝนตกฟ้าคะนอง โดยทั่วไปแล้วสัญญาณรบกวนในช่องสัญญาณจะสร้างปัญหาให้กับอุปกรณ์ภาครับ โดยทำให้ไม่สามารถแปลสัญญาณข้อมูลที่ถูกส่งมาได้อย่างถูกต้อง สำหรับแลนไร้สาย IEEE 802.11 นอกจากปัญหาดังกล่าวแล้วหากสัญญาณรบกวนในช่องสัญญาณที่ใช้อยู่มีกำลังสูงพอประมาณ โปรโทคอล CSMA/CA ซึ่งเป็นกลไกทำหน้าที่ควบคุมสิทธิในการส่งสัญญาณของอุปกรณ์แลนไร้สายจะไม่อนุญาตให้อุปกรณ์ใดๆ ทำการส่งสัญญาณได้เลย ผลที่เกิดขึ้นจากสัญญาณรบกวนในช่องสัญญาณนอกจากจะทำให้สมรรถนะของแลนไร้สายลดลงแล้วยังอาจทำให้เครือข่ายตกอยู่ในสภาวะปฏิเสธการให้บริการ (Denial-of-Service) ด้วย

การโจมตีจากลูกข่ายด้วยกัน (Client-to-client attack)

เครื่องลูกข่ายไร้สายสามารถเชื่อมต่อกับลูกข่ายไร้สายอื่นโดยไม่จำเป็นต้องผ่านแอ็กเซสพอยน์ในการเชื่อมต่อแบบแอดฮอค (Ad Hoc) หรือเพียร์-ทู-เพียร์ (peer-to-peer) โดยที่เจ้าของลูกข่ายไม่รู้ตัว ดังนั้น นอกเหนือจากองค์การป้องกันการโจมตีจากภายนอกแล้วยังต้องระวังการบุกรุกจากภายในด้วย รูปแบบของการโจมตีประกอบด้วย

การโจมตีการแบ่งปันแฟ้มและบริการ TCP/IP อื่นๆ (File Sharing and Other TCP/IP Service Attacks)

เครื่องลูกข่ายไร้สายมักเปิดบริการต่างๆ ของ TCP/IP ที่ไม่ได้ใช้งานทิ้งไว้ เช่น การแบ่งปันแฟ้ม การไม่ปิดช่องโหว่ การกำหนดค่าติดตั้งที่ไม่ถูกต้อง เป็นต้น เช่นเดียวกับเครื่องลูกข่ายในระบบมีสายทั่วไป แต่ระบบไร้สายนั้นเปิดโอกาสให้ถูกโจมตีได้ง่ายดายกว่า

การปฏิเสธการให้บริการ (DoS: Denial-of-Service)

หากไม่มีการระมัดระวังที่ดีพอ อุปกรณ์ไร้สายอาจส่งแพ็กเก็ตปริมาณมหาศาลไปโจมตีลูกข่ายไร้สายอื่นๆ หรือถูกใช้เป็นฐานในการโจมตีผู้อื่นด้วยการโจมตีแบบทำให้ใช้การไม่ได้ (DoS) นอกจากนั้น การกำหนดเลขไอพี หรือ MAC แอดเดรสซ้ำกันทั้งโดยเจตนาหรือไม่เจตนา ก็อาจเป็นสาเหตุทำความเสียหายแก่เครือข่ายได้

การโจมตีรหัสผ่านแบบ Brute Force เพื่อเข้าสู่แอ็กเซสพอยน์ (Brute Force Attacks Against Access Point Passwords)

แอ็กเซสพอยน์ส่วนใหญ่นิยมใช้รหัสผ่านหรือกุญแจชุดเดียวกันสำหรับเครื่องลูกข่ายทั้งหมด ผู้บุกรุกจึงสามารถโจมตีโดยการเดารหัสผ่าน หรืออาศัยพจนานุกรมรหัสผ่าน (Password dictionary) ที่ทำการเปรียบเทียบทุกค่าที่เป็นไปได้ของรหัสผ่าน ผู้บุกรุกจะสามารถเดารหัสผ่านได้ด้วยการเข้าถึงแค่เพียงครั้งแรก ดังนั้น การใช้งานแอ็กเซสพอยน์ในลักษณะนี้จึงไม่ยุ่งยากนัก รวมทั้งการตั้งรหัสผ่านที่ไม่แข็งแรง ก็ทำให้การเจาะรหัสผ่านสามารถทำได้ด้วยเวลาเพียงเล็กน้อย

นอกจากนั้น รหัสผ่านของแอ็กเซสพอยน์ที่ไม่ค่อยเปลี่ยนแปลงบ่อยๆ โอกาสที่พนักงานลาออกจากองค์กรไปก็ยังสามารถใช้รหัสผ่านเดิมเพื่อลักลอบเข้าถึงทรัพยากรขององค์กรได้ องค์กรขนาดใหญ่ที่มีแอ็กเซสพอยน์จำนวนมากจึงต้องเข้มงวดในเรื่องการนโยบายความปลอดภัยไปใช้อย่างรัดกุม

การโจมตีการเข้ารหัส (Attacks against Encryption)

802.11b ใช้ระบบการเข้ารหัสที่เรียกว่า WEP (Wired Equivalent Privacy) ซึ่งกลไกมีช่องโหว่ที่อาจทำให้ผู้โจมตีสามารถคำนวณหา key stream หรือรหัสลับที่ใช้ในเครือข่ายได้ การเจาะกลไกการเข้ารหัสของ WEP มีหลายรูปแบบเช่น การทดสอบรหัสทุกค่าที่เป็นไปได้ การสร้างพจนานุกรมของ Key Stream และการทำนายรหัสลับจาก Key Stream

กลไกการตรวจสอบผู้ใช้ (WEP Authentication) แบบ Shared Key ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 WLAN มีช่องโหว่ทำให้ผู้โจมตีสามารถล่วงรู้ความลับส่วนหนึ่งของเครือข่ายซึ่งผู้โจมตีสามารถนำไปใช้เพื่อผ่านการตรวจสอบและได้รับอนุญาตให้ใช้เครือข่ายได้อย่างถูกต้องหรือใช้ในการเข้ารหัสข้อมูลได้ นอกจากนั้นผู้โจมตียังสามารถที่จะถอดรหัสข้อมูลได้บางส่วนหรืออาจจะสามารถถอดรหัสลับของเครือข่ายได้ในที่สุดเมื่อผู้โจมตีรวบรวมข้อมูลดังกล่าวจนเพียงพอ

กลไกการตรวจสอบและอนุญาตผู้ใช้แบบใช้รหัสผ่าน (Shared-Key WEP Authentication) ตามมาตรฐาน IEEE 802.11 นั้นถูกเจาะได้ไม่ยาก และยังเป็นช่องโหว่ให้ผู้โจมตีสามารถคำนวณหารหัสลับของเครือข่ายได้ ซึ่งจะทำให้ความปลอดภัยของเครือข่าย IEEE 802.11 WLAN หดไปโดยสิ้นเชิง ดังนั้น ผู้ดูแลระบบจึงควรหลีกเลี่ยงการใช้กลไกตรวจสอบแบบ WEP โดยเปลี่ยนไปใช้เทคนิคอื่นเพื่อทำการตรวจสอบและอนุญาตผู้ใช้ เช่น WPA WPA2 เป็นต้น

การกำหนดค่าติดตั้งที่ผิดพลาด (Misconfiguration)

การติดตั้งแอพลิเคชันบางแห่งได้ละเลยการกำหนดค่าความปลอดภัย ซึ่งอาจเกิดจากเพื่อให้สะดวกต่อการใช้งาน หรือผู้ดูแลขาดความรู้ความเข้าใจและความตระหนักด้านความเสี่ยงความปลอดภัยของระบบไร้สาย รวมทั้งการกำหนดค่าที่ไม่ถูกต้อง ส่งผลให้การกำหนดค่าติดตั้งได้ถูกกละเลยไป หากองค์กรใช้ผลิตภัณฑ์ต่างยี่ห้อกันจำนวนมาก วิธีการกำหนดค่าที่ถูกต้องเหมาะสมก็ย่อมขึ้นอยู่กับข้อกำหนดที่เหมาะสมของแต่ละผลิตภัณฑ์อีกด้วย ซึ่งสร้างความยุ่งยากแก่ผู้ดูแลระบบได้

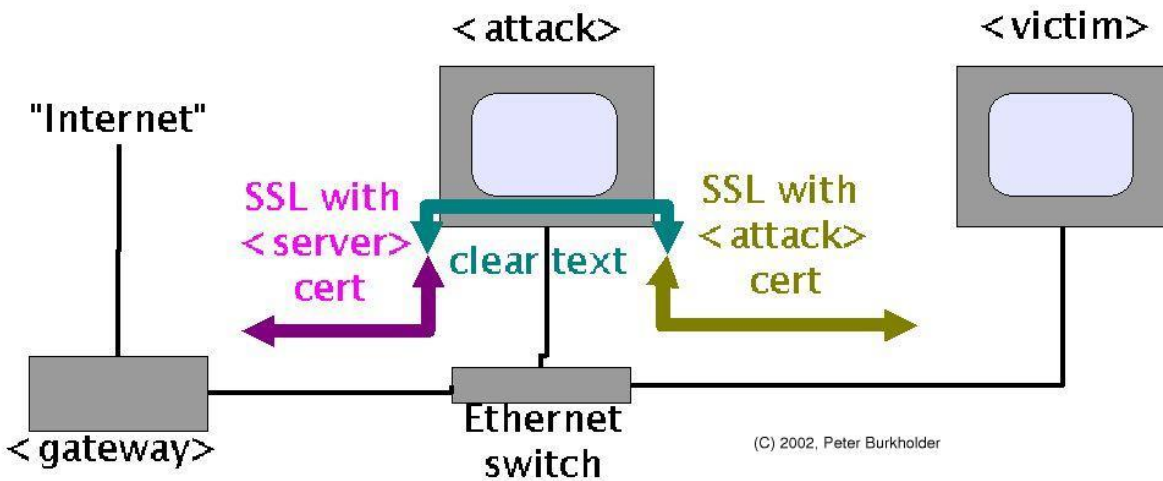
การโจมตีแบบ Man-in-Middle (MiM) หรือ Man-In-The-Middle (MITM)

การโจมตีแบบ Man In The Middle หรือ การแทรกแซงการสื่อสาร เป็นการโจมตีที่ผู้โจมตีเข้ามาแทรกแซงการสื่อสารของ A และ B โดยสามารถดักฟังหรือดักจับข้อมูลการสื่อสารระหว่าง A และ B ได้

ในการโจมตีด้วย MITM จะพบได้ทั้งแลนแบบมีสายและไร้สาย โดยในระยะแรกที่มีการใช้ฮับ ผู้โจมตีก็จะใช้โปรแกรมสเนฟเฟอร์ต่างๆ ในการดักจับข้อมูล เนื่องจากการทำงานของฮับจะทำการส่งข้อมูลไปทุกพอร์ตบนฮับ โปรแกรมสเนฟเฟอร์ก็สามารถดักจับข้อมูลได้ไม่ยาก

เมื่อมีการนำสวิตช์มาใช้แทนฮับ การโจมตีก็ต้องปรับเปลี่ยนวิธี เนื่องจากอุปกรณ์ประเภทสวิตช์จะส่งข้อมูลไปเฉพาะที่พอร์ตปลายทางเท่านั้น จึงป้องกันการดักจับข้อมูลด้วย MITM ได้

อย่างไรก็ตาม ปัจจุบันการโจมตีด้วย MITM จะอาศัยการทำงานที่เรียกว่า ARP Spoofing หรือ ARP Poisoning เพื่อที่จะหลอกให้ Gateway เข้าใจว่าเครื่องของผู้โจมตีเป็นเครื่องของเหยื่อ และหลอกเหยื่อให้เข้าใจว่าเครื่องของผู้โจมตีเป็น Gateway ดังรูป 11.1 จะทำให้ข้อมูลที่ส่งจากเครื่องเหยื่อจะมาถึงที่เครื่องของผู้โจมตีก่อนที่จะส่งต่อไป Gateway จึงทำให้ผู้โจมตีสามารถดักจับข้อมูลของเหยื่อได้



รูป 11.1 รูปแบบการโจมตีแบบ MITM โดยใช้ webMITM

(ที่มา: <http://www.pburkholder.com/sysadmin/SSL-mitm/index.php>)

ในการโจมตีแบบ Man-in-Middle ผู้โจมตีจะลวงให้ผู้ใช้งานเชื่อมต่อเข้ากับอุปกรณ์สถานีแม่ข่ายของผู้โจมตีซึ่งจะทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลที่ใช้รับส่งอยู่ได้ เนื่องจากมาตรฐาน IEEE 802.11 ไม่ได้บังคับให้สถานีผู้ใช้งานทำการ Authenticate สถานีแม่ข่ายก่อนเข้ารับบริการ ซึ่งสถานีผู้ใช้งานสามารถเชื่อมต่อเข้ากับสถานีแม่ข่ายใดๆ ก็ได้ที่ให้บริการ และโดยปกติสถานีผู้ใช้งานจะเลือกที่จะเชื่อมต่อเข้ากับสถานีแม่ข่ายที่มีกำลังรับส่งสูงกว่า ดังนั้นผู้โจมตีอาจสามารถล่อลวงให้สถานีผู้ใช้งานเชื่อมต่อกับสถานีแม่ข่ายของผู้โจมตีที่มีกำลังรับส่งสูงกว่าได้

11.1.2 แนวคิดการป้องกันการบุกรุกแบบไร้สาย

วิธีหลักในการรักษาความปลอดภัยเครือข่ายไร้สาย แบ่งออกเป็น 3 ประการ

สำหรับเครือข่ายแบบปิด (เช่น ผู้ใช้ตามบ้านและองค์กร) วิธีที่นิยมใช้กันมากที่สุดคือการกำหนดค่าข้อจำกัดการเข้าถึงในจุดเชื่อมต่อข้อจำกัดเหล่านี้อาจรวมถึงการเข้ารหัสและการตรวจสอบที่อยู่ MAC ระบบป้องกันการบุกรุกแบบไร้สาย (Wireless Intrusion Prevention Systems)สามารถนำมาใช้เพื่อรักษาความปลอดภัยเครือข่าย LAN ไร้สายในเครือข่ายรูปแบบนี้

สำหรับผู้ให้บริการเชิงพาณิชย์ฮอตสปอตและองค์กรขนาดใหญ่ โซลูชันที่ได้รับความนิยมมักจะเป็นเครือข่ายไร้สายแบบเปิดที่ไม่มีการเข้ารหัส แต่แยกตัวโดยคลื่นเชิง ผู้ใช้จะไม่สามารถเข้าถึงอินเทอร์เน็ตหรือทรัพยากรเครือข่ายท้องถิ่นใดๆ ได้ในตอนแรก ผู้ให้บริการเชิงพาณิชย์มักจะส่งต่อทราฟฟิกเว็บทั้งหมดไปยังพอร์ทัล

แบบ Captive ซึ่งรองรับการชำระเงินและ/หรือการอนุญาต อีกวิธีหนึ่งคือการกำหนดให้ผู้ที่ใช้เชื่อมต่อกับเครือข่ายที่มีสิทธิพิเศษอย่างปลอดภัยโดยใช้ VPN

เครือข่ายไร้สายมีความปลอดภัยน้อยกว่าเครือข่ายแบบใช้สาย ในสำนักงานหลายแห่ง ผู้บุกรุกสามารถเข้ามาและเชื่อมต่อคอมพิวเตอร์ของตนเองเข้ากับเครือข่ายแบบใช้สายได้อย่างง่ายดายโดยไม่มีปัญหาใดๆ จึงสามารถเข้าถึงเครือข่ายได้ นอกจากนี้ ผู้บุกรุกจากระยะไกลยังสามารถเข้าถึงเครือข่ายผ่านช่องทางลับเช่น Back Orifice ได้อีก ด้วยวิธีแก้ปัญหาลักษณะนี้ไปอย่างหนึ่งคือการเข้ารหัสแบบ end-to-end โดยมีการตรวจสอบสิทธิ์อิสระสำหรับทรัพยากรทั้งหมดที่ไม่ควรเปิดเผยต่อสาธารณะ

ยังไม่มีระบบที่ออกแบบมาอย่างพร้อมเพรียงเพื่อป้องกันการใช้งานการสื่อสารไร้สายโดยมิชอบ หรือเพื่อปกป้องข้อมูลและฟังก์ชันต่างๆ ของคอมพิวเตอร์และหน่วยงานอื่นๆ ที่สื่อสารไร้สาย อย่างไรก็ตาม มีระบบการประเมินมาตรการที่ดำเนินการโดยรวมตามความเข้าใจร่วมกัน ซึ่งถือเป็นมาตรฐานที่ทันสมัย ระบบการประเมินนี้เป็นฉันทามติระดับนานาชาติตามที่ระบุไว้ใน ISO/IEC 15408

11.2 วิศวกรรมความมั่นคงปลอดภัยในมาตรฐาน IEEE 802.11

แลนไร้สายมีปัญหาเกี่ยวกับประเด็นด้านความปลอดภัย ทั้ง IEEE และ Wi-Fi Alliance จึงได้มีการพัฒนากลไกรักษาความปลอดภัยขึ้นมาเพื่อแก้ปัญหาดังกล่าว ในที่นี้จะสรุปกลไกสำคัญที่ใช้ในแลนไร้สายได้แก่ WEP, IEEE802.11i, IEEE802.11X, WPA/WPA2 และ WPA3

11.2.1 WEP (Wired Equivalent Privacy)

มาตรฐาน IEEE 802.11 ได้กำหนดให้มีทางเลือกสำหรับสร้างความปลอดภัยให้กับเครือข่าย LAN แบบไร้สาย ด้วยกลไกซึ่งมีชื่อเรียกว่า WEP (Wired Equivalent Privacy) ซึ่งถูกออกแบบมาเพื่อเพิ่มความปลอดภัยกับเครือข่าย LAN แบบไร้สายให้ใกล้เคียงกับความปลอดภัยของเครือข่าย LAN แบบที่ใช้สายนำสัญญาณ (IEEE 802.3 Ethernet) บทบาทของ WEP แบ่งเป็น 2 ส่วนหลักๆ คือ

การเข้ารหัส (Encryption) เพื่อป้องกันมิให้ผู้ที่ไม่มีรหัสข้อมูลสามารถเข้าใจหรือเปลี่ยนแปลงข้อมูลที่แพร่กระจายอยู่ในอากาศได้

การพิสูจน์ตัวตนจริง (Authentication) เพื่อป้องกันมิให้ผู้ที่ไม่มีรหัสผ่านสามารถเข้าใช้เครือข่ายได้

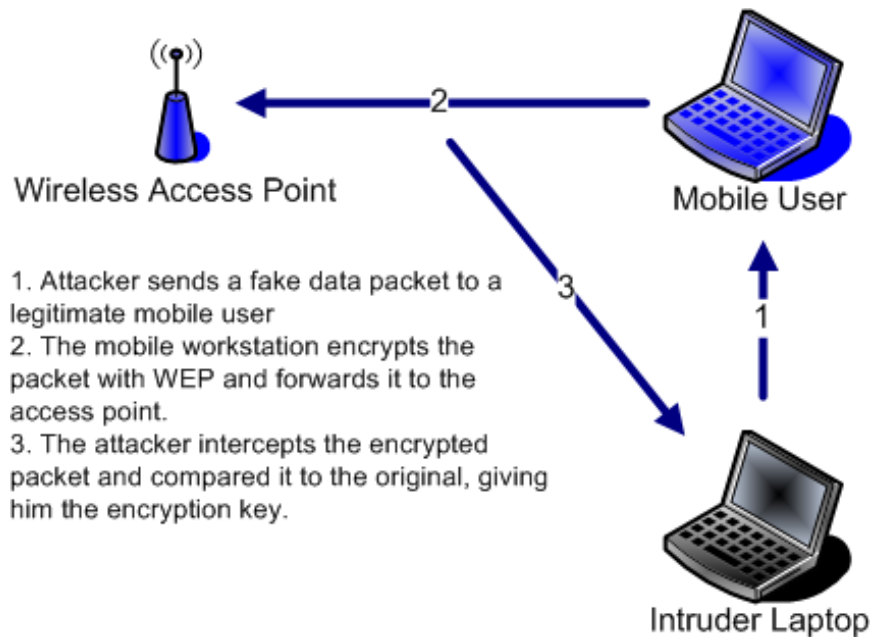
อย่างไรก็ตาม มาตรฐานความปลอดภัยแบบ WEP ถือว่ามีประสิทธิภาพต่ำ เนื่องจาก WEP ใช้หลักการในการเข้าและถอดรหัสข้อมูลที่เป็นแบบสมมาตร (symmetrical scheme) โดยกระบวนการเข้ารหัสและถอดรหัสใช้กุญแจลับ (shared key/secret key) ดอกเดียวกัน ซึ่งถือว่ามีความปลอดภัยต่ำ

ส่วนการพิสูจน์ตัวตนจริงตามมาตรฐาน IEEE 802.11 นั้น ได้กำหนดให้มีกลไกสำหรับการพิสูจน์ 2 ลักษณะ ได้แก่ การพิสูจน์ตัวตนจริงแบบระบบเปิด (Open System Authentication) และการพิสูจน์ตัวตนจริงแบบกุญแจร่วม (Shared Key Authentication)

การพิสูจน์ตัวตนจริงแบบระบบเปิด การตรวจสอบผู้ใช้ในลักษณะนี้เป็นทางเลือกแบบ default ที่กำหนดไว้ในมาตรฐาน IEEE 802.11 ในการตรวจสอบแบบนี้จะไม่ตรวจสอบรหัสลับจากผู้ใช้ กล่าวคือ ถือได้ว่าไม่มีการตรวจสอบนั่นเอง เป็นการอนุญาตให้ผู้ใช้ใดๆ ก็ยังสามารถเข้ามารับส่งสัญญาณในเครือข่ายได้

การพิสูจน์ตัวตนจริงแบบกุญแจร่วม จะอนุญาตให้สถานีผู้ใช้ซึ่งมีรหัสลับของเครือข่ายนี้เท่านั้นที่สามารถเข้ามารับส่งสัญญาณกับอุปกรณ์ที่ทำหน้าที่เป็นสถานีแม่ข่ายได้ โดยมีการใช้เทคนิคการถามตอบ (challenge-response) ที่ใช้กันทั่วไปผนวกกับการเข้ารหัสด้วย WEP เป็นกลไกสำหรับการตรวจสอบ การตรวจสอบแบบนี้จะทำได้ก็ต่อเมื่อมีการ Enable การเข้ารหัสด้วย WEP รูป 11.2 แสดงขั้นตอนการโจมตี WEP ของผู้บุกรุก

- 1) ผู้โจมตีจะส่งแพคเกจข้อมูลปลอมไปยังผู้ใช้อุปกรณ์แบบเคลื่อนที่ซึ่งใช้งานปกติ
- 2) เครื่องของผู้ใช้จะเข้ารหัสแพคเกจและส่งต่อไปยังจุดเชื่อมต่อ (access point)
- 3) ผู้โจมตีจะดักจับแพคเกจที่เข้ารหัสนั้น จากนั้น ทำการเปรียบเทียบกับต้นฉบับเพื่อแปลงกลับเป็นค่ากุญแจเข้ารหัส



รูป 11.2 ขั้นตอนการโจมตี WEP

(ที่มา: <http://windowsdevcenter.com/pub/a/windows/2007/06/26/windows-wireless-lan-security-primer.html>)

11.2.2 มาตรฐาน IEEE 802.11i-2004

IEEE 802.11i - 2004 หรือ 802.11i เป็นต้นฉบับในการแก้ไข IEEE 802.11 ร่างมาตรฐานได้ให้สัตยาบันที่ 24 มิถุนายน 2004 มาตรฐานนี้จะกำหนดกลไกการรักษาความปลอดภัยสำหรับเครือข่ายไร้สาย โดยใช้คำว่า ความปลอดภัย แทนการพิสูจน์ตัวตนจริง และความเป็นส่วนตัว (Privacy) ของข้อความในมาตรฐานเดิม ทำการ WEP พร้อมกับเริ่มเผยแพร่มาตรฐาน IEEE 802.11-2007

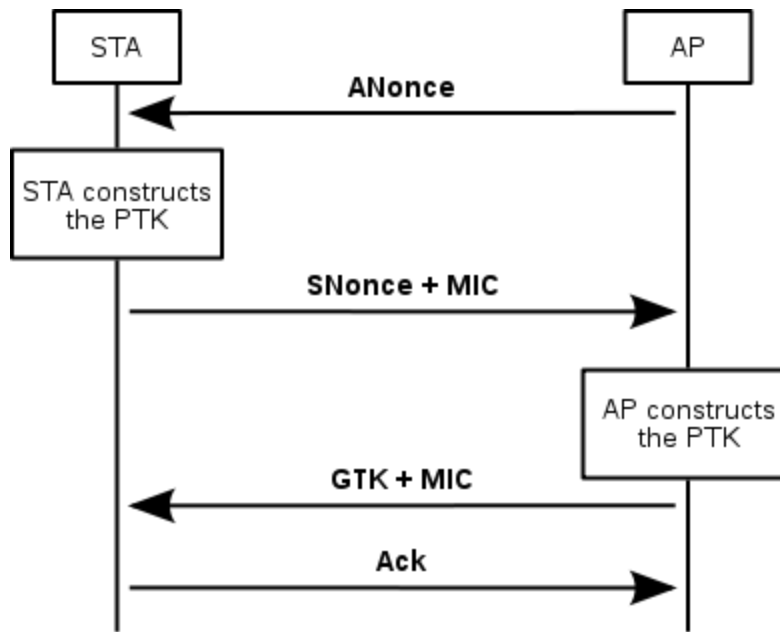
802.11i ถูกนำมาใช้แทนที่การรักษาความปลอดภัยข้อมูลแบบ WEP ซึ่งแสดงให้เห็นว่ามีจุดอ่อนด้านความปลอดภัยที่รุนแรง ในขณะที่ยังรอคอยการแก้ปัญหาจาก WEP กลุ่ม Wi-Fi Alliance ได้พัฒนากลไกความปลอดภัยที่รัดกุมกว่าเรียกว่า Wi-Fi Protected Access (WPA) มาใช้งานก่อนหน้านี้

IEEE 802.11i ได้มีการแก้ไข IEEE 802.11-1999 โดยใช้ Robust Security Network (RSN) ซึ่งขึ้นอยู่กับ IEEE 802.1X ด้วยวิธี 4-Way handshake ร่วมกับ Group Key Handshake เพื่อสร้างกรรมวิธีการเข้ารหัสลับที่แข็งแกร่ง

4-Way Handshake

กระบวนการพิสูจน์ตัวตนจริงจะมีการพิจารณา 2 ปัจจัย ได้แก่ จุดเชื่อมต่อ (AP) ยังคงต้องตรวจสอบตัวเองไปยังเครื่องลูกข่าย (STA) และกุญแจสำหรับเข้ารหัสทราฟฟิก การแลกเปลี่ยน EAP (Extensible Authentication Protocol) ในขั้นตอนก่อนหน้านี้จะสร้างกุญแจร่วม PMK (Pairwise Master Key) โดยที่กุญแจนี้ได้ถูกออกแบบมาเพื่อใช้ตลอดทุกเซสชัน 4-way handshake ใช้เพื่อสร้างกุญแจสำคัญอื่นๆ ที่เรียกว่า PTK (Pairwise Transient) โดยมีคุณสมบัติดังต่อไปนี้ PMK, AP nonce (ANonce), nonce STA (SNonce), AP MAC address, และ MAC address STA ผลลัพธ์ที่ได้จะถูกนำไปผ่านฟังก์ชันแฮชในการเข้ารหัสลับ

กระบวนการ handshake ยังให้ GTK (Group Temporal Key) ที่ใช้ในการถอดรหัสทราฟฟิกทั้งแบบมัลติแคสต์ (multicast) และบรอดแคสต์ (broadcast) ขั้นตอนการแลกเปลี่ยนข้อความในระหว่างกระบวนการจับมือแสดงในรูป 11.3



รูป 11.3 4-Way Handshake

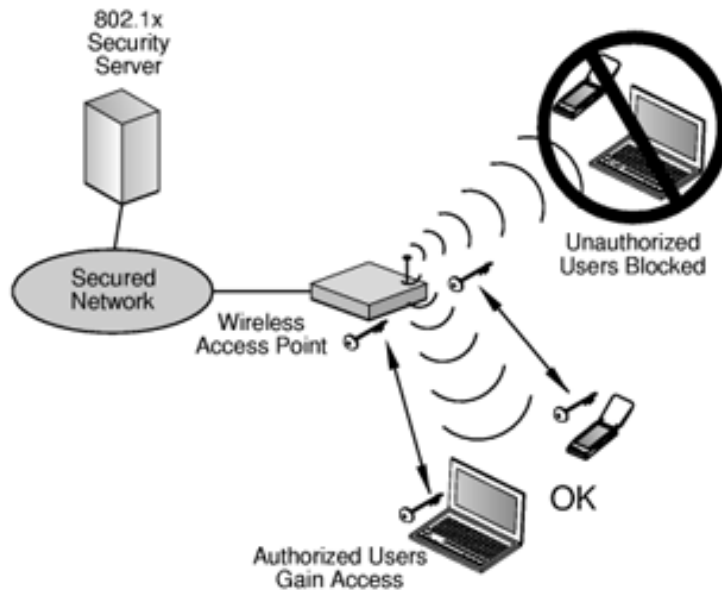
(ที่มา: http://en.wikipedia.org/wiki/IEEE_802.11i-2004)

- 1) AP ส่ง nonce-value ไปที่ STA (ANonce) เครื่องลูกข่ายทั้งหมดจะทำการสร้าง PTK ขึ้นมา
- 2) STA ส่ง nonce-value ของ (SNonce) ไปยัง AP พร้อมกับ MIC (Message Integrity Code) รวมถึงการตรวจสอบ Message Authentication and Integrity Authentication Code (MAIC)
- 3) AP จะส่ง GTK และหมายเลขลำดับพร้อมกับ MIC อื่น โดยหมายเลขลำดับนี้จะถูกใช้ในเฟรมมัลติแคสต์หรือบรอดแคสต์ถัดไป เพื่อให้ได้รับ STA ที่ใช้ตรวจสอบขั้นพื้นฐาน
- 4) STA จะส่งการยืนยันไปยัง AP

11.2.3 มาตรฐาน IEEE 802.1X

IEEE802.1X เป็นมาตรฐานของกระบวนการพิสูจน์ตัวตนจริง โดยกำหนดการห่อหุ้ม (encapsulation) ของ Extensible Authentication Protocol (EAP) บน IEEE 802 ซึ่งเป็นที่รู้จักกันเป็น "EAP over LANs" หรือ EAPOL เดิมถูกออกแบบไว้สำหรับ IEEE 802.3 Ethernet แต่ใน 802.1X - 2001 ได้ชี้แจงให้เหมาะสมกับเทคโนโลยีอื่น ๆ IEEE 802 LAN เช่น IEEE 802.11 และ Fiber Distributed Data Interface (ISO 9314-2) ใน 802.1X - 2004 protocol EAPOL แก้ไขปรับปรุงสำหรับใช้กับ IEEE 802.1AE (MACSec) และ 802.1AR IEEE (Identity Device Secure, DevID) ใน 802.1X - 2010

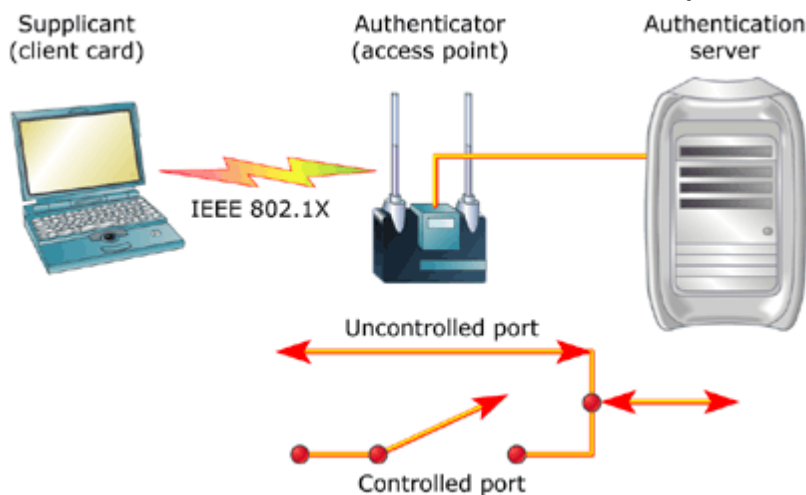
รูป 11.4 แสดงสถาปัตยกรรมของ 802.11i



รูป 11.4 แสดงสถาปัตยกรรมของ 802.11i

(ที่มา: <http://www.airtightnetworks.com/home/resources/knowledge-center/80211i.html>)

802.11X กำหนดกรอบการทำงานของพิสูจน์ตัวตนจริงและการตรวจสอบสิทธิ์ของอุปกรณ์ที่เชื่อมต่อเข้าสู่เครือข่าย โดยกำหนดองค์ประกอบของการแลกเปลี่ยนข้อมูลออกเป็น 3 ส่วน ได้แก่ ผู้ร้องขอ (supplicant), ผู้ตรวจสอบ (Authenticator) และแม่ข่ายตรวจสอบ (Authentication server) ดังรูป 11.5

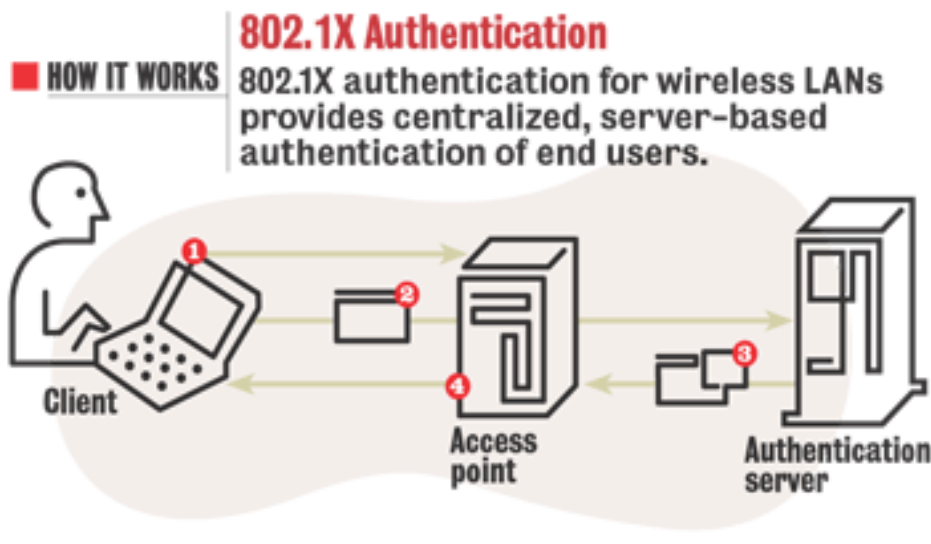


รูป 12.5 IEEE 802.11X ที่ใช้ในระบบ 802.11i

(ที่มา: http://www.embedded.com/columns/specialreports/34400002?_requestid=299821)

802.11X เป็นมาตรฐานระบบรักษาความปลอดภัย ที่จะตรวจสอบบุคคลที่จะเข้าใช้งาน รวมไปถึงการอนุญาตให้ใช้งาน โดยจะอิงตามพอร์ต คืออนุญาตเป็นรายพอร์ตไป ปัจจุบันมีใช้งานในในอุปกรณ์หลายตัวแล้ว เพราะเป็นส่วนหนึ่งของมาตรฐาน WPA โดยระบบ 802.1x นี้จะใช้โพรโทคอลคือ EAP (Extensible Authentication Protocol) จะสามารถรองรับเซิร์ฟเวอร์ที่ใช้ตรวจสอบบุคคลได้หลากหลาย เช่น Kerberos และ RADIUS เป็นต้น

การรับรองความถูกต้อง 802.1X สามารถช่วยสนับสนุนการรักษาความปลอดภัยสำหรับเครือข่าย 802.11 แบบไร้สาย และเครือข่าย อีเทอร์เน็ตแบบมีสาย 802.1X จะใช้เซิร์ฟเวอร์การรับรองความถูกต้องเพื่อตรวจสอบผู้ใช้ และกำหนดการเข้าใช้เครือข่าย 802.1X สามารถทำงานกับคีย์ Wired Equivalent Privacy (WEP) หรือ Wi-Fi Protected Access (WPA) บนเครือข่ายแบบไร้สายได้ โดยปกติการรับรองความถูกต้องประเภทนี้จะใช้เมื่อเชื่อมต่อกับเครือข่ายในที่ทำงาน รูป 11.6 IEEE 802.1X



รูป 11.6 ขั้นตอนการพิสูจน์ตัวตนจริงของผู้ใช้ผ่านเครื่องแม่ข่ายตามมาตรฐาน 802.11X
(ที่มา: <http://www.networkworld.com/details/7173.html>)

จากรูป

ขั้นตอนที่ 1 ลูกข่ายจะส่งข้อความ “เริ่ม (start)” ไปยังแอ็กเซสพอยน์เพื่อระบุตัวตนของลูกข่าย

ขั้นตอนที่ 2 ลูกข่ายจะส่งแพ็กเก็ตที่บรรจุด้วยการระบุตัวตนผ่านไปยังแอ็กเซสพอยน์ โดยแอ็กเซสพอยน์จะส่งต่อเพื่อพิสูจน์ตัวตนจริงที่เครื่องแม่ข่าย

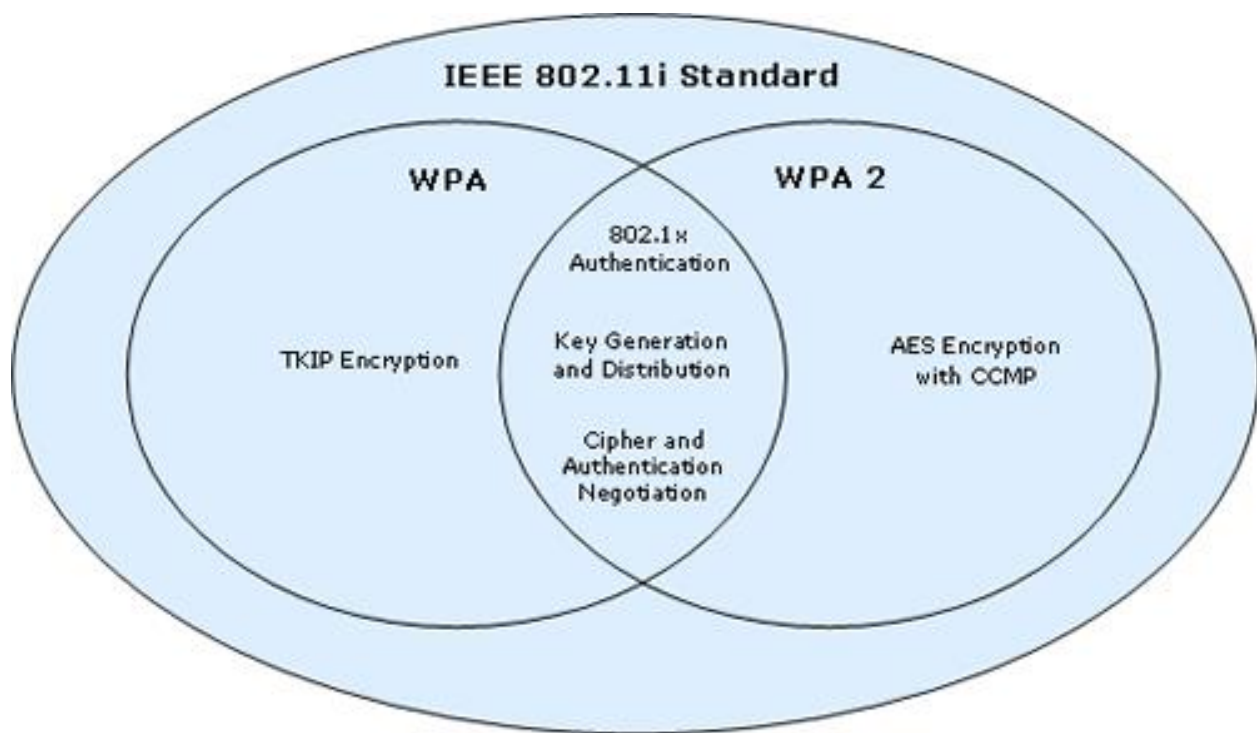
ขั้นตอนที่ 3 แม่ข่ายซึ่งทำหน้าที่พิสูจน์ตัวตนจริงจะส่งแพ็กเก็ต “ยอมรับ (accept)” กลับไปยังแอ็กเซสพอยน์

ขั้นตอนที่ 4 แอ็กเซสพอยน์ท์จะกำหนดพอร์ตของลูกค้าภายในกระบวนการพิสูจน์ตัวตน จากนั้น จึงจะอนุญาตให้มีการจราจรต่อไปได้

11.2.4 Wi-Fi Protected Access (WPA และ WPA2)

Wi-Fi Protected Access (WPA และ WPA2) เป็นโปรแกรมการรับรองที่พัฒนาโดย Wi-Fi Alliance เพื่อใช้งานร่วมกับผลิตภัณฑ์ที่ได้รับการรับรอง Wi-Fi Certified เพื่อรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไร้สายภายหลังที่มีการค้นพบช่องโหว่ร้ายแรงในระบบ WEP ก่อนหน้านี้

โพรโทคอล WPA ดำเนินตามกรอบส่วนใหญ่ของมาตรฐาน 802.11i IEEE โดย Wi-Fi Alliance ตั้งใจจะให้ WPA เป็นมาตรฐานกลางในระหว่างการรอ 802.11i แล้วเสร็จ โดยเฉพาะ Temporal Key Integrity Protocol (TKIP) ที่ถูกนำไปใส่ไว้ใน WPA cards interface ของเครือข่ายไร้สาย จึงกล่าวได้ว่า WPA และ WPA2 เป็น subset ของมาตรฐาน 802.11i ดังรูป 11.7



รูป 11.7 WPA/WPA2 ภายใต้มาตรฐาน 802.11i

(ที่มา: <http://palisade.plynt.com/issues/2007May/wpa-security/>)

Wi-Fi Protected Access (WPA และ WPA2) เป็นโพรโทคอลรับรองความปลอดภัยสำหรับแลนไร้สายที่พัฒนาโดย Wi-Fi Alliance เพื่อแทนที่ WEP ที่ถูกพบข้อบกพร่องร้ายแรงก่อนหน้านี้ โพรโทคอล WPA ยึดตามข้อกำหนดของมาตรฐาน IEEE 802.11i โดย Wi-Fi Alliance ตั้งใจให้ WPA เป็นมาตรการระดับกลางโดยใช้ระบบกุญแจแบบ Temporal Key Integrity Protocol (TKIP)

เป็นมาตรฐานแทนที่ WEP พัฒนบนพื้นฐาน IEEE 802.11i ใช้ Dynamic Key Distribution และ IEEE 802.11x ร่วมกันทำงาน การเข้ารหัสแบบ AES (Advanced Encryption Standard) ด้วย คีย์ ขนาด 128, 192 หรือ 256 บิต WPA จะเข้ารหัสข้อมูล และจะตรวจสอบเพื่อให้แน่ใจว่าไม่มีการปรับเปลี่ยน คีย์เพื่อความปลอดภัยของเครือข่าย นอกจากนั้น WPA ยังรับรองความถูกต้องผู้ใช้ เพื่อช่วยทำให้มั่นใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่จะสามารถเข้าถึงเครือข่ายได้ WPA มีการรับรองความถูกต้องสองประเภท คือ WPA และ WPA2 WPA

WPA2 สร้างขึ้นบนเพิ่มวิธีการเข้ารหัสชื่อ CCMP (Counter Mode with Cipher Block Chaining Message authentication Code Protocol) ได้รับการออกแบบให้ทำงานกับการเชื่อมต่อเครือข่ายแบบไร้สาย แต่อาจไม่สามารถทำงานกับจุดเข้าใช้งานหรือเราเตอร์รุ่นที่เก่ากว่า WPA2 จะมีความปลอดภัยมากกว่า WPA แต่จะไม่ทำงานกับการเชื่อมต่อเครือข่ายรุ่นเก่ากว่าบางรุ่น WPA ได้รับการออกแบบให้ใช้กับเซิร์ฟเวอร์การรับรองความถูกต้อง 802.1X ซึ่งจะให้คีย์ที่แตกต่างกันกับผู้ใช้แต่ละราย ซึ่งจะเรียกว่า WPA-Enterprise หรือ WPA2-Enterprise นอกจากนั้นยังสามารถใช้โหมดคีย์ก่อนการเข้าร่วมกัน (PSK) ที่ผู้ใช้ทุกคนจะได้รับวลีรหัสผ่านเดียวกัน ซึ่งจะเรียกว่า WPA-Personal หรือ WPA2-Personal

11.2.5 WPA3

Wi-Fi CERTIFIED นำเสนอโพรโทคอลความปลอดภัยที่ล้ำสมัย ครอบคลุมการเข้ารหัสและการตรวจสอบสิทธิ์อุปกรณ์ Wi-Fi CERTIFIED มาพร้อมกับระบบรักษาความปลอดภัยล่าสุด และพอร์ตโฟลิโอเทคโนโลยีที่พัฒนาอย่างต่อเนื่องเพื่อคงความแข็งแกร่ง ตอบสนองความต้องการการใช้งานที่ทันสมัย และสอดคล้องกับความก้าวหน้าทางเทคโนโลยี

WPA3™ นำเสนอโพรโทคอลความปลอดภัยที่ล้ำสมัย ช่วยลดความซับซ้อนของการรักษาความปลอดภัย Wi-Fi ④ช่วยให้การตรวจสอบยืนยันตัวตนมีความแข็งแกร่งมากขึ้น มอบความแข็งแกร่งของการเข้ารหัสที่เพิ่มขึ้นสำหรับตลาดข้อมูลที่มีความอ่อนไหวสูง และรักษาความยืดหยุ่นของเครือข่ายที่สำคัญต่อภารกิจ

WPA3 เป็นสิ่งจำเป็นสำหรับอุปกรณ์ Wi-Fi CERTIFIED และมีคุณสมบัติเพิ่มเติมสำหรับเครือข่ายส่วนบุคคลและเครือข่ายองค์กรโดยเฉพาะ ผู้ใช้ WPA3-Personal จะได้รับการปกป้องที่เพิ่มขึ้นจากการพยายามเดารหัสผ่าน ขณะที่ผู้ใช้ WPA3-Enterprise สามารถใช้ประโยชน์จากโพรโทคอลความปลอดภัยระดับสูงสำหรับเครือข่ายข้อมูลสำคัญได้แล้ว

เครือข่าย WPA3:

- ใช้โพรโทคอลความปลอดภัยล่าสุด
- ไม่อนุญาตให้ใช้โพรโทคอลเก่าที่ล้าสมัย
- ต้องใช้ Protected Management Frames (PMF)

มาตรฐาน WPA3 คือการเข้าถึงแบบป้องกัน Wi-Fi 3 เป็นมาตรฐานสำหรับเครือข่ายไร้สาย (Wi-Fi) รุ่นใหม่เพิ่มความปลอดภัยให้มากที่สุดยิ่งกว่า WPA2 จะต้องเป็นไปตามความต้องการส่วนบุคคล, ลักษณะตัวตน และการป้องกันประเภทต่างๆ หมายถึงต่างๆ แบบต่างๆ (การโจมตีพจนานุกรมออฟไลน์) และความเชื่อในเครือข่าย Wi-Fi สาธารณะ

คุณสมบัติ WPA3

WPA3 มีที่สำคัญมากใน WPA2:

WPA3-ส่วนบุคคล: SAE (Simultaneous Authentication of Equals): PSK (Pre-Shared Key) แบบเก่าๆ ในส่วนของคีย์ที่มีความปลอดภัยในกรณีที่สามารถป้องกันได้ที่แบบไหนบ้างได้

การส่งต่อความลับ: สืบค้นข้อมูลของผู้ที่จะเข้าถึงข้อมูลได้และข้อมูลต่างๆ ที่เคยทราบมาก่อนได้

WPA3-องค์กร: โดยปกติแล้วเครื่องมือนี้จะยกระดับความปลอดภัยสูงสุดสำหรับข้อมูลสำคัญมากในองค์กรและระบบปฏิบัติการ

การป้องกันในเครือข่ายสาธารณะ: WPA3 จะช่วยให้การดักฟังและปลอมแปลงข้อมูล (Spoofing) ในเครือข่าย Wi-Fi เปิดสาธารณะเช่นในคาเฟ่หรือสนามบิน

ทำไม WPA3 ถึงมีความสำคัญ?

ความปลอดภัยอีกครั้ง: WPA3 ให้การป้องกันที่เพิ่มขึ้นสำหรับเครือข่าย Wi-Fi ของคุณจากภัยคุกคามทางธรรมชาติ

ความปลอดภัยที่เพิ่มขึ้นใน IoT: ตรวจสอบอุปกรณ์ Internet of Things (IoT) ต่อไป

มาตรฐานเทคโนโลยีใหม่: WPA3 ถือว่ามาตรฐานในปัจจุบันอุปกรณ์ Wi-Fi รุ่นใหม่สำหรับ Wi-Fi 6E และ Wi-Fi 7 ใช้คลื่นความถี่ 6GHz.

WPA3 คือมาตรฐานความปลอดภัย Wi-Fi รุ่นใหม่ที่ยกระดับความปลอดภัยขึ้นมาใหม่วิธีการยืนยันตัวตน, การรักษา, และการป้องกันระบบต่างๆ แจ้งให้ทราบว่าไร้สายมี ความปลอดภัยและได้รับการยกย่องสำหรับผู้ใช้งานทั่วไปและองค์กร

11.2.6 เปรียบเทียบโพรโทคอลความปลอดภัยเครือข่ายไร้สาย 4 ประเภท

WEP, WPA, WPA2 และ WPA3 เป็น โพรโทคอลความปลอดภัยเครือข่ายไร้สาย 4 ประเภท โดยแต่ละประเภทมีระดับความปลอดภัยที่เพิ่มขึ้น

WPA2 ซึ่งใช้การเข้ารหัส AES เป็นที่นิยมใช้กันทั่วไป อย่างไรก็ตาม WPA3 มีคุณสมบัติด้านความปลอดภัยเพิ่มเติม เช่น การเข้ารหัสที่แข็งแกร่งขึ้นและการป้องกันการโจมตีที่ซับซ้อน โพรโทคอลเหล่านี้กำหนดระดับการเข้าถึงของผู้ใช้และอุปกรณ์ ไม่ว่าจะใช้โพรโทคอลใด คุณจำเป็นต้องมีความปลอดภัยที่แข็งแกร่งเพื่อปกป้องเครือข่ายไร้สายและข้อมูลสำคัญ รูป 11.8 เปรียบเทียบโพรโทคอลความปลอดภัยทั้ง 4 ประเภท ซึ่งมีรายละเอียดดังนี้

WEP vs WPA vs WPA2 vs WPA3				
	WEP	WPA	WPA2	WPA3
Release Year	1997	2003	2004	2018
Encryption	RC4	TKIP / RC4	AES-CCMP	AES-CCMP / AES-GCMP
Session Key	64/128 bit	128 bit	128 bit	128/256 bit
Authentication	Open system, shared key	Pre-shared key	Pre-shared key	AES-CCMP / AES-GCMP
Level of Security	Very low	Low	Moderate	High
Weakness	Insecure encryption easily exploited by hackers	Weak encryption, compatibility issues	Vulnerable to key reinstallation attack (KRACK)	Complex deployment

รูป 11.8 เปรียบเทียบโพรโทคอลความปลอดภัยทั้ง 4 ประเภท
(ที่มา: esecurityplanet.com)

ความเป็นส่วนตัวเทียบเท่าแบบมีสาย (WEP)

WEP พัฒนาขึ้นในปี พ.ศ. 2540 ออกแบบมาเพื่อรักษาความปลอดภัยเครือข่ายไร้สายโดยใช้การเข้ารหัสและการจำกัดการเข้าถึง อย่างไรก็ตาม การพึ่งพาการเข้ารหัส RC4 ที่ไม่ปลอดภัยและการรับรองความถูกต้องด้วยคีย์ที่ใช้ร่วมกันทำให้เครือข่ายมีความเสี่ยงต่อการถูกโจมตี แม้ว่าในตอนแรก WEP จะมีการเข้ารหัสคล้ายกับเครือข่ายแบบมีสาย แต่ข้อบกพร่องของ WEP ถูกแฮ็กเกอร์นำไปใช้ประโยชน์อย่างกว้างขวาง ทำให้ WEP ล้าสมัยไปแล้ว

การยุติการใช้โพรโทคอลนี้ทำให้เกิดทางเลือกที่แข็งแกร่งยิ่งขึ้น เช่น WPA (Wi-Fi Protected Access) แม้จะมีข้อบกพร่อง แต่ความเรียบง่ายและการนำไปใช้อย่างแพร่หลายของ WEP ในตอนแรกก็ดึงดูดความสนใจ แต่ใน

ที่สุดช่องโหว่ที่มีอยู่กับดั่งประโยชน์ โดยเน้นย้ำถึงความสำคัญของการปรับปรุงมาตรฐานความปลอดภัยไร้สายอย่างต่อเนื่อง

การเข้าถึง Wi-Fi ที่ได้รับการป้องกัน (WPA)

WPA เปิดตัวในปี พ.ศ. 2546 และกลายเป็นมาตรฐานที่สืบทอดมาจาก WEP ได้อย่างมีประสิทธิภาพ โดยสามารถแก้ไขข้อบกพร่องต่างๆ ได้ WPA ใช้การเข้ารหัสแบบ Temporal Key Integrity Protocol (TKIP) เพื่อปรับปรุงการจัดการคีย์และการตรวจสอบความถูกต้อง WPA มีสองโหมด ได้แก่ WPA-Personal สำหรับเครือข่ายภายในบ้าน และ WPA-Enterprise สำหรับองค์กรที่ใช้เซิร์ฟเวอร์ RADIUS

การเข้ารหัส 128 บิตของ WPA ให้การป้องกันที่เหนือกว่ามาตรฐานการเข้ารหัสที่อ่อนแอกว่าของ WEP อย่างไรก็ตาม การเข้ารหัสนี้ยังคงอ่อนแอกว่า WPA2 อยู่มาก ส่งผลให้เกิดข้อบกพร่องและปัญหาความเข้ากันได้ที่อาจเกิดขึ้น การนำ WPA มาใช้อาจจำเป็นต้องปรับเปลี่ยนฮาร์ดแวร์ ซึ่งเป็นปัญหาสำหรับผู้ที่ใช้อุปกรณ์รุ่นเก่า

การเข้าถึง Wi-Fi ที่ได้รับการป้องกัน II (WPA2)

WPA2 เปิดตัวในปี พ.ศ. 2547 เป็นอีกหนึ่งมาตรฐานความปลอดภัยไร้สายที่ใช้ประโยชน์จากเทคนิคการเข้ารหัส AES เพื่อมอบความปลอดภัยที่แข็งแกร่ง ข้อได้เปรียบเหนือ WPA ได้แก่ การบริหารจัดการที่ดีกว่าและความเสี่ยงต่อการถูกโจมตีที่ต่ำลง WPA2 ได้รับการยอมรับอย่างกว้างขวางในฐานะมาตรฐานอุตสาหกรรม ช่วยให้มั่นใจได้ถึงความสามารถในการทำงานร่วมกันของอุปกรณ์

อย่างไรก็ตาม ช่องโหว่ต่างๆ เช่น การโจมตีการติดตั้งคีย์ซ้ำ (KRACK) ถือเป็นความเสี่ยงด้านความปลอดภัย แม้ว่าจะเหมาะสมกับเครือข่ายภายในบ้านส่วนใหญ่ แต่ปัญหาอาจเกิดขึ้นในองค์กรที่มีการโจมตีที่ซับซ้อนแพร่หลายมากกว่า นอกจากนี้ อุปกรณ์รุ่นเก่าที่ไม่รองรับ WPA2 อาจจำเป็นต้องอัปเดต

แม้จะมีปัญหาดังกล่าว WPA2 ก็ยังคงใช้งานอยู่ แต่ก็มีควมพยายามอย่างต่อเนื่องที่จะแก้ไขภัยคุกคามและจุดอ่อนที่เพิ่มมากขึ้น

การเข้าถึง Wi-Fi ที่ได้รับการป้องกัน III (WPA3)

WPA3 เปิดตัวในปี 2018 นำเสนอการเข้ารหัสที่ได้รับการปรับปรุง การป้องกันการโจมตีแบบบรูทฟอร์ซด้วยพหุนามที่ดีขึ้น และการกำหนดค่าอุปกรณ์ที่ง่ายขึ้นผ่าน Wi-Fi Easy Connect แม้จะมีการปรับปรุงเหล่านี้ แต่การยอมรับอย่างกว้างขวางยังคงล่าช้า WPA3 มีสามประเภท ได้แก่ WPA3-Personal สำหรับใช้งานที่บ้าน WPA3-Enterprise สำหรับการตั้งค่าองค์กร และ Wi-Fi Enhanced Open สำหรับเครือข่ายที่ไม่ต้องใช้รหัสผ่าน

แม้ว่า WPA3 จะช่วยเพิ่มความปลอดภัยโดยรวมของเครือข่าย แต่ก็มีข้อเสียคือความซับซ้อนในการใช้งาน ผู้ใช้ใช้งานน้อย และปัญหาความเข้ากันได้กับอุปกรณ์รุ่นเก่า แม้จะมีข้อดี แต่การใช้งาน WPA3 อย่างเต็มรูปแบบยังไม่เกิดขึ้น ซึ่งเป็นสัญญาณบ่งบอกถึงการเปลี่ยนแปลงอย่างช้าๆ จากโพรโทคอลความปลอดภัยแบบเก่าไปสู่มาตรฐานที่ทันสมัยกว่านี้

11.3 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi

การปกป้องเครือข่าย Wi-Fi จากการเข้าถึงโดยไม่ได้รับอนุญาตโดยใช้วิธีการเข้ารหัส เครื่องมือไฟร์วอลล์ ซอฟต์แวร์ SSID ที่ปลอดภัย ซอฟต์แวร์ VPN และซอฟต์แวร์รักษาความปลอดภัยเครือข่ายไร้สาย

11.3.1 แนวทางรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi

แนวทางเหล่านี้ช่วยลดโอกาสที่ช่องโหว่ความปลอดภัยจะประสบความสำเร็จ 5 วิธี ช่วยเพิ่มความปลอดภัยและความสมบูรณ์ของเครือข่ายและข้อมูลสำคัญขององค์กร รูป 11.9 มีรายละเอียดดังนี้



รูป 11.9 มาตรการรักษาความมั่นคงปลอดภัยเครือข่าย Wi-Fi
(ที่มา: esecurityplanet.com)

1) ใช้การเข้ารหัส

การเข้ารหัสจะเข้ารหัสข้อมูลเครือข่าย ทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลสำคัญได้ยากขึ้น การเข้ารหัสเครือข่าย Wi-Fi โดยใช้มาตรฐาน WPA2 หรือ WPA3 เพื่อปกป้องข้อมูล อัปเดตโปรโตคอลการเข้ารหัสเป็นเวอร์ชันล่าสุดเพื่อความปลอดภัยสูงสุดของเครือข่ายและป้องกันภัยคุกคามและการรั่วไหลของข้อมูลที่อาจเกิดขึ้น

2) เปิดใช้งานไฟร์วอลล์เราเตอร์

เปิดใช้งานไฟร์วอลล์ของเราเตอร์เพื่อเพิ่มการป้องกันไวรัส มัลแวร์ และแฮกเกอร์ ตรวจสอบสถานะในการตั้งค่าเราเตอร์เพื่อเพิ่มประสิทธิภาพการป้องกันเครือข่าย แบ่งส่วนที่ละเอียดอ่อนในเครือข่ายเพื่อเพิ่มความปลอดภัย และพิจารณาติดตั้งไฟร์วอลล์บนอุปกรณ์ที่เชื่อมต่อทั้งหมดเพื่อการปกป้องที่สมบูรณ์

3) ปกป้อง Service Set Identifier (SSID)

เพื่อรักษาความปลอดภัยเครือข่ายไร้สาย ควรเก็บข้อมูลส่วนบุคคล เช่น นามสกุล ไว้ไม่ให้ปรากฏใน SSID ใช้ข้อมูลที่ผิดปกติเพื่อให้แฮกเกอร์โจมตีเครือข่ายของเราได้ยากขึ้น โดยใช้เทคนิคต่างๆ เช่น การโจมตีแบบ Evil Twin การปกปิด SSID ของเรายังช่วยลดความเสี่ยงจากการตกเป็นเหยื่อของจุดเชื่อมต่อที่เป็นอันตรายและการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งจะช่วยยกระดับความปลอดภัยโดยรวมของเครือข่ายไร้สาย

4) ใช้ประโยชน์จากเครือข่ายส่วนตัวเสมือน (VPN)

VPN ปกป้องเครือข่าย Wi-Fi ด้วยการเข้ารหัสข้อมูล ทำให้ผู้ที่อาจแอบฟังบนเครือข่าย Wi-Fi สาธารณะไม่สามารถอ่านข้อมูลได้ ควรเลือกใช้ VPN ที่ใช้การเข้ารหัส AES-256 มาตรฐานอุตสาหกรรม และเพิ่มความปลอดภัยเป็น 2 เท่าด้วยการใช้โปรโตคอลโอเพนซอร์สที่เชื่อถือได้เพื่อการปกป้องที่มากขึ้น แอป VPN หลายตัวมีฟีเจอร์ที่เป็นส่วนตัวเพิ่มเติม เช่น การบล็อกโฆษณา การแยกอุโมงค์ และความสามารถ VPN สองเท่า ซึ่งช่วยเพิ่มความปลอดภัยและความเป็นส่วนตัวของเครือข่ายโดยรวม

5) ติดตั้งซอฟต์แวร์รักษาความปลอดภัยแบบไร้สาย

ซอฟต์แวร์รักษาความปลอดภัยไร้สายช่วยยกระดับความปลอดภัยเครือข่าย Wi-Fi ด้วยการผสมผสานความสามารถต่างๆ เช่น การวิเคราะห์ประสิทธิภาพ การสแกนเครือข่าย การสำรวจพื้นที่ การวิเคราะห์สเปกตรัม การทำแผนที่ความร้อน การตรวจสอบ การวิเคราะห์ปริมาณการรับส่งข้อมูล การดักจับแพ็กเก็ตการทดสอบการเจาะระบบการตรวจสอบ และการจัดการ ฟีเจอร์เหล่านี้ช่วยให้ผู้ใช้สามารถระบุช่องโหว่ ตรวจสอบการเข้าถึงที่ไม่พึงประสงค์ และใช้มาตรการรักษาความปลอดภัยที่มีประสิทธิภาพเพื่อปกป้องเครือข่าย Wi-Fi ของตนจากภัยคุกคามและการละเมิดที่อาจเกิดขึ้น

11.3.2 ความปลอดภัยแบบไร้สายในสภาพแวดล้อมเฉพาะ

ความปลอดภัยแบบไร้สายจะแตกต่างกันไปตามการตั้งค่าต่างๆ เช่น เครือข่าย Wi-Fi ที่บ้าน เครือข่ายไร้สายในธุรกิจ และเครือข่ายสาธารณะ เพื่อป้องกันภัยคุกคาม แต่ละสถานที่จึงจำเป็นต้องมีมาตรการป้องกันที่เหมาะสม

1) การรักษาความปลอดภัย Wi-Fi ที่บ้าน

การรักษาความปลอดภัยเครือข่าย Wi-Fi ที่บ้านไม่เพียงแต่ช่วยปกป้องข้อมูลส่วนบุคคลของเราเท่านั้น แต่ยังรับประกันการเชื่อมต่อเครือข่ายที่เสถียรและเชื่อถือได้อีกด้วย นี่คือการเคล็ดลับบางประการในการเสริมความแข็งแกร่งให้กับเครือข่าย Wi-Fi ที่บ้านของเราและลดความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้น

- **รหัสผ่านที่ปลอดภัย:** สร้างรหัสผ่าน Wi-Fi ที่แข็งแกร่งและอัปเดตเป็นประจำเพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต
- **ตรวจสอบอุปกรณ์:** ตรวจสอบอุปกรณ์ที่เชื่อมโยงเป็นประจำเพื่อดูว่ามีกิจกรรมที่ผิดปกติหรือการเข้าถึงที่ไม่ได้รับอนุญาตหรือไม่
- **ตรวจสอบข้อมูลประจำตัวของเราเตอร์:** เข้าถึงอินเทอร์เฟซเว็บของเราเตอร์ เลือกการตั้งค่าการดูแลระบบ และเปลี่ยนการเข้าสู่ระบบและรหัสผ่านเริ่มต้น
- **อัปเดตอุปกรณ์:** อัปเดตเฟิร์มแวร์ของเราเตอร์และอุปกรณ์ที่เกี่ยวข้องให้เป็นปัจจุบันเพื่อป้องกันช่องโหว่และเพื่อให้มั่นใจถึงความปลอดภัยที่เหมาะสมที่สุด
- **วางเราเตอร์ในตำแหน่งที่ดีที่สุด:** วางเราเตอร์ในตำแหน่งที่เหมาะสมเพื่อให้ครอบคลุมพื้นที่สูงสุดและมีการรบกวนสัญญาณน้อยที่สุด

2) การรักษาความปลอดภัยเครือข่ายไร้สายทางธุรกิจ

การใช้นโยบายการรักษาความปลอดภัยเครือข่ายไร้สายที่มีประสิทธิภาพจะช่วยป้องกันการโจมตีทางไซเบอร์ควบคู่ไปกับการปฏิบัติตามกฎระเบียบและความไว้วางใจของลูกค้า ต่อไปนี้คือแนวทางสำคัญบางประการในการเสริมสร้างเครือข่ายธุรกิจและลดภัยคุกคามด้านความปลอดภัยที่อาจเกิดขึ้น:

- **จำกัด การแชร์รหัสผ่าน:** แชร์รหัสผ่านเฉพาะกับบุคลากรที่เกี่ยวข้องเท่านั้น และเปลี่ยนรหัสผ่านเป็นประจำเพื่อความปลอดภัย
- **อัปเดตโปรโตคอลการเข้ารหัส:** เพื่อปรับปรุงความปลอดภัยของเครือข่าย ให้แทนที่การเข้ารหัส WEP ที่ล้าสมัยด้วยโปรโตคอลที่ทันสมัยกว่า เช่น WPA2/WPA3
- **แบ่งส่วนเครือข่ายธุรกิจและผู้มาเยือน:** เพื่อปกป้องข้อมูลที่ละเอียดอ่อนของธุรกิจของเรา ให้กำหนดเส้นทางกิจกรรมของแขกและกิจกรรมที่ไม่ใช่ธุรกิจไปยังเครือข่ายที่แยกจากกัน
- **ติดตั้งไฟร์วอลล์:** ใช้ประโยชน์จากไฟร์วอลล์เพื่อตรวจจับและป้องกันโปรแกรมที่อาจเป็นอันตราย
- **จำกัดการเชื่อมต่อ DHCP:** ตรวจสอบและลบอุปกรณ์ที่ผิดกฎหมายเป็นประจำ และพิจารณาทำงานร่วมกับผู้จำหน่ายระบบรักษาความปลอดภัยเครือข่ายเพื่อรับโซลูชันความปลอดภัยเครือข่ายที่ครอบคลุม

3) การรักษาความปลอดภัยเครือข่ายสาธารณะ

ด้วยจำนวนจุดเชื่อมต่อ Wi-Fi สาธารณะที่เพิ่มขึ้นในร้านกาแฟ สนามบิน และสถานที่สาธารณะอื่นๆ ผู้ใช้จึงจำเป็นต้องดำเนินการเชิงรุกเพื่อปกป้องความเป็นส่วนตัวและความปลอดภัยทางดิจิทัลของตนเอง นี่คือการเคลียร์พื้นฐาน 5 ข้อสำหรับการท่องเว็บอย่างปลอดภัยบนเครือข่ายสาธารณะ

- **ใช้ซอฟต์แวร์ป้องกันไวรัส:** ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัสเพื่อตรวจจับและแจ้งเตือนเกี่ยวกับความเสี่ยงของมัลแวร์บนเครือข่าย Wi-Fi สาธารณะ
- **หลีกเลี่ยงการเข้าถึงข้อมูลที่ละเอียดอ่อน:** อย่าเข้าถึงข้อมูลที่เป็นความลับหรือแอปใดๆ บนเครือข่ายสาธารณะที่ไม่ได้รับการป้องกัน แม้ว่าเราจะใช้ VPN ก็ตาม
- **ใช้ประโยชน์จาก VPN:** เปิด VPN ของเราเพื่อเข้ารหัสการส่งข้อมูลผ่าน Wi-Fi สาธารณะ รักษาความเป็นส่วนตัวและความปลอดภัยโดยสร้างอุโมงค์ที่ปลอดภัยสำหรับการถ่ายโอนข้อมูล
- **ระวัง อีเมล ฟิชชิง:** ใช้ความระมัดระวังขณะตรวจสอบเนื้อหาอีเมล ตรวจสอบลิงก์ที่น่าสงสัย และยืนยันตัวตนผู้ส่ง
- **ปิดใช้งานการแชร์ไฟล์หรือการเชื่อมต่ออัตโนมัติ:** ปิดการตั้งค่าการเชื่อมต่ออัตโนมัติและฟังก์ชันการแชร์ไฟล์บนอุปกรณ์เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาตบนเครือข่าย Wi-Fi สาธารณะ

11.3.3 กลไกการตรวจสอบสิทธิ์ 4 ประการสำหรับการรักษาความปลอดภัยเครือข่ายไร้สาย

กลไกการตรวจสอบความถูกต้องช่วยเสริมความปลอดภัยด้วยการกำหนดให้ผู้ใช้ต้องตรวจสอบยืนยันตัวตนผ่านวิธีการต่างๆ เช่น การตรวจสอบความถูกต้องหลายปัจจัย (MFA) การลงชื่อเข้าใช้ครั้งเดียว (SSO) การตรวจสอบความถูกต้องโดยใช้รหัสผ่าน และการตรวจสอบความถูกต้องโดยไม่ต้องใช้รหัสผ่าน

1) การตรวจสอบสิทธิ์แบบหลายปัจจัย (MFA)

MFA เป็นมาตรการรักษาความปลอดภัยที่ต้องใช้หลักฐานยืนยันตัวตนอย่างน้อยสองชุด เช่น รหัสผ่านร่วมกับโทเค็นทางกายภาพหรือข้อมูลไบโอเมตริกซ์ MFA ช่วยเพิ่มความปลอดภัยด้วยการเพิ่มขั้นตอนการยืนยันตัวตนนอกเหนือจากการใช้รหัสผ่าน ลดความเสี่ยงในการเข้าถึงโดยไม่ได้รับอนุญาต และป้องกันภัยคุกคามทางไซเบอร์ เช่น ฟิชชิงและการโจรกรรมข้อมูลประจำตัว ทางเลือกอื่นของ MFA ได้แก่ แอปพลิเคชันตรวจสอบสิทธิ์อีเมล และ SMS

2) การลงชื่อเข้าใช้ครั้งเดียว (SSO)

SSO ช่วยให้ผู้ใช้สามารถเข้าสู่ระบบแอปพลิเคชันหนึ่งได้ทันที และเข้าถึงแอปพลิเคชันอื่นๆ ได้ในหลายแพลตฟอร์มและโดเมน ช่วยลดความจำเป็นในการเข้าสู่ระบบหลายครั้ง ช่วยยกระดับประสบการณ์และประสิทธิภาพการใช้งาน โดเมนกลางจะจัดการการตรวจสอบสิทธิ์และแชร์เซสชันกับโดเมนอื่นๆ แต่โปรโตคอลเฉพาะอาจแตกต่างกันไปในการจัดการการแชร์เซสชัน

3) การตรวจสอบสิทธิ์โดยใช้รหัสผ่าน

การยืนยันตัวตนด้วยรหัสผ่านจะยืนยันตัวตนของผู้ใช้โดยการขอให้ผู้ใช้ระบุทั้งชื่อผู้ใช้และรหัสผ่าน ข้อมูลประจำตัวเหล่านี้จะถูกเปรียบเทียบกับข้อมูลที่เก็บไว้ในฐานข้อมูลของระบบ และหากตรงกัน ระบบจะอนุญาตให้เข้าถึงข้อมูลได้ แม้ว่าการยืนยันตัวตนจะเป็นเรื่องง่ายสำหรับผู้ใช้ แต่ก็จำเป็นต้องมีขั้นตอนทางเทคนิคเพิ่มเติมเพื่อรักษาความปลอดภัยและการควบคุมการเข้าถึง

4) การตรวจสอบสิทธิ์แบบไม่ต้องใช้รหัสผ่าน

การยืนยันตัวตนแบบไร้รหัสผ่านได้เข้ามาแทนที่การป้อนรหัสผ่านแบบเดิมด้วยวิธีการใหม่ที่ปลอดภัยกว่า ยกตัวอย่างเช่น ไบโอมेटริกซ์จะตรวจสอบคุณสมบัติเฉพาะตัว เช่น ลักษณะใบหน้า ในขณะที่บางระบบใช้ปัจจัยการครอบครอง เช่น รหัสผ่านแบบใช้ครั้งเดียว การยืนยันตัวตนแบบไร้รหัสผ่านช่วยเพิ่มความปลอดภัยโดยไม่จำเป็นต้องใช้รหัสผ่านอีกต่อไป แต่กลับพึ่งพาไบโอมेटริกซ์ ปัจจัยการครอบครอง และลิงก์พิเศษที่ส่งมาทางอีเมลแทน

11.4 ภัยคุกคามเครือข่ายไร้สายและผลกระทบต่อองค์กร

จากที่กล่าวมาข้างต้นเกี่ยวกับการเติบโตอย่างรวดเร็วของการใช้งานเครือข่ายไร้สายที่มาเป็นส่วนสำคัญหนึ่งในการดำเนินธุรกิจ รวมถึงชีวิตประจำวันของทุกคน ทำให้มีความจำเป็นต้องมีความก้าวหน้าของเทคโนโลยีด้านความปลอดภัยในการใช้งานเพื่อรองรับการเติบโตนี้ อีกทั้ง ภัยคุกคามที่เกิดขึ้นทางเครือข่ายไร้สายก็สามารถเกิดขึ้นได้ง่าย เนื่องจาก whacker (Wireless Hacker) ไม่มีความจำเป็นต้องเข้าถึงพื้นที่ทางกายภาพ เพื่อเชื่อมต่อเครือข่ายขององค์กรก็สามารถที่จะเข้าถึงเครือข่ายขององค์กรได้ โดยใช้เพียงแค่เครื่องมือ (tool) ทั่วไปที่หาได้จากอินเทอร์เน็ต และยังยากต่อการที่จะถูกตรวจจับ เทคนิคอย่าง Warchalking, Wardriving และ War flying ถูกนำมาใช้ในการค้นหาเครือข่ายไร้สาย และจุดอ่อนของเครือข่ายไร้สาย นอกจากนั้น เครือข่ายไร้สายสาธารณะอย่างในร้านกาแฟ โรงแรม หรือสนามบิน ก็เป็นเป้าหมายสำคัญอีกจุดหนึ่ง เพราะนักธุรกิจ พนักงานขององค์กร ก็ใช้เครือข่ายเหล่านี้ในการรับส่งข้อมูลสำคัญขององค์กร

11.4.1 ภัยคุกคามเครือข่ายไร้สาย Wi-Fi Chalking

วิธีการที่ถูกใช้ในการค้นหาเครือข่ายไร้สายแบบเปิด (Open wireless network) มีหลายเทคนิค ดังนี้

- WarWalking เป็นเทคนิคการค้นหาเครือข่ายไร้สาย โดยการใช้ laptop หรือ อุปกรณ์พกพาที่มีการเปิดหาสัญญาณ Wi-Fi และเดินหาสัญญาณตามจุดต่างๆ และอาจมีการทำ WarChalking เพื่อทำสัญลักษณ์ตามจุดที่พบว่ามีเครือข่ายไร้สายที่สามารถเพื่อใช้เชื่อมต่ออินเทอร์เน็ตได้ฟรี ข้อเสียของวิธีการนี้คือการเคลื่อนที่ไปตามจุดนั้นทำได้ช้า

- WarFlying เป็นเทคนิคการค้นหาเครือข่ายไร้สาย โดยใช้ laptop หรือ อุปกรณ์พกพาที่มีการเปิดหาสัญญาณ Wi-Fi และบินเหนือพื้นที่เพื่อค้นหาเครือข่ายไร้สายแบบเปิด (Open wireless network) โดยอาจเรียกอีกชื่อหนึ่งว่า WarStroming
- WarDriving เป็นเทคนิคการค้นหาเครือข่ายไร้สายเช่นเดียวกับ Warwalking และ WarFlying แต่จะทำการขับรถไปรอบพื้นที่ของเป้าหมาย เพื่อระบุจุดที่มีสัญญาณ Wi-Fi
- WarChalking เป็นชื่อนิยามที่มาจาก Whacker ที่ใช้ชอล์กในการเขียนตามผนัง เสา หรือ พื้นในพื้นที่สาธารณะ เพื่อระบุจุดที่มีเครือข่ายไร้สายแบบเปิด (Open wireless network) ที่สามารถใช้เชื่อมต่ออินเทอร์เน็ตได้ฟรี

11.4.2 ภัยคุกคามเครือข่ายไร้สาย Access control attacks

เป็นการโจมตีที่ต้องการที่จะเจาะเข้าระบบเครือข่ายภายใน โดยการหลบหลีกมาตรการการควบคุมการเข้าถึงเครือข่ายไร้สายอย่างเช่น MAC Filtering หรือ Wi-Fi port access control ซึ่งภัยคุกคามในลักษณะนี้เกิดขึ้นโดยวิธีการที่หลากหลายจากผู้บุกรุกขึ้นอยู่กับมาตรการควบคุมที่องค์กรใช้ เช่น

- MAC Spoofing: เป็นวิธีการปลอมแปลง MAC Address คอมพิวเตอร์หรืออุปกรณ์ของผู้บุกรุกให้ตรงกับ MAC Address ของผู้ใช้งาน เพื่อหลบหลีกมาตรการป้องกันอย่าง MAC Filtering โดยมี Software มากมายที่สามารถใช้เพื่อเปลี่ยนค่า MAC Address ได้ เช่น SMAC หรือ WiControl
- Rogue Access Point: ใช้ในการสร้าง Backdoor เพื่อเป็นทางผ่านเข้าเครือข่ายภายในของเป้าหมาย โดยการนำ AP มาเชื่อมต่อกับเครือข่ายภายใน และปล่อยสัญญาณให้ผู้บุกรุกสามารถเชื่อมต่อเข้ามายังเครือข่ายได้
- AP Misconfiguration: เป็นการภัยคุกคามที่เกิดขึ้นจากการตั้งค่าของ AP อย่างไม่ปลอดภัย เช่น ใช้ค่าตั้งต้นจากผลิตภัณฑ์ ส่งผลให้มีช่องโหว่ที่ผู้บุกรุกสามารถใช้เจาะระบบเครือข่ายไร้สายได้
- Unauthorized association: เป็นภัยคุกคามหลักที่เกิดขึ้นกับเครือข่ายไร้สาย โดยผู้บุกรุกจะใช้วิธีการหลากหลายรูปแบบ เพื่อเชื่อมต่อกับเครือข่ายไร้สายของเป้าหมายให้ได้ซึ่งวิธีการป้องกันจะขึ้นอยู่กับวิธีการที่ผู้บุกรุกใช้

11.4.3 ภัยคุกคามเครือข่ายไร้สาย Integrity attacks

เป็นรูปแบบภัยคุกคามจากการโจมตีที่ผู้บุกรุกจะส่งข้อมูลปลอม เช่น Forged control, Management, Data frame ผ่านทางเครือข่ายไร้สายมาที่ AP เพื่อให้ AP ใช้ข้อมูลปลอมเหล่านี้ในการกระทำการโจมตีในรูปแบบอื่น เช่น DoS (Denial of service) และเทคนิคการโจมตีที่ใช้หลักการของ Integrity attacks มาร่วมโจมตีก็มีหลากหลาย เช่น WEP Injection, Data Replay และ Initialization vector replay attack เป็นต้น

11.4.4 ภัยคุกคามเครือข่ายไร้สาย Confidentiality attacks

เป็นรูปแบบภัยคุกคามจากการโจมตีที่บุกรุกดักจับข้อมูลที่รับส่งผ่านเครือข่ายไร้สาย ไม่ว่าข้อมูลเหล่านั้นจะอยู่ในรูปแบบที่ไม่เข้ารหัส (Clear text) หรือเข้ารหัส (Encrypted) โดยเทคนิคการโจมตีในรูปแบบนี้มีหลายวิธีการ เช่น

- Eavesdropping: เป็นการดักจับข้อมูลสำคัญที่ส่งผ่านทางเครือข่ายไร้สาย โดยเฉพาะเครือข่ายที่ไม่ได้มีการเข้ารหัส เครื่องมือที่ใช้ในการโจมตีแบบนี้ เช่น Ethereal และ Ettercap
- Evil Twin AP: เป็นการสร้าง AP ปลอมขึ้นมาเพื่อหลอกเป้าหมายให้มาเชื่อมต่อ เพื่อดักข้อมูลในการรับส่ง โดย AP ปลอมจะถูกตั้งค่าให้กระจาย (Broadcast) Beacon Frame ที่มีชื่อ SSID เหมือนกันกับของเป้าหมายเพื่อหลอกผู้ใช้งาน
- Man-in-the-Middle attack: เป็นการใช้เทคนิค Man-in-the-Middle attack ปกติ ควบคู่กับ Evil Twin AP เพื่อดักการส่งข้อมูลของเป้าหมาย
- Masquerading: เป็นเทคนิคที่ใช้ในการปลอมแปลงเป็นบุคคลที่มีสิทธิ์ในการเข้าถึงระบบ อย่างการขโมยบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อใช้ Login เข้าระบบ โดยไม่ได้จำกัดวิธีการที่ได้มาซึ่ง Credential ของผู้ใช้งานจริง เช่น ใช้โปรแกรมประเภท Key logger หรือแอบใช้คอมพิวเตอร์ของผู้ใช้งานจริงที่ไม่ได้ล็อกหน้าจอ

ดังนั้น การเชื่อมต่อกับเครือข่ายไร้สายเราต้องพิจารณาถึงเรื่องการรักษา ความปลอดภัยของข้อมูลซึ่งถึงว่าเป็นเรื่องที่สำคัญมากยิ่งขึ้นใน กรณีของเครือข่ายคอมพิวเตอร์ที่ใช้สายต่อทั่วไปเนื่องจากการเปิด กว้างของเครือข่ายซึ่งผู้ใดก็ตามที่มีเครื่องคอมพิวเตอร์ที่ติดตั้ง อุปกรณ์NICต่างก็มีโอกาสเชื่อมต่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ ได้เท่าเทียมกันไม่ว่าจะเป็นเครือข่ายที่ตั้งใจเปิดให้บริการกับสาธารณะ ไปจนถึงเครือข่ายเฉพาะองค์กร

11.4.5 วิธีการสร้างความปลอดภัยสำหรับเครือข่ายไร้สาย

การติดตั้งเครือข่ายไร้สายเพื่อใช้งานในองค์กร ควรจะต้องมีการคำนึงถึงในเรื่องความปลอดภัย โดยหลักการที่ควรปฏิบัติมี ดังนี้

- **จัดทำ AP Configuration Policy:** ทางองค์กรควรจัดทำนโยบาย รวมไปถึงมาตรฐานในการตั้งค่าการใช้งานของ AP และให้ทางผู้ดูแลตั้งค่าให้เป็นไปตามมาตรฐานก่อนใช้งาน โดยในมาตรฐานควรประกอบไปด้วยการเปลี่ยนค่าตั้งต้นของระบบ (Default) เช่น SSID, Username, Password และ SNMP Community String ปิดการใช้งาน Service ที่ไม่จำเป็น เช่น SNMP, Telnet และการตั้งค่าความปลอดภัย เช่น WPA2-PSK, WPA2 Enterprise

- **ตรวจจับ Unauthorized AP:** ผู้ดูแลระบบควรสแกนหา AP แปกปลอมที่ไม่ได้รับอนุญาตให้ติดตั้ง เพื่อป้องกันไม่ให้ผู้บุกรุกใช้ AP เหล่านี้เป็นช่องทางในการเข้าถึงเครือข่ายภายในขององค์กร
- **กำหนดให้มีการประเมินด้านความปลอดภัย:** องค์กรควรจัดให้มีการตรวจสอบ (Audit) เกี่ยวกับความปลอดภัยของเครือข่ายไร้สาย รวมถึงการทดสอบเจาะระบบ และการทบทวน Firewall Rule/ACL ในการกรองข้อมูลที่เข้าออกระหว่าง Wireless และ Wired Network
- **ตั้งค่าความปลอดภัยของ Client:** สำหรับ Client ที่ได้รับการอนุญาตให้ใช้งานเครือข่ายไร้สาย ควรมีการตรวจสอบการตั้งค่าอย่างเป็นประจำ โดยควรจะต้องเปิดใช้งาน Personnel Firewall, การตั้งค่า VPN เมื่อไปใช้เครือข่ายไร้สายนอกองค์กร และการติดตั้งระบบป้องกันโปรแกรมมัลแวร์
- **ใช้ VPN สำหรับองค์กรที่ต้องการความปลอดภัยขั้นสูงสุด:** โดยทั่วไป VPN จะถูกใช้เมื่อ Client ไปเชื่อมต่อกับเครือข่ายภายนอก แต่ก็สามารถนำมาประยุกต์ใช้งานกับ Intranet ได้ ถ้าองค์กรต้องการเพิ่มประสิทธิภาพด้านความปลอดภัยในการใช้งาน

11.5 มาตรการป้องกันการโจมตีทางเครือข่ายไร้สาย

11.5.1 แนวปฏิบัติที่ดีสำหรับป้องกันความปลอดภัยเครือข่ายไร้สาย

กล่าวโดยสรุป คือ หลักการที่เป็นแนวปฏิบัติที่ดีที่สามารถนำไปใช้ป้องกันการโจมตีทางเครือข่ายไร้สายมี ดังนี้

- เปลี่ยนค่า SSID ไม่ใช่ค่าตั้งต้น (Default)
- เปลี่ยนรหัสผ่านในการเข้าถึงอุปกรณ์ AP และ router รวมถึงเปิดใช้งาน Firewall
- ตั้งค่า MAC Address Filtering
- เปิดใช้งานการเข้ารหัส และเปลี่ยน Passphrase อย่างสม่ำเสมอ
- ใช้ฟังก์ชัน SSID Clocking เพื่อไม่ให้บุคคลอื่นสามารถเห็น SSID ขององค์กร
- ติดตั้ง Firewall เพื่อควบคุมข้อมูลเข้าออกระหว่างเครือข่ายไร้สาย และเครือข่ายภายในขององค์กร
- ตรวจสอบ Configuration ของอุปกรณ์ Wireless อย่างสม่ำเสมอ
- ใช้เทคโนโลยีด้านความปลอดภัยอื่นมาเสริมในการเข้ารหัส เช่น IPSec

ต่อไปนี้เป็นแนวทางทั่วไปในการรักษาความปลอดภัยเครือข่าย สำหรับเครือข่ายในบ้านและในสำนักงานขนาดเล็ก

ปรับปรุงคอมพิวเตอร์ของคุณอยู่เสมอ

เมื่อต้องการรักษาคอมพิวเตอร์บนเครือข่ายขององค์กรให้ปลอดภัยมากขึ้น ให้เปิดการปรับปรุงอัตโนมัติบนคอมพิวเตอร์แต่ละเครื่อง Windows สามารถติดตั้งการปรับปรุงที่สำคัญและที่แนะนำได้โดยอัตโนมัติ หรือ

เฉพาะการปรับปรุงที่สำคัญเท่านั้น การปรับปรุงที่สำคัญมีประโยชน์อย่างยิ่ง เช่น ทำให้มีความปลอดภัยและความน่าเชื่อถือเพิ่มมากขึ้น การปรับปรุงที่แนะนำสามารถจัดการกับปัญหาที่ไม่ร้ายแรง และช่วยพัฒนาประสบการณ์ด้านการใช้คอมพิวเตอร์ของผู้ใช้ทั่วไปได้ การปรับปรุงที่เป็นทางเลือกจะไม่มีการดาวน์โหลดหรือติดตั้งโดยอัตโนมัติ

ใช้ไฟร์วอลล์

ไฟร์วอลล์จะช่วยป้องกันไม่ให้แฮกเกอร์หรือซอฟต์แวร์ที่เป็นอันตราย เช่น หนอน เข้าถึงคอมพิวเตอร์ขององค์กรผ่านทางเครือข่ายหรืออินเทอร์เน็ต นอกจากนี้ ไฟร์วอลล์ยังช่วยหยุดไม่ให้คอมพิวเตอร์ของเราส่งซอฟต์แวร์ที่เป็นอันตรายไปยังคอมพิวเตอร์เครื่องอื่นโดยไม่รู้ตัวอีกด้วย

การเปิดหรือปิด Windows Firewall

เรียกใช้ซอฟต์แวร์ป้องกันไวรัสบนคอมพิวเตอร์แต่ละเครื่อง ไฟร์วอลล์ ช่วยป้องกันหนอนและแฮกเกอร์ แต่ไม่ได้รับการออกแบบให้ป้องกันไวรัส ดังนั้นควรติดตั้งและใช้โปรแกรมป้องกันไวรัส ไวรัสอาจมาจากเอกสารแนบข้อความอีเมล แฟ้มบนแผ่นซีดีหรือดีวีดี หรือแฟ้มที่ดาวน์โหลดจากอินเทอร์เน็ต ตรวจสอบให้แน่ใจว่ามีการปรับปรุงโปรแกรมป้องกันไวรัสอยู่เสมอ และมีการตั้งค่าให้สแกนเครื่องคอมพิวเตอร์เป็นประจำ

ใช้เราเตอร์เพื่อใช้การเชื่อมต่ออินเทอร์เน็ตร่วมกัน

ให้ใช้เราเตอร์ หรือที่เรียกว่า อุปกรณ์เกตเวย์ในที่พักอาศัย เพื่อใช้การเชื่อมต่ออินเทอร์เน็ตร่วมกัน โดยปกติอุปกรณ์เหล่านี้จะอยู่ในตัวไฟร์วอลล์และคุณลักษณะอื่นๆ ที่สามารถป้องกันเครือข่ายจากการคุกคามของแฮกเกอร์ได้ดียิ่งขึ้น

อย่าเข้าสู่ระบบในฐานะผู้ดูแล

เมื่อใช้โปรแกรมต่างๆ ที่ต้องการการเข้าถึงอินเทอร์เน็ต เช่น เว็บเบราว์เซอร์ หรือโปรแกรมอีเมล ควรเข้าสู่ระบบในฐานะผู้ใช้มาตรฐานแทนที่จะเป็นฐานะผู้ดูแล เนื่องจากมีไวรัสและหนอนหลายชนิดที่ไม่สามารถถูกเก็บและเรียกใช้บนคอมพิวเตอร์ของเราได้ เว้นแต่เราได้เข้าสู่ระบบในฐานะผู้ดูแล

เหตุใดจึงควรใช้บัญชีผู้ใช้มาตรฐาน (standard user) แทนบัญชีผู้ดูแล (administrator)

บัญชีมาตรฐาน สามารถช่วยป้องกันคอมพิวเตอร์ของเราโดยการป้องกันไม่ให้ผู้ใช้ทำการเปลี่ยนแปลงที่ส่งผลกระทบต่อทุกคนที่ใช้คอมพิวเตอร์ ในการใช้งานทั่วไป ควรสร้างบัญชีมาตรฐานสำหรับผู้ใช้แต่ละราย เมื่อเราเข้าสู่ระบบ Windows โดยใช้บัญชีมาตรฐาน ก็สามารถทำสิ่งต่างๆ ได้เช่นเดียวกับที่ใช้บัญชีผู้ดูแล แต่ถ้าต้องการทำบางสิ่งบางอย่างที่ส่งผลกระทบต่อผู้ใช้คอมพิวเตอร์รายอื่นๆ เช่น การติดตั้งซอฟต์แวร์หรือการเปลี่ยนการตั้งค่าความปลอดภัย Windows อาจขอให้เราป้อนรหัสผ่านสำหรับบัญชีผู้ดูแล

11.5.2 มาตรการความปลอดภัยของเครือข่ายแบบไร้สายสำหรับองค์กร

ในกรณีที่องค์กรมีเครือข่ายแบบไร้สาย มีข้อควรระวังด้านความปลอดภัยเพิ่มเติมที่ควรปฏิบัติดังต่อไปนี้

ใช้คีย์เพื่อความปลอดภัยของเครือข่าย

ในเครือข่ายแบบไร้สาย ควรติดตั้งคีย์หรือการเข้ารหัสลับเพื่อความปลอดภัยของเครือข่าย ซึ่งจะเปิดใช้งานการเข้ารหัสลับ การเข้ารหัสลับจะทำให้ไม่มีใครสามารถเชื่อมต่อกับเครือข่ายของเราได้หากไม่มีคีย์เพื่อความปลอดภัย นอกจากนั้นข้อมูลใดๆ ที่ส่งผ่านเครือข่ายจะมีการเข้ารหัสลับ เพื่อให้อ่านข้อมูลได้เฉพาะคอมพิวเตอร์ที่มีคีย์ในการถอดรหัสเท่านั้น ซึ่งเป็นการป้องกันความพยายามในการเข้าถึงเครือข่ายของเราโดยไม่มีสิทธิ์ วิธีการเข้ารหัสลับของเครือข่ายแบบไร้สายโดยทั่วไปคือ Wi-Fi Protected Access (WPA) และ WPA2 ควรเลือกใช้กลไกการเข้ารหัสของ WEP ในเครือข่าย IEEE 802.11 WLAN หากไม่มีกลไกสำหรับเข้ารหัสข้อมูลอื่นๆ ที่ปลอดภัยกว่าให้เลือกใช้ ถึงแม้ว่ากลไกการเข้ารหัสของ WEP จะมีช่องโหว่ก็ตามแต่ก็สามารถสร้างความปลอดภัยให้กับเครือข่ายได้ในระดับหนึ่ง เนื่องจากซอฟต์แวร์ Aircrack หรือ WEPCrack สำหรับเจาะรหัสลับในเครือข่าย IEEE 802.11 WLAN ซึ่งถูกพัฒนาบนระบบปฏิบัติการ Linux มีการติดตั้งที่ค่อนข้างยุ่งยากโดยเฉพาะอย่างยิ่งสำหรับผู้ไม่มีความชำนาญกับระบบปฏิบัติการ Linux ดังนั้น กลไกการเข้ารหัสของ WEP จึงสามารถกีดกันผู้โจมตีสมัครเล่นจำนวนหนึ่งซึ่งไม่สามารถติดตั้งซอฟต์แวร์ดังกล่าวได้

เปลี่ยนรหัสผ่านและชื่อผู้ดูแลเริ่มต้นบนเราเตอร์หรือแอ็กเซสพอยน์

ในกรณีที่เรามีเราเตอร์หรือแอ็กเซสพอยน์ เราอาจใช้ชื่อและรหัสผ่านเริ่มต้นเพื่อติดตั้งอุปกรณ์ ผู้ผลิตส่วนใหญ่จะใช้รหัสผ่านและชื่อเริ่มต้นเดียวกันสำหรับอุปกรณ์ทั้งหมดของตน ซึ่งทำให้มีบางคนสามารถเข้าถึงเราเตอร์หรือจุดเข้าใช้งานของคุณได้โดยที่ผู้ดูแลไม่รู้ เพื่อหลีกเลี่ยงจากความเสียดังกล่าว ให้เปลี่ยนชื่อผู้ใช้ของผู้ดูแลและรหัสผ่านเริ่มต้นสำหรับเราเตอร์ของเรา จึงควรตรวจสอบข้อมูลที่มาพร้อมกับอุปกรณ์เพื่อดูขั้นตอนในการเปลี่ยนชื่อและรหัสผ่าน

ในการติดตั้งอุปกรณ์ IEEE 802.11 WLAN คือเปลี่ยน Login ID และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ดังกล่าว ผู้ดูแลระบบควรเลือกใช้ Login ID และรหัสผ่านที่มีความแข็งแรงสูงเพื่อให้ผู้โจมตีไม่สามารถเดาหรือเจาะรหัสได้โดยง่ายและควรมีการเปลี่ยน Login ID และรหัสผ่านอย่างสม่ำเสมอ เพื่อสะดวกต่อการใช้งานโดยปกติ ค่า default ของแอ็กเซสพอยน์หลายยี่ห้อจะใช้รหัสผ่านเพื่อการรัน SNMP Simple (Simple Network Management Protocol) ด้วยค่าทั่วไป เช่น 3COM ใช้คำว่า “public” หรือ “comcomcom” เป็นต้น นอกจากนี้ผู้ดูแลระบบไม่ควรอนุญาตให้มีการตั้งค่าการทำงานของอุปกรณ์ผ่านอินเทอร์เน็ตด้วย SNMP เพื่อป้องกันไม่ให้ผู้โจมตีซึ่งอาจทราบข้อมูลของ Login ID และรหัสผ่านจากการดักฟังหรือเจาะรหัส สามารถอ่านหรือ

ปรับเปลี่ยนค่าการทำงานของอุปกรณ์ผ่านเครือข่ายได้ มาตรการเหล่านี้เป็นสิ่งที่ผู้ดูแลระบบควรปฏิบัติในการติดตั้งอุปกรณ์ทุกชนิดมิใช่แต่เพียงอุปกรณ์ IEEE 802.11 เท่านั้น

เปลี่ยนค่า SSID เริ่มต้น

เราเตอร์และแอ็กเซสพอยน์ท์จะใช้ชื่อเครือข่ายแบบไร้สายที่เรียกว่าตัวระบุชุดบริการ (SSID: Service Set Identifier) ผู้ผลิตส่วนใหญ่จะใช้ SSID เดียวกันสำหรับเราเตอร์และจุดเข้าใช้งานทั้งหมดของตน จึงควรเปลี่ยน SSID เริ่มต้น เพื่อรักษาเครือข่ายแบบไร้สายไม่ให้ทับซ้อนกับเครือข่ายแบบไร้สายอื่นที่อาจใช้ SSID เริ่มต้นเดียวกับเรา ถ้าบริเวณใกล้เคียงมีเครือข่ายอยู่มากกว่าหนึ่งเครือข่าย การระบุหาเครือข่ายไร้สายไหนเป็นของเราย่อมจะง่ายยิ่งขึ้น เนื่องจากโดยปกติ SSID จะแสดงอยู่ในรายการเครือข่ายที่พร้อมใช้งาน ให้ตรวจสอบข้อมูลที่มาพร้อมกับอุปกรณ์เพื่อดูขั้นตอนในการเปลี่ยน SSID เริ่มต้น

ตัวอย่างของ SSID เริ่มต้นของอุปกรณ์แต่ละยี่ห้อ

“tsunami” – Cisco

”101” – 3Com

“RoamAbout Default Network Name” – Lucent/Cabletron

“Compaq” – Compaq

“WLAN” – Addtron

“intel” – Intel

“linksys” – Linksys

“Default SSID”, “Wireless” – Other manufacturers

จัดวางเราเตอร์และแอ็กเซสพอยน์ท์อย่างระมัดระวัง

สัญญาณแบบไร้สายสามารถส่งได้ไกลสองสามร้อยฟุต ดังนั้น สัญญาณจากเครือข่ายของเราสามารถออกอากาศไปภายนอกบ้านได้ เราสามารถจำกัดพื้นที่ที่สัญญาณแบบไร้สายจะส่งถึงได้ โดยจัดวางเราเตอร์หรือจุดเข้าใช้งานให้ใกล้กับจุดกึ่งกลางของบ้านมากกว่าที่จะให้อยู่ใกล้หน้าต่างหรือผนังด้านนอก

ปิดกั้นการทำงานในโหมด Adhoc หรือ Peer-to-Peer

การใช้งานในโหมด Adhoc หรือ Peer-to-Peer ทำให้อุปกรณ์ IEEE 802.11 สามารถติดต่อสื่อสารถึงกันได้โดยไม่ต้องผ่านอุปกรณ์แม่ข่าย ในกรณีที่คอมพิวเตอร์ของผู้ใช้มีการติดตั้งอุปกรณ์ IEEE 802.11 และอนุญาตให้มีการใช้งานในโหมดดังกล่าว ผู้บุกรุกซึ่งอยู่ในบริเวณใกล้เคียงภายในระยะของคลื่นสัญญาณวิทยุอาจจะสามารถเชื่อมต่อเข้ากับคอมพิวเตอร์ของผู้ใช้นั้นได้โดยตรง ผู้บุกรุกสามารถเข้าถึง ดัดแปลงหรือทำลายไฟล์และข้อมูล

ความลับ สร้างประตูลับ (backdoor) เรียกใช้งานรหัสต่างๆ หรือกระทำการอื่นๆ ได้ตามประสงค์บนระบบของเรา จึงควรไม่อนุญาตให้อุปกรณ์แลนไร้สายทำงานในโหมด Peer-to-Peer เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี ซึ่งการปิดกันประเภทนี้จะไม่ส่งผลกระทบต่อการใช้งานของผู้ใช้ทั่วไป เพราะโดยปกติแล้วอุปกรณ์ IEEE 802.11 จะถูกติดตั้งให้ใช้งานในโหมด Infrastructure เพื่ออนุญาตให้ผู้ใช้สามารถเชื่อมต่อเข้ากับอินเทอร์เน็ตได้

ควบคุม MAC Address ของผู้ใช้

การป้องกันไม่ให้ผู้บุกรุกสามารถเข้าใช้เครือข่ายได้คือการควบคุม MAC Address ของอุปกรณ์แลนไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address ดังที่กำหนดไว้เท่านั้นให้ใช้เครือข่ายได้อย่างถูกต้อง ซึ่งโดยปกติแล้ว อุปกรณ์แม่ข่าย (AP) ของ IEEE 802.11 ซึ่งใช้กันอยู่ทั่วไปจะมีฟังก์ชันดังกล่าวติดตั้งไว้ให้เลือกใช้ได้ด้วย แต่วิธีการเช่นนี้ อาจไม่สะดวกสำหรับระบบไร้สายขนาดใหญ่ที่มีอุปกรณ์ 802.11 WLAN จำนวนมาก จึงเหมาะสำหรับแลนไร้สายขนาดเล็กหรือตามที่พักอาศัย นอกจากนั้นหากผู้บุกรุกใช้วิธีการปลอม MAC Address (MAC Address spoofing) ซึ่งสามารถทำได้โดยวิธีการดักฟังสัญญาณ (แม้จะมีการเข้ารหัสข้อความก็ตามแต่ MAC Header จะไม่ถูกเข้ารหัส) อย่างไรก็ตาม หากไม่มีวิธีป้องกันที่ดีกว่านี้ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address ของผู้ใช้ ย่อมปลอดภัยกว่าการไม่ได้ควบคุมป้องกันใดๆ เลย

หลีกเลี่ยงการใช้ DHCP

การใช้ DHCP (Dynamic Host Control Protocol) ซึ่งเป็นกลไกเพื่อแจก IP Address ให้แก่เครื่องลูกข่ายโดยอัตโนมัติ เพื่อความสะดวกต่อผู้ใช้งานมากในการเชื่อมต่อเข้ากับอินเทอร์เน็ตโดยไม่จำเป็นต้องจดจำ IP Address ของแต่ละเครื่อง อีกทั้งยังเป็นเครื่องมือช่วยบริหาร IP Address ได้อย่างมีประสิทธิภาพ แต่ขณะเดียวกัน การใช้ DHCP ก็ทำให้ผู้ที่บุกรุกแลนไร้สายได้แล้วสามารถเชื่อมต่อเข้าใช้อินเทอร์เน็ตได้โดยสะดวกเช่นเดียวกัน ดังนั้น ผู้ดูแลระบบควรหลีกเลี่ยงการใช้ DHCP ซึ่งจะทำให้ผู้โจมตีต้องใช้ความพยายามสูงขึ้นในการต่อเชื่อมเข้ากับเครือข่ายอินเทอร์เน็ต

11.5.3 การป้องกันการปฏิเสธการให้บริการ

การโจมตีแบบ DoS ส่วนใหญ่นั้นตรวจจับได้ง่าย อย่างไรก็ตาม การโจมตีหลายครั้งนั้นยากที่จะหยุดยั้งแม้หลังจากตรวจพบแล้ว ต่อไปนี้คือสามวิธีที่นิยมใช้กันมากที่สุดในการหยุดยั้งการโจมตีแบบ DoS

แบล็กโฮลลิง (Black holing)

เป็นวิธีหนึ่งที่เป็นไปได้ในการหยุดยั้งการโจมตีแบบ DoS นี่คือการสถานการณ์ที่เราทิ้งแพ็กเก็ต IP ทั้งหมดจากผู้โจมตี นี่ไม่ใช่กลยุทธ์ที่ตลกในระยะเวลา เพราะผู้โจมตีสามารถเปลี่ยนที่อยู่ต้นทางได้อย่างรวดเร็ว

การดำเนินการนี้อาจส่งผลเสียหากดำเนินการโดยอัตโนมัติ ผู้โจมตีอาจตั้งใจปลอมแปลงแพ็กเก็ตการโจมตีด้วยที่อยู่ IP ของพันธมิตรองค์กร การป้องกันแบบอัตโนมัติอาจบล็อกการรับส่งข้อมูลที่ต้องการจากพันธมิตรนั้น และก่อให้เกิดปัญหาเพิ่มเติม

การตรวจสอบแฮนด์เชค (Validating the handshake)

การตรวจสอบความถูกต้องของแฮนด์เชคเกี่ยวข้องกับการสร้างการเปิดแบบปลอม และจะไม่จัดสรรทรัพยากรจนกว่าผู้ส่งจะยืนยัน ไฟร์วอลล์บางตัวจัดการกับ SYN flood โดยการตรวจสอบความถูกต้องของแฮนด์เชค TCP ล่วงหน้า ซึ่งทำได้โดยการสร้างการเปิดแบบปลอม เมื่อใดก็ตามที่เซกเมนต์ SYN มาถึง ไฟร์วอลล์จะส่งเซกเมนต์ SYN/ACK กลับมา โดยไม่ส่งเซกเมนต์ SYN ไปยังเซิร์ฟเวอร์เป้าหมาย

ไฟร์วอลล์จะส่งเซกเมนต์ SYN เดิมไปยังเซิร์ฟเวอร์ที่ตั้งใจไว้ในตอนแรกก็ต่อเมื่อไฟร์วอลล์ได้รับ ACK ซึ่งจะเกิดขึ้นเฉพาะในการเชื่อมต่อที่ถูกต้องเท่านั้น ไฟร์วอลล์จะไม่จัดสรรทรัพยากรสำหรับการเชื่อมต่อเมื่อเซกเมนต์ SYN มาถึง ดังนั้นการจัดการเซกเมนต์ SYN ปลอมจำนวนมากจึงเป็นภาระเล็กน้อย

การจำกัดอัตรา (Rate limiting)

การจำกัดอัตราสามารถใช้เพื่อลดปริมาณการรับส่งข้อมูลบางประเภทให้เหลือเพียงปริมาณที่สามารถรับมือได้อย่างเหมาะสม การแพร่สัญญาณไปยังเครือข่ายภายในยังคงสามารถใช้ได้ แต่ในอัตราที่จำกัดเท่านั้น วิธีนี้ใช้สำหรับการโจมตีแบบ DoS ที่ละเอียดอ่อนกว่า วิธีนี้มีประโยชน์หากการโจมตีมีเป้าหมายที่เซิร์ฟเวอร์เพียงเครื่องเดียว เนื่องจากวิธีนี้จะทำให้สายส่งข้อมูลอย่างน้อยบางส่วนเปิดกว้างสำหรับการสื่อสารอื่นๆ

การจำกัดอัตราทำให้ทั้งผู้โจมตีและผู้ใช้งานรู้สึกหงุดหงิด วิธีนี้ช่วยได้แต่ไม่ได้แก้ปัญหาได้ทั้งหมด เมื่อทราฟฟิก DoS อุดตันสายเชื่อมต่ออินเทอร์เน็ต ไฟร์วอลล์ชายแดนก็ไม่สามารถช่วยเหลือสถานการณ์ได้ การโจมตี DoS ส่วนใหญ่เป็นปัญหาของชุมชน ซึ่งสามารถหยุดยั้งได้ด้วยความช่วยเหลือจาก ISP และองค์กรต่างๆ ที่คอมพิวเตอร์ของพวกเขาถูกควบคุมเป็นบอตและถูกใช้โจมตีบริษัทอื่นๆ

ปัจจุบันเครือข่ายไร้สายได้รับความนิยมอย่างกว้างขวาง หลายขีดจำกัดของเครือข่ายแบบมีสายเดิมลงได้อย่างรวดเร็ว แต่ก็มาพร้อมกับความเสี่ยงของภัยคุกคามรูปแบบต่างๆ ดังที่ได้อธิบายไว้ข้างต้น แม้ปัจจุบันได้มีการพัฒนาการรักษาความปลอดภัยไว้หลากหลายวิธีขึ้นมาเพื่อรับมือกับภัยคุกคามที่เกิดขึ้น อย่างไรก็ตาม กลไกเหล่านั้นยังไม่สามารถปกป้องเครือข่ายไร้สายได้สมบูรณ์แบบ อีกทั้งวิธีการการโจมตีก็ได้พัฒนาไปสู่วิธีการใหม่ๆ อยู่เสมออีกด้วยเช่นกัน

11.6 สรุปบท

เนื้อหาในบทนี้กล่าวถึงกลยุทธ์การรับมือและป้องกันการโจมตีแบบ DoS และภัยคุกคามในเครือข่ายไร้สาย โดยครอบคลุมทั้งวิธีเชิงเทคนิค เช่น การตรวจสอบ handshake การจำกัดอัตราทราฟฟิก และบทวิเคราะห์

เกี่ยวกับวิวัฒนาการของมาตรฐานความปลอดภัยตั้งแต่ WEP ถึง WPA3 รวมถึงมาตรการองค์กรที่จำเป็น สะท้อนให้เห็นว่าแม้จะมีการพัฒนาเทคโนโลยีและมาตรการต่างๆ อย่างต่อเนื่อง เครือข่ายไร้สายยังต้องเผชิญกับความท้าทายด้านความมั่นคงปลอดภัยและการโจมตีรูปแบบใหม่อยู่เสมอ

11.7 บทวิเคราะห์และมุมมองเชิงวิชาการ: “ความมั่นคงปลอดภัยเครือข่ายไร้สาย (Wireless Network Security)”

เอกสารคำสอน บทเรียน “ความมั่นคงปลอดภัยเครือข่ายไร้สาย” ของรายวิชา **หลักการความมั่นคงทางไซเบอร์** ได้วิเคราะห์เชิงลึกถึงประเภทการโจมตี การป้องกันเชิงวิศวกรรม และวิวัฒนาการของมาตรฐาน IEEE 802.11 ตั้งแต่ WEP → WPA → WPA2 → WPA3 รวมถึงภัยคุกคามและมาตรการองค์กรที่ต้องใช้เพื่อลดความเสี่ยง หัวข้อนี้ถือเป็นรากฐานสำคัญสำหรับการเรียนการสอนด้าน Cybersecurity เนื่องจากเครือข่ายไร้สายมีบทบาทอย่างมากต่อการดำเนินชีวิตประจำวันและธุรกิจในยุคดิจิทัล สรุปสาระสำคัญของมุมมองและบทวิเคราะห์ทางวิชาการได้ดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

- **ประเภทการโจมตี:** ครอบคลุม 8 รูปแบบ ได้แก่ *insertion attack, interception, jamming, client-to-client, brute-force password, encryption attack, misconfiguration* และ *MITM*
- **แนวคิดการป้องกัน:** เช่น MAC filtering, WIPS (Wireless Intrusion Prevention System), captive portal และ VPN สำหรับองค์กรและผู้ให้บริการ
- **วิวัฒนาการของมาตรฐานความปลอดภัย:**
 - WEP – ใช้ RC4 และ shared key แต่ถูกเจาะได้ง่าย
 - WPA/WPA2 – เพิ่ม TKIP, AES และ 4-way handshake ภายใต้มาตรฐาน 802.11i
 - WPA3 – ใช้ *Simultaneous Authentication of Equals (SAE)* เพื่อป้องกัน dictionary/brute-force attack พร้อมบังคับใช้ PMF (Protected Management Frame)
- **มาตรการองค์กร:** เช่น การ audit, ปิดพอร์ตสถิติที่ไม่ได้ใช้, แบ่ง VLAN, ใช้ MFA และ SSO ร่วมกับการตรวจสอบสิทธิ์ 802.1X

2) มุมมองเชิงวิชาการและความก้าวหน้าปัจจุบัน

1. **จาก WPA2 → WPA3 และ Wi-Fi 6/6E/7** WPA3 ช่วยเพิ่มความแข็งแกร่งของการเข้ารหัสและยืนยันตัวตน แต่ความท้าทายคืออัตราการใช้งานที่ยังไม่แพร่หลาย จำเป็นต้องให้ผู้เรียนเข้าใจทั้ง ข้อจำกัดของ WPA2 และศักยภาพของ WPA3

2. **Zero Trust Wireless** แนวคิด Zero Trust ถูกประยุกต์กับ Wi-Fi โดยให้ผู้เรียนศึกษา *identity-based access control, micro-segmentation* และการตรวจสอบต่อเนื่อง ซึ่งช่วยลดผลกระทบจาก rogue AP และ insider attack
3. **AI-driven Wireless Security** จาก WIPS ที่ใช้ signature-based ปัจจุบันมีการใช้ **AI/ML anomaly detection** และ **MITRE ATT&CK for Wireless** ใน SOC ทำให้การเฝ้าระวัง proactive มากขึ้น
4. **Wireless Security กับ IoT/5G** IoT และ 5G กำลังเปลี่ยนภาพรวม wireless security ไปสู่ความท้าทายใหม่ เช่น *low-power encryption, edge security* และ *massive device authentication*

3) ประสบการณ์และการสอดแทรกเชิงการสอน

จากประสบการณ์ทางวิชาชีพและวิชาการ พบว่าผู้เรียนมักคิดว่า *Wi-Fi = ง่ายและฟรี* จึงขาดความตระหนักด้านความปลอดภัย การออกแบบกิจกรรมให้ทดลอง *wardriving, rogue AP detection* และ *packet sniffing* จะช่วยให้ผู้เรียน “เห็นจริง” ว่าภัยคุกคามไร้สายสามารถเกิดขึ้นได้ง่ายดาย และเรียนรู้ว่าการป้องกันไม่ได้ขึ้นกับอุปกรณ์เท่านั้น แต่ขึ้นกับ *policy, monitoring* และ *user awareness*

บทเรียนนี้ให้ภาพรวมที่แข็งแกร่งเกี่ยวกับ *wireless attack vectors, IEEE 802.11 security evolution* และ *best practices* อย่างไรก็ตาม เพื่อตอบโจทย์ยุคดิจิทัล จำเป็นต้องอัปเดตการสอนด้วย **WPA3, Zero Trust Wireless, AI-driven SOC, IoT/5G Security** และ **MITRE ATT&CK** เพื่อให้นักศึกษาเข้าใจทั้งพื้นฐานและการประยุกต์ใช้งานเชิงลึก

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายการโจมตีแบบ Man-in-the-Middle (MITM) ในเครือข่ายไร้สาย

แนวคำตอบ: ผู้โจมตีแทรกกลางการสื่อสารระหว่างผู้ใช้และ AP เช่น ARP Spoofing/Evil Twin ดักข้อมูล login, session

ข้อ 2. เปรียบเทียบ WEP, WPA, WPA2 และ WPA3

แนวคำตอบ: WEP = อ่อนแอ, WPA = TKIP, WPA2 = AES, WPA3 = SAE, PMF, ปลอดภัยที่สุด

ข้อ 3. วิเคราะห์ภัยคุกคามแบบ Wi-Fi Chalking และผลกระทบ

แนวคำตอบ: ใช้ WarDriving/Walking/Flying หา AP เปิด → ผู้ไม่หวังดีใช้เชื่อมต่อ → ขโมยข้อมูล/โจมตีระบบ

ข้อ 4. อธิบายการทำงานของ IEEE 802.1X

แนวคำตอบ: ใช้ EAPOL ตรวจสอบ 3 ฝ่าย (Supplicant, Authenticator, Authentication Server) → อนุญาต/ปฏิเสธการเชื่อมต่อ

ข้อ 5. เสนอแนวทางป้องกันการโจมตีใน Wi-Fi สาธารณะ

แนวคำตอบ: ใช้ WPA3, VPN, ปิด SSID, Captive Portal, ไม่ใช้ WEP

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. ข้อใดไม่ใช่การโจมตีไร้สาย

ก. Jamming

ข. Evil Twin

ค. SQL Injection

ง. MITM

เฉลย: ค

ข้อ 2. การโจมตีด้วยการเดารหัสผ่าน AP จัดเป็นการโจมตีแบบใด

ก. Brute Force

ข. Encryption Attack

ค. Jamming

ง. WarDriving

เฉลย: ก

ข้อ 3. WEP มีจุดอ่อนสำคัญใด

ก. ใช้การเข้ารหัส RC4 ที่อ่อนแอ

ข. รองรับ AES-256

ค. มี PMF

ง. ป้องกัน Brute Force ได้

เฉลย: ก

ข้อ 4. WPA2 ใช้การเข้ารหัสใด

ก. RC4

ข. TKIP

ค. AES

ง. MD5

เฉลย: ค

ข้อ 5. WPA3 ใช้ฟีเจอร์ใดเพิ่มความปลอดภัย

ก. SAE

ข. WEP

ค. RC4

ง. DES

เฉลย: ก

ข้อ 6. IEEE 802.1X มีองค์ประกอบใดบ้าง

ก. Supplicant, Authenticator, Server

ข. Client, Switch, ISP

ค. User, Firewall, Gateway

ง. Host, AP, NAT

เฉลย: ก

ข้อ 7. การโจมตีแบบ Rogue Access Point มีผลใด

ก. สร้าง AP ปลอมให้ผู้ใช้เชื่อมต่อ

ข. ป้องกันการเข้าถึง AP จริง

ค. ลดสัญญาณรบกวน

ง. เร่งความเร็ว Wi-Fi

เฉลย: ก

ข้อ 8. กลไกใดใช้ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ก. WEP

ข. WPA3

ค. SSID Broadcasting

ง. Jamming

เฉลย: ข

ข้อ 9. การโจมตี Wi-Fi Chalking มักใช้วิธีใด

ก. WarDriving

ข. VPN

ค. Firewall

ง. Captive Portal

เฉลย: ก

ข้อ 10. ข้อใดเป็นมาตรการป้องกัน Wi-Fi สาธารณะ

ก. ใช้ VPN

ข. ใช้ WEP

ค. เปิด SSID

ง. ปิด Firewall

เฉลย: ก

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ. (ม.ป.ป.). *ความมั่นคงปลอดภัยเครือข่ายไร้สาย (Wireless Network Security)*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Kurose, J., & Ross, K. (2021). *Computer Networking: A Top-Down Approach*.

IEEE. (2020). *IEEE 802.11ax-2020: Wi-Fi 6 Standard*.

MITRE. (2023). *ATT&CK Framework: Wireless Tactics*.

NIST. (2020). *Zero Trust Architecture (SP 800-207)*.

Wi-Fi Alliance. (2019). *WPA3 Security Enhancements*.

Stallings, W. (2021). *Wireless Communications & Security*. Pearson.

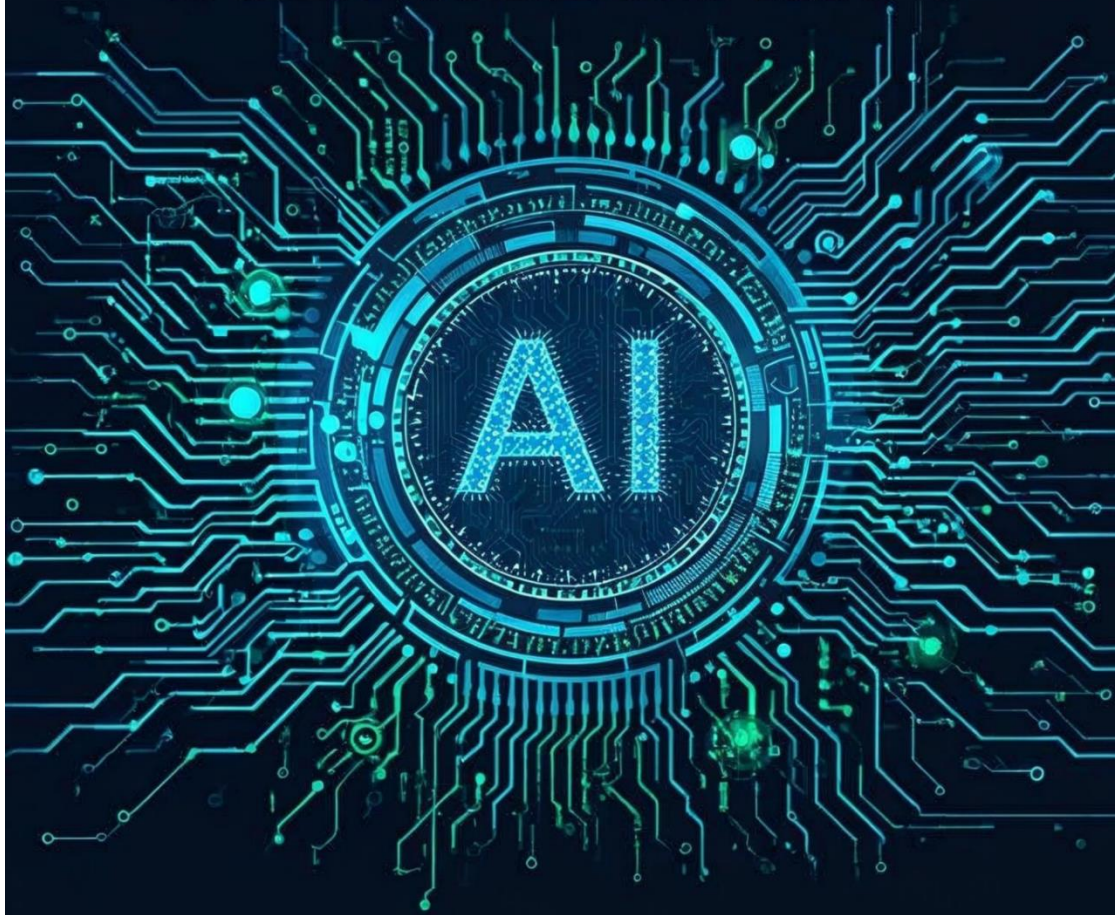
บทที่ 12

ความมั่นคงปลอดภัยในระบบปฏิบัติการ

Security in Operating Systems

วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์

CYBERSECURITY



ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ

บทที่ 12 ความมั่นคงปลอดภัยในระบบปฏิบัติการ (Security in Operating Systems)

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบบทนี้ นักศึกษาจะสามารถ:

- 1) อธิบายความแตกต่างระหว่าง การป้องกัน (Protection) และ ความมั่นคงปลอดภัย (Security) ในระบบปฏิบัติการได้
- 2) วิเคราะห์และอธิบายโครงสร้างการป้องกัน (Protection Structure) เช่น ACL, C-list และ Access Matrix ได้
- 3) อธิบายแนวคิด โดเมนการป้องกัน (Protection Domain) และการให้อำนาจ (Capability) ได้
- 4) อธิบายกลไกการพิสูจน์ตัวตนจริง (Authentication) และปัญหาของรหัสผ่าน/ชีวมิติได้
- 5) วิเคราะห์ภัยคุกคามจากโปรแกรมอันตราย (Malware) เช่น ไวรัส หนอน ม้าโทรจัน ประตูลับ ได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบบทนี้ นักศึกษาจะสามารถ:

- 1) ระบุเป้าหมายของการป้องกันในระบบปฏิบัติการ เช่น การจำกัดสิทธิ์ การป้องกันข้อมูลร่วมกัน
- 2) อธิบายวิธีการควบคุมสิทธิ์การเข้าถึงด้วย ACL, C-list และ Access Matrix
- 3) วิเคราะห์ตัวอย่างระบบ (Unix, Multics) ที่ใช้แนวคิดโดเมนการป้องกันได้
- 4) อธิบายข้อดี-ข้อเสียของวิธีการยืนยันตัวตน เช่น รหัสผ่าน, one-time password, biometrics
- 5) เสนอแนวทางป้องกันการโจมตีระบบปฏิบัติการโดยอาศัยกลไกการป้องกันและมาตรการเชิงนโยบายได้

3. หัวข้อเนื้อหา

12.1 การป้องกันและความมั่นคงปลอดภัย

- 12.1.1 เป้าหมายของการป้องกัน
- 12.1.2 การใช้สารสนเทศร่วมกัน
- 12.1.3 การพิสูจน์ตัวตนจริง
- 12.2 โครงสร้างการป้องกัน
 - 12.2.1 รายการควบคุมการเข้าถึง หรือ ACL
 - 12.2.2 รายการให้อำนาจ หรือ C-list
- 12.3 โดเมนของการป้องกัน
 - 12.3.1 โครงสร้างโดเมน (Domain Structure)
 - 12.3.2 ยูนิกซ์
 - 12.3.3 มัลทิกซ์ (MULTICS)
- 12.4 การให้อำนาจ
 - 12.4.1 ระบบคอมพิวเตอร์แบบการให้อำนาจ (Capability-Based Computer System)
 - 12.4.2 การกำหนดเลขที่อยู่แบบการให้อำนาจ (Capability-based addressing)
 - 12.4.3 คำสั่งปฏิบัติการบนอ็อบเจกต์และการให้อำนาจ
 - 12.4.4 การแบ่งปันการป้องกันของอ็อบเจกต์
 - 12.4.5 การป้องกันการให้อำนาจ
- 12.5 การใช้งานเมทริกซ์การเข้าถึง
 - 12.5.1 ตารางส่วนกลาง (Global Table)
 - 12.5.2 รายการเข้าถึงสำหรับอ็อบเจกต์ (Access List for Objects)
 - 12.5.3 กลไกการยึด-กุญแจ (Lock-Key Mechanism)
 - 12.5.4 เปรียบเทียบ
 - 12.5.5 การถอนสิทธิ์การเข้าถึง
- 12.6 การพิสูจน์ตัวตนจริง
 - 12.6.1 รหัสผ่าน
 - 12.6.2 จุดอ่อนของรหัสผ่าน
 - 12.6.3 รหัสผ่านที่ถูกเข้ารหัส
 - 12.6.4 รหัสผ่านแบบใช้ครั้งเดียว
 - 12.6.5 ชีวมิติ
- 12.7 โปรแกรมอันตราย
 - 12.7.1 หนอนและไวรัส
 - 12.7.2 ม้าโทรจัน และประตูลับ
 - 12.7.3 การเข้ารหัสลับ

12.8 สรุปบท

12.9 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา: บริษัท *RMUTT EduTech* ใช้เซิร์ฟเวอร์กลางเก็บข้อมูลนักศึกษา พบว่ามีพนักงานบางรายเข้าถึงแฟ้มข้อมูลของตนเองไม่มีสิทธิ์ และมีการติดตั้งโปรแกรมแปลกปลอม (Trojan) ลงในระบบ ทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4–5 คน):

1. วิเคราะห์ปัญหาที่เกิดขึ้นจากการออกแบบสิทธิ์การเข้าถึง
2. ศึกษาโครงสร้าง ACL, C-list และ Access Matrix เพื่อเสนอแนวทางแก้ไข
3. เสนอวิธีการพิสูจน์ตัวตนจริงที่เหมาะสม เช่น multi-factor authentication, biometrics
4. เสนอวิธีตรวจจับและป้องกัน malware ภายในระบบปฏิบัติการ

ประเด็นการเรียนรู้ที่แทรก:

- การป้องกัน vs ความมั่นคงปลอดภัย
- ACL, C-list, Access Matrix
- โดเมนการป้องกัน (Protection Domain)
- การพิสูจน์ตัวตนจริง (Authentication)
- Malware (ไวรัส, หนอน, Trojan, Backdoor)

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ปัญหา (25)	ครอบคลุมและเชื่อมโยงกับทฤษฎี	ครบถ้วนแต่ยังไม่ลึก	กล่าวบางส่วน	ไม่ถูกต้อง
การเสนอวิธีแก้ไขสิทธิ์การเข้าถึง (25)	ครบถ้วนทั้ง ACL, C-list, Matrix	ครบเพียงบางส่วน	กล่าวไม่ครบ	ไม่มีข้อเสนอ
การเสนอวิธี Authentication (25)	ครอบคลุมหลายวิธีและเหมาะสม	ครบแต่ยังไม่เจาะลึก	กล่าวเพียงบางส่วน	ไม่เสนอ
การป้องกัน Malware (25)	ครอบคลุมและมีวิธีตรวจจับ	ครบเพียงบางส่วน	กล่าวไม่ชัดเจน	ไม่เสนอ

บทที่ 12 ความมั่นคงปลอดภัยในระบบปฏิบัติการ

การรบกวนการใช้ทรัพยากรบนระบบคอมพิวเตอร์ถือเป็นภัยคุกคามที่น่าเกรงขามอย่างยิ่งในระบบปฏิบัติการ ธรรมชาติของภัยคุกคามนั้นขึ้นอยู่กับธรรมชาติของทรัพยากรและวิธีการใช้ทรัพยากรนั้น เพื่อทำความเข้าใจเกี่ยวกับการป้องกันและความมั่นคงปลอดภัย (protection and security) เนื้อหาในบทนี้ จะกล่าวถึงภัยคุกคามต่อข้อมูลที่ถูกจัดเก็บอยู่ในระบบเป็นหลัก เนื่องจากภัยคุกคามประเภทนี้ล้วนมีลักษณะที่คล้ายคลึงกันและมีความซับซ้อนมากที่สุด

12.1 การป้องกันและความมั่นคงปลอดภัย

กระบวนการทั้งหมดในระบบปฏิบัติการจะต้องได้รับการปกป้องจากการแทรกสลับโดยกิจกรรมของกระบวนการอื่นๆ ด้วยเหตุนี้ จึงมีอาศัยกลไกต่างๆ จำนวนมากถูกใช้เพื่อรับรองว่าแฟ้มต่างๆ, ส่วนของหน่วยความจำ, ซีพียู และทรัพยากรอื่นๆ จะสามารถถูกใช้งานได้เฉพาะกระบวนการที่ได้รับอนุญาตจากระบบปฏิบัติการให้มีสิทธิ์ใช้เท่านั้น

การป้องกัน (protection) หมายถึง กลไกสำหรับควบคุมการเข้าถึงของโปรแกรม, กระบวนการ, หรือผู้ใช้ต่างๆ ต่อทรัพยากรต่างๆ ที่ถูกกำหนดไว้โดยระบบคอมพิวเตอร์ กลไกดังกล่าวนี้จะต้องจัดเตรียมวิธีในการวางข้อกำหนดร่วมกับวิธีในการบังคับใช้ให้เป็นไปตามข้อกำหนดดังกล่าว นั้น ความแตกต่างระหว่างการป้องกันและความมั่นคงปลอดภัย (security) ได้แก่

-**การป้องกัน** เกี่ยวข้องกับการปกป้องข้อมูลของผู้ใช้และโปรแกรมจากการถูกรบกวนโดยผู้ใช้อื่นๆ ในระบบที่มีสิทธิ์ มุ่งที่ผู้ใช้ภายใน

-**ความมั่นคงปลอดภัย** เกี่ยวข้องกับการปกป้องข้อมูลของผู้ใช้และโปรแกรมจากการถูกรบกวนโดยผู้ใชภายนอกซึ่งไม่มีสิทธิ์ มุ่งที่ผู้ใชภายนอก

12.1.1 เป้าหมายของการป้องกัน

เนื่องจากปัจจุบัน ระบบคอมพิวเตอร์มีความสลับซับซ้อนมากขึ้นและมีแอปพลิเคชันที่หลากหลายเพิ่มขึ้นเป็นจำนวนมาก จึงจำเป็นที่จะต้องปกป้องบูรณภาพ (integrity) หรือความถูกต้องเพิ่มมากขึ้นตามไปด้วย การป้องกันนั้นมีต้นแบบมาจากการทำงานในระบบปฏิบัติการแบบมัลติโปรแกรมมิงที่มีความจำเป็นต้องปกป้องพฤติกรรมที่ไว้วางใจไม่ได้ของผู้ใช้ต่างๆ ที่อาจเสี่ยงต่อความมั่นคงปลอดภัยในการใช้งานร่วมกันของพื้นที่ของชื่อเชิงตรรกะอย่างเช่นสารบบของแฟ้ม หรือพื้นที่ของชื่อเชิงกายภาพอย่างเช่นหน่วยความจำ แนวคิดด้านการป้องกันสมัยใหม่ล้วนได้รับการพัฒนาให้มีขีด

ความสามารถเพิ่มขึ้นในการรับประกันความเชื่อถือได้ในการใช้ทรัพยากรร่วมกันของระบบที่ซับซ้อนมากยิ่งขึ้นในปัจจุบัน

มีเหตุผลหลายประการที่จำเป็นต้องมีการจัดเตรียมการป้องกัน กล่าวคือ เพื่อป้องกันและจำกัดขอบเขตในการเข้าถึงระบบโดยผู้ประสงค์ร้าย และยิ่งไปกว่านั้น เพื่อประกันว่า ทุกส่วนของแต่ละโปรแกรมที่กำลังทำงานอยู่ในระบบจะดำเนินไปในทิศทางที่สอดคล้องต้องกัน โดยระบบจะอนุญาตให้มีการใช้ทรัพยากรเฉพาะที่เป็นไปตามนโยบายที่กำหนดไว้เท่านั้น นี่จึงถือเป็นการรับประกันในความเชื่อถือได้ของระบบอย่างแท้จริง

การป้องกันที่ดีจะมีส่วนช่วยเพิ่มความเชื่อถือได้ของระบบ เพราะสามารถตรวจพบความผิดปกติที่เกิดขึ้นระหว่างส่วนประกอบของระบบย่อยทั้งหลายได้ การตรวจพบความผิดปกติได้ก่อนจะช่วยป้องกันมิให้ระบบเกิดความเสียหายที่มากกว่าเดิม รวมทั้งยังสามารถปกป้องทรัพยากรจากการถูกใช้โดยผู้มีเจตนาร้ายได้ทันทั่วถึง ในระบบที่มีการป้องกันที่ดีจะมีวิธีการที่ชัดเจนแตกต่างกันระหว่างการใช้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต

บทบาทของการป้องกันในระบบคอมพิวเตอร์ก็คือการจัดเตรียมกลไกเพื่อบังคับให้การใช้ทรัพยากรนั้นเป็นไปตามนโยบายที่กำหนด นโยบายดังกล่าวสามารถนำไปใช้ได้หลายวิธี ตั้งแต่การติดตั้งถาวรไว้ตั้งแต่การออกแบบ, การปรับแต่งให้เหมาะสมกับสภาพแวดล้อมในการใช้งาน จนถึงกำหนดให้เจาะจงไว้เฉพาะผู้ใช้แต่ละรายในการปกป้องแฟ้มและโปรแกรมก็ได้ ระบบการป้องกันที่ดีจะต้องมีความยืดหยุ่นในการกำหนดนโยบายให้สอดคล้องกับสภาพการใช้งานในลักษณะต่างๆ ได้

ในบทนี้ จะอธิบายถึงกลไกการป้องกันที่ระบบปฏิบัติการจำเป็นต้องจัดเตรียมไว้เพื่อให้ผู้ออกแบบแอปพลิเคชันสามารถนำไปปรับแต่งให้เหมาะสมที่จะใช้ป้องกันซอฟต์แวร์ที่ออกแบบ

นโยบาย (policy) และกลไก (mechanism) นั้นมีความแตกต่างกัน โดยที่กลไกนั้นเป็นการตัดสินใจว่าจะทำได้อย่างไร ส่วนนโยบายเป็นการตัดสินใจว่าจะทำอะไร ความสำคัญของทั้งนโยบายและกลไกอยู่ที่ความยืดหยุ่น เพราะนโยบายเหมือนกับการเปลี่ยนจากที่หนึ่งไปสู่ที่หนึ่ง หรือจากเวลาหนึ่งไปสู่อีกเวลาหนึ่ง นอกจากนั้น การเปลี่ยนแปลงนโยบายในหลายกรณีจำเป็นต้องมีการปรับเปลี่ยนค่ากำหนดต่างๆ ในตารางหรือพารามิเตอร์บางอย่างของกลไกอีกด้วย

12.1.2 การใช้สารสนเทศร่วมกัน

ในระบบปฏิบัติการมีกลไกการป้องกันการใช้เพื่อปกป้องการแทรกสลับระหว่างกระบวนการต่างๆ วิธีหนึ่งที่ใช้สำหรับหลีกเลี่ยงการไม่เกิดร่วมก็คือการใช้รูปแบบหนึ่งของการป้องกันที่มีเพียงเจ้าของทรัพยากรเท่านั้นจึงมีสิทธิ์ใช้ แต่ผู้อื่นนั้นย่อมไม่มีสิทธิ์ รูปแบบดังกล่าวนี้จำเป็นอย่างยิ่งสำหรับทรัพยากรที่มีเคอร์เนลของระบบปฏิบัติการเป็นเจ้าของ อย่างไรก็ตาม อาจไม่เหมาะสมสำหรับแฟ้มที่ถูกสร้างและเป็นเจ้าของโดยผู้ใช้ทั่วไป เพราะเจ้าของอาจมีความต้องการแบ่งปันข้อมูลและโปรแกรม

บางอย่างแก่ผู้ใช้อื่นๆ บางทีจึงเรียกรูปแบบการแบ่งปันทรัพยากรนี้ว่า การแบ่งปันการควบคุม (controlled sharing)

การแบ่งปันการควบคุมแฟ้มมักจัดการโดยยึดหลัก “รู้เท่าที่จำเป็น (need-to-know)” ซึ่งเจ้าของแฟ้มจะเป็นผู้ตัดสินใจเองว่าจะอนุญาตให้แกใครเข้าถึงอะไรได้บ้างและในระดับใด

ตารางที่ 12.1 ความมั่นคงปลอดภัยและการป้องกัน: นโยบายและกลไก

ความมั่นคงปลอดภัย	นโยบาย	กำหนดว่าใครจะเป็นผู้ใช้ของระบบ ฟังก์ชันนี้กระทำโดยผู้บริหารระบบ
	กลไก	1. เพิ่มหรือลบผู้ใช้ 2. ตรวจสอบว่าคนนี้เป็นผู้ใช้ของระบบหรือไม่
การป้องกัน	นโยบาย	กำหนดว่าผู้ใช้คนใดสามารถเข้าถึงแฟ้มที่กำหนดไว้ได้หรือไม่ ฟังก์ชันนี้กระทำโดยเจ้าของผู้สร้างแฟ้ม
	กลไก	1. ตั้งหรือเปลี่ยนแปลงข้อมูลเกี่ยวกับการป้องกันของแฟ้ม 2. ตรวจสอบว่าแฟ้มนี้สามารถถูกเข้าถึงได้โดยผู้ใช้นี้หรือไม่

ตารางที่ 12.1 อธิบายกลไกและนโยบายของความมั่นคงปลอดภัยและการป้องกัน นโยบายความมั่นคงปลอดภัยจะกำหนดว่าใครสามารถได้รับอนุญาตให้ใช้ได้ในระบบ ส่วนนโยบายการป้องกันจะกำหนดว่า ผู้ใช้คนใดสามารถเข้าถึงแฟ้มอะไรได้บ้าง นโยบายทั้งคู่จะใช้อยู่ด้านนอกของโดเมนระบบปฏิบัติการ โดยผู้บริหารระบบจะเป็นผู้พิจารณาว่าคนใดจะได้รับอนุญาตให้เป็นผู้ใช้ในระบบ ในทำนองเดียวกัน เมื่อมีการสร้างแฟ้มใหม่ขึ้นมา ผู้สร้างจะเป็นตั้งค่าว่าผู้ใช้คนใดควรมีสิทธิ์เข้าถึงแฟ้มนี้ได้บ้าง ส่วนกลไกความมั่นคงปลอดภัยและการป้องกันจะถูกใช้เพื่อทำการตรวจสอบขณะใช้งานเพื่อให้เป็นไปตามนโยบายที่กำหนดไว้

กลไกความมั่นคงปลอดภัยจะเพิ่มผู้ใช้นี้ใหม่เข้าไปหรือตรวจสอบว่าบุคคลผู้นี้เป็นผู้ใช้ของระบบหรือไม่ กลไกต่อมา เรียกว่า การพิสูจน์ตัวจริง ซึ่งจะถูกนำไปใช้ต่อเมื่อบุคคลผู้นั้นต้องการเข้าใช้ระบบ โดยมีกลไกการป้องกันซึ่งตั้งค่าข้อมูลการป้องกันสำหรับแฟ้มหรือใช้ตรวจสอบอีกทอดหนึ่งถ้าผู้นั้นได้รับอนุญาตให้เข้าถึงแฟ้มนั้นได้ กลไกดังกล่าวจะเกี่ยวข้องอีกครั้งหนึ่งเมื่อมีกระบวนการต้องการเข้าใช้แฟ้มบางชนิด หรือเมื่อเจ้าของทำการเปลี่ยนแปลงรายการของผู้ใช้

12.1.3 การพิสูจน์ตัวตนจริง

การพิสูจน์ตัวตนจริง (Authentication) คือ การทวนสอบเอกลักษณ์ของผู้ใช้ การพิสูจน์ตัวตนจริงนี้เป็นกลไกสำคัญของความมั่นคงปลอดภัย โดยที่ระบบปฏิบัติจะใช้เพื่อตัดสินว่าบุคคลผู้นี้เป็นผู้ใช้ที่ได้รับอนุญาตของระบบหรือไม่ อย่างไรก็ตาม การทวนสอบเอกลักษณ์ส่วนบุคคลเชิงกายภาพสำหรับระบบปฏิบัตินั้นมีความยุ่งยากซับซ้อน ระบบปฏิบัติการจึงทำการพิสูจน์ตัวตนได้เพียง “ความรู้” โดยที่ระบบปฏิบัติการจะสร้างอะไรบางอย่างซึ่งมีเฉพาะเจ้าของและระบบปฏิบัตินั้นที่สามารถรู้ได้ ระบบปฏิบัติการจะยอมรับว่าผู้ใช้คนนี้เป็น u_i ก็ต่อเมื่อเขาผู้นั้นสามารถแสดงให้เห็นว่าผู้นั้นรู้จักสิ่งนั้นของ u_i

การพิสูจน์ตัวตนจริงจะกระทำขณะที่ทำการล็อกอินเข้าสู่ระบบ โดยการป้อนรหัสผ่าน (password) ของผู้ใช้ ระบบจะจัดเก็บข้อมูลเกี่ยวกับรหัสผ่านในแฟ้มระบบอยู่ในรูปแบบ

$(user\_id, password\_info)$

ข้อมูลรหัสผ่านทั้งหมดจะถูกป้องกันโดยการเข้ารหัส (encryption) เมื่อผู้ใช้ x ของระบบทำการลงทะเบียนแล้วตั้งหรือเปลี่ยนรหัสผ่านที่เรียกว่า pw_x ก็จะถูกเข้ารหัสเก็บไว้ในแฟ้มรหัสผ่าน คือ $password\_info = E_k(pw_x)$ โดยที่ $E_k(pw_x)$ คือรูปแบบที่ถูกเข้ารหัสของ pw_x เมื่อผู้ใช้ล็อกอิน ก็จะต้องใส่รหัสผ่าน ซึ่งเรียกว่า $presented\_password$ จากนั้น ระบบจะทำการตรวจสอบ

$E_k(presented\_password) = password\_info ?$

และจะยอมรับว่าเป็นผู้ใช้ตัวจริงถ้าการตรวจสอบเสร็จสิ้น

นี่เป็นวิธีง่ายๆ ที่สามารถใช้ควบคุมรหัสผ่านของผู้ใช้แต่ละคนไม่ให้เกิดความสับสนปะปนกัน อย่างไรก็ตาม กรณวิธีในการเข้ารหัสผ่านนั้นอาจมีความเสี่ยงที่จะถูกโจมตีได้ง่ายหากเลือกใช้กรณวิธีในการเข้ารหัสที่แบบสมมาตรหรือกุญแจดอกเดียว (symmetric or single-key scheme) จะมีความมั่นคงปลอดภัยสูงกว่ามากหากเลือกใช้กรณวิธีในการเข้ารหัสแบบอสมมาตรหรือแบบกุญแจสองดอก (asymmetric or two-key scheme)

หลังจากตรวจสอบรหัสผ่านของผู้ใช้ขณะทำการล็อกอินแล้ว รหัสผู้ที่จะถูกเก็บไว้ในแฟ้มข้อมูลของเอร์เนลจนกระทั่งผู้ใช้ออกจากระบบ ในระหว่างการใช้งาน เมื่อกระบวนการของผู้ใช้มีความจำเป็นต้องคำนวณหรือเรียกใช้ทรัพยากร เอร์เนลก็จะใช้รหัสผู้ใช้นั้นเพื่อตัดสินใจว่าจะอนุญาตให้สามารถเข้าถึงทรัพยากรนั้นหรือไม่

ในอนาคต ชีวมาตรหรือไบโอเมตริกซ์ (biometrics) ระบบปฏิบัติจะทำการตรวจสอบตัวตนของผู้ใช้โดยอาศัยไบโอเมตริกซ์ของผู้ใช้ โดยใช้คุณลักษณะเฉพาะเชิงกายภาพของผู้ใช้แต่ละคน

อย่างเช่น ลายนิ้วมือ, ม่านตา, รูปทรงใบหน้า, รูปทรงของมือ, เสียงพูด เป็นต้น ซึ่งจะช่วยกำจัดข้อบกพร่องของการพิสูจน์ตัวตนโดยอาศัยความรู้เหมือนที่ผ่านมา อย่างไรก็ตาม ความแพร่หลายของเทคนิคไบโอเมตริกซ์นั้นขึ้นอยู่กับค่าใช้จ่ายและอุปกรณ์ที่จำเป็นต้องใช้ รวมทั้งความเชื่อถือได้ของระบบการตรวจสอบอีกด้วย

12.2 โครงสร้างการป้องกัน

โครงสร้างการป้องกัน (Protection Structure) ใช้เอกสิทธิ์การเข้าถึง (access privilege) ซึ่งหมายถึงสิทธิ์ในการสร้างรูปแบบที่เจาะจงของการเข้าถึงแฟ้ม ตัวอธิบายการเข้าถึง (access descriptor) ใช้อธิบายเอกสิทธิ์การเข้าถึงแฟ้ม เรามักใช้ตัวย่อเพียง 3 ตัวในการแทนสิทธิ์การเข้าถึงแฟ้มเหล่านั้น ได้แก่ r , w และ x ซึ่งหมายถึงสิทธิ์ในการอ่าน (read), เขียน (write) และกระทำการ (execute) กับข้อมูลหรือโปรแกรมในแฟ้มหนึ่งๆ ตัวอธิบายการเข้าถึงสามารถถูกเข้ารหัสบิต (bit-encoded) สำหรับหน่วยความจำได้อย่างมีประสิทธิภาพ ซึ่งใช้หนึ่งบิตเพื่อแทนการมีหรือไม่มีสิทธิ์ของแต่ละตัวได้

ผู้ใช้นึงคนสามารถมีสิทธิ์ที่จะเข้าถึงได้หนึ่งหรือมากกว่าหนึ่งแฟ้มได้ เช่นเดียวกับแฟ้มหนึ่งๆ ย่อมสามารถเข้าถึงได้โดยผู้ใช้นามากกว่าหนึ่งคน ข้อมูลควบคุมการเข้าถึง (access control information) สำหรับแฟ้มหนึ่ง บางทีเรียกว่า ข้อมูลการเข้าถึง (access information) จะใช้เป็นที่รวบรวมตัวอธิบายสิทธิ์ที่จะเข้าถึงของผู้ใช้ต่างๆ

ข้อมูลเพื่อการป้องกันจะประกอบด้วยเอกสิทธิ์การเข้าถึงของผู้ใช้และข้อมูลควบคุมการเข้าถึงสำหรับแฟ้มต่างๆ จะถูกจัดเก็บอยู่ในเมทริกซ์ที่เรียกว่า เมทริกซ์ควบคุมการเข้าถึง (ACM-access control matrix) หรือบางทีเรียกสั้นๆ เมทริกซ์การเข้าถึง (Access Matrix) ในแนวแถวจะใช้อธิบายเอกสิทธิ์การเข้าถึงของผู้ใช้ต่างๆ แนวคอลัมน์จะใช้อธิบายข้อมูลควบคุมการเข้าถึงของแฟ้มต่างๆ ดังนั้น $ACM(u_i, f_j) = a_{ij}$ ใช้ในความหมายว่า ผู้ใช้ u_i สามารถเข้าถึงแฟ้ม f_j ด้วยเอกสิทธิ์การเข้าถึง a_{ij} ภาพที่ 10.1 แสดงถึง ACM ผู้ใช้ Jay มีสิทธิ์เข้าถึง {อ่าน, เขียน} สำหรับแฟ้ม beta แต่อ่านได้เพียงอย่างเดียวสำหรับแฟ้ม alpha ในรูปแบบของการเข้ารหัสบิต ตัวอธิบายการเข้าถึงสิทธิ์การเข้าถึง {read, write} อาจอยู่ในรูปสายอักขระ 110 โดยที่ 1 ตัวแรกหมายถึงสิทธิ์ในการอ่าน 1 ตัวที่สองหมายถึงสิทธิ์ในการเขียน และ 0 ตัวที่สามหมายถึงไม่มีสิทธิ์ในการกระทำการ

Files →

<i>Users</i> ↓	alpha	beta	gamma
Jay	{r}	{r,w}	
Anita	{r,w,x}		{r}
Sheila			{r}

ข้อดีประการแรกของ ACM ก็คือความง่ายและประสิทธิภาพในการเข้าถึงข้อมูลการป้องกัน ประการต่อมา ACM คือข้อมูลการป้องกันทั้งหมดที่ถูกจัดเก็บไว้ในโครงสร้างข้อมูลเดียวกัน ดังนั้น เมื่อมีการเปลี่ยนแปลงเอกสิทธิ์การเข้าถึงของผู้ใช้หรือของแฟ้มใดๆ ก็ตามก็สามารถทำได้โดยง่าย อย่างไรก็ตาม ข้อจำกัดของ ACM ก็คือ ขนาดและความเบาบาง ACM ต้องการพื้นที่ในหน่วยความจำขนาดใหญ่พอสมควรในระหว่างดำเนินงาน ส่วนความเบาบางเกิดขึ้นจากความจริงที่ว่า ถ้าผู้ใช้คนหนึ่งมีสิทธิ์ในการเข้าถึงเพียงเล็กน้อยกับแฟ้มต่างๆ เป็นจำนวนมาก ดังนั้น ในสายอักขระของ ACM ก็จะบรรจุไปด้วย 0 เป็นจำนวนมาก แต่ตามเกณฑ์ที่กำหนดไว้นั้น จำนวนของข้อมูลควบคุมการเข้าถึงจะต้องน้อยกว่าขนาดของ ACM จึงเป็นประเด็นที่หลีกเลี่ยงไม่ได้ในการออกแบบวิธีการแทนโครงสร้างข้อมูลดังกล่าว

อุปกรณ์ของ ACM แบ่งออกเป็น 2 ส่วน ได้แก่ ขนาดของ ACM จะต้องลดลงโดยการลดจำนวนแถวของเมทริกซ์ เพื่อแก้ปัญหานี้ ยูนิกซ์จะทำการกำหนดเอกสิทธิ์การเข้าถึงไว้เป็นแบบส่วนกลางแทนที่จะเป็นแบบรายผู้ใช้แต่ละคน ผู้ใช้ทั้งหมดแบ่งออกเป็น 3 กลุ่ม ได้แก่

- เจ้าของแฟ้ม
- ผู้ใช้ที่สังกัดอยู่ในกลุ่มเดียวกับเจ้าของ
- ผู้ใช้ทั้งหมดในระบบ

ดังนั้น ในแนวแถวของ ACM จึงใช้เพียง 3 แถว ความเบาบางของ ACM วัดได้จากการใช้รายการในการจัดเก็บข้อมูลการป้องกันมากกว่าแถวหรือคอลัมน์ของเมทริกซ์ ในการเก็บสิทธิ์ที่จะเข้าถึงของผู้ใช้ ถ้าผู้ใช้รายนั้นไม่มีสิทธิ์ก็ใช้เพียงคู่ของ (ผู้ใช้, แฟ้ม) ก็พอ แต่ถ้าใช้แทนข้อมูลการป้องกันก็จะเก็บเป็น 3 ช่อง (ผู้ใช้, แฟ้ม, เอกสิทธิ์การเข้าถึง) แต่รายการดังกล่าวนี้ไม่สามารถค้นหาได้อย่างมีประสิทธิภาพได้ถ้าผู้ใช้ต้องการค้นหาแบบเจาะจงสิทธิ์การเข้าถึงของแฟ้มใดแฟ้มหนึ่งโดยเฉพาะ ดังนั้น จึงมีการจัดการรายการเพื่อให้มีประสิทธิภาพในการค้นหา ดังนี้

1. รายการควบคุมการเข้าถึง หรือ ACL (access control lists)
2. รายการให้อำนาจ หรือ C-list (capability lists)

ACL จะถูกเก็บไว้ในแถวเดียวกันกับคอลัมน์ของ ACM จึงบรรจุไว้ด้วยข้อมูลควบคุมการเข้าถึงสำหรับแฟ้มหนึ่งๆ ในระบบ เมื่อผู้ใช้พยายามใช้แฟ้ม ACL ของแฟ้มนั้นก็จะถูกค้นหา ส่วน C-list จะถูกเก็บไว้ในแถวเดียวกันกับ ACM ซึ่งใช้อธิบายเอกสิทธิ์การเข้าถึงของผู้ใช้หรือกลุ่มผู้ใช้ เวลาที่ผู้ใช้ต้องการใช้แฟ้ม C-list ก็จะถูกค้นหา

ACL ถูกนำไปใช้อย่างแพร่หลายในระบบปฏิบัติการสำหรับการป้องกัน แต่ C-list ยังสามารถถูกนำไปใช้ป้องกันทรัพยากรอย่างเช่นโปรแกรม หรืออ็อปเจกต์ข้อมูลในหน่วยความจำ

12.2.1 รายการควบคุมการเข้าถึง หรือ ACL

ACL (access control lists) ของแฟ้มต่างๆ จะถูกจัดเก็บไว้ที่สารบบของแฟ้มนั้น ซึ่งจะปรากฏแตกต่างกันสำหรับผู้ใช้งานแต่ละคนในการเข้าถึงแฟ้ม เมื่อใดก็ตามที่กระบวนการต้องการเปิดแฟ้ม ระบบปฏิบัติการจะค้นหารหัสของผู้ใช้ที่สร้างกระบวนการนั้นขึ้นมา และตรวจสอบสิทธิ์ในการเข้าถึง เมื่อได้รับอนุญาตจึงทำการเปิดโหมดที่เหมาะสมในการใช้งาน ถ้าไม่อนุญาตกระบวนการนั้นก็จะถูกยกเลิกไป

เมื่อผู้ใช้ Anita สร้างแฟ้มชื่อ alpha ขึ้นมา เธอจะลงทะเบียนข้อมูลควบคุมการเข้าถึงสำหรับแฟ้ม alpha กับระบบ ซึ่งข้อมูลจะอยู่ในรูปแบบดังนี้

{(รหัสผู้ใช้, เอกสิทธิ์การเข้าถึง), ... },

ประกอบกันเข้าเป็น ACL สำหรับแฟ้ม alpha ตัวอย่างในภาพที่ 13.2 แสดงถึงรายการควบคุมการเข้าถึงของ alpha {(Jay,{read}), (Anita, {read, write, execute})}, ซึ่งปรากฏว่า Jay สามารถอ่านแฟ้ม alpha ได้อย่างเดียว ในขณะที่ Anita สามารถอ่าน, เขียน และกระทำการแฟ้มนี้ได้ ส่วน Sheila ไม่มีสิทธิ์ใดๆ เลยที่จะเข้าถึงแฟ้ม alpha ระบบแฟ้มส่วนใหญ่เจ้าของจะได้รับเอกสิทธิ์การเข้าถึงได้โดยปริยาย

File name	Location info	Protection info	Flags
alpha		{(Jay, {r}), (Anita, {r,w,x})}	
beta		{(Jay, {r,w})}	
gamma		{(Anita, {r}),(Sheila, {r})}	

ขั้นตอนที่เกี่ยวข้องในการเข้าถึงแฟ้ม gamma โดยผู้ใช้ชื่อ Sheila เป็นดังนี้

1. Sheila ทำการล็อกอิน
2. ระบบจะทำการพิสูจน์ตัวจริงของ Sheila โดยถามรหัสผ่านของเธอ
3. กระบวนการจะถูกเริ่มต้นโดย Sheila ทำการเรียกการเปิดแฟ้ม (gamma, ...) เพื่อแก้ไข

4. ระบบปฏิบัติการจะทำการตรวจสอบ ถ้า ACL ของแฟ้ม gamma บรรจุไว้ด้วยเอกสิทธิ์การเข้าถึงแบบ “เขียน” ก็จะอนุญาตเธอ

ในขั้นตอนที่ 2 นั้น ถ้าระบบพิสูจน์ว่าไม่ใช่ตัวจริงของ Sheila ก็จะปฏิเสธการเข้าถึงระบบ การใช้รายการควบคุมการเข้าถึงนั้นอาจประสบกับปัญหาในทางปฏิบัติบางประการ ถ้าผู้ใช้ในระบบมีจำนวนมาก ก็จะทำให้ขนาดของ ACL พลุ่ยใหญ่ไปด้วย และจะมีค่าใช้จ่ายด้านพื้นที่ขนาดใหญ่ในระบบ เวลาที่ ACL ทำการค้นหาเพื่อตรวจสอบการเข้าถึงแฟ้มต่างๆ ก็จะใช้เวลานานไปด้วย เพื่อแก้ปัญหาเรื่องหน่วยความจำและเวลาของซีพียู เราสามารถใช้การกำหนดข้อมูลควบคุมการเข้าถึงเป็นกลุ่มของผู้ใช้แทนที่จะใช้เป็นผู้ใช้แต่ละคน

12.2.2 รายการให้อำนาจ หรือ C-list

การให้อำนาจจะใช้แทนเอกสิทธิ์การเข้าถึงของผู้ใช้สำหรับแฟ้มหนึ่งๆ ข้อมูลที่เกี่ยวข้องกับการให้อำนาจของผู้ใช้จะถูกจัดเก็บไว้ในรายการให้อำนาจ (capability list หรือ C-list) ซึ่งอยู่ในรูปแบบ

{(รหัสแฟ้ม, เอกสิทธิ์การเข้าถึง), ...}

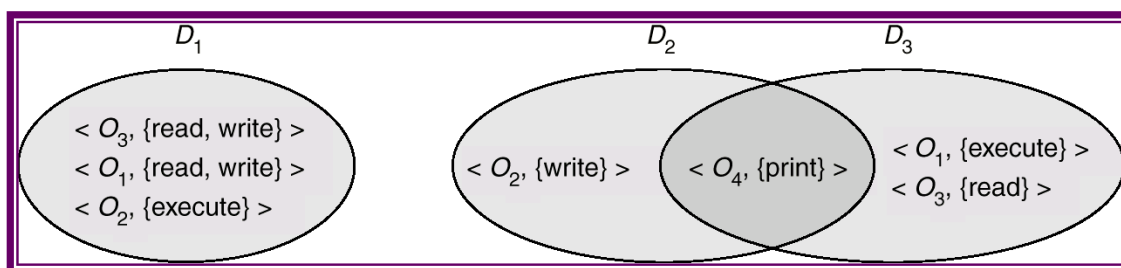
แสดง C-list สำหรับ Anita {(alpha, {read, write, execute}), (gamma, {read})} Anita สามารถอ่าน, เขียน และกระทำการแฟ้ม alpha ได้ และสามารถอ่านแฟ้ม gamma ได้ แต่เธอไม่สามารถเข้าถึงแฟ้ม info ได้เพราะไม่มีรายการ info อยู่ใน C-list เมื่อ Anita ต้องการเข้าถึงบางแฟ้ม ระบบปฏิบัติการก็จะยินยอมให้เธอเข้าถึงได้เท่าที่สิทธิ์ซึ่งปรากฏอยู่รายการเท่านั้น เช่นเดียวกับกรณีของ ACL ผู้ใช้ที่ปลอมตัวจะไม่สามารถผ่านการพิสูจน์ตัวจริงได้ในขณะล็อกอินเข้าสู่ระบบ และรหัสของผู้ใช้จะถูกเก็บไว้ใน C-list ที่ถูกต้อง C-list มักมีขนาดเล็ก ซึ่งทำให้ลดเวลาและค่าใช้จ่ายในการใช้งานเพื่อควบคุมการเข้าถึงแฟ้มในระบบ

(alpha, {r,w,x})
(gamma, {r})

12.3 โดเมนของการป้องกัน

ระบบคอมพิวเตอร์นั้นคือหน่วยรวมของกระบวนการและอ็อบเจกต์ต่างๆ โดยที่อ็อบเจกต์มีความหมายรวมทั้งฮาร์ดแวร์อ็อบเจกต์ (เช่น ซีพียู, ส่วนของหน่วยความจำ, เครื่องพิมพ์, ดิสก์ และหน่วยขับแถบบันทึก) และซอฟต์แวร์อ็อบเจกต์ (เช่น แฟ้ม, โปรแกรม และเซมาฟอร์) แต่ละอ็อบเจกต์จะมีชื่อที่ใช้เรียกแตกต่างกัน ซึ่งสามารถเข้าถึงได้โดยดำเนินการไปตามข้อกำหนดที่วางไว้อย่างชัดเจน โดยกำหนดขอบเขตหรือโดเมนของการป้องกัน (domain of protection) ไว้ โดยทั่วไป อ็อบเจกต์จะมีแบบชนิดข้อมูลนามธรรม (abstract data type)

การใช้งานอ็อบเจกต์แต่ละชนิดก็ขึ้นอยู่กับประเภทของอ็อบเจกต์นั้นๆ เช่น ซีพียูก็สามารถกระทำการได้เพียงอย่างเดียว ส่วนของหน่วยความจำสามารถอ่านและเขียนได้ ในขณะที่ซีดี-รอมและดีวีดี-รอม สามารถอ่านได้ หน่วยขับแถบบันทึกสามารถเขียนและหมุนซ้ำ แฟ้มข้อมูลสามารถเปิด, อ่าน, เขียน, ปิด และลบ ส่วนแฟ้มโปรแกรม สามารถอ่าน, เขียน, กระทำการ และลบได้ ดัง รูป 12.1



รูป 12.1 ระบบที่ประกอบด้วย 3 โดเมนการป้องกัน

ที่มา (Silberschatz et. al., 2003, p. 631)

กระบวนการควรได้รับอนุญาตให้เข้าถึงทรัพยากรเหล่านั้นเท่าที่ตนเองมีสิทธิ์ นอกจากนั้นในเวลาหนึ่งๆ กระบวนการควรได้รับอนุญาตให้เรียกใช้ทรัพยากรเฉพาะที่จำเป็นต้องภารกิจขณะนั้นเสร็จเท่านั้น ไม่ควรให้ถือเพื่อไว้ นี่ยังคงเข้ากันได้กับหลักการที่เรียกว่า “รู้เท่าที่จำเป็น” ซึ่งมีส่วนช่วยจำกัดขอบเขตความเสียหายที่อาจเกิดขึ้นจนเป็นเหตุให้ระบบล้มเหลวได้

12.3.1 โครงสร้างโดเมน (Domain Structure)

วิธีการนี้จะอำนวยความสะดวกให้กระบวนการหนึ่งๆ ทำงานได้ภายใต้ **โดเมนการป้องกัน (protection domain)** ซึ่งจะระบุถึงทรัพยากรต่างๆ ที่กระบวนการนั้นจะสามารถเรียกใช้ได้ ในแต่ละโดเมนจะกำหนดกลุ่มของอ็อบเจกต์และประเภทของการปฏิบัติการที่สามารถเรียกใช้ได้ภายใต้อ็อบเจกต์เหล่านั้น ความสามารถที่จะกระทำการกับอ็อบเจกต์นั้นเรียกว่า **สิทธิ์ที่จะเข้าถึง (access**

right) โดเมน (domain) คือหน่วยรวมของสิทธิที่จะเข้าถึง ซึ่งมีการระบุไว้เป็นคู่ๆ <ชื่อ-อ็อบเจกต์, สิทธิที่จะเข้าถึง> ตัวอย่างเช่น ถ้าโดเมน D มีสิทธิที่จะเข้าถึง <file F , {read,write}> กระบวนการที่กระทำการบนโดเมน D จะสามารถทำได้เพียง อ่านและเขียนแฟ้ม F เท่านั้น ไม่สามารถกระทำการอื่นใดได้อีกบนอ็อบเจกต์นี้

เราสามารถแบ่งปันสิทธิที่จะเข้าถึงระหว่างโดเมนกันได้ถ้ายังไม่ต้องการร่วมเข้าเป็นโดเมนเดียวกัน ตัวอย่างดังภาพที่ 10.4 เรามี 3 โดเมน ได้แก่ D_1 , D_2 และ D_3 สิทธิที่จะเข้าถึงของ < O_4 , {print}> ซึ่งใช้ร่วมกันได้ทั้ง D_2 และ D_3 แสดงว่ากระบวนการในโดเมนทั้งคู่สามารถ พิมพ์อ็อบเจกต์ O_4 ได้ ส่วนกระบวนการที่กระทำการอยู่ในโดเมน D_1 นั้นสามารถอ่านและเขียนอ็อบเจกต์ O_1 ได้ หรืออีกนัยหนึ่ง มีเพียงกระบวนการที่อยู่ในโดเมน D_3 เท่านั้นที่อาจกระทำการอ็อบเจกต์ O_1 ได้

การเชื่อมโยงเข้าด้วยกันระหว่างกระบวนการกับโดเมนอาจกระทำแบบตายตัวก็ได้ถ้ากลุ่มของทรัพยากรนั้นมีไว้ใช้งานได้ตลอดเวลาสำหรับกระบวนการนั้น หรือแบบพลวัตก็ได้ แต่การใช้โดเมนการป้องกันแบบพลวัตย่อมมีความซับซ้อนและใช้ประโยชน์ได้ดีกว่าแบบตายตัว

ถ้ามีการเชื่อมโยงระหว่างกระบวนการเข้ากับโดเมนเป็นแบบตายตัว และเราต้องการยึดติดกับหลักการ “รู้เท่าที่จำเป็น” กลไกนั้นจะต้องมีสภาพพร้อมที่จะเปลี่ยนแปลงเนื้อหาของโดเมนนั้น โดยกระบวนการอาจจำเป็นต้องกระทำการถึง 2 ขั้นตอน เช่น อาจต้องการสิทธิที่จะอ่านขั้นตอนหนึ่ง และสิทธิที่จะเขียนอีกขั้นตอนหนึ่ง ถ้าโดเมนเป็นแบบคงที่ เราจะต้องนิยามโดเมนไว้ทั้งการอ่านและเขียน แต่ถ้าเราจะอนุญาตให้มีการแก้ไขเนื้อหาของโดเมนได้ ก็อาจกระทบต่อหลักการของการกำหนดสิทธิที่จะเข้าถึงแบบน้อยที่สุดได้

ถ้ามีการเชื่อมโยงแบบพลวัต กลไกดังกล่าวจะต้องอนุญาตให้กระบวนการสามารถสลับไปมาระหว่างโดเมนหนึ่งสู่โดเมนหนึ่งได้ ซึ่งอาจต้องยินยอมให้เนื้อหาของโดเมนถูกเปลี่ยนแปลงได้

โดเมนสามารถมีคุณลักษณะหลายประการ

1. ผู้ใช้แต่ละคนอาจเป็นหนึ่งโดเมน ในกรณีนี้ กลุ่มของอ็อบเจกต์ที่สามารถเข้าถึงได้จะขึ้นอยู่กับเอกลักษณ์ของผู้ใช้ การสลับโดเมนจะเกิดขึ้นเมื่อมีการเปลี่ยนแปลงผู้ใช้ โดยปกติเกิดขึ้นเมื่อมีการลงบันทึกออก (logout) และมีผู้ใช้คนใหม่บันทึกเข้า (login) มา
2. แต่ละกระบวนการอาจเป็นหนึ่งโดเมน ในกรณีนี้ กลุ่มของอ็อบเจกต์ที่สามารถเข้าถึงได้จะขึ้นอยู่กับเอกลักษณ์ของกระบวนการ การสลับโดเมนจะเกิดขึ้นเมื่อกระบวนการหนึ่งส่งข่าวสารไปยังอีกกระบวนการหนึ่ง และเมื่อมีการรอคอยการตอบรับ
3. แต่ละกระบวนการคำสั่งอาจเป็นหนึ่งโดเมน ในกรณีนี้กลุ่มของอ็อบเจกต์ที่จะสามารถเข้าถึงได้จะต้องสอดคล้องกับตัวแปรเฉพาะที่ที่ได้นิยามไว้ภายในกระบวนการคำสั่งนั้น การสลับโดเมนจะเกิดขึ้นเมื่อมีการเรียกกระบวนการคำสั่ง

พิจารณาจากโหมดคู่กันมาตรฐาน (dual mode; โหมดมอนิเตอร์-ผู้ใช้) ซึ่งเป็นแบบจำลองของการกระทำของระบบปฏิบัติการ เมื่อกระบวนการกระทำในโหมดมอนิเตอร์ อาจกระทำการคำสั่งเอกสิทธิ์ (privilege instruction) และได้รับสิทธิ์โดยสมบูรณ์ในการควบคุมระบบคอมพิวเตอร์ อีกนัยหนึ่ง ถ้ากระบวนการกระทำในโหมดผู้ใช้ ก็จะสามารถเรียกใช้ได้เฉพาะคำสั่งแบบไม่มีเอกสิทธิ์เท่านั้น ซึ่งสามารถทำงานอยู่ภายในส่วนหน่วยความจำที่ได้ถูกกำหนดไว้ล่วงหน้าแล้วเท่านั้น สองโหมดเหล่านี้จะช่วยปกป้องระบบปฏิบัติการ (การทำงานในโหมดมอนิเตอร์) จากการแทรกสลับของกระบวนการผู้ใช้ (การทำงานในโดเมนผู้ใช้) อย่างไรก็ตาม ในระบบปฏิบัติการแบบมัลติโปรแกรมมิง โหมดคู่กันดังกล่าวยังไม่เพียงพอ เพราะว่าผู้ใช้ก็ต้องการป้องกันการแทรกสลับจากผู้ใช้คนอื่น ๆ ด้วย

12.3.2 ยูนิกซ์

กระบวนการของยูนิกซ์มีสถานะกำลังดำเนินงาน (running state) อยู่ 2 สถานะ ได้แก่ ผู้ใช้และเคอร์เนล ในขณะที่อยู่ในสถานะกำลังดำเนินงานของผู้ใช้ กระบวนการจะเข้าถึงพื้นที่หน่วยความจำของตนเอง, แฟ้มต่างๆ ในระบบตามที่รหัสผู้ใช้ของตนได้รับสิทธิ์ให้เข้าถึง และทรัพยากรอื่นๆ ที่ได้รับการจัดสรร กระบวนการสามารถเข้าถึงโครงสร้างข้อมูลของเคอร์เนลและเนื้อหาทั้งหมดของหน่วยความจำได้โดยการเปลี่ยนจากสถานะผู้ใช้เป็นสถานะกำลังดำเนินงานของเคอร์เนลผ่าน system call เมื่อกระบวนการกลับคืนจาก system call สู่สถานะของผู้ใช้ ก็จะได้รับสิทธิ์เท่าเดิมก่อนที่จะเข้าสู่ system call

คุณลักษณะของ suuid ของยูนิกซ์อีกวิธีการหนึ่งคือการเปลี่ยนโดเมนการป้องกันแบบพลวัต การเข้าถึงเอกสิทธิ์ของกระบวนการจะถูกตัดสินโดย uid ของกระบวนการนั้น เมื่อเคอร์เนลสร้างกระบวนการขึ้นมาจากกระบวนการหนึ่ง ก็จะตั้ง uid ของกระบวนการนั้นไปยัง id ของผู้ใช้ที่สร้างกระบวนการนั้นขึ้นมา โดยอาศัยคุณลักษณะของ setuid จะใช้ในการเปลี่ยนแปลง uid ของกระบวนการแบบชั่วคราว setuid สามารถถูกใช้งานผ่าน system call โดยกระบวนการ หรือถูกใช้เมื่อกระบวนการทำการ exec เพื่อทำการโปรแกรมก็ได้ จากนั้น กระบวนการจะใช้ setuid ผ่าน system call กับ id ของตนเองเพื่อย้อนกลับไปเป็น uid เดิมของตน

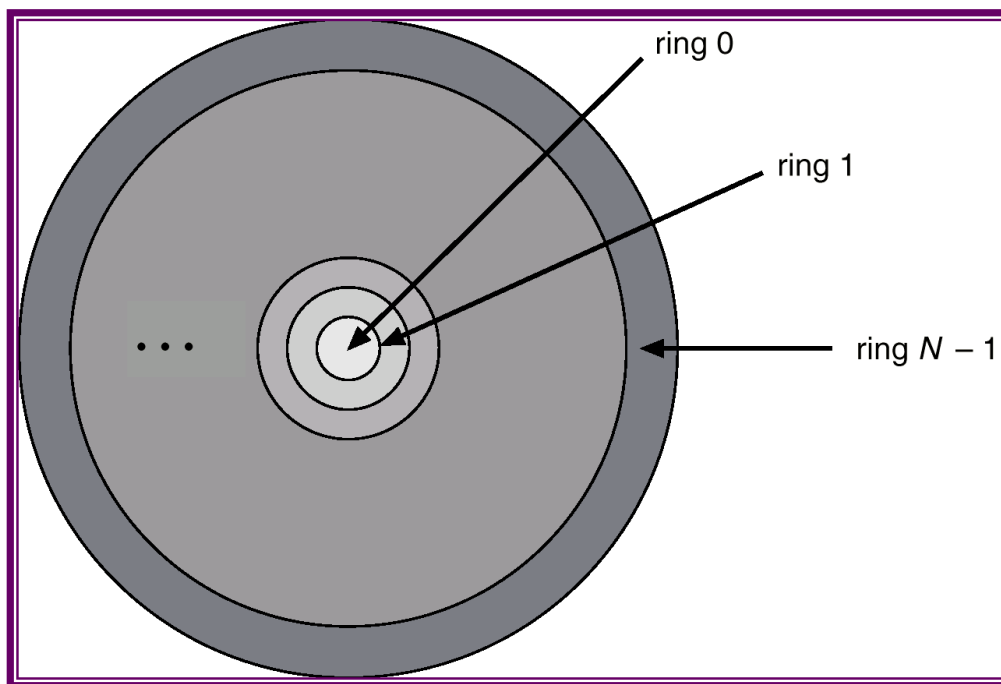
โปรแกรมที่ถูกกระทำโดยการเรียกคุณลักษณะของ setuid จะทำการตั้ง setuid bit ไว้ในรายการสารบบของตนเอง เมื่อโปรแกรมกระทำเสร็จเรียบร้อยแล้ว เคอร์เนลก็จะเปลี่ยน uid ของกระบวนการที่ทำการโปรแกรมชั่วคราวนั้นกลับไปยังโปรแกรมเดิมของตน วิธีการนี้เป็นการใส่กระบวนการลงในโดเมนการป้องกันได้อย่างมีประสิทธิภาพ เพื่อให้กระบวนการของผู้ใช้สามารถใช้อิทธิพลชั่วคราวของเคอร์เนลเพื่อจะทำการบางอย่างในฐานะสิทธิ์ของเคอร์เนลได้ โดยไม่สามารถละเมิดการป้องกันของระบบได้

12.3.3 มัลทิกซ์ (MULTICS)

มัลทิกซ์มีโดเมนการป้องกันแบบ 64 ชั้นโดยจัดการโครงสร้างในลักษณะของวงแหวน วงแหวนแต่ละวงมีหมายเลขกำกับอยู่เริ่มจากวงในสุดออกไปยังวงนอกสุด แบ่งโดเมนการป้องกันออกเป็นลำดับชั้น ดังภาพที่ 13.5 โดยวงในสุดจะมีเอกสิทธิ์การเข้าถึงครอบคลุมวงนอกทั้งหมด และลดหลั่นลงมาเรื่อยๆ แต่ละกระบวนการคำสั่งของโปรแกรมจะถูกกำหนดโดเมนการป้องกันไว้ และสามารถกระทำการได้เฉพาะกระบวนการที่อยู่ในโดเมนวงเดียวกันเท่านั้น ส่วนประกอบของรหัสของกระบวนการหนึ่งอาจประกอบด้วยกระบวนการคำสั่งในโดเมนการป้องกันที่แตกต่างกัน

การขัดจังหวะจะเกิดขึ้นเมื่อกระบวนการกำลังทำการอยู่ในโดเมนการป้องกัน D_i ทำการเรียกกระบวนการคำสั่งที่ถูกกำหนดไปยังโดเมนการป้องกัน D_j โดยที่ $D_j \neq D_i$ ในการกระทำการกระบวนการคำสั่ง โดเมนการป้องกันควรจะเปลี่ยนไปเป็น D_j โดยเคอร์เนลจะทำการตรวจสอบว่ากระบวนการนั้นดำเนินไปตามกฎสำหรับการเปลี่ยนโดเมนการป้องกันหรือไม่ กล่าวคือ การเปลี่ยนโดเมนการป้องกันจะได้รับอนุญาตถ้ากระบวนการที่กำลังดำเนินงานอยู่ในโดเมน D_i แล้วทำการเรียกกระบวนการคำสั่งซึ่งอยู่ในโดเมนที่สูงกว่า แต่ถ้ากระบวนการต้องการเข้าสู่โดเมนที่ต่ำกว่าจะต้องเรียกกระบวนการคำสั่งเฉพาะพิเศษซึ่งเรียกว่า gate ถ้ามีความพยายามในการเรียกกระบวนการคำสั่งใดๆ ที่อยู่ในชั้นต่ำกว่าโดยไม่ผ่าน gate การเรียกนั้นจะล้มเหลวและถูกยกเลิกไป ถ้ามีการเรียกที่ถูกต้องเหมาะสมตามกฎ โดเมนการป้องกันของกระบวนการนั้นก็จะได้รับให้มีการเปลี่ยนอย่างชั่วคราวไปยังโดเมนที่เหมาะสมเพื่อให้สามารถกระทำการภายในโดเมนการป้องกันและเข้าทรัพยากรตามที่ได้รับเอกสิทธิ์ หลังจากนั้นโดเมนการป้องกันของกระบวนการนั้นก็จะคืนค่ากลับไปยังค่าเดิมของ D_i

อย่างไรก็ตาม โครงสร้างการป้องกันของมัลทิกซ์นั้นมีความซับซ้อนมากและมีค่าใช้จ่ายสูงในการเปลี่ยนสถานะและการตรวจสอบในขณะที่ทำการเรียกกระบวนการคำสั่ง และโดยธรรมชาติของโครงสร้างแบบลำดับชั้นนั้นเป็นการบังคับให้โดเมนของวงต่ำจะต้องเก็บเอกสิทธิ์การเข้าถึงของโดเมนการป้องกันที่สูงกว่าไว้ทั้งหมด นอกจากนั้น โครงสร้างเช่นนี้จึงไม่อนุญาตให้มีการรวมเอกสิทธิ์การเข้าถึงของต่างโดเมนอีกด้วย ซึ่งทำให้ผู้ใช้ขาดอิสระที่จะกำหนดเกี่ยวกับการป้องกัน



รูป 12.2 โครงสร้างวงแหวนของมัลติทิกซ์

ที่มา (D M Dhamdhere, 2020, p.234)

12.3.4 การให้อำนาจ

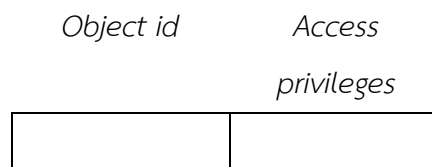
แนวคิดเกี่ยวกับการให้อำนาจ (Capability) ถูกนำเสนอให้เป็นกลไกสำหรับการแบ่งปันและการป้องกัน โดยดัดแปลง C-list ให้เหมาะสมเพื่อเป็นกลไกทั่วไปสำหรับการป้องกันแพ้ม

การให้อำนาจ คือการใช้โทเค็นแทนเอกสิทธิ์การเข้าถึงสำหรับอ็อบเจกต์ การให้อำนาจจะบรรจุไว้ด้วยรหัสของอ็อบเจกต์และรายการของตัวอธิบายการเข้าถึงอ็อบเจกต์นั้น ซึ่งอ็อบเจกต์นั้นอาจเป็นได้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในระบบ กระบวนการจะเป็นเจ้าของการให้อำนาจ และอนุญาตให้กระบวนการเข้าถึงอ็อบเจกต์ได้ตามที่ระบุไว้อย่างชัดเจนในเอกสิทธิ์การเข้าถึง

การป้องกันสามารถนำไปใช้ได้ดังต่อไปนี้ กระบวนการเป็นเจ้าของการให้อำนาจสำหรับอ็อบเจกต์หนึ่งๆ ถ้ากระบวนการเป็นเจ้าของอ็อบเจกต์ใดๆ ก็จะได้รับสิทธิ์จากระบบปฏิบัติการที่จะมีอำนาจเข้าถึงอ็อบเจกต์นั้นๆ ตามที่กำหนดไว้เมื่อมีการสร้างอ็อบเจกต์ขึ้นมา กระบวนการหนึ่งสามารถส่งผ่านอำนาจไปยังอีกกระบวนการหนึ่งได้ ดังนั้น อำนาจทั้งหมดใน C-list จะสามารถถูกเรียกใช้ได้ด้วยวิธีที่ถูกต้องเท่านั้น ไม่สามารถลักลอบหรือแอบสร้างกระบวนการขึ้นมาอย่างลับๆ ได้

กระบวนการสามารถเข้าถึงอ็อบเจกต์ได้ก็ต่อเมื่อกระบวนการนั้นเป็นเจ้าของอำนาจของอ็อบเจกต์นั้น วิธีการเช่นนี้แตกต่างไปจากการป้องกันผ่าน ACL โดยการให้รหัสของผู้ที่สร้างกระบวนการนั้นขึ้นมาเป็นผู้เล่นบทบาทหลักในการใช้การป้องกัน เมื่อมีการใช้ C-list ในการป้องกันการแบ่งปันอ็อบเจกต์จะเกิดขึ้นได้ดังนี้ กระบวนการที่สร้างอ็อบเจกต์จะได้รับอำนาจที่บรรจุไว้ด้วยเอกสิทธิ์การเข้าถึงทุกอย่างที่สามารถเป็นไปได้ ผู้สร้างกระบวนการยังสามารถใช้อำนาจนี้ไปสร้างการให้อำนาจแบบกลุ่มย่อย (subset capability) ขึ้นมาสำหรับอ็อบเจกต์ที่ไม่มีเอกสิทธิ์บางอย่างได้ แล้วส่งผ่านไปยังกระบวนการอื่นเพื่อให้ใช้งาน

รูปแบบของการให้อำนาจ เป็นไปตามภาพที่ 13.6 การให้อำนาจประกอบไปด้วย 2 ส่วน ได้แก่รหัสอ็อบเจกต์ (object id) และเอกสิทธิ์การเข้าถึง (access privilege) แต่ละอ็อบเจกต์จะมีรหัสที่ไม่ซ้ำกันเลยในระบบ ส่วนเอกสิทธิ์การเข้าถึงจะบรรจุไว้ด้วยบิตที่ถูกเข้ารหัสของตัวอธิบายการเข้าถึง ดังนั้น แต่ละบิตในเอกสิทธิ์การเข้าถึงจึงใช้แทนการมีหรือไม่มีสิทธิ์ตามที่ระบุไว้



เราจะใช้สัญลักษณ์ $Cap_k(obj_i)$ ในความหมายว่า การให้อำนาจสำหรับอ็อบเจกต์ obj_i ตรีชนีล่าง ($_k$) ของ Cap จะใช้แสดงความแตกต่างระหว่างอ็อบเจกต์ ไม่ได้มีนัยสำคัญ เพื่อความง่าย ตัวอย่างต่อไปนี้จะไม่ใช้ตรีชนีล่างสำหรับการให้อำนาจเดี่ยวๆ ของอ็อบเจกต์

ตัวอย่างต่อไปนี้ สมมติว่า การให้อำนาจต่อไปนี้แก่แฟ้ม alpha ในระบบ

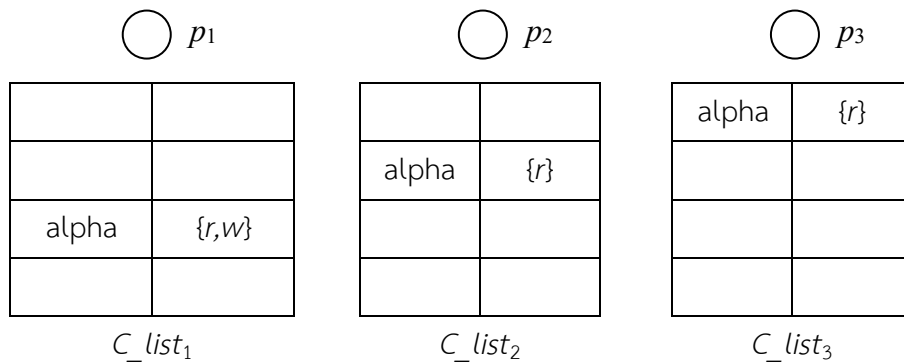
1. กระบวนการ p_3 ถือครอง $Cap_1(\alpha)$
2. กระบวนการ p_1 ถือครอง $Cap_2(\alpha)$ และ
3. กระบวนการ p_2 ถือครอง $Cap_4(\alpha)$

$Cap_1(\alpha)$ กับ $Cap_4(\alpha)$ มีเอกสิทธิ์การเข้าถึงอย่างเดียวกัน (อ่าน) บนกระบวนการ p_3 และ p_2 ในขณะที่ $Cap_2(\alpha)$ มีเอกสิทธิ์การเข้าถึง (อ่านและเขียน) บนกระบวนการ p_1

12.3.4.1 ระบบคอมพิวเตอร์แบบการให้อำนาจ (Capability-Based Computer System)

ระบบคอมพิวเตอร์แบบการให้อำนาจหมายถึงระบบที่มีสถาปัตยกรรมที่ใช้การให้อำนาจในการกำหนดเลขที่อยู่ (addressing) และการป้องกันสำหรับอ็อบเจกต์ทั้งหมดในระบบ อ็อบเจกต์อาจ

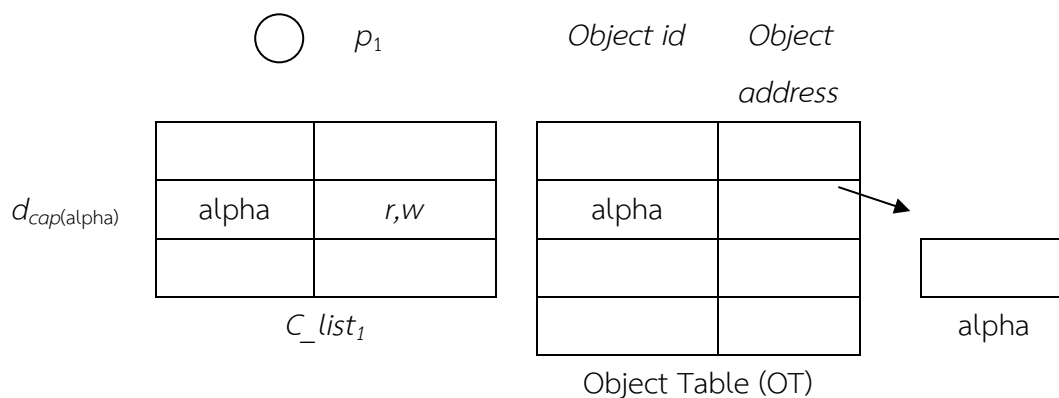
มีชีวิตยาวอย่างเช่น แฟ้ม หรือมีชีวิตสั้นอย่างเช่นโครงสร้างข้อมูลและสำเนาของโปรแกรมในหน่วยความจำ ปัจจุบัน มีการนำสถาปัตยกรรมแบบการให้อำนาจไปใช้ทั้งนารทดลองและเชิงพาณิชย์ อินเทล iapx-432 ถือเป็นตัวอย่างเป็นที่ชัดเจนสำหรับผลิตภัณฑ์หน่วยประมวลผลที่ใช้สถาปัตยกรรมแบบการให้อำนาจ



แสดงถึงระบบที่ใช้การให้อำนาจ แต่ละกระบวนการใน C-list จะอธิบายเอกลักษณ์การเข้าถึง ดังนั้น กระบวนการ p_1 , p_2 และ p_3 ถือครองอำนาจของ alpha ตามตัวอย่างข้างบน กระบวนการสามารถเข้าถึงอ็อปเจกต์ได้ตามอำนาจที่ตนเองถือครองอยู่ ระบบคอมพิวเตอร์ที่ใช้การให้อำนาจจะแตกต่างจากระบบคอมพิวเตอร์ดั้งเดิมดังต่อไปนี้

1. ระบบจะไม่เชื่อมโยงหน่วยความจำเข้ากับกระบวนการอย่างชัดเจน เพียงแต่เชื่อมโยง C-list กับกระบวนการต่างๆ เท่านั้น
2. การให้อำนาจใน C-list อาจถูกใช้เพื่อเข้าถึงอ็อปเจกต์ใดๆ ก็ได้ในระบบ (ในหน่วยความจำหรือดิสก์) สถานที่อยู่ของอ็อปเจกต์ล้วนไม่สำคัญสำหรับกระบวนการ
3. อ็อปเจกต์แบบอายุยาวอย่างเช่นแฟ้ม และอายุสั้นอย่างข้อมูลและโปรแกรมในหน่วยความจำสามารถเข้าถึงได้ในรูปแบบเดียวกัน

ข้อแตกต่างเหล่านี้เกิดขึ้นจากวิธีในการเข้าถึงอ็อปเจกต์ในระบบคอมพิวเตอร์แบบการให้อำนาจ



12.3.4.2 การกำหนดเลขที่อยู่แบบการให้อำนาจ (Capability-based addressing)

ภาพที่ 13.8 แสดงวิธีการของการกำหนดเลขที่อยู่แบบให้อำนาจของอ็อบเจกต์ ตารางอ็อบเจกต์ (OT-object table) เป็นตารางบรรจุข้อมูลที่อยู่ของอ็อบเจกต์ทั้งหมดในระบบ เลขที่อยู่อ็อบเจกต์ (object address) จะเก็บรายการตารางอ็อบเจกต์ซึ่งแสดงเลขที่อยู่ของอ็อบเจกต์ในหน่วยความจำหลักหรือรองของคอมพิวเตอร์ การเข้าถึงอ็อบเจกต์สามารถทำได้โดยกระบวนการ p_1 เรียกคำสั่งปฏิบัติการ $\langle opn \rangle$ บนอ็อบเจกต์โดยใช้รูปแบบคำสั่งดังนี้

$$\langle opn \rangle \quad d_{cap}$$

โดยที่ d_{cap} จะแทนที่ C-list ของ p_1 ระบบจะทำการแทนที่นี้ในการเก็บการให้อำนาจใน C-list ของ p_1 ในที่นี้คือ $Cap(\alpha)$ รหัสอ็อบเจกต์ในรายการอำนาจ α จะใช้เก็บที่อยู่รายการของ α ใน OT เลขที่อยู่ของอ็อบเจกต์ในรายการ OT จะถูกใช้คำสั่งปฏิบัติการ $\langle opn \rangle$ บน α จะมีการใช้เทคนิคพิเศษในการแปลงเลขที่อยู่ในบัพเฟอร์ (เรจิสเตอร์และหน่วยความจำแคช) เพื่อให้การเข้าถึงเป็นไปอย่างมีประสิทธิภาพ

การกำหนดเลขที่อยู่แบบให้อำนาจช่วยให้มีความยืดหยุ่นแก่ระบบปฏิบัติการ ระบบปฏิบัติการสามารถเปลี่ยนแปลงที่อยู่ของอ็อบเจกต์ได้ดีกว่าในการจัดการหน่วยความจำ หรือเคลื่อนย้ายระหว่างหน่วยความจำกับดิสก์ด้วยประสิทธิภาพที่คุ้มค่างบค่าใช้จ่าย โดยไม่มีผลกระทบต่อ การเข้าถึงอ็อบเจกต์ของโปรแกรมใดๆ ข้อดีเหล่านี้เรียกว่า การกำหนดเลขที่อยู่แบบเอกรูป (uniform addressing) ซึ่งเป็นข้อดีของการให้อำนาจ

12.3.4.3 คำสั่งปฏิบัติการบนอ็อบเจกต์และการให้อำนาจ

เมื่อกระบวนการ p_k เป็นเจ้าของ $Cap(obj_i)$ สามารถปฏิบัติการบน obj_i ในการเข้าถึงเอกสิทธิ์ตามอำนาจที่ได้รับดังนี้

- อ่านอ็อบเจกต์
- แก้ไขอ็อบเจกต์
- ทำลายอ็อบเจกต์
- สำเนาอ็อบเจกต์
- กระทำการอ็อบเจกต์

ต่อจากนั้น p_k ยังสามารถปฏิบัติการกับ $Cap(obj_i)$ ได้ดังนี้

- ทำสำเนาของการให้อำนาจ
- สร้างการให้อำนาจแบบกลุ่มย่อย
- ใช้อำนาจในการกำหนดพารามิเตอร์ในกระบวนการคำสั่งหรือฟังก์ชัน call
- ส่งผ่านอำนาจเพื่อให้กระบวนการอื่นใช้
- ลบการให้อำนาจ

ในระบบของการให้อำนาจหลายประเภท การปฏิบัติการเหล่านี้จะมีการป้องกันผ่านการให้เอกสิทธิ์การเข้าถึงในระบบการให้อำนาจ ดังนั้น กระบวนการอาจสามารถสร้างการให้อำนาจแก่กลุ่มย่อยของ $Cap(obj_i)$ ได้ก็ต่อเมื่อมีเอกสิทธิ์แบบ “สร้างการให้อำนาจแก่กลุ่มย่อย” ส่วนปฏิบัติการอื่นๆ ก็จะได้รับ การป้องกันในตนเองเดียวกัน

12.3.4.3 การแบ่งปันการป้องกันของอ็อบเจกต์

การเข้าถึงอ็อบเจกต์ในระบบการให้อำนาจจะดำเนินไปดังนี้

1. เมื่อกระบวนการ p_i ต้องการเรียกคำสั่งปฏิบัติการบนอ็อบเจกต์ Obj_i ก็จะกระทำการคำสั่งในรูปแบบ

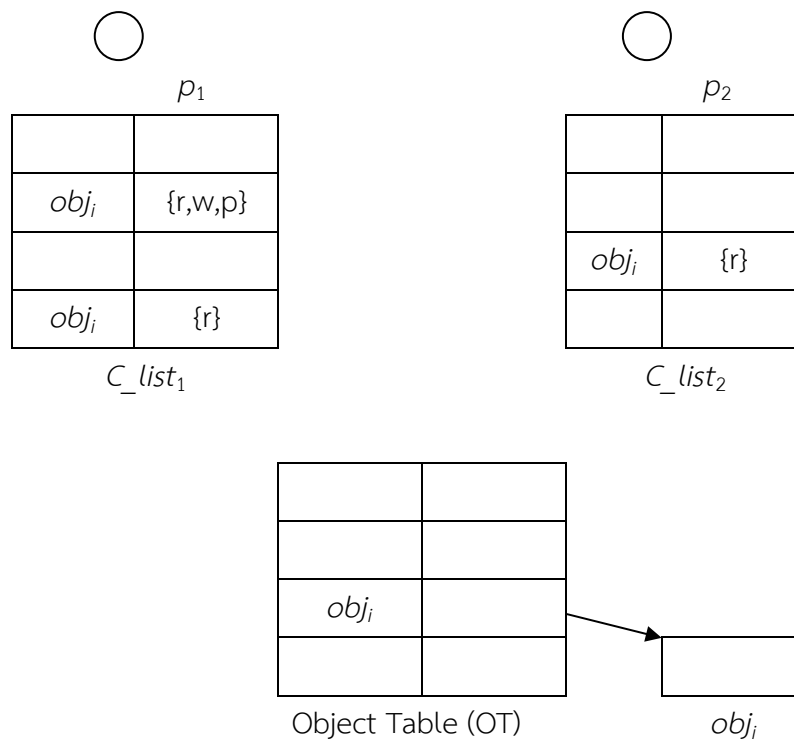
$$\langle op_1 \rangle \ d_{Cap(obj_i)}$$

โดยที่ $\langle op_1 \rangle$ คือรหัสปฏิบัติการที่ต้องการกระทำ

2. ซีพียูจะตรวจสอบว่าการกระทำของ op_1 ประกอบด้วยเอกสิทธิ์การเข้าถึงซึ่งบรรจุอยู่ใน $Cap(obj_i)$ หรือไม่ ถ้าอยู่ก็ทำตามคำสั่งนั้น ถ้าไม่อยู่ก็จะเข้าสู่การขัดจังหวะ
3. ระบบปฏิบัติการจะยกเลิกกระบวนการถ้ามีการขัดจังหวะเกิดขึ้น

ถ้า op_1 มีค่า “สร้างอ็อบเจกต์ใหม่” อยู่ ซีพียูก็สามารถปฏิบัติการอื่นๆ ได้ โดยสามารถสร้างอ็อบเจกต์ขึ้นมาใหม่พร้อมทั้งสร้างรายการของ OT ใหม่ได้ จากนั้นจะใส่รหัสอ็อบเจกต์ใหม่และที่อยู่ของอ็อบเจกต์ใหม่นั้นลงในรายการ สร้างอำนาจซึ่งบรรจุไว้ด้วยเอกสิทธิ์การเข้าถึงเท่าที่สามารถเป็นไปได้สำหรับอ็อบเจกต์และใส่ลงใน C-list ของ p_i นอกจากนั้น ยังใส่ $Cap(obj_i)$ ลงในเรจิสเตอร์ผลลัพธ์ของปฏิบัติการ op_1 กระบวนการ p_i จะเก็บค่านี้ไว้ใช้ในการเข้าถึง obj_i ในอนาคต

การแบ่งปันอ็อบเจกต์จะเกิดขึ้นเมื่อกระบวนการส่งผ่านอำนาจสำหรับอ็อบเจกต์ไปยังกระบวนการอื่น กระบวนการที่ได้รับอำนาจก็จะเข้าสู่ C-list ของตัวเอง การแบ่งปันและการป้องกันจะเป็นไปโดยปริยายเพราะ C-list ของทั้งคู่ล้วนบรรจุอยู่ในอ็อบเจกต์นั้น



12.3.4.4 การป้องกันการให้อำนาจ

ผลลัพธ์ C-list ของกระบวนการ p_1 และ p_2 กระบวนการเป็นเจ้าของเอกสิทธิ์การเข้าถึงที่แตกต่างกันสำหรับ obj_i

การป้องกันการให้อำนาจนั้นอยู่บนพื้นฐานของสมมุติฐานที่ว่า การให้อำนาจไม่สามารถปลอมแปลงหรือปิดเป็นได้ อย่างไรก็ตาม สมมุติฐานดังกล่าวนี้จะเกิดผิดพลาดถ้ากระบวนการสามารถเข้าถึง C-list และแก้ไขอำนาจที่อยู่ใน C-list นั้นได้ ตัวอย่างเช่น ในภาพที่ 10.9 อาจมีการเปลี่ยนแปลงสิทธิ์ของ obj_i ให้เป็น “เขียน” ด้วยตัวเองได้ ก็อาจใช้อำนาจนั้นแก้ไขอ็อบเจกต์ obj_i ได้เช่นกัน อันเนื่องมาจากการสืบทอดอำนาจ

การป้องกันการสืบทอดอำนาจนี้ จะต้องแยกการให้อำนาจออกจากอ็อบเจกต์ชนิดอื่นๆ อย่างชัดเจน และจะต้องแปลได้โดยเครื่องเชิงธรรมนาม (abstract machine) บนโปรแกรมที่ดำเนินงานระดับสูงเท่านั้น การให้อำนาจมีความแตกต่างจากข้อมูลประเภทอื่นๆ ได้แก่

1. แต่ละอ็อบเจกต์จะมีป้ายระบุที่บอกประเภทของการให้อำนาจหรือความสามารถในการเข้าถึงข้อมูลไว้ โปรแกรมประยุกต์จะไม่สามารถเข้าถึงป้ายระบุได้โดยตรง แต่จะใช้ฮาร์ดแวร์หรือเฟิร์มแวร์สนับสนุนเงื่อนไขดังกล่าวนี้ โดยอาจใช้เพียงหนึ่งบิตก็สามารถจำแนกความแตกต่างได้แล้ว แต่โดยทั่วไปจะใช้มากกว่าหนึ่งบิต วิธีเช่นนี้จะช่วยให้อ็อบ

เจกต์ทุกชนิดมีป้ายระบุชนิดของอ็อบเจกต์ติดไว้ในระดับฮาร์ดแวร์ ดังนั้น ฮาร์ดแวร์จะสามารถจำแนกได้ชัดเจนว่าเป็นเลขจำนวนเต็ม, เลขจุดลอยตัว, ตัวชี้, บูลีน, อักขระ, ชุดคำสั่ง, การให้อำนาจ และค่าที่เริ่มต้นใหม่โดยอาศัยป้ายระบุเหล่านั้น

2. วิธีถัดมา, พื้นที่ที่อยู่ที่ถูกเชื่อมโยงเข้ากับโปรแกรมจะแบ่งออกเป็น 2 ส่วน ส่วนแรกจะสามารถเข้าถึงได้โดยโปรแกรม และข้อมูลปกติของโปรแกรมและชุดคำสั่ง อีกส่วนหนึ่งจะบรรจุไว้ด้วยรายการให้อำนาจที่เข้าถึงได้เฉพาะระบบปฏิบัติการเท่านั้น การแบ่งส่วนหน่วยความจำในลักษณะดังกล่าวนี้จะใช้ประโยชน์ในการสนับสนุนวิธีการดังกล่าว

12.4 การใช้งานเมทริกซ์การเข้าถึง

นอกเหนือจากการใช้งานเมทริกซ์การเข้าถึงในระบบคอมพิวเตอร์ที่อิงอยู่กับการให้อำนาจแล้ว ยังมีวิธีอื่นๆ ที่น่าสนใจ ต่อไปนี้จะเปรียบเทียบวิธีการแบบตารางส่วนกลาง, รายการเข้าถึงสำหรับอ็อบเจกต์ และกลไกการยึด-กุญแจ

12.4.1 ตารางส่วนกลาง (Global Table)

การใช้เมทริกซ์การเข้าถึงอย่างง่ายที่สุดคือการใช้ตารางส่วนกลางที่ประกอบด้วยชุดของ $\langle \text{โดเมน}, \text{อ็อบเจกต์}, \text{เอกลักษณ์การเข้าถึง} \rangle$ เมื่อใดก็ตามที่คำสั่งปฏิบัติการ M ถูกกระทำการอยู่บนอ็อบเจกต์ O_j ภายในโดเมน D_i ตารางส่วนกลางจะทำการค้นหา $\langle D_i, O_j, R_k \rangle$ พร้อมกับ $M \in R_k$ ถ้าพบก็จะอนุญาตให้ดำเนินต่อไป ถ้าไม่พบก็จะเกิดการขัดจังหวะเพื่อนำไปสู่การยกเลิกกลางคัน วิธีการเช่นนี้สามารถทนทานต่อความเสียหายหลายประเภทได้ แต่เนื่องจากตารางส่วนกลางมักมีขนาดใหญ่ จึงไม่สามารถเก็บไว้ในหน่วยความจำได้ตลอดเวลา อีกทั้งต้องการไอ/โอเพิ่มเติมด้วย จึงนิยมใช้เทคนิคหน่วยความจำเสมือนเข้ามาช่วยจัดการตารางนี้ นอกจากนั้น เป็นการยากที่จะใช้ข้อได้เปรียบของกลุ่มอ็อบเจกต์พิเศษหรือโดเมน ตัวอย่างเช่น ถ้าทุกคนสามารถอ่านอ็อบเจกต์โดยเฉพาะได้จะต้องแบ่งรายการในทุกๆ โดเมน ซึ่งไม่สะดวก

12.4.2 รายการเข้าถึงสำหรับอ็อบเจกต์ (Access List for Objects)

แต่ละคอลัมน์ในเมทริกซ์การเข้าถึงสามารถใช้เหมือนกับรายการเข้าถึงของอ็อบเจกต์หนึ่ง แต่รายการที่ว่างเปล่าสามารถละทิ้งไปได้ รายการผลลัพธ์ของแต่ละอ็อบเจกต์จะประกอบด้วยชุด $\langle \text{โดเมน}, \text{เอกลักษณ์การเข้าถึง} \rangle$ ซึ่งกำหนดให้ทุกโดเมนด้วยชุดของรายการสิทธิ์การเข้าถึงของอ็อบเจกต์นั้น

วิธีนี้สามารถขยายผลอย่างง่าย ๆ โดยการกำหนดค่าปริยายไว้สำหรับเอกสิทธิ์การเข้าถึงเมื่อคำสั่งปฏิบัติการ M บนอ็อบเจกต์ O_j อยู่ในเมน D_i เราจะสามารถค้นหาสิทธิ์การเข้าถึงของอ็อบเจกต์ O_j ได้โดยดูจากรายการ $\langle D_i, R_k \rangle$ พร้อมกับ $M \in R_k$ ถ้ารายการนี้ถูกพบก็จะอนุญาตคำสั่งปฏิบัติการนั้นได้ แต่ถ้าไม่พบก็ตรวจสอบกับค่าปริยาย ถ้า M อยู่ในชุดค่าปริยาย จึงจะอนุญาตให้เข้าถึงได้ มิฉะนั้น ก็จะปฏิเสธคำสั่งนั้นหรือยกเลิก โดยทั่วไป เรามักตรวจสอบกับค่าปริยายก่อนที่จะค้นหารายการเข้าถึง

12.4.3 กลไกการยึด-กุญแจ (Lock-Key Mechanism)

วิธีการแบบการยึด-กุญแจ เป็นวิธีที่ประนีประนอมระหว่างรายการเข้าถึงกับรายการให้อำนาจ แต่ละอ็อบเจกต์จะมีรายการของบิตที่มีรูปแบบเฉพาะตัวเรียกว่า การยึด (lock) ในทำนองเดียวกัน แต่ละโดเมนก็จะมีรายการของบิตที่มีรูปแบบเฉพาะตัวเรียกว่า กุญแจ (key) กระบวนการที่จะกระทำการในโดเมนนั้นได้ก็ต่อเมื่อมีโดเมนนั้นมีกุญแจที่สอดคล้องกับการยึดของอ็อบเจกต์นั้น

ในกรณีของรายการให้อำนาจ รายการของกุญแจสำหรับโดเมนจะต้องถูกจัดการโดยระบบปฏิบัติการในนามในโดเมน ผู้ใช้ไม่มีสิทธิ์แก้ไขรายการของกุญแจหรือการยึดได้โดยตรง

12.4.4 เปรียบเทียบ

รายการเข้าถึงจะสอดคล้องโดยตรงกับความต้องการของผู้ใช้ เมื่อผู้ใช้สร้างอ็อบเจกต์ขึ้นมา ก็จะเป็นผู้กำหนดว่าจะสามารถเข้าถึงอ็อบเจกต์ได้อย่างไรบ้าง ด้วยคำสั่งอะไรบ้าง อย่างไรก็ตาม เนื่องจากข้อมูลเกี่ยวกับสิทธิ์ในการเข้าถึงโดเมนนั้นไม่อยู่เฉพาะ ในการพิจารณาเลือกชุดของสิทธิ์การเข้าถึงสำหรับแต่ละโดเมนจึงทำได้ยาก นอกจากนั้น ทุกครั้งที่เข้าถึงอ็อบเจกต์จะต้องถูกตรวจสอบเสมอ โดยการค้นหารายการเข้าถึง ดังนั้น ในระบบขนาดใหญ่จะมีรายการเข้าถึงที่มีขนาดใหญ่มากตามไปด้วย ซึ่งจะมีปัญหาในเรื่องความล่าช้า

รายการให้อำนาจไม่สอดคล้องกับความต้องการของผู้ใช้โดยตรง แต่สามารถใช้ประโยชน์ได้ดีสำหรับกระบวนการ เพราะข้อมูลการเข้าถึงซึ่งอยู่เฉพาะที่ กระบวนการที่พยายามเข้าถึงจะต้องแสดงอำนาจเพื่อการเข้าถึงนั้น จากนั้น ระบบการป้องกันจะทำการตรวจสอบเพียงแค่อำนาจนั้นถูกต้องหรือไม่เท่านั้น อย่างไรก็ตาม การถอดถอนอำนาจนั้นอาจไม่สะดวกนัก

กลไกการยึด-กุญแจ เป็นการประนีประนอมระหว่างวิธีการทั้งคู่ กลไกนี้จึงมีทั้งประสิทธิภาพและความยืดหยุ่นที่ขึ้นอยู่กับความยาวกุญแจ กุญแจสามารถส่งผ่านได้อย่างอิสระจากโดเมนหนึ่งสู่โดเมนหนึ่ง นอกจากนั้น เอกสิทธิ์การเข้าถึงอาจถูกถอดถอนได้อย่างมีประสิทธิภาพด้วยเทคนิคง่าย ๆ โดยการเปลี่ยนการยึดบางอย่างที่สอดคล้องกับอ็อบเจกต์นั้น

ระบบส่วนใหญ่ใช้ผสมผสานระหว่างรายการเข้าถึงกับการให้อำนาจ เมื่อกระบวนการพยายามเข้าถึงข้อบกพร่องครั้งแรก ก็จะทำการค้นหารายการเข้าถึง ถ้ามีการปฏิเสธ ก็จะเกิดการขัดจังหวะซึ่งนำไปสู่การยกเลิกในที่สุด ถ้าถูกต้องก็จะทำการผูกติดอำนาจนั้นไว้กับกระบวนการ ในการแสดงคราวต่อไปก็จะทำได้อย่างรวดเร็ว ภายหลังจากการเข้าถึงครั้งสุดท้าย อำนาจก็จะถูกทำลายไป กลยุทธ์ดังกล่าวนี้มีใช้ในระบบมัลติทริกซ์และคาล (CAL) ซึ่งระบบทั้งคู่ใช้ทั้งรายการเข้าถึงและรายการให้อำนาจ

ตัวอย่างต่อไปนี้จะพิจารณาระบบแฟ้มที่แต่ละแฟ้มจะเชื่อมโยงเข้ากับรายการเข้าถึง เมื่อกระบวนการเปิดแฟ้ม, เริ่มสร้างสารบบจะค้นหาแฟ้มนั้น, ตรวจสอบการอนุญาตให้เข้าถึง และจองพื้นที่บัพเฟอร์ไว้ ข้อมูลดังกล่าวทั้งหมดจะถูกบันทึกลงในรายการใหม่ในตารางแฟ้มที่เชื่อมโยงเข้ากับกระบวนการนั้น คำสั่งปฏิบัติการจะคืนค่าดรรชนีไปยังตารางนี้เพื่อเปิดแฟ้มใหม่ ทุกคำสั่งบนแฟ้มนี้จะถูกสร้างโดยข้อกำหนดของดรรชนีไปยังตารางแฟ้มดังกล่าว รายการในตารางแฟ้มก็จะชี้ไปยังแฟ้มและบัพเฟอร์ เมื่อปิดแฟ้ม รายการตารางแฟ้มนี้ก็จะถูกลบไป ตารางแฟ้มจะถูกบำรุงรักษาโดยระบบปฏิบัติการ เพื่อผู้ใช้จะได้ไม่กระทำให้อายุโดยไม่ได้ตั้งใจ ด้วยเหตุนี้ ผู้ใช้จึงสามารถเข้าถึงได้เฉพาะแฟ้มที่เปิดอยู่เท่านั้น โดยมีการตรวจสอบการเข้าถึงในขณะที่ทำการเปิดแฟ้มเพื่อรับรองถึงการป้องกัน กลยุทธ์นี้ถูกใช้ในยูนิกซ์

สิทธิ์ในการเข้าถึงจะต้องยังคงถูกตรวจสอบในแต่ละครั้งของการเข้าถึง และรายการตารางแฟ้มจะยินยอมให้อำนาจเฉพาะคำสั่งที่ได้รับอนุญาตเท่านั้น ถ้าแฟ้มถูกเปิดเพื่ออ่าน อำนาจการอ่านจะถูกใส่ไว้ในรายการของตารางแฟ้มนั้น ถ้ามีความพยายามในการเขียนแฟ้มนั้น ระบบจะสามารถตรวจพบการละเมิดการป้องกันนี้โดยการเปรียบเทียบคำสั่งปฏิบัติการที่ต้องการเข้ากับอำนาจที่ระบุไว้ในรายการตารางแฟ้ม

12.4.5 การถอนสิทธิ์การเข้าถึง

ในระบบการป้องกันแบบพลวัต บางครั้งเราอาจมีความต้องการถอนสิทธิ์การเข้าถึงข้อบกพร่องซึ่งกำลังถูกใช้ร่วมกันโดยผู้ใช้อย่างไรก็ตาม อาจมีคำถามมากมายเกิดขึ้นเกี่ยวกับการถอนสิทธิ์ดังต่อไปนี้

1. **ทันทีกับล่าช้า** (immediate versus delayed) เมื่อมีการถอนสิทธิ์ จะมีผลเกิดขึ้นทันทีหรือล่าช้าออกไป และถ้าล่าช้าออกไปเราจะรู้ได้อย่างไรว่าจะเกิดขึ้นเมื่อใด
2. **เลือกได้กับทั่วไป** (selective versus general) เมื่อสิทธิ์การเข้าถึงข้อบกพร่องถูกเพิกถอน จะเกิดผลกระทบต่อผู้ใช้ทั้งหมดที่มีสิทธิ์บนข้อบกพร่องนั้น หรือสามารถเลือกเพิกถอนเฉพาะผู้ใช้เพียงบางกลุ่มได้
3. **บางส่วนกับทั้งหมด** (partial versus total) เราสามารถถอนสิทธิ์เพียงส่วนย่อยของสิทธิ์ที่เชื่อมโยงกับข้อบกพร่องนั้น หรือจะต้องถอนสิทธิ์ทั้งหมดของข้อบกพร่องนั้น

4. **ชั่วคราวหรือถาวร** (temporary versus permanent) เราสามารถถอนสิทธิ์ออกไปอย่างถาวร โดยสิทธิ์การเข้าถึงนั้นจะไม่สามารถเรียกกลับมาได้อีก หรือสามารถถอนได้เพียงชั่วคราว สิทธิ์นั้นจะคืนกลับมาภายหลัง

ด้วยวิธีการแบบสิทธิ์การเข้าถึง การถอนสิทธิ์นั้นกระทำได้ง่าย เพียงแต่ค้นหาสิทธิ์การเข้าถึง จากนั้นลบออกจากรายการ การถอนสิทธิ์นั้นทำได้แบบทันที, สามารถเลือกได้หรือทั่วไปก็ได้, ทั้งหมดหรือบางส่วนก็ได้ และถาวรหรือชั่วคราวก็ได้

อย่างไรก็ตาม การถอนสิทธิ์ในระบบการให้อำนาจนั้นมีความยุ่งยากกว่าแบบอื่น เนื่องจากการให้อำนาจจะกระจายไปทั้งระบบ เราจำเป็นต้องค้นหาก่อนที่จะเพิกถอน ดังนั้น วิธีการถอดถอนสิทธิ์ในการให้อำนาจจะมีขั้นตอนดังต่อไปนี้

1. **การได้มาใหม่** (reacquisition) จะมีการลบการให้อำนาจออกไปจากโดเมนเป็นระยะๆ เมื่อกระบวนการต้องการใช้ ก็จะตรวจหาว่าสิทธิ์ดังกล่าวถูกลบออกไปแล้วหรือยัง กระบวนการอาจจะพยายามร้องขอสิทธิ์กลับคืนมาใหม่ได้ แต่ถ้ายิ่งการเข้าถึงของกระบวนการถูกลบไปแล้ว กระบวนการนั้นจะไม่สามารถร้องขออำนาจใหม่ได้
2. **ตัวชี้กลับ** (back-pointer) รายการของตัวชี้จะถูกบำรุงรักษาไว้โดยอ็อปเจกต์แต่ละตัว การชี้ไปยังทุกอำนาจจะเชื่อมโยงกับอ็อปเจกต์นั้นๆ เมื่อต้องการถอดถอนก็เพียงแต่วิ่งตามตัวชี้เหล่านั้น และเปลี่ยนแปลงอำนาจเท่าที่จำเป็น วิธีการนี้ถูกปรับแต่งในระบบมัลทิกซ์ เป็นเรื่องที่ต้องตรงไปตรงมาแต่มีค่าใช้จ่ายสูง
3. **ทางอ้อม** (indirection) ตัวชี้การให้อำนาจไปยังอ็อปเจกต์โดยอ้อม การให้อำนาจแต่ละชุดจะชี้ไปยังรายการที่เจาะจงในตารางส่วนกลางแล้วค่อยชี้กลับไปที่อ็อปเจกต์ เวลาถอนสิทธิ์ก็ต้องค้นหาตารางส่วนกลางจากรายการที่ต้องการ จากนั้นค่อยลบออก รายการตารางนี้จะใช้งานได้โดยไม่ยุ่งยาก เนื่องจากทั้งอำนาจและรายการในตารางบรรจุไว้ด้วยชื่อเฉพาะของอ็อปเจกต์เอาไว้ ทั้งอ็อปเจกต์และรายการตารางจะต้องตรงกัน แต่วิธีนี้ไม่อนุญาตให้ถอนสิทธิ์แบบเลือกได้
4. **กุญแจ** (keys) กุญแจคือบิตที่มีรูปแบบเฉพาะตัวที่สามารถเชื่อมโยงเข้ากับการให้อำนาจแต่ละชุด กุญแจจะถูกกำหนดขึ้นเมื่อมีการสร้างการให้อำนาจ และไม่สามารถแก้ไขหรือตรวจหาได้โดยกระบวนการที่เป็นเจ้าของ (เพราะเป็นหน้าที่ของระบบปฏิบัติการ) **กุญแจหลัก** (master key) จะเชื่อมโยงเข้ากับแต่ละอ็อปเจกต์สามารถนิยามหรือแทนที่โดยคำสั่งปฏิบัติการ set-key เมื่อการให้อำนาจถูกสร้างขึ้นมา ค่าปัจจุบันของกุญแจหลักจะถูกโยงเข้ากับการให้อำนาจ เวลาใช้อำนาจก็จะมีกระบวนการเปรียบเทียบระหว่างกุญแจกับกุญแจหลัก ถ้าตรงกันก็อนุญาตให้การปฏิบัติการนั้นดำเนินต่อไป ถ้าไม่ตรงกันก็จะยกเลิกการถอนสิทธิ์ทำได้โดยแทนกุญแจหลักด้วยค่าใหม่โดยคำสั่ง set-key

การถอนสิทธิ์วิธีนี้ไม่สามารถทำแบบเลือกได้ เนื่องจากมีเพียงกุญแจหลักเท่านั้นที่โยงเข้ากับแต่ละอ็อบเจกต์ เว้นเสียแต่ที่เราโยงรายการของกุญแจทั้งหมดเข้ากับแต่ละอ็อบเจกต์จึงจะสามารถเลือกถอนได้ วิธีสุดท้าย เราอาจจัดกลุ่มกุญแจทั้งหมดเป็นตารางส่วนกลางของกุญแจชุดเดียว การให้อำนาจจะใช้ได้ต่อเมื่อมีกุญแจที่ตรงกับกุญแจบางดอกในตารางส่วนกลาง การถอนสิทธิ์ก็ทำได้โดยลบเฉพาะที่ตรงกับกุญแจในตาราง วิธีนี้ จะโยงกุญแจแต่ละดอกเข้ากับหลายอ็อบเจกต์ และมีกุญแจหลายดอกสามารถโยงเข้ากับแต่ละอ็อบเจกต์ได้ ซึ่งเป็นวิธีที่มีความยืดหยุ่นสูงสุด

ในวิธีแบบกุญแจนั้น คำสั่งปฏิบัติการในการใส่กุญแจเข้าไปในรายการ ลบออกจากรายการ ไม่ควรให้ผู้ใช้งานทุกคนใช้ โดยเฉพาะอย่างยิ่ง มีความสมเหตุสมผลที่จะอนุญาตให้เฉพาะผู้ที่เป็นเจ้าของอ็อบเจกต์เท่านั้นจึงจะมีสิทธิ์ได้

12.6 การพิสูจน์ตัวตนจริง

ปัญหาใหญ่ของระบบความมั่นคงปลอดภัยสำหรับระบบปฏิบัติการก็คือ การพิสูจน์ตัวตนจริง (authentication) เพื่อพิสูจน์ว่า ผู้ที่กำลังร้องขอการใช้บริการอยู่นั้นเป็นใครเพื่อระบบจะได้อนุญาตหรือปฏิเสธการเข้าถึงบริการดังกล่าว กระบวนการพิสูจน์ตัวตนจริงนี้เป็นเรื่องสำคัญมากโดยเฉพาะอย่างยิ่งในระบบปฏิบัติการปัจจุบัน โดยทั่วไป การพิสูจน์ตัวตนจริงนั้นจะมีพื้นฐานในการพิสูจน์เรื่องใดเรื่องหนึ่งใน 3 เรื่อง ได้แก่ ความเป็นเจ้าของของผู้ใช้ (กุญแจหรือบัตร), ความรู้ของผู้ใช้ (ตัวระบุผู้ใช้และรหัสผ่าน) และ/หรือคุณลักษณะของผู้ใช้ (ลายนิ้วมือ, ม่านตา, หรือลายเซ็น)

12.6.1 รหัสผ่าน

การพิสูจน์ตัวตนจริงผู้ใช้ที่นิยมใช้กันมากที่สุดในระบบปฏิบัติการ ได้แก่การให้ผู้ใช้ระบุรหัสผ่าน (password) การป้องกันระบบโดยใช้รหัสผ่านเป็นวิธีที่เข้าใจได้โดยง่าย และวิธีสร้างก็ง่าย กล่าวคือระบบจะสร้างรหัสผู้ใช้ (user ID) หรือชื่อบัญชี (account name) ของผู้ใช้ หรือบางทีเรียกว่าชื่อผู้ใช้ (user name) เวลาใช้งานผู้ใช้จะต้องบอกรหัสผ่านที่สอดคล้องกับชื่อผู้ใช้ ระบบจึงจะยอมรับว่าผู้นั้นเป็นผู้ใช้ตัวจริง วิธีสร้างที่ง่ายที่สุดคือการจัดเก็บรายชื่อและรหัสผ่านควบคู่กันไป

ในระหว่างการพิสูจน์ตัวตนจริงของผู้ใช้นั้น ในขณะที่ผู้ใช้พิมพ์รหัสผ่านลงไป ระบบคอมพิวเตอร์จะไม่แสดงอักขระที่พิมพ์ออกมา (อาจแสดงเป็นสัญลักษณ์แทน) เพื่อความมั่นคงปลอดภัยจากการแอบดูและจดจำโดยผู้อื่น

ในระบบที่ไม่มีการป้องกันโดยวิธีอื่น รหัสผ่านมักถูกใช้ปกป้องอ็อบเจกต์ต่างๆในระบบคอมพิวเตอร์ การเชื่อมโยงรหัสผ่านเข้ากับทรัพยากรแต่ละชนิด เช่น แฟ้ม เป็นต้น เมื่อใดก็ตามที่ต้องการเข้าถึงทรัพยากรดังกล่าวก็จำเป็นต้องระบุรหัสผ่านลงไป ถักรหัสผ่านถูกต้อง จึงจะได้ใช้

ทรัพยากรนั้น บางระบบรหัสผ่านอาจกำหนดไว้แตกต่างกันตามชนิดของคำสั่งปฏิบัติการ เช่น การอ่าน, การเพิ่ม และการปรับปรุง

12.6.2 จุดอ่อนของรหัสผ่าน

เนื่องจาก รหัสผ่านมักถูกนำไปใช้กันอย่างแพร่หลายเนื่องจากง่ายต่อความเข้าใจและใช้งาน อย่างไรก็ตาม ปัญหาที่เกิดขึ้นเกี่ยวข้องกับการเก็บรหัสผ่านให้เป็นความลับ โดยไม่มีใครสามารถเดาได้ แต่รหัสผ่านอาจถูกถูกเดาได้ ถูกเปิดเผย โดยไม่ตั้งใจ, การแกะรอย หรือเจ้าของเป็นผู้บอกรหัสผ่านแก่บุคคลอื่น

โดยทั่วไปมีอยู่ 2 วิธีในการเดารหัสผ่านคืออะไร วิธีแรก ผู้บุกรุก (intruder) รู้จักกับเจ้าของรหัสหรือรู้ข้อมูลส่วนตัวของเจ้าของรหัส เช่น ชื่อสัตว์เลี้ยง, ชื่อพ่อแม่, วันเดือนปีเกิดของเจ้าของ เป็นต้น ซึ่งข้อมูลเหล่านี้มักนำไปตั้งเป็นรหัสผ่าน อีกวิธีหนึ่ง ผู้บุกรุกพยายามรวบรวมข้อมูลส่วนตัวของเจ้าของรหัสผ่านที่เป็นประโยชน์ต่อการนำไปผสมปนเปกันแล้วเดาว่าเป็นรหัสผ่าน ดังนั้น รหัสผ่านสั้นๆ จะทำให้เดาได้ง่ายกว่า โดยทดลองเดาไล่ไปเรื่อยๆ จนกว่าจะถูกต้อง ตัวอย่างเช่น รหัสผ่านที่มีความยาว 4 ตัว จะสามารถสร้างรูปแบบที่แตกต่างกันของรหัสผ่านได้ 10000 รูปแบบ แต่โดยเฉลี่ยแล้ว การเดาประมาณ 5000 ครั้งก็สามารถคาดเดาออกว่ารหัสผ่านแท้จริงคืออะไร การตั้งรหัสผ่านที่ยาวขึ้นจะทำให้การเดานั้นยากและใช้เวลานานขึ้นด้วย

หลักทั่วไปของรหัสผ่านที่ดีคือ ไม่ใช่คำที่มีความหมาย หรืออยู่ในพจนานุกรม (ซึ่งสามารถเดาได้โดยอาศัยโปรแกรมเดารหัสผ่าน) รหัสผ่านที่เป็นตัวเลขจะเดายากกว่าตัวอักษรในขนาดที่เท่ากัน รหัสผ่านที่เป็นตัวเลขผสมตัวอักษรทั้งตัวเล็กและใหญ่รวมทั้งใช้อักขระพิเศษด้วยจะยิ่งยากต่อการเดายิ่ง แต่การตั้งรหัสยาวๆ เช่นนั้นทำให้เจ้าของเองจดจำไม่ได้อาจต้องเขียนไว้ที่ใดที่หนึ่ง ซึ่งก็เสี่ยงต่อการค้นพบและเดาได้ในที่สุด

รหัสผ่านนั้นสามารถสร้างขึ้นมาโดยระบบคอมพิวเตอร์หรือผู้ใช้เป็นผู้กำหนดเองก็ได้ รหัสผ่านที่สร้างโดยคอมพิวเตอร์จะยากต่อการจดจำ แต่ถ้าสร้างโดยผู้ใช้นั้นจะง่ายต่อการเดา บางระบบจะกำหนดช่วงเวลาหมดอายุของรหัสผ่านที่เจ้าของต้องเปลี่ยนรหัสใหม่ แต่ผู้ใช้นั้นก็มักเปลี่ยนกลับมาใช้รหัสเดิมที่เคยตั้งไปแล้วสลับไปมา ซึ่งกลายเป็นจุดอ่อนให้สามารถเดาได้อีก บางระบบจึงเก็บประวัติของรหัสผ่านไว้ด้วย ผู้ใช้จะไม่สามารถนำรหัสผ่านเก่ามาตั้งใหม่ได้

12.6.3 รหัสผ่านที่ถูกเข้ารหัส

ปัญหาหนึ่งของรหัสผ่านก็คือการเก็บรักษาความลับของรหัสผ่านไว้ในระบบคอมพิวเตอร์ ในระบบยูนิคซ์ จะใช้วิธีการเข้ารหัส (encryption) แพ้มที่ใช้เก็บรหัสผ่านให้เป็นความลับ โดยใช้

ฟังก์ชันที่ยุ่งยากหรือเป็นไปได้ที่จะถอดรหัส แต่ง่ายต่อการคำนวณ ถ้ารู้ค่า x ในฟังก์ชัน $f(x)$ ก็สามารถคำนวณค่าของฟังก์ชัน $f(x)$ ได้ แต่ถ้ารู้แต่เพียงฟังก์ชัน $f(x)$ เท่านั้นจะไม่สามารถหาค่าของ x ได้เลย ฟังก์ชัน $f(x)$ นี้ ถือเป็นขั้นตอนวิธีสำหรับแปลงรหัสผ่านที่ใช้กันโดยทั่วไป

แต่ข้อเสียของวิธีนี้คือ ระบบจะไม่สามารถควบคุมจำนวนรหัสผ่านที่อยู่ในระบบทั้งหมดได้ แม้รหัสผ่านจะถูกแปลงแล้วก็ตาม แต่ใครก็ตามที่คัดลอกแฟ้มที่เก็บรหัสผ่านไปก็สามารถนำไปแปลงกลับโดยใช้ฟังก์ชัน $f(x)$ ได้เช่นกัน โปรแกรมที่ใช้ในการแปลงกลับรหัสผ่านบนระบบยูนิกซ์มีอยู่มากมาย ซึ่งสามารถทำได้โดยใช้เวลาไม่นานนักบนเทคโนโลยีฮาร์ดแวร์ของคอมพิวเตอร์ที่มีความเร็วสูงเช่นปัจจุบัน ดังนั้น ยูนิกซ์รุ่นใหม่ๆ จึงทำการซ่อนแฟ้มที่เก็บรหัสผ่านเอาไว้

12.6.4 รหัสผ่านแบบใช้ครั้งเดียว

ในการแก้ปัญหาการแกะรอยและเดาไปเรื่อยๆ ระบบจะใช้วิธีตั้งรหัสผ่านแบบคู่ (paired password) เมื่อเริ่มต้น ระบบจะทำการสุ่มเลือกและแสดงส่วนแรกของรหัสผ่าน เพื่อให้ผู้ใช้ตอบกลับส่วนที่เหลือ ในระบบนี้บางทีเรียกว่าระบบร้องทัก/ตอบกลับ (challenge/respond) ซึ่งเป็นระบบความมั่นคงปลอดภัยที่ดัดแปลงมาจากที่ใช้ในการทหาร เมื่อหน่วยลาดตระเวนในสนามรบพบฝ่ายตรงข้ามแต่ไม่แน่ใจว่าเป็นฝ่ายเดียวกันหรือ ฝ่ายแรกจะใช้วิธีการร้องทัก อีกฝ่ายหนึ่งก็จะตอบกลับมา ถ้าคำตอบสอดคล้องตรงกับคำร้องทัก (ตามที่ได้ตกลงกันไว้แต่แรก) ก็เป็นการพิสูจน์ได้ว่าเป็นฝ่ายเดียวกัน คำร้องทัก/ตอบกลับนี้จะเปลี่ยนแปลงไปเรื่อยๆ โดยไม่ซ้ำกัน ระบบนี้เป็นส่วนหนึ่งของระบบรหัสผ่านแบบใช้ได้ครั้งเดียว

ในระบบรหัสผ่านแบบใช้ได้ครั้งเดียว (one-time password) รหัสจะแตกต่างกันทุกครั้งที่ร้องขอเข้าสู่ระบบ เป็นอีกวิธีหนึ่งที่ใช้ในการป้องกันผู้มีสิทธิใช้งานจริงเปิดเผยรหัสผ่านแก่ผู้อื่นที่ไม่มีสิทธิใช้ระบบได้ ปัจจุบันการใช้งานในเชิงการค้าก็มีการใช้ระบบรหัสผ่านแบบใช้ได้ครั้งเดียว อย่างเช่น SecurID จะใช้เครื่องคำนวณที่มีลักษณะเหมือนบัตรเครดิต มีแป้นพิมพ์และจอภาพ ผู้ใช้ต้องใส่รหัสที่เรียกว่ารหัสส่วนบุคคล (Personal Identification Number หรือ PIN) จากนั้น ระบบจะแสดงรหัสผ่านให้เห็น ผู้ใช้ต้องพิมพ์รหัสผ่านให้ตรงกับที่เห็น ระบบจึงจะยอมรับ บางระบบ ผู้ใช้ต้องพิมพ์รหัสส่วนบุคคล (PIN) จากนั้น ระบบจะแสดงรหัสผ่านแบบใช้ได้ครั้งเดียว ผู้ใช้ต้องพิมพ์ไปตามที่เห็น แม้แต่ในการสมัครลงทะเบียนเพื่อขอไปรษณีย์อิเล็กทรอนิกส์ของเว็บไซต์ผู้ให้บริการไปรษณีย์อิเล็กทรอนิกส์แบบไม่เสียเงิน (free e-mail) ระหว่างการกรอกข้อมูลลงทะเบียนออนไลน์นั้น ระบบจะแสดงรหัสผ่านขึ้นที่จอภาพเพื่อให้ผู้สมัครป้อนรหัสผ่านตามที่เห็น ระบบนี้ก็ถือเป็นการใช้รหัสผ่านแบบใช้ได้ครั้งเดียวเช่นกัน ระบบนี้มีไว้เพื่อป้องกันไม่ให้โปรแกรมการลงทะเบียนอัตโนมัติเพื่อขอที่อยู่ไปรษณีย์อิเล็กทรอนิกส์ไปใช้เพื่อการค้า การใช้รหัสส่วนบุคคลร่วมกับรหัสผ่านแบบใช้ได้ครั้งเดียวนี้ ถือเป็นรูปแบบหนึ่งของการพิสูจน์ตัวจริงแบบสองตัวประกอบ (two-factor authentication) ซึ่งถือ

ว่าเป็นระบบการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสูงกว่าการพิสูจน์ตัวตนแบบตัวประกอบเดียว (single-factor authentication)

อีกวิธีหนึ่ง คือการใช้สมุดรายการรหัสผ่าน โดยผู้ใช้จะได้รับสมุดรหัสผ่าน (code book หรือ one-time pad) ซึ่งเป็นรายการของรหัสผ่านที่ใช้ได้เพียงครั้งเดียวมาให้ แม้มีผู้แอบเห็นรหัสผ่านของผู้ใช้ในขณะป้อน ก็ไม่สามารถนำไปใช้ต่อไปได้ เพราะรหัสผ่านจะเปลี่ยนไปทุกครั้งที่มีการเข้าสู่ระบบใหม่

12.6.5 ชีวมิติ

การพิสูจน์ตัวตนโดยใช้คุณลักษณะเชิงกายภาพของผู้ใช้ เรียกว่า ชีวมิติ (biometrics) โดยอาศัยลักษณะเชิงกายภาพ รูปแบบการแสดงตัวตนบางประเภทไม่สามารถปลอมแปลงได้โดยง่าย อย่างเช่น ลักษณะเชิงกายภาพของแต่ละคน วิธีการแบบชีวมิติจึงพยายามใช้คุณลักษณะเหล่านี้ในอุปกรณ์ความมั่นคงปลอดภัย เป็นศาสตร์ที่ว่าด้วยการพิสูจน์ตัวตนโดยใช้การตรวจวัดคุณลักษณะเฉพาะทางร่างกาย คุณลักษณะเฉพาะที่มีความเป็นเอกลักษณ์สามารถใช้บ่งชี้ตัวตนได้อย่างเช่น ลักษณะเส้นสายของที่ปรากฏบนลายนิ้วมือ, ลักษณะเส้นเลือดดำที่อยู่ในลูกนัยน์ตา, ริมฝีปาก, ลักษณะรูปทรงโดยรวมของโครงใบหน้า เป็นต้น

ระบบความมั่นคงปลอดภัยที่ใช้วิธีการพิสูจน์ตัวตนแบบชีวมิติ จัดเป็นเทคนิคการแสดงตัวตนที่ไม่สามารถปลอมแปลงได้โดยง่ายในระบบความมั่นคงปลอดภัย แต่เป็นระบบที่มักมีค่าใช้จ่ายสูงกว่าวิธีอื่นๆ แต่ระบบนี้ก็มีจุดอ่อนที่สามารถปลอมตัวได้ง่าย ตัวอย่างเช่น ในระบบที่ใช้การสแกนลายนิ้วมือเพื่อพิสูจน์ตัวตนนั้น ถ้ามีผู้บุกรุกมีภาพสแกนลายนิ้วมือของผู้ใช้ ก็จะสามารถผ่านเข้าสู่ระบบได้อย่างง่ายดาย และการปลอมแปลงด้วยวิธีนี้มีค่าใช้จ่ายเพียงเล็กน้อยเท่านั้น

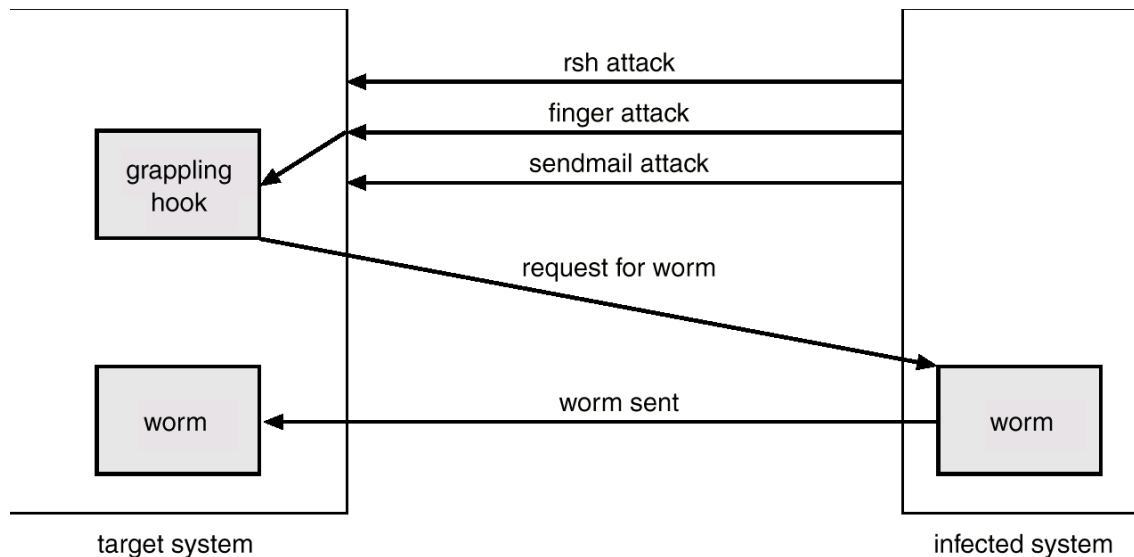
12.7 โปรแกรมอันตราย

เมื่อโปรแกรมถูกเขียนโดยผู้ใช้คนหนึ่ง และถูกใช้โดยอีกคนหนึ่ง ดังนั้น อาจเกิดการใช้ที่ผิดพลาดขึ้นได้ หรืออาจมีพฤติกรรมที่ไม่อาจคาดเดาได้ เมื่อเกิดเหตุการณ์เช่นนี้ ก็ถือเป็นภัยคุกคามที่มีต่อระบบความมั่นคงปลอดภัยของคอมพิวเตอร์ได้

12.7.1 หนอนและไวรัส

หนอนและไวรัสจัดเป็นรูปแบบของมหันตภัยของระบบคอมพิวเตอร์ หนอน (worm) คือโปรแกรมที่ทำซ้ำตัวเองขยายตัวเพิ่มมากขึ้นไปเรื่อยๆ บนหน่วยความจำหรือหน่วยเก็บงานกระทั่งพื้นที่ว่างในหน่วยความจำหรือหน่วยเก็บไม่มีพื้นที่เหลืออยู่ หนอนมักมีการแพร่โดยอาศัยเครือข่าย

คอมพิวเตอร์และอินเทอร์เน็ต ตัวอย่างของหนอนได้แก่โปรแกรมหนอนที่ถูกปล่อยโดยนักศึกษาคณะหนึ่งที่มีมหาวิทยาลัยคอร์แนลสามารถท่องเที่ยวผ่านเครือข่ายอินเทอร์เน็ตโดยอีเมลและทำการปิดระบบของคอมพิวเตอร์ลงประมาณพันกว่าเครื่องที่อยู่รอบๆ เมืองในเวลาเพียงไม่กี่ชั่วโมง



รูป 12.3 หนอนอินเทอร์เน็ตของมอริส (Morris Internet worm)

ที่มา (Silberschatz et. al., 2003, p. 667)

หนอนคอมพิวเตอร์จะประกอบด้วยโปรแกรม 2 ส่วน ได้แก่ โปรแกรมส่วนเกาะติด (grappling hook หรือบางที่เรียกว่า bootstrap หรือ vector) และโปรแกรมหลัก (main program) โปรแกรมส่วนเกาะติดประกอบด้วยรหัสคำสั่งจำนวน 99 บรรทัด เขียนขึ้นด้วยภาษาซี ชื่อ 1.c โปรแกรมส่วนนี้จะทำงานบนแต่ละเครื่องที่ติดเชื้อ ในขณะที่ทำงาน มันจะส่งข่าวสารติดต่อกลับมายังเครื่องคอมพิวเตอร์ต้นทางที่ปล่อยเชื้อออกไป แล้วเรียกโปรแกรมหลักเพื่อให้งานบนเครื่องที่ติดเชื่อนั้น ดังแสดงในภาพที่ 13.10 หลังจากนั้น หนอนจะมองหาเครื่องอื่นๆ ที่อยู่ในเครือข่ายเดียวกันเพื่อทำการแพร่เชื้อไปยังเครื่องเหล่านั้น จากนั้น จึงเริ่มมองหาเครื่องที่อยู่ในเครือข่ายใกล้เคียงกันเพื่อทำการแพร่เชื้อ

ส่วนไวรัส (virus) คือโปรแกรมผิดปกติที่สามารถติดเชื้อและแพร่เชื้อตัวมันเองไปยังระบบคอมพิวเตอร์ จากนั้นทำลายหรือสร้างความเสียหายแก่ข้อมูล ไวรัสสามารถแพร่เชื้อผ่าน 2 ทาง

โดยฟลอปปีดิสก์ ทางแรกของการติดเชื้อไวรัสจะมาจากแผ่นฟลอปปีดิสก์ที่ติดเชื้อแล้ว เมื่อนำแผ่นที่ติดเชื้อไปใช้ยังคอมพิวเตอร์เครื่องอื่นๆ ไวรัสจะทำการแพร่เชื้อไปยังเครื่องเหล่านั้น

โดยเครือข่าย ทางที่สองคือผ่านทางเครือข่ายคอมพิวเตอร์โดยเฉพาะอย่างยิ่งอินเทอร์เน็ต อย่างเช่น อีเมล (มักับแฟ้มไวรัสที่แนบมาพร้อมกับอีเมล), บูลเลตินบอร์ด, จากแฟ้มหรือซอฟต์แวร์ฟรีที่ดาวน์โหลดจากอินเทอร์เน็ต, ห้องสนทนา โปรแกรมสนทนาออนไลน์ (instant message) ปัจจุบัน มีการค้นพบไวรัสชนิดใหม่ที่สามารถแพร่เชื้อผ่านหน้าเว็บได้ โดยเพียงแค่ผู้ใช้เข้าไปเยี่ยมชม เว็บไซด์ที่มีเว็บไวรัสเท่านั้นก็สามารถถูกติดเชื้อได้

โดยทั่วไป ไวรัสจะติดเชื้อมอยู่ในฮาร์ดดิสก์คอมพิวเตอร์ และจะแสดงอาการตั้งแต่ แสดงข้อความ, แสดงภาพเคลื่อนไหว, ลบแฟ้มบางชนิด, ลบข้อมูลหรือทำให้แฟ้มข้อมูลใช้การไม่ได้, ลบซอฟต์แวร์หรือทำให้ซอฟต์แวร์ทำงานผิดพลาด ไปจนกระทั่งลบทุกสิ่งทุกอย่างที่อยู่ในเครื่องคอมพิวเตอร์ ทั้งนี้ ขึ้นอยู่กับประเภทของไวรัส

การจัดการเกี่ยวกับปัญหาไวรัส อาจจะเริ่มจากการติดตั้งโปรแกรมประเภทต่อต้านไวรัส เช่น McAfee, Norton Anti Virus เป็นต้น โดยจำเป็นต้องทำการปรับปรุงแฟ้มข้อมูลไวรัสอย่างสม่ำเสมอ จากเว็บไซต์ของเจ้าของผลิตภัณฑ์, ทำการสแกนแผ่นฟลอปปีดิสก์ที่จะนำมาใช้กับเครื่องของเรา ก่อนเสมอ, สแกนแฟ้มทุกแฟ้มที่แนบมาในอีเมลก่อนเปิดอ่าน รวมทั้งแฟ้มและซอฟต์แวร์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนที่จะใช้งานหรือติดตั้งเสมอ

ไวรัสมีหลากหลายรูปแบบ แต่มักมีอยู่ 2 ชนิดหลักๆ ได้แก่ ไวรัสประเภทบูตเซกเตอร์ (boot sector virus) และไวรัสประเภทแฟ้ม (file virus) ปัจจุบันมีไวรัสชนิดหนึ่งที่มักติดเชื้อ ได้แก่ ไวรัสประเภทมาโคร (macro virus)

ไวรัสประเภทบูตเซกเตอร์ (boot-sector virus) บูตเซกเตอร์ เป็นดิสก์บริเวณที่ส่วนของซอฟต์แวร์ระบบจะใช้ในการเริ่มต้นระบบเมื่อตอนเปิดเครื่องคอมพิวเตอร์ คำสั่งที่ถูกฝังอยู่ในบริเวณนี้ จะถูกแทนที่ด้วยรหัสของไวรัส ดังนั้น เมื่อคอมพิวเตอร์ถูกเปิดเครื่องขึ้นมา ไวรัสก็จะถูกประจุเข้าสู่หน่วยความจำหลัก และพร้อมจะแพร่เชื้อไปยังแผ่นฟลอปปีดิสก์หรือคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย ตัวอย่างเช่น AntCMOS, AntiEXE, From.A, NYB (New York Boot), Ripper, Stoned.Empire.Money เป็นต้น

ไวรัสประเภทแฟ้ม (file virus) จะแพร่เชื้อไปยังแฟ้มประเภทโปรแกรมที่มักใช้ในการเริ่มต้นคอมพิวเตอร์ (ในดอสมักเป็นแฟ้มที่ลงท้ายด้วย .com และ .exe) เมื่อโปรแกรมเหล่านี้เริ่มทำงาน โปรแกรมไวรัสก็จะเริ่มทำงานไปพร้อมๆ กันด้วย โดยการประจุตัวเองเข้าไปไว้ในหน่วยความจำหลักและทำการแพร่เชื้อไปยังแฟ้มอื่นๆ

ไวรัสบางชนิดได้ผสมผสานระหว่างไวรัสประเภทบูตเซกเตอร์เข้ากับประเภทแฟ้มเข้าด้วยกัน มีความสามารถเพิ่มมากขึ้น โดยสามารถติดเชื้อได้ทั้งส่วนที่เป็นบูตเซกเตอร์ และแฟ้ม

โปรแกรม ซึ่งยากต่อการตรวจจับโดยโปรแกรมต่อต้านไวรัส ตัวอย่างเช่น Junkie และ Parity Boot เป็นต้น ไวรัสประเภทนี้อาจมีความสามารถในการเปลี่ยนรูปตัวเองและรหัสไวรัสไปได้เรื่อยๆจนกระทั่งแทบไม่มีร่องรอยที่แน่นอน เพื่อหลีกเลี่ยงการตรวจจับของโปรแกรมต่อต้านไวรัส เช่น One Half เป็นต้น

ไวรัสประเภทมาโคร (macro virus) มาโครเป็นกลุ่มคำสั่งที่ถูกเขียนขึ้นและฝังไว้เป็นส่วนหนึ่งของแฟ้มเพื่อสั่งให้ปฏิบัติการบางอย่างได้ ไวรัสประเภทนี้ได้ถูกเขียนในรูปแบบของมาโครแล้วฝังไว้เป็นส่วนหนึ่งแฟ้มซึ่งอาจเป็นเอกสารของไมโครซอฟต์เวิร์ดหรือเอ็กเซล ทำให้หลีกเลี่ยงการตรวจจับของโปรแกรมต่อต้านไวรัสได้ง่าย ตัวอย่างเช่น Concept, Laroux เป็นต้น

บอมบ์ (bomb) แตกต่างจากไวรัสประเภทอื่นๆ เมื่อไวรัสได้แพร่เชื้อไปยังเครื่องปลายทางแล้วสามารถรอเวลาหรือสถานการณ์บางอย่างเกิดขึ้นจึงสั่งให้ไวรัสโจมตีเครื่องปลายทางได้ ไวรัสที่แสดงผลเมื่อถึงเวลาที่กำหนดไว้เรียกว่า ทุ้มบอมบ์ (time bomb) เช่น Friday the 13th virus ที่เริ่มโจมตีเฉพาะวันศุกร์ที่ 13 และไวรัสที่รอให้ถึงเหตุการณ์หรือเงื่อนไขที่กำหนดไว้เกิดขึ้นจึงจะเริ่มโจมตี เรียกว่า ลอจิกบอมบ์ (logic bomb)

12.7.2 ม้าโทรจัน และประตูลับ

ม้าโทรจัน (Trojan horse) เป็นโปรแกรมที่ไม่ประสงค์ดีต่อระบบได้ถูกสร้างและฝังไว้กับโปรแกรมปกติทั่วไปอย่างเช่นเกมคอมพิวเตอร์ ภายหลังจากที่โปรแกรมปกติทำงาน โปรแกรมม้าโทรจันก็เริ่มทำงานไปพร้อมๆ กันโดยที่ผู้ใช้แทบไม่รู้ตัว โปรแกรมเหล่านี้อาจถูกตรวจจับได้ยากจากโปรแกรมต่อต้านไวรัสทั่วไป เนื่องจากไม่มีรหัสของไวรัสที่โดดเด่นนัก และการแพร่เชื้อก็กระทำอย่างช้าๆ แบบค่อยเป็นค่อยไป ตัวอย่างเช่น FormatC เป็นต้น

ประตูลับ (trapdoor or backdoor) เป็นโปรแกรมที่ถูกออกแบบมาให้เปิดช่องทางลับทิ้งไว้เพื่อที่จะได้เข้ามากระทำทุจริตได้ในภายหลังโดยไม่สามารถถูกตรวจพบได้ง่าย การทิ้งประตูลับไว้ในโปรแกรมเช่นนี้มีอันตรายมาก ซึ่งอาจเกิดได้ทั้งตั้งใจและไม่ตั้งใจของผู้ออกแบบสร้างระบบ

12.7.3 การเข้ารหัสลับ

วิธีการหนึ่งที่นิยมนำมาใช้ในการปกป้องความมั่นคงปลอดภัยของข้อมูลนั้นได้แก่ การเข้ารหัสลับ (encryption) คือกรรมวิธีการเปลี่ยนแปลงข้อมูลไปสู่รูปแบบที่ไม่สามารถใช้งานได้จนกว่าจะนำไปผ่านกระบวนการถอดรหัสลับ (decryption) ซึ่งเป็นวิธีการย้อนกลับเพื่อเปลี่ยนแปลงข้อมูลผ่านการเข้ามาแล้วให้อยู่ในรูปแบบที่สามารถอ่านได้

การเข้ารหัสสามารถนำไปใช้ประโยชน์ได้ดีในองค์กรต่างๆ ที่ตระหนักด้านความมั่นคงปลอดภัย เช่น หน่วยงานทหาร, ธนาคาร, และโดยเฉพาะอย่างยิ่งการทำธุรกรรมต่างๆ ด้านพาณิชย์อิเล็กทรอนิกส์ผ่านเครือข่ายอินเทอร์เน็ต

กระบวนการเข้ารหัสข้อมูลนั้นปัจจุบันมีหลากหลายวิธี แต่หลักการสำคัญการวิธีการเหล่านี้คือ การที่ข้อมูลถูกส่งผ่านไปบนเครือข่ายคอมพิวเตอร์สามารถใช้สื่อกลางในการส่งที่ไม่ปลอดภัย (insecure channel) นั้น จำเป็นต้องมีการสร้างเกราะป้องกันกับความลับของข้อมูลก่อนที่จะส่งไปเสียก่อน จุดประสงค์หลักคือการรักษาความลับของข้อมูลเพื่อประกันว่าข้อมูลจะไม่ถูกเปิดเผยแก่บุคคลอื่นที่ไม่ใช่ผู้รับปลายทางโดยตรง หลักการสำคัญของกระบวนการเข้ารหัสมีดังนี้

- 1) นำข้อความที่สามารถอ่านได้ (clear text) มาผ่านกระบวนการเข้ารหัส (encryption) โดยอาศัยกุญแจการเข้ารหัส (encryption key)

- 2) ผลที่ได้คือข้อความที่ไม่สามารถอ่านได้ (cipher text)

- 3) เมื่อต้องการอ่านข้อความที่ผ่านการเข้ารหัส จำเป็นต้องนำไปผ่านกระบวนการถอดรหัส (decryption) เพื่อเปลี่ยนแปลงข้อความที่ไม่สามารถอ่านได้ให้เป็นข้อความเดิมที่สามารถอ่านได้อีกครั้งหนึ่ง ในขั้นตอนนี้ต้องอาศัยกุญแจถอดรหัส (decryption key)

ดังนั้น ผู้ใดก็ตามที่จะสามารถอ่านข้อความที่ได้รับมาได้นั้นจำเป็นต้องมีกุญแจถอดรหัส ถ้ากุญแจเข้ารหัสและกุญแจถอดรหัสเหมือนกัน เรียกกระบวนการเข้าและถอดรหัสว่า การเข้ารหัสลับแบบกุญแจสมมาตร (symmetric-key encryption) หรือวิธีการเข้ารหัสแบบกุญแจดอกเดียว (single-key scheme) แต่ถ้ากุญแจเข้ารหัสและถอดรหัสแตกต่างกัน เรียกว่า การเข้ารหัสลับแบบกุญแจอสมมาตร (asymmetric-key encryption) หรือ วิธีการเข้ารหัสแบบกุญแจสองดอก (two-key scheme) โดยดอกแรกเป็นกุญแจส่วนตัว (private key) ส่วนดอกที่สองเป็นกุญแจสาธารณะ (public key) การเข้ารหัสลับวิธีหลังนี้ถือว่ามี ความมั่นคงปลอดภัยสูงกว่าวิธีแรกมาก และเป็นที่นิยมใช้ในการทำธุรกรรมแบบพาณิชย์อิเล็กทรอนิกส์ผ่านอินเทอร์เน็ต

กระบวนการเข้ารหัสและถอดรหัสเรียกว่า วิทยาการรหัสลับ (cryptography) ซึ่งเป็นศาสตร์ที่ว่าด้วยการรักษาความลับของข้อมูลโดยวิธีการเข้ารหัส ส่วนกระบวนการตรงกันข้ามที่ใช้ขโมยความลับของข้อมูลที่เข้ารหัส เรียกว่า นักวิเคราะห์รหัสลับ (cryptanalysis) เป็นเทคนิควิธีในการวิเคราะห์การเข้ารหัส บางทีเรียกว่า การทำลายการเข้ารหัส (break encryption)

12.8 สรุปบท

ระบบคอมพิวเตอร์จะบรรจุไว้ด้วยฮาร์ดแวร์หลายชนิด และมีความจำเป็นต้องป้องกันการใช้งานที่ผิดพลาด การป้องกันจะมุ่งที่ผู้ใช้ภายในเป็นหลัก ในขณะที่ความปลอดภัยจะเน้นที่ผู้ใช้ภายนอก ระบบคอมพิวเตอร์ การป้องกันและความมั่นคงปลอดภัยจะใช้ได้โดยมีการกำหนดนโยบายและกลไก

เข้ามาช่วย อี้อุปเจกต์อาจเป็นฮาร์ดแวร์ (อย่างเช่น หน่วยความจำ, เวลาซีพียู หรืออุปกรณ์ไอ/โอ) หรือซอฟต์แวร์ (เช่น แฟ้ม, โปรแกรม และแบบชนิดข้อมูลนามธรรม) สิทธิ์การเข้าถึงจะเป็นตัวระบุการอนุญาตให้เข้าใช้ได้หรือไม่เมื่อต้องการปฏิบัติการบนอี้อุปเจกต์นั้น โดเมนคือชุดของสิทธิ์การเข้าถึงกระบวนการต่างๆ จะกระทำการภายในโดเมน และอาจใช้สิทธิ์ที่มีอยู่ในโดเมนนั้นเพื่อเข้าถึงและแก้ไขอี้อุปเจกต์ ในระหว่างดำเนินงาน กระบวนการอาจมีการส่งผ่านโดเมนการป้องกันไปยังโดเมนอื่นๆ ได้

การใช้เมทริกซ์การเข้าถึงถือเป็นแบบจำลองทั่วไปของการป้องกัน เพราะมีการจัดเตรียมกลไกและนโยบายการป้องกันไว้ การแบ่งแยกระหว่างกลไกและนโยบายถือเป็นคุณลักษณะสำคัญของการออกแบบ

การใช้งานเมทริกซ์ของการเข้าถึงอาจทำได้โดยโยงรายการเข้าถึงเข้ากับแต่ละอี้อุปเจกต์ หรือโยงรายการให้อำนาจเข้ากับแต่ละโดเมน ซึ่งอาจทำแบบพลวัตหรือแบบตายตัวก็ได้

ในระบบจริงๆ อาจมีข้อจำกัดมาก และใช้เพียงการป้องกันสำหรับแฟ้มเท่านั้น ยูนิกซ์จะใช้การป้องกันเกี่ยวกับการอ่าน, เขียน และกระทำการซึ่งแยกออกไปสำหรับเจ้าของ, กลุ่ม และแฟ้มสาธารณะสำหรับแฟ้มแต่ละแฟ้ม ส่วนระบบมัลทิกซ์ จะใช้โครงสร้างแบบวงแหวนเพิ่มเข้าไปเพื่อการเข้าถึงแฟ้ม

กระบวนการพิสูจน์ตัวจริงเป็นเรื่องสำคัญมากโดยเฉพาะอย่างยิ่งในระบบปฏิบัติการปัจจุบัน โดยทั่วไป การพิสูจน์ตัวจริงนั้นจะมีพื้นฐานในการพิสูจน์เรื่องใดเรื่องหนึ่งใน 3 เรื่อง ได้แก่ ความเป็นเจ้าของของผู้ใช้ (กุญแจหรือบัตร), ความรู้ของผู้ใช้ (ตัวระบุผู้ใช้และรหัสผ่าน) และ/หรือคุณลักษณะของผู้ใช้ (ลายนิ้วมือ, ม่านตา, หรือลายเซ็น) การพิสูจน์ตัวจริงที่นิยมใช้ได้แก่ รหัสผ่าน, จุดอ่อนของรหัสผ่าน, รหัสผ่านที่ถูกเข้ารหัส, รหัสผ่านแบบใช้ได้ครั้งเดียว และชีวมิติ ส่วนโปรแกรมอันตรายนั้นถือเป็นภัยคุกคามต่อระบบความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้แก่ หนอนอินเทอร์เน็ตและไวรัสชนิดต่างๆ ม้าโทรจันและประตูลับ

วิธีการหนึ่งที่นิยมนำมาใช้ในการปกป้องความมั่นคงปลอดภัยของข้อมูลนั้นได้แก่ การเข้ารหัสลับ (encryption) คือกรรมวิธีการเปลี่ยนแปลงข้อมูลไปสู่รูปแบบที่ไม่สามารถใช้งานได้จนกว่าจะนำไปผ่านกระบวนการถอดรหัสลับ (decryption) ซึ่งเป็นวิธีการย้อนกลับเพื่อเปลี่ยนแปลงข้อมูลผ่านการเข้ามาแล้วให้อยู่ในรูปที่สามารถอ่านได้ การเข้ารหัสลับมี 2 แบบ แบบแรกเรียกว่า การเข้ารหัสลับแบบกุญแจสมมาตร และแบบกุญแจสมมาตร

12.9 สรุปบท

เนื้อหาในบทนี้กล่าวถึงแนวคิดพื้นฐานเกี่ยวกับการป้องกันและความมั่นคงปลอดภัยของระบบปฏิบัติการ โดยเน้นการจัดการสิทธิ์การเข้าถึงอี้อุปเจกต์ต่างๆ ทั้งฮาร์ดแวร์และซอฟต์แวร์ การพิสูจน์ตัวจริงของผู้ใช้ และการป้องกันภัยคุกคาม เช่น ไวรัส หนอนอินเทอร์เน็ต และโปรแกรม

อันตรายต่างๆ รวมถึงการใช้งานเทคนิคเข้ารหัสข้อมูลเพื่อรักษาความลับและความปลอดภัยระบบปฏิบัติการจึงถือเป็นรากฐานสำคัญในการดูแลคุณภาพและความเชื่อถือได้ของทรัพยากรในระบบคอมพิวเตอร์

12.10 บทวิเคราะห์และมุมมองเชิงวิชาการ: “ความมั่นคงปลอดภัยในระบบปฏิบัติการ (Operating System Security)”

เอกสารคำสอนในบท *ความมั่นคงปลอดภัยในระบบปฏิบัติการ* มุ่งเน้นการอธิบายกลไกและนโยบายการป้องกัน (protection and security) ที่ระบบปฏิบัติการจัดเตรียมไว้ เพื่อรักษาบูรณภาพ (integrity) และความเชื่อถือได้ (reliability) ของการใช้ทรัพยากร เช่น ไฟล์ หน่วยความจำ และกระบวนการ ประเด็นนี้ถือเป็นแกนกลางในการเรียนการสอนด้าน Cybersecurity เพราะระบบปฏิบัติการเป็น “ฐานราก” ที่รองรับทั้งซอฟต์แวร์และฮาร์ดแวร์ การทำความเข้าใจกลไกเหล่านี้จึงเป็นพื้นฐานสำหรับนักศึกษาในการก้าวสู่การออกแบบและบริหารระบบที่มั่นคงปลอดภัย ในที่นี้จะเสนอบทวิเคราะห์และมุมมองดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

- **ความแตกต่าง Protection vs Security:** *Protection* เน้นปกป้องข้อมูลและโปรแกรมจากผู้ภายใน ส่วน *Security* มุ่งเน้นการปกป้องจากผู้บุกรุกภายนอก
- **โครงสร้างการป้องกัน (Protection Structures):** ใช้ *Access Control Matrix (ACM)*, *ACL* และ *C-list* เพื่อควบคุมสิทธิ์การเข้าถึงไฟล์และอ็อบเจกต์ในระบบ
- **Domain of Protection:** ระบบสามารถกำหนดขอบเขตการเข้าถึงเป็นโดเมน (เช่น user domain, process domain) พร้อมกลไก dynamic switching
- **การให้อำนาจ (Capability):** ใช้ token แทนสิทธิ์การเข้าถึง (capability list) ที่สามารถส่งผ่านระหว่าง process ได้อย่างยืดหยุ่น
- **การพิสูจน์ตัวตนจริง (Authentication):** ตั้งแต่รหัสผ่าน, password hashing, one-time password ไปจนถึง biometrics
- **ภัยคุกคามใน OS:** เช่น worm, virus, trojan, backdoor และการเข้ารหัสลับในเชิงป้องกัน/โจมตี

2) มุมมองเชิงวิชาการและความก้าวหน้าปัจจุบัน

1. จาก Access Control → Attribute-based Access Control (ABAC) ACM, ACL, C-list คือจุดเริ่มต้น แต่ระบบสมัยใหม่ขยายสู่ RBAC และ ABAC เพื่อรองรับนโยบายที่ซับซ้อนและเป็นพลวัต (dynamic)
2. จาก Password → Multi-factor Authentication (MFA) & Passwordless รหัสผ่านมีข้อจำกัด ปัจจุบันองค์กรนิยมใช้ MFA, Hardware token (เช่น FIDO2), และ

passwordless authentication เพื่อลดความเสี่ยงจากการโจมตีด้วย brute-force หรือ phishing

3. จาก Protection Domain → Virtualization & Container Security แนวคิด domain ถูกนำมาประยุกต์ใน VM และ container โดยใช้ isolation + sandboxing เพื่อป้องกัน cross-tenant attack
4. Capability Systems → Trusted Execution Environments (TEE) แนวคิด capability พัฒนาสู่ Intel SGX, ARM TrustZone ที่ใช้ hardware-based isolation เพื่อเพิ่มความมั่นคงปลอดภัย
5. OS Malware Defense → EDR/XDR จากการมุ่งเน้น anti-virus และ signature-based detection ปัจจุบันระบบปฏิบัติการเสริมด้วย Endpoint Detection and Response (EDR) และ XDR ที่ใช้ AI วิเคราะห์พฤติกรรม

3) ประสบการณ์และการสอดแทรกเชิงการสอน

จากประสบการณ์ทางวิชาชีพและทางวิชาการผู้สอนพบว่า นักศึกษามักเข้าใจระบบปฏิบัติการเพียงในเชิงการใช้งาน แต่ไม่ลึกถึงระดับ security model การนำ *real-world breach cases* เช่น EternalBlue (Windows SMB exploit) หรือ Dirty COW (Linux privilege escalation) มาใช้เป็น case study ทำให้นักศึกษาเห็นว่า ช่องโหว่ใน OS อาจนำไปสู่การโจมตีเครือข่ายทั้งองค์กร วิธีการสอนที่ผสมทฤษฎี + case study + lab จึงช่วยให้นักศึกษามีทักษะวิเคราะห์และออกแบบระบบที่ปลอดภัยยิ่งขึ้น

บท “ความมั่นคงปลอดภัยในระบบปฏิบัติการ” วางรากฐานด้าน protection mechanism, access control, domain, authentication และ malware defense อย่างไรก็ตาม เพื่อสะท้อนความก้าวหน้าทางวิชาการ จึงควรเสริมเนื้อหา MFA, ABAC, virtualization security, TEEs, และ EDR/XDR เพื่อให้นักศึกษาเข้าใจทั้ง พื้นฐานและแนวโน้มใหม่ ที่เกิดขึ้นในอุตสาหกรรม

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายความแตกต่างระหว่าง Protection และ Security ในระบบปฏิบัติการ

แนวคำตอบ: Protection = ป้องกันข้อมูลจากผู้ใช้งานภายใน, Security = ป้องกันจากผู้ใช้งานภายนอก

ข้อ 2. อธิบายโครงสร้าง ACL และ C-list พร้อมยกตัวอย่างการใช้งาน

แนวคำตอบ: ACL = ระบุสิทธิ์ในแฟ้มต่อผู้ใช้, C-list = ระบุสิทธิ์ของผู้ใช้ต่อแฟ้ม

ข้อ 3. อธิบายแนวคิด Protection Domain พร้อมเปรียบเทียบใน Unix และ Multics

แนวคำตอบ: Domain = กลุ่มสิทธิ์ที่กระบวนการเข้าถึงได้; Unix = setuid, Multics = วงแหวน (Ring)

ข้อ 4. วิเคราะห์ปัญหาของการใช้รหัสผ่านแบบดั้งเดิมนาน ๆ

แนวคำตอบ: เสี่ยงถูกดักจับ/เดาได้, ควรใช้ one-time password หรือ biometrics

ข้อ 5. ยกตัวอย่าง Malware 3 ชนิดในระบบปฏิบัติการและอธิบายผลกระทบ

แนวคำตอบ: ไวรัส = ทำลายไฟล์, หนอน = กระจายตัวเอง, Trojan = เปิดช่องโหว่ Backdoor

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. เป้าหมายหลักของการป้องกันในระบบปฏิบัติการคืออะไร

ก. เพิ่มความเร็ว CPU

ข. ปกป้องบูรณภาพของข้อมูล

ค. ลดต้นทุนฮาร์ดแวร์

ง. เพิ่มจำนวนผู้ใช้พร้อมกัน

เฉลย: ข

ข้อ 2. ACL ใช้เก็บข้อมูลใด

ก. สิทธิ์ของผู้ใช้ต่อแฟ้ม

ข. สิทธิ์ของแฟ้มต่อผู้ใช้

ค. รหัสผ่านทั้งหมด

ง. รายการโปรแกรมที่อนุญาต

เฉลย: ข

ข้อ 3. C-list ใช้เก็บข้อมูลใด

ก. สิทธิ์ของผู้ใช้ต่อแฟ้ม

ข. สิทธิ์ของแฟ้มต่อผู้ใช้

ค. รายการโปรแกรมที่รันได้

ง. รหัสผ่านทั้งหมด

เฉลย: ก

ข้อ 4. Protection Domain ของ Multics ใช้แนวคิดใด

ก. Tree Structure

ข. Ring Structure

ค. Mesh Structure

ง. Grid Structure

เฉลย: ข

ข้อ 5. setuid ใน Unix ใช้ทำอะไร

ก. เปลี่ยนรหัสผ่านผู้ใช้

ข. เปลี่ยนสิทธิ์การเข้าถึงของกระบวนการชั่วคราว

ค. ตรวจสอบความถูกต้องของไฟล์

ง. สแกนหา Malware

เฉลย: ข

ข้อ 6. วิธีใดเป็น Authentication ที่แข็งแกร่งที่สุด

ก. Password ธรรมดา

ข. One-time Password

ค. Biometrics

ง. Username + Password

เฉลย: ค

ข้อ 7. Trojan มักสร้างปัญหาใด

- ก. ทำลายฮาร์ดแวร์ทันที
- ข. เปิดช่องโหว่ Backdoor
- ค. เพิ่มความเร็วระบบ
- ง. ป้องกันไวรัสอื่น

เฉลย: ข

ข้อ 8. กลไกใดเป็นการประนีประนอมระหว่าง ACL และ C-list

- ก. Firewall
- ข. Lock-Key Mechanism
- ค. OTP
- ง. Hash Function

เฉลย: ข

ข้อ 9. Access Matrix ใช้เพื่ออะไร

- ก. แสดงสิทธิ์การเข้าถึงระหว่างผู้ใช้และอ็อบเจกต์
- ข. เก็บรหัสผ่านทั้งหมด
- ค. ตรวจสอบ Malware
- ง. ตรวจสอบการทำงานของ CPU

เฉลย: ก

ข้อ 10. ข้อใดไม่ใช่การพิสูจน์ตัวตนจริง

- ก. Password
- ข. Biometrics
- ค. CAPTCHA
- ง. Defragmentation

เฉลย: ง

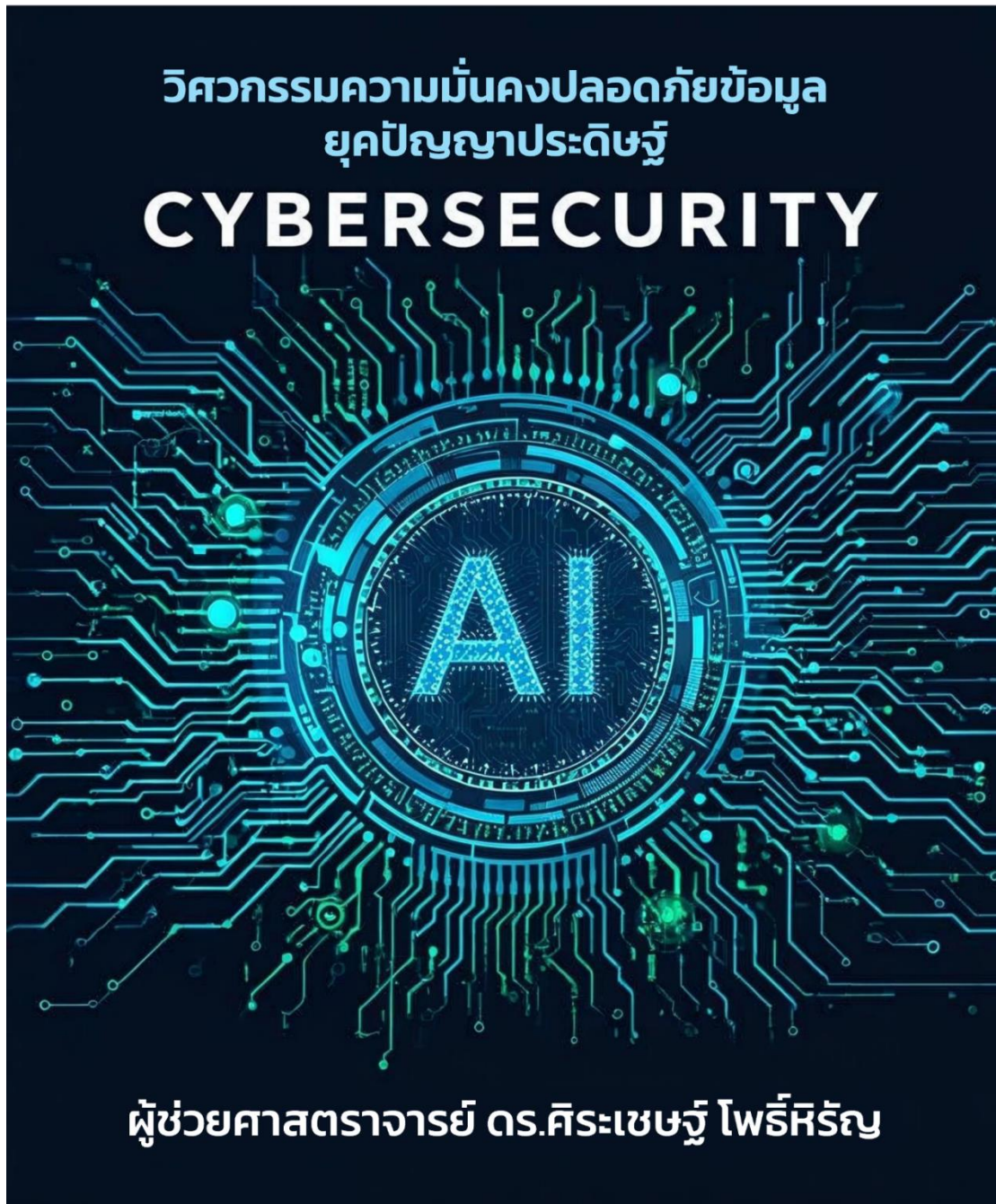
บรรณานุกรมท้ายบท

- วิเชษฐ์ พลายมาศ. ระบบปฏิบัติการ (Operating Systems). กรุงเทพฯ: ซีเอ็ดดูเคชั่น, 2552.
- Abadi, M. and Gordon, A. D. (1999). A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, Vol. 148, No. 1, January.
- C. C. Center. (2001). CERT Advisory CA-2001-19 “Code Red” Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. <http://www.cert.org/advisories/CA-2001-19.html>.
- C. C. Center. (2001). CERT Advisory CA-2001-26 “Nimda Worm”. <http://www.cert.org/advisories/CA-2001-26.html>.
- C. I. A. Capability, (2004). Network Intrusion Detector Overview. <http://ciac.llnl.gov/cstc/nid/intro.html>.
- Garfinkel, S., & Spafford, G. (2021). *Practical UNIX and Internet Security*. O’Reilly.
- Microsoft. (2021). *Windows Security Hardening Guidelines*.
- MITRE. (2023). *ATT&CK Framework: Privilege Escalation & Persistence*.
- NIST. (2020). *Zero Trust Architecture (SP 800-207)*.
- Peter Mell, Donald Marks, and Mark McLarnon, (2000). A Denial-of-Service Resistant Intrusion Detection Architecture, *Computer Networks*, Special Issue on Intrusion Detection, Elsevier Science BV.
- Red Hat. (2022). *SELinux Guide*.
- S. Bellovin, M. Leech, and T. Taylor, (2001). ICMP Traceback Messages. Internet draft, work in progress. <http://search.ietf.org/internetdrafts/draft-floyd-pushback-messages-00.txt>.
- S. Floyd, S. M. Bellovin, J. Ioannidis, K. Kompella, R. Mahajan, and V. Paxson, (2001). Pushback Messages for Controlling Aggregates in the Network. Internet draft, work in progress.
- Silberschatz, Galvin And Gagne, (2003). *Operating System Concepts*, sixth edition, John Wiley & Sons.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2020). *Operating System Concepts* (10th ed.). Wiley.
- Stallings, W. (2021). *Computer Security: Principles and Practice*. Pearson.

William Stallings.(2000). Operating Systems; Internal and Design Principles.
forth edition. Prentice-Hall. [http://search.ietf.org/internet-drafts/draft-ietf-
itrac-01.txt](http://search.ietf.org/internet-drafts/draft-ietf-itrace-01.txt).

บทที่ 13

แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์



บทที่ 13 แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบหัวข้อนี้ นักศึกษาจะสามารถ:

1. อธิบายแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับกฎหมายและมาตรฐานไทย เช่น พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2555, พ.ร.บ.ไซเบอร์ 2562, และ พ.ร.บ. PDPA 2562 ได้
2. วิเคราะห์ความแตกต่างของมาตรการรักษาความมั่นคงปลอดภัย 3 ระดับ (พื้นฐาน-กลาง-เคร่งครัด) ได้
3. ประเมินมาตรการตามกรอบ NIST CSF (Identify, Protect, Detect, Respond, Recover) ในบริบทของ CII ได้
4. เชื่อมโยงมาตรการด้านความมั่นคงกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ได้
5. ประยุกต์ใช้แนวทางเชิงลึกด้าน Cybersecurity (เช่น BCP, Incident Response, System Hardening) กับสถานการณ์จริงในองค์กรได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อจบหัวข้อนี้ นักศึกษาจะสามารถ:

1. ระบุและอธิบายมาตรการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2555
2. อธิบายความสำคัญของหน่วยงานโครงสร้างพื้นฐาน (CII) และกรอบมาตรฐาน พ.ร.บ.ไซเบอร์ 2562
3. วิเคราะห์กรอบมาตรการ NIST CSF (Identify, Protect, Detect, Respond, Recover) กับการจัดการภัยคุกคามไซเบอร์
4. อธิบายหลักการสำคัญและสิทธิของเจ้าของข้อมูลตาม PDPA
5. เสนอแนวทางปฏิบัติและการกู้คืนระบบหลังภัยคุกคามไซเบอร์ได้

3. หัวข้อเนื้อหา

13.1 แนวปฏิบัติและการรายงานตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

13.1.1 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับพื้นฐาน

13.1.2 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับกลาง

13.1.3 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับ
เคร่งครัด

13.1.4 สรุปแนวปฏิบัติและการรายงานตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

13.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์หน่วยงานโครงสร้างพื้นฐาน

13.2.1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐาน

13.2.2 หน่วยงานโครงสร้างพื้นฐาน (CII)

13.2.3 โครงสร้างของกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

13.2.4 กรอบการดำเนินงานที่ครอบคลุม

13.2.5 กระบวนการจัดทำรายงานที่ระบุในประกาศ

13.2.6 เหตุผลความจำเป็นในการดำเนินการ

13.3 แนวปฏิบัติการเชิงลึก การย้าย และการกู้คืน

13.3.1 การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)

13.3.2 มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

13.3.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

13.3.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

13.3.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

13.3.6 กลไกการขับเคลื่อน การบังคับใช้ และการรายงาน

13.3.7 ความสำคัญและความจำเป็นในการดำเนินการ

13.3.8 สรุปแนวปฏิบัติการ การย้าย การกู้คืน และการรายงานสำหรับหน่วยงานโครงสร้างพื้นฐาน

13.4 สารสนเทศส่วนบุคคล

13.4.1 ภาพรวม

13.4.2 สารสำคัญของ PDPA

13.4.3 นิยามศัพท์ที่เกี่ยวข้อง

13.4.4 สิ่งที่จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ (Privacy Notice)

13.4.5 ฐานการประมวลผลข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

13.4.6 สิทธิของเจ้าของข้อมูลส่วนบุคคล

13.4.7 สรุปแนวปฏิบัติการและการรายงานสารสนเทศส่วนบุคคล

13.5 บทวิเคราะห์และมุมมองเชิงวิชาการ

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา:

หน่วยงานราชการแห่งหนึ่งใช้ระบบฐานข้อมูลประชาชน มีความพยายามโจมตีจาก Ransomware และพบการรั่วไหลของข้อมูลส่วนบุคคลบางส่วน นักศึกษาต้องวิเคราะห์และเสนอแนวทางรับมือ

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

1. วิเคราะห์การละเมิดความมั่นคงไซเบอร์และผลกระทบที่เกิดขึ้น
2. อ้างอิงกรอบกฎหมาย/มาตรฐานที่เกี่ยวข้อง (รัฐธรรมนูญอิเล็กทรอนิกส์, พ.ร.บ.ไซเบอร์, PDPA)
3. เสนอแนวทางการตอบสนองและกู้คืนระบบ (Incident Response + BCP)
4. จัดทำ Flow Diagram ของมาตรการป้องกันและแก้ไข

ประเด็นการเรียนรู้ที่แทรก:

- มาตรการตาม พ.ร.บ.รัฐธรรมนูญอิเล็กทรอนิกส์ พ.ศ.2555
- กรอบมาตรฐาน CII และ พ.ร.บ.ไซเบอร์ 2562
- NIST CSF Functions (Identify, Protect, Detect, Respond, Recover)
- หลักการ PDPA และสิทธิของเจ้าของข้อมูล
- แนวทาง BCP/Incident Response

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ปัญหา (25)	ครอบคลุมทั้งภัยไซเบอร์และผลกระทบ	ครอบคลุมแต่ยังไม่ลึก	วิเคราะห์บางส่วน	ไม่ถูกต้อง
การอ้างอิงกฎหมาย/มาตรฐาน (25)	ระบุครบ (พ.ร.บ.รัฐธรรมนูญ, ไซเบอร์, PDPA)	ระบุเพียงบางส่วน	ระบุไม่ครบ	ไม่อ้างอิง

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การเสนอแนวทางแก้ไข (30)	ครอบคลุม Incident Response + BCP	ครอบคลุม บางส่วน	กล่าวไม่ ชัดเจน	ไม่เสนอ
การนำเสนอ (20)	ชัดเจน + Flow Diagram	ชัดเจน	พอใช้	ไม่ชัดเจน

13. แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถใช้ประโยชน์ได้

เนื้อหาในส่วนนี้จะเน้นวิเคราะห์การประยุกต์ใช้กรอบมาตรฐานอ้างอิงที่สำคัญและกฎหมายไทยที่เกี่ยวข้องในการนำมาสร้างมาตรการและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับองค์กร มีวัตถุประสงค์สำคัญ 3 ประการ

ประการแรก เพื่อให้องค์กรสามารถออกแบบมาตรการและแนวปฏิบัติที่สอดคล้องกับเงื่อนไขข้อกำหนดแนวปฏิบัติมาตรการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

ประการที่สอง เพื่อให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) สามารถออกแบบมาตรการและแนวปฏิบัติที่สอดคล้องกับเงื่อนไขข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรอง

ประการที่สาม เพื่อให้องค์กรสามารถออกแบบมาตรการและแนวปฏิบัติที่สอดคล้องกับเงื่อนไขข้อกำหนดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายลำดับรอง

13.1 แนวปฏิบัติและการรายงานตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

แนวปฏิบัติมาตรการการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย ฉบับนี้ ได้กำหนดระดับวิธีการแบบปลอดภัยเป็น 3 ระดับ ได้แก่ ระดับพื้นฐาน ระดับกลาง และระดับเคร่งครัด

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศเป็นมาตรการสำหรับการใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย ซึ่งครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศและสารสนเทศในระบบนั้น โดยการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วยระบบสารสนเทศต้องดำเนินการตามมาตรการที่เกี่ยวข้องตามประกาศฉบับนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน

ทั้งนี้ มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ แบ่งออกเป็น 11 ข้อ ได้แก่

- 1) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ
- 2) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร
- 3) การบริหารจัดการทรัพยากรสารสนเทศ
- 4) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร
- 5) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม
- 6) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
- 7) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
- 8) การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
- 9) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด
- 10) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง
- 11) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

13.1.1 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับพื้นฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยใน **ระดับพื้นฐาน** ต้องปฏิบัติดังนี้

ข้อ 1. การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการหน่วยงานต้องกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยผ่านการอนุมัติและผลักดันโดยผู้บริหารระดับสูง และมีการประกาศนโยบายดังกล่าวให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบโดยทั่วกัน

ข้อ 2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

2.1 ผู้บริหารระดับสูงของหน่วยงานมีหน้าที่ดูแลรับผิดชอบงานด้านสารสนเทศของหน่วยงานให้การสนับสนุน และกำหนดทิศทางการดำเนินงานเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจน รวมทั้งมีการมอบหมายงานที่เกี่ยวข้องให้กับผู้ปฏิบัติงานอย่างชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใด ๆ

2.2 สำหรับระบบสารสนเทศใหม่ มีการกำหนดขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่าง ๆ เช่น การบริหารจัดการผู้ใช้งานระบบ หรือความสามารถในการทำงาน ร่วมกันได้ระหว่างระบบเดิมและระบบใหม่

2.3 มีการกำหนดสัญญาการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-agreement) ที่สอดคล้องกับสถานการณ์และความต้องการของหน่วยงานในการปกป้องข้อมูล Disclosure สารสนเทศ

2.4 มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการอนุญาตให้ผู้ให้บริการที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน

2.5 สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาสารสนเทศ ควร มีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศระบุไว้ในข้อตกลง

ข้อ 3. การบริหารจัดการทรัพย์สินสารสนเทศมีการเก็บบันทึกข้อมูลทรัพย์สินสารสนเทศ โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

ข้อ 4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

4.1 กำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยด้านสารสนเทศของพนักงาน หรือหน่วยงาน หรือบุคคลภายนอกที่จ้าง โดยให้สอดคล้องกับความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่หน่วยงานประกาศใช้

4.2 ผู้บริหารระดับสูงของหน่วยงานต้องกำหนดให้พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้าง ปฏิบัติงานตามนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยที่หน่วยงานประกาศใช้

4.3 กำหนดให้มีขั้นตอนการลงโทษพนักงานที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคง ปลอดภัยด้านสารสนเทศในหน่วยงาน

4.4 กำหนดหน้าที่ความรับผิดชอบในการยุติการจ้าง หรือการเปลี่ยนแปลงสถานะการจ้างให้ชัดเจน และ มอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

4.5 พนักงาน หน่วยงานหรือบุคคลภายนอกที่ว่าจ้างต้องส่งคืนทรัพย์สินสารสนเทศของหน่วยงานเมื่อ สิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงานให้กับหน่วยงาน

4.6 ให้ยกเลิกสิทธิของพนักงาน หน่วยงานหรือบุคคลภายนอกในการเข้าใช้งานระบบสารสนเทศ เมื่อ สิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญาหรือข้อตกลงการปฏิบัติงาน และให้ปรับเปลี่ยนระดับสิทธิในการ เข้าใช้งานระบบสารสนเทศให้เหมาะสมเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบใด ๆ เกิดขึ้น

ข้อ 5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

5.1 ให้มีการป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้ งาน ระบบสารสนเทศและข้อมูลสารสนเทศ

5.2 มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันภัยจากภายนอก ภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

5.3 จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่าง ๆ และ เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

5.4 มีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือที่อาจหยุดชะงัก จากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting utilities)

5.5 มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งความถูกต้องครบถ้วนและอยู่ในสภาพพร้อม ใช้ งานอยู่เสมอ

ข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบ คอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

6.1 มีการจัดทำ ปรับปรุง และดูแลเอกสารขั้นตอนการปฏิบัติงานที่อยู่ในสภาพพร้อมใช้งาน เพื่อให้ พนักงานสามารถนำไปปฏิบัติได้

6.2 มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างปฏิบัติตามสัญญา หรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และ ระดับการให้บริการ

6.3 มีการติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของบุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ

6.4 จัดให้มีเกณฑ์การตรวจรับระบบสารสนเทศที่มีการปรับปรุง หรือที่มีเวอร์ชันใหม่ และควรมีการทดสอบระบบสารสนเทศทั้งในช่วงการพัฒนาระบบและก่อนการตรวจรับ

6.5 มีขั้นตอนควบคุมการตรวจสอบ ป้องกัน และกักกันในกรณีมีการใช้งานโปรแกรมไม่พึงประสงค์ และให้มีการสร้างความตระหนักรู้ให้กับผู้ใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศเกี่ยวกับโปรแกรมไม่พึงประสงค์

6.6 มีการสำรองข้อมูลสารสนเทศ และทดสอบการนำกลับมาใช้งาน โดยให้เป็นไปตามนโยบายการสำรองข้อมูลที่หน่วยงานประกาศใช้

6.7 มีการบริหารจัดการการควบคุมเครือข่ายคอมพิวเตอร์ เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่ายดังกล่าว

6.8 มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการโดยหน่วยงานเอง หรือจ้างช่วงไปยัง ผู้ให้บริการภายนอก

6.9 จัดให้มีนโยบายและขั้นตอนปฏิบัติงาน รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

6.10 จัดให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

6.11 จัดให้มีนโยบายและขั้นตอนการปฏิบัติงาน เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนผ่านระบบสารสนเทศที่มีการเชื่อมต่อกับระบบสารสนเทศต่าง ๆ

6.12 มีการป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต

6.13 มีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

6.14 สำหรับข้อมูลสารสนเทศที่มีการเผยแพร่ต่อสาธารณชน ให้มีการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต และเพื่อรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ

6.15 มีการเก็บบันทึกข้อมูล Audit log ซึ่งบันทึกข้อมูลกิจกรรมการใช้งานของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่าง ๆ เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง

6.16 มีขั้นตอนการเฝ้าติดตามสังเกตการใช้งานระบบสารสนเทศ และมีการติดตามประเมินผลการติดตามสังเกตดังกล่าวอย่างสม่ำเสมอ

6.17 มีการป้องกันระบบสารสนเทศที่จัดเก็บ Log และข้อมูล Log เพื่อป้องกันการเข้าถึงหรือแก้ไขเปลี่ยนแปลงโดยมิได้รับอนุญาต

6.18 มีการจัดเก็บ Log ที่เกี่ยวข้องกับการดูแลระบบสารสนเทศโดยผู้ดูแลระบบ (System administrator หรือ System operator)

ข้อ 7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

7.1 จัดให้มีนโยบายควบคุมการเข้าถึง โดยจัดทำเป็นเอกสาร และมีการติดตามทบทวนให้นโยบายดังกล่าวสอดคล้องกับข้อกำหนดหรือความต้องการด้านการดำเนินงานหรือการให้บริการ และด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

7.2 จัดให้มีการลงทะเบียนบัญชีผู้ใช้งานระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้อย่างเป็นทางการ เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศใด ๆ ของหน่วยงาน

7.3 การกำหนดสิทธิในการเข้าถึงระดับสูง ให้ทำอย่างจำกัดและอยู่ภายใต้การควบคุมการใช้งาน

7.4 ผู้ใช้งานต้องดูแลป้องกันอุปกรณ์สารสนเทศใดที่อยู่ภายใต้ความดูแลรับผิดชอบ ในระหว่างที่ไม่มี การใช้งาน

7.5 จำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง และข้อกำหนดการใช้งานแอปพลิเคชันเพื่อการดำเนินงาน

7.6 ให้ผู้ใช้งานทุกคนมีบัญชีผู้ใช้งานเป็นของตนเอง และให้ระบบสารสนเทศมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้

7.7 ให้อยู่ติหรือปิดหน้าจอการใช้งานระบบสารสนเทศโดยอัตโนมัติ หากไม่มีการใช้งานเกินระยะเวลาสูงสุดที่กำหนดไว้

7.8 จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่าง ๆ ในแอปพลิเคชันของผู้ใช้งานและผู้ดูแลระบบสารสนเทศ โดยให้สอดคล้องกับนโยบายการเข้าถึงที่ได้กำหนดไว้

7.4 กำหนดนโยบายและแนวทางการจัดการด้านความมั่นคงปลอดภัย เพื่อลดความเสี่ยงในการใช้งาน อุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ เช่น แล็ปท็อปคอมพิวเตอร์ (Laptop Computer) หรือ สมาร์ทโฟน (Smartphone) เป็นต้น

ข้อ 8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

8.1 ในการจัดทำข้อกำหนดขั้นต่ำของระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ให้มีการระบุข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศไว้ด้วย

8.2 ให้ดูแล ควบคุม ติดตามตรวจสอบการทำงานในการแจ้งช่วงพัฒนาซอฟต์แวร์

ข้อ 9. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิดผ่านช่องทางการบริหารจัดการที่เหมาะสมโดยเร็วที่สุด

ข้อ 10. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้กำหนดแผนเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศหลังเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อให้ข้อมูลสารสนเทศอยู่ในสภาพพร้อมใช้งานตามระดับที่กำหนดไว้ภายในระยะเวลาที่กำหนดไว้

ข้อ 11. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

11.1 ให้มีการระบุไว้ให้ชัดเจนถึงแนวทางในการดำเนินงานของระบบสารสนเทศที่มีความสอดคล้องตามกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน โดยต้องจัดทำเป็นเอกสาร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

11.2 ป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

11.3 พนักงานของหน่วยงานต้องดูแลให้งานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศที่อยู่ในขอบเขตความรับผิดชอบได้ดำเนินการไปโดยสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่าง ๆ ของหน่วยงาน

13.1.2 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับกลาง

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับกลาง ให้ปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐาน และต้องปฏิบัติเพิ่มเติมอีกจำนวน 10 ข้อ สรุปได้ดังนี้

ข้อ 1. การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการ หน่วยงานต้องวางแผนการติดตามและประเมินผล การใช้งานความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อย่างสม่ำเสมอ เพื่อปรับปรุงหากมีการเปลี่ยนแปลงใด ๆ ภายในหน่วยงาน ทั้งนี้ เพื่อให้เหมาะสมกับสถานการณ์การใช้งาน และคงความมีประสิทธิภาพอยู่เสมอ

ข้อ 2. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร (แนวปฏิบัติ 3 ข้อตามเอกสารแนบท้าย)

ข้อ 3. การบริหารจัดการทรัพยากรสารสนเทศ (แนวปฏิบัติ 4 ข้อตามเอกสารแนบท้าย)

ข้อ 4. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร พนักงาน หน่วยงานหรือบุคคลภายนอกต้องได้รับการอบรมเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน และได้รับการสื่อสารให้ทราบถึงนโยบายหรือระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานประกาศใช้อย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลง

ข้อ 5. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (แนวปฏิบัติ 2 ข้อตามเอกสารแนบท้าย)

ข้อ 6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (แนวปฏิบัติ 5 ข้อตามเอกสารแนบท้าย)

ข้อ 7. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (แนวปฏิบัติ 8 ข้อตามเอกสารแนบท้าย)

ข้อ 8. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (แนวปฏิบัติ 6 ข้อตามเอกสารแนบท้าย)

ข้อ 9. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง (แนวปฏิบัติ 3 ข้อตามเอกสารแนบท้าย)

ข้อ 10. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (แนวปฏิบัติ 5 ข้อตามเอกสารแนบท้าย)

13.1.3 มาตรการการรักษาความมั่นคงปลอดภัยตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ ระดับเคร่งครัด

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ให้ปฏิบัติ ตามมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในระดับพื้นฐานและระดับกลาง และต้องปฏิบัติเพิ่มเติมอีกจำนวน 9 ข้อ สรุปได้ดังนี้

- ข้อ 1. การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร (แนวปฏิบัติ 3 ข้อตามเอกสารแนบท้าย)
- ข้อ 2. การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร (แนวปฏิบัติ 2 ข้อตามเอกสารแนบท้าย)
- ข้อ 3. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (แนวปฏิบัติ 6 ข้อตามเอกสารแนบท้าย)
- ข้อ 4. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (แนวปฏิบัติ 9 ข้อตามเอกสารแนบท้าย)
- ข้อ 5. การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (แนวปฏิบัติ 8 ข้อตามเอกสารแนบท้าย)
- ข้อ 6. การจัดหาหรือจัดให้มีการพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ (แนวปฏิบัติ 6 ข้อตามเอกสารแนบท้าย)
- ข้อ 7. การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (แนวปฏิบัติ 3 ข้อตามเอกสารแนบท้าย)
- ข้อ 8. การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง ให้มีการระบุเหตุการณ์ใด ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และความเป็นไปได้ในการเกิดผลกระทบ ตลอดจนผลต่อเนื่องจากการหยุดชะงักนั้นในแง่ของความมั่นคงปลอดภัยด้านสารสนเทศ
- ข้อ 9. การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (แนวปฏิบัติ 2 ข้อตามเอกสารแนบท้าย)

13.1.4 สรุปแนวปฏิบัติและการรายงานตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

ตามประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ พ.ศ. 2555 กำหนดวิธีการแบบปลอดภัย 3 ระดับ: พื้นฐาน กลาง และเคร่งครัด โดยมาตรฐานนี้ครอบคลุมด้านความลับ ความครบถ้วน และความพร้อมใช้งาน ผู้ดำเนินธุรกรรมทางอิเล็กทรอนิกส์ต้องปฏิบัติตามมาตรการตามประกาศ พร้อมพิจารณาความเสี่ยงที่ประเมินไว้

13.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐาน

13.2.1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐาน

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐาน (CII) และกฎหมายลำดับรอง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2568

วัตถุประสงค์หลัก

ในยุคเทคโนโลยี ภัยคุกคามไซเบอร์ส่งผลต่อทั้งองค์กรและโครงสร้างพื้นฐานของประเทศ รัฐบาลไทยจึงออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หรือพรบ.ไซเบอร์ฯ เพื่อรับมืออย่างเป็นระบบ เอกสารแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงไซเบอร์ พ.ศ. 2568 เป็นแนวทางสำหรับหน่วยงานรัฐและ CII ในการจัดทำมาตรฐานความมั่นคงตามกฎหมาย ถือเป็นเครื่องมือสำคัญในการขับเคลื่อนการดำเนินงานด้านนี้ มีวัตถุประสงค์หลัก ดังนี้

ประการแรก เอกสารฉบับนี้จัดทำขึ้นตาม พ.ร.บ. ไซเบอร์ฯ เพื่อกำหนดแนวทางปฏิบัติที่ชัดเจนให้หน่วยงานต่างๆ นำไปใช้ หากขาดแนวทางเหล่านี้ การปฏิบัติตามกฎหมายอาจไม่เป็นไปในทิศทางเดียวกันและส่งผลต่อความมั่นคงของประเทศ

ประการที่สอง เน้นการปกป้องข้อมูลและระบบสารสนเทศตามหลักการ CIA (Confidentiality, Integrity, Availability) เพื่อคุ้มครองสินทรัพย์ดิจิทัลสำคัญ โดยเฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญ (CII) เช่น ระบบพลังงาน สื่อสาร การเงิน สาธารณสุข และขนส่ง ซึ่งหากถูกโจมตีอาจส่งผลกระทบต่อประเทศ

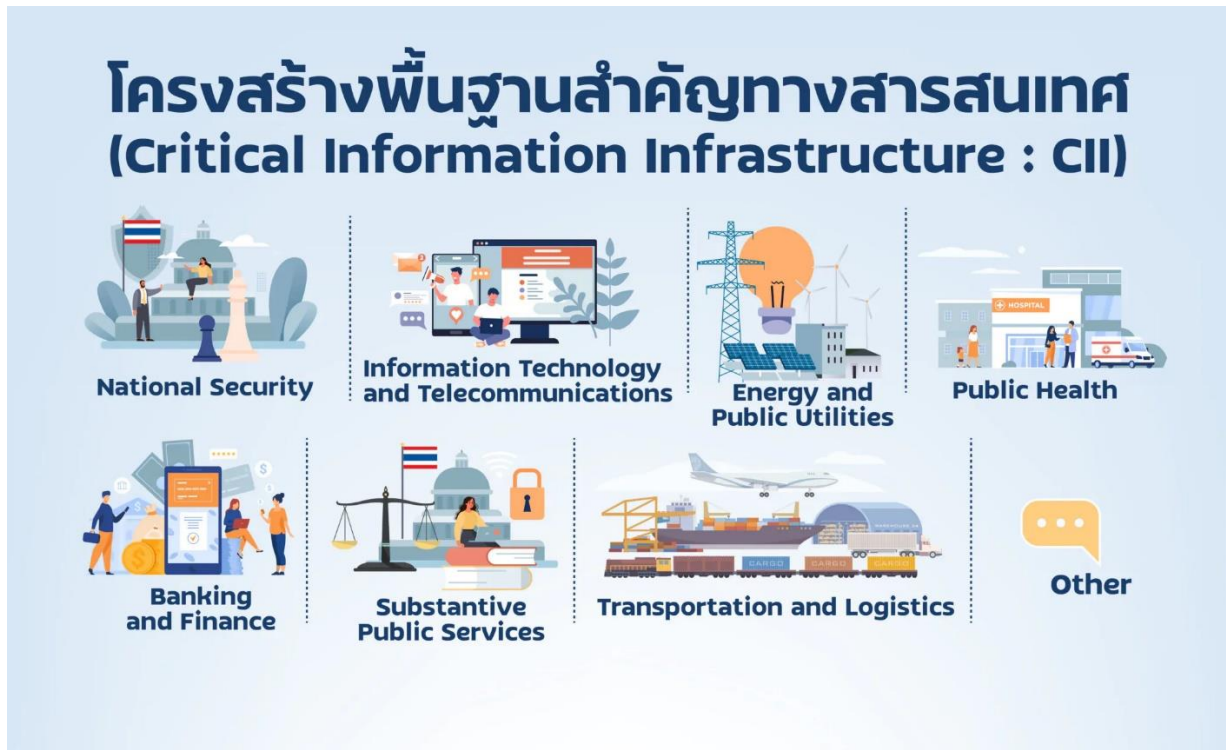
ประการที่สาม มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2568 ส่งเสริมให้เกิดแนวทางปฏิบัติร่วมกัน ลดความซ้ำซ้อน และช่วยให้องค์กรกลางอย่าง NCSA สามารถติดตามและประเมินสถานะไซเบอร์ของประเทศได้มีประสิทธิภาพมากขึ้น นอกจากนี้ ยังสนับสนุนการทำงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแลที่มีมาตรฐานเฉพาะ เช่น กสทช. เพื่อให้ทุกฝ่ายดำเนินการสอดคล้องกับมาตรฐานต่างๆ

13.2.2 หน่วยงานโครงสร้างพื้นฐาน (CII)

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศตามมาตรา 49 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านต่าง ๆ ดังรูป 13.1 ดังต่อไปนี้

- (1) ด้านความมั่นคงของรัฐ
- (2) ด้านบริการภาครัฐที่สำคัญ
- (3) ด้านการเงินการธนาคาร
- (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- (5) ด้านการขนส่งและโลจิสติกส์
- (6) ด้านพลังงานและสาธารณูปโภค
- (7) ด้านสาธารณสุข
- (8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม



รูป 13.1 หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) 8 ประเภท

(ที่มา: สกมช.)

หน่วยงาน CII เกิดขึ้นได้อย่างไร ?

ตามมาตรา 49 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีการกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โดย สกมช. กำหนดให้หน่วยงานควบคุมหรือกำกับดูแล ดำเนินการ 5 ขั้นตอน ดังนี้



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



- 1 การระบุกระบวนการที่สำคัญ**
โดยพิจารณาร่วมกับเจ้าของกระบวนการ หน่วยงานที่คาดว่าจะเป็หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ใช้งาน ผู้บริหาร หรือผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ทั้งภายในและภายนอกหน่วยงานควบคุมหรือกำกับดูแล
- 2 การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการที่สำคัญ**
โดยพิจารณาประเภทผลกระทบ พร้อมระดับผลกระทบ ที่อาจเกิดขึ้นกรณีไม่สามารถดำเนินการการกิจหรือบริการที่สำคัญ และส่งผลกระทบต่อชีวิตและทรัพย์สินของประชาชน
- 3 การประเมินเวลาการหยุดชะงักที่ยอมรับได้**
โดยพิจารณาจากระยะเวลาในการกู้คืนระบบ และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายที่สอดคล้องกับวามสำคัญของกระบวนการที่สำคัญ เพื่อกำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก
- 4 เลือกกระบวนการที่สำคัญและการระบุทรัพย์สินสารสนเทศ**
โดยเลือกกระบวนการที่สำคัญซึ่งมีค่า Maximum Tolerance Downtime : MTD น้อยที่สุด จากนั้น ให้พิจารณาทรัพย์สินสารสนเทศที่จำเป็นต่อการดำเนินกระบวนการที่สำคัญ ครอบคลุมคอมพิวเตอร์ ระบบคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์เครือข่าย ฐานข้อมูล หรืออื่น ๆ ในการให้บริการของระบบ
- 5 การระบุหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**
โดยพิจารณากำหนดหน่วยงานที่เป็นเจ้าของกรรมสิทธิ์ ของทรัพย์สินสารสนเทศ ในข้อ 4 เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

รูป 13.2 สกมช. กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการ 5 ขั้นตอน

(ที่มา: สกมช.)

โดย สกมช. กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลดำเนินการ 5 ขั้นตอน รูป 14.2 ดังนี้

- (1) การระบุกระบวนการที่สำคัญ
- (2) การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการที่สำคัญ

- (3) การประเมินเวลาการหยุดชะงักที่ยอมรับได้
- (4) เลือกระบบการที่สำคัญและการระบุทรัพยากรสารสนเทศ
- (5) การระบุหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

13.2.3 โครงสร้างของกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

โครงสร้างของประมวลแนวทางปฏิบัติและกรอบมาตรฐานที่กำหนดไว้ในเอกสารประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้มีความชัดเจนและครอบคลุมทุกมิติของการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ โดยแบ่งออกเป็นสองส่วนหลัก ได้แก่

ประมวลแนวทางปฏิบัติ ซึ่งเน้นไปที่การวางแผนและการบริหารจัดการ เช่น แผนการตรวจสอบ การประเมินความเสี่ยง และแผนการรับมือภัยคุกคาม

กรอบมาตรฐาน ซึ่งครอบคลุม 5 ฟังก์ชันหลักของความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การรับมือ (Respond), และการฟื้นฟู (Recover) การแบ่งโครงสร้างเช่นนี้ทำให้หน่วยงานต่างๆ มีกรอบการทำงานที่ชัดเจนในการพัฒนามาตรการป้องกันและรับมือภัยคุกคามได้อย่างครบวงจร

เอกสารฉบับนี้ได้กำหนดโครงสร้างประมวลแนวทางปฏิบัติและกรอบมาตรฐานอย่างมีระบบ โดยครอบคลุมทุกด้านที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

ส่วนประมวลแนวทางปฏิบัติมุ่งเน้นการวางแผนและการจัดการ เช่น การดำเนินการตรวจสอบ การประเมินความเสี่ยง และการจัดเตรียมแผนรับมือภัยคุกคาม

สำหรับกรอบมาตรฐาน ได้แบ่งออกเป็น 5 ฟังก์ชันหลัก ได้แก่ การระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond) และการฟื้นฟู (Recover) โครงสร้างดังกล่าวสนับสนุนให้หน่วยงานต่างๆ สามารถดำเนินงานด้านการพัฒนาและบังคับใช้มาตรการป้องกันและรับมือกับภัยคุกคามไซเบอร์ได้อย่างต่อเนื่องและมีประสิทธิภาพ

13.2.4 กรอบการดำเนินงานที่ครอบคลุม

ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปี 2568 มุ่งเน้นกระบวนการจัดทำและการดูแลเอกสารแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงไซเบอร์ เพื่อให้เอกสารมีความถูกต้อง ทันสมัย และนำไปใช้ได้จริง

เอกสารด้านความมั่นคงปลอดภัยสารสนเทศแบ่งเป็น 6 ประเภท ได้แก่ นโยบาย, ขั้นตอนปฏิบัติ/ระเบียบปฏิบัติ, กระบวนการ/แนวทาง, มาตรฐาน, แผน และเอกสารสนับสนุน การจำแนกนี้ช่วยให้เข้าใจบทบาทและลำดับอำนาจหน้าที่ของแต่ละประเภท เพื่อลดความสับสนและให้การดำเนินงานสอดคล้องกับเป้าหมายองค์กร

13.2.5 กระบวนการจัดทำรายงานที่ระบุในประกาศ

วงจรชีวิตของเอกสาร (Document Lifecycle) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2568

- เริ่มจากการศึกษากฎหมายและกฎระเบียบที่เกี่ยวข้อง พร้อมขอสนับสนุนจากผู้บริหารเพื่อความถูกต้องและทรัพยากรที่เหมาะสม
- ร่างเอกสารให้ตรงกับบริบทและความเสี่ยงของหน่วยงาน ไม่ใช่วิธีคัดลอกมาตรงๆ เพื่อให้สามารถนำไปใช้ได้จริง
- เปิดรับความคิดเห็นจากผู้มีส่วนได้ส่วนเสียทุกฝ่าย เพื่อให้เอกสารมีความครอบคลุมและปฏิบัติได้จริง
- อนุมัติและสื่อสารเอกสารอย่างเป็นทางการโดยคำนึงถึงระดับความลับ เพื่อให้ทุกคนเข้าใจและปฏิบัติตาม
- ติดตามประสิทธิผล ปรับปรุงเอกสารเมื่อมีความเปลี่ยนแปลงสำคัญ เพื่อให้แนวทางปฏิบัติทันสมัยและเหมาะสมอยู่เสมอ

13.2.6 เหตุผลความจำเป็นในการดำเนินการ

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2568 ที่ครอบคลุมนี้มาจากหลายปัจจัย ได้แก่:

- การกำหนดประเภทเอกสารและมาตรฐานกระบวนการอย่างชัดเจน ช่วยให้ทุกหน่วยงานมีแนวทางเดียวกัน ลดความสับสนและประสานงานได้ดีขึ้น
- การอนุมัติและทบทวนโดยผู้บริหารระดับสูง ยืนยันถึงความมุ่งมั่นขององค์กรในความมั่นคงปลอดภัยไซเบอร์ และเสริมสร้างความน่าเชื่อถือ
- เน้นการปรับปรุงตามสถานการณ์จริง กลยุทธ์ใหม่ และเทคโนโลยี เพื่อให้สามารถรองรับภัยคุกคามที่เปลี่ยนแปลงได้ทันเวลา

- กระบวนการที่เปิดโอกาสให้บุคลากรมีส่วนร่วม การสื่อสาร และการฝึกอบรมต่อเนื่อง สร้างวัฒนธรรมความมั่นคงปลอดภัยที่เข้มแข็ง

บทสรุปส่วนที่ 1 และ ส่วนที่ 2 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกาศนี้มีบทบาทสำคัญในการสร้างมาตรฐานความมั่นคงปลอดภัยไซเบอร์ของไทย ช่วยคุ้มครองสินทรัพย์ดิจิทัล และเตรียมพร้อมรับมือภัยคุกคาม หากหน่วยงานไม่ปฏิบัติตามจะเพิ่มความเสี่ยงต่อข้อมูลสำคัญ การดำเนินการตามกรอบนี้อย่างจริงจังจึงเป็นพื้นฐานสำคัญในการจัดการและปกป้องสินทรัพย์ดิจิทัลของประเทศ

13.3 แนวปฏิบัติการเชิงลึกตามมาตรฐานของ NIST CSF

โครงสร้างแนวปฏิบัติเชิงลึกตามกรอบ 5 ด้านของ NIST CSF2.0 (Cybersecurity Framework) เอกสารแนบท้ายประกาศสภ. พ.ศ. 2568 ครอบคลุมมาตรการสำคัญต่างๆ ตามกรอบมาตรฐาน 5 หัวข้อหลัก (Identify, Protect, Detect, Respond, Recover) ซึ่งแต่ละหัวข้อมีความเชื่อมโยงและเสริมซึ่งกันและกันอย่างเป็นระบบ สรุปได้ดังนี้

13.3.1 การระบุความเสี่ยงที่อาจเกิดขึ้น (Identify)

มุ่งความสำคัญของการทำความเข้าใจสินทรัพย์และสภาพแวดล้อมทางไซเบอร์ขององค์กร

แนวทางการจัดการทรัพย์สิน: กำหนดให้หน่วยงานดำเนินการจัดทำและดูแลทะเบียนทรัพย์สินอย่างละเอียด ซึ่งครอบคลุมข้อมูลฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย บุคลากร และสถานที่ การบริหารจัดการทรัพย์สินเป็นองค์ประกอบพื้นฐานของการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากช่วยระบุสินทรัพย์สำคัญที่ต้องดูแล นอกจากนี้ยังควรมีมาตรการจัดการกับ Shadow IT (เทคโนโลยีสารสนเทศที่ไม่ได้รับการควบคุม) ซึ่งอาจก่อให้เกิดความเสี่ยงที่ไม่สามารถประเมินได้ การดำเนินการนี้มีวัตถุประสงค์เพื่อสร้างภาพรวมที่ถูกต้องเกี่ยวกับสิ่งที่ต้องปกป้อง และหากขาดข้อมูลดังกล่าว องค์กรอาจไม่สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

แนวทางการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์: สรุปกระบวนการประเมินความเสี่ยง โดยนิยามความเสี่ยงเป็นฟังก์ชันของโอกาสเกิดและผลกระทบ กำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ต่างกันตามประเภทธุรกิจ และเน้นให้หน่วยงานเข้าใจความเสี่ยงจริงเพื่อจัดสรรทรัพยากรอย่างเหมาะสมและรับมือภัยคุกคามสำคัญ

13.3.2 มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

มุ่งเน้นการวางมาตรการเพื่อลดโอกาสการเกิดภัยคุกคาม

แนวทางการควบคุมการเข้าถึง: กำหนดมาตรการเข้มงวดสำหรับบุคลากร อุปกรณ์ และอินเทอร์เน็ตที่ได้รับอนุญาต รวมถึง PAM การแบ่งการควบคุมภายใน-ภายนอก และระบบบันทึกส่วนกลาง เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

แนวทางการทำให้ระบบมีความแข็งแกร่ง (System Hardening): มุ่งเน้นการลดช่องโหว่ของระบบปฏิบัติการ แอปพลิเคชัน เครือข่าย และฐานข้อมูล โดยใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) และการจัดการการเปลี่ยนแปลง (Change Management) ที่รัดกุม ความจำเป็นคือการลด “พื้นผิวการโจมตี” (Attack Surface) ขององค์กร ซึ่งจะช่วยลดโอกาสที่ผู้ไม่ประสงค์ดีจะใช้ช่องโหว่เพื่อเข้าถึงระบบ

แนวทางการทำให้ระบบแข็งแกร่ง (System Hardening) คือการลดช่องโหว่ของระบบด้วยมาตรฐานการกำหนดค่าความมั่นคงปลอดภัยและการจัดการเปลี่ยนแปลงอย่างเข้มงวด เพื่อลด “พื้นผิวการโจมตี” และลดความเสี่ยงจากภัยคุกคาม

แนวทางการจัดการการเชื่อมต่อระยะไกล (Remote Connection): กำหนดนโยบายและมาตรการเพื่อความปลอดภัยสำหรับการทำงานระยะไกล ครอบคลุมการใช้อุปกรณ์ต่างๆ และการกำหนดระดับการเข้าถึง ป้องกันจุดอ่อนในการเชื่อมต่อระยะไกลจากการโจมตี

13.3.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

มุ่งเน้นการตรวจสอบและเฝ้าระวังภัยคุกคาม หน่วยงานต้องตั้งกลไกตรวจจับและเฝ้าระวังภัยไซเบอร์ รวมถึงการจัดประเภท วิเคราะห์เหตุการณ์ และระบุภัยคุกคามต่อบริการสำคัญโดยใช้ข้อมูลจากหลายแหล่ง (Log, IDS/IPS, DLP, SIEM) เพื่อให้พบความผิดปกติได้เร็วและรับมือก่อนเกิดความเสียหาย

13.3.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มุ่งเน้นการตอบสนองอย่างรวดเร็วและมีประสิทธิภาพเมื่อเกิดเหตุการณ์ แผนรับมือภัยคุกคามไซเบอร์ (เอกสารแนบ 3): ระบุโครงสร้างและหน้าที่ของทีมรับมือเหตุการณ์ ขั้นตอนตอบสนอง และการเก็บรักษาหลักฐาน โดยมีเป้าหมายเพื่อจำกัดความเสียหายและกำจัดภัยคุกคามอย่างรวดเร็ว

แนวทางการจัดทำแผนการสื่อสารในภาวะวิกฤต (เอกสารแนบ 13): กำหนดขั้นตอนสื่อสารภายใน-ภายนอก การตั้งทีมสื่อสาร โฆษก และช่องทางเผยแพร่ เพื่อควบคุมการรับรู้ของสาธารณะ ลดความตื่นตระหนก และรักษาชื่อเสียงองค์กร

13.3.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

มุ่งเน้นการกู้คืนระบบสู่สภาวะปกติ แนวทางการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) กำหนดให้มีการจัดทำ BCP เพื่อให้หน่วยงานสามารถให้บริการที่สำคัญต่อไปได้แม้จะเกิดการหยุดชะงักจากภัยคุกคามไซเบอร์ รวมถึงการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) เพื่อกำหนดระยะเวลาสูงสุดที่ยอมรับได้ (MTD, RTO, RPO) และระบุทรัพยากรที่จำเป็นในการกู้คืน ความจำเป็นคือการ “รับประกันความต่อเนื่อง” ของการดำเนินงานและบริการสำคัญของประเทศ

13.3.6 กลไกการขับเคลื่อน การบังคับใช้ และการรายงาน

เอกสารประกาศสภมช. พ.ศ. 2568 นี้ไม่ได้เป็นเพียงแค่ชุดคำแนะนำ แต่เป็นกรอบที่ได้รับการสนับสนุนด้วยกลไกการขับเคลื่อนและการบังคับใช้ที่สำคัญ ประกอบด้วย

การตรวจสอบ (Audit) : หน่วยงานต้องมีการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้งโดยผู้ตรวจสอบที่ได้รับอนุมัติ เพื่อประเมินประสิทธิผลและความเหมาะสมของมาตรการควบคุม นี่คือนโยบายสำคัญในการรับรองว่าแนวทางปฏิบัติเหล่านี้ถูกนำไปใช้อย่างถูกต้องและมีประสิทธิภาพ

การฝึกซ้อม (Exercise) : กำหนดให้มีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้งสำหรับแผนสำคัญต่างๆ เพื่อทดสอบความพร้อมของบุคลากรและแผนงานจริง การฝึกซ้อมช่วยให้หน่วยงานระบุจุดอ่อนและปรับปรุงแนวทางการรับมืออย่างต่อเนื่อง

การรายงาน: กำหนดให้หน่วยงาน CII ต้องส่งผลสรุปรายงานการประเมินความเสี่ยงและรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อ NCSA ภายใน 30 วันนับจากวันที่ดำเนินการแล้วเสร็จ กลไกการรายงานนี้ทำให้ NCSA สามารถติดตามสถานะภาพรวมของความมั่นคงปลอดภัยไซเบอร์ของประเทศได้

13.3.7 ความสำคัญและความจำเป็นในการดำเนินการ

การดำเนินการตามเอกสาร “ประกาศสภมช. พ.ศ. 2568” หรือ “ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” ฉบับนี้จึงมีความสำคัญและจำเป็นอย่างยิ่งยวด ดังนี้:

การป้องกันความเสียหาย: การปฏิบัติตามแนวทางไซเบอร์ช่วยลดผลกระทบทั้งทางตรงและทางอ้อม

สร้างความเชื่อมั่น: รักษาความมั่นคงปลอดภัยของข้อมูลและบริการ เพื่อเสริมความไว้วางใจของประชาชน

ความพร้อมรับมือ: มีแผนรับมือและดำเนินงานต่อเนื่อง ช่วยตอบสนองเหตุฉุกเฉินได้รวดเร็วและมีประสิทธิภาพ

มาตรฐานสากล: แนวทางนี้สอดคล้องกับมาตรฐาน เช่น ISO และ NIST ยกระดับความมั่นคงประเทศ

ความร่วมมือ: การแบ่งปันข้อมูลภัยคุกคามระหว่างหน่วยงานช่วยเพิ่มศักยภาพในการป้องกันร่วมกัน

ดังนั้น การดำเนินการตามเอกสารนี้เป็นสิ่งจำเป็นสำหรับทุกหน่วยงาน เพื่อปกป้องสินทรัพย์ดิจิทัล เสริมสร้างความมั่นคงโครงสร้างพื้นฐาน และรับมือภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง

13.3.8 สรุปแนวปฏิบัติการ การย้าย การกู้คืน และการรายงานสำหรับหน่วยงานโครงสร้างพื้นฐาน

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐาน หรือ CII เนื้อหาส่วนนี้นำเสนอแนวทางและมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและไซเบอร์สำหรับหน่วยงานรัฐและโครงสร้างพื้นฐานสำคัญ หรือ CII โดยมุ่งปกป้องข้อมูลและระบบตามหลัก CIA สอดคล้องกับ พ.ร.บ. ไซเบอร์ฯ ปี 2562 เพื่อให้หน่วยงานดำเนินการตามมาตรฐานเดียวกัน ลดความเสี่ยงและผลกระทบจากภัยคุกคาม พร้อมทั้งส่งเสริมการประสานงานกับองค์กรกำกับดูแลต่างๆ ภายใต้กรอบอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

13.4 สารสนเทศส่วนบุคคล

สารสนเทศส่วนบุคคลหรือข้อมูลส่วนบุคคล (Personal data) จะใช้แนวปฏิบัติการตามมาตรการรักษาความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองทั่วไปแห่งสหภาพยุโรป หรือ GDPR (General Data Protection Regulation) พรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) และกฎหมายลำดับรอง

13.4.1 ภาพรวม

มาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล หมายถึง มาตรการที่กำหนดขึ้นเพื่อรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล เพื่อป้องกันการสูญหาย, เข้าถึง, ใช้, เปลี่ยนแปลง, แก้ไข หรือเปิดเผยโดยปราศจากอำนาจหรือโดยมิชอบ โดยต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) โดยผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องมีมาตรการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้ ให้สอดคล้องกับพระราชบัญญัติฉบับนี้ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ที่ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องจัดให้มีมาตรการความมั่นคงปลอดภัยตลอดวงจรชีวิตข้อมูลส่วนบุคคล ดังรูป 13.3 ซึ่งครอบคลุมมาตรการด้านการบริหารจัดการ (Administrative Measure) มาตรการด้านเทคนิค (Technical Measure) และมาตรการด้านกายภาพ (Physical Measure)

13.4.2 สารสำคัญของ PDPA

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลของไทย (Personal Data Protection: PDPA) ได้กำหนดให้การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล (หรือการประมวลผลข้อมูลส่วนบุคคล) ของเจ้าของข้อมูลซึ่งเป็นบุคคลธรรมดา จะต้องมีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้ง เนื่องจาก PDPA มีวัตถุประสงค์เพื่อทำให้การประมวลผลข้อมูลส่วนบุคคลนั้นอยู่บนพื้นฐานตามกฎหมายโดยใช้หลักการสำคัญของการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้ข้อมูลส่วนบุคคลเช่นเดียวกันกับ General Data Protection Regulation (GDPR) รูป 13.4 ซึ่งเป็นเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ดังนั้น ทุกหน่วยงานทั้งภาครัฐเอกชน รวมทั้งสถานศึกษา ซึ่งไม่อยู่ในรายชื่อหน่วยงานที่ได้รับการยกเว้นตามพรบ.ฉบับนี้ จึงจำเป็นต้องเตรียมความพร้อมในการดำเนินการให้สอดคล้องกับ พ.ร.บ. ดังกล่าว ซึ่งมีผลบังคับใช้ ในวันที่ 31 พฤษภาคม 2564



รูป 13.3 วงจรชีวิตข้อมูลส่วนบุคคล

(ที่มา: สคส.)



รูป 13.4 หลักการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR

(ที่มา: สคส.)

13.4.3 นิยามศัพท์ที่เกี่ยวข้อง

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ทั้งนี้ มีผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ดังนี้

“ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” (Data Processor) หมายความว่า บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

13.4.4 สิ่งที่จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ (Privacy Notice)

- แจ้งวัตถุประสงค์ของการเก็บข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย แจ้งให้เจ้าของข้อมูลให้ทราบถึงเหตุผลและความจำเป็นตามกฎหมาย รวมทั้งผลกระทบที่เป็นไปได้จากการไม่ให้อข้อมูลส่วนบุคคล ต้องมีการกำหนดระยะเวลาใน การเก็บรวบรวมอย่างชัดเจน ประเภทของบุคคล หรือหน่วยงานซึ่งข้อมูลส่วนบุคคลอาจจะถูกเปิดเผย ข้อมูลของบุคคลหรือหน่วยงานที่เป็นผู้ควบคุมข้อมูล ส่วนบุคคล/สถานที่ติดต่อ/วิธีการติดต่อ

- ข้อมูลที่ห้ามเก็บ และข้อยกเว้น กรณีเป็นข้อมูลอ่อนไหว (Sensitive Personal Data) หากจะเก็บข้อมูลต้องขอความยินยอม (Consent) ได้แก่ เชื้อชาติ เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ, ข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูล ตามที่คณะกรรมการประกาศกำหนด

- กรณีข้อยกเว้นหรือในการเก็บข้อมูลสามารถกระทำได้โดยไม่ต้องขอความยินยอม (Consent) ได้แก่ วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์, ประโยชน์สาธารณะด้านสาธารณสุข, คัมครอง แรงงาน, ประกันสังคม, หลักประกันสุขภาพแห่งชาติ, ศึกษาวิจัยทางวิทยาศาสตร์, ประวัติศาสตร์ และสถิติ

13.4.5 ฐานการประมวลผลข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ฐานกฎหมาย PDPA คือ "หลักการที่กฎหมาย PDPA กำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องมีเหตุอันชอบธรรมรองรับ" ซึ่งหลักการดังกล่าวมี 7 ประการ ได้แก่ ฐานความยินยอม, ฐานพันธะสัญญา, ฐานหน้าที่ตามกฎหมาย, ฐานประโยชน์ที่สำคัญต่อชีวิต, ฐานภารกิจของรัฐ, ฐานประโยชน์อันชอบธรรม, และฐานข้อมูลที่เปิดเผยต่อสาธารณะ องค์กรต้องเลือกฐานกฎหมายที่เหมาะสมกับวัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคล และต้องดำเนินการตามสิทธิของเจ้าของข้อมูลตามกฎหมาย

อย่างไรก็ดี ฐานความยินยอม นั้น ถือเป็นฐานที่มีความไม่มั่นคงมากที่สุดจากบรรดาฐานการประมวลผลข้อมูลทั้งหมด จึงควรพิจารณาเลือกใช้เป็นลำดับสุดท้าย เนื่องจากหากเจ้าของข้อมูลไม่ยินยอม ผู้ประมวลผลข้อมูลก็จะมีสิทธิ อีกทั้งเจ้าของข้อมูลสามารถขอเพิกถอนความยินยอมได้ตลอดเวลาด้วย

13.4.6 สิทธิของเจ้าของข้อมูลส่วนบุคคล

มีจำนวน 8 สิทธิ ได้แก่

- (1) สิทธิที่จะได้รับการแจ้งให้ทราบ (Right to be informed)
- (2) สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- (3) สิทธิในการได้รับและโอนถ่ายข้อมูล (Right to data portability)
- (4) สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- (5) สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล (Right to erasure / Right to be forgotten)
- (6) สิทธิในการเพิกถอนความยินยอม (Right to withdraw consent)
- (7) สิทธิในการขอระงับการใช้ข้อมูล (Right to restrict processing)
- (8) สิทธิขอให้แก้ไขข้อมูล (Right of rectification)

วัตถุประสงค์

- ค้ำครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล
- ป้องกันการละเมิดข้อมูลส่วนบุคคล

หลักการ

“ความมั่นคงปลอดภัย” หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจาก อำนาจหรือโดยมิชอบ

ข้อ 4 ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าวอย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้ รูป 13.5

(1) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(2) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจ รวมถึง

มาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิด และผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รูป 14.5

(3) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษา ความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ(information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น การตรวจสอบและเฝ้า ระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและ เหตุการณ์ละเมิดข้อมูลส่วนบุคคล และการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ ละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

(4) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ให้อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกัน หรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ประกอบกัน

(5) สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษา ความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบ สารสนเทศที่เกี่ยวข้องกับการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์ จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์และแอป พลิเคชัน อย่างเหมาะสมตามระดับ ความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควร ประกอบด้วยมาตรการ ป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่ มาตรการ บางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

(6) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยการดำเนินการดังต่อไปนี้ที่เหมาะสมตามระดับความ เสี่ยง โดยคำนึงถึงความจำเป็นในการเข้าถึงและใช้งาน ตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และ เปิดเผยข้อมูลส่วนบุคคล การรักษา ความมั่นคงปลอดภัยตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไป ได้ในการดำเนินการประกอบกัน

หลักการสำคัญของ...

มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

กรณีผู้ควบคุมข้อมูลส่วนบุคคลได้รับการยกเว้นการใช้บังคับ PDPA

ผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลที่ไม่อยู่ภายใต้บังคับของ PDPA ไม่ว่าทั้งหมดหรือบางส่วน ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานตามประกาศ กคส. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับ พ.ศ. 2566

ซึ่งมีหลักการสำคัญที่ต้องดำเนินการอย่างน้อยดังต่อไปนี้...

- 1** จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม อันประกอบด้วย มาตรการเชิงองค์กร มาตรการเชิงเทคนิค และมาตรการทางกายภาพ โดยคำนึงถึงความสามารถในการสร้างไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคลตามระดับความเสี่ยง

 - มีมาตรการในการกำหนดสิทธิในการเข้าถึงและใช้งาน
 - การตรวจสอบย้อนหลังการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้งาน เป็นต้น
 - มีมาตรการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยแก่บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน
 - ควรมีมาตรการที่ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ หรือมีการแฝงข้อมูล หรือมีการเข้ารหัส เป็นต้น
- 2** ต้องมีการทบทวนมาตรการรักษาความมั่นคงปลอดภัย เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย
- 3** ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือบุคคลหรือมีบุคคลที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้

(ข้อมูลเดือนกุมภาพันธ์ 2567)

ที่มา : ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับการยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับ พ.ศ. 2566 ข้อ 4 ข้อ 5 ข้อ 6 และข้อ 7

pdpc
กคส.

รูป 13.5 หลักการสำคัญของมาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลตาม PDPA

(ที่มา: สคส.)

(ก) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน (identity proofing and authentication) และ การอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งาน (authorization) ที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น (need-to-know basis) ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น (principle of least privilege)

(ข) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม ซึ่งอาจรวมถึง การลงทะเบียนและการถอนสิทธิผู้ใช้งาน (user registration and de-registration) การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (user access provisioning) การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ (management of privileged access rights) การบริหารจัดการข้อมูลความลับสำหรับ การพิสูจน์ตัวตนของผู้ใช้งาน (management of secret authentication information of users) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (removal or adjustment of access rights)

(ค) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกัน การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งรวมถึงกรณีที่เป็น การกระทำนอกเหนือบทบาทหน้าที่ที่ได้รับมอบหมาย ตลอดจนการลักลอบ ทำสำเนาข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และการลักขโมยอุปกรณ์จัดเก็บ หรือประมวลผลข้อมูลส่วนบุคคล

(ง) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง แก้ไข หรือลบ ข้อมูลส่วนบุคคล (audit trails) ที่เหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(7) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูล ส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มี การปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และ ความเป็นไปได้ในการดำเนินการประกอบกัน



! ไม่ควรเปิดเผย !

ข้อมูลส่วนบุคคลเกินความจำเป็น

ในกรณีที่มีความจำเป็นในการเผยแพร่หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน ควรแทนตัวเลขของข้อมูลส่วนบุคคลด้วยการเติม X 5 ตัวเป็นอย่างน้อย หรือ **“X5”** เพื่อพรางไม่ให้มีการระบุตัวได้โดยง่าย และเป็นการป้องกันการนำข้อมูลส่วนบุคคลของประชาชนไปใช้โดยมิชอบ

การพรางหรือแทนข้อมูลส่วนบุคคลด้วยตัวอักษร X 5 ตัว เป็นอย่างน้อย เช่น



เบอร์โทรศัพท์

ควรแทนตัวเลขด้านหน้าหรือด้านหลังด้วย X5

ตัวอย่าง: XX XXXX 5678
08 123X XXXX

เลขบัตรประชาชน

ควรแทนด้วย X 4 ตัวด้านหน้าและหลัง

ตัวอย่าง: X XXX5 6789X XX X



รูป 13.6 การอำพรางข้อมูลส่วนบุคคลเป็นมาตรการหนึ่งในการรักษาความลับ

(ที่มา: สคส.)

ข้อ 5 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามข้อ 4 เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคง ปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับ

หน่วยงานหรือกิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็น ต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยตามวรรคหนึ่ง เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยง ที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

ข้อ 6 ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล ส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูล ส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำตามข้อ 4 โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและ วัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบ จากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

ข้อ 7 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

13.4.7 สรุปแนวปฏิบัติการและการรายงานสารสนเทศส่วนบุคคล

กล่าวโดยสรุปสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือ PDPA ฉบับนี้ มีไว้เพื่อคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล และป้องกันการละเมิดข้อมูลส่วนบุคคล ทุกหน่วยงานตามประกาศ จำเป็นต้องมีมาตรการหลักเพื่อการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล ประกอบด้วย (1) มาตรการบริหารจัดการ: กำหนดนโยบายและขั้นตอนการปฏิบัติงาน เช่น การกำหนดสิทธิการเข้าถึง, การบริหารจัดการผู้ใช้งาน, การกำหนดหน้าที่ความรับผิดชอบ, และการตรวจสอบย้อนหลัง (2) มาตรการทางเทคนิค: การรักษาความมั่นคงปลอดภัยของระบบ เช่น การพิสูจน์ตัวตน, การอนุญาตการเข้าถึง, และการตรวจสอบการเข้าถึงข้อมูล และ (3) มาตรการทางกายภาพ การควบคุมการเข้าถึงพื้นที่ที่จัดเก็บข้อมูล เช่น การจำกัดการเข้าใช้งานเฉพาะผู้ที่เกี่ยวข้อง, การควบคุมการเข้าถึงอุปกรณ์ที่จัดเก็บข้อมูล กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

องค์กรต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลตามประกาศ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งกำหนดรายละเอียดของมาตรการรักษาความมั่นคงปลอดภัยที่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องปฏิบัติ โดยต้องดำเนินการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม เพื่อให้สอดคล้องกับ ข้อกำหนดของกฎหมาย และการดำเนินการตามมาตรฐานนี้เป็นหน้าที่ตามกฎหมายที่ผู้ควบคุมและประมวลผล ข้อมูลส่วนบุคคลต้องปฏิบัติตาม เพื่อหลีกเลี่ยงเหตุแห่งการรั่วไหลข้อมูลส่วนบุคคล รูป 13.7



รูป 13.7 สาเหตุหลักของการรั่วไหลข้อมูลส่วนบุคคล

(ที่มา: สคส.)

สรุปแนวปฏิบัติมาตรการรักษาความมั่นคงปลอดภัยด้านข้อมูลส่วนบุคคลตาม PDPA กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) กำหนดให้องค์กรและผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการที่ครอบคลุมทั้งด้านการบริหารจัดการ ทางเทคนิค และทางกายภาพ เพื่อป้องกันการเข้าถึง ใช้ เปิดเผย หรือแก้ไขข้อมูลโดยมิชอบ พร้อม

กำหนดให้มีการทบทวนมาตรการอย่างต่อเนื่องและสร้างความตระหนักรู้ในองค์กร เพื่อคุ้มครองสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลอย่างมีประสิทธิภาพตามมาตรฐานกฎหมาย

13.5 สรุป

เนื้อหาในบทนี้เน้นการสร้างมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตาม PDPA โดยกำหนดให้มีมาตรการทั้งด้านการบริหารจัดการ ทางเทคนิค และทางกายภาพ เพื่อป้องกันการเข้าถึง ใช้ หรือเปิดเผยข้อมูลโดยมิชอบ พร้อมทั้งเน้นการทบทวนและสร้างความตระหนักรู้ให้กับองค์กรอย่างต่อเนื่อง เพื่อคุ้มครองสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลให้เป็นไปตามมาตรฐานกฎหมายที่กำหนด

13.6 บทวิเคราะห์และมุมมองเชิงวิชาการ: “แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถใช้ประโยชน์ได้”

บทที่ 13 ของเอกสารคำสอน หัวข้อ *แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถใช้ประโยชน์ได้* ถือเป็นการบูรณาการองค์ความรู้ด้าน กฎหมายไซเบอร์ของไทย (พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544, พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พ.ร.บ. คຸ່ມครองข้อมูลส่วนบุคคล พ.ศ. 2562) เข้ากับกรอบมาตรฐานสากล เช่น NIST Cybersecurity Framework (CSF) และ ISO/IEC 27001 เพื่อสร้างมาตรการที่สามารถนำไปปฏิบัติได้จริงในระดับองค์กรและโครงสร้างพื้นฐานสำคัญ (CII) มีบทวิเคราะห์และมุมมองเชิงวิชาการดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

- มาตรการตามกฎหมายธุรกรรมอิเล็กทรอนิกส์: จัดระดับการป้องกัน 3 ชั้น (พื้นฐาน, กลาง, เคร่งครัด) ครอบคลุม 11 มาตรการ เช่น นโยบายความมั่นคงปลอดภัย, การควบคุมการเข้าถึง, การจัดการเครือข่าย, การบริหารเหตุการณ์, และการ audit
- หน่วยงานโครงสร้างพื้นฐาน (CII): ต้องปฏิบัติตามกรอบของ พ.ร.บ. ไซเบอร์ฯ พ.ศ. 2562 โดยยึดหลักการ Identify – Protect – Detect – Respond – Recover ครอบคลุมทั้งการประเมินความเสี่ยง, การป้องกัน, การเฝ้าระวัง, การตอบสนอง และการฟื้นฟู
- แนวปฏิบัติการเชิงลึก: เน้น system hardening, PAM (Privileged Access Management), remote connection security, SIEM และ incident response plan ที่มีการสื่อสารเชิงวิกฤติอย่างเป็นระบบ
- การคุ้มครองข้อมูลส่วนบุคคล (PDPA): อธิบายสิทธิ 8 ประการของเจ้าของข้อมูล, privacy notice, ฐานการประมวลผล และมาตรการด้านองค์กร-เทคนิค-กายภาพ ซึ่งเทียบเคียงกับ GDPR

2) มุมมองเชิงวิชาการและความก้าวหน้าปัจจุบัน

1. จาก Compliance → Cyber Resilience เดิมมาตรการถูกมองว่าเป็นภาระทางกฎหมาย ปัจจุบันแนวคิด Cyber Resilience มุ่งสร้าง *ความพร้อมต่อภัยคุกคาม* และ *การฟื้นฟูเร็ว* แทนการทำเพื่อตามกฎหมายเท่านั้น

2. **Integration: ISO 27001 + NIST CSF + PDPA** การสอนควรให้ผู้เรียนเข้าใจว่า การบูรณาการหลายมาตรฐาน (ISO สำหรับ ISMS, NIST สำหรับโครงสร้างการปฏิบัติ, PDPA สำหรับ data protection) คือทางรอดขององค์กร
3. **จาก Manual Audit → Continuous Compliance** ใช้ GRC platforms และ AI-driven audit tools ในการตรวจสอบนโยบาย/การเข้าถึงอย่างอัตโนมัติและ real-time
4. **จาก Incident Response → Threat Hunting & Intelligence Sharing** นอกจาก IR Plan องค์กรควรสอนการทำ threat hunting, CTI sharing (ผ่านระบบเช่น TAXII/STIX) เพื่อให้สอดคล้องกับแนวคิด proactive security
5. **PDPA → Privacy by Design** จากการทำ privacy notice ภายหลัง ปัจจุบันควรสอนแนวคิด Privacy by Design (PbD) ที่ฝังการคุ้มครองข้อมูลไว้ตั้งแต่การออกแบบระบบ

3) ประสบการณ์และการสอดแทรกเชิงการสอน

ในประสบการณ์ทางวิชาชีพและการสอน ผู้สอนมักพบว่า นักศึกษาเข้าใจกฎหมายแยกส่วน เช่น PDPA ≠ Cybersecurity Act แต่ไม่เห็นการบูรณาการ เมื่อออกแบบกิจกรรม *policy mapping exercise* ให้นักศึกษาเชื่อมโยงกฎหมายไทยกับ ISO/NIST แล้วจำลอง policy จริง จะช่วยให้ผู้เรียนเข้าใจว่าการออกแบบมาตรการคือ **ทั้งกฎหมาย + เทคนิค + บริหารจัดการ**

กล่าวโดยสรุป บทนี้แสดงให้เห็นว่า **มาตรการไซเบอร์ที่ใช้ประโยชน์ได้** ต้องอิงทั้งกฎหมายไทย (พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์, พ.ร.บ. ไซเบอร์, พ.ร.บ. PDPA) และมาตรฐานสากล (ISO 27001, NIST CSF, GDPR) การเรียนการสอนควรขับเคลื่อนจาก compliance-based → resilience-based พร้อมทั้งบูรณาการ Privacy by Design, AI-driven monitoring และ threat intelligence เพื่อสร้างบุคลากรที่พร้อมทำงานในโลกจริง

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายมาตรการรักษาความมั่นคงปลอดภัย 3 ระดับ ตามกฎหมายธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2555

แนวคำตอบ: ระดับพื้นฐาน = นโยบาย, Log, สำรองข้อมูล / ระดับกลาง = เพิ่มการตรวจสอบ, การอบรม / ระดับ
เคร่งครัด = มาตรการกายภาพ, การทดสอบ, BCP

ข้อ 2. วิเคราะห์ความสำคัญของ CII ต่อความมั่นคงของประเทศ

แนวคำตอบ: CII = ระบบพลังงาน การเงิน ขนส่ง สุขภาพ ฯลฯ หากถูกโจมตี → กระทบเศรษฐกิจและความ
มั่นคง

ข้อ 3. อธิบายกรอบ NIST CSF และยกตัวอย่างการนำไปใช้ในองค์กร

แนวคำตอบ: 5 Functions (Identify, Protect, Detect, Respond, Recover) → ใช้ใน Risk Assessment,
SOC, Incident Response

ข้อ 4. อธิบายสิทธิของเจ้าของข้อมูลส่วนบุคคลตาม PDPA

แนวคำตอบ: 8 สิทธิ เช่น สิทธิรับรู้ สิทธิคัดค้าน สิทธิขอลบ สิทธิเข้าถึงข้อมูล ฯลฯ

ข้อ 5. เสนอแผนตอบสนองเมื่อเกิดการโจมตี Ransomware ในองค์กร

แนวคำตอบ: ตัดการเชื่อมต่อ → กักกัน → แจ้งผู้เกี่ยวข้อง → ฟื้นฟูจาก Backup → รายงานต่อ NCSA/
เจ้าของข้อมูล

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. มาตรการความมั่นคงปลอดภัยทางไซเบอร์ตามกฎหมายธุรกรรมอิเล็กทรอนิกส์ พ.ศ.2555 แบ่งเป็นกี่ระดับ

ก. 2

ข. 3

ค. 4

ง. 5

เฉลย: ข

ข้อ 2. ข้อใดไม่ใช่ตัวอย่างของ CII

- ก. โรงไฟฟ้า
- ข. ระบบธนาคาร
- ค. ระบบขนส่ง
- ง. ร้านกาแฟอินเทอร์เน็ต

เฉลย: ง

ข้อ 3. กรอบมาตรฐาน NIST CSF ประกอบด้วยกี่ฟังก์ชันหลัก

- ก. 3
- ข. 4
- ค. 5
- ง. 6

เฉลย: ค

ข้อ 4. ข้อใดเป็นมาตรการในฟังก์ชัน Protect

- ก. Asset Management
- ข. Access Control
- ค. Incident Response
- ง. Recovery Planning

เฉลย: ข

ข้อ 5. ข้อใดคือสิทธิของเจ้าของข้อมูลส่วนบุคคลตาม PDPA

- ก. สิทธิเข้าถึงข้อมูล
- ข. สิทธิเลิกจ้าง
- ค. สิทธิในการถอน
- ง. สิทธิใช้สาธารณูปโภค

เฉลย: ก

ข้อ 6. พ.ร.บ.ไซเบอร์ 2562 มีเป้าหมายใด

- ก. ควบคุมค่าอินเทอร์เน็ต
- ข. คุ้มครองโครงสร้างพื้นฐาน CII
- ค. จำกัดสิทธิเสรีภาพประชาชน
- ง. เพิ่มความเร็วอินเทอร์เน็ต

เฉลย: ข

ข้อ 7. ข้อใดเป็นมาตรการในฟังก์ชัน Detect ของ NIST CSF

ก. Asset Inventory

ข. Backup

ค. Monitoring & Logging

ง. Data Encryption

เฉลย: ค

ข้อ 8. Ransomware มักส่งผลกระทบต่อ

ก. ข้อมูลถูกล็อกเข้ารหัส

ข. ความเร็วเครือข่ายเพิ่มขึ้น

ค. การเข้าถึงระบบง่ายขึ้น

ง. ค่าไฟลดลง

เฉลย: ก

ข้อ 9. กฎหมายใดเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ก. พ.ร.บ.ธุรกรรมอิเล็กทรอนิกส์

ข. พ.ร.บ.ไซเบอร์

ค. พ.ร.บ. PDPA

ง. พ.ร.บ.ลิขสิทธิ์

เฉลย: ค

ข้อ 10. การจัดทำ BCP มีเป้าหมายใด

ก. ลดค่าใช้จ่าย

ข. รับประกันความต่อเนื่องของบริการ

ค. เพิ่มจำนวนผู้ใช้ระบบ

ง. ขยายระบบคลาวด์

เฉลย: ข

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิริเชษฐ์ โพธิ์ศิริ. (ม.ป.ป.). *แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถใช้ประโยชน์ได้*. เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับแก้ไขเพิ่มเติม)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*.

ISO/IEC 27001:2022. *Information Security Management Systems*.

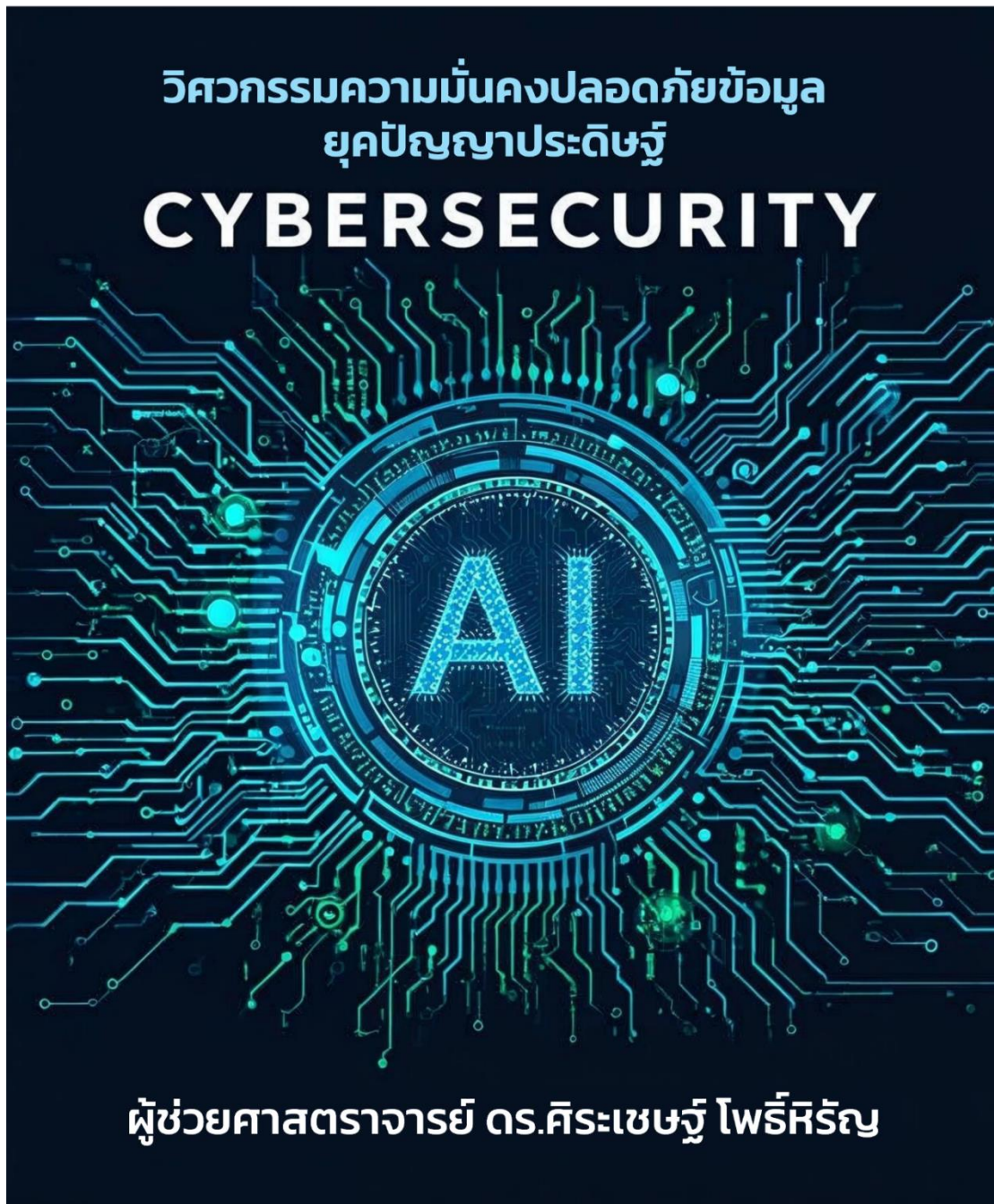
MITRE. (2023). *ATT&CK for Enterprise*.

NIST. (2018). *Cybersecurity Framework (CSF) 1.1*.

NIST. (2020). *Zero Trust Architecture (SP 800-207)*.

บทที่ 14

แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์



วิศวกรรมความมั่นคงปลอดภัยข้อมูล
ยุคปัญญาประดิษฐ์
CYBERSECURITY

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์สิทธิ์

บทที่ 14 แนวโน้มวิศวกรรมความมั่นคงปลอดภัยไซเบอร์ยุคปัญญาประดิษฐ์

1. ผลลัพธ์การเรียนรู้ (Learning Outcomes)

เมื่อเรียนจบหัวข้อนี้ นักศึกษาจะสามารถ:

- 1) อธิบายปัจจัยสำคัญที่ขับเคลื่อนความซับซ้อนทางไซเบอร์และภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงไปได้
- 2) วิเคราะห์ผลกระทบจากความก้าวหน้าของคอมพิวเตอร์ควอนตัมและ AI ต่อระบบความมั่นคงปลอดภัยไซเบอร์ได้
- 3) อธิบายหลักการและความสำคัญของ Post-Quantum Cryptography และ Quantum Key Distribution ได้
- 4) ประเมินการประยุกต์ใช้ AI ในการป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์ได้
- 5) สังเคราะห์แนวโน้มการบูรณาการ AI กับวิทยาการรหัสควอนตัมในอนาคตของ Cybersecurity ได้

2. วัตถุประสงค์การเรียนรู้ (Learning Objectives)

เมื่อเรียนจบหัวข้อนี้ นักศึกษาจะสามารถ:

- 1) ระบุและอธิบายปัจจัยหลักที่ก่อให้เกิดความซับซ้อนในภูมิทัศน์ไซเบอร์ (เช่น ความตึงเครียดทางภูมิรัฐศาสตร์, Generative AI, ช่องว่างทักษะ)
- 2) อธิบายความเสี่ยงของคอมพิวเตอร์ควอนตัมต่อระบบเข้ารหัสแบบดั้งเดิม เช่น RSA, ECC
- 3) อธิบายแนวคิด Post-Quantum Cryptography และการกระจายกุญแจเชิงควอนตัม (QKD)
- 4) วิเคราะห์การใช้ AI ใน Cybersecurity เช่น การตรวจจับมัลแวร์อัตโนมัติ, การตรวจสอบการสื่อสารเชิงวิศวกรรมสังคม
- 5) เสนอแนวทางบูรณาการ AI และวิทยาการรหัสควอนตัมเพื่อเพิ่มความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์

3. หัวข้อเนื้อหา

14.1 ภูมิทัศน์ของความก้าวหน้าด้านเทคโนโลยีดิจิทัลกับความมั่นคงปลอดภัยทางไซเบอร์

14.1.1 ปัจจัยสำคัญที่ขับเคลื่อนความซับซ้อนทางไซเบอร์

14.1.2 ภูมิทัศน์ภัยคุกคามทางไซเบอร์

14.1.3 การเตรียมพร้อมรับมือกับภัยคุกคามควอนตัม

14.2 ความก้าวหน้าควอนตัมคอมพิวเตอร์: ความเสี่ยง ผลกระทบ และความท้าทาย

14.2.1 ความสำคัญของคอมพิวเตอร์ควอนตัม

14.2.2 นิยามศัพท์สำคัญ

14.2.3 วิทยาการรหัสลับ (Cryptography) แบบดั้งเดิม

14.2.4 การแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution)

14.2.5 คอมพิวเตอร์ควอนตัม (Quantum Computer)

14.2.6 ภัยคุกคามจากคอมพิวเตอร์ควอนตัม

14.2.7 ประเภทระบบรหัสลับที่โดนผลกระทบ

14.3 วิทยาการรหัสลับควอนตัม

14.3.1 ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum cryptography)

14.3.2 การกระจายกุญแจเชิงควอนตัม (Quantum key distribution)

14.3.3 ระบบแบบผสม (Hybrid Solutions)

14.3.4 แนวคิดริเริ่มเกี่ยวกับการเข้ารหัสยุคหลังควอนตัม (PQC Initiative)

14.3.5 มาตรฐานการเข้ารหัสหลังควอนตัม

14.3.6 ความท้าทายในการใช้การเข้ารหัสควอนตัมในการรักษาความมั่นคงปลอดภัย

14.4 ปัญหาประติษฐ์กับความมั่นคงปลอดภัยข้อมูล

14.4.1 AI ในด้านความปลอดภัยทางไซเบอร์คืออะไร?

14.4.2 AI ช่วยป้องกันการโจมตีทางไซเบอร์ได้อย่างไร?

14.4.3 การทำระบบอัตโนมัติรักษาความปลอดภัยข้อมูลทางไซเบอร์มีความปลอดภัยหรือไม่?

14.4.4 การประยุกต์ใช้ AI ในด้านความปลอดภัยข้อมูลทางไซเบอร์

14.5 บทวิเคราะห์บูรณาการปัญหาประติษฐ์และวิทยาการรหัสควอนตัมในบริบทความมั่นคงปลอดภัยไซเบอร์

14.5.1 ภาพรวม

14.5.2 บทวิจารณ์ความก้าวหน้าในการเข้ารหัสควอนตัม

14.5.3 บทวิจารณ์การบูรณาการ AI กับการเข้ารหัสควอนตัม

4. กิจกรรมการเรียนรู้ในชั้นเรียน (กรณีศึกษา)

กรณีศึกษา:

บริษัท *RMUTT FinTech Asia* ให้บริการธุรกรรมทางการเงินออนไลน์ทั่วโลก กำลังเผชิญภัยคุกคามจากทั้ง Ransomware ที่ขับเคลื่อนด้วย Generative AI และความเสี่ยงจากการมาถึงของคอมพิวเตอร์ควอนตัมที่สามารถเจาะระบบเข้ารหัส RSA ได้

คำสั่งสำหรับนักศึกษา (แบ่งกลุ่ม 4-5 คน):

1. วิเคราะห์ภัยคุกคามที่องค์กรกำลังเผชิญจาก AI และ Quantum Computing
2. เสนอแนวทางการปรับปรุงการเข้ารหัสให้พร้อมสู่ยุค Post-Quantum
3. เสนอการใช้ AI ในเชิงป้องกัน (เช่น Threat Detection, Incident Response Automation)
4. สรุปเป็น Infographic แนวทางป้องกันองค์กรที่ยั่งยืน

ประเด็นการเรียนรู้ที่แทรก:

- Generative AI กับภัยคุกคาม (Phishing, Deepfake, RaaS)
- Quantum Threats ต่อ RSA/ECC
- Post-Quantum Cryptography (PQC)
- Quantum Key Distribution (QKD)
- การบูรณาการ AI + Cryptography

5. เกณฑ์คะแนน Rubric 4 ระดับ (100 คะแนน):

เกณฑ์	4 (ยอดเยี่ยม)	3 (ดี)	2 (พอใช้)	1 (ควรปรับปรุง)
การวิเคราะห์ภัยคุกคาม (25)	ครอบคลุมทั้ง AI และ Quantum	ครอบคลุมเพียงด้านเดียว	วิเคราะห์บางส่วน	ไม่ถูกต้อง
การเสนอแนวทาง PQC (25)	ครอบคลุมหลายอัลกอริทึมและการนำไปใช้จริง	ครอบคลุมบางส่วน	กล่าวไม่ชัดเจน	ไม่เสนอ
การเสนอ AI Security (25)	เสนอหลายวิธีพร้อมเหตุผล	เสนอเพียงบางส่วน	กล่าวไม่ครบ	ไม่เสนอ
การนำเสนอ (25)	ชัดเจน + Infographic	ชัดเจน	พอใช้	ไม่ชัดเจน

14. แนวโน้มวิศวกรรมความมั่นคงปลอดภัยทางไซเบอร์ในยุคปัญญาประดิษฐ์

ในโลกไซเบอร์ที่ซับซ้อนซึ่งเต็มไปด้วยความไม่แน่นอนทางภูมิรัฐศาสตร์ ความไม่เท่าเทียมทางไซเบอร์ที่ขยายตัว และภัยคุกคามทางไซเบอร์ที่ซับซ้อน ผู้นำจะต้องมีแนวคิดที่เน้นความปลอดภัยเป็นอันดับแรก เนื้อหาต่อไปนี้จะนำเสนอความก้าวหน้าของปัญญาประดิษฐ์และคอนแทกคอมพิวเตอร์และปัญญาประดิษฐ์ที่มีผลกระทบต่องานด้านวิศวกรรมความมั่นคงปลอดภัยข้อมูลในประเด็นสำคัญความเสี่ยง ผลกระทบ และความท้าทาย

14.1 ภูมิทัศน์ของความก้าวหน้าด้านเทคโนโลยีดิจิทัลกับความมั่นคงปลอดภัยทางไซเบอร์

แม้ว่ารายงาน Global Cybersecurity Outlook ฉบับปี 2024 ของฟอรัมเศรษฐกิจโลก (World Economy Forum หรือ WEF) จะเน้นย้ำถึงความเหลื่อมล้ำที่เพิ่มมากขึ้นในโลกไซเบอร์ แต่รายงานในปีนี้ก็กลับเผยให้เห็นถึงความซับซ้อนที่เพิ่มมากขึ้นของภูมิทัศน์ไซเบอร์ ซึ่งส่งผลกระทบอย่างลึกซึ้งและกว้างไกลต่อองค์กรและประเทศชาติ ความซับซ้อนนี้เกิดจากปัจจัยหลายประการที่ทวีความรุนแรงขึ้น ได้แก่ ความตึงเครียดทางภูมิรัฐศาสตร์ที่ทวีความรุนแรงขึ้น ส่งผลให้สภาพแวดล้อมมีความไม่แน่นอนมากขึ้น การบูรณาการและการพึ่งพาห่วงโซ่อุปทานที่ซับซ้อนมากขึ้น นำไปสู่ภูมิทัศน์ความเสี่ยงที่คลุมเครือและคาดเดาไม่ได้มากขึ้น

14.1.1 ปัจจัยสำคัญที่ขับเคลื่อนความซับซ้อนทางไซเบอร์

ความซับซ้อนที่เพิ่มมากขึ้นนี้ส่งผลกระทบอย่างลึกซึ้งและกว้างไกลต่อองค์กรและประเทศชาติ ก่อให้เกิดความท้าทายใหม่ๆ ในการรักษาความยืดหยุ่นทางไซเบอร์ ปัจจัยสำคัญที่ขับเคลื่อนความซับซ้อนทางไซเบอร์ประกอบด้วย รูป 14.1

ความตึงเครียดทางภูมิรัฐศาสตร์: ความตึงเครียดทางภูมิรัฐศาสตร์ที่เพิ่มสูงขึ้นกำลังสร้างสภาพแวดล้อมระดับโลกที่ไม่แน่นอนมากขึ้น ส่งผลกระทบโดยตรงต่อภูมิทัศน์ไซเบอร์และเพิ่มความเสี่ยงที่อาจเกิดขึ้น

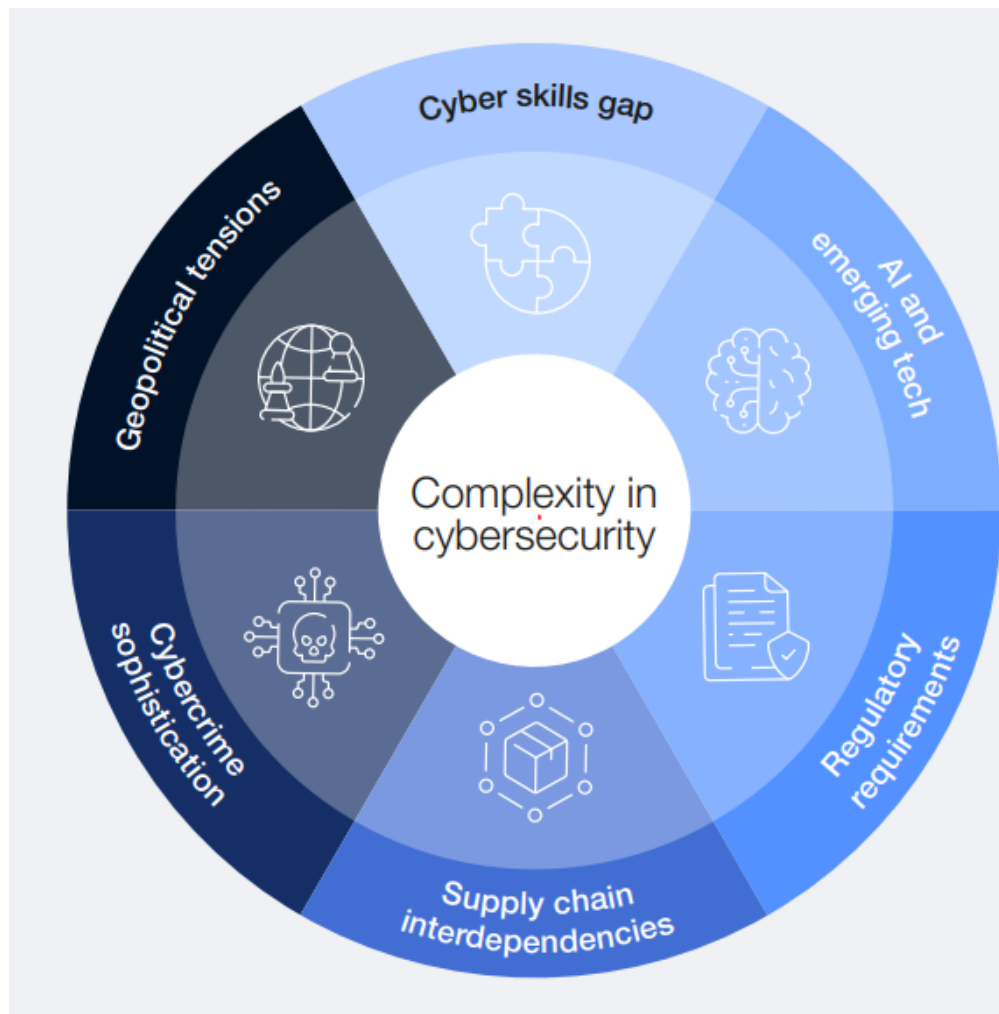
ห่วงโซ่อุปทานที่ซับซ้อน: การบูรณาการและการพึ่งพาห่วงโซ่อุปทานที่ซับซ้อนมากขึ้นทำให้สภาพแวดล้อมความเสี่ยงทางไซเบอร์คลุมเครือและคาดเดาไม่ได้มากขึ้น

เทคโนโลยีใหม่ ๆ: การนำเทคโนโลยีใหม่ ๆ มาใช้อย่างรวดเร็ว เช่น Generative AI นำมาซึ่งช่องโหว่ใหม่ๆ เนื่องจากอาชญากรไซเบอร์ใช้ประโยชน์จากเทคโนโลยีเหล่านี้ในการโจมตีที่ซับซ้อนและมีขนาดใหญ่ขึ้น

ช่องว่างด้านทักษะที่เพิ่มมากขึ้น: ช่องว่างด้านทักษะไซเบอร์กำลังขยายกว้างขึ้น ทำให้องค์กรต่างๆ รับมือกับภัยคุกคามทางไซเบอร์ที่ซับซ้อนได้อย่างมีประสิทธิภาพได้ยากขึ้น

ภาระด้านกฎระเบียบ: จำนวนกฎระเบียบทั่วโลกที่เพิ่มมากขึ้นทำให้องค์กรต่างๆ ต้องแบกรับภาระด้านการปฏิบัติตามกฎระเบียบอย่างมาก ส่งผลให้มาตรการรักษาความปลอดภัยทางไซเบอร์มีความซับซ้อนมากขึ้น

การนำเทคโนโลยีใหม่ๆ มาใช้อย่างรวดเร็วก่อให้เกิดช่องโหว่ใหม่ๆ เนื่องจากอาชญากรไซเบอร์ใช้ประโยชน์จากเทคโนโลยีเหล่านี้ได้อย่างมีประสิทธิภาพเพื่อเพิ่มความซับซ้อนและขยายขอบเขตการใช้งาน ขณะเดียวกัน การขยายตัวของข้อกำหนดด้านกฎระเบียบทั่วโลกกำลังเพิ่มภาระในการปฏิบัติตามกฎระเบียบให้กับองค์กรต่างๆ ความท้าทายทั้งหมดนี้ยิ่งทวีความรุนแรงขึ้นจากช่องว่างด้านทักษะที่กว้างขึ้น ทำให้การจัดการความเสี่ยงทางไซเบอร์อย่างมีประสิทธิภาพเป็นเรื่องท้าทายอย่างยิ่ง



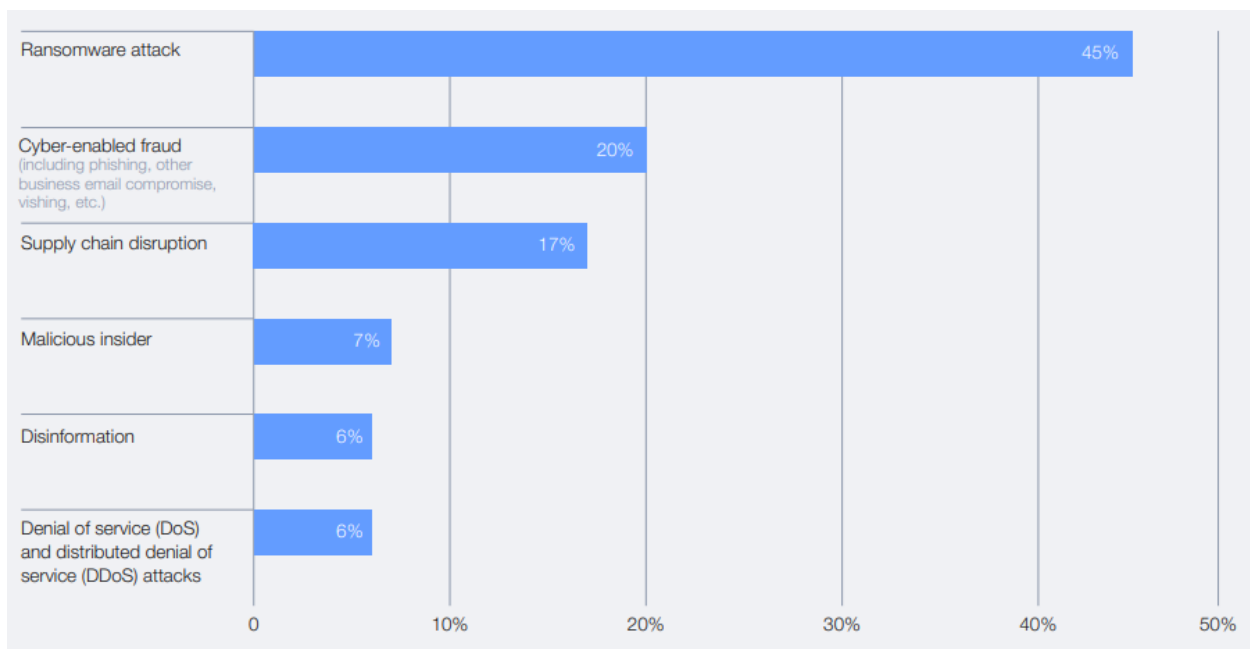
รูป 14.1 ปัจจัยที่ทำให้เกิดความซับซ้อนของธรรมชาติของความปลอดภัยทางไซเบอร์

(ที่มา: WEF)

นอกจากนี้ยังทำให้ช่องว่างระหว่างองค์กรที่สามารถปรับตัวเข้ากับเทคโนโลยีใหม่ๆ และองค์กรที่ประสบปัญหารุนแรงยิ่งขึ้น ซึ่งอาจส่งผลให้ช่องว่างด้านความยืดหยุ่นทางไซเบอร์กว้างขึ้น

14.1.2 ภูมิทัศน์ภัยคุกคามทางไซเบอร์

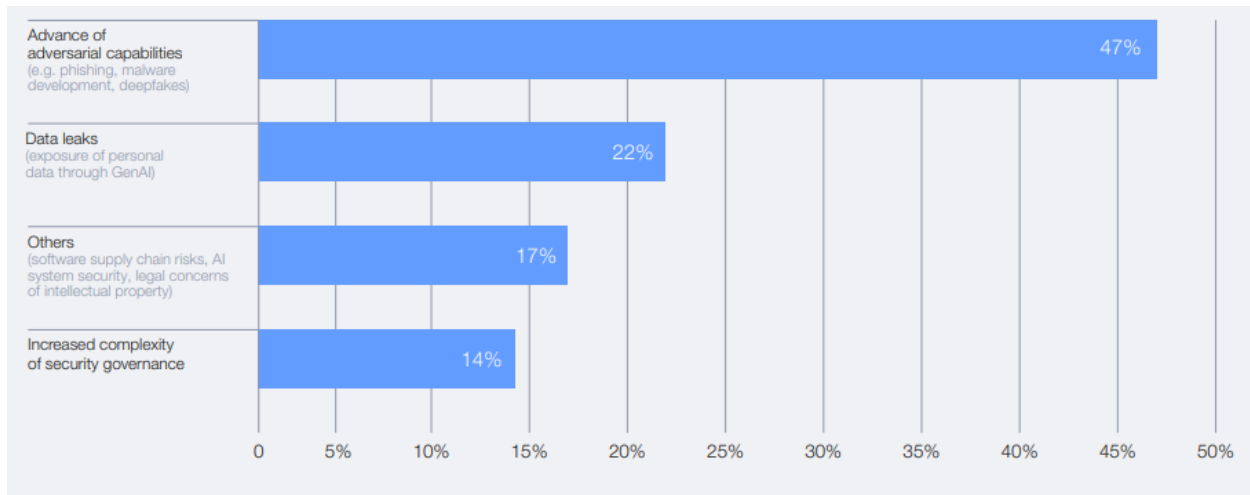
การถอดรหัสความซับซ้อน ในขณะนี้อาชญากรทางไซเบอร์เริ่มใช้เครื่องมือขั้นสูง ภูมิทัศน์ของภัยคุกคามที่เปลี่ยนแปลงไปต้องการกลยุทธ์ที่สร้างสรรค์เพื่อต่อสู้กับการโจมตีที่ซับซ้อนและมีขอบเขตกว้างไกลมากขึ้น วิวัฒนาการของอาชญากรรมไซเบอร์ จากรายงานดังกล่าวระบุว่า แรนซัมแวร์ยังคงเป็นความเสี่ยงทางไซเบอร์อันดับต้นๆ ขององค์กรในแต่ละปี โดยผู้ตอบแบบสอบถาม 45% ระบุว่าแรนซัมแวร์เป็นประเด็นที่น่ากังวลอันดับต้นๆ ในการสำรวจปีนี้ จากข้อมูลของผู้นำในการประชุมประจำปีว่าด้วยความมั่นคงปลอดภัยไซเบอร์ 2024 พบว่าควรมีการคาดการณ์ถึงนวัตกรรมใหม่ๆ ที่สำคัญในการโจมตีด้วยแรนซัมแวร์ ประกอบกับการนำแรนซัมแวร์แบบบริการ (RaaS) มาใช้อย่างต่อเนื่อง ซึ่งส่งผลให้แรนซัมแวร์กลายเป็นสินค้าโภคภัณฑ์ การฉ้อโกงทางไซเบอร์เป็นความเสี่ยงทางไซเบอร์ขององค์กรอันดับสองในปี 2025 ซึ่งซีไอโอมองว่าเป็นภัยคุกคามสำคัญควบคู่ไปกับแรนซัมแวร์ และการหยุดชะงักของห่วงโซ่อุปทาน ในขณะเดียวกัน การโจรกรรมข้อมูลประจำตัวก็กลายเป็นประเด็นสำคัญอันดับต้นๆ และกลายเป็นความเสี่ยงทางไซเบอร์ส่วนบุคคลหลักสำหรับทั้งผู้บริหารระดับสูงด้านความปลอดภัยสารสนเทศ (CISO) และซีไอโอ รูป 14.2 ความเสี่ยงที่องค์กรกังวลมากที่สุด



รูป 14.2 ความเสี่ยงที่องค์กรกังวลมากที่สุด

(ที่มา: WEF)

อาชญากรไซเบอร์กำลังใช้ GenAI เพื่อเลียนแบบรูปแบบการสื่อสารของผู้บริหารระดับสูงขององค์กรได้อย่างน่าเชื่อถือ เครื่องมือเหล่านี้ใช้ประโยชน์จากข้อมูลเชิงบริบทจากแหล่งข้อมูลต่างๆ เช่น โซเชียลมีเดีย แอลงการณ สารณะ หรือเอกสารที่รั่วไหล ทำให้ความพยายามทางวิศวกรรมสังคมมีความซับซ้อนและยากต่อการระบุตัวตนมากขึ้น GenAI ยังสนับสนุนผู้โจมตีในการพัฒนาการโจมตีทางวิศวกรรมสังคมที่น่าเชื่อถือในภาษาที่หลากหลายยิ่งขึ้น ซึ่งช่วยให้ผู้ก่อภัยคุกคามสามารถกำหนดเป้าหมายผู้คนจำนวนมากขึ้นในหลายประเทศด้วยต้นทุนที่ต่ำลง



รูป 14.3 ปัญหาความปลอดภัยทางไซเบอร์เชื่อมโยงกับ GenAI

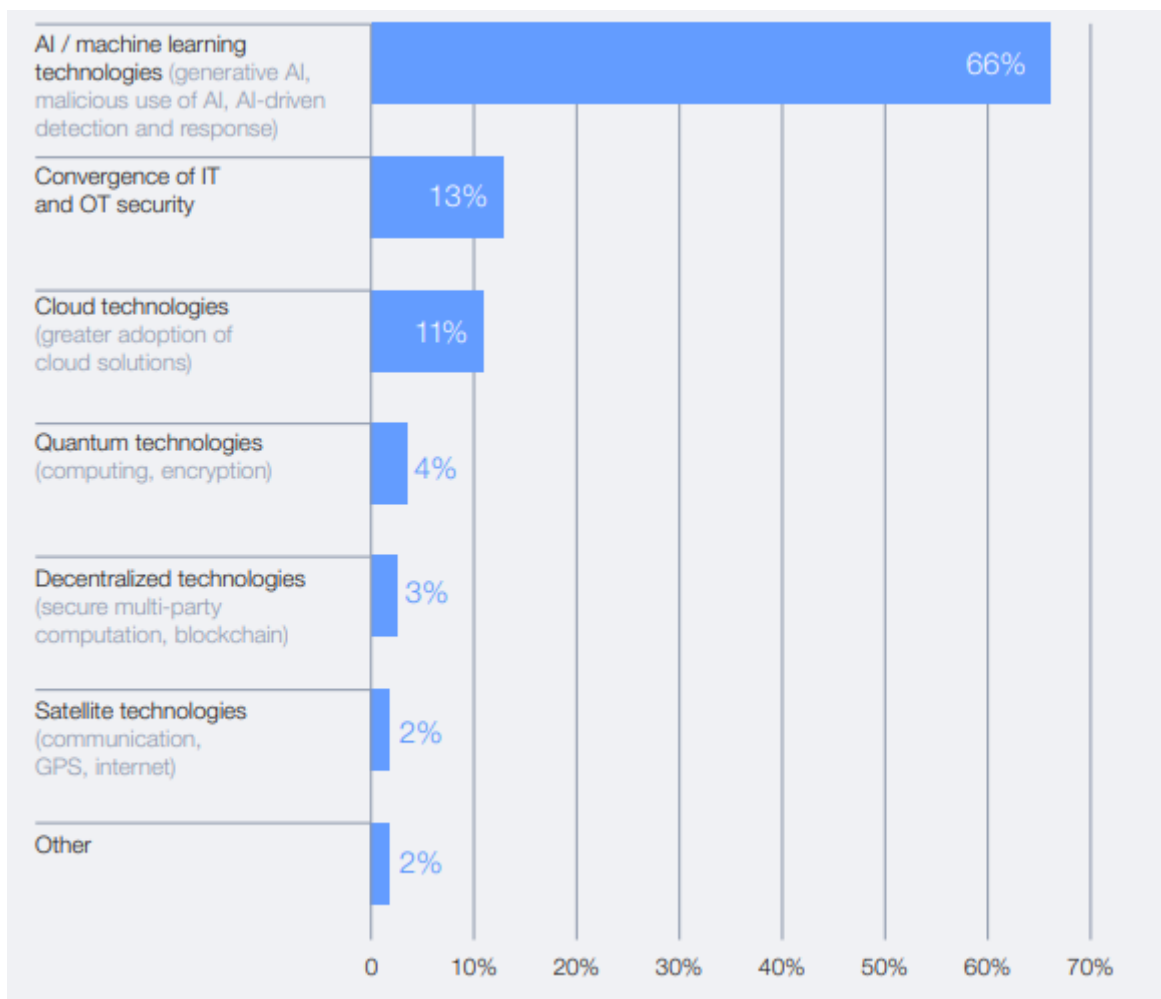
(ที่มา: WEF)

รูป 14.3 แสดงให้เห็นถึงความกังวลความก้าวหน้าของความสามารถในการต่อต้าน เช่น การฟิชชิ่ง การพัฒนาเมลแวร์ ดีปเฟก การรั่วไหลของข้อมูล (การเปิดเผยข้อมูลส่วนบุคคลผ่าน GenAI) อื่นๆ (ความเสี่ยงต่อห่วงโซ่อุปทานซอฟต์แวร์ ความปลอดภัยของระบบ AI ข้อกังวลทางกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา) ความซับซ้อนที่เพิ่มขึ้นของการกำกับดูแลความปลอดภัย

เทคโนโลยีใหม่ๆ นำเสนอโอกาสสำคัญสำหรับองค์กรต่างๆ ในการเพิ่มประสิทธิภาพและเพิ่มประสิทธิภาพการดำเนินงาน ส่งผลให้หลายองค์กรกำลังพัฒนากลยุทธ์เพื่อผสมผสานรวมเทคโนโลยีเหล่านี้เข้ากับโครงสร้างพื้นฐานอย่างแข็งขัน อย่างไรก็ตาม ความเสี่ยงทางไซเบอร์ที่เกี่ยวข้องกับเทคโนโลยีพื้นฐานหรือการนำไปใช้งานในองค์กรมักไม่ได้รับความสนใจและการพิจารณาอย่างเพียงพอ แม้ว่า AI จะไม่ใช่ปรากฏการณ์ใหม่ แต่การเกิดขึ้นของ GenAI ได้เร่งการนำ AI มาใช้ในองค์กรต่างๆ ทั่วโลก องค์กรต่างๆ กำลังทดสอบหรือนำเทคโนโลยี AI มาใช้เพื่อเพิ่มประสิทธิภาพและสร้างรายได้เปรียบในการแข่งขัน

อย่างไรก็ตาม องค์กรส่วนใหญ่ยังไม่ได้ออกแบบกลยุทธ์และกระบวนการเพื่อความปลอดภัยในการใช้งานเสมอไป เมื่อนำเทคโนโลยีใหม่ๆ มาใช้ สิ่งสำคัญอย่างยิ่งที่องค์กรต่างๆ จะต้องประเมินความเสี่ยงทางไซเบอร์ที่เกี่ยวข้องและนำมาตราการควบคุมความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องมาใช้ เพื่อให้มั่นใจถึงความสามารถในการ

ดำเนินงานและความยืดหยุ่นทางไซเบอร์ของธุรกิจในช่วงกว้าง จากการสำรวจของ GCO พบว่า 66% ขององค์กรคาดการณ์ว่า AI จะมีผลกระทบสำคัญที่สุดต่อความปลอดภัยทางไซเบอร์ในปีหน้า อย่างไรก็ตาม มีเพียง 37% ของผู้ตอบแบบสอบถามที่รายงานว่ามีการประเมินความปลอดภัยของเครื่องมือ AI ก่อนการใช้งาน สิ่งนี้สร้างความเสี่ยงที่องค์กรอาจนำระบบ AI มาใช้หรือปรับใช้ ไม่ว่าจะพัฒนาภายในหรือรับมาจากผู้ให้บริการบุคคลที่สามก็ตาม โดยไม่ได้พิจารณาความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องและมาตรการบรรเทาที่เกี่ยวข้องอย่างครบถ้วน ขณะเดียวกันอาจนำช่องโหว่ต่างๆ เข้ามาในระบบไอทีของตนได้



รูป 14.4 การคาดการณ์ช่องโหว่ทางไซเบอร์ตั้งแต่ปี 2025 เป็นต้นไป

(ที่มา: WEF)

จากรูป 14.4 แสดงอันดับภัยคุกคามที่อาจจะส่งผลกระทบต่อความปลอดภัยทางไซเบอร์มากที่สุดในช่วง 12 เดือนข้างหน้า 5 อันดับสูงสุด พบว่า (1) เทคโนโลยีการเรียนรู้ของ AI/machine (AI เชิงสร้างสรรค์ การใช้ AI อย่างผิดวัตถุประสงค์ การตรวจจับและการตอบสนองที่ขับเคลื่อนด้วย AI) เป็นผลกระทบอันดับสูงสุด (2) การ

ผสมรวมความปลอดภัยด้าน IT และ OT (3) เทคโนโลยีคลาวด์ (การนำโซลูชันคลาวด์มาใช้มากขึ้น) (4) เทคโนโลยีควอนตัม (การประมวลผล การเข้ารหัส) (5) เทคโนโลยีแบบกระจายอำนาจ (การประมวลผลหลายฝ่ายที่ปลอดภัย บล็อกเชน) ส่วนเทคโนโลยีดาวเทียม (การสื่อสาร GPS อินเทอร์เน็ต) และอื่นๆ เป็นอันดับรองลงมา

14.1.3 การเตรียมพร้อมรับมือกับภัยคุกคามควอนตัม

การเตรียมพร้อมรับมือกับภัยคุกคามควอนตัม 40% ขององค์กรกำลังดำเนินขั้นตอนเชิงรุกเพื่อทำความเข้าใจภัยคุกคามควอนตัม การประมวลผลควอนตัมนำเสนอโอกาสทางเศรษฐกิจและวิทยาศาสตร์ที่สำคัญด้วยการปลดล็อกพลังการประมวลผลที่ไม่เคยมีมาก่อน อย่างไรก็ตาม ความก้าวหน้าของการประมวลผลควอนตัมยังเร่งให้เกิดความเสี่ยงด้านความปลอดภัย โดยเฉพาะอย่างยิ่งศักยภาพในการเจาะระบบเข้ารหัสที่สาธารณะ ซึ่งมีความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยของระบบดิจิทัล เช่น ธนาคารออนไลน์และการสื่อสารของรัฐบาล แม้ว่าระยะเวลาสำหรับศักยภาพสูงสุดของการประมวลผลควอนตัมยังคงไม่แน่นอน แต่ความเสี่ยงด้านความปลอดภัยของควอนตัมที่เกี่ยวข้องได้เกิดขึ้นแล้ว

ในการประชุมกลุ่มย่อยในการประชุมประจำปีว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ ปี 2024 องค์กร 40% ระบุว่าได้เริ่มดำเนินการเชิงรุกโดยการประเมินความเสี่ยงเพื่อทำความเข้าใจภัยคุกคามจากควอนตัม หลายองค์กรเริ่มเฝ้าระวังภัยคุกคามมากขึ้น เช่น กรณี "เก็บเกี่ยวตอนนี้ ถอดรหัสทีหลัง" ซึ่งผู้ไม่ประสงค์ดีจะรวบรวมข้อมูลที่เข้ารหัสไว้ในขณะนี้ และวางแผนที่จะถอดรหัสเมื่อการประมวลผลควอนตัมสามารถเจาะระบบเข้ารหัสที่มีอยู่ได้ ซึ่งก่อให้เกิดความท้าทายอย่างมากต่อความปลอดภัยของข้อมูลทั้งในปัจจุบันและอนาคต

อย่างไรก็ตาม บางองค์กรยังคงรอการสนับสนุนจากมาตรฐานอุตสาหกรรม แนวทางปฏิบัติ และกฎระเบียบของรัฐบาล ได้มีการพยายามหลายครั้งเพื่อกระตุ้นให้เกิดการดำเนินการดังกล่าว กลุ่มผู้เชี่ยวชาญด้านไซเบอร์ G7 ได้ระบุรายการความเสี่ยงต่อความมั่นคงปลอดภัยของระบบการเงิน พร้อมให้คำแนะนำสำคัญแก่รัฐบาลและธนาคารกลาง พร้อมกับเรียกร้องให้มีการดำเนินการฟอรัมเศรษฐกิจโลก (World Economic Forum) ร่วมมือกับสำนักงานกำกับดูแลทางการเงิน (Financial Conduct Authority) ได้พัฒนาคำแนะนำเพื่อแจ้งขั้นตอนการควบคุมระดับโลก เพื่อช่วยให้มั่นใจว่าแนวทางด้านความปลอดภัยควอนตัมจะมีความสอดคล้องและร่วมมือกันทั่วโลก

เมื่อเร็วๆ นี้ สถาบันมาตรฐานและการเข้ารหัสแห่งชาติ (NIST) ได้เผยแพร่มาตรฐานอัลกอริทึมหลังการเข้ารหัสควอนตัม (Post-Quantum Cryptography: PQC) ที่ได้รับการรอกอยอย่างมาก 3 มาตรฐาน ซึ่งสร้างขึ้นเพื่อรับมือกับการโจมตีทางไซเบอร์จากคอมพิวเตอร์ควอนตัม นอกเหนือจากมาตรฐาน PQC แล้ว เทคโนโลยีอื่นๆ เช่น การกระจายคีย์ควอนตัม (QKD) และการสร้างเลขสุ่มควอนตัม (QRNG) ก็ได้รับความสนใจเช่นกัน เนื่องจากเทคโนโลยีเหล่านี้สามารถช่วยลดความเสี่ยงจากการเข้ารหัสด้วยควอนตัมเป็นการเข้ารหัสด้วยที่สาธารณะ ไม่ว่า

จะใช้แบบเดี่ยวหรือแบบผสมผสาน การเปลี่ยนผ่านที่ประสบความสำเร็จเริ่มต้นด้วยรากฐานทางไซเบอร์ที่แข็งแกร่ง และกลยุทธ์ความพร้อมด้านคอนตัมที่ชัดเจน โดยเน้นย้ำถึงความจำเป็นที่องค์กรต่างๆ ต้องเริ่มต้นเส้นทางความพร้อมด้านคอนตัมตั้งแต่วันนี้

14.2 ความก้าวหน้าคอนตัมคอมพิวเตอร์: ความเสี่ยง ผลกระทบ และความท้าทาย

ความก้าวหน้าทางเทคโนโลยีครั้งสำคัญ 2 ประการที่เกิดขึ้นในยุคปัจจุบัน ส่งผลกระทบต่อบทบาทและความเสี่ยงของระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ ข้อมูล และความเป็นส่วนตัวอย่างไม้อาจหลีกเลี่ยงได้ โดยเฉพาะอย่างยิ่งในด้านปัญญาประดิษฐ์ (AI) และคอมพิวเตอร์ควอนตัม ได้นำมาซึ่งการเปลี่ยนแปลงครั้งสำคัญทางเทคโนโลยี ความก้าวหน้าเหล่านี้ส่งผลกระทบอย่างลึกซึ้งต่อวิทยาการเข้ารหัสลับเชิงควอนตัม ซึ่งเป็นสาขาที่ระเบียบวิธีของ AI มีศักยภาพมหาศาลในการเพิ่มประสิทธิภาพและความทนทานของระบบการเข้ารหัสลับ

อย่างไรก็ตาม การเกิดขึ้นของคอมพิวเตอร์ควอนตัมได้สร้างความท้าทายใหม่สำหรับอัลกอริทึมความปลอดภัยที่มีอยู่ซึ่งมักเรียกกันว่า "ภัยคุกคามเชิงควอนตัม" แม้จะมีความท้าทายเหล่านี้ แต่ก็ยังมีแนวทางที่น่าสนใจสำหรับการผสมรวม AI ที่ใช้โครงข่ายประสาทเทียมเข้ากับวิทยาการเข้ารหัสลับ ซึ่งมีความหมายสำคัญต่อกระบวนการทัศนความปลอดภัยดิจิทัลในอนาคต บทสรุปนี้เน้นย้ำประเด็นสำคัญในจุดเชื่อมโยงระหว่าง AI และวิทยาการเข้ารหัสลับเชิงควอนตัม รวมถึงประโยชน์ที่อาจเกิดขึ้นจากวิทยาการเข้ารหัสลับที่ขับเคลื่อนด้วย AI ความท้าทายที่ต้องได้รับการแก้ไข และโอกาสของการแสวงหาองค์ความรู้ใหม่แบบสหวิทยาการนี้

14.2.1 ความสำคัญของคอมพิวเตอร์ควอนตัม

การรักษาความมั่นคงปลอดภัยข้อมูลในปัจจุบันอยู่ภายใต้หลักการพื้นฐานสำคัญ 3 ประการ ประกอบด้วย การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้ (Availability) ที่เรียกว่าสามเสาของความมั่นคงปลอดภัย (CIA Triad) โดยมีเทคโนโลยีดิจิทัลที่เป็นรากฐานสำคัญของการดำรงไว้ซึ่งหลักการ CIA Triad ดังกล่าว คือ วิทยาการรหัสลับ (Cryptography) ซึ่งมีองค์ประกอบหลัก คือ วิทยาการรหัสลับที่ใช้กุญแจแบบสมมาตร (Symmetric Key) หรือระบบกุญแจลับ (Secret Key) และแบบอสมมาตร (Asymmetric Key) หรือกุญแจสาธารณะ (Public Key Cryptography) ซึ่งระบบรหัสลับทั้งสองวิธีถูกใช้งานอย่างแพร่หลาย โดยถูกใช้เป็นองค์ประกอบพื้นฐานในกระบวนการแลกเปลี่ยนข้อมูลให้มีความปลอดภัย เช่น การแลกเปลี่ยนกุญแจระบบรหัสลับ (Key Exchange) การกระจายกุญแจ (Key Distribution) การลงลายมือชื่อดิจิทัล (Digital Signatures) และการพิสูจน์ตัวตนจริง (Authentication) เป็นต้น

ทั้งนี้ หากระบบรหัสลับทั้งแบบกุญแจลับและแบบกุญแจสาธารณะถูกโจมตี ผู้ไม่ประสงค์ดีอาจปลอมแปลงเอกสารอิเล็กทรอนิกส์โดยใช้ลายมือชื่อดิจิทัลปลอมเพื่อการทำธุรกรรมโดยไม่ได้รับอนุญาตหรือแอบอ้างเป็นบุคคลอื่นได้ ข้อมูลหรือทรัพยากรดิจิทัลที่สำคัญก็ปราศจากการป้องกัน

คอมพิวเตอร์ควอนตัมขนาดใหญ่ (Large-Scale Quantum Computers) ที่กำลังถูกพัฒนาขึ้นนี้มีความสามารถในการโจมตีระบบรหัสลับแบบกุญแจสาธารณะ ซึ่งจากการประมาณการในรายงานโดย Gouzien ระบบรหัสลับ RSA-2048 อาจสามารถถูกแยกตัวประกอบเพื่อถอดรหัสลับได้ภายใน 177 วันด้วยคอมพิวเตอร์ควอนตัมขนาด 13,436 คิวบิตและหน่วยความจำแบบ multimode" ส่งผลให้ความมั่นคงปลอดภัยของระบบการสื่อสารในปัจจุบันลดลงไปอย่างมาก และมีความเสี่ยงที่จะส่งผลกระทบในวงกว้างทั้งทางด้านเศรษฐกิจ สังคม และความมั่นคง

14.2.2 นิยามศัพท์สำคัญ

“กลศาสตร์ควอนตัม (Quantum Mechanics)” หมายความว่า ทฤษฎีทางฟิสิกส์ที่ใช้ในการอธิบายพฤติกรรมและคุณสมบัติของระบบที่มีขนาดเล็กในระดับอะตอม

“คอมพิวเตอร์ควอนตัม (Quantum Computer)” หมายความว่า คอมพิวเตอร์ที่ใช้ปรากฏการณ์ทางฟิสิกส์ของระบบที่มีขนาดเล็กในระดับอะตอมซึ่งสามารถอธิบายได้ด้วยทฤษฎีกลศาสตร์ควอนตัม ในการคำนวณและประมวลผลทางคอมพิวเตอร์ โดยมีคุณสมบัติในการแก้ปัญหาทางคณิตศาสตร์บางประเภท ที่คอมพิวเตอร์ธรรมดาไม่สามารถแก้ได้อย่างมีประสิทธิภาพ

“วิทยาการรหัสลับ (Cryptography)” หมายความว่า ศาสตร์ที่เกี่ยวข้องกับหลักการ วิธีการ และวิธีการในการรักษาความปลอดภัยข้อมูล ซึ่งรวมถึงการรักษาความลับ ความสมบูรณ์ของข้อมูล การไม่ปฏิเสธ และความถูกต้องแท้จริง

“การเข้ารหัสลับ (Encryption)” หมายความว่า กระบวนการใดๆ ที่ใช้ในการเข้ารหัสเพื่อแปลงข้อความธรรมดาที่สามารถอ่านได้ (Plaintext) เป็นข้อความเข้ารหัสหรือข้อความไซเฟอร์ (Ciphertext) เพื่อป้องกันไม่ให้บุคคลอื่นนอกจากผู้รับที่ตั้งใจไว้อ่านข้อมูลนั้น

“การถอดรหัสลับ (Decryption)” หมายความว่า การแปลงข้อความหรือข้อมูลจากรูปแบบที่ถูกเข้ารหัสลับและไม่สามารถอ่านได้ (Ciphertext) ให้กลับไปอยู่ในรูปแบบเดิมที่สามารถอ่านได้ (Plaintext)

“วิทยาการรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography)” หมายความว่า ระบบรหัสลับที่ใช้กุญแจรหัสลับ (Secret Key) ดอกเดียวกันในการเข้ารหัสลับและถอดรหัสลับ

“วิทยาการรหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Cryptography)” หรือ “ระบบรหัสลับกุญแจสาธารณะ (Public Key Cryptography)” หมายความว่า ระบบรหัสลับที่คู่กุญแจ (Key pair) ประกอบด้วย กุญแจสาธารณะ (Public Key) ใช้เข้ารหัสลับเพื่อรักษาความลับ หรือตรวจสอบความครบถ้วน

แท้จริงของข้อมูล และกุญแจส่วนตัว (Private Key) ใช้สำหรับถอดรหัสลับหรือลงลายมือชื่อดิจิทัลเพื่อรับรองความแท้จริงของข้อมูล โดยกุญแจส่วนตัวต้องจัดเก็บไว้เป็นความลับ ในขณะที่กุญแจสาธารณะสามารถส่งต่อและเปิดเผยให้กับผู้อื่นได้

“การลงลายมือชื่อดิจิทัล (Digital Signature)” หมายความว่า ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับด้วยระบบรหัสลับแบบกุญแจสมมาตรโดยใช้กุญแจส่วนตัว (Private Key) ในการลงลายมือชื่อ และใช้กุญแจสาธารณะ (Public Key) ที่เป็นคู่กุญแจกันในการตรวจสอบลายมือชื่อ ทำให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (Authenticity) และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (Data Integrity) รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดชอบจากข้อความที่ตนเองลงลายมือชื่อได้ (Non-Repudiation)

“ฟังก์ชันแฮช (Hash Function)” หมายความว่า กระบวนการทางด้านคณิตศาสตร์ที่ใช้แปลงข้อมูลให้กลายเป็นข้อมูลย่อย (Digest) โดยข้อมูลย่อยจะมีขนาดคงที่ (Fixed Size) ไม่ว่าข้อมูลตั้งต้นจะมีขนาดเท่าใดก็ตาม

“ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum Cryptography System: PQC)” หมายความว่า ระบบรหัสลับที่ใช้อัลกอริทึมที่ทนทานต่อการโจมตีจากคอมพิวเตอร์ควอนตัม (Quantum-Resistant Algorithm)

“การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD)” หมายความว่า กระบวนการทางควอนตัมสำหรับการสร้างและกระจายกุญแจรหัสลับ (Key Distribution) อย่างปลอดภัย

“การเข้ารหัสยุคหลังควอนตัม (Post-Quantum Cryptography: PQC)” คือ กระบวนการเข้ารหัสข้อมูลที่เกิดขึ้นมาเพื่อปกป้องข้อมูลจากการมาถึงของคอมพิวเตอร์ควอนตัม ซึ่งผู้เชี่ยวชาญและทำงานเกี่ยวข้องกับความปลอดภัยและการรักษาความลับข้อมูลต่างมีความกังวลว่าจะมีความสามารถเจาะผ่านเทคโนโลยีการเข้ารหัสแบบเดิมที่ใช้อยู่ได้อย่างง่ายดาย จึงแบ่งได้ออกเป็น 2 ส่วน คือ เทคโนโลยีการเข้ารหัส และ การพัฒนาคอมพิวเตอร์ควอนตัม

14.2.3 วิทยาการรหัสลับ (Cryptography) แบบดั้งเดิม

เนื้อหาวิทยาการรหัสลับปรากฏโดยละเอียดแล้วในบทที่ผ่านมา แต่ในที่นี้จะกล่าวโดยสรุปเพื่อให้เห็นถึงความสำคัญของความเสี่ยงที่เกิดขึ้นจากยุคคอมพิวเตอร์ควอนตัม เทคโนโลยีการเข้ารหัสแบบดั้งเดิมเป็นแนวทางปฏิบัติในการปกป้องข้อมูลโดยใช้อัลกอริทึม แฮช และลายเซ็นดิจิทัล และการเข้ารหัส ซึ่งข้อมูลนั้นอาจถูกพิกเอาไว้เป็นไฟล์ในฮาร์ดดิสก์อยู่ในระหว่างการส่งต่อในเครือข่ายอิเล็กทรอนิกส์ที่มีการสื่อสารสองฝ่ายขึ้นไป หรือใช้งานอยู่ระหว่างการประมวลผล การเข้ารหัสมีเป้าหมาย สำคัญอยู่ 4 ข้อ คือ

การรักษาความลับ - ข้อมูลจะต้องใช้งานได้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น

การรักษาความถูกต้อง - ตรวจสอบได้แน่นอนว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลง

การยืนยันตัวตน - ยืนยันความถูกต้องของข้อมูลหรือระบุตัวตนผู้ใช้ได้

การปฏิเสธความรับผิดชอบ - ป้องกันผู้ใช้ปฏิเสธความรับผิดชอบข้อมูลที่ส่งออกไป

ส่วนประกอบหลักของเทคโนโลยีการเข้ารหัสก็คือ “การเข้ารหัสลับ (encryption)” และ “การถอดรหัสลับ (decryption)” โดยการเข้ารหัสลับคือการทำให้ข้อมูลที่อ่านได้ (plaintext) ไปทำการแปลงข้อมูล แปลงสภาพให้กลายเป็นข้อมูลที่ไม่สามารถอ่านได้ (ciphertext) ก่อนส่งต่อข้อมูลไปยังผู้รับปลายทางที่มีชุดเข้ารหัสที่ตรงกันทำ การถอดรหัสลับ (decryption) ที่ครอบคลุมออกด้วยการถอดข้อมูล ให้ข้อมูลที่ไม่สามารถอ่านได้กลับมาเป็นข้อมูลที่สามารถอ่านได้เหมือนเดิม

เทคโนโลยีการเข้ารหัสลับที่ใช้เป็นมาตรฐานและได้รับความนิยมด้วยกัน 2 แบบ คือการเข้ารหัสลับแบบกุญแจสมมาตร (Symmetric Key Encryption) และการเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Encryption) ซึ่งความแตกต่างของการเข้ารหัสสองแบบคือ แบบสมมาตรทั้งผู้ส่งและผู้รับจะมีกุญแจรหัสเหมือนกัน ส่วนแบบอสมมาตรนั้น กุญแจจะแบ่งออกเป็นสองชุด คือ กุญแจส่วนตัว (Private Key) กับกุญแจสาธารณะ (Public Key) ซึ่งผู้ส่งกับผู้รับข้อมูลจะใช้คนละชุดเพื่อเข้ารหัสและถอดรหัส

ความแข็งแกร่งของการเข้ารหัสแบบสมมาตรขึ้นอยู่กับ 2 ปัจจัย คือ การแจกจ่ายกุญแจเข้ารหัส (Key Distribution) และอัลกอริธึมที่ใช้เข้ารหัส (Encryption algorithms) ซึ่งในปัจจุบันนี้ได้มีการนำกลศาสตร์ควอนตัม (Quantum Mechanics) เข้ามาใช้เพื่อให้การเข้ารหัสมีความปลอดภัยมากยิ่งขึ้น

- การแจกจ่ายกุญแจเข้ารหัสโดยใช้กลศาสตร์ควอนตัม เรียกว่าการแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution; QKD)
- การนำกลศาสตร์ควอนตัมมาใช้เสริมความแข็งแกร่งของอัลกอริธึมในการเข้ารหัสถูกเรียกว่า Post-quantum Cryptography

14.2.4 การแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution)

วิทยาการรหัสลับเชิงควอนตัมเป็นเทคโนโลยีการเข้ารหัสที่ถูกนำเสนอขึ้นมาเป็นครั้งแรกโดย Stephen Wiesner ในช่วงต้นทศวรรษ 1970 เทคโนโลยีดังกล่าวเป็นการใช้ปรากฏการณ์ทางฟิสิกส์ควอนตัมในการทำให้ช่องการสื่อสารระหว่าง 2 บุคคลบนระบบเครือข่ายมีความปลอดภัย ต่อมาในปี 1984 Charles Bennet และ Gilles Brassard ได้พัฒนาต่อยอดเพื่อใช้กลศาสตร์ควอนตัมในการแจกจ่ายกุญแจเข้ารหัส และเรียกอัลกอริธึมที่ใช้ว่า **BB84** ซึ่งภายหลังได้ถูกนำมาใช้งานกันอย่างแพร่หลายในปัจจุบัน [18] การแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม

มีจุดเด่น คือ ผู้ส่งและผู้รับสามารถตรวจจับได้ว่า กุญแจการเข้ารหัสถูกแอบดักฟังหรือเก็บข้อมูลโดยบุคคลที่สาม โดยอาศัยคุณสมบัติของกลศาสตร์ควอนตัม [2]

นอกจากอัลกอริธึม BB84 แล้ว ในปัจจุบันยังมีอัลกอริธึมที่ใช้สำหรับแจกจ่ายกุญแจเข้ารหัสอีกมากมาย เช่น B92, Entanglement-based QKD, QBC และอื่นๆ [9] ซึ่งในบทความนี้จะโฟกัสที่ BB84 ซึ่งเป็นอัลกอริธึมที่แพร่หลาย

ระดับความมั่นคงปลอดภัยของการเข้ารหัสลับเรามักพิจารณาจากตัวแปรสองเรื่องคือ **ความซับซ้อนของอัลกอริธึมที่ใช้เข้ารหัส** และ **ขนาดความยาวของกุญแจรหัส**

กุญแจที่ใช้เข้ารหัสจะมีหน่วยวัดจำนวนรหัสที่ใช้งานเรียกว่า “บิต (bit)” ยิ่งจำนวนบิตมากเท่าไรการเข้ารหัสก็ยิ่งมีความซับซ้อนและใช้เวลาทั้งการเข้ารหัสและถอดรหัสมากขึ้นตามไปด้วย ปัจจุบันขนาดกุญแจเข้ารหัสตามมาตรฐานความปลอดภัยที่มีความมั่นคงคือ 256 บิต

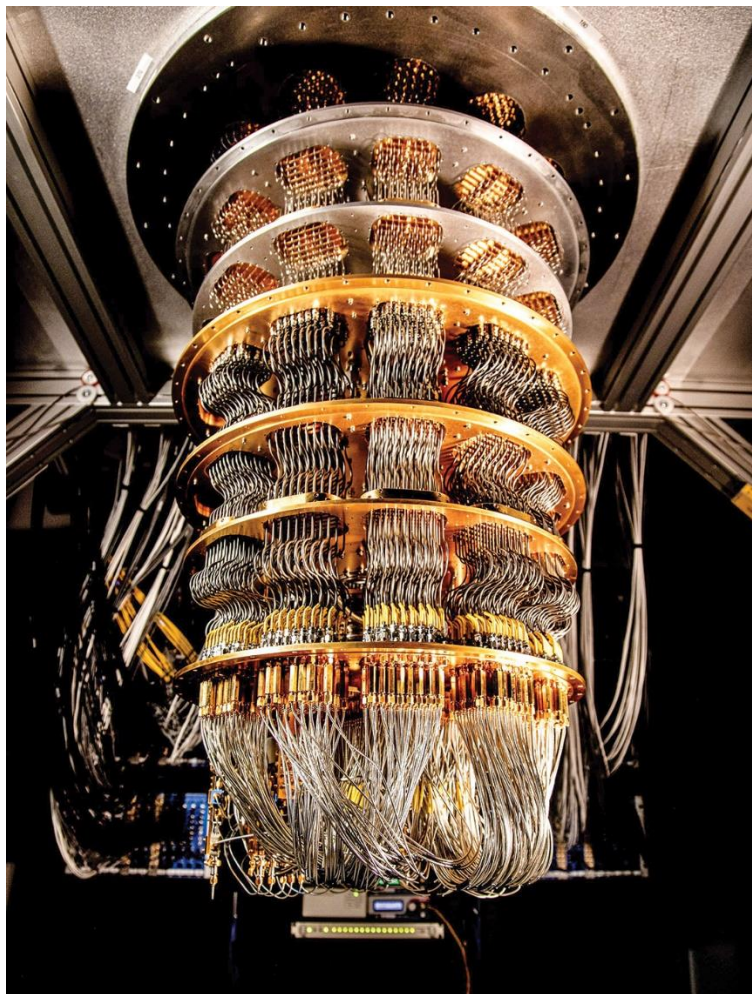
14.2.5 คอมพิวเตอร์ควอนตัม (Quantum Computer)

คอมพิวเตอร์ควอนตัม คือคอมพิวเตอร์ที่พัฒนาจากเทคโนโลยีการคำนวณแบบควอนตัม (Quantum Computing) ที่อาศัยคุณสมบัติเชิงควอนตัมของอนุภาคในระดับอะตอมมาเป็นต้นแบบในการพัฒนาเทคโนโลยีด้านนี้ขึ้น ควอนตัมเป็นการศึกษากลไกของอนุภาคต่าง ๆ ภายในโครงสร้างอะตอมที่นักวิทยาศาสตร์เริ่มสนใจศึกษามาตั้งแต่ปลายศตวรรษที่ 19 จนเข้าสู่ศตวรรษที่ 20 ได้เริ่มมีแนวคิดทฤษฎีเกี่ยวกับควอนตัมออกมาอย่างต่อเนื่อง นักวิทยาศาสตร์ที่จุดประกายการศึกษาเกี่ยวกับควอนตัมที่สำคัญสองคนหลักก็คือ แวนเนอร์ ไฮเซนเบิร์ก (Werner Heisenberg) กับ แอร์วิน ชเรอดิงเงอร์ (Erwin Schrodinger) ได้พยายามอธิบายปรากฏการณ์ทางควอนตัมที่ไม่สามารถใช้ทฤษฎีหลักการเชิงกลศาสตร์แบบเดิมอธิบายได้อีกต่อไป คุณลักษณะที่เป็นเอกลักษณ์ของควอนตัม มีดังนี้

เมื่อเราแยกอนุภาคของแสงออกจากกันและวัดค่าอนุภาคหนึ่ง อนุภาคที่แยกออกอีกตัวจะเปลี่ยนเป็นอีกค่าทันที ไม่ว่าอยู่ห่างกันแค่ไหนก็ตาม ปรากฏการณ์นี้เรียกว่า การพัวพันเชิงควอนตัม (Quantum Entanglement) เป็นต้นทางให้เกิดการพัฒนา เทคโนโลยีการสื่อสารควอนตัม (Quantum Communication) ขึ้น

ทฤษฎีความไม่แน่นอนเชิงควอนตัม (Uncertainty Principle) หลักการข้อนี้นำมาจากข้อเสนอของ ไฮเซนเบิร์ก ที่ว่า เราไม่สามารถทราบตำแหน่งและวัดค่าโมเมนตัมของอนุภาคในเวลาเดียวกันได้อย่างแม่นยำ อนุภาคสามารถมีสถานะ “มากกว่าหนึ่ง” ได้ในเวลาเดียวกัน การทับซ้อนของสถานะของอนุภาคเรียกว่า “ซูเปอร์โพสิชัน (Superposition)” ด้วยคุณสมบัติ “ซูเปอร์โพสิชัน” นี้เอง จึงมีการนำความรู้เกี่ยวกับควอนตัมมาใช้ในการพัฒนากระบวนการ คำนวณควอนตัม จนเป็นที่มาของคอมพิวเตอร์ควอนตัมในปัจจุบัน รูป 12.1

ความแตกต่างระหว่างคอมพิวเตอร์แบบเดิมที่ใช้กันทั่วไปกับคอมพิวเตอร์ควอนตัมที่ทั่วโลกกำลังพัฒนาขึ้น แตกต่างตั้งแต่พื้นฐานการประมวลผล ในคอมพิวเตอร์แบบเดิมนั้น เรียกหน่วยการประมวลผลว่า “บิต (bit)” ซึ่งอาศัยกระบวนการทางอิเล็กทรอนิกส์แสดงการประมวลผลออกมาเป็น 0 กับ 1 ค่าใดค่าหนึ่งเท่านั้น ในขณะที่คอมพิวเตอร์ควอนตัมเรียกหน่วยการประมวลผลว่า “คิวบิต (qubit)” อาศัยหลักการพัวพันทางควอนตัม และซูเปอร์โพสิชันของการหมุนอิเล็กตรอนหรือการเลี้ยวเบนของโฟตอน ซึ่งการแสดงผลในแบบควอนตัมสามารถแสดงออกมาเป็นทั้ง 0 1 หรือทั้งสองค่าเลยก็ได้ นอกจากนี้ความสามารถในการประมวลผลของคอมพิวเตอร์แบบเดิมจะเป็นสมการเชิงเส้น (linear) โดยประมวลผลตามลำดับ ต่างจากคอมพิวเตอร์ควอนตัมจะเป็นสมการเชิงพหุนาม (exponential) ทำให้ความเร็วและความสามารถในการประมวลผลข้อมูลแตกต่างกันมหาศาล



รูป 14.5 ตัวอย่างคอมพิวเตอร์ควอนตัมของ Google's quantum

(ที่มา: nature.org)

แม้ปัจจุบันจะยังเป็นช่วงเริ่มต้นของการพัฒนาคอมพิวเตอร์ควอนตัม ศักยภาพของเครื่องต้นแบบที่ออกมา ก็สามารถเร่งการพัฒนาด้านความรู้และเทคโนโลยีอุตสาหกรรมหลายด้านในระดับปฏิวัติองค์ความรู้ ไม่ว่าจะเป็นด้านการแพทย์ วัสดุศาสตร์ และการเงิน แน่นอนว่าผลกระทบด้านความปลอดภัยก็เริ่มส่งผลแล้วเช่นกัน

ทีมวิจัยของจีนได้รายงานการแยกตัวประกอบเลขด้วยคอมพิวเตอร์ควอนตัมแบบ RSA ระดับ 48 บิต ด้วยคอมพิวเตอร์ควอนตัมขนาดเพียง 10 คิวบิต เท่านั้น และคาดว่าจะสามารถเจาะรหัส RSA-2048 ที่มีระดับความปลอดภัย 2048 บิต ได้ด้วยคอมพิวเตอร์ควอนตัมขนาด 372 คิวบิต แม้จะมีข้อโต้แย้ง จาก สก็อต แอรอนสัน (Scott Aaronson) นักวิจัยคอมพิวเตอร์ควอนตัม และผู้อำนวยการ Quantum Information Center ของมหาวิทยาลัยเท็กซัส ออกมาให้ความเห็นว่ารายงานของจีนฉบับนี้มีช่องโหว่ ในการตั้งสมมติฐานและยังไม่สามารถสรุปผลออกมาตามที่รายงานได้ แต่เป็นที่แน่ชัดแล้วว่า ระบบความปลอดภัยข้อมูลดิจิทัลในปัจจุบันจะพบปัญหาแน่นอนเมื่อคอมพิวเตอร์ควอนตัมพร้อมใช้งานเชิงธุรกิจ จึงถือเป็นเรื่องเร่งด่วนที่ภาครัฐและเอกชนต่างพยายามพัฒนาระดับความปลอดภัยการเข้ารหัสข้อมูลให้สูงขึ้น

14.2.6 ภัยคุกคามจากคอมพิวเตอร์ควอนตัม

คอมพิวเตอร์ควอนตัมอาศัยคุณสมบัติเชิงควอนตัมในการคำนวณและประมวลผลทางคอมพิวเตอร์ ทำให้มีคุณสมบัติในการแก้ปัญหาทางคณิตศาสตร์บางประเภทที่คอมพิวเตอร์ในปัจจุบันยังไม่สามารถแก้ปัญหได้อย่างมีประสิทธิภาพและต้องใช้เวลาในการแก้ปัญหาดังกล่าว เช่น ปัญหาการแยกตัวประกอบของจำนวนเต็ม (Integer Factorization) การจำลองทางคณิตศาสตร์ (Simulation) และการคำนวณหาค่าเหมาะสมที่สุด (Optimization) ความสามารถในการประมวลผลของคอมพิวเตอร์ควอนตัมอาจถูกนำไปใช้เพื่อก่อให้เกิดประโยชน์ต่อเศรษฐกิจ และสังคม เช่น การพัฒนาวัสดุหรือตัวยาชนิดใหม่ การวินิจฉัยโรค และ การเพิ่มประสิทธิภาพในห่วงโซ่อุปทาน (Supply Chain Optimization) ทว่า ผู้ไม่ประสงค์ดีก็อาจนำคอมพิวเตอร์ควอนตัมไปใช้ในทางที่ผิด เช่น การโจมตีระบบของความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันได้

จากการศึกษาของ Daniels, K. และ Marcellino, C. (2009) ในหนังสือ Security of Quantum Cryptography using Photons for Quantum Key Distribution ระบุไว้ว่า ระบบการเข้ารหัสลับจะปลอดภัยจากการโจมตีเชิงกลศาสตร์ควอนตัมภายใต้เงื่อนไข 4 ประการ ได้แก่

- 1) บุคคลที่สามต้องไม่สามารถเข้าถึงหรือยุ่งเกี่ยวกับอุปกรณ์ที่ใช้สำหรับ Encode/Decode โฟตอนได้
- 2) อุปกรณ์สำหรับสุ่มบิตระหว่างผู้ส่งและผู้รับต้องเชื่อถือได้ และต้องเป็นการสุ่มแบบไม่มีเงื่อนไข เช่น ใช้ Quantum Random Bit Generator

3) ช่องทางติดต่อสื่อสารสาธารณะจะต้องใช้วิธีการพิสูจน์ตัวตนแบบปลอดภัยอย่างไรเงื่อนไข (Unconditionally Secure) หมายถึง วิทยาการรหัสลับที่ผู้โจมตีมีทรัพยากรอย่างไรขีดจำกัด เช่น จำนวนหน่วยประมวลผล, จำนวนคอมพิวเตอร์ที่ใช้, เวลา เป็นต้น ไม่สามารถเจาะระบบได้

4) แหล่งกำเนิดแสงต้องปล่อยโฟตอนเดี่ยวเท่านั้น

อย่างไรก็ตาม การติดตั้ง QKD ในภาคปฏิบัติยังคงถือว่ามีความท้าทายอยู่ เนื่องจากเงื่อนไขทั้ง 4 ประการนั้นสามารถทำให้เป็นจริงได้ยาก โดยเฉพาะการสร้างแหล่งกำเนิดโฟตอนเดี่ยว ระบบ QKD ในชีวิตจริงใช้แสงเลเซอร์เป็นแหล่งกำเนิดโฟตอน ซึ่งแสงเลเซอร์นี้จะทำการปล่อยโฟตอนที่หลายลูก ส่งผลให้แฮ็กเกอร์สามารถโจมตีแบบ Photon Number Splitting (PNS) เพื่อดักฟังข้อมูลได้

ระบบรักษาความปลอดภัยในปัจจุบัน เช่น Transport Layer Security (TLS) มีองค์ประกอบพื้นฐานสำคัญ คือ อัลกอริทึมรหัสลับทั้งประเภทกุญแจสมมาตรและกุญแจสมมาตรในการรักษาความปลอดภัย ในการสื่อสารผ่านทางอินเทอร์เน็ต ซึ่งเป็นอัลกอริทึมที่คอมพิวเตอร์ทั่วไปในปัจจุบันถ้าไม่มีกุญแจที่ใช้ในการเข้ารหัสลับจะไม่สามารถถอดรหัสลับได้ในระยะเวลาอันสั้น ซึ่งซูเปอร์คอมพิวเตอร์ (Supercomputer) อาจต้องใช้เวลามากกว่าพันปีในการถอดรหัสลับอัลกอริทึมรหัสลับดังกล่าว ทว่า คอมพิวเตอร์ควอนตัมอาจจะใช้เวลาเพียงไม่กี่ชั่วโมงในการถอดรหัสลับอัลกอริทึมเดียวกันนี้

14.2.7 ประเภทระบบรหัสลับที่โดนผลกระทบ

14.2.7.1 ระบบรหัสลับแบบกุญแจสมมาตร (Asymmetric Key Cryptography)

คอมพิวเตอร์ควอนตัมขนาดใหญ่สามารถใช้ในการประมวลผลอัลกอริทึมประเภท Shor (Shor's Algorithm) เพื่อการแก้ปัญหาทางคณิตศาสตร์ประเภทการแยกตัวประกอบเฉพาะ (Prime Factorization Problem) และลอการิทึมไม่ต่อเนื่อง (Discrete Logarithm Problem) ซึ่งสามารถนำไปใช้โจมตีระบบรหัสลับแบบกุญแจสมมาตร เช่น อัลกอริทึมประเภท Rivest-Shamir-Adleman (RSA) Diffie-Hellman และ Elliptic-Curve Cryptography (ECC) ได้รวดเร็วกว่าคอมพิวเตอร์ทั่วไปแบบเอกซ์โพเนนเชียล (Exponential Speed-Up) ส่งผลให้โปรโตคอล หรืออัลกอริทึมสำหรับการสื่อสารและแลกเปลี่ยนข้อมูลซึ่งอาศัยระบบรหัสลับแบบกุญแจสมมาตรเป็นองค์ประกอบ เช่น การลงลายมือชื่อดิจิทัล (Digital Signatures) และการแลกเปลี่ยนกุญแจ (Key Exchange) อาจไม่มีความปลอดภัยเพียงพออีกต่อไป

โปรโตคอลและอัลกอริทึมเหล่านี้มีความเสี่ยงจากการถูกโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลังโดยผู้ไม่ประสงค์ดี (Threat Actor) อาจดำเนินการดักฟังระบบเครือข่ายการสื่อสาร และจัดเก็บข้อมูลที่เป็นความลับ จากนั้นนำไปถอดรหัสลับในอนาคต ภายหลังจากที่คอมพิวเตอร์ควอนตัมขนาดใหญ่ได้ถูกพัฒนาขึ้นแล้ว นอกจากนี้ การลงลายมือชื่อดิจิทัลบนเอกสารอิเล็กทรอนิกส์ก็มีความเสี่ยง โดยผู้ไม่ประสงค์ดีอาจใช้

คอมพิวเตอร์ควอนตัมเพื่อคำนวณหากุญแจส่วนตัวเพื่อใช้ในการลงลายมือชื่อบนเอกสารสำคัญและแอบอ้างเป็นบุคคลอื่น

14.2.7.2 ระบบรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography)

ความปลอดภัยของระบบรหัสลับแบบกุญแจสมมาตรนั้น มีฐานปัญหาทางคณิตศาสตร์ที่แตกต่างจากระบบรหัสลับแบบกุญแจสมมาตร ทำให้ไม่สามารถใช้อัลกอริทึมประเภท Shor ในการโจมตีด้วยความเร็วที่เพิ่มมากขึ้นแบบเอกซ์โพเนนเชียลได้ โดยอัลกอริทึมสำหรับการโจมตีระบบรหัสลับแบบกุญแจสมมาตรคืออัลกอริทึมประเภท Grover (Grover's Algorithm) ซึ่งมีความรวดเร็วมากกว่าอัลกอริทึมแบบดั้งเดิม แบบยกกำลังสอง (Quadratic Speed-Up) เท่านั้น ดังนั้น อัลกอริทึมสำหรับการสื่อสารและแลกเปลี่ยนข้อมูลซึ่งอาศัยระบบรหัสลับแบบกุญแจสมมาตร เช่น Advanced Encryption Standard (AES) จึงได้รับผลกระทบจากการถูกโจมตีด้วยคอมพิวเตอร์ควอนตัมน้อยกว่าอัลกอริทึมที่ใช้ระบบรหัสลับแบบกุญแจสมมาตร

หากคอมพิวเตอร์ควอนตัมขนาดใหญ่ถูกพัฒนาขึ้น องค์กรอาจดำเนินการเพิ่มความยาวของกุญแจรหัสลับให้มากขึ้นเป็นสองเท่า เพื่อให้ระบบสารสนเทศมีระดับความปลอดภัยจากคอมพิวเตอร์ควอนตัมเทียบเท่ากับระบบเดิม ทั้งนี้ การเพิ่มความยาวของกุญแจนั้นอาจไม่สามารถดำเนินการได้โดยง่าย เนื่องจากข้อจำกัดในทั้งทางด้านซอฟต์แวร์และฮาร์ดแวร์ของแอปพลิเคชันที่มีการใช้งานขององค์กร โดยเฉพาะในระบบที่มีการใช้งานเป็นเวลายาวนานและในอุปกรณ์ขนาดเล็ก เช่น อุปกรณ์ IoTs (Internet of Things) อาจมีขนาดหน่วยความจำไม่เพียงพอทำให้องค์กรอาจมีความจำเป็นต้องพิจารณาใช้ทางเลือกอื่น

14.2.7.3 การเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง (Harvest Now, Decrypt Later)

ผู้ไม่ประสงค์ดีรวมถึงอาชญากรหรือผู้ก่อการร้ายข้ามชาติ อาจจะดำเนินการเก็บรวบรวมข้อมูลสำคัญขององค์กรหรือหน่วยงานของรัฐที่ถูกเข้ารหัสลับไว้ตั้งแต่ตอนนี้ และจัดเก็บไว้เพื่อรอวันที่คอมพิวเตอร์ควอนตัมถูกพัฒนาถึงจุดที่สามารถถอดรหัสลับข้อมูลเหล่านี้ได้ในอนาคต ดังนั้น ข้อมูลความลับที่มีความจำเป็นต้องจัดเก็บรักษาไว้เป็นระยะเวลานานมากกว่า 10 ปี เช่น ข้อมูลทางการทหาร ความลับทางธุรกิจ และข้อมูลทางด้านสุขภาพ เป็นต้น อาจมีความเสี่ยง ณ วินาทีต่อการถูกโจมตีแบบ Harvest Now, Decrypt Later ตัวอย่าง ที่สำคัญและเกิดขึ้นจริงในประวัติศาสตร์คือ โครงการเวโนนา (Venona Project) ในช่วงสงครามเย็น ซึ่งรัฐบาลประเทศสหรัฐอเมริกาดำเนินการเก็บเกี่ยวและจัดเก็บข้อมูลสื่อสารที่ถูกเข้ารหัสลับของสหภาพโซเวียตเพื่อการถอดรหัสลับในภายหลังระหว่างปี พ.ศ. 2486 ถึง พ.ศ. 2523 ทำให้สามารถดำเนินการจับกุมสายลับที่ปฏิบัติการจารกรรมในประเทศสหรัฐอเมริกาได้

14.3 วิทยาการรหัสลับควอนตัม

การเข้ารหัสด้วยควอนตัม (Quantum Cryptography) คือชุดวิธีการที่ใช้กฎของกลศาสตร์ควอนตัมที่แปลกประหลาดแต่เข้าใจง่าย เพื่อเข้ารหัส ส่ง และถอดรหัสข้อมูลอย่างปลอดภัย การเข้ารหัสด้วยควอนตัมใช้อุปกรณ์ควอนตัม เช่น เซ็นเซอร์ที่สามารถบันทึกอนุภาคแสงแต่ละอนุภาค (โฟตอน) เพื่อปกป้องข้อมูลจากการโจมตีแบบต่อต้าน แม้ว่าการเข้ารหัสด้วยควอนตัมจะมีความท้าทายทางเทคนิค แต่ก็มิชข้อได้เปรียบเหนือระบบการเข้ารหัสแบบเดิมที่ไม่ใช่ควอนตัม ยกตัวอย่างเช่น วิธีการเข้ารหัสด้วยควอนตัมมีศักยภาพในการตรวจจับและขัดขวางผู้ดักฟังที่พยายามดักจับข้อมูลได้ดีกว่า

ตัวอย่างแรกๆ ของโปรโตคอลการเข้ารหัสควอนตัมที่เรียกว่า การกระจายคีย์ควอนตัม (QKD) ใช้สตริงบิตหรืออักขระของคอมพิวเตอร์ (เรียกว่า คีย์เข้ารหัส) ร่วมกันโดยพันธมิตรที่เชื่อถือได้สองรายเพื่อเข้ารหัสและถอดรหัสข้อมูล แม้ว่าคีย์เข้ารหัสจะไม่ใช่ควอนตัม แต่มันถูกส่งผ่านโดยใช้อนุภาคควอนตัม หรือโฟตอน ในปี พ.ศ. 2547 นักวิทยาศาสตร์ชาวออสเตรียได้ใช้ QKD เพื่อสร้างการเชื่อมต่อที่ปลอดภัยสำหรับการโอนเงินจากธนาคารไปยังศาลาว่าการกรุงเวียนนา

อย่างไรก็ตาม ระบบ QKD ยังคงมีช่องโหว่ทั้งทางเทคโนโลยีและทฤษฎี ซึ่งช่องโหว่บางส่วนอาจทำให้ผู้ดักฟังสามารถดักจับและถอดรหัสข้อความได้ เนื่องจากข้อจำกัดเหล่านี้สำนักงานความมั่นคงแห่งชาติ จึงไม่แนะนำให้ใช้ QKD สำหรับระบบความมั่นคงแห่งชาติ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของเทคโนโลยีสารสนเทศในยุคของคอมพิวเตอร์ควอนตัมสามารถดำเนินการได้หลากหลายวิธี ปัจจุบันวิธีการหลัก คือ การปรับเปลี่ยนระบบรหัสลับในปัจจุบันไปใช้ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum Cryptography: PQC) ซึ่งประกอบไปด้วยอัลกอริทึมที่ถูกพัฒนาให้มีความทนทานต่อการโจมตีจากคอมพิวเตอร์ควอนตัม อีกวิธีการสำคัญหนึ่งคือการใช้การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD)

14.3.1 ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum cryptography)

ระบบรหัสลับสำหรับยุคควอนตัม (PQC) คือการเข้ารหัสที่ออกแบบมาเพื่อป้องกันการโจมตีจากคอมพิวเตอร์ควอนตัม โดยใช้ปัญหาทางคณิตศาสตร์ที่คอมพิวเตอร์ทุกประเภทไม่สามารถแก้ได้อย่างมีประสิทธิภาพ PQC ถูกพัฒนาเพื่อทดแทนระบบเดิม เช่น RSA, DH และ ECC ที่เสี่ยงต่อการถูกเจาะด้วยเทคโนโลยีควอนตัม อัลกอริทึม PQC สามารถใช้งานกับโครงสร้างพื้นฐานและอินเทอร์เน็ตปัจจุบัน แต่โดยทั่วไปจะใช้กุญแจรหัสลับขนาดใหญ่กว่าแบบดั้งเดิม ทำให้ต้นทุนการจัดเก็บและส่งข้อมูลสูงขึ้น การอัปเดตระบบสารสนเทศไปใช้ PQC ในองค์กรอาจซับซ้อนและมีผลกระทบต่อองค์ประกอบอื่น ๆ ของระบบ รวมถึงอาจต้องปรับปรุงฮาร์ดแวร์เพื่อรองรับการประมวลผลและหน่วยความจำที่เพียงพอสำหรับ PQC

องค์กรควรปรับปรุงระบบสารสนเทศให้มีความยืดหยุ่น รองรับการเปลี่ยนแปลงอัลกอริทึมรหัสลับได้อย่างรวดเร็ว (Crypto Agility) เพื่อเตรียมพร้อมสู่ยุคควอนตัม แม้จะมีมาตรฐานอัลกอริทึม PQC ที่หลากหลาย แต่ยังต้องพัฒนาและทดสอบต่อเนื่อง เพราะบางอัลกอริทึม อย่าง SIKE อาจถูกพบจุดอ่อนในอนาคต ดังนั้น ระบบควรสามารถสับเปลี่ยนอัลกอริทึมได้อย่างง่ายดาย

ถึงแม้ว่าอัลกอริทึม PQC จะถูกเริ่มพัฒนามาตั้งแต่หลายปีก่อนและได้รับการพัฒนาอย่างต่อเนื่อง จนในปัจจุบันมีอัลกอริทึม PQC จำนวนหนึ่งที่มีความสนใจจากผู้เชี่ยวชาญบางกลุ่มและบางองค์กร แต่อัลกอริทึม PQC เหล่านี้ยังคงอยู่ในช่วงการพัฒนาและยังไม่สมบูรณ์เต็มที่ ยังจำเป็นต้องมีการศึกษาเพิ่มเติม และการทดสอบอย่างเข้มงวดจึงจะเชื่อมั่นได้ว่ามีความมั่นคงปลอดภัยและเหมาะกับการใช้งานในสภาพแวดล้อมจริง

14.3.2 การกระจายกุญแจเชิงควอนตัม (Quantum key distribution)

การกระจายกุญแจเชิงควอนตัม (QKD) คือวิธีแลกเปลี่ยนกุญแจรหัสลับโดยใช้ปรากฏการณ์ควอนตัมและฮาร์ดแวร์เฉพาะทางสำหรับส่งคิวบิตแสง หากมีการดักฟัง การเปลี่ยนแปลงของคิวบิตจะช่วยให้ตรวจสอบได้ทันที ทำให้มั่นใจว่าข้อมูลปลอดภัยและเหมาะสำหรับใช้ในโพรโทคอลสื่อสารอื่น ๆ

การแลกเปลี่ยนกุญแจด้วยกระบวนการประเภท QKD มีความปลอดภัยในทางทฤษฎี (Theoretically Secure) จากทั้งคอมพิวเตอร์แบบดั้งเดิมและคอมพิวเตอร์ควอนตัม ทั้งนี้ QKD นั้นมีข้อจำกัดในแง่ของการใช้งาน ทำให้ใช้ได้กับบางกรณีการใช้งานที่เฉพาะเจาะจงเท่านั้น ข้อจำกัดของเทคโนโลยี QKD ในปัจจุบันมีดังนี้

- QKD เหมาะสำหรับการใช้งานระยะทางไม่เกิน 125 กิโลเมตรผ่านใยแก้วนำแสงแบบจุดต่อจุด โดยอนาคตอาจใช้ Quantum repeaters หรือดาวเทียมเพื่อขยายระยะทางได้
- อัตราแลกเปลี่ยนกุญแจของ QKD ต่ำกว่าโพรโทคอลแบบเก่า แม้ปัจจุบัน QKD จะเกิน 1 Mbps แต่ก็เหมาะกับบางแอปพลิเคชันเท่านั้น
- QKD มีความจำเป็นต้องใช้ฮาร์ดแวร์เฉพาะทางซึ่งอาจมีต้นทุนสูง
- QKD ใช้แลกเปลี่ยนกุญแจได้ แต่ไม่รองรับการยืนยันตัวตน จึงต้องใช้วิธีหรือโพรโทคอลอื่นสำหรับยืนยันตัวตนเมื่อสร้างเครือข่าย QKD
- QKD อาจมีความเสี่ยงต่อช่องโหว่ด้านความปลอดภัยของอุปกรณ์ฮาร์ดแวร์ รวมถึงการโจมตีแบบ Side-Channel ที่อาศัยการวิเคราะห์ข้อมูล เช่น ความร้อนหรือคลื่นแม่เหล็กไฟฟ้าจากอุปกรณ์ฮาร์ดแวร์

14.3.3 ระบบแบบผสม (Hybrid Solutions)

การพัฒนาระบบสารสนเทศให้มีความทนทานจากการโจมตีโดยคอมพิวเตอร์ควอนตัมนี้สามารถดำเนินการได้หลากหลายวิธี โดยเทคโนโลยีที่แตกต่างกันสามารถนำมาใช้ร่วมกันเพื่อส่งเสริมและชดเชยข้อจำกัดของกันและกันได้ ดังนั้น จึงควรนำเทคโนโลยีเหล่านี้มาใช้งานร่วมกันอย่างเหมาะสมเพื่อให้การย้ายระบบรหัสลับเป็นไปได้อย่างราบรื่น ใช้งานได้ดี และมีประสิทธิภาพ

ในการจัดทำระบบสารสนเทศแบบผสมระหว่างระบบรหัสลับแบบดั้งเดิมและ PQC องค์กรควรประเมินความต้องการภายในองค์กรตนเองเพื่อที่จะได้วางแผนการออกแบบระบบเพื่อลดความเสี่ยงต่างๆ ให้มีความเหมาะสมกับสินทรัพย์ทางสารสนเทศและแอปพลิเคชันขององค์กร ANSSI BSI และ IETF ได้ให้ความเห็นว่ามีวิธีการแบบผสมที่คุ้มค่าที่สุดคือการผสมระบบรหัสลับแบบดั้งเดิมและ PQC ด้วยกัน ซึ่งทาง IETF เพิ่งออก RFC 9370 สำหรับ IKEv2 โดยใช้การแลกเปลี่ยนกุญแจรหัสลับผสมทั้งแบบดั้งเดิมและแบบที่ทนทานต่อการโจมตีด้วยควอนตัมเพื่อใช้ในการสร้างกุญแจรหัสลับสุดท้าย

14.3.4 แนวคิดริเริ่มเกี่ยวกับการเข้ารหัสยุคหลังควอนตัม (PQC Initiative)

สำนักงานความมั่นคงปลอดภัยโครงสร้างพื้นฐานและไซเบอร์ (Cyber Security and Infrastructure Security Agency: CISA) แห่งประเทศสหรัฐอเมริกา ได้เสนอแนวคิดริเริ่มในการพัฒนาเทคโนโลยีการเข้ารหัสหลังยุคควอนตัม มีหลักการที่เป็นแนวทางให้การนำเทคโนโลยีมาใช้งานไว้ 4 ข้อคือ

การประเมินความเสี่ยง ประเมินช่องโหว่ของระบบโครงสร้างพื้นฐานที่สำคัญของสหรัฐอเมริกา โดยประเมินความเสี่ยงใน 55 ฟังก์ชันสำคัญระดับชาติ (National Critical Functions: NCFs) การพิจารณาความสำคัญในระดับมหภาคของแต่ละฟังก์ชันของ NCF นั้น CISA จะประเมินจาก ความสำคัญของการข้อมูลที่ต้องได้รับการปกป้องจุดที่มีความเสี่ยงสูง การเปลี่ยนแปลงระดับการเข้ารหัสหลังยุคควอนตัมว่าดำเนินการถึงจุดไหนแล้ว และสิ่งที่ต้องการการสนับสนุนจากรัฐบาลกลาง

การวางแผน แผนที่ CISA ทำงานร่วมกับพันธมิตรควมมุ่งเน้นด้านทรัพยากรและการมีส่วนร่วมของผู้ประกอบการและผู้ปฏิบัติงาน ทั้งในภาครัฐและเอกชน

นโยบายและมาตรฐาน ทำงานกับพันธมิตรเพื่อส่งเสริมการนำนโยบายด้านมาตรฐาน และ ข้อกำหนดไปใช้ในการปรับปรุงด้านความปลอดภัยของหน่วยงานบริหารพลเรือนของรัฐบาลกลาง (Federal Civilian Executive Branch: FCEB) รัฐ ท้องถิ่น พื้นที่ชนเผ่า รวมไปถึงดินแดน (SLTT) ในส่วนโครงสร้างพื้นฐานที่สำคัญและเทคโนโลยีพื้นฐานที่สนับสนุน

การมีส่วนร่วมและตระหนักรู้ มีส่วนร่วมกับผู้มีส่วนได้ส่วนเสียในการพัฒนาแผนบรรเทา ผลกระทบ และ สนับสนุนการนำมาตรฐานไปใช้ทันทีพร้อมใช้งานทั้งในส่วน FCEB SLTT และโครงสร้างพื้นฐานสำคัญต่าง ๆ รวมถึง พัฒนาผลิตภัณฑ์ด้านเทคนิคเพื่อสนับสนุนพันธกิจ เหล่านี้ให้ลุล่วง

ในส่วนการคัดกรองเทคโนโลยีตัวอย่างสำหรับเป็นมาตรฐานในการพัฒนาเทคโนโลยีการเข้ารหัสยุคหลัง ควอนตัมนั้น NIST ได้พิจารณาเทคโนโลยีให้ผ่านการพิจารณาในรอบที่สามได้แก่ CRYSTALS-KYBER CRYSTALS-Dilithium Falcon และ SPHINCS โดยแบ่งเป็นกลไกการเข้ารหัสแบบกุญแจลับ 1 และลายเซ็น ดิจิทัล 3 แบบ

14.3.5 มาตรฐานการเข้ารหัสหลังควอนตัม

นักวิจัยทั่วโลกกำลังเร่งพัฒนาเทคโนโลยีดิจิทัลแบบใหม่ที่เรียกว่าคอมพิวเตอร์ควอนตัม ซึ่งสามารถทำสิ่ง ต่างๆ มากมายที่คอมพิวเตอร์ทั่วไปทำไม่ได้ ซึ่งรวมถึงการทำลายระบบป้องกันที่รักษาความปลอดภัยข้อมูล อิเล็กทรอนิกส์ที่เป็นความลับ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) สหรัฐอเมริกา กำลังเป็นผู้นำความ พยายามระดับโลกในการสร้างระบบป้องกันทางอิเล็กทรอนิกส์เพื่อรับมือกับการโจมตีประเภทนี้ ผ่านโครงการ Post-Quantum Cryptography (PQC) ซึ่งเปิดตัวมาตรฐาน PQC ฉบับสมบูรณ์สามมาตรฐานแรกในปี พ.ศ. 2567 NIST เปิดตัวมาตรฐานการเข้ารหัสหลังควอนตัม 3 มาตรฐานแรกที่เสร็จสมบูรณ์ วันที่ 13 สิงหาคม 2567 รูป 12.3

อัลกอริทึมชุดแรกที่ NIST ประกาศใช้สำหรับการเข้ารหัสหลังควอนตัมนี้มีพื้นฐานมาจากโครงตาข่ายที่มี โครงสร้างและฟังก์ชันแฮช ซึ่งเป็นกลุ่มปัญหาทางคณิตศาสตร์ 2 กลุ่มที่สามารถต้านทานการโจมตีของ คอมพิวเตอร์ควอนตัมได้ โดยได้เปิดตัวชุดเครื่องมือเข้ารหัสชุดสุดท้ายที่ออกแบบมาเพื่อทนทานต่อการโจมตีจาก คอมพิวเตอร์ควอนตัม มาตรฐานการเข้ารหัสหลังควอนตัมเหล่านี้ช่วยรักษาความปลอดภัยข้อมูลอิเล็กทรอนิกส์ใน วงกว้าง ตั้งแต่ข้อความอีเมลที่เป็นความลับไปจนถึงธุรกรรมอีคอมเมิร์ซที่ขับเคลื่อนเศรษฐกิจยุคใหม่ NIST กำลัง สนับสนุนให้ผู้ดูแลระบบคอมพิวเตอร์เริ่มเปลี่ยนผ่านไปสู่มาตรฐานใหม่โดยเร็วที่สุด

NIST ได้สรุปชุดอัลกอริทึมการเข้ารหัสหลักที่ออกแบบมาเพื่อต้านทานการโจมตีทางไซเบอร์จาก คอมพิวเตอร์ควอนตัม นักวิจัยทั่วโลกกำลังเร่งสร้างคอมพิวเตอร์ควอนตัมที่จะทำงานในรูปแบบที่แตกต่างอย่าง สั้นชิงจากคอมพิวเตอร์ทั่วไป และสามารถถอดรหัสลับในปัจจุบันที่มอบความปลอดภัยและความเป็นส่วนตัวให้กับ ทุกสิ่งที่เราทำออนไลน์ได้ อัลกอริทึมที่ประกาศในวันนี้ได้รับการกำหนดไว้ในมาตรฐานชุดแรกที่เสร็จสมบูรณ์ จาก โครงการมาตรฐานการเข้ารหัสหลังควอนตัม (PQC) ของ NIST และพร้อมใช้งานได้ทันที

มาตรฐานใหม่ทั้งสามนี้ถูกสร้างขึ้นเพื่ออนาคต เทคโนโลยีคอมพิวเตอร์ควอนตัมกำลังพัฒนาอย่างรวดเร็ว และผู้เชี่ยวชาญบางคนคาดการณ์ว่าอุปกรณ์ที่มีความสามารถในการเจาะระบบการเข้ารหัสในปัจจุบันอาจปรากฏ

เครดิต: N. Hanacek/NIST

การเข้ารหัสถือเป็นภาระหนักในสังคมดิจิทัลยุคใหม่ การเข้ารหัสช่วยปกป้องความลับทางอิเล็กทรอนิกส์มากมายนับไม่ถ้วน เช่น เนื้อหาในอีเมล บันทึกทางการแพทย์ และคลังภาพ รวมถึงข้อมูลสำคัญต่อความมั่นคงของ

ชาติ ข้อมูลที่เข้ารหัสสามารถส่งผ่านเครือข่ายคอมพิวเตอร์สาธารณะได้ เนื่องจากไม่สามารถอ่านได้โดยทุกคน ยกเว้นผู้ส่งและผู้รับที่ตั้งใจไว้

เครื่องมือเข้ารหัสอาศัยใจทฤษฎีคณิตศาสตร์ที่ซับซ้อน ซึ่งคอมพิวเตอร์ทั่วไปพบว่ายากหรือเป็นไปไม่ได้ที่จะแก้ อย่างไรก็ตาม คอมพิวเตอร์ควอนตัมที่มีประสิทธิภาพเพียงพอจะสามารถคัดกรองวิธีแก้ปัญหานั้นได้จำนวนมากได้อย่างรวดเร็ว ซึ่งถือเป็นการเอาชนะการเข้ารหัสในปัจจุบัน อัลกอริทึมที่ NIST กำหนดมาตรฐานนั้นอิงจากใจทฤษฎีคณิตศาสตร์ที่แตกต่างกัน ซึ่งอาจสร้างอุปสรรคต่อทั้งคอมพิวเตอร์ทั่วไปและคอมพิวเตอร์ควอนตัม

การเข้ารหัสใช้คณิตศาสตร์เพื่อปกป้องข้อมูลอิเล็กทรอนิกส์ที่ละเอียดอ่อน รวมถึงเว็บไซต์และอีเมลที่ปลอดภัย ระบบเข้ารหัสถูกแจกจ่ายสาธารณะที่ใช้กันอย่างแพร่หลาย ซึ่งอาศัยใจทฤษฎีคณิตศาสตร์ที่คอมพิวเตอร์ไม่สามารถแก้ได้ ช่วยให้มั่นใจได้ว่าเว็บไซต์และข้อความเหล่านี้จะไม่สามารถเข้าถึงได้โดยบุคคลที่สามที่ไม่พึงประสงค์ ก่อนตัดสินใจเลือก NIST ไม่เพียงแต่พิจารณาความปลอดภัยของคณิตศาสตร์พื้นฐานของอัลกอริทึมเท่านั้น แต่ยังพิจารณาถึงแอปพลิเคชันที่ดีที่สุดสำหรับอัลกอริทึมเหล่านั้นด้วย

มาตรฐานใหม่นี้ออกแบบมาสำหรับงานสำคัญสองประการที่มักใช้การเข้ารหัส ได้แก่ การเข้ารหัสทั่วไป ซึ่งใช้เพื่อปกป้องข้อมูลที่แลกเปลี่ยนกันผ่านเครือข่ายสาธารณะ และลายเซ็นดิจิทัล ซึ่งใช้สำหรับการยืนยันตัวตน NIST ได้ประกาศเลือกอัลกอริทึม 4 แบบ ได้แก่ CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+ และ FALCON ซึ่งกำหนดมาตรฐานในปี 2022 และเผยแพร่ร่างมาตรฐานทั้งสามฉบับในปี 2023 ร่างมาตรฐานฉบับที่สี่ซึ่งใช้ FALCON มีกำหนดเผยแพร่ปลายปี 2024

แม้ว่าจะไม่มีการเปลี่ยนแปลงที่สำคัญใดๆ เกิดขึ้นกับมาตรฐานนับตั้งแต่มีการร่างเวอร์ชัน แต่ NIST ก็ได้เปลี่ยนชื่ออัลกอริทึมเพื่อระบุเวอร์ชันที่ปรากฏในมาตรฐานขั้นสุดท้ายสามมาตรฐาน ซึ่งได้แก่:

มาตรฐานการประมวลผลข้อมูลของรัฐบาลกลาง (FIPS) 203 มีวัตถุประสงค์เพื่อเป็นมาตรฐานหลักสำหรับการเข้ารหัสทั่วไป ข้อดีอย่างหนึ่งของมาตรฐานนี้คือถูกแจกจ่ายเข้ารหัสที่มีขนาดเล็กกว่ามาก ซึ่งทั้งสองฝ่ายสามารถแลกเปลี่ยนกันได้อย่างง่ายดาย รวมถึงความเร็วในการทำงาน มาตรฐานนี้ใช้อัลกอริทึม CRYSTALS-Kyber ซึ่งได้เปลี่ยนชื่อเป็น ML-KEM ซึ่งย่อมาจาก Module-Lattice-Based Key-Encapsulation Mechanism

FIPS 204 มีวัตถุประสงค์เพื่อเป็นมาตรฐานหลักสำหรับการปกป้องลายเซ็นดิจิทัล มาตรฐานนี้ใช้อัลกอริทึม CRYSTALS-Dilithium ซึ่งได้เปลี่ยนชื่อเป็น ML-DSA ซึ่งย่อมาจาก Module-Lattice-Based Digital Signature Algorithm

FIPS 205 ออกแบบมาสำหรับลายเซ็นดิจิทัลเช่นกัน มาตรฐานนี้ใช้อัลกอริทึม Sphincs+ ซึ่งได้เปลี่ยนชื่อเป็น SLH-DSA ซึ่งย่อมาจาก Stateless Hash-Based Digital Signature Algorithm มาตรฐานนี้ใช้วิธีการทางคณิตศาสตร์ที่แตกต่างจาก ML-DSA และมีวัตถุประสงค์เพื่อใช้เป็นวิธีสำรองในกรณีที่ ML-DSA พบว่ามีช่องโหว่



รูป 14.7 การเดินทางสู่อัลกอริทึมที่ทนทานต่อควอนตัม: ความคิดริเริ่มของ NIST

(ที่มา: NIST)

ในทำนองเดียวกัน เมื่อร่างมาตรฐาน FIPS 206 ที่สร้างขึ้นโดยใช้ FALCON ได้รับการเผยแพร่ อัลกอริทึมดังกล่าวจะถูกเรียกว่า FN-DSA ซึ่งย่อมาจาก FFT (fast-Fourier transform) โดยใช้อัลกอริทึมลายเซ็นดิจิทัลแบบอิง NTRU-Lattice

14.3.6 ความท้าทายในการใช้การเข้ารหัสควอนตัมในการรักษาความมั่นคงปลอดภัย

14.3.6.1 การใช้การเข้ารหัสควอนตัมเพื่อส่งและรับข้อมูลอย่างปลอดภัยมีอะไรบ้าง

การเข้ารหัสควอนตัมจำเป็นต้องใช้อุปกรณ์ที่มีความไวสูงเป็นพิเศษและมีสัญญาณรบกวนต่ำ อุปกรณ์ดังกล่าวสามารถส่งและบันทึกโฟตอน อะตอม หรืออนุภาคอื่นๆ ได้อย่างน่าเชื่อถือ เพื่อเข้ารหัสและส่งข้อความ แต่ไม่มีเครื่องมือใดทำงานได้อย่างสมบูรณ์แบบ ข้อจำกัดทางกายภาพของอุปกรณ์ก่อให้เกิดข้อบกพร่องที่อาจเกิดขึ้นในการเข้ารหัสควอนตัม ผู้ดักฟังสามารถใช้ประโยชน์จากข้อบกพร่องเหล่านี้เพื่อหลีกเลี่ยงการตรวจจับได้

ตัวอย่างเช่น ระบบเข้ารหัสควอนตัมหลายระบบเข้ารหัสข้อมูลโดยใช้โฟตอน แทนจะเป็นไปไม่ได้เลยที่จะสร้างเครื่องตรวจจับที่บันทึกโฟตอนทุกตัวที่กระทบ หรือการใช้แหล่งกำเนิดแสงที่สร้างโฟตอนได้ครั้งละหนึ่งตัวเสมอ บางครั้งระบบเหล่านี้ก็ปล่อยโฟตอนออกมาหลายตัวพร้อมกัน

การตรวจจับที่ผิดพลาด (เช่น การบันทึกโฟตอนในขณะที่ไม่มีอยู่) จะต้องถูกจำกัดให้น้อยที่สุด ชุดโฟตอนทั้งหมดในข้อความต้องถูกส่งและรับเพื่อเข้ารหัสและถอดรหัสข้อความอย่างถูกต้อง และฮาร์ดแวร์ต้องถูกสร้างขึ้นเพื่อป้องกันการปลอมแปลงโดยผู้บุกรุกที่พยายามขโมยข้อความ

ในทางทฤษฎี นักวิทยาศาสตร์สามารถปิดช่องโหว่เหล่านี้ได้มากมายด้วยการใช้โปรโทคอลที่ซับซ้อนยิ่งขึ้น บางครั้งโปรโทคอลเหล่านี้ถูกเรียกว่า "ไม่ขึ้นกับอุปกรณ์" เนื่องจากความปลอดภัยของโปรโทคอลนั้น "ไม่ขึ้นกับ" คุณสมบัติทางกายภาพหลายประการของอุปกรณ์ที่ดำเนินการตามโปรโทคอล

การสร้างอุปกรณ์ดังกล่าวไม่ใช่เรื่องง่าย แต่ NIST เป็นผู้ดำเนินการพัฒนาและสร้างเครื่องตรวจจับที่มีความละเอียดอ่อน ซึ่งเป็นองค์ประกอบสำคัญที่มีการประยุกต์ใช้งานได้ไกลเกินกว่าการเข้ารหัสด้วยควอนตัม ซึ่งรวมถึงเครื่องตรวจจับโฟตอนเดี่ยวที่ทำงานที่อุณหภูมิใกล้ศูนย์สัมบูรณ์ ซึ่งช่วยลดสัญญาณรบกวนและทำให้สามารถบันทึกโฟตอนแต่ละตัวได้อย่างแม่นยำ

14.3.6.2 ระบบการสื่อสารควอนตัมในโลกแห่งความเป็นจริงจะส่งข้อมูลได้อย่างไร

ระบบสื่อสารควอนตัมในชีวิตจริงอาจใช้โฟตอนในการส่งข้อมูลเป็นระยะทางหลายร้อยกิโลเมตรภายในเส้นใยแก้วนำแสง ในระยะทางที่ไกลเช่นนี้ การดูดซับโฟตอนในเส้นใยแก้วนำแสงจะจำกัดความสามารถในการส่งข้อมูลและรักษาคุณสมบัติควอนตัมที่เปราะบางของโฟตอน เช่น การพันกัน คุณสมบัติเหล่านี้มีความสำคัญอย่างยิ่งต่อการทำงานของระบบเข้ารหัสด้วยควอนตัม

เพื่อหลีกเลี่ยงปัญหานี้ นักวิทยาศาสตร์ของ NIST และนักวิจัยท่านอื่นๆ กำลังทดลองใช้โฟตอนในชุดเส้นใยแก้วนำแสงที่สั้นกว่าซึ่งเชื่อมต่อกันในเครือข่ายควอนตัม การดุดกลืนแสงอาจเป็นปัญหาได้แม้ในเครือข่ายของเส้นใยแก้วนำแสงที่สั้นกว่า ในระบบคลาสสิก (ไม่ใช่ควอนตัม) การสูญเสียดังกล่าวสามารถแก้ไขได้ด้วยการคัดลอกและขยายข้อมูล แต่ทฤษฎีบทไม่โคลนนิ่งไม่อนุญาตให้สิ่งนี้เกิดขึ้นในระบบควอนตัม ในทางกลับกัน นักวิทยาศาสตร์กำลังพัฒนาอุปกรณ์ที่เรียกว่าควอนตัมรีพีตเตอร์ ซึ่งจะกระจายและแลกเปลี่ยนความพันกันระหว่างโฟตอนในเครือข่ายควอนตัม ก่อให้เกิดความพันกันระยะไกลเพียงเส้นเดียวจากความพันกันระยะสั้นจำนวนมาก ซึ่งทำให้สามารถส่งข้อมูลควอนตัมได้ในระยะทางที่ไกลกว่าที่เป็นไปได้มาก

14.3.6.3 การเข้ารหัสด้วยควอนตัมสามารถพิสูจน์ได้อย่างไรว่าผู้ส่งข้อความคือตัวจริง?

ระบบเข้ารหัสควอนตัมมีเป้าหมายเพื่อสร้างช่องทางการสื่อสารที่ปลอดภัยระหว่างผู้ส่งและผู้รับ แต่เราจะมั่นใจได้อย่างไรว่าผู้ส่งหรือผู้รับไม่ใช่ผู้แอบอ้าง?

วิธีหนึ่งในการตรวจสอบคือการตรวจสอบตำแหน่งที่ตั้งของพวกเขา ตัวอย่างเช่น หากนักการทูตกำลังส่งข้อความลับกลับไปยังประเทศบ้านเกิดของพวกเขา เขาต้องการตรวจสอบว่าเซิร์ฟเวอร์คอมพิวเตอร์ที่กำลังสื่อสารด้วยนั้นอยู่ในประเทศของเขาจริงหรือไม่ เพื่อดำเนินการดังกล่าว นักวิจัยกำลังพัฒนาวิธีการที่เรียกว่า การตรวจสอบตำแหน่งควอนตัม (QPV) ซึ่งผู้รับจะต้องจัดการคิวบิตในลักษณะเฉพาะที่สามารถทำได้เฉพาะเมื่อคิวบิตอยู่ในตำแหน่งที่ควรจะเป็นเท่านั้น

ยังไม่มีผู้นำ QPV มาใช้ นักวิทยาศาสตร์จากศูนย์ร่วมด้านข้อมูลควอนตัมและวิทยาการคอมพิวเตอร์ ซึ่งเป็นความร่วมมือด้านการวิจัยระหว่าง NIST และมหาวิทยาลัยแมริแลนด์ เป็นหนึ่งในผู้ที่ศึกษาวิธีการทำให้ QPV ทำงานได้ในโลกแห่งความเป็นจริง

แม้ในกรณีที่ดีที่สุด QPV ก็สามารถยืนยันได้เพียงว่าผู้ส่ง *อยู่ที่ไหน ไม่ใช่ว่าเป็นใคร* ในการยืนยันตัวตนของผู้ส่ง ผู้ตรวจสอบจะรวมวิธีการเข้ารหัสควอนตัมเข้ากับใบรับรองดิจิทัล ซึ่งเป็นไฟล์อิเล็กทรอนิกส์ที่ทำหน้าที่เป็นรูปแบบหนึ่งของการระบุตัวตนออนไลน์ ใบรับรองประกอบด้วยข้อมูลต่างๆ เช่น ชื่อผู้ใช้ บริษัท หรือแผนก และที่อยู่ IP หรือหมายเลขซีเรียลของอุปกรณ์ ใบรับรองดิจิทัลประกอบด้วยสำเนาของคีย์สาธารณะจากผู้ถือใบรับรอง ซึ่งต้องจับคู่กับคีย์ส่วนตัวที่ตรงกันเพื่อยืนยันว่าเป็นของจริง

14.3.6.4 ความสับสนเชิงควอนตัมคืออะไร และมีบทบาทอย่างไรในระบบเข้ารหัสเชิงควอนตัม?

ตัวเลขสุ่มมีความสำคัญอย่างยิ่งต่อการเข้ารหัสและรักษาความปลอดภัยข้อมูลในเครือข่ายอิเล็กทรอนิกส์ ซึ่งเป็นกระบวนการที่เกิดขึ้นหลายร้อยพันล้านครั้งต่อวัน แต่ตัวเลขเหล่านี้ไม่ได้มีการสุ่มอย่างแท้จริง เนื่องจากมักถูกสร้างขึ้นโดยอุปกรณ์ทางกายภาพแบบคลาสสิก (ไม่ใช่ควอนตัม) ซึ่งผลลัพธ์แบบสุ่มที่คาดว่าจะเกิดขึ้นนั้นสามารถสร้างขึ้นได้จากส่วนประกอบ (เช่น ชิปคอมพิวเตอร์) ที่มีพฤติกรรมที่คาดการณ์ได้

ยกตัวอย่างเช่น การโยนเหรียญอาจดูเหมือนสุ่ม แต่ผลลัพธ์สามารถคาดการณ์ได้หากสามารถมองเห็นเส้นทางที่แน่นอนของเหรียญขณะที่มันกลิ้งไป เครื่องสร้างตัวเลขสุ่มในคอมพิวเตอร์อาจอาศัยซอฟต์แวร์ที่สร้างลำดับบิตจากจุดเริ่มต้นที่เรียกว่า "seed" อย่างไรก็ตาม seed ไม่ได้สุ่มอย่างสมบูรณ์และสามารถแสดงรูปแบบที่คาดการณ์ได้

ในทางกลับกัน ความสับสนแบบควอนตัมนั้นเป็นแบบสุ่มอย่างสมบูรณ์ เครื่องสร้างเลขสุ่มที่แท้จริงนั้นสามารถอาศัยระบบควอนตัมได้เท่านั้น เนื่องจากมีเพียงอนุภาคควอนตัมเท่านั้นที่ทำหน้าที่ในลักษณะที่ไม่สามารถคาดเดาได้อย่างสิ้นเชิง ตัวอย่างเช่น การสลายตัวของกัมมันตภาพรังสีของอะตอม ซึ่งพฤติกรรมถูกควบคุมโดยกลศาสตร์ควอนตัม เวลาที่อะตอมกัมมันตภาพรังสีสลายตัวนั้นมีความสุ่มอย่างสมบูรณ์ และพฤติกรรมสุ่มนี้สามารถนำมาใช้สร้างเลขสุ่มได้

ตัวอย่างเช่น หากคุณคูณอะตอมสลายตัวด้วยนาฬิกาที่เริ่มต้นที่ศูนย์วินาที อะตอมที่สลายตัวในช่วงวินาที "คี่" (1, 3, 5 เป็นต้น) สามารถกำหนดให้เป็น 0 ได้ และอะตอมที่สลายตัวในช่วงวินาที "คู่" (2, 4, 6 เป็นต้น) สามารถกำหนดให้เป็น 1 ได้ ด้วยวิธีนี้ ตัวอย่างอะตอมกัมมันตภาพรังสีจึงสามารถสร้างสตริงสุ่มของ 0 และ 1 ได้ นักวิจัยที่ NIST ได้พัฒนา เครื่องสร้างตัวเลขสุ่มที่แท้จริงโดยใช้ประโยชน์จากพฤติกรรมที่ไม่สามารถคาดเดาได้ในลักษณะเดียวกันของโฟตอนที่เคลื่อนที่ผ่านเขาวงกตของเลนส์และส่วนประกอบออปติกอื่นๆ

นักวิจัยอาศัยความสุ่มเชิงควอนตัมเพื่อส่งข้อมูลอย่างปลอดภัย ตัวเลขสุ่มเหล่านี้จะสร้าง “กุญแจ”ลับสำหรับเข้ารหัสและถอดรหัสข้อมูล แม้ว่าผู้เข้ารหัสมักใช้อัลกอริทึมทางคณิตศาสตร์ที่สามารถประมาณค่าสตริงของตัวเลขสุ่มได้ แต่กุญแจดังกล่าวก็ยังคงมีความเสี่ยงต่อแฮกเกอร์ เนื่องจากไม่ได้เป็นสิ่งที่คาดเดาได้ยาก

วิธีการแบบควอนตัมสร้างบิตดิจิทัล (1 และ 0) โดยใช้โฟตอน และเป็นส่วนหนึ่งของความพยายามอย่างต่อเนื่องเพื่อปรับปรุงสัญญาณสุ่มสาธารณะ ของ NIST ซึ่งกระจายบิตสุ่มสำหรับแอปพลิเคชัน เช่น การคำนวณที่ปลอดภัยที่เกี่ยวข้องกับคอมพิวเตอร์ในหลายตำแหน่งบนเครือข่าย

14.3.6.5 การเข้ารหัสควอนตัมสามารถรักษาความปลอดภัยในการประมวลผลข้อมูลส่วนตัวของเราบนเครือข่ายคอมพิวเตอร์ระยะไกลได้อย่างไร

นักวิทยาศาสตร์กำลังพัฒนาวิธีการเข้ารหัสควอนตัมเพื่อรับประกันความปลอดภัยของข้อมูลของเรา นอกเหนือไปจากการสื่อสารแบบธรรมดา ธุรกิจและองค์กรอื่นๆ มักส่งข้อมูลส่วนบุคคลของเราไปยังระบบคอมพิวเตอร์ระยะไกลหรือระบบคลาวด์ ซึ่งเข้าถึงได้ผ่านอินเทอร์เน็ต เนื่องจากพวกเขาไม่มีพลังการประมวลผลเพียงพอที่จะประมวลผลข้อมูลด้วยตนเอง อย่างไรก็ตาม สิ่งนี้กลับกลายเป็นปัญหา

แม้ว่าข้อมูลจะถูกเข้ารหัสก่อนที่จะเข้าถึงระบบเหล่านี้ แต่โดยทั่วไปแล้วจะต้องถอดรหัสเพื่อให้เครือข่ายสามารถประมวลผลได้ ซึ่งทำให้ข้อมูลมีความเสี่ยงต่อแฮกเกอร์ ซึ่งรวมถึงผู้ที่ควบคุมเครือข่ายซึ่งอาจไม่น่าเชื่อถือ

ด้วยการใช้หลักการควอนตัมของการซ้อนทับและการพันกัน นักวิจัยได้ค้นพบวิธีที่จะช่วยปิดช่องโหว่นี้ ข้อมูลที่เข้ารหัสด้วยคิวบิตสามารถถูกส่งไปยังเครือข่ายในลักษณะที่สามารถประมวลผลและส่งคืนอย่างปลอดภัย โดยที่เครือข่ายระยะไกลไม่สามารถทราบลักษณะของข้อมูลนั้น หรือปัญหาการคำนวณที่เครือข่ายได้รับมอบหมายให้ดำเนินการ กลยุทธ์ในการรักษาความปลอดภัยของข้อมูลนี้เรียกว่า การประมวลผลควอนตัมแบบตาบอด

โดยสรุป การเข้ารหัสด้วยควอนตัมใช้ประโยชน์จากกฎพื้นฐานของกลศาสตร์ควอนตัมเพื่อปกป้องข้อมูลและรับรองความถูกต้องของผู้ส่งและผู้รับข้อมูลนั้น นักวิทยาศาสตร์ของ NIST กำลังดำเนินการทดสอบและพัฒนา ระบบการเข้ารหัสด้วยควอนตัม สร้างเซ็นเซอร์ที่สามารถส่งและรับข้อความที่เข้ารหัสด้วยควอนตัมได้อย่างแม่นยำ และกำหนดมาตรฐานความสามารถของระบบการเข้ารหัสด้วยควอนตัม

หลักการเดียวกันกับที่เป็นพื้นฐานของการเข้ารหัสด้วยควอนตัม ทำให้สามารถพัฒนาคอมพิวเตอร์ควอนตัมได้ ซึ่งมีศักยภาพในการถอดรหัสรูปแบบที่ไม่ใช่ควอนตัมได้หลายรูปแบบ รวมถึงรูปแบบที่ใช้ปกป้องข้อมูลบนอินเทอร์เน็ตในปัจจุบัน นี่คือการเข้ารหัสหลังควอนตัม การเข้ารหัสหลังควอนตัมเตรียมความพร้อมสำหรับยุคอนาคตด้วยการปรับปรุงคอมพิวเตอร์แบบคลาสสิก (ที่ไม่ใช่ควอนตัม) ที่มีอยู่เดิมด้วยอัลกอริทึมที่ต้านทานการถอดรหัสโดยคอมพิวเตอร์ควอนตัม

14.4 ปัญญาประดิษฐ์กับความมั่นคงปลอดภัยข้อมูล

ในปี 2568 ธุรกิจต่างๆ จะต้องปรับกลยุทธ์เพื่อความยืดหยุ่นในการปฏิบัติงานในยุค AI โดยเน้นย้ำถึงความจำเป็นของแพลตฟอร์มความปลอดภัยแบบรวมศูนย์ AI ที่โปร่งใส และพันธมิตรข้ามสายงานเพื่อความยั่งยืนและความน่าเชื่อถือ

ภูมิทัศน์ของภัยคุกคามกำลังพัฒนาอย่างรวดเร็วการนำ AI มาใช้ในระยะเริ่มแรกของอาชญากรไซเบอร์ในยุคแรกเพื่อสร้างแผนการฟิชชิงและสมิซชิงที่ปรับแต่งได้เฉพาะบุคคล ซึ่งใช้ประโยชน์จากทั้งข้อมูลสาธารณะและข้อมูลส่วนบุคคล ปัจจุบันเราจะเห็นการเพิ่มขึ้นของ AI เชิงปฏิบัติที่กำหนดเป้าหมายไปที่โมเดลการเรียนรู้ของเครื่องเพื่อปิดการใช้งานระบบตรวจจับภัยคุกคามอัตโนมัติ

ภาคส่วนโครงสร้างพื้นฐานที่สำคัญ เช่น การดูแลสุขภาพ พลังงาน ธนาการ การขนส่ง และศูนย์ข้อมูล คาดว่าจะเผชิญกับความเสี่ยงที่สูงขึ้น ภาคส่วนเหล่านี้ถือเป็นเป้าหมายที่น่าสนใจเนื่องจากมีทรัพย์สินทางปัญญาและคลังข้อมูลสำคัญจำนวนมาก ทำให้มีความเสี่ยงต่อการหยุดชะงักที่ซับซ้อน

ตั้งแต่ปี 2569 เป็นต้นไป การโจมตีทางไซเบอร์ขั้นสูงส่วนใหญ่จะใช้ AI เพื่อดำเนินการโจมตีแบบหลายชั้นแบบพลวัต ซึ่งสามารถปรับเปลี่ยนมาตรการป้องกันได้ทันที การใช้งาน AI ที่เพิ่มสูงขึ้นทั้งจากผู้โจมตีและผู้ป้องกันจะเปลี่ยนแปลงภูมิทัศน์ด้านความมั่นคงปลอดภัยไซเบอร์ให้กลายเป็นการแข่งขันด้าน AI อย่างต่อเนื่องความสำเร็จในปีใหม่นี้จะขึ้นอยู่กับความสามารถรวมโซลูชันด้านความปลอดภัยและข้อมูลให้เป็นแพลตฟอร์มเดียว ความก้าวหน้าในการสร้างกรอบการกำกับดูแลและความไว้วางใจใน AI และการนำ AI มาใช้ควบคุมการปฏิบัติการด้านความปลอดภัย

14.4.1 AI ในด้านความปลอดภัยทางไซเบอร์คืออะไร?

ปัญญาประดิษฐ์ (AI) หมายถึงการประยุกต์ใช้อัลกอริทึมอัจฉริยะและเทคนิคการเรียนรู้ของเครื่องจักรเพื่อเพิ่มประสิทธิภาพการตรวจจับ ป้องกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ AI ช่วยให้ ระบบ รักษาความปลอดภัยทางไซเบอร์สามารถวิเคราะห์ข้อมูลจำนวนมหาศาล ระบุรูปแบบ และตัดสินใจอย่างรอบรู้ ด้วยความเร็วและขนาดที่เหนือขีดความสามารถของมนุษย์

บทบาทของ AI ในการเสริมสร้างมาตรการรักษาความมั่นคงปลอดภัยนั้นมีความหลากหลาย AI สามารถทำงานประจำต่างๆ เช่น การวิเคราะห์บันทึกและการสแกนช่องโหว่เป็นระบบอัตโนมัติช่วยให้นักวิเคราะห์มนุษย์มีเวลาไปทุ่มเทกับกิจกรรมที่ซับซ้อนและมีความสำคัญเชิงกลยุทธ์มากขึ้น AI ในด้านความมั่นคงปลอดภัยไซเบอร์มีบทบาทสำคัญในการตรวจจับภัยคุกคาม ระบบที่ขับเคลื่อนด้วย AI สามารถตรวจจับภัยคุกคามได้แบบเรียลไทม์ ช่วยให้ตอบสนองและบรรเทาภัยคุกคามได้อย่างรวดเร็ว นอกจากนี้ AI ยังสามารถปรับตัวและพัฒนา เรียนรู้จากข้อมูลใหม่ๆ อย่างต่อเนื่อง และพัฒนาความสามารถในการระบุและรับมือกับภัยคุกคามที่เกิดขึ้นใหม่

AI ในด้านความมั่นคงปลอดภัยไซเบอร์ปฏิบัติกรตรวจสอบจับภัยคุกคาม ตอบสนองโดยอัตโนมัติ และเสริมสร้างการจัดการช่องโหว่ AI ช่วยพัฒนากลยุทธ์ความมั่นคงปลอดภัยไซเบอร์ด้วยการวิเคราะห์พฤติกรรม ตรวจสอบจับพิกซ์และปรับตัวให้เข้ากับภัยคุกคามใหม่ๆ ส่งผลให้สามารถป้องกันเชิงรุกและปกป้องข้อมูลสำคัญได้

14.4.2 AI ช่วยป้องกันการโจมตีทางไซเบอร์ได้อย่างไร?

AI ในด้านความปลอดภัยทางไซเบอร์ช่วยเสริมข้อมูลด้านภัยคุกคามทางไซเบอร์ช่วยให้ผู้เชี่ยวชาญด้านความปลอดภัย โดยสามารถ:

1) **ค้นหาลักษณะของการโจมตีทางไซเบอร์:** AI วิเคราะห์ข้อมูลปริมาณมหาศาลเพื่อระบุรูปแบบและตัวบ่งชี้การบุกรุก วิธีนี้ช่วยให้ทีมรักษาความปลอดภัยสามารถระบุพฤติกรรมเครือข่ายที่น่าสงสัย ความพยายามในการเข้าสู่ระบบที่ผิดปกติ และการรับส่งข้อมูลที่ผิดปกติจากอุปกรณ์ IoT หรืออุปกรณ์ปลายทางได้แบบเรียลไทม์

2) **เสริมสร้างการป้องกัน:** AI สามารถช่วยให้ทีมรักษาความปลอดภัยสามารถแยกอุปกรณ์ที่ถูกบุกรุก บล็อกทราฟฟิกที่เป็นอันตราย และหยุดยั้งมัลแวร์ได้ด้วยการตรวจสอบระบบอย่างต่อเนื่อง นอกจากนี้ AI ยังคาดการณ์พื้นที่เสี่ยงสูงที่มีโอกาสเกิดการละเมิดได้มากที่สุด ช่วยให้องค์กรสามารถจัดการช่องโหว่เชิงรุกก่อนที่จะก่อให้เกิดข้อกังวลร้ายแรง

3) **วิเคราะห์ข้อมูลเพื่อยืนยันตัวตนผู้ใช้:** เครื่องมือ AI ช่วยให้ทีมรักษาความปลอดภัยวิเคราะห์ข้อมูลยืนยันตัวตนผู้ใช้ เช่น ลายนิ้วมือ รูปแบบการพิมพ์ และรูปแบบเสียง นอกจากนี้ เครื่องมือเหล่านี้ยังสามารถตรวจสอบพฤติกรรมผู้ใช้ระหว่างเซสชัน ตรวจสอบจับความผิดปกติ และดำเนินการยืนยันเพิ่มเติมเมื่อจำเป็น

4) **ระบุการโจมตีไปยังผู้ก่อภัยคุกคามเฉพาะ:** AI สามารถวิเคราะห์เครื่องมือที่ใช้ ที่อยู่ IP และรูปแบบพฤติกรรม และเชื่อมโยงเหตุการณ์กับผู้ก่อภัยคุกคามที่รู้จัก ซึ่งช่วยให้ทีมรักษาความปลอดภัยเข้าใจและระบุกลุ่มภัยคุกคามเฉพาะเจาะจงได้ง่าย

5) **ปรับปรุงการตรวจจับพิกซ์และสแปม:** AI ช่วยสแกนลิงก์อีเมล ไฟล์แนบ และข้อความ บล็อกความพยายามพิกซ์และสแปมก่อนที่จะถูกลาม

6) **รองรับการแบ่งปันข้อมูลภัยคุกคามร่วมกัน:** AI ช่วยให้องค์กรสามารถมีส่วนร่วมและรับประโยชน์จากความรู้ร่วมกันภายในชุมชนด้านความปลอดภัย ปรับปรุงความยืดหยุ่นร่วมกันต่อภัยคุกคามที่ขับเคลื่อนโดย AI ที่เปลี่ยนแปลงไป

14.4.3 การทำระบบอัตโนมัติรักษาความปลอดภัยข้อมูลทางไซเบอร์มีความปลอดภัยหรือไม่?

ปัจจุบันการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องอาศัยการแทรกแซงจากมนุษย์ อย่างไรก็ตาม งานต่างๆ เช่น การตรวจสอบระบบ สามารถทำโดยอัตโนมัติได้ด้วย AI การทำให้กระบวนการทำงาน

เป็นแบบอัตโนมัติจะช่วยเพิ่มขีดความสามารถด้านข้อมูลภัยคุกคามขององค์กร และประหยัดเวลาในการค้นหาภัยคุกคามใหม่ๆ ซึ่งเป็นสิ่งสำคัญอย่างยิ่งเมื่อ **การโจมตีทางไซเบอร์** มีความซับซ้อนมากขึ้น

ระบบอัตโนมัติด้านความปลอดภัยทางไซเบอร์ที่ใช้ AI มีความปลอดภัย เนื่องจากได้รับการพัฒนาจากกรณีการใช้งานที่มีอยู่แล้วในสภาพแวดล้อมทางธุรกิจที่หลากหลาย ตัวอย่างเช่น ทีมทรัพยากรบุคคล (HR) และทีมเทคโนโลยีสารสนเทศ (IT) ใช้ AI เพื่อเตรียมความพร้อมพนักงานใหม่ และมอบทรัพยากรและระดับการเข้าถึงที่เหมาะสมเพื่อให้พวกเขาทำงานได้อย่างมีประสิทธิภาพ

ระบบอัตโนมัติมีความสำคัญอย่างยิ่งในด้านความปลอดภัยทางไซเบอร์ เนื่องจากปัจจุบันยังมีปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญด้านความปลอดภัยอย่างต่อเนื่อง ซึ่งช่วยให้องค์กรต่างๆ สามารถเพิ่มประสิทธิภาพการลงทุนด้านความปลอดภัยและปรับปรุงการดำเนินงานได้โดยไม่ต้องกังวลเรื่องการหาบุคลากรที่มีทักษะเพิ่มเติม สามารถสรุปประโยชน์ของการใช้ AI อัตโนมัติในด้านความปลอดภัยทางไซเบอร์ ได้ดังนี้

1) ประหยัดต้นทุน : การผสมผสานความปลอดภัยทางไซเบอร์เข้ากับ AI ช่วยให้การรวบรวมข้อมูลรวดเร็วยิ่งขึ้น ทำให้การรับมือกับเหตุการณ์ต่างๆ เป็นไปอย่างมีประสิทธิภาพและคล่องตัวมากขึ้น นอกจากนี้ยังช่วยลดความจำเป็นที่ผู้เชี่ยวชาญด้านความปลอดภัยจะต้องทำงานด้วยตนเองซึ่งใช้เวลานาน เพื่อให้สามารถมุ่งเน้นไปที่กิจกรรมเชิงกลยุทธ์ที่เพิ่มมูลค่าให้กับธุรกิจได้มากขึ้น

2) การกำจัดข้อผิดพลาดของมนุษย์ : จุดอ่อนที่พบบ่อยของระบบป้องกันความปลอดภัยแบบดั้งเดิมคือความจำเป็นในการแทรกแซงโดยมนุษย์ ซึ่งอาจนำไปสู่ข้อผิดพลาดของมนุษย์ที่มีค่าใช้จ่ายสูง ปัญญาประดิษฐ์ในด้านความปลอดภัยทางไซเบอร์ช่วยลดองค์ประกอบของมนุษย์ออกจากกระบวนการรักษาความปลอดภัยส่วนใหญ่ วิธีนี้มีประสิทธิภาพมากกว่า เพราะสามารถจัดสรรทรัพยากรมนุษย์ไปยังตำแหน่งที่ต้องการมากที่สุดได้

3) การตัดสินใจที่ดีขึ้น : การทำให้ระบบรักษาความปลอดภัยทางไซเบอร์เป็นแบบอัตโนมัติช่วยให้องค์กรสามารถระบุและแก้ไขข้อบกพร่องที่อาจเกิดขึ้นในกลยุทธ์ด้านความปลอดภัยได้ ด้วยวิธีนี้ องค์กรจึงสามารถดำเนินขั้นตอนที่เป็นทางการ ซึ่งส่งผลให้สภาพแวดล้อมไอทีมีความปลอดภัยมากขึ้น

อย่างไรก็ตาม องค์กรต่างๆ จำเป็นต้องตระหนักว่าอาชญากรไซเบอร์กำลังปรับวิธีการเพื่อต่อต้านเครื่องมือรักษาความปลอดภัยทางไซเบอร์ AI ใหม่ๆ แอ็กเกอร์ยังใช้ AI เพื่อสร้างการโจมตีขั้นสูงและปล่อยมัลแวร์รูปแบบใหม่และรูปแบบที่อัปเดต เพื่อโจมตีทั้งระบบแบบดั้งเดิมและระบบที่เสริมประสิทธิภาพด้วย AI

14.4.4 การประยุกต์ใช้ AI ในด้านความปลอดภัยข้อมูลทางไซเบอร์

14.4.4.1 การป้องกันด้วยรหัสผ่านและการยืนยันตัวตน

ปัญญาประดิษฐ์ (AI) ในด้านความมั่นคงปลอดภัยไซเบอร์ ช่วยให้องค์กรต่างๆ สามารถปกป้องรหัสผ่านและรักษาความปลอดภัยบัญชีผู้ใช้ได้ดียิ่งขึ้นผ่าน**การยืนยันตัวตน** เว็บไซต์ส่วนใหญ่มีฟีเจอร์ที่อนุญาตให้ผู้ใช้เข้าสู่

ระบบเพื่อซื้อสินค้าหรือกรอกแบบฟอร์มติดต่อเพื่อให้กรอกข้อมูลสำคัญได้ จำเป็นต้องมีการรักษาความปลอดภัยเพิ่มเติมเพื่อรักษาความปลอดภัยของข้อมูลและป้องกันไม่ให้ข้อมูลตกไปอยู่ในมือของผู้ไม่ประสงค์ดี

เครื่องมือ AI เช่น CAPTCHA ระบบจดจำใบหน้า และเครื่องสแกนลายนิ้วมือ เป็นต้น ช่วยให้องค์กรต่างๆ ตรวจจับได้โดยอัตโนมัติว่าความพยายามในการเข้าสู่ระบบเป็นของจริงหรือไม่ โซลูชันเหล่านี้ช่วยป้องกันกลวิธีก่ออาชญากรรมทางไซเบอร์ เช่น การโจมตีแบบ Brute-force และการยึดยึดข้อมูลส่วนบุคคลซึ่งอาจทำให้เครือข่ายทั้งหมดขององค์กรตกอยู่ในความเสี่ยง

14.4.4.2 การควบคุมการตรวจจับและป้องกันฟิชชิง

ฟิชชิง ยังคงเป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่สำคัญที่สุดที่ธุรกิจในทุกอุตสาหกรรมต้องเผชิญ AI ในโซลูชันความปลอดภัยอีเมลช่วยให้บริษัทต่างๆ สามารถค้นพบความผิดปกติและตัวบ่งชี้ของข้อความอันตราย AI สามารถวิเคราะห์เนื้อหาและบริบทของอีเมล เพื่อค้นหาได้อย่างรวดเร็วว่าเป็นข้อความสแปม เป็นส่วนหนึ่งของแคมเปญฟิชชิง หรือเป็นอีเมลจริง ยกตัวอย่างเช่น AI สามารถระบุสัญญาณของฟิชชิงได้อย่างรวดเร็วและง่ายดาย เช่น การปลอมแปลงอีเมล (email spoofing) ผู้ส่งปลอมแปลง และชื่อโดเมนที่สะกดผิด เป็นต้น

เทคนิคอัลกอริทึม ML ช่วยให้ AI สามารถเรียนรู้จากข้อมูลเพื่อวิเคราะห์ข้อมูลได้อย่างแม่นยำยิ่งขึ้น และพัฒนาเพื่อรับมือกับภัยคุกคามใหม่ๆ นอกจากนี้ยังช่วยให้ AI เข้าใจวิธีการสื่อสาร พฤติกรรมทั่วไป และรูปแบบข้อความของผู้ใช้ได้ดียิ่งขึ้น ซึ่งเป็นสิ่งสำคัญอย่างยิ่งต่อการป้องกันภัยคุกคามขั้นสูง เช่น การโจมตีแบบสเปียร์ฟิชชิง (spear phishing) ซึ่งเกี่ยวข้องกับการโจมตีโดยผู้โจมตีที่พยายามปลอมตัวเป็นบุคคลสำคัญ เช่น ซีอีโอของบริษัท AI สามารถสกัดกั้นกิจกรรมที่น่าสงสัยเพื่อป้องกันการโจมตีแบบสเปียร์ฟิชชิงก่อนที่จะสร้างความเสียหายให้กับเครือข่ายและระบบขององค์กร

14.4.4.3 การจัดการความเสี่ยง

ในขณะที่อาชญากรไซเบอร์ใช้วิธีการและเทคนิคที่ซับซ้อนมากขึ้น ช่องโหว่ใหม่ๆ หลายพันแห่งถูกค้นพบ และรายงานทุกปี ส่งผลให้ธุรกิจต่างๆ ประสบปัญหาในการจัดการกับช่องโหว่ใหม่ๆ จำนวนมากที่พบเจอทุกวัน และระบบดั้งเดิมของพวกเขาไม่สามารถป้องกันภัยคุกคามที่มีความเสี่ยงสูงเหล่านี้ได้แบบเรียลไทม์

โซลูชันความปลอดภัยที่ขับเคลื่อนด้วย AI เช่น การวิเคราะห์พฤติกรรมผู้ใช้และเอนทิตี (UEBA) ช่วยให้ธุรกิจต่างๆ สามารถวิเคราะห์กิจกรรมของอุปกรณ์ เซิร์ฟเวอร์ และผู้ใช้ ช่วยให้สามารถระบุพฤติกรรมที่ผิดปกติหรือผิดปกติที่อาจบ่งชี้ถึง การโจมตีแบบ Zero-day ได้ AI ในด้านความมั่นคงปลอดภัยไซเบอร์สามารถปกป้องธุรกิจจากช่องโหว่ที่ไม่ทราบก่อนที่จะมีการรายงานและแก้ไขอย่างเป็นทางการ

14.4.4.4 ความปลอดภัยเครือข่าย

ความปลอดภัยของเครือข่ายเกี่ยวข้องกับกระบวนการที่ใช้เวลานานในการสร้างนโยบายและการทำความเข้าใจโครงสร้างเครือข่าย เมื่อมีนโยบายแล้ว องค์กรต่างๆ จะสามารถกำหนดกระบวนการต่างๆ เพื่อระบุการเชื่อมต่อที่ถูกต้องตามกฎหมาย เปรียบเทียบกับการเชื่อมต่อที่อาจต้องมีการตรวจสอบพฤติกรรมที่อาจเป็นอันตราย

นโยบายเหล่านี้ยังสามารถช่วยให้องค์กรต่างๆ ปรับใช้และบังคับใช้แนวทางการรักษาความปลอดภัยแบบ Zero Trust ได้อีกด้วย

อย่างไรก็ตาม การสร้างและดูแลรักษานโยบายบนเครือข่ายหลายเครือข่ายต้องใช้เวลาและความพยายามด้วยตนเองเป็นจำนวนมาก องค์กรต่างๆ มักไม่ได้ปรับใช้หลักการตั้งชื่อที่ถูกต้องสำหรับแอปพลิเคชันและเวิร์กโหลด ซึ่งหมายความว่าทีมรักษาความปลอดภัยอาจต้องใช้เวลามากขึ้นในการพิจารณาว่าเวิร์กโหลดใดเป็นของแอปพลิเคชันเฉพาะ AI จะเรียนรู้รูปแบบการรับส่งข้อมูลเครือข่ายขององค์กรเมื่อเวลาผ่านไป ทำให้สามารถแนะนำนโยบายและเวิร์กโหลดที่เหมาะสมได้

14.4.4.5 การวิเคราะห์พฤติกรรม

การวิเคราะห์พฤติกรรมช่วยให้องค์กรต่างๆ สามารถระบุภัยคุกคามที่เปลี่ยนแปลงไปและช่องโหว่ที่ทราบอยู่แล้วได้ ระบบป้องกันความปลอดภัยแบบดั้งเดิมอาศัยลายเซ็นการโจมตีและตัวบ่งชี้การบุกรุก (IOC) เพื่อค้นพบภัยคุกคาม อย่างไรก็ตาม ด้วยการโจมตีใหม่ๆ หลายพันครั้งต่อชั่วโมงการไซเบอร์เกิดขึ้นทุกปี แนวทางนี้จึงไม่สามารถใช้งานได้จริง

องค์กรต่างๆ สามารถใช้การวิเคราะห์พฤติกรรมเพื่อเพิ่มประสิทธิภาพกระบวนการตรวจจับภัยคุกคามได้โดยใช้โมเดล AI เพื่อพัฒนาโปรไฟล์ของแอปพลิเคชันที่ติดตั้งบนเครือข่าย และประมวลผลข้อมูลอุปกรณ์และผู้ใช้จำนวนมาก จากนั้นข้อมูลขาเข้าจะถูกวิเคราะห์เทียบกับโปรไฟล์เหล่านั้นเพื่อป้องกันกิจกรรมที่อาจเป็นอันตราย

14.4.4.6 เครื่องมือรักษาความปลอดภัยข้อมูลทางไซเบอร์ที่ขับเคลื่อนด้วย AI

ปัจจุบัน เทคโนโลยีความมั่นคงปลอดภัยข้อมูลในยุค AI ได้มีการผสาน AI รวมเข้ากับเครื่องมือรักษาความปลอดภัยทางไซเบอร์หลายตัวเพื่อเพิ่มประสิทธิภาพการทำงาน ต่อไปนี้คือตัวอย่างบางส่วน

1) โซลูชันความปลอดภัยปลายทางที่ขับเคลื่อนด้วย AI

โซลูชันเหล่านี้ใช้ประโยชน์จาก AI เพื่อตรวจจับและตอบสนองต่อภัยคุกคามบนจุดสิ้นสุด เช่น แล็ปท็อป เดสก์ท็อป และอุปกรณ์พกพาอย่างแท้จริง เพื่อปกป้องอุปกรณ์เหล่านี้จาก มัลแวร์ แรนซัมแวร์ และการโจมตีอื่นๆ

2) NGFW ที่ใช้ AI

ไฟร์วอลล์รุ่นถัดไป (NGFW: Next-Generation Firewall) ที่ผสมผสานความสามารถ AI มออบการป้องกันภัยคุกคามขั้นสูง ป้องกันการบุกรุก และควบคุมแอปพลิเคชัน เสริมความแข็งแกร่งให้กับความปลอดภัยของเครือข่าย

3) ข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (SIEM)

โซลูชัน SIEM (Security Information and Event Management) ที่ขับเคลื่อนด้วย AI จะวิเคราะห์บันทึกและเหตุการณ์ด้านความปลอดภัยจากแหล่งต่างๆ ช่วยให้ตรวจจับภัยคุกคาม ตรวจสอบ และตอบสนองได้รวดเร็วยิ่งขึ้น

4) โซลูชันความปลอดภัยบนคลาวด์ที่ขับเคลื่อนด้วย AI

โซลูชันเหล่านี้ใช้ AI เพื่อปกป้องข้อมูลและแอปพลิเคชันในสภาพแวดล้อมคลาวด์ เพื่อให้มั่นใจถึงความปลอดภัยและการปฏิบัติตามข้อกำหนด

5) โซลูชัน NDR ที่ขับเคลื่อนด้วย AI สำหรับการตรวจจับภัยคุกคามทางไซเบอร์

โซลูชันการตรวจจับและตอบสนองเครือข่าย (NDR: Network Detection and Response) ที่มีความสามารถของ AI คอยตรวจสอบปริมาณการใช้งานเครือข่ายเพื่อระบุและตอบสนองต่อภัยคุกคามที่ซับซ้อนซึ่งอาจหลีกเลี่ยงมาตรการรักษาความปลอดภัยแบบดั้งเดิม

14.4.4.7 อนาคตของ AI ในด้านความปลอดภัยทางไซเบอร์

AI ในด้านความมั่นคงปลอดภัยไซเบอร์กำลังมีบทบาทสำคัญมากขึ้นในการต่อสู้กับภัยคุกคามทางไซเบอร์ขั้นสูง เนื่องจาก AI เรียนรู้อย่างต่อเนื่องจากข้อมูลที่ได้รับเทคโนโลยีใหม่ๆ ที่สร้างขึ้นจากกระบวนการและเทคนิคของ AI จึงมีความสำคัญอย่างยิ่งต่อการระบุภัยคุกคามล่าสุด และป้องกันไม่ให้แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ใหม่ๆ ได้เร็วที่สุดเท่าที่จะเป็นไปได้

AI โดยเฉพาะอย่างยิ่ง Generative AI สามารถนำไปใช้ในด้านความปลอดภัยทางไซเบอร์ได้อย่างไร สามารถสรุปได้ดังนี้

Generative AI ซึ่งเป็นที่รู้จักในด้านความสามารถในการสร้างข้อมูลใหม่ที่คล้ายกับข้อมูลที่มีอยู่แล้ว ถือเป็นเครื่องมืออันทรงพลังสำหรับการปรับปรุงกลยุทธ์และการป้องกันด้านความปลอดภัยทางไซเบอร์

- **การจำลองสถานการณ์ที่สมจริง:** Generative AI สามารถสร้างการจำลองการโจมตีทางไซเบอร์ที่สมจริงอย่างยิ่ง ช่วยให้ทีมรักษาความปลอดภัยสามารถทดสอบระบบป้องกันและแผนการรับมือเหตุการณ์กับภัยคุกคามที่อาจเกิดขึ้นได้หลากหลายรูปแบบ แนวทางเชิงรุกนี้ช่วยระบุช่องโหว่และปรับปรุงการเตรียมพร้อมก่อนการโจมตีจริงจะเกิดขึ้น
- **การคาดการณ์สถานการณ์การโจมตี:** ด้วยการวิเคราะห์ชุดข้อมูลขนาดใหญ่ของการโจมตีและเหตุการณ์ด้านความปลอดภัยในอดีต ปัญญาประดิษฐ์ (AI) สามารถระบุรูปแบบและแนวโน้ม ทำให้สามารถคาดการณ์สถานการณ์การโจมตีที่อาจเกิดขึ้นในอนาคตได้ ความสามารถในการคาดการณ์นี้ช่วยให้องค์กรต่างๆ ก้าวล้ำหน้าอาชญากรไซเบอร์หนึ่งก้าว และนำมาตราการรับมือเชิงรุกมาใช้
- **เพิ่มประสิทธิภาพการตรวจจับภัยคุกคาม:** Generative AI สามารถเสริมประสิทธิภาพ ระบบ **ตรวจจับภัยคุกคาม** (Threat Detection and Response: TDR) ด้วยการสร้างข้อมูลสังเคราะห์ที่เลียนแบบรูปแบบการโจมตีในโลกแห่งความเป็นจริง วิธีนี้ช่วยขยายข้อมูลการฝึกอบรมสำหรับโมเดลการเรียนรู้ของเครื่องช่วยเพิ่มความสามารถในการระบุและแจ้งเตือนภัยคุกคามแม้เพียงเล็กน้อยหรือภัยคุกคามใหม่ๆ

Generative AI ทำหน้าที่เป็นพันธมิตรอันทรงพลังในการต่อสู้กับภัยคุกคามทางไซเบอร์ที่กำลังดำเนินอยู่ ด้วยการสร้างแบบจำลองที่สมจริง การคาดการณ์สถานการณ์การโจมตี และการปรับปรุงการตรวจจับภัยคุกคาม AI

จะช่วยให้ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์สามารถป้องกันองค์กรของตนได้อย่างเชิงรุก และก้าวลำนำหน้าภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา

14.4.4.8 ประโยชน์ของปัญญาประดิษฐ์ (AI) ในการจัดการความเสี่ยงทางไซเบอร์

การนำ AI มาใช้ในด้านความปลอดภัยทางไซเบอร์มีประโยชน์มากมายสำหรับองค์กรที่ต้องการจัดการความเสี่ยง ประโยชน์โดยทั่วไปมีดังนี้:

1) **การเรียนรู้อย่างต่อเนื่อง** ความสามารถของ AI พัฒนาอย่างต่อเนื่องเมื่อเรียนรู้จากข้อมูลใหม่ๆ เทคนิคต่างๆ เช่น การเรียนรู้เชิงลึกและ ML ช่วยให้ AI สามารถจดจำรูปแบบ สร้างบรรทัดฐานของกิจกรรมปกติ และค้นพบกิจกรรมที่ผิดปกติหรือน่าสงสัยที่เบี่ยงเบนไปจากกิจกรรมนั้น ความสามารถในการเรียนรู้อย่างต่อเนื่องของ AI ทำให้แฮกเกอร์หลบเลี่ยงการป้องกันขององค์กรได้ยากขึ้น

2) **การค้นพบภัยคุกคามที่ไม่รู้จัก** เมื่ออาชญากรไซเบอร์คิดค้นวิธีการโจมตีที่ซับซ้อนมากขึ้น องค์กรต่างๆ มักตกอยู่ในความเสี่ยงต่อภัยคุกคามที่ไม่รู้จัก ซึ่งอาจสร้างความเสียหายอย่างใหญ่หลวงต่อเครือข่าย AI นำเสนอโซลูชันสำหรับการทำแผนที่และป้องกันภัยคุกคามที่ไม่รู้จัก รวมถึงช่องโหว่ที่ผู้ให้บริการซอฟต์แวร์ยังไม่สามารถระบุหรือแก้ไขได้

3) **ปริมาณข้อมูลมหาศาล** ระบบ AI สามารถจัดการและเข้าใจข้อมูลจำนวนมหาศาลที่ผู้เชี่ยวชาญด้านความปลอดภัยทำไม่ได้ ด้วยวิธีนี้ องค์กรต่างๆ จะสามารถค้นพบภัยคุกคามใหม่ๆ โดยอัตโนมัติท่ามกลางข้อมูลปริมาณมหาศาลและปริมาณการรับส่งข้อมูลบนเครือข่าย ซึ่งระบบดั้งเดิมอาจไม่สามารถตรวจจับได้

4) **การจัดการช่องโหว่ที่ดีขึ้น** นอกจากการค้นพบภัยคุกคามใหม่ๆ แล้ว AI ยังช่วยให้องค์กรสามารถจัดการช่องโหว่ต่างๆ ได้ดียิ่งขึ้น ช่วยให้ประเมินระบบได้อย่างมีประสิทธิภาพมากขึ้น ปรับปรุงการแก้ปัญหา และตัดสินใจได้ดีขึ้น นอกจากนี้ยังสามารถระบุจุดอ่อนในเครือข่ายและระบบต่างๆ เพื่อให้องค์กรสามารถมุ่งเน้นไปที่งานด้านความปลอดภัยที่สำคัญที่สุดได้อย่างต่อเนื่อง

5) **ยกระดับมาตรการรักษาความปลอดภัยโดยรวม** การจัดการความเสี่ยงจากภัยคุกคามต่างๆ ด้วยตนเอง ตั้งแต่การโจมตีแบบปฏิเสธการให้บริการ (DDoS) การโจมตีแบบฟิชชิง ไปจนถึงแรนซัมแวร์อาจเป็นเรื่องยากและใช้เวลานาน แต่ด้วย AI องค์กรต่างๆ สามารถตรวจจับการโจมตีประเภทต่างๆ ได้แบบเรียลไทม์ พร้อมจัดลำดับความสำคัญและป้องกันความเสี่ยงได้อย่างมีประสิทธิภาพ

6) **การตรวจจับและการตอบสนองที่ดีขึ้น** การตรวจจับภัยคุกคามเป็นองค์ประกอบสำคัญของการปกป้องข้อมูลและเครือข่าย ความปลอดภัยทางไซเบอร์ที่ขับเคลื่อนด้วย AI สามารถส่งผลให้สามารถตรวจจับข้อมูลที่น่าเชื่อถือได้อย่างรวดเร็ว และตอบสนองต่อภัยคุกคามใหม่ๆ ได้อย่างเป็นระบบและทันท่วงทีมากขึ้น

14.5 บทวิเคราะห์บูรณาการปัญญาประดิษฐ์และวิทยาการรหัสควอนตัมในบริบทความมั่นคงปลอดภัยไซเบอร์

14.5.1 ภาพรวม

การเข้ารหัสแบบควอนตัมเป็นสาขาย่อยขั้นสูงของการเข้ารหัสที่ใช้หลักการของกลศาสตร์ควอนตัม เพื่อให้มั่นใจว่าการสื่อสารมีความปลอดภัย ต่างจากการเข้ารหัสแบบดั้งเดิม ซึ่งโดยทั่วไปจะใช้อัลกอริทึมทางคณิตศาสตร์ที่ซับซ้อนในการเข้ารหัสข้อมูล การเข้ารหัสแบบควอนตัมใช้คุณสมบัติทางกายภาพของอนุภาคควอนตัม เช่น โฟตอน เพื่อสร้างระบบการสื่อสารที่มีความปลอดภัยโดยเนื้อแท้

รากฐานสำคัญของการเข้ารหัสด้วยควอนตัมคือการกระจายคีย์ควอนตัม (QKD) ซึ่งเป็นวิธีการที่ช่วยให้ทั้งสองฝ่ายสามารถสร้างคีย์ลับแบบสุ่มที่ใช้ร่วมกันได้ ซึ่งเป็นสิ่งจำเป็นสำหรับการเข้ารหัสและถอดรหัสข้อความในลักษณะที่สามารถตรวจจับการมีอยู่ของผู้ดักฟังได้ ความปลอดภัยของ QKD มีรากฐานมาจากหลักการกลศาสตร์ควอนตัมพื้นฐาน เช่น หลักความไม่แน่นอนของไฮเซนเบิร์กและพันนาการควอนตัม

หลักความไม่แน่นอนของไฮเซนเบิร์กระบุว่า การวัดระบบควอนตัมจะเปลี่ยนแปลงสถานะอย่างหลีกเลี่ยงไม่ได้ ดังนั้น หากผู้แอบฟังพยายามดักฟังและวัดคีย์ควอนตัม ก็จะทำให้เกิดความผิดปกติที่ตรวจจับได้ ซึ่งจะแจ้งเตือนผู้สื่อสารถึงการมีอยู่ของการบุกรุก

เอ็นแทงเกิลควอนตัมเป็นแนวคิดพื้นฐานอีกประการหนึ่งในกลศาสตร์ควอนตัมที่เชื่อมโยงอนุภาคควอนตัมสองตัวเข้าด้วยกัน เพื่อให้สถานะของอนุภาคหนึ่งส่งผลต่อสถานะของอีกอนุภาคหนึ่งทันที โดยไม่คำนึงถึงระยะห่างระหว่างอนุภาคทั้งสอง คุณสมบัตินี้สามารถนำมาใช้เพื่อสร้างกุญแจความปลอดภัยระหว่างสองฝ่ายได้

ประโยชน์หลักของการเข้ารหัสด้วยควอนตัมคือศักยภาพในการสร้างช่องทางการสื่อสารที่ป้องกันการดักฟังได้ การเข้ารหัสนี้เอาชนะข้อจำกัดหลายประการของวิธีการเข้ารหัสแบบดั้งเดิม โดยเฉพาะอย่างยิ่งในการพัฒนาศักยภาพการประมวลผล เช่น คอมพิวเตอร์ควอนตัม สิ่งนี้ทำให้การเข้ารหัสเป็นสาขาการศึกษาที่สำคัญยิ่งในการสร้างความมั่นใจในความปลอดภัยของข้อมูลสำคัญในยุคคอมพิวเตอร์ควอนตัม

การบรรจบกันของ AI และการเข้ารหัสควอนตัมเป็นหัวข้อที่ได้รับความสนใจอย่างมากในหมู่ผู้เชี่ยวชาญด้านวิทยาศาสตร์และเทคโนโลยี ทั้งสองสาขาได้เปลี่ยนแปลงอุตสาหกรรมของตนเองไปอย่างมาก โดย AI ได้ก้าวหน้าอย่างโดดเด่นในด้านการดูแลสุขภาพและการเงิน ด้วยการใช้ประโยชน์จากความสามารถอันโดดเด่นในการประมวลผลข้อมูล จัดจํารูปแบบ และตัดสินใจอย่างชาญฉลาด ขณะเดียวกัน การเข้ารหัสควอนตัมยังมอบความปลอดภัยที่เหนือชั้นโดยอิงตามกฎฟิสิกส์ โดยส่วนใหญ่ผ่านการกระจายคีย์ควอนตัม (QKD) และโปรโตคอลที่เกี่ยวข้อง

การผสมผสานระหว่าง AI และการเข้ารหัสควอนตัมไม่ใช่เรื่องบังเอิญ ในยุคดิจิทัลปัจจุบันที่มีการถ่ายโอนข้อมูลจำนวนมากและภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงขึ้น การผสมผสานพลังการประมวลผลของ AI เข้ากับ

มาตรการรักษาความปลอดภัยที่เข้มแข็งของการเข้ารหัสควอนตัมจึงเป็นเรื่องที่สมเหตุสมผล ด้วยการตรวจสอบข้อมูลจำนวนมาก อัลกอริทึม AI มีศักยภาพในการยกระดับกระบวนการเข้ารหัสควอนตัม ให้แข็งแกร่งและมีประสิทธิภาพมากขึ้น ในขณะเดียวกัน การเข้ารหัสควอนตัมยังสามารถเป็นกรอบการทำงานที่ปลอดภัยสำหรับระบบ AI ทำให้มั่นใจได้ว่าข้อมูลและอัลกอริทึมที่ระบบจัดการจะปลอดภัยจากการละเมิด

การเข้ารหัสด้วยควอนตัมมีความสำคัญเพิ่มมากขึ้นเรื่อยๆ เนื่องจากการมาถึงของคอมพิวเตอร์ควอนตัมที่กำลังจะมาถึง คอมพิวเตอร์เหล่านี้สามารถถอดรหัสลับแบบคลาสสิกได้ภายในระยะเวลาอันสั้น ซึ่งถือเป็นภัยคุกคามสำคัญต่อความมั่นคงปลอดภัยทางไซเบอร์ยุคใหม่ ดังนั้น การผสมผสานปัญญาประดิษฐ์ (AI) และการเข้ารหัสด้วยควอนตัมจึงไม่ใช่แค่เพียงแนวทางเชิงวิชาการเท่านั้น แต่ยังเป็นมาตรการที่จำเป็นในการแก้ไขปัญหาเร่งด่วนนี้อีกด้วย

การบรรจบกันของ AI และการเข้ารหัสควอนตัม ถือเป็นการผสมผสานครั้งสำคัญระหว่างสองศาสตร์แห่งการเปลี่ยนแปลง AI ได้เปลี่ยนแปลงวิธีการประมวลผลและวิเคราะห์ข้อมูล ขณะที่การเข้ารหัสควอนตัมมอบความปลอดภัยที่เหนือชั้นในการรับส่งข้อมูล ในขณะที่สองศาสตร์นี้ยังคงพัฒนาอย่างต่อเนื่อง จุดบรรจบของทั้งสองศาสตร์นี้จึงเป็นพื้นที่ที่น่าสนใจสำหรับการสำรวจ บทความนี้จะสำรวจปฏิสัมพันธ์ ความก้าวหน้าที่จะเกิดขึ้น และความท้าทายของ AI และการเข้ารหัสควอนตัม

14.5.2 บทวิจารณ์ความก้าวหน้าในการเข้ารหัสควอนตัม

รากฐานของการเข้ารหัสควอนตัมสามารถสืบย้อนกลับไปได้ถึงต้นศตวรรษที่ 20 กลศาสตร์ควอนตัมก่อให้เกิดความท้าทายและโอกาสสำหรับการประมวลผลข้อมูล เนื่องจากคุณสมบัติที่ขัดกับสัญชาตญาณของระบบควอนตัม เช่น การซ้อนทับและการพันกัน

ในช่วงทศวรรษ 1970 และ 1980 มีความก้าวหน้าสำคัญเกิดขึ้นในทฤษฎีสารสนเทศควอนตัม ชาร์ลส์ เบนเน็ตต์ และกิลล์ บราสซาร์ด ได้นำเสนอแนวคิดการกระจายคีย์ควอนตัม (QKD) ในปี 1984 ด้วยโปรโตคอล BB84 ซึ่งอ้างอิงจากงานวิจัยด้านกลศาสตร์ควอนตัมและทฤษฎีสารสนเทศก่อนหน้านี้ โปรโตคอลนี้ใช้หลักการของกลศาสตร์ควอนตัมเพื่อให้ทั้งสองฝ่ายสามารถสร้างคีย์สุ่มลับที่ใช้ร่วมกันได้อย่างปลอดภัยตามกฎฟิสิกส์

ในช่วงหลายปีต่อมา มีการพัฒนาที่สำคัญทั้งในเชิงทฤษฎีและปฏิบัติของการเข้ารหัสด้วยควอนตัม นอกจากการกระจายข้อมูลที่สำคัญแล้ว โปรโตคอลการเข้ารหัสด้วยควอนตัมยังได้ขยายขอบเขตให้ครอบคลุมถึงลายเซ็นดิจิทัลควอนตัมและการสื่อสารโดยตรงที่ปลอดภัย ด้วยความก้าวหน้าของโฟโตนิกส์และเทคโนโลยีควอนตัม โปรโตคอลเหล่านี้จึงถูกนำไปใช้งานและทดสอบในสถานการณ์จริง ซึ่งเปิดประตูสู่เครือข่ายการสื่อสารที่ปลอดภัยด้วยควอนตัมเชิงพาณิชย์

แม้จะมีต้นกำเนิดมาจากขนบวิทยาศาสตร์ที่แตกต่างกัน แต่ปัญญาประดิษฐ์และการเข้ารหัสควอนตัมก็ได้หลอมรวมกันผ่านข้อมูลเชิงลึกพื้นฐาน ความก้าวหน้าทางเทคโนโลยี และการแสวงหาความเข้าใจและนวัตกรรม

อย่างต่อเนื่อง การหลอมรวมกันนี้นำมาซึ่งโอกาสและความท้าทายมากมาย ซึ่งอาจพลิกโฉมความมั่นคงปลอดภัยของข้อมูลและปัญญาประดิษฐ์

14.5.3 บทวิจารณ์การบูรณาการ AI กับการเข้ารหัสควอนตัม

ความก้าวหน้าทางเทคโนโลยีด้าน AI และควอนตัมคอมพิวเตอร์ตั้งนั้นยิ่งใหญ่มากนำไปสู่การเปลี่ยนแปลงครั้งสำคัญในหลายสาขารวมถึงวิทยาการเข้ารหัสลับ หนึ่งในวัตถุประสงค์หลักของการบูรณาการ AI เข้ากับวิทยาการเข้ารหัสลับควอนตัมคือการใช้ประโยชน์จากความสามารถในการประมวลผลของ AI เพื่อเพิ่มประสิทธิภาพ ความปลอดภัย และความทนทานของระบบวิทยาการเข้ารหัสลับควอนตัม ระเบียบวิธีของ AI ที่มีความสามารถในการประมวลผลข้อมูลจำนวนมาก จดจำรูปแบบที่ซับซ้อน และปรับตัวเข้ากับสถานการณ์ใหม่ๆ สามารถมีส่วนสำคัญในการปรับปรุงโพรโทคอลวิทยาการเข้ารหัสลับควอนตัมให้เหมาะสมที่สุด และรับมือกับความท้าทายที่ซับซ้อนที่เผชิญอยู่

ในขณะเดียวกัน การเข้ารหัสควอนตัมยังเป็นช่องทางพิเศษในการปกป้องระบบ AI ด้วยความมั่นคงปลอดภัยพื้นฐานตามกฎของกลศาสตร์ควอนตัม การบูรณาการนี้มีความเหมาะสมและเหมาะสมกับยุคดิจิทัลของเรา ซึ่งโดดเด่นด้วยการแลกเปลี่ยนข้อมูลอย่างกว้างขวางและภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงขึ้น บทบาทของ AI จึงมีความสำคัญอย่างยิ่งยวด การวิเคราะห์และตีความชุดข้อมูลขนาดใหญ่ทำให้อัลกอริทึม AI สามารถมีบทบาทสำคัญในการยกระดับความปลอดภัยและประสิทธิภาพของแนวทางปฏิบัติด้านการเข้ารหัสควอนตัม

อย่างไรก็ตาม การเกิดขึ้นของคอมพิวเตอร์ควอนตัมได้นำมาซึ่งความท้าทายครั้งใหม่ที่น่าเกรงขามสำหรับระบบเข้ารหัสลับ นั่นคือ “ภัยคุกคามจากควอนตัม” ภัยคุกคามนี้คุกคามวิธีการเข้ารหัสลับแบบดั้งเดิม โดยมีรากฐานมาจากข้อเท็จจริงที่ว่าคอมพิวเตอร์ควอนตัมมีศักยภาพที่จะทำลายอัลกอริทึมการเข้ารหัสลับจำนวนมากที่ใช้อยู่ในปัจจุบัน ดังนั้น การทำงานร่วมกันของปัญญาประดิษฐ์ (AI) และการเข้ารหัสลับด้วยควอนตัมจึงไม่ใช่แค่การศึกษาเชิงวิชาการ แต่เป็นวิวัฒนาการที่จำเป็นในแนวทางของเราในการสร้างความมั่นคงปลอดภัยทางดิจิทัล วิธีการที่ขับเคลื่อนด้วย AI ในการเข้ารหัสลับด้วยควอนตัมมีจุดมุ่งหมายเพื่อคาดการณ์ บรรเทา และป้องกันภัยคุกคามจากควอนตัมอย่างแข็งแกร่ง เพื่อให้มั่นใจถึงอนาคตของการประมวลผลที่ปลอดภัย

บทวิจารณ์นี้จะเห็นถึงปฏิสัมพันธ์ระหว่าง AI และการเข้ารหัสควอนตัม โดยสำรวจพัฒนาการในอดีต ความท้าทายที่เกิดขึ้นจากการกำเนิดของคอมพิวเตอร์ควอนตัม และศักยภาพในการเปลี่ยนแปลงของการผสมผสาน โดยมุ่งหวังที่จะให้ความเข้าใจที่ครอบคลุมเกี่ยวกับภูมิทัศน์ปัจจุบัน และโอกาสอันน่าตื่นเต้นที่การผสมผสานสหวิทยาการนี้จะมอบให้กับอนาคตของการประมวลผลที่ปลอดภัย

การทบทวนภัยคุกคามควอนตัม “ภัยคุกคามควอนตัม” หมายถึงช่องโหว่ที่อาจเกิดขึ้นกับระบบเข้ารหัสที่มีอยู่ในปัจจุบัน เมื่อเผชิญกับขีดความสามารถในการประมวลผลควอนตัมขั้นสูง วิธีการเข้ารหัสเช่น RSA และ ECC (Elliptic Curve Cryptography) ขึ้นอยู่กับความยากในการคำนวณของปัญหาทางคณิตศาสตร์เฉพาะ ตัวอย่างเช่น

RSA อาศัยความท้าทายในการแยกตัวประกอบจำนวนเฉพาะขนาดใหญ่ และ ECC ขึ้นอยู่กับความซับซ้อนในการแก้ปัญหาลอการิทึมไม่ต่อเนื่องของเส้นโค้งวงรี ปัญหาเหล่านี้ซึ่งปัจจุบันถือว่ายากสำหรับคอมพิวเตอร์แบบดั้งเดิม อาจได้รับการแก้ไขอย่างมีประสิทธิภาพโดยคอมพิวเตอร์ควอนตัมโดยใช้อัลกอริทึม เช่น อัลกอริทึมของชอร์

คอมพิวเตอร์ควอนตัมทำงานบนหลักการของกลศาสตร์ควอนตัม เช่น การซ้อนทับและการพันกัน เพื่อประมวลผลข้อมูลที่แตกต่างไปจากคอมพิวเตอร์แบบดั้งเดิม ความสามารถนี้ช่วยให้คอมพิวเตอร์สามารถคำนวณเฉพาะเจาะจงได้อย่างมีประสิทธิภาพมากกว่าคอมพิวเตอร์แบบดั้งเดิมมาก อัลกอริทึมของชอร์แสดงให้เห็นว่าคอมพิวเตอร์ควอนตัมสามารถแยกตัวประกอบจำนวนมากได้เร็วกว่าอัลกอริทึมที่เป็นที่รู้จักมากที่สุดที่ทำงานบนคอมพิวเตอร์แบบดั้งเดิมแบบเลขชี้กำลัง ส่งผลให้ระบบเข้ารหัสที่อาศัยความยากของปัญหาเหล่านี้เพื่อความปลอดภัยจะมีความเสี่ยงเมื่อคอมพิวเตอร์ควอนตัมที่มีประสิทธิภาพเพียงพอได้รับการพัฒนาขึ้น

ภัยคุกคามจากควอนตัมไม่ใช่แค่ความกังวลเชิงทฤษฎี แต่เป็นความจริงในอนาคตอันใกล้ การถือกำเนิดของคอมพิวเตอร์ควอนตัมจึงจำเป็นต้องมีการพัฒนาระบบเข้ารหัสแบบใหม่ที่ปลอดภัยจากการโจมตีด้วยควอนตัม ซึ่งมักเรียกว่าการเข้ารหัสแบบ 'ต้านทานควอนตัม' หรือ 'หลังควอนตัม' ระบบเหล่านี้มีเป้าหมายที่จะใช้อัลกอริทึมและวิธีการเข้ารหัสที่คอมพิวเตอร์ควอนตัมไม่สามารถเจาะเข้าไปได้อย่างมีประสิทธิภาพ

การผสมรวม AI เข้ากับการเข้ารหัสควอนตัมถือเป็นกลยุทธ์ในการรับมือกับภัยคุกคามนี้ ความสามารถในการจดจำรูปแบบและการคาดการณ์ขั้นสูงของ AI สามารถช่วยในการพัฒนา ทดสอบ และเพิ่มประสิทธิภาพอัลกอริทึมที่ต้านทานควอนตัมได้ นอกจากนี้ AI ยังสามารถมีส่วนร่วมในการประเมินและปรับใช้ระบบการเข้ารหัสแบบเรียลไทม์ ทำให้ระบบมีความทนทานต่อสภาพแวดล้อมของการประมวลผลควอนตัมที่เปลี่ยนแปลงอย่างรวดเร็ว ซึ่งทำให้การผสมรวม AI และการเข้ารหัสควอนตัมเป็นงานวิจัยสำคัญเพื่อสร้างความมั่นใจในความปลอดภัยและความเป็นส่วนตัวของข้อมูลในยุคการประมวลผลควอนตัมที่กำลังจะมาถึง

14.6 สรุป

เนื้อหาในบทนี้กล่าวถึงการบูรณาการปัญญาประดิษฐ์ (AI) กับการเข้ารหัสควอนตัม เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัลในยุคที่คอมพิวเตอร์ควอนตัมมีแนวโน้มคุกคามระบบเข้ารหัสแบบเดิม AI ถูกนำมาใช้ในการเพิ่มประสิทธิภาพและความปลอดภัยให้กับอัลกอริทึมต้านทานควอนตัม พร้อมทั้งวิเคราะห์แนวโน้มเทคโนโลยีและมาตรการรับมือภัยคุกคามใหม่ ๆ ในภูมิทัศน์ไซเบอร์สมัยใหม่

14.6 บทวิเคราะห์และมุมมองเชิงวิชาการ: “แนวโน้มวิศวกรรมความมั่นคงปลอดภัยในยุค AI และควอนตัมคอมพิวเตอร์”

เอกสารคำสอนบทที่ 14 แนวโน้มวิศวกรรมความมั่นคงปลอดภัยในยุค AI นำเสนอการเปลี่ยนผ่านครั้งสำคัญในภูมิทัศน์ของความมั่นคงปลอดภัยทางไซเบอร์ จากการขับเคลื่อนด้วย ภูมิรัฐศาสตร์ ห่วงโซ่อุปทานเทคโนโลยีใหม่ (Generative AI, Cloud, IoT, Blockchain) และภัยคุกคามจากควอนตัมคอมพิวเตอร์ ไปสู่การสร้างมาตรการความปลอดภัยที่บูรณาการ AI + Quantum Cryptography เพื่อเตรียมพร้อมต่อความท้าทายในอนาคต มีบทวิเคราะห์และมุมมองเชิงวิชาการดังนี้

1) การสังเคราะห์องค์ความรู้จากบทเรียน

ภูมิทัศน์ดิจิทัล: ความตึงเครียดทางภูมิรัฐศาสตร์ ห่วงโซ่อุปทานซับซ้อน ช่องว่างทักษะ และภาระกฎระเบียบ ทำให้ความซับซ้อนทางไซเบอร์เพิ่มขึ้น

ภัยคุกคามหลัก: แรนซัมแวร์, RaaS, การฉ้อโกงไซเบอร์, การขโมยตัวตน และการใช้ GenAI ในการโจมตี social engineering เช่น deepfake, phishing หลายภาษา

ควอนตัมคอมพิวเตอร์: มีศักยภาพในการเจาะระบบเข้ารหัสปัจจุบัน (RSA, ECC) และทำให้เกิดภัยคุกคาม Harvest Now – Decrypt Later

Post-Quantum Cryptography (PQC): อัลกอริทึมใหม่ เช่น CRYSTALS-Kyber, Dilithium, Falcon, SPHINCS ที่ NIST ประกาศมาตรฐานในปี 2027 เพื่อรับมือการโจมตีควอนตัม

Quantum Key Distribution (QKD): ใช้คุณสมบัติควอนตัมในการกระจายกุญแจอย่างปลอดภัย แม้ยังมีข้อจำกัดด้านระยะทาง อัตราแลกเปลี่ยน และต้นทุนฮาร์ดแวร์

AI for Cybersecurity: ใช้ AI/ML ใน threat detection, anomaly detection, automated response, SOC automation แต่ก็มีความเสี่ยงด้าน adversarial AI

2) มุมมองเชิงวิชาการและความก้าวหน้า

- AI-driven Cyber Defense

จาก signature-based IDS → AI-powered anomaly detection

SOC 2.0 ใช้ GenAI วิเคราะห์ log และ response แบบ real-time

- **Quantum-safe Cryptography**

การเปลี่ยนจาก RSA/ECC → PQC + QKD

แนวคิด *Crypto Agility*: ระบบต้องเปลี่ยนอัลกอริทึมได้ทันทีเมื่อมีช่องโหว่ใหม่

- **Hybrid Security Models**

รวม PQC + classical crypto + QKD → สร้าง resilience

การออกมาตรฐาน RFC สำหรับ IKEv2 hybrid key exchange

- **Zero Trust + AI + Quantum Security**

Zero Trust ถูกเสริมด้วย AI-based monitoring

Quantum-safe protocols จะกลายเป็นมาตรฐานของ Zero Trust Architecture

- **Ethical & Governance in AI Security**

ประเด็นการใช้ AI ใน deepfake, misinformation

ความจำเป็นในการพัฒนา *AI governance framework*

3) ประสบการณ์และการสอดแทรกเชิงการสอน

จากประสบการณ์ทางวิชาชีพและการสอน พบว่านักศึกษามักมองว่า Quantum เป็นเรื่อง “ไกลตัว” แต่เมื่อยกตัวอย่าง *Harvest Now, Decrypt Later* ที่อาจส่งผลกระทบต่อข้อมูลสุขภาพและการเงินในอีก 10–20 ปี นักศึกษาจะตระหนักถึง “ความสำคัญของการวางแผนระยะยาว” การเชื่อมโยง *AI + Quantum* ผ่านการทำ workshop “ออกแบบ SOC แห่งอนาคต” ช่วยให้นักศึกษาฝึกการคิดเชิงระบบ และเข้าใจการบูรณาการสหวิทยาการ

กล่าวโดยสรุป บทนี้สะท้อนว่า **AI และ Quantum Computing คือ double-edged sword** ของ cybersecurity พบว่า AI สามารถช่วยตรวจจับและตอบสนองได้เร็วขึ้น แต่ก็อาจถูกใช้สร้างภัยคุกคามที่สมจริงยิ่งขึ้น และ Quantum อาจทำลายระบบเข้ารหัสเดิม แต่ก็สร้างแนวทางใหม่ (PQC, QKD) การสอนในระดับอุดมศึกษาควรยกระดับจาก *defense-based* → *resilience-based* โดยใช้ **AI-driven SOC, PQC, QKD และ Zero Trust** เพื่อให้นักศึกษามีความพร้อมต่อภัยคุกคามไซเบอร์ในยุคใหม่

แบบทดสอบท้ายบท

ก) ข้อสอบอัตนัย 5 ข้อ + แนวคำตอบ

ข้อ 1. อธิบายปัจจัยที่ทำให้ภูมิทัศน์ภัยคุกคามทางไซเบอร์ซับซ้อนขึ้นในยุค AI

แนวคำตอบ: ความตึงเครียดภูมิรัฐศาสตร์, Generative AI, ช่องว่างทักษะ, ภาระกฎระเบียบ, ห่วงโซ่อุปทาน

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข้อ 2. อธิบายความเสี่ยงจากคอมพิวเตอร์ควอนตัมต่อระบบเข้ารหัส RSA/ECC

แนวคำตอบ: ใช้ Shor's Algorithm แตกตัวประกอบจำนวนเฉพาะได้เร็ว ทำให้ RSA/ECC ไม่ปลอดภัย

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข้อ 3. Post-Quantum Cryptography มีความสำคัญอย่างไร

แนวคำตอบ: พัฒนาอัลกอริทึมใหม่ที่ทนทานต่อการโจมตีจาก Quantum Computer เช่น CRYSTALS-Kyber, Dilithium

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข้อ 4. AI สามารถช่วยป้องกันภัยไซเบอร์ได้อย่างไร

แนวคำตอบ: ใช้ตรวจจับพฤติกรรมผิดปกติ, วิเคราะห์ Malware, ป้องกัน Phishing, Automate Incident Response

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข้อ 5. เสนอแนวทางบูรณาการ AI และ Quantum Cryptography เพื่อเพิ่ม Cybersecurity

แนวคำตอบ: ใช้ AI วิเคราะห์ประสิทธิภาพ PQC, ใช้ AI ตรวจสอบช่องโหว่ของ QKD, ใช้ Hybrid Solutions

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข) ข้อสอบปรนัย 10 ข้อ (ก. ข. ค. ง) พร้อมเฉลย

ข้อ 1. ปัจจัยใดเป็นตัวขับเคลื่อนความซับซ้อนทางไซเบอร์

ก. ความตึงเครียดภูมิรัฐศาสตร์

ข. การบูรณาการห่วงโซ่อุปทาน

ค. Generative AI

ง. ถูกทุกข้อ

เฉลย: ง

14_แนวโน้มวิศวกรรมความมั่นคงปลอดภัย...

ข้อ 2. ภัยใดที่ถูกจัดเป็นอันดับต้นในรายงาน WEF 2024

ก. DDoS

ข. Ransomware

ค. Spyware

ง. SQL Injection

เฉลย: ข

ข้อ 3. การโจมตี Harvest Now, Decrypt Later เกี่ยวข้องกับภัยใด

ก. AI

ข. Cloud Computing

ค. Quantum Computing

ง. Blockchain

เฉลย: ค

ข้อ 4. อัลกอริทึมใดเป็น Post-Quantum Cryptography ที่ NIST รับรอง

ก. RSA

ข. ECC

ค. CRYSTALS-Kyber

ง. DES

เฉลย: ค

ข้อ 5. Quantum Key Distribution (QKD) มีคุณสมบัติเด่นข้อใด

ก. ตรวจจับการดักฟังได้

ข. ใช้ได้ไม่เกิน 10 กิโลเมตร

ค. ใช้รหัสผ่านแทนกุญแจ

ง. ไม่ต้องใช้อุปกรณ์เฉพาะ

เฉลย: ก

ข้อ 6. AI สามารถป้องกันการโจมตีได้โดยมีประสิทธิภาพ

ก. Phishing & Deepfake

ข. การพิมพ์เอกสารผิด

ค. ความผิดพลาดของมนุษย์

ง. การลี้มรหัสผ่าน

เฉลย: ก

ข้อ 7. ปัจจัยใดเป็นอุปสรรคต่อ Cybersecurity ที่มีประสิทธิภาพ

ก. ช่องว่างทักษะบุคลากร

ข. กฎระเบียบที่เพิ่มขึ้น

ค. ความซับซ้อนของเทคโนโลยีใหม่

ง. ถูกทุกข้อ

เฉลย: ง

ข้อ 8. Generative AI ถูกใช้โดยอาชญากรไซเบอร์เพื่ออะไร

ก. เร่งความเร็วการเข้ารหัส

ข. เลียนแบบการสื่อสารผู้นำองค์กร

ค. ลดต้นทุน Data Center

ง. ป้องกัน Quantum Threats

เฉลย: ข

ข้อ 9. ข้อใดเป็น Hybrid Solution ในการเข้ารหัสยุคควอนตัม

- ก. ใช้ RSA เดิมเพียงอย่างเดียว
- ข. ผสม PQC กับระบบดั้งเดิม
- ค. ใช้รหัสผ่านเพิ่มขึ้น
- ง. ตัดการใช้ Encryption

เฉลย: ข

ข้อ 10. การใช้ AI กับ PQC ช่วยองค์กรได้อย่างไร

- ก. วิเคราะห์ประสิทธิภาพและตรวจหาช่องโหว่
- ข. ลดต้นทุน Hardware
- ค. ลดความต้องการบุคลากรด้าน Cybersecurity
- ง. ทำให้ Quantum Threats หายไปทันที

เฉลย: ก

บรรณานุกรมท้ายบท

ผู้ช่วยศาสตราจารย์ ดร.ศิระเชษฐ์ โพธิ์หิรัญ. (ม.ป.ป.). *แนวโน้มวิศวกรรมความมั่นคงปลอดภัยในยุค AI*.

เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.

Brundage, M., et al. (2020). The Malicious Use of AI: Forecasting, Prevention, and Mitigation.

CISA. (2023). Quantum-Readiness Initiative.

Kshetri, N. (2023). AI and Cybersecurity: Trends and Implications.

MITRE. (2023). ATT&CK Framework for Emerging Technologies.

NIST. (2024). Post-Quantum Cryptography Standards.

Petar Radanliev (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology. <https://doi.org/10.1186/s40543-024-00416-6>

World Economic Forum. (2024). Global Cybersecurity Outlook.

World Economic Forum (WEF), Global Cybersecurity Outlook 2025, INSIGHT REPORT, JANUARY 2025.

Sirachet Phodhiran, Pichate Kunakornvong, Pongpon Nilaphruek, Jaturapith Krohkaew, Niti Witthayawiroj, Padma Nyoman Crisnapati, Yamin Thwe. A Competency-Based Curriculum for Fostering Artificial Intelligence Skills in Thai Children and Youth. International Journal of Engineering Trends and Technology. Volume 72 Issue 10, 357-372, October 2024, Seventh Sense Research Group. ISSN: 2231-5381/<https://doi.org/10.14445/22315381/-V72110P135>

Stallings, W. (2021). Cryptography and Network Security. Pearson.

บรรณานุกรม

ภาษาไทย

- กรมอุตุนิยมวิทยา. (2564). *ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น*. กรุงเทพฯ: กรมอุตุนิยมวิทยา.
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.
- พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับแก้ไขเพิ่มเติม).
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอนรายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์*. มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: ความรู้เบื้องต้นเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: การโจมตีทางไซเบอร์และการตรวจหาการบุกรุก (Cyber Attacking and Intrusion Detection)*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: การออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย (Secured Network Design)*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: ความมั่นคงปลอดภัยเครือข่ายไร้สาย (Wireless Network Security)*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: สถาปัตยกรรมความมั่นคงปลอดภัยข้อมูล*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: ภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์: ช่องโหว่ ภัยคุกคาม พื้นฐานของมัลแวร์ และความเสี่ยง*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). *เอกสารคำสอน: พื้นฐานวิทยาการรหัสลับ (Cryptography Overview)*. รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.

- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). เอกสารคำสอน: วิศวกรรมเครือข่ายการสื่อสาร (Communications Networks Engineering). รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). เอกสารคำสอน: ไฟร์วอลล์และระบบอำพราง (Firewall and Anonymity Systems). รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). เอกสารคำสอน: ระบบประกันระดับสูงโดยใช้เครือข่ายส่วนตัวเสมือน (VPN). รายวิชา 02323207 หลักการความมั่นคงทางไซเบอร์, มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). เอกสารคำสอน: แนวทางการสร้างมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สามารถใช้ประโยชน์ได้. มทร.ธัญบุรี.
- ศิระเชษฐ์ โพธิ์หิรัญ, ผศ.ดร. (ม.ป.ป.). เอกสารคำสอน: แนวโน้มวิศวกรรมความมั่นคงปลอดภัยในยุค AI. มทร.ธัญบุรี.
- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2566). รายงานสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ประเทศไทย ปี 2566. DEPA.
- สำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (NCSA). (2568). สถิติภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ ปี 2568. <https://www.ncsa.or.th/policy/threat-statistics>
- สำนักงานพัฒนารัฐบาลดิจิทัล (DGA). (2565). มาตรฐานความมั่นคงปลอดภัยสารสนเทศภาครัฐ. กรุงเทพฯ: DGA.
- วิเชษฐ์ พลายมาศ. (2552). ระบบปฏิบัติการ (Operating Systems). กรุงเทพฯ: ซีเอ็ดดูเคชั่น.

ภาษาอังกฤษ

- Abadi, M., & Gordon, A. D. (1999). A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148(1).
- Anderson, J. P. (1980). *Computer Security Threat Monitoring and Surveillance*. James P. Anderson Co.
- Anderson, R. (2021). *Security Engineering* (Chs. 1–2).
- Bernstein, D. J. (2005). Cache-timing attacks on AES. (manuscript).

- Brundage, M., et al. (2020). *The Malicious Use of AI: Forecasting, Prevention, and Mitigation*.
- Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*.
- Center for Internet Security (CIS). (2021). *CIS Critical Security Controls v8*.
- Center for Strategic and International Studies (CSIS). (2023). *Economic Impact of Cybercrime: A Global Perspective*.
- Cisco Systems. (2021). *Network Security Design Guide*.
- Cisco Systems. (2022). *SD-WAN Design Guide*.
- Cybersecurity Ventures. (2023). *Global Cybercrime Damages Report 2023*.
- Donenfeld, J. (2018). WireGuard: Next Generation Kernel Network Tunnel. (whitepaper).
- Egevang, K., & Francis, P. (1994). The IP Network Address Translator (NAT) (RFC 1631). IETF.
- ENISA. (2023). *Threat Landscape Report 2023*. European Union Agency for Cybersecurity.
- Floyd, S., Bellovin, S., Ioannidis, J., Kompella, K., Mahajan, R., & Paxson, V. (2001). Pushback messages for controlling aggregates in the network. *Internet Draft*.
- Gartner. (2021). *Market Guide for Zero Trust Network Access (ZTNA)*.
- Gartner. (2021). *Market Guide for Secure Access Service Edge (SASE)*.
- Garcia-Teodoro, P., et al. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*.
- Garfinkel, S., & Spafford, G. (2021). *Practical UNIX and Internet Security*. O'Reilly.
- Heady, R., Luger, G., & Servilla, M. (1990). *The Architecture of a Network-Level Intrusion Detection System*. University of New Mexico.
- Huttunen, A., et al. (2005). UDP Encapsulation of IPsec ESP Packets (NAT-T) (RFC 3948). IETF.
- IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corp.
- IEEE. (2020). *IEEE 802.11ax-2020: Wi-Fi 6 Standard*.

- International Telecommunication Union. (n.d.). *ITU-T X.800: Security Architecture for OSI*.
- ISO. (1989). *ISO/IEC 7498-2:1989. Information Processing Systems – OSI Reference Model – Security Architecture*.
- ISO/IEC. (2013). *ISO/IEC 27001:2013 – Information Security Management Systems Requirements*.
- ISO/IEC. (2015). *ISO/IEC 27033-1: Network security—Part 1: Overview and concepts*.
- ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information Security Management Systems*.
- Johnson, J. (1997). *The Evolution of British Sigint: 1653–1939*. HMSO.
- Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). *Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296)*. IETF.
- Kindervag, J. (2010). No More Chewy Centers: Introducing Zero Trust. Forrester.
- Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*.
- Kurose, J., & Ross, K. (2021). *Computer Networking: A Top-Down Approach*.
- Kshetri, N. (2023). AI and Cybersecurity: Trends and Implications.
- Larsen, D. (2019). Creating an American culture of secrecy: Cryptography in Wilson-era diplomacy. *Diplomatic History*.
- McKinsey & Company. (2023). *Digital Transformation in the Post-Pandemic Era*.
- MITRE. (2023). *ATT&CK Framework for Enterprise*.
- MITRE. (2023). *ATT&CK Framework: Wireless Tactics*.
- MITRE. (2023). *ATT&CK for Emerging Technologies*.
- National Institute of Standards and Technology (NIST). (2001). *FIPS 197: Advanced Encryption Standard (AES)*.
- NIST. (2007). *SP 800-57: Recommendation for Key Management*.
- NIST. (2017). *SP 800-38D: Recommendation for GCM and GMAC*.

- NIST. (2018). *Cybersecurity Framework (CSF) 1.1*.
- NIST. (2018). *FIPS 202: SHA-3 Standard*.
- NIST. (2018). *SP 800-56A Rev.3: Recommendation for Key Establishment*.
- NIST. (2020). *Guide to IPsec VPNs (SP 800-77 Rev.1)*.
- NIST. (2020). *Zero Trust Architecture (SP 800-207)*.
- NIST. (2021). *Guide to Intrusion Detection and Prevention Systems (IDPS) (SP 800-94)*.
- NIST. (2024). *Cybersecurity Framework (CSF) 2.0*.
- NIST. (2024). *Post-Quantum Cryptography Standards*.
- NIST. (2025). *SP 800-61r3: Computer Security Incident Handling Guide*.
- OWASP Foundation. (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. OWASP.
- Petar, R. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*. <https://doi.org/10.1186/s40543-024-00416-6>
- Ponemon Institute. (2023). *State of Cybersecurity Report 2023*.
- Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., & Lear, E. (1996). Address Allocation for Private Internets (RFC 1918). IETF.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207).
- Satid Vongprateep, and **Wichet Plaimart**, Survival Architecture for Distributed Intrusion Detection System (dIDS) using Mobile Agent. The Sixth IEEE International Symposium on Network Computing and Applications (NCA 2007). 12-14 July 2007, Cambridge, Massachusetts, USA.
- Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy (NIST SP 800-41r1).

- Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94).
- Sebag–Montefiore, H. (2011). *Enigma: The Battle for the Code*. Orion.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2020). *Operating System Concepts* (10th ed.). Wiley.
- Silberschatz, A., Galvin, P. B., & Gagne, G. (2003). *Operating System Concepts* (6th ed.). Wiley.
- Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE S&P*.
- Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
- Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.
- Stallings, W. (2021). *Foundations of Modern Networking*. Pearson.
- Stallings, W. (2021). *Wireless Communications & Security*. Pearson.
- Stallings, W. (2021). *Computer Security: Principles and Practice*. Pearson.
- Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.
- Stallings, W., & Brown, L. (2024). *Computer Security: Principles and Practice*. Pearson.
- Symantec Corporation. (2023). *Internet Security Threat Report 2023*. Broadcom.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage.
- **Wichet Plaimart** and Sartid Vongpradhip (2011). A Sustainable Component of Intrusion Detection System using Survival Architecture on Mobile Agent, Intrusion Detection Systems, Pawel Skrobanek (Ed.).
- Wi-Fi Alliance. (2019). *WPA3 Security Enhancements*.

- World Economic Forum (WEF). (2024). *Global Cybersecurity Outlook 2024*.
- World Economic Forum (WEF). (2025). *Global Cybersecurity Outlook 2025*.
- Sirachet Phodhiran, Pichate Kunakornvong, Pongpon Nilaphruek, Jaturapith Krohkaew, Niti Witthayawiroj, Padma Nyoman Crisnapati, Yamin Thwe. A Competency-Based Curriculum for Fostering Artificial Intelligence Skills in Thai Children and Youth. *International Journal of Engineering Trends and Technology*. Volume 72 Issue 10, 357-372, October 2024, Seventh Sense Research Group. ISSN: 2231-5381/[https://doi.org/10.14445/22315381/ - V72110P135](https://doi.org/10.14445/22315381/-V72110P135)

อภิธานศัพท์

บทที่ 1-2: พื้นฐานและสถาปัตยกรรม

- **Access Control List (ACL):** รายการควบคุมสิทธิ์การเข้าถึงทรัพยากรในระบบ
- **Active Attack:** การโจมตีที่แทรกแซงหรือดัดแปลงข้อมูลโดยตรง
- **Availability (ความพร้อมใช้งาน):** การรับประกันว่าระบบและข้อมูลสามารถเข้าถึงได้ตลอดเวลา
- **Confidentiality (การรักษาความลับ):** การป้องกันไม่ให้ข้อมูลรั่วไหลแก่ผู้ไม่ได้รับอนุญาต
- **Integrity (ความถูกต้องครบถ้วน):** การป้องกันไม่ให้ข้อมูลถูกแก้ไขโดยไม่ได้รับอนุญาต
- **CIA Triad:** กรอบแนวคิดด้านความมั่นคงสารสนเทศที่ประกอบด้วย Confidentiality, Integrity, Availability
- **Defense-in-Depth:** กลยุทธ์การป้องกันหลายชั้นเพื่อลดความเสี่ยง
- **ISO/IEC 27001:** มาตรฐานระบบบริหารจัดการความมั่นคงสารสนเทศ

บทที่ 3-4: ภัยคุกคามและการโจมตี

- **Brute Force Attack:** การเดาห้สซ้ำๆ จนกว่าจะพบรหัสที่ถูกต้อง
- **Buffer Overflow:** การโจมตีโดยใส่ข้อมูลเกินขอบเขตหน่วยความจำ
- **Denial of Service (DoS):** การโจมตีทำให้ระบบไม่สามารถให้บริการได้
- **Distributed DoS (DDoS):** การโจมตี DoS โดยใช้หลายเครื่องพร้อมกัน
- **Exploit:** ซอฟต์แวร์หรือโค้ดที่ใช้ประโยชน์จากช่องโหว่
- **Malware (มัลแวร์):** ซอฟต์แวร์ที่ประสงค์ร้าย เช่น ไวรัส หนอน ม้าโทรจัน แรนซัมแวร์
- **Phishing:** การหลอกลวงให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว
- **SQL Injection:** การฝังโค้ด SQL อันตรายเข้าไปในคำสั่งฐานข้อมูล
- **Zero-Day Exploit:** การโจมตีที่อาศัยช่องโหว่ที่ยังไม่ถูกแก้ไข

บทที่ 5-6: ไฟร์วอลล์และ VPN

- **Firewall:** ระบบกรองและควบคุมการรับส่งข้อมูลเครือข่าย

- **Intrusion Detection System (IDS):** ระบบตรวจจับการบุกรุก
- **Intrusion Prevention System (IPS):** ระบบป้องกันการบุกรุก
- **NAT (Network Address Translation):** การแปลงหมายเลข IP ภายใน-ภายนอก
- **VPN (Virtual Private Network):** เครือข่ายเสมือนที่เข้ารหัสการเชื่อมต่อ
- **IPsec:** โพรโทคอลสำหรับเข้ารหัสและตรวจสอบข้อมูลใน VPN
- **Split Tunneling:** การกำหนดให้ VPN ใช้เฉพาะบางทราฟฟิก

บทที่ 7: วิทยาการรหัสลับ

- **AES (Advanced Encryption Standard):** อัลกอริทึมเข้ารหัสมาตรฐานสากล
- **RSA:** อัลกอริทึมเข้ารหัสแบบกุญแจสมมาตร
- **ECC (Elliptic Curve Cryptography):** การเข้ารหัสโดยใช้สมการเส้นโค้งวงรี
- **Hash Function:** ฟังก์ชันแปลงข้อมูลเป็นค่าคงที่ เช่น SHA-256
- **Digital Signature:** กลไกยืนยันความถูกต้องและที่มาของข้อมูล
- **Key Management:** การสร้าง แจกจ่าย และจัดเก็บกุญแจเข้ารหัส

บทที่ 8–10: เครือข่ายและไร้สาย

- **LAN (Local Area Network):** เครือข่ายท้องถิ่น
- **DMZ (Demilitarized Zone):** โซนกึ่งกลางระหว่างเครือข่ายภายในและอินเทอร์เน็ต
- **SSID (Service Set Identifier):** ชื่อเครือข่าย Wi-Fi
- **WEP/WPA/WPA2/WPA3:** มาตรฐานความปลอดภัยไร้สาย
- **Rogue Access Point:** จุดเชื่อมต่อไร้สายที่ไม่ได้รับอนุญาต
- **Evil Twin Attack:** การสร้าง AP ปลอมเพื่อหลอกผู้ใช้

บทที่ 11–12: ความมั่นคงในไร้สายและระบบปฏิบัติการ

- **802.11ax (Wi-Fi 6):** มาตรฐาน Wi-Fi รุ่นใหม่ รองรับความเร็วสูงและประสิทธิภาพดีขึ้น
- **802.11i:** มาตรฐานด้านความปลอดภัยไร้สาย (WPA2)

- **Access Matrix:** ตารางที่กำหนดสิทธิ์ผู้ใช้ต่อวัตถุในระบบ
- **Capability List (C-list):** รายการสิทธิ์การเข้าถึงที่ผูกกับผู้ใช้หรือโปรเซส
- **Mandatory Access Control (MAC):** การควบคุมสิทธิ์ตามนโยบายกลาง
- **Role-Based Access Control (RBAC):** การกำหนดสิทธิ์ตามบทบาทของผู้ใช้

บทที่ 13: มาตรการความมั่นคง

- **PDPA (Personal Data Protection Act):** พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- **Cybersecurity Act 2562:** พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- **CII (Critical Information Infrastructure):** โครงสร้างพื้นฐานสารสนเทศสำคัญ
- **Incident Response:** การตอบสนองต่อเหตุการณ์ความมั่นคงไซเบอร์
- **Business Continuity Plan (BCP):** แผนความต่อเนื่องทางธุรกิจ

บทที่ 14: แนวโน้มยุค AI และ Quantum

- **AI Security:** การใช้ AI ในการตรวจจับ วิเคราะห์ และป้องกันภัยไซเบอร์
- **Generative AI Threats:** ภัยคุกคามจาก AI สร้างเนื้อหา เช่น Deepfake, Phishing อัตโนมัติ
- **Quantum Computer:** คอมพิวเตอร์ที่ใช้ควอนตัมบิตในการประมวลผล
- **Post-Quantum Cryptography (PQC):** อัลกอริทึมเข้ารหัสที่ทนทานต่อ Quantum Computer
- **Quantum Key Distribution (QKD):** การกระจายกุญแจโดยใช้คุณสมบัติของควอนตัม
- **Zero Trust Security:** แนวคิดที่ไม่เชื่อถือผู้ใช้หรืออุปกรณ์ใดโดยอัตโนมัติ

