

สารบัญ

	หน้า
บทที่ 1 พื้นฐานด้านความมั่นคงของระบบคอมพิวเตอร์	1-17
1.1 ความเป็นมาและความสำคัญ	1
1.2 นิยามความมั่นคงของระบบคอมพิวเตอร์	2
1.3 ความท้าทายด้านความมั่นคง	3
1.4 ศัพท์เฉพาะทางด้านความมั่นคง	4
1.5 การคุกคามความมั่นคง	6
1.6 การคุกคามส่วนต่างๆ ของระบบคอมพิวเตอร์	7
1.7 การละเมิดความมั่นคง	9
1.8 อนุกรมวิธานด้านความมั่นคง	11
1.9 มาตรการรับมือ	12
1.10 มาตรฐานสถาปัตยกรรมด้านความมั่นคง	14
1.11 ยุทธศาสตร์ในการรักษาความมั่นคงของระบบคอมพิวเตอร์	15
1.12 บทสรุป	16
ศัพท์ทบทวน	17
แบบฝึกหัด	17
รายการอ้างอิง	17
บทที่ 2 วิทยาการรหัสลับ	19-58
2.1 วิทยาการรหัสลับโดยสังเขป	19
2.2 ศัพท์เฉพาะ	20
2.3 แบบแผนวิทยาการรหัสลับ	20
2.4 กระบวนการเข้ารหัสและการวิเคราะห์รหัสลับ	23
2.5 ประเภทของการโจมตีในการถอดรหัส	31
2.6 การออกแบบกระบวนการเข้ารหัส	31
2.7 การเข้ารหัสแบบสมมาตร	32
2.8 มาตรฐานการเข้ารหัสลับข้อมูล	34
2.9 ทริปเปิลดีอีเอส	39

สารบัญ (ต่อ)

	หน้า
2.10 มาตรฐานการเข้ารหัสลับข้อมูลขั้นสูง	40
2.11 การกระจายคีย์	46
2.12 การเข้ารหัสโดยใช้คีย์สาธารณะ	46
2.13 Rivest-Shamir-Adelman (RSA)	47
2.14 ใบรับรองดิจิทัล	50
2.15 การพิสูจน์ข้อความจริง	52
2.16 ลายเซ็นดิจิทัล	55
2.17 บทสรุป	56
ศัพท์ทบทวน	57
แบบฝึกหัด	58
รายการอ้างอิง	58
บทที่ 3 ความมั่นคงด้านซอฟต์แวร์	59-94
3.1 ความหมายของมัลแวร์	60
3.2 ศัพท์เฉพาะของมัลแวร์	60
3.3 การแบ่งประเภทของมัลแวร์	61
3.4 ไวรัส	62
3.5 มาตรการรับมือกับไวรัส	65
3.6 วิวัฒนาการของแอนติไวรัส	67
3.7 เทคนิคแอนติไวรัสขั้นสูง	68
3.8 หนอน	71
3.9 มาตรการรับมือหนอน	75
3.10 บอต	78
3.11 รูทคิท	79
3.12 จุดอ่อนของซอฟต์แวร์ ที่เกิดจากการพัฒนาซอฟต์แวร์	80
3.13 การล้นของบัฟเฟอร์	80
3.14 การจัดการข้อมูลนำเข้าของโปรแกรม	87

สารบัญ (ต่อ)

	หน้า
3.15 การโจมตีโดยการยิงหรือฉีดยา	89
3.16 การตรวจสอบข้อมูลนำเข้าและวากยสัมพันธ์อย่างสมเหตุสมผล	89
3.17 การพัฒนาซอฟต์แวร์และการสร้างไฟล์แพคเกจ	90
3.18 ข้อแตกต่างระหว่างคุณภาพของซอฟต์แวร์และความมั่นคงของซอฟต์แวร์	91
3.19 บทสรุป	92
ศัพท์ทบทวน	93
แบบฝึกหัด	93
รายการอ้างอิง	94
บทที่ 4 ความมั่นคงของฐานข้อมูล	95-113
4.1 ระบบการจัดการฐานข้อมูล	95
4.2 ฐานข้อมูลเชิงสัมพันธ์	96
4.3 ความมั่นคงของฐานข้อมูล	98
4.4 ความถูกต้องและความน่าเชื่อถือสำหรับฐานข้อมูล	99
4.5 การควบคุมการเข้าถึงฐานข้อมูล	100
4.6 การควบคุมการเข้าถึงโดยใช้คำสั่ง SQL	101
4.7 การควบคุมการเข้าถึงตามบทบาท	102
4.8 ข้อมูลที่เป็นความลับ	103
4.9 การอนุมาน	104
4.10 มาตรการรับมือกับการอนุมาน	106
4.11 การป้องกันและต่อต้านการอนุมาน	108
4.12 การโจมตีด้วยการตามรอย	109
4.13 การเข้ารหัสฐานข้อมูล	111
4.14 บทสรุป	112
ศัพท์ทบทวน	113
แบบฝึกหัด	113
รายการอ้างอิง	113

สารบัญ (ต่อ)

	หน้า
บทที่ 5 การพิสูจน์ตนและการควบคุมการเข้าถึง	115-138
5.1 การพิสูจน์ตัวจริง	115
5.2 การพิสูจน์ตนโดยการเข้ารหัสผ่าน	116
5.3 การใช้โทเค็นในการพิสูจน์ตน	119
5.4 การพิสูจน์ตนโดยใช้ชีวมาตร	121
5.5 การพิสูจน์ตัวจริงระยะไกล โดยใช้ Challenge-Response	124
5.6 การพิสูจน์ตัวจริงในระบบประมวลผลแบบกระจายโดยใช้ Kerberos	124
5.7 การโจมตีการพิสูจน์ตัวจริง	126
5.8 การควบคุมการเข้าถึง	127
5.9 นโยบายการควบคุมการเข้าถึง	128
5.10 การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ	130
5.11 การควบคุมการเข้าถึงตามบทบาทหน้าที่	132
5.12 บทสรุป	136
ศัพท์ทบทวน	137
แบบฝึกหัด	138
รายการอ้างอิง	138
บทที่ 6 ความมั่นคงของระบบปฏิบัติการ	139-158
6.1 หน้าที่ของระบบปฏิบัติการ	139
6.2 การทำงานของระบบปฏิบัติการ	140
6.3 การป้องกันโดยทั่วไปของระบบปฏิบัติการ	142
6.4 การพิสูจน์ตัวจริง โดยใช้รหัสผ่านบนระบบปฏิบัติการยูนิกซ์	143
6.5 การคุ้มครองการใช้งานหน่วยความจำ	145
6.6 กลไกการคุ้มครองไฟล์	148
6.7 ระบบปฏิบัติการที่ไวใจได้	150
6.8 การเปรียบเทียบคุณลักษณะด้านความมั่นคงของระบบปฏิบัติการทั่วไปและระบบปฏิบัติการที่ไวใจได้	152

สารบัญ (ต่อ)

	หน้า
6.9 การออกแบบความมั่นคงในส่วนของเคอร์เนล	153
6.10 บทสรุป	156
ศัพท์ทบทวน	157
แบบฝึกหัด	157
รายการอ้างอิง	158
บทที่ 7 ความมั่นคงด้านเครือข่าย	159-206
7.1 การปฏิเสธการให้บริการ	159
7.2 การโจมตีโดยการลวงเลขที่อยู่ไอพี	160
7.3 การโจมตีโดยการทำให้ท่วม	161
7.4 การควบคุมการโจมตีแบบกระจายตามลำดับขั้น	165
7.5 การโจมตีแบบการสะท้อนกลับและการขยาย	166
7.6 การป้องกันการโจมตีจนทำให้เกิดการปฏิเสธการให้บริการ	170
7.7 ผู้บุกรุก	172
7.8 เทคนิควิธีการบุกรุก	176
7.9 ระบบตรวจจับการบุกรุก	177
7.10 ฮันนี่พอท	188
7.11 ไฟร์วอลล์ และระบบป้องกันการบุกรุก	189
7.12 Virtual Private Networks	200
7.13 บทสรุป	204
ศัพท์ทบทวน	205
แบบฝึกหัด	206
รายการอ้างอิง	206
บทที่ 8 ความมั่นคงของเครือข่ายไร้สาย	207-228
8.1 บทนำ	207
8.2 การคุกคามบนเครือข่ายไร้สาย	208
8.3 มาตรการความมั่นคงสำหรับเครือข่ายไร้สาย	210

สารบัญ (ต่อ)

	หน้า
8.4 มาตรฐานของการสื่อสารบนเครือข่ายไร้สาย IEEE 802.11	211
8.5 มาตรฐาน 802.1X การควบคุมการเข้าถึงทางพอร์ตสำหรับเครือข่ายไร้สาย	214
8.6 กลไกรักษาความมั่นคงสำหรับเครือข่ายไร้สายแบบ WEP	216
8.7 การพิสูจน์ทราบตัวตนของเครือข่ายไร้สาย	218
8.8 การพิสูจน์ทราบตัวตนในมาตรฐาน IEEE 802.11i	221
8.9 บทสรุป	226
ศัพท์ทบทวน	227
แบบฝึกหัด	228
รายการอ้างอิง	228
บทที่ 9 ความมั่นคงของเว็บ	229-251
9.1 ความเป็นมาและความสำคัญ	229
9.2 HTTP (HyperText Transfer Protocol) และ Cookie	230
9.3 โพรโทคอลเอชทีทีพีเอส และเอสเอสแอล	233
9.4 ช่องโหว่ของเอสเอสแอล	239
9.5 การโจมตีโดยใช้ Cross Site Script (XSS)	241
9.6 การโจมตีโดยการยิงหรือฉีด	244
9.7 การโจมตีโดยใช้ Cross Site Request Forgery (CSRF หรือ XCRF)	246
9.8 แนวทางการป้องกันและรักษาความมั่นคงของเว็บ	248
9.9 บทสรุป	249
ศัพท์ทบทวน	250
แบบฝึกหัด	250
รายการอ้างอิง	251
บทที่ 10 ความมั่นคงของโมบายแอปพลิเคชัน	253-278
10.1 ความเป็นมาและความสำคัญ	253
10.2 การคุกคามและพฤติกรรมของโมบายมัลแวร์	254
10.3 ความมั่นคงของแอนดรอยด์แอปพลิเคชัน	256

สารบัญ (ต่อ)

	หน้า
10.4 คุณลักษณะของแอนดรอยด์มัลแวร์	263
10.5 การตรวจจับแอนดรอยด์มัลแวร์	268
10.6 งานวิจัยที่ตรวจจับมัลแวร์แอปพลิเคชันบนระบบปฏิบัติการแอนดรอยด์	270
10.7 ความมั่นคงของไอโอเอส แอปพลิเคชัน	274
10.8 บทสรุป	275
ศัพท์ทบทวน	276
แบบฝึกหัด	276
รายการอ้างอิง	276
บทที่ 11 แบบจำลองด้านความมั่นคง	279-297
11.1 ความหมายของรูปนัยแบบจำลองความมั่นคง	279
11.2 นโยบายด้านความมั่นคง	280
11.3 แบบจำลองความมั่นคง	282
11.4 ระบบที่ไว้ใจได้	290
11.5 การประเมินความมั่นคง	294
11.6 บทสรุป	295
ศัพท์ทบทวน	296
แบบฝึกหัด	296
รายการอ้างอิง	297
บทที่ 12 การบริหารจัดการด้านความมั่นคง	299-320
12.1 ความหมายและความสำคัญของการบริหารจัดการความมั่นคง ของระบบคอมพิวเตอร์	299
12.2 การวางแผนรักษาความมั่นคง	300
12.3 แผนดำเนินธุรกิจอย่างต่อเนื่อง	303
12.4 แผนการตอบสนองเมื่อเกิดอุบัติเหตุ	305
12.5 การวิเคราะห์ความเสี่ยง	306
12.6 นโยบายความมั่นคงขององค์กร	311

สารบัญ (ต่อ)

	หน้า
12.7 ความมั่นคงทางกายภาพ	312
12.8 ศูนย์คอมพิวเตอร์สำรอง หรือศูนย์การกู้คืนระบบจากความเสียหาย	313
12.9 มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ	314
12.10 บทสรุป	319
ศัพท์ทบทวน	319
แบบฝึกหัด	320
รายการอ้างอิง	320
บทที่ 13 จริยธรรมและกฎหมายที่เกี่ยวข้องกับความมั่นคงของระบบคอมพิวเตอร์	321-345
13.1 กฎหมายและความมั่นคงของระบบคอมพิวเตอร์	322
13.2 ทรัพย์สินทางปัญญา	323
13.3 การคุ้มครองฮาร์ดแวร์คอมพิวเตอร์	327
13.4 สิทธิของนายจ้างและลูกจ้าง	332
13.5 จริยธรรมและประเด็นความมั่นคงของระบบคอมพิวเตอร์	334
13.6 กฎหมายและอาชญากรรมทางคอมพิวเตอร์	338
13.7 บทสรุป	344
ศัพท์ทบทวน	345
แบบฝึกหัด	345
รายการอ้างอิง	345