

สารบัญ

	หน้า
สารบัญ.....	(6)
รายการตาราง.....	(9)
รายการภาพประกอบ.....	(10)
บทที่	
1 บทนำ.....	1
1.1 ความสำคัญและที่มาของงานวิทยานิพนธ์.....	1
1.2 การตรวจเอกสาร.....	3
1.3 วัตถุประสงค์ของวิทยานิพนธ์.....	4
1.4 ขอบเขตและวิธีการดำเนินการวิจัย.....	4
1.4.1 การออกแบบและพัฒนาโปรแกรมตรวจจับการบุกรุก.....	5
1.4.2 การปรับปรุงระบบปฏิบัติการด้วยกลไกการตรวจจับการบุกรุก.....	5
1.4.3 การทดสอบประสิทธิภาพของระบบปฏิบัติการที่ได้รับการแก้ไข.....	5
1.5 ขั้นตอนและระยะเวลาการดำเนินการ.....	5
1.5.1 ขั้นตอนการดำเนินการ.....	5
1.5.2 ระยะเวลาการดำเนินการ.....	7
1.6 สถานที่และเครื่องมือที่ใช้ในงานวิจัย.....	7
1.7 ประโยชน์ที่คาดว่าจะได้รับ.....	8
2 ทฤษฎี หลักการและงานวิจัยที่เกี่ยวข้อง.....	9
2.1 บทนำ.....	9
2.2 ภัยคุกคามและการบุกรุกระบบคอมพิวเตอร์.....	9
2.2.1 ช่องทางของการบุกรุก.....	10
2.2.1.1 Race condition.....	11
2.2.1.2 Buffer overflow.....	12
2.2.1.3 Rootkit.....	16
2.2.2 ผลกระทบของการบุกรุกระบบ.....	17
2.3 การจัดอนุกรมวิธานของการบุกรุก.....	18

สารบัญ (ต่อ)

	หน้า
2.4 ระบบตรวจจับการบุกรุก.....	23
2.4.1 แนวทางของการตรวจจับการบุกรุก.....	24
2.4.2 คุณลักษณะของระบบตรวจจับการบุกรุกที่ดี.....	26
2.4.3 คุณลักษณะของการตรวจจับการบุกรุกที่เหมาะสมสำหรับการพัฒนากลไกการตรวจจับการบุกรุกในระบบปฏิบัติการ.....	27
2.5 ระบบปฏิบัติการยูนิกซ์.....	28
2.5.1 โปรแกรมและโปรเซสของระบบปฏิบัติการยูนิกซ์.....	28
2.5.2 สถาปัตยกรรมของระบบปฏิบัติการยูนิกซ์.....	29
2.5.3 ซิซเต็มคอลลของระบบปฏิบัติการ.....	30
2.5.4 โปรแกรมแบบ setuid/setgid.....	31
2.6 การตรวจจับการบุกรุกด้วยวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซส.....	32
2.6.1 การนิยามสถานะ.....	32
2.6.2 กฎสนับสนุน.....	36
2.7 สรุป.....	37
3 การวิเคราะห์และออกแบบกลไกการตรวจจับการบุกรุก.....	38
3.1 บทนำ.....	38
3.2 การติดตามการทำงานของโปรเซส.....	38
3.2.1 วิธีการติดตามการทำงานของโปรเซส.....	39
3.2.2 โปรเซสแบบปกติ.....	41
3.2.3 โปรเซสแบบ setuid.....	42
3.2.4 สรุปผลการศึกษาโปรเซสแบบปกติและโปรเซสแบบ setuid.....	44
3.3 การวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซสและกฎสนับสนุน.....	45
3.3.1 การวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซส.....	45
3.3.2 การนิยามสถานะ.....	46
3.3.3 การวิเคราะห์กฎสนับสนุน.....	48
3.3.3.1 กฎสนับสนุนข้อที่ 0.....	48
3.3.3.2 กฎสนับสนุนข้อที่ 1.....	49

สารบัญ (ต่อ)

	หน้า
3.3.3.3 กฎสนับสนุนข้อที่ 2	50
3.3.3.4 กฎสนับสนุนข้อที่ 3	52
3.3.3.5 กฎสนับสนุนข้อที่ 4	53
3.3.3.6 กฎสนับสนุนข้อที่ 5	56
3.3.3.7 ซิซเพิ่มเติมคอลที่มีผลกระทบต่อความปลอดภัยต่อระบบ	57
3.4 การวิเคราะห์ข้อมูลนำเข้า	59
3.5 บทสรุป	59
4 ระบบตรวจจับการบุกรุกในระดับโปรแกรมประยุกต์	61
4.1 บทนำ	61
4.2 สถาปัตยกรรมของโปรแกรมตรวจจับการบุกรุก	61
4.3 ข้อมูลนำเข้าของโปรแกรมตรวจจับการบุกรุก	63
4.4 การพัฒนาโปรแกรมตรวจจับการบุกรุก	63
4.4.1 โครงสร้างของโปรแกรม ktruss	63
4.4.2 การอ่านโปรแกรมนำเข้าจากโปรแกรม ktruss	64
4.4.3 โมดูลที่สำคัญของโปรแกรมตรวจจับการบุกรุก	66
4.5 การติดตามการทำงานของโปรเซสในระบบปฏิบัติการ	70
4.6 การทดสอบประสิทธิภาพของโปรแกรมตรวจจับการบุกรุก	71
4.6.1 การทดสอบความแม่นยำตามกฎสนับสนุน	71
4.6.2 การทดสอบความแม่นยำด้วยโปรแกรมบุกรุกที่ได้จากการสืบค้นทางอินเทอร์เน็ต	74
4.6.3 การทดสอบเพื่อหาผลกระทบของโปรแกรมตรวจจับการบุกรุกที่มีต่อระบบปฏิบัติการ	75
4.7 บทสรุป	76
5 กลไกการตรวจจับการบุกรุก	77
5.1 บทนำ	77
5.2 สถาปัตยกรรมของกลไกการตรวจจับการบุกรุก	78
5.3 การแก้ไขซิซเพิ่มเติมคอลของระบบปฏิบัติการ	78

สารบัญ (ต่อ)

	หน้า
5.3.1 โครงสร้างของซีซีทีเอ็มคอลในระบบปฏิบัติการเน็ตบีเอสดี.....	78
5.3.2 การอ่านข้อมูลนำเข้าสำหรับกลไกการตรวจจับการบุกรุก.....	80
5.3.3 โมดูลสำคัญที่เกี่ยวข้องกับกลไกการตรวจจับการบุกรุก.....	82
5.3.4 การแก้ไขซีซีทีเอ็มคอลที่เกี่ยวข้องกับความปลอดภัย.....	84
5.4 บทสรุป.....	87
6 ประสิทธิภาพของกลไกการตรวจจับการบุกรุก.....	88
6.1 บทนำ.....	88
6.2 การทดสอบประสิทธิภาพของกลไกการตรวจจับการบุกรุก.....	88
6.2.1 การทดสอบความแม่นยำของกลไกการตรวจจับการบุกรุก.....	88
6.2.1.1 การทดสอบความแม่นยำในระดับโมดูล.....	89
6.2.1.2 การทดสอบด้วยโปรแกรมบุกรุก.....	93
6.2.1.3 การทดสอบระบบในสภาวะแวดล้อมจริง.....	94
6.2.2 การทดสอบความคงทนของกลไกการตรวจจับการบุกรุก.....	99
6.2.2.1 การทดสอบระบบเมื่อทรัพยากรของระบบเหลืออยู่น้อย.....	100
6.2.2.2 การทดสอบระบบเมื่อมีโปรเซสบุกรุกจำนวนมาก.....	101
6.3 การทดสอบเพื่อหาผลกระทบที่มีต่อชุดคำสั่งของระบบปฏิบัติการ.....	101
6.3.1 การทดสอบหาผลกระทบต่อโปรแกรมแบบ setuid.....	102
6.3.2 การทดสอบหาผลกระทบจากการทำงานในสถานการณ์จริง.....	103
6.4 การทดสอบหาประสิทธิภาพของระบบปฏิบัติการหลังจากที่แก้ไขซีซีทีเอ็มคอล.....	104
6.4.1 กรณีทดสอบ.....	104
6.4.2 วิธีการวัดเวลาการทำงานของซีซีทีเอ็มคอล.....	105
6.4.3 ผลการวัดเวลาการทำงานของซีซีทีเอ็มคอลแต่ละกลุ่ม.....	105
6.5 บทสรุป.....	110
7 บทสรุป ปัญหาและข้อเสนอแนะ.....	111
7.1 บทนำ.....	111
7.2 สรุปผลการทำวิทยานิพนธ์.....	111
7.3 ผลที่ได้จากการทำวิทยานิพนธ์ชุดนี้.....	113

สารบัญ (ต่อ)

	หน้า
7.4 ปัญหาและอุปสรรคของการทำวิทยานิพนธ์.....	114
7.5 ข้อเสนอแนะ.....	115
บรรณานุกรม.....	115
ภาคผนวก.....	117
. รหัสต้นฉบับของระบบปฏิบัติการเฉพาะส่วนของซีซีทีเอ็มคอล.....	118
ผลงานตีพิมพ์เผยแพร่จากวิทยานิพนธ์.....	134
ประวัติผู้เขียน.....	150

รายการตาราง

ตาราง		หน้า
2.1	การจัดอนุกรมวิธานของการบุกรุกตามแนวคิดของ Simon	23
3.1	ผลของการติดตามการเรียกใช้ซิชเพิ่มคอลของโปรเซส ls ด้วยคำสั่ง ktrace	39
3.2	ความหมายของ trace point ของซิชเพิ่มคอล ktrace()	40
3.3	ผลของการติดตามการเรียกใช้ซิชเพิ่มคอลของโปรเซส ls ด้วยคำสั่ง ktrace	41
3.4	ผลของการติดตามการเรียกใช้ซิชเพิ่มคอลของโปรเซส passwd ด้วยคำสั่ง ktrace	43
3.5	การกำหนดค่าให้สัญลักษณ์ในระบบปฏิบัติการเน็ตบีเอสดี	46
3.6	การนิยามสถานะเมื่อโปรเซสมีค่าประจำสถานะเป็นค่าต่างๆ	47
3.7	แสดงผลการศึกษาความสัมพันธ์ของแฟ้ม /etc/master.passwd และ /etc/passwd สำหรับการสร้างชื่อบัญชีผู้ใช้	54
3.8	ชื่อซิชเพิ่มคอลที่มีผลกระทบต่อความปลอดภัยของระบบ	58
4.1	ข้อมูลนำเข้าของระบบตรวจจับการบุกรุก	68
4.2	ผลการทดสอบความแม่นยำด้วยโปรแกรมบุกรุก	74
5.1	ชื่อข้อมูลและวิธีการอ่านข้อมูลนำเข้า	80
5.2	การอ่านค่าพารามิเตอร์ของซิชเพิ่มคอล open()	82
5.3	กลุ่มของซิชเพิ่มคอลซึ่งจัดจำแนกตามวิธีการแก้ไข	84
6.1	กรณีทดสอบและผลการทดสอบสำหรับ โมดูลการนิยามสถานะ	89
6.2	กรณีทดสอบสำหรับการทดสอบ โมดูลพิจารณาคุณสมบัติ	90
6.3	กรณีทดสอบของการทดสอบ โมดูลตอบสนอง	91
6.4	กรณีทดสอบของการทดสอบด้วยโปรแกรมบุกรุกซึ่งจัดจำแนกตามผลกระทบ	93
6.5	เปรียบเทียบทรัพยากรของระบบปฏิบัติการระหว่างเหตุการณ์ปกติและสถานะเครียด	100
6.6	เวลาที่ใช้ในการทำงานของซิชเพิ่มคอลก่อนและหลังการแก้ไข	106

รายการภาพประกอบ

ภาพประกอบ	หน้า
2.1 โครงสร้างของหน่วยความจำแสดก	14
2.2 โครงสร้างของหน่วยความจำแสดกเมื่อเกิด buffer overflow	15
2.3 สถาปัตยกรรมแบบชั้นของระบบปฏิบัติการยูนิกซ์	29
2.4 การเปลี่ยนแปลงสถานะของโปรเซส	33
2.5 การเปลี่ยนแปลงสถานะของโปรเซสทั้ง 6 สถานะ	35
3.1 แผนภาพการเปลี่ยนแปลงสถานะของโปรเซสแบบปกติและแบบ setuid	44
3.2 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 0	48
3.3 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 1	49
3.4 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 2 ด้วยซิกเซ็มคอด open()	51
3.5 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 2 ด้วยซิกเซ็มคอดกลุ่ม chmod	52
3.6 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 3	53
3.7 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 4	56
3.8 แผนภาพการเปลี่ยนแปลงสถานะของการตรวจจับการบุกรุกซึ่งละเมิดกฎสนับสนุนข้อที่ 5	57
4.1 สถาปัตยกรรมของโปรแกรมตรวจจับการบุกรุก	61
4.2 โมดูลของโปรแกรม ktruss	64
4.3 โปรเซสเริ่มต้นของระบบปฏิบัติการ	71
5.1 สถาปัตยกรรมของกลไกการตรวจจับการบุกรุกของระบบปฏิบัติการ	76
5.2 โครงสร้างข้อมูล struct proc, struct pcred และ struct ucred	81
5.3 โครงสร้างแสดงความสัมพันธ์ของโปรเซส	83

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
6.1 ผลการทำงานของกลไกการตรวจจับการบุกรุก	94
6.2 การจัดเตรียมระบบเพื่อทดสอบการทำงานของกลไกการตรวจจับการบุกรุก	95
6.3 ผลการทดสอบระบบในแฟ้ม /var/log/vsftpd.log	96
6.4 ผลการทดสอบระบบในแฟ้ม /var/log/authlog	98
6.5 เวลาที่ใช้ในการทำงานของซีซเต็มคอด setuid() ก่อนและหลังการแก้ไข	107
6.6 เวลาที่ใช้ในการทำงานของซีซเต็มคอด fchmod() ก่อนและหลังการแก้ไข	108
6.7 เวลาที่ใช้ในการทำงานของซีซเต็มคอด execve() ก่อนและหลังการแก้ไข	108
6.8 เวลาที่ใช้ในการทำงานของซีซเต็มคอด open() ก่อนและหลังการแก้ไข	109