การพัฒนาชั้นการเข้ารหัสลับสำหรับการใช้งานผ่านไปยังระบบยูนิกซ์อย่างปลอดภัยจากเครื่องคอมพิวเตอร์ส่วนบุคคล

นาย ไพโรจน์ ต้นศิริอนุสรณ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
พ.ศ. 2538

ISBN 974-632-746-1

DEVELOPMENT OF ENCRYPTION LAYER FOR TRANSPARENT SECURED ACCESS FROM A PC TO THE UNIX SYSTEM

Mr. Piroj Tonsirianusorn

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science

Department of Computer Engineering

Graduate School

Chulalongkorn University

1995

ISBN 974-632-746-1

หัวข้อวิทยานิพนธ์	การพัฒนาชั้นการเข้ารหัสลับสำหรับการใช้งานผ่านไปยังระบบยูนิกซ์อย่างปลอดภัยจากเครื่องคอมพิวเตอร์ส่วนบุคคล
โดย	นาย ไพโรจน์ ต้นศิริอนุสรณ์
ภาควิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร. ยรรยง เต็งอำนวย

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย
(รองศาสตราจารย์ ดร. สันติ ถุงสุวรรณ)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

.....อาจารย์ที่ปรึกษา
(อาจารย์ ดร. ยรรยง เต็งอำนวย)

.....กรรมการ
(อาจารย์ ธงชัย โรจน์กังสดาล)

.....กรรมการ
(อาจารย์ ญาใจ ลิ่มปิยะกรณ์)

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสีเขียวนี้เพียงแผ่นเดียว

ไพโรจน์ ต้นศิริอนุสรณ์:การพัฒนาชั้นการเข้ารหัสลับสำหรับการใช้งานผ่านไปยังระบบยูนิกซ์อย่างปลอดภัยจากเครื่องคอมพิวเตอร์ส่วนบุคคล (DEVELOPMENT OF ENCRYPTION LAYER FOR TRANSPARENT SECURED ACCESS FROM A PC TO THE UNIX SYSTEM) อ.ที่ปรึกษา : อ.ดร.ยรรยง เต็งอำนวย,65 หน้า. ISBN 974-632-746-1

การวิจัยนี้มีจุดมุ่งหมายในการพัฒนาระบบการเข้ารหัสลับข้อมูลสำหรับ โปรโตคอลทีซีพี/ไอพี เพื่อการใช้งานระบบปฏิบัติการยูนิกซ์จากเครื่องคอมพิวเตอร์ส่วนบุคคล โดยไม่จำเป็นต้องแก้ไขโปรแกรมต้นฉบับใดๆของโปรแกรมให้บริการ หรือ โปรแกรมขอรับบริการของระบบเดิม

ขอบเขตของการวิจัยนี้ คือ โปรแกรมขอรับบริการบนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้แพกเกตไดรเวอร์, โปรแกรมให้บริการอยู่บนระบบปฏิบัติการยูนิกซ์ และ การสื่อสารข้อมูลใช้อีเทอร์เนต

การวิจัยแบ่งการพัฒนาออกเป็น 4 ส่วน ได้แก่ 1.โปรเซสเกตเวย์ทำหน้าที่เข้ารหัสลับและถอดรหัสลับบนยูนิกซ์,2.โปรแกรมให้บริการคีย์บนยูนิกซ์,3.โปรแกรมการเข้ารหัสลับสำหรับแพกเกตไดรเวอร์ และ 4.โปรแกรมขอรับบริการคีย์บนดอส

การวิจัยครั้งนี้มีข้อจำกัดในเรื่องการเข้ารหัสลับและถอดรหัสลับที่ต่างชั้นของการสื่อสารข้อมูลทำให้การเข้ารหัสลับทำได้ในระดับไบต์เท่านั้น อย่างไรก็ตามการวิจัยยังคงพบว่าสามารถป้องกันการดักบันทึกข้อมูลจากโปรแกรมที่ทำหน้าที่ดักข้อมูลจากอีเทอร์เนตต่างๆได้ นอกจากนี้โปรแกรมยังสามารถทำงานได้บนระบบปฏิบัติการยูนิกซ์ต่างๆได้

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2538 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

C618055 : MAJOR COMPUTER SCIENCE
KEY WORD: TCP/IP/PROTOCOL / ENCRYPTION / UNIX / PACKET DRIVER

PIROJ TONSIRIANUSORN : DEVELOPMENT OF ENCRYPTION LAYER FOR TRANSPARENT SECURED ACCESS FROM A PC TO THE UNIX SYSTEM · THESIS ADVISOR : YUNYONG TENG-AMNUAY.Ph.D. 65 pp. ISBN 974-632-746-1

This research has the objective to develop the encryption system for TCP/IP protocol to access UNIX operating system from a personal computer without any modification of the program (source code) of the server and client.

The scope of this research is to develop the encryption system for client programs on personal computer which is using packet driver . server programs on the UNIX operating system and using Ethernet Communication.

Development compose of 4 parts. 1. Gateway process for encryption and decryption on UNIX. 2. Key server process on UNIX. 3. Encryption program for packet driver and 4. Key request program on DOS.

This research ha limitation on encryption data in different level of protocol stack. So encryption is only byte encryption. Howerver the system can protect some wire tapping from any Ethernet tapping program. The programs can also be implemented in many UNIX operating system.

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2538 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงได้โดยความช่วยเหลืออย่างดียิ่งของ อาจารย์ ดร. ยรรยง เต็งอำนวย ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้ให้คำแนะนำและขอเสนอแนะในการทำวิจัยมาตลอด ขอขอบคุณ อาจารย์ธงชัย โรจน์กังสดาล ที่ให้คำแนะนำและช่วยเหลือ ขอบคุณ คุณธีระพล ภูมิสัทธรรม ที่ได้ให้ความช่วยเหลืออำนวยความสะดวกสำหรับเครื่องมือประกอบการวิจัย รวมทั้งขอบคุณเพื่อนทั้งหลายที่เป็นกำลังใจ และ ให้คำแนะนำมาโดยตลอด

สุดท้ายนี้ผู้วิจัยขอกราบขอบพระคุณบิดา-มารดา ที่สนับสนุนและเป็นกำลังใจตลอดมา รวมทั้งครู-อาจารย์ทั้งหลายที่ได้เคยประสิทธิประสาทวิชาให้กับผู้วิจัยมาจนปัจจุบัน

. . . . . .

สารบัญ

สารบัญตาราง

สารบัญภาพ

หน้า