

การพัฒนาขั้นการเข้ารหัสลับสำหรับการใช้งานผ่านไปยังระบบยูนิกซ์
อย่างปลอดภัยจากเครื่องคอมพิวเตอร์ส่วนบุคคล



นาย ไพโรจน์ ต้นศิริอนุสรณ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

พ.ศ. 2538

ISBN 974-632-746-1

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

I16654638

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

พิมพ์ต้นฉบับบทความวิจัยวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว



ไฟโรจน์ ดนตรีอนุสรณ์: การพัฒนาชั้นการเข้ารหัสลับสำหรับการใช้งานผ่านไปยังระบบยูนิกซ์
อย่างปลอดภัยจากเครื่องคอมพิวเตอร์ส่วนบุคคล (DEVELOPMENT OF ENCRYPTION LAYER
FOR TRANSPARENT SECURED ACCESS FROM A PC TO THE UNIX SYSTEM)

อ.ที่ปรึกษา : อ.ดร.ยรรยง เต็งอ้วนวย, 65 หน้า. ISBN 974-632-746-1

การวิจัยนี้มุ่งมุ่งหมายในการพัฒนาระบบการเข้ารหัสลับข้อมูลสำหรับ โปรโตคอลที่ซีพี/ไอพี
เพื่อการใช้งานระบบปฏิบัติการยูนิกซ์จากเครื่องคอมพิวเตอร์ส่วนบุคคล โดยไม่จำเป็นต้องแก้ไขโปรแกรม
ต้นฉบับไคของโปรแกรมให้บริการ หรือ โปรแกรมขอรับบริการของระบบเดิม

ขอบเขตของการวิจัยนี้ คือ โปรแกรมขอรับบริการบนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้
แพคเกจไครเวอร์, โปรแกรมให้บริการอยู่บนระบบปฏิบัติการยูนิกซ์ และการสื่อสารข้อมูลใช้เทอร์เน็ต

การวิจัยแบ่งการพัฒนาออกเป็น 4 ส่วน ได้แก่ 1. โปรเซสเกตเวย์ทำหน้าที่เข้ารหัสลับและ
ถอดรหัสลับบนยูนิกซ์, 2. โปรแกรมให้บริการคีย์บนยูนิกซ์, 3. โปรแกรมการเข้ารหัสลับสำหรับแพคเกจไคร
เวอร์ และ 4. โปรแกรมขอรับบริการคีย์บนคอส

การวิจัยครั้งนี้มีข้อจำกัดในเรื่องการเข้ารหัสลับและถอดรหัสลับที่ต่างชั้นของการสื่อสารข้อมูล
ทำให้การเข้ารหัสลับทำได้ในระดับไคเท่านั้น อย่างไรก็ตามการวิจัยยังคงพบว่าจะสามารถป้องกันการดัก
บันทึกข้อมูลจากโปรแกรมที่ทำหน้าที่ดักข้อมูลจากอีเทอร์เน็ตต่างๆได้ นอกจากนี้โปรแกรมยังสามารถทำงาน
ไคบนระบบปฏิบัติการยูนิกซ์ต่างๆได้

ภาควิชา วิศวกรรมคอมพิวเตอร์

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์

ปีการศึกษา 2538

ลายมือชื่อนิสิต 

ลายมือชื่ออาจารย์ที่ปรึกษา 

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม



G618055 : 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. However 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

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์

ปีการศึกษา 2538

ลายมือชื่อนิสิต 

ลายมือชื่ออาจารย์ที่ปรึกษา 

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม



กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงได้โดยความช่วยเหลืออย่างยิ่งของ อาจารย์ ดร. ยรรยง เต็งอำนวย ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้ให้คำแนะนำและขอเสนอแนะในการทำวิจัย มาตลอด ขอขอบคุณ อาจารย์ธงชัย โรจน์กังสดาล ที่ให้คำแนะนำและช่วยเหลือ ขอขอบคุณ คุณธีระพล ภูมิสีธรรม ที่ได้ให้ความช่วยเหลืออำนวยความสะดวกสำหรับเครื่องมือประกอบการ วิจัย รวมทั้งขอบคุณเพื่อนทั้งหลายที่เป็นกำลังใจ และ ให้คำแนะนำมาโดยตลอด

สุดท้ายนี้ผู้วิจัยขอกราบขอบพระคุณบิดา-มารดา ที่สนับสนุนและเป็นกำลังใจตลอด มา รวมทั้งครู-อาจารย์ทั้งหลายที่ได้เคยประสิทธิ์ประสาทวิชาให้กับผู้วิจัยมาจนปัจจุบัน

.....



สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	ฉ
กิตติกรรมประกาศ	ณ
สารบัญตาราง	ญ
สารบัญภาพ	ณ
บทที่	
1. บทนำ	1
2. แนวคิดและทฤษฎีที่เกี่ยวข้อง	5
3. การออกแบบและพัฒนา	23
4. การทดสอบระบบงาน	42
5. สรุปการวิจัยและข้อเสนอแนะ	45
รายการอ้างอิง	48
ภาคผนวก	
ก. การใช้งานระบบ	51
ข. ตัวอย่างแพคเกจที่ได้รับการเข้ารหัสลับ	55
ประวัติผู้เขียน	65

สารบัญตาราง

	หน้า
ตารางที่ 2.1 ที่อยู่ของไอพีระดับต่างๆ	8

สารบัญภาพ

	หน้า
รูปที่ 2.1 แสดงความสัมพันธ์ของชั้นต่างของโปรโตคอลที่ซีพี/ไอพี	6
รูปที่ 2.2 การห่อหุ้มแพกเกต	10
รูปที่ 2.3 เฟรมอีเทอร์เน็ต	11
รูปที่ 2.4 การเข้ารหัสลับ	11
รูปที่ 2.5 การเข้ารหัสลับในระดับการเชื่อมโยงข้อมูล	13
รูปที่ 2.6 การเข้ารหัสลับระดับทรานสปอร์ต	13
รูปที่ 2.7 การเข้ารหัสลับระดับเครือข่าย	14
รูปที่ 2.8 แพกเกตไดรเวอร์	18
รูปที่ 2.9 การรับส่งข้อมูลผ่านทางแพกเกตไดรเวอร์	20
รูปที่ 2.10 เกตเวย์ของโปรแกรมประยุกต์จดหมายอิเล็กทรอนิกส์และเอฟทีพี สำหรับขออาร์เอฟซี	22
รูปที่ 3.1 ความสัมพันธ์ของส่วนประกอบต่างๆ	24
รูปที่ 3.2 การทำงานของโปรเซสเกตเวย์	26
รูปที่ 3.3 รูปแบบของข้อมูลเพื่อการสืบค้นข้อมูลเซสชันคีย์	27
รูปที่ 3.4 การเชื่อมโยงระหว่างโปรเซสเกตเวย์สำหรับเข้ารหัสลับ และ โปรเซสให้บริการ โปรแกรมประยุกต์	28
รูปที่ 3.5 โปรเซสเกตเวย์ในการทำงานกับเอฟทีพี	28
รูปที่ 3.6 ลักษณะการสลับเปลี่ยนตัวอักษร	30
รูปที่ 3.7 การเข้ารหัสลับของเซสชันคีย์	32
รูปที่ 3.8 การทำงานของโปรแกรมการเข้ารหัสลับสำหรับแพกเกตไดรเวอร์	34
รูปที่ 3.9 ลักษณะของตัวจัดการอินเตอร์รัพของ PKTCRYPT	36
รูปที่ 3.10 แสดงความสัมพันธ์ในการทำงานระหว่างโปรแกรมที่เรียกใช้แพกเกตไดรเวอร์, PKCRYPT และ แพกเกตไดรเวอร์	38
รูปที่ 3.11 อีเทอร์เน็ตเฟรม	39
รูปที่ 3.12 ไอพีแพกเกตที่รับส่งผ่านแพกเกตไดรเวอร์	39
รูปที่ 5.1 ลักษณะของข้อมูลของโปรโตคอลชั้นต่างๆ	45