โปรแกรมตรวจสอบแฟ้มข้อมูลบนลีนุกซ์

Linux File Integrity Checker

จัดทำโดย

นาย ธนาวุฒิ ธนามี 43015359

นาย อภิเชษฐ์ วิหคโต 43015397

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2545

ปริญญานิพนธ์ปีการศึกษา 2545

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะ วิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง โปรแกรมตรวจสอบแฟ้มข้อมูลบนลีนุกซ์

Linux File Integrity Checker

ผู้จัดทำ

1. นาย ธนาวุฒิ ธนามี รหัสประจำตัว 43015359
2. นาย อภิเชษฐ์ วิหคโต รหัสประจำตัว 43015397

.....อาจารย์ที่ปรึกษา

(อาจารย์ ธนา หงษ์สุวรรณ)

.....อาจารย์ที่ปรึกษา

(อาจารย์ อัครเดช วัชระภูพงษ์)

โปรแกรมตรวจสอบแฟ้มข้อมูลบนลีนุกซ์

นาย ธนาวุฒิ	ธนามี	
นาย อภิเชษฐ์	วิหคโต	
อาจารย์ ธนา	หงษ์สุวรรณ	อาจารย์ที่ปรึกษา
อาจารย์ อัครเดช	วัชระภูพงษ์	อาจารย์ที่ปรึกษา

บทคัดย่อ

ปัจจุบันระบบเครือข่ายมีความสำคัญมากขึ้น นำมาใช้ในการดำเนินงานธุรกรรมสำคัญๆ แต่การติดตั้งและดูแลระบบเครือข่ายให้มีความปลอดภัยต่อเหล่าอาชญากรทางอินเทอร์เน็ตนั้นยังคงเป็นไปอย่างไม่สมบูรณ์ โครงงานนี้เป็นโครงงานที่พัฒนาเพื่อศึกษาและสร้างตัวตรวจสอบแฟ้มข้อมูลบนลีนุกซ์เป็นการรักษาความปลอดภัยเชิงรับซึ่งลีนุกซ์จะมองทุกอย่าง เช่น อุปกรณ์ต่าง ๆ เป็นแฟ้มข้อมูล ดังนั้นจึงเน้นการรักษาความปลอดภัย ไปที่แฟ้มข้อมูลของระบบเป็นหลัก โดยยึดหลักการว่าการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับแฟ้มข้อมูลของระบบและไม่ได้เกิดจากการกระทำของตัวระบบเองแล้วมีความเสี่ยงที่จะมีการบุกรุกเกิดขึ้นได้ โดยการตรวจสอบจะใช้ MD5 มาช่วยในการตรวจสอบเพื่อแยกแยะการเปลี่ยนแปลงของแฟ้มข้อมูล

นอกจากนี้ยังตรวจสอบว่ามีการเข้าถึงแฟ้มข้อมูลมีการแก้ไขสิทธิของแฟ้มข้อมูล และมีการเปลี่ยนแปลงของไอโหนด ดังนั้นเมื่อมีการเปลี่ยนแปลง ณ. จุดใดจะเก็บข้อมูลของการเปลี่ยนแปลงนั้นๆไว้จึงง่ายต่อการที่ผู้ดูแลระบบจะตรวจสอบว่ามีการบุกรุกระบบนั้นๆหรือไม่

จุดสนใจของโครงงานนี้อยู่ที่ระบบแฟ้มข้อมูลและโพรเซสที่ทำงานในระบบแพลตฟอร์มลีนุกซ์และพัฒนาโดยภาษาซี

Linux File Integrity Checker

Mr. Thanawut	Thanamee	
Mr. Apichet	Wihokto	
Mr. Thana	Hongsuwan	Advisor
Mr. Akkradach	Watcharapupong	Advisor

ABSTRACT

Nowadays, the network system is used to run out many important businesses but the way to set up and maintain the network system to be more safety and can prevent the system is insecure and incomplete. This project is developed to create the Linux File Integrity Checker, which is a protective security. Because Linux looks everything as a file, the project will focus at a system file by look at all of the system files' changes. If the changes do not come from it's own system, that's mean there is a risk of attacking. The inspection use MD5 to distinguish the changes of system file.

In addition to check file access, file permission edition and I-node change. Every changes will be kept for checking later.

This project pays attention to the system file and the process that work in Linux platform and be developed with C language.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี ด้วยความช่วยเหลือและได้รับความร่วมมือและได้รับคำปรึกษาจากอาจารย์ที่ปรึกษาทั้งสองท่านคือ อาจารย์ ธนา หงษ์สุวรรณและอาจารย์ อัครเดช วัชระภูพงษ์ ที่คอยให้คำแนะนำและเอาใส่ดูแลการทำโครงงานและตรวจสอบความถูกต้องของปริญญานิพนธ์ ซึ่งทางคณะผู้จัดทำต้องขอกราบขอบพระคุณเป็นอย่างสูง

นอกจากนี้ต้องขอกราบขอบคุณอาจารย์ประจำภาควิชา วิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ช่วยประสิทธิ์ประสาทวิชาความรู้ให้แก่คณะผู้จัดทำ อีกทั้งภาควิชาวิศวกรรมคอมพิวเตอร์ที่เอื้อเฟื้ออุปกรณ์ สถานที่อำนวยความสะดวกสบาย ต่าง ๆ ในการทำโครงงานนี้

ขอบขอบคุณเพื่อน ๆ ห้องพี่ทุกคนที่เป็นกำลังใจให้ เพื่อนชาวไอแซ็ก (ISAG)ได้แก่ พี่ต่อ พี่เชาว์ พี่เดียร์ และอีกหลายคนที่ทำวิจัยในห้องไอแซ็กที่คอยช่วยเหลือเมื่อยามมีข้อบกพร่องและช่วยกันแก้ไข

สุดท้ายนี้ที่ขาดไม่ได้ขอขอบพระคุณบุคคลที่ทำให้เรามีวันนี้ คือ บิดา มารดาที่เคารพเป็นอย่างยิ่งที่ให้กำเนิดคนนี้ขึ้นมา ที่คอยให้กำลังใจ เป็นห่วงเป็นใย ให้คำสั่งสอน ให้การศึกษาอย่างสูงสุด พร้อมทั้งให้การสนับสนุนปัจจัยในด้านต่าง ๆ นับเป็นพระคุณอย่างยิ่งสุดที่จะหาอะไรมาเปรียบเทียบได้

คณะผู้จัดทำขอระลึกถึงพระคุณอันยิ่งใหญ่สุดที่จะประมาณกว่านี้ไว้กว่าชีวิตหาไม่และขอกราบพระคุณทุกท่านไว้ ณ ที่นี้ด้วย

นาย ธนาวุฒิ ธนามี

นาย อภิเชษฐ์ วิหคโต

สารบัญ

บทคัดย่อ	**I**
Abstract	**II**
กิตติกรรมประกาศ	**III**
สารบัญ	**IV**
สารบัญรูป	**VI**
สารบัญตาราง	**VII**
บทที่ 1 บทนำ	**1**
1.1 ที่มาของปัญหา	1
1.2 วัตถุประสงค์ของโครงการ	1
1.3 ขอบเขตของโครงงาน	1
1.4 ประโยชน์ที่คาดว่าจะได้รับ	2
บทที่ 2 ความรู้เบื้องต้นเกี่ยวกับระบบแฟ้มข้อมูล	**3**
2.1 ระบบไฟล์	3
2.2 ระบบชื่อไฟล์ในลีนุกซ์	4
2.3 ระบบไฟล์ในลีนุกซ์	4
2.4 การจัดแบ่งพาร์ติชั่นของระบบไฟล์	5
2.5 การจัดไดเร็กทอรี่ของระบบไฟล์ลีนุกซ์	6
2.6 ไอโหนด	6
2.7 ประเภทของไฟล์	7
2.8 การจัดการไฟล์และไดเร็กทอรี่	8
2.9 ไฟล์สำคัญในการใช้งาน	13
2.10 สรุป	14
บทที่ 3 การทำงานกับไฟล์	**15**
3.1 โครงสร้างของไฟล์บนระบบลีนุกซ์	15
3.2 ไดเร็กทอรี่ที่สำคัญบนยูนิกซ์	15
3.3 ไฟล์ของอุปกรณ์	16
3.4 เรียกใช้งานฟังก์ชั่นระดับต่ำ	17
3.5 ฟังก์ชั่นการแอ็กเซสไฟล์ในระดับต่ำ	18
3.6 ฟังก์ชั่นระดับต่ำอื่น ในการจัดการไฟล์	22

สารบัญ (ต่อ)

3.7 ไลบรารีฟังก์ชั่น 24

3.8 ไลบรารี่ฟังก์ชั่นมาตรฐานสำหรับการอินพุต/เอาต์พุตข้อมูล 25

3.9 ฟังก์ชั่นจัดการรูปแบบการอินพุตและเอาต์พุตข้อมูล 29

3.10การจัดการกับไฟล์และไดเร็กทอรี 30

3.11ตรวจสอบไดเร็กทอรี่ 31

3.12 การระบุ error ของฟังก์ชั่น 32

บทที่ 4 การตรวจสอบความถูกต้องของข้อมูล 35

4.1 เนื้อหาโดยสังเขป 35

4.2 คำศัพท์และความหมายของสิ่งที่กล่าวในบทนี้ 35

4.3 MD5 อัลกอริทึม 36

4.4 ข้อแตกต่างระหว่าง MD5 และ MD4 42

4.5 สรุป 42

บทที่ 5 การวางแผนออกแบบและการสร้าง 43

5.1 ภาพรวมและโครงสร้างของโปรแกรม 43

5.2 การทำงานของแต่ละโปรเซสของการทำงานการอ่านการเก็บข้อมูลการใช้แฟ้มข้อมูล 44

5.3 การทำงานในแต่ละส่วนของการทำงานของการติดต่อกับผู้ดูแลระบบ 46

5.4 การทำงานของโปรแกรม 46

บทที่ 6 การทดลองและผลการทดลอง 50

บทที่ 7 วิจารณ์และสรุป 55

7.1 ผลการทำงานของโปรแกรม 55

7.2 แนวทางพัฒนาต่อ 55

7.3 ปัญหาที่พบในการทำโครงงาน 55

บรรณานุกรรม 56

สารบัญรูป

รูปที่ 3 – 1 ค่าตารางไอโหนดและตำแหน่งที่เก็บบนแผ่นดิสก์ 15

รูปที่ 3 – 2 โครงสร้างของไฟล์แบบต้นไม้ 16

รูปที่ 3 – 3 ฟังก์ชั่นการทำงานระดับต่ำ 18

รูปที่ 3 – 4 ขั้นตอนการทำงานของฟังก์ชั่น open 20

รูปที่ 3 – 5 ตำแหน่งต่างของ lseek 23

รูปที่ 3 – 6 การทำงานของฟังก์ชั่นระดับต่ำ 25

รูปที่ 4 – 1 แสดงการคำนวณแบบ MD5 37

รูปที่ 4 – 2 กระบวนการทำในหนึ่งบล็อกของ MD5 40

รูปที่ 4 – 3 แสดงการทำหนึ่งโอเปอร์เรเตอร์ของ MD5 [abcd k s i] 41

รูปที่ 5 - 1 ขั้นตอนการทำงานของการอ่านการเก็บข้อมูลการใช้งานแฟ้มข้อมูล 44

รูปที่ 5 – 2 ขั้นตอนการทำงานของส่วนผู้ดูแลระบบ 46

รูปที่ 6 – 1 การทดลองการเพิ่มแฟ้มข้อมูลที่จะตรวจสอบ 50

รูปที่ 6 – 2 การลบแฟ้มข้อมูลออกจากการตรวจสอบ 51

รูปที่ 6 – 3 ดูรายงานการเปลี่ยนแปลงในวันที่ 31/01/2003 เวลา 15 –16 นาฬิกา 52

รูปที่ 6 – 4 ดูรายการเปลี่ยนแปลงในวันที่ 31/01/2003 53

รูปที่ 6 – 5 แสดงการเปลี่ยนแปลงทั้งหมดที่เกิดขึ้น 54

สารบัญตาราง

ตารางที่ 2-1 ระบบไฟล์ของระบบปฏิบัติการชนิดต่างๆ 3

ตารางที่ 2-2 ระบบชื่อและขนาดของไฟล์ในรูปแบบต่างๆ 4

ตารางที่ 2-3 สิทธิในการเข้าใช้งาน 10

ตารางที่ 2-4 สิทธิขั้นต่ำในการใช้งานไฟล์ 11

ตารางที่ 2-5 การเปลี่ยนแปลงสิทธิโดยใช้ตัวอักษร 11

ตารางที่ 2-6 การกำหนดสิทธิของไฟล์และไดเรกทอรีโดยใช้ umask 12

ตารางที่ 2-7 ไฟล์สำคัญในระดับผู้ใช้ 13

ตารางที่ 2-8 ไฟล์สำคัญระดับใช้งาน 13

ตาราง 3 – 1 โหมดการทำงาน 20

ตารางที่ 3 – 2 ออพชั่นเพิ่มเติม 20

ตารางที่ 3 – 3 ค่าของ umask 21

ตารางที่ 3 – 4 โครงสร้างข้อมูล stat 24

ตารางที่ 4 – 1 เงื่อนไขของฟังก์ชั่น 41