

การพัฒนาระบบความมั่นคงของเทคโนโลยีโดยอาศัยระบบการเข้ารหัสลับ

นายธีระพล ภูมิสังขธรรม



ศูนย์วิทยพัชร์พยากร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

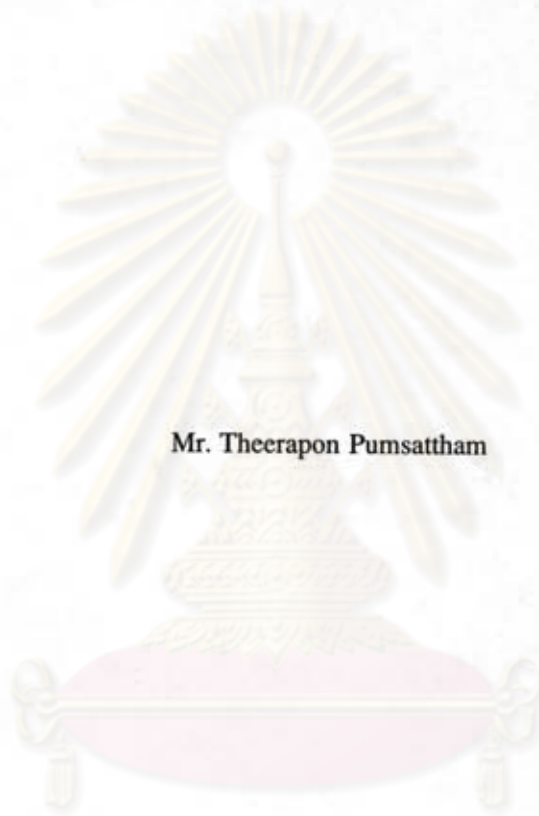
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

พ.ศ. 2539

ISBN 974-633-481-6

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

DEVELOPMENT OF TELNET AUTHENTICATION WITH CRYPTO SYSTEM



Mr. Theerapon Pumsattham

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science

Department of Computer Engineering

Graduate School

Chulalongkorn University

1996

ISBN 974-633-481-6

หัวข้อวิทยานิพนธ์

การพัฒนาระบบความมั่นคงของเทคโนโลยี โดยอาศัยระบบการเข้ารหัสลับ

โดย

นายธีระพล ภูมิศาสตร์

ภาควิชา

วิศวกรรมคอมพิวเตอร์

อาจารย์ที่ปรึกษา

อาจารย์ ดร.ชรรยง เต็งอำนาจ



บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นำวิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาโทบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย
(รองศาสตราจารย์ ดร. สันติ ฤงสุวรรณ)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ สมชาย ทยานอง)

.....อาจารย์ที่ปรึกษา
(อาจารย์ ดร. ชรรยง เต็งอำนาจ)

.....กรรมการ
(อาจารย์ จารุมาศ ปิ่นทอง)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. สาทิต วงศ์ประทีป)

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว

ธีระพล ภูมิศาสตร์ธรรม : การพัฒนาระบบความมั่นคงของเทลเน็ตโดยอาศัยระบบการเข้ารหัสลับ
(DEVELOPMENT OF TELNET AUTHENTICATION WITH CRYPTO SYSTEM) อ.ที่

ปรึกษา : อ. ดร. ชรรong เต็งอำนาจ, 70 หน้า. ISBN 974-633-481-6



จุดมุ่งหมายของการวิจัยคือ การพัฒนาระบบการเข้ารหัสข้อมูลสำหรับโปรโตคอลเทลเน็ต เพื่อสร้างช่องทางการสื่อสารที่ปลอดภัย ในการใช้งานระยะไกลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไปยังเครื่องคอมพิวเตอร์ระบบยูนิกซ์ โดยการแก้ไขโปรแกรมต้นฉบับของโปรแกรมเทลเน็ตผู้ให้บริการที่ทำงานบนระบบปฏิบัติการคอส และโปรแกรมเทลเน็ตผู้ให้บริการที่ทำงานบนระบบปฏิบัติการยูนิกซ์ และกระบวนการเข้ารหัสข้อมูลที่ใช้เป็นแบบบล็อกไซเฟอร์

การวิจัยได้เสนอแนวทางการพัฒนาเป็น 3 ส่วน ได้แก่ 1. การเจรจาทางเลือกสำหรับการเข้ารหัสข้อมูลของโปรโตคอลเทลเน็ต 2. การแลกเปลี่ยนเซสชันคีย์ 3. การเข้ารหัสข้อมูลและการถอดรหัสข้อมูล

ผลการทดสอบพบว่า สามารถเข้ารหัสข้อมูลที่ส่งผ่านระหว่างโปรแกรมเทลเน็ตผู้ให้บริการและโปรแกรมเทลเน็ตผู้ให้บริการในลักษณะบล็อกไซเฟอร์ ป้องกันการลอบดักข้อมูลจากโปรแกรมที่ทำหน้าที่ดักข้อมูลในระบบเครือข่ายอินเทอร์เน็ตได้ และโปรแกรมเทลเน็ตผู้ให้บริการสามารถทำงานบนระบบปฏิบัติการยูนิกซ์แบบต่างๆ ได้

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา วิศวกรรมคอมพิวเตอร์
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์
ปีการศึกษา 2538

ลายมือชื่อนิสิต
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

C618123 : MAJOR COMPUTER SCIENCE

KEY WORD:

TELNET PROTOCOL / UNIX / ENCRYPTION / BLOCK CIPHER

THEERAPON PUMSATTHAM : DEVELOPMENT OF TELNET AUTHENTICATION
WITH CRYPTO SYSTEM. THESIS ADVISOR : YUNYONG TENG-AMNUAY, Ph.D.

70 pp. ISBN 974-633-481-6

The objectives of this research is to develop the encryption system for telnet protocol, to implement the secure channel for using remote access from a personnel computer to UNIX machines by modifying the telnet client program on DOS and telnet server program on UNIX and algorithm of the encryption system is block cipher mode.

This research presents the development in of 3 parts. 1. Process of option negotiation for encryption of telnet protocol. 2. Process of session key exchanging. 3. Process of encryption and decryption.

The result can encrypt transmission data between telnet client program and telnet server program in block cipher mode. This can protect eavesdropping from any packet eavesdrop program and server program can be implemented on any type of UNIX operating system.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา.....วิศวกรรมคอมพิวเตอร์

สาขาวิชา.....วิทยาศาสตร์คอมพิวเตอร์

ปีการศึกษา..... 2538

ลายมือชื่อนิสิต..... 

ลายมือชื่ออาจารย์ที่ปรึกษา..... 

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....



กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จล่วงได้ โดยได้รับความช่วยเหลือจากอาจารย์ที่ปรึกษาวิทยานิพนธ์ อาจารย์ ดร. ชรรยง เต็งอำนวยการ ได้ให้คำแนะนำในการทำวิจัยมาโดยตลอด ขอขอบคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ให้ทุนอุดหนุนการศึกษาและการทำวิจัย ขอขอบคุณ คุณไพโรจน์ คันศิริอนุสรณ์ ที่ได้ให้คำแนะนำ รวมทั้งขอขอบคุณเพื่อนทุกคนที่เป็นกำลังใจ และให้คำแนะนำโดยตลอด

สุดท้ายนี้ผู้วิจัยขอกราบขอบพระคุณบิดา มารดา และพี่ทุกคน ที่สนับสนุนและเป็นกำลังใจตลอดมา รวมทั้งครูและอาจารย์ทั้งหลายที่ได้เคยประสิทธิ์ประสาทวิชาให้กับผู้วิจัยมาจนถึงปัจจุบัน

ธีระพล ภูมิสัตธรรม

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญ



	หน้า
บทคัดย่อภาษาไทย.....	ง
บทคัดย่อภาษาอังกฤษ.....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญตาราง.....	ช
สารบัญภาพ.....	ฅ
บทที่	
1. บทนำ.....	1
2. แนวคิดและทฤษฎีที่เกี่ยวข้อง.....	5
3. การออกแบบและพัฒนา.....	28
4. การทดสอบระบบงาน.....	45
5. สรุปการวิจัยและข้อเสนอแนะ.....	47
รายการอ้างอิง.....	50
ภาคผนวก	
ก. การใช้งานโปรแกรม.....	53
ข. ตัวอย่างของแพคเกจที่ผ่านในระบบเครือข่าย.....	58
ประวัติผู้เขียน.....	70

สารบัญตาราง

	หน้า
ตารางที่ 2.1 คำสั่งของโปรโตคอลเทลเน็ต.....	8
ตารางที่ 2.2 ลักษณะการเจรจาทางเลือก.....	9
ตารางที่ 2.3 อาร์เอฟซีต่างๆ ที่อธิบายรายละเอียดของแต่ละทางเลือก.....	10
ตารางที่ 2.4 การเข้ารหัสด้วยคีย์กลุ่มย่อย และการถอดรหัสด้วยคีย์กลุ่มย่อยของ IDEA....	25
ตารางที่ 5.1 เปรียบเทียบขนาดของโปรแกรมเทลเน็ตเดิมกับโปรแกรมใหม่.....	49



ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญภาพ

	หน้า
รูปที่ 2.1 แสดงการทำงานของโปรโตคอลเทลเน็ต.....	6
รูปที่ 2.2 แสดงไฟไนต์สเตตเมชีนของโปรโตคอลเทลเน็ต.....	12
รูปที่ 2.3 แสดงไฟไนต์สเตตเมชีนของเทลเน็ตผู้ให้บริการ.....	13
รูปที่ 2.4 แสดงไฟไนต์สเตตเมชีนของเทลเน็ตผู้ให้บริการ.....	13
รูปที่ 2.5 แสดงการเข้ารหัสข้อมูลก่อนส่งผ่านระบบเครือข่าย.....	15
รูปที่ 2.6 แสดงการเข้ารหัสข้อมูลจากต้นทางถึงปลายทาง.....	17
รูปที่ 2.7 แสดงการเข้ารหัสข้อมูลระหว่างจุดเชื่อมโยง.....	18
รูปที่ 2.8 แสดงการเข้ารหัส และถอดรหัสข้อมูล.....	19
รูปที่ 2.9 แสดงลักษณะการทำงานของ IDEA.....	23
รูปที่ 3.1 แสดงการทำงานของโปรแกรมเทลเน็ตที่มีระบบการเข้ารหัส.....	29
รูปที่ 3.2 แสดงการเจรจาทางเลือกสำหรับการเข้ารหัสข้อมูล และการแลกเปลี่ยน เซสชันคีย์.....	33
รูปที่ 3.3 แสดงไฟไนต์สเตตเมชีนของการเจรจาทางเลือกสำหรับการเข้ารหัสข้อมูล.....	36
รูปที่ 3.4 แสดงไฟไนต์สเตตเมชีนของการเจรจาทางเลือกในส่วนย่อย.....	37
รูปที่ 3.5 แสดงลำดับขั้นตอนการทำงานของโปรแกรมเทลเน็ตผู้ให้บริการ.....	38
รูปที่ 3.6 แสดงลำดับขั้นตอนการทำงานของโปรแกรมเทลเน็ตผู้ให้บริการ.....	39
รูปที่ 3.7 แสดงการทำงานของโปรแกรมเทลเน็ตผู้ให้บริการที่มีการเข้ารหัสข้อมูล....	40
รูปที่ 3.8 แสดงการทำงานของโปรแกรมเทลเน็ตผู้ให้บริการที่มีการเข้ารหัสข้อมูล.....	40
รูปที่ 3.9 แสดงรูปแบบข้อมูลของการส่งคีย์สาธารณะ.....	41
รูปที่ 3.10 แสดงการเข้ารหัสเซสชันคีย์.....	42
รูปที่ 3.11 แสดงรูปแบบข้อมูลของการส่งเซสชันคีย์ที่ถูกเข้ารหัส.....	42
รูปที่ 3.12 แสดงการเข้ารหัสข้อมูลของ IDEA.....	43
รูปที่ 3.13 แสดงการเพิ่มข้อมูลส่วนหัว และการแพคคิงข้อมูลสู่กรอบบล็อก.....	44
รูปที่ 5.1 แสดงรูปแบบข้อมูลเปรียบเทียบระหว่างการส่งผ่านข้อมูลปกติ และข้อมูล ที่เข้ารหัสตามโปรโตคอลทีซีพีไอพี.....	48