การพัฒนาระบบความมั่นคงของเทลเน็ตโดยอาศัยระบบการเข้ารหัสลับ

นายธีระพล ภูมิสัทธรรม

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
พ.ศ. 2539

ISBN 974-633-481-6

DEVELOPMENT OF TELNET AUTHENTICATION WITH CRYPTO SYSTEM

Mr. Theerapon Pumsattham

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	การพัฒนาระบบความมั่นคงของเทลเน็ตโดยอาศัยระบบการเข้ารหัสลับ
โดย	นายธีระพล ภูมิสัทธรรม
ภาควิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ยรรยง เต็งอำนวย

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ สมชาย ทยานยง)

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

.....กรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. สาธิต วงศ์ประทีป)

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสีเขียวนี้เพียงแผ่นเดียว

ธีระพล ภูมิสัทธรรม : การพัฒนาระบบความมั่นคงของเทลเน็ตโดยอาศัยระบบการเข้ารหัสลับ (DEVELOPMENT OF TELNET AUTHENTICATION WITH CRYPTO SYSTEM) อ.ที่ปรึกษา : อ. ดร. ยรรยง เต็งอำนวย, 70 หน้า. ISBN 974-633-481-6

จุดมุ่งหมายของการวิจัยคือ การพัฒนาระบบการเข้ารหัสข้อมูลสำหรับโปรโตคอลเทลเน็ต เพื่อสร้างช่องทางการสื่อสารที่ปลอดภัย ในการใช้งานระยะไกลจากเครื่องคอมพิวเตอร์ส่วนบุคคลไปยังเครื่องคอมพิวเตอร์ระบบยูนิกซ์ โดยการแก้ไขโปรแกรมต้นฉบับของโปรแกรมเทลเน็ตผู้ขอรับบริการที่ทำงานบนระบบปฏิบัติการดอส และโปรแกรมเทลเน็ตผู้ให้บริการที่ทำงานบนระบบปฏิบัติการยูนิกซ์ และกระบวนการเข้ารหัสข้อมูลที่ใช้เป็นแบบบล็อคไซเฟอร์

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

ผลการทดสอบพบว่า สามารถเข้ารหัสข้อมูลที่ส่งผ่านระหว่างโปรแกรมเทลเน็ตผู้ขอรับบริการและโปรแกรมเทลเน็ตผู้ให้บริการในลักษณะบล็อคไซเฟอร์ ป้องกันการลอบดักข้อมูลจากโปรแกรมที่ทำหน้าที่ดักข้อมูลในระบบเครือข่ายอีเทอร์เน็ตได้ และโปรแกรมเทลเน็ตผู้ให้บริการสามารถทำงานบนระบบปฏิบัติการยูนิกซ์แบบต่างๆ ได้

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....
ปีการศึกษา 2538 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.

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2538 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงได้ โดยได้รับความช่วยเหลือจากอาจารย์ที่ปรึกษาวิทยานิพนธ์ อาจารย์ ดร. ยรรยง เต็งอำนวย ได้ให้คำแนะนำในการทำวิจัยมาโดยตลอด ขอขอบคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ให้ทุนอุดหนุนการศึกษาและการทำวิจัย ขอขอบคุณ คุณไพโรจน์ ต้นศิริอนุสรณ์ ที่ได้ให้คำแนะนำ รวมทั้งขอขอบคุณเพื่อนทุกคนที่เป็นกำลังใจ และให้คำแนะนำโดยตลอด

สุดท้ายนี้ผู้วิจัยขอกราบขอบพระคุณบิดา มารดา และพี่ทุกคน ที่สนับสนุนและเป็นกำลังใจตลอดมา รวมทั้งครูและอาจารย์ทั้งหลายที่ได้เคยประสิทธิประสาทวิชาให้กับผู้วิจัยมาจนถึงปัจจุบัน

ธีระพล ภูมิสัทธรรม

สารบัญ

สารบัญตาราง

สารบัญภาพ