สารบาญ

หน้า

บทคัดย่อ..... (3)
Abstract..... (4)
กิตติกรรมประกาศ..... (5)
สารบาญ..... (6)
รายการตาราง..... (11)
รายการภาพประกอบ..... (12)
ตัวย่อและสัญลักษณ์..... (14)
บทที่
1 บทนำ..... 1
1.1 ความสำคัญและที่มาของหัวข้อวิจัย..... 1
1.2 การตรวจเอกสาร..... 4
1.3 วัตถุประสงค์..... 5
1.4 ขอบเขตของการวิจัย..... 5
1.5 ขั้นตอนและวิธีดำเนินการวิจัย..... 6
1.6 ประโยชน์ที่คาดว่าจะได้รับ..... 6
2 ทฤษฎี หลักการ และงานวิจัยที่เกี่ยวข้อง..... 7
2.1 บทนำ..... 7
2.2 ภัยคุกคามระบบคอมพิวเตอร์..... 7
2.3 ช่องทางส่วนใหญ่ที่ผู้บุกรุกใช้ในการเข้าสู่ระบบ..... 10
2.4 ลักษณะการบุกรุกและผลกระทบ..... 12
2.5 ระบบตรวจจับการบุกุก..... 20
2.6 ประเภทของระบบตรวจจับการบุกรุก..... 22
2.7 ค่าประจำตัวผู้ใช้..... 27
2.8 System call..... 28
2.9 การเปลี่ยนแปลงสถานะ..... 32
2.10 กฎที่ใช้สนับสนุนระบบตรวจจับการบุกรุก..... 38
2.11 สรุป..... 39

สารบาญ (ต่อ)

	หน้า
3 การวิเคราะห์ ออกแบบระบบและการพัฒนาโปรแกรม	40
3.1 บทนำ	40
3.2 ภาพรวมของระบบตรวจจับการบุกรุกที่พัฒนาขึ้น	40
3.3 การเก็บรวบรวมและการวิเคราะห์ข้อมูลเข้า	41
3.4 การวิเคราะห์การบุกรุก	48
3.5 การวิเคราะห์กฎที่ใช้สนับสนุนการตรวจจับการบุกรุก	50
3.6 การออกแบบข้อมูลนำเข้า	60
3.7 การออกแบบโปรแกรมที่ใช้ในการตรวจจับตามกฎแต่ละข้อ	61
3.8 การออกแบบโปรแกรมที่ใช้ในการตรวจจับทั้งระบบ	64
3.9 แผนภาพกระแสข้อมูล	65
3.10 กลไกสถานะ	70
3.11 แผนผังระบบ	73
3.12 แผนผังการทำงานของการตรวจสอบการบุกรุก	76
3.13 การพัฒนาโปรแกรม	81
3.14 สรุป	87
4 การทดสอบระบบตรวจจับการบุกรุก	88
4.1 บทนำ	88
4.2 สภาพแวดล้อมในการทดสอบระบบ	88
4.3 การทดสอบการตรวจจับการบุกรุกตามเงื่อนไขสำหรับกฎแต่ละข้อ	89
4.4 การทดสอบการบุกรุกโดยใช้โปรแกรมการบุกรุกจากอินเตอร์เน็ต	103
4.5 ผลจากการทดสอบการตรวจจับการบุกรุก	110
4.6 การทดสอบการตัดสินผิดทางบวก	110
4.7 การทดสอบประสิทธิภาพของระบบ	111
4.8 สรุป	117
5 สรุปการวิจัย และข้อเสนอแนะ	118
5.1 บทนำ	118
5.2 สรุปการวิจัยระบบตรวจจับการบุกรุก	118

สารบาญ (ต่อ)

หน้า

5.3 การใช้งานระบบตรวจจับการบุกรุก..... 119

5.4 ปัญหาและข้อจำกัด..... 119

5.5 ข้อเสนอแนะ..... 120

บรรณานุกรม..... 121

ผลงานตีพิมพ์เผยแพร่จากวิทยานิพนธ์..... 125

ประวัติผู้เขียน..... 132

รายการตาราง

ตาราง	หน้า
1. ผลกระทบเมื่อผู้บุกรุกได้มาซึ่งบัญชีผู้ใช้ในระบบ	13
2. ผลกระทบที่เกิดขึ้นเมื่อผู้บุกรุกเข้าถึงแฟ้มข้อมูล	17
3. ผลกระทบอื่น ๆ ที่เกิดขึ้นเมื่อผู้บุกรุกบุกรุกระบบได้สำเร็จ	18
4. ส่วนหนึ่งของผลที่ได้จากการติดตามการเรียกใช้ system call ของคำสั่ง "ls" โดยใช้คำสั่ง ktrace	42
5. ส่วนหนึ่งของผลที่ได้จากการติดตามการเรียกใช้ system call ของคำสั่งปกติ โดยใช้คำสั่ง ktrace ที่แก้ไขแล้ว	43
6. trpoints(trace points) ของ system call *ktrace()*	44
7. ส่วนหนึ่งของผลที่ได้จากการติดตามการเรียกใช้ system call ของคำสั่งพิเศษ โดยใช้คำสั่ง ktrace ที่แก้ไขแล้ว	46
8. รายละเอียดระบบปฏิบัติการ NetBSD ที่ใช้ในการทดสอบระบบ	88
9. แสดงผลการทดสอบการตรวจจับการบุกรุก	110
10. แสดงผลการทดสอบการเรียกใช้งานคำสั่งระบบ	111
11. ตารางเปรียบเทียบเวลาที่ใช้ในการคอมไพล์เคอร์เนล	112
12. ผลจากการใช้โปรแกรม top เพื่อดูขนาดของไฟล์ที่ใช้ตรวจจับการบุกรุก	113

รายการภาพประกอบ

ภาพประกอบ	หน้า
1. ระบบเฝ้าติดตามเสนอโดย Anderson	21
2. แสดงการทำงานของ system call	29
3. แสดงการเปลี่ยนแปลงสถานะเมื่อเรียกใช้คำสั่งปกติ	36
4. แสดงการเปลี่ยนแปลงสถานะเมื่อเรียกใช้คำสั่งที่มีการกำหนด set-user-ID bit	36
5. แสดงการเปลี่ยนแปลงสถานะเมื่อเรียกใช้คำสั่งที่มีการกำหนด set-group-ID bit	37
6. แสดงภาพรวมของลักษณะการเปลี่ยนแปลงสถานะของทุกสถานะ	37
7. State transition diagram แสดงการทำงานของคำสั่งปกติ	47
8. State transition diagram แสดงการทำงานของคำสั่งพิเศษ (setuid โปรแกรม)	47
9. รูปแบบการโจมตีโดยทั่วไป	49
10. State transition diagram สำหรับการบุกรุกตามกฎข้อที่ 0 กรณีที่ 1	51
11. State transition diagram สำหรับการบุกรุกตามกฎข้อที่ 0 กรณีที่ 2	51
12. State transition diagram สำหรับการบุกรุกตามกฎข้อที่ 1 กรณีที่ 1	52
13. State transition diagram สำหรับการบุกรุกตามกฎข้อที่ 1 กรณีที่ 2	53
14. State transition diagram สำหรับการบุกรุกโดยสร้างโปรแกรมประเภท setuid กรณีที่ 1	54
15. State transition diagram สำหรับการบุกรุกโดยสร้างโปรแกรมประเภท setuid กรณีที่ 2	55
16. State transition diagram สำหรับการบุกรุกกรณีที่มีการแก้ไขไฟล์โปรแกรมระบบ	56
17. State transition diagram สำหรับการบุกรุกกรณีที่พยายามเรียกใช้ไฟล์รหัสผ่าน	57
18. State transition diagram สำหรับการบุกรุกกรณีที่มีการเรียกใช้ system call ที่ไม่ได้รับการอนุญาต	59
19. System Module	64
20. DFD ระดับสูงระบบตรวจจับการบุกรุก	66
21. ภาพรวม DFD ระบบตรวจจับการบุกรุก	67
22. DFD ระดับย่อยของโปรเซสที่ 2 การตรวจสอบสถานะ	67
23. DFD ระดับย่อยของโปรเซสที่ 3 การตรวจจับการบุกรุก	68
24. DFD ระดับย่อยของโปรเซสที่ 3.2 การตรวจสอบ trpoint ประเภท system call	68
25. DFD ระดับย่อยของโปรเซสที่ 3.3 การตรวจสอบ trpoint ประเภท ktr_namei	69

รายการภาพประกอบ (ต่อ)

ภาพประกอบ	หน้า
26. DFD ระดับย่อยของโปรเซสที่ 3.4 การหยุดการทำงานของโปรเซสที่เข้าข่ายการบุกรุก	69
27. DFD ระดับย่อยของโปรเซสที่ 3.2.2 การตรวจสอบ flag และ mode ของ system call *open()*	70
28. กลไกสถานะ	71
29. กลไกสถานะของกระบวนการตรวจจับการบุกรุกเมื่อมีเหตุการณ์ทำให้เกิดการเปลี่ยนแปลงของค่า UID EUID GID หรือ EGID ของโปรเซส	71
29. แผนผังระบบการตรวจจับการบุกรุกในภาพรวม	73
30. แผนผังระบบการทำงานของฟังก์ชัน Load2Buff()	74
31. แผนผังระบบการทำงานของการตรวจสอบสถานะ	75
31. แผนผังระบบการทำงานของการตรวจสอบการบุกรุก	76
32. แผนผังระบบการทำงานของฟังก์ชัน ktrnamei()	77
33. แผนผังระบบการทำงานของฟังก์ชัน chk_cmd()	78
34. แผนผังระบบการทำงานของฟังก์ชัน chk_mode()	78
35. แผนผังระบบการทำงานของฟังก์ชัน chk_flag_mode()	79
36. แผนผังระบบการทำงานของฟังก์ชัน chk_path()	80
37. แผนผังระบบการทำงานของฟังก์ชัน killsid()	80
38. ตัวอย่างการบันทึกข้อมูลโปรเซสที่ถูกติดตามในล็อคไฟล์	83
39. กราฟแสดงการเปลี่ยนแปลงขนาดไฟล์ที่ใช้ตรวจจับการบุกรุก	116

ตัวย่อและสัญลักษณ์

DDIS	=	Distributed Intrusion Detection System
DFD	=	Data Flow Diagram
DoS	=	Denial of Service
EID	=	Effective Identifier
EGID	=	Effective Group Identifier
EUID	=	Effective User Identifier
FSA	=	Finite State Automata
FSM	=	Finite State Machine
GID	=	Group Identifier
HIDS	=	Host-based Intrusion Detection System
IDES	=	Intrusion Detection Expert System
IDS	=	Intrusion Detection System
ISOA	=	Information Security Officer's Assistant
MIDAS	=	Multics Intrusion Detection and Alerting System
NADIR	=	Network Anomaly Detection and Intrusion Reporter
NIDS	=	Network-based Intrusion Detection System
NSM	=	Network Security Monitor
RBID	=	Rule-based Intrusion Detection System
UID	=	User Identifier