

การพัฒนาโปรแกรมตรวจสอบความมั่นคงสำหรับยูนิกซ์

นายธงชัย โรจน์กังสดาล



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

พ.ศ. 2536

ISBN 974-582-855-6

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

018828 117365999

DEVELOPMENT OF SECURITY CHECKING PROGRAM FOR UNIX

MR. THONGCHAI ROJKANGSADAN

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science

Department of Computer Engineering

Graduate School

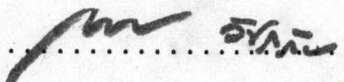
Chulalongkorn University

1993

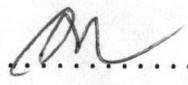
ISBN 974-582-855-6

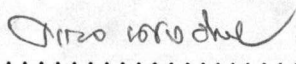
หัวข้อวิทยานิพนธ์ การพัฒนาโปรแกรมตรวจสอบความมั่นคงสำหรับยูนิกซ์
โดย นายธงชัย โรจน์กั้งสตาล
ภาควิชา วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา อาจารย์ ดร. ยรรยง เต็งอำนวยการ

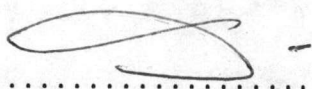
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของ
การศึกษาตามหลักสูตรปริญญาโทบัณฑิต

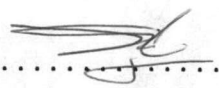
.....  คณบดีบัณฑิตวิทยาลัย
(ศาสตราจารย์ ดร. ถาวร วัชรากัญ)

คณะกรรมการสอบวิทยานิพนธ์

.....  ประธานกรรมการ
(รองศาสตราจารย์ เตือน สิ้นธุ์พันธ์ประทุม)

.....  อาจารย์ที่ปรึกษา
(อาจารย์ ดร. ยรรยง เต็งอำนวยการ)

.....  กรรมการ
(รองศาสตราจารย์ สมชาย ทยานอง)

.....  กรรมการ
(อาจารย์ จารุมাত্র ปิ่นทอง)



พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว

ธงชัย วิจารณ์กมล : การพัฒนาโปรแกรมตรวจสอบความมั่นคงสำหรับยูนิกซ์
(DEVELOPMENT OF SECURITY CHECKING PROGRAM FOR UNIX) อ.ที่ปรึกษา :
อ.ดร.ยรรยง เต็งอำนาจ, 66 หน้า. ISBN 974-582-855-6

การวิจัยครั้งนี้มีจุดมุ่งหมายเพื่อพัฒนาโปรแกรมตรวจสอบความมั่นคงสำหรับยูนิกซ์ โปรแกรมตรวจสอบความมั่นคงสำหรับยูนิกซ์ประกอบด้วย ส่วนติดต่อผู้ใช้ ซึ่งมีลักษณะเป็นเมนู พัฒนาโดยใช้ภาษา ซี และชุดคำสั่งเคิร์ล และชุดโปรแกรมตรวจสอบความมั่นคง ซึ่งเป็นชุดของโปรแกรมย่อยที่ทำหน้าที่ตรวจสอบจุดหละหลวมในระบบยูนิกซ์ เมื่อโปรแกรมตรวจพบจุดหละหลวมในที่ใดก็จะแจ้งให้ผู้ใช้ทราบ พร้อมทั้งมีข้อความช่วยเหลือ

ผลการวิจัยพบว่า โปรแกรมตรวจสอบความมั่นคงนี้ สามารถตรวจพบจุดหละหลวมความมั่นคงซึ่งพบเสมอในระบบยูนิกซ์ทั่วไป ทำให้ผู้ใช้สามารถแก้ไขได้ทันที

ภาควิชา วิศวกรรมคอมพิวเตอร์
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์
ปีการศึกษา 2535

ลายมือชื่อนิสิต
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

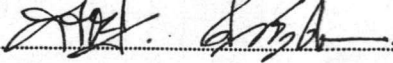
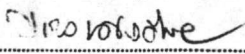
C117056 : MAJOR COMPUTER SCIENCE
KEY WORD: SECURITY/PROGRAM/UNIX OPERATING SYSTEM

THONGCHAI ROJKANGSADAN : DEVELOPMENT OF SECURITY CHECKING PROGRAM
FOR UNIX. THESIS ADVISOR : YUNYONG TENG-AMNUAY, Ph.D. 66 PP.
ISBN 974-582-855-6

This study was to develop security checking program suite for UNIX.
It consists of user interface which uses C language and CURSES library for
development. The suite consists of a set of security checking programs which
check security holes under UNIX. When they found any security holes they
will notify the system administrator and suggest remedy with help messages.

It was found that the security checking program could find common
security holes under UNIX. So user can close any security holes in time.

ภาควิชา วิศวกรรมคอมพิวเตอร์
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์
ปีการศึกษา 2535

ลายมือชื่อนิสิต 
ลายมือชื่ออาจารย์ที่ปรึกษา 
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยความช่วยเหลืออย่างดียิ่ง ของอาจารย์ ดร. ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำและข้อคิดเห็นต่างๆ แก่ผู้วิจัยและตรวจสอบแก้ไขวิทยานิพนธ์ฉบับนี้ ทำให้มีความถูกต้องและสมบูรณ์มากที่สุด ผู้วิจัยขอกราบขอบพระคุณในความกรุณาเป็นอย่างสูง

ขอขอบพระคุณ ท่านคณะกรรมการสอบวิทยานิพนธ์ ที่ได้ช่วยพิจารณา ให้คำแนะนำตรวจทาน แก้ไข และอนุมัติวิทยานิพนธ์ฉบับนี้

ขอขอบคุณเพื่อนๆ สาขาวิทยาศาสตร์คอมพิวเตอร์ ทุกท่านที่ให้ความช่วยเหลือ ตลอดจนเป็นกำลังใจแก่ผู้วิจัยตลอดมา

ท้ายสุดนี้ ผู้วิจัยใคร่กราบขอบพระคุณ บิดา-มารดา ซึ่งเป็นผู้มีพระคุณแก่ผู้วิจัยอย่างหาที่เปรียบมิได้ ซึ่งคอยให้กำลังใจและสนับสนุนผู้วิจัยมาโดยตลอด คุณความดีใดที่เกิดจากงานวิทยานิพนธ์ครั้งนี้ ผู้วิจัยขออุทิศแก่ บิดา-มารดาของผู้วิจัย หากมีข้อผิดพลาดประการใด ผู้วิจัยขออภัยมา ณ ที่นี้ด้วย

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ฉ
สารบัญตาราง	ญ
สารบัญภาพ	ณ

บทที่

1. บทนำ	1
ความเป็นมาของปัญหา	1
วัตถุประสงค์ของการวิจัย	3
ขอบเขตการวิจัย	3
ขั้นตอนการวิจัย	3
ประโยชน์ที่คาดว่าจะได้รับ	4
2. ชุดคำสั่งเคิร์ส	5
ความเป็นมา	5
โครงสร้างของวินโดว์	5
โครงสร้างของโปรแกรมเคิร์ส	6

ฟังก์ชันที่เกี่ยวข้องกับการกำหนดสถานะของโปรแกรม	7
ฟังก์ชันที่เกี่ยวข้องกับวินโดว์	8
ฟังก์ชันที่เกี่ยวข้องกับการอ่านและแสดงผลข้อมูล	11
การแปลชุดคำสั่งโปรแกรมเคิร์ล	12
3. โครงสร้างความมั่นคงของระบบยูนิกซ์	13
นิยามที่เกี่ยวข้อง	13
Trusted Computing Base	14
โครงสร้างระบบความมั่นคงของยูนิกซ์	18
การตรวจสอบผู้ใช้	18
แฟ้มข้อมูล /etc/passwd และ /etc/shadow	18
ประเภทของผู้ใช้ในระบบยูนิกซ์	19
ประเภทของแฟ้มข้อมูลในระบบยูนิกซ์	20
กลไกการอารักขาแฟ้มข้อมูล	20
sticky bit	21
การได้สิทธิ์ชั่วคราว	22
4. การออกแบบและพัฒนาส่วนติดต่อผู้ใช้	24
ขั้นตอนการออกแบบโปรแกรม	24
การออกแบบโปรแกรมส่วนติดต่อผู้ใช้	24
การทำงานของโปรแกรม	25
ฟังก์ชัน main()	25
ฟังก์ชัน main_menu()	25
ฟังก์ชัน win_menu_user()	27
ฟังก์ชัน showmenu()	28

5. การออกแบบและพัฒนาชุดโปรแกรมตรวจสอบความมั่นคง	29
การออกแบบชุดโปรแกรมตรวจสอบความมั่นคง	29
ชุดโปรแกรมตรวจสอบความมั่นคงสำหรับผู้ใช้	31
chkpath.sh	31
chkuser.sh	32
trojan.sh	33
ชุดโปรแกรมตรวจสอบความมั่นคงของระบบ	33
passwd.sh	33
checkdir.sh	34
checkfile.sh	35
device.sh	35
ชุดโปรแกรมตรวจสอบความมั่นคงทางด้านเครือข่าย	36
ftp.sh	36
tcpchk.sh	36
tcpfile.sh	37
uucp.sh	38
ชุดโปรแกรมตรวจสอบความมั่นคงด้านอื่นๆ	38
chkmail.sh	38
chkmisc.sh	39
config.sh	39
suid1.sh	40
suid2.sh	40
sulog.sh	41
6. รายงานผลการวิจัย	42
สภาพแวดล้อมของการพัฒนาโปรแกรม	42
ความเร็วในการทำงาน	42

รูปแบบการแสดงผล	45
ข้อเสนอแนะในการนำโปรแกรมไปใช้งาน	45
7. สรุปผลการวิจัยและข้อเสนอแนะ	46
สรุปผลการวิจัย	46
ปัญหาที่พบระหว่างการวิจัย	46
ข้อเสนอแนะ	47
แนวทางวิจัยต่อ	48
บรรณานุกรม	49
ภาคผนวก	51
ภาคผนวก ก. รูปแบบของจอภาพ	52
ภาคผนวก ข. รูปแบบของการแสดงผล	57
ประวัติผู้เขียน	66

สารบัญตาราง

ตารางที่		หน้า
6.1	แสดงการเปรียบเทียบระหว่างเครื่อง MAMMOTH 386 และ STAR SERVER 486	43
6.2	แสดงผลเปรียบเทียบความเร็วในการทำงาน ระหว่าง เครื่อง MAMMOTH 386 และ STAR SERVER 486	44

สารบัญภาพ

ภาพที่	หน้า
3.1 ความสัมพันธ์ระหว่าง subject, reference monitor, ฐานข้อมูลควบคุม และแฟ้มตรวจสอบ	15
3.2 ภาพแสดงความสัมพันธ์ ที่เกิดจากการใช้ คำสั่ง more /etc/passwd	17