การเพิ่มความมั่นคงให้แก่ระบบรหัสผ่านแบบใช้ครั้งเดียวด้วยเทคนิคการเข้ารหัส

นาย อนุชาติ ทัศนวิบูลย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2541

ISBN 974-331-476-8

SECURITY IMPROVEMENT FOR THE ONE-TIME PASSWORD SYSTEM USING CRYPTOGRAPHY

MR. ANUCHART TASSANAVIBOON

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Computer Science

Department of Computer Engineering

Graduate School

Chulalongkorn University

Academic Year 1998

ISBN 974-331-476-8

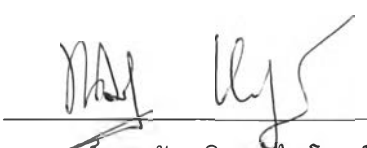
หัวข้อวิทยานิพนธ์	การเพิ่มความมั่นคงให้แก่ระบบรหัสผ่านแบบใช้ครั้งเดียวด้วยเทคนิคการเข้ารหัส
โดย	นาย อนุชาติ ทัศนวิบูลย์
ภาควิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ยรรยง เต็งอำนวย

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

คณบดีบัณฑิตวิทยาลัย

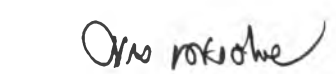
(ศาสตราจารย์ นายแพทย์ ศุภวัฒน์ ชุติวงศ์)

คณะกรรมการสอบวิทยานิพนธ์



ประธานกรรมการ

(อาจารย์ ดร.ณัฐวุฒิ หนูไพโรจน์)

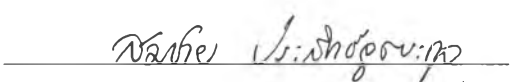


อาจารย์ที่ปรึกษา

(อาจารย์ ดร.ยรรยง เต็งอำนวย)

กรรมการ

(อาจารย์จารุมาตร ปิ่นทอง)



กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สมชาย ประสิทธิ์จูตระกูล)

อนุชาติ ทัศนวิบูลย์ : การเพิ่มความมั่นคงให้แก่ระบบรหัสผ่านแบบใช้ครั้งเดียวด้วยเทคนิคการเข้ารหัส (SECURITY IMPROVEMENT FOR THE ONE-TIME PASSWORD SYSTEM USING CRYPTOGRAPHY) อ. ที่ปรึกษา : อ. ดร. ยรรยง เต็งอำนวย, 120 หน้า. ISBN 974-331-476-8.

การใช้รหัสผ่านในการควบคุมการเข้าถึงคอมพิวเตอร์ เป็นวิธีที่ถูกใช้งานอย่างแพร่หลายมากที่สุด ถึงแม้ว่าจะมีข้อบกพร่องบางประการ เช่น การถูกดักฟังทางเครือข่าย การปลอมตัว และการคาดเดารหัสผ่าน แต่สามารถแก้ไขได้โดยการใช้รหัสผ่านแบบใช้ครั้งเดียว รวมถึงการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่าย การพิสูจน์ตัวจริงของเครื่องให้บริการและเครื่องขอใช้บริการด้วยวิธีการเข้ารหัส เป็นต้น

การวิจัยนี้เป็นการนำเอาเทคนิคการเข้ารหัสมาใช้เสริมความมั่นคงให้กับระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียวของนายพิษณุ เกริกอำไพสุรกิจ โดยการนำเอาเทคนิคการเข้ารหัสแบบคีย์ลับเฉพาะมาใช้ในการเข้ารหัสข้อมูล และเทคนิคการเข้ารหัสแบบคีย์สาธารณะมาใช้ในการพิสูจน์ตัวจริงของเครื่อง ผลจากการวิจัยทำให้สามารถเพิ่มความมั่นคงให้กับระบบรหัสผ่านแบบใช้ครั้งเดียว

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2541 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

C818504 : MAJOR COMPUTER SCIENCE
KEY WORD: SECURITY / ENCRYPTION / CRYPTOGRAPHY / PASSWORD
ANUCHART TASSANAVIBOON : SECURITY IMPROVEMENT FOR THE ONE-TIME PASSWORD SYSTEM USING CRYPTOGRAPHY. THESIS ADVISOR : YUNYONG TENG-AMNUAY. Ph.D. 120 pp. ISBN 974-331-476-8.

Access control using password code is a popular method to verify a computer user. However, the method contains several security weaknesses such as password eavesdropping, network spoofing and off-line password guessing. Certain techniques; such as one-time password, encrypted communication channel and end-computer authentication using cryptography; are proposed to improve the security weakness of the method.

In this thesis, an encryption technique is employed to enhance the access control security for the one-time password method proposed by Mr. Pitsanu Kertumpaisurakit. The proposed technique uses secret key to encrypt data and public key to authenticate end-computers. The results show that the security of the one-time-use password method was improved.

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา .....
ปีการศึกษา 2541 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม .....

กิตติกรรมประกาศ

การทำวิทยานิพนธ์ฉบับนี้สามารถสำเร็จลุล่วงได้ด้วยดีนั้น ผู้วิจัยขอขอบพระคุณ ท่านอาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้ให้คำแนะนำและข้อคิดเห็นในการทำวิจัยมาด้วยดีโดยตลอด จนวิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ ขอขอบพระคุณ คณาจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่านที่ได้มีส่วนให้ความรู้กับผู้วิจัยเพื่อนำมาใช้ประกอบการทำวิจัย

ท้ายนี้ขอขอบคุณ คุณสกล ลาภอำนวยผล คุณวัลลภ แซ่เจีย คุณรักชนก แย้มนันท์ และเพื่อนนิสิตปริญญาโท ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน ที่มีส่วนให้ข้อเสนอแนะและให้กำลังใจแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง
บทคัดย่อภาษาอังกฤษ ..... จ
กิตติกรรมประกาศ ..... ฉ
สารบัญ ..... ช
สารบัญตาราง ..... ฌ
สารบัญรูป ..... ญ

บทที่ 1 บทนำ 1
1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ 2
1.3 ขอบเขตของการวิจัย 2
1.4 ขั้นตอนและวิธีการดำเนินการวิจัย 3
1.5 ประโยชน์ที่คาดว่าจะได้รับ 3

บทที่ 2 แนวคิดและทฤษฎีที่เกี่ยวข้อง 4
2.1 เทคนิคการเข้ารหัส 4
2.2 การพิสูจน์ตัวจริงโดยใช้เทคนิคการเข้ารหัส 7
2.3 การแลกเปลี่ยนคีย์ 10
2.4 ระบบรหัสผ่านแบบใช้ครั้งเดียว 10
2.5 โพรโทคอล เอสเอสแอล 12

บทที่ 3 การออกแบบระบบ 21
3.1 หลักการทำงานของระบบ 21
3.2 องค์ประกอบของระบบ 22
3.3 ลำดับการทำงานของระบบ 23
3.4 โครงสร้างและลำดับการทำงานของโปรแกรม 26

3.5 ลำดับการทำงานของโพรโทคอล 40
3.6 รูปแบบของกลุ่มข้อมูล 44
3.7 สถานะการทำงานของระบบ 46
3.8 โครงสร้างฐานข้อมูลของระบบ 47

บทที่ 4 การพัฒนาระบบ 53
4.1 หลักการพัฒนาโปรแกรม 53
4.2 เครื่องมือพัฒนาระบบ 56

บทที่ 5 การทดสอบโปรแกรม 80
5.1 อุปกรณ์ที่ใช้ในการทดสอบ 80
5.2 ขั้นตอนการติดตั้งระบบเพื่อการทดสอบ 81
5.3 ขั้นตอนการทดสอบระบบ 88
5.4 ผลการทดสอบระบบ 89

บทที่ 6 สรุปผลการวิจัยและข้อเสนอแนะ 101
6.1 สรุปผลการวิจัย 101
6.2 ข้อจำกัดและปัญหาที่พบจากการวิจัย 103
6.3 ข้อเสนอแนะ 104

รายการอ้างอิง 107

ภาคผนวก ก. 108

ภาคผนวก ข. 114

ประวัติผู้วิจัย 120

สารบัญตาราง

หน้า

ตารางที่ 3.1 รายละเอียดประเภทต่างๆ ของกลุ่มข้อมูล 44
ตารางที่ 3.2 ความหมายของบิทต่างๆ ในรหัสแสดงผลลัพธ์ 45
ตารางที่ 3.3 ตารางข้อมูลผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว 48
ตารางที่ 3.4 ตารางข้อมูลรหัสผ่านแบบใช้ครั้งเดียว 50
ตารางที่ 3.5 ตารางข้อมูลเครื่องที่ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว 50
ตารางที่ 6.1 แสดงความแตกต่างระหว่างระบบรหัสผ่านของเก่ากับของใหม่ 102

สารบัญรูป

หน้า

รูปที่ 2.1 แสดงการทำงานของการเข้ารหัสและการถอดรหัส 4
รูปที่ 2.2 แสดงการทำงานของการเข้ารหัสและการถอดรหัสแบบใช้คีย์ลับเฉพาะ 5
รูปที่ 2.3 แสดงการทำงานของการเข้ารหัสด้วยคีย์สาธารณะและ
ทำการถอดรหัสด้วยคีย์ส่วนตัว 6
รูปที่ 2.4 แสดงการทำงานของการเข้ารหัสด้วยคีย์ส่วนตัวและ
ทำการถอดรหัสด้วยคีย์สาธารณะ 7
รูปที่ 2.5 แสดงโพรโทคอลที่ใช้ในการพิสูจน์ตัวจริงชนิดทางเดียว
ด้วยเทคนิคการเข้ารหัสแบบใช้คีย์สาธารณ 8
รูปที่ 2.6 แสดงโพรโทคอลที่ใช้ในการพิสูจน์ตัวจริงชนิดสองทาง
ด้วยเทคนิคการเข้ารหัสแบบใช้คีย์สาธารณะ 9
รูปที่ 2.7 แผนผังแสดงการทำงานของระบบรหัสผ่านแบบใช้ครั้งเดียว 10
รูปที่ 2.8 แสดงการทำงานของโพรโทคอลที่ใช้ในระบบรหัสผ่านแบบใช้ครั้งเดียว
ที่ปรับปรุงด้วยเทคนิคการเข้ารหัส 11
รูปที่ 2.9 แสดงหลักการทำงานของโพรโทคอล เอสเอสแอล 13
รูปที่ 2.10 แสดงลำดับการทำงานของการพิสูจน์ตัวจริงของผู้ให้บริการ 17
รูปที่ 2.11 แสดงลำดับการทำงานของการพิสูจน์ตัวจริงของผู้ขอใช้บริการ 19
รูปที่ 3.1 แสดงระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียว
ที่เสริมความปลอดภัยด้วยชั้นโพรโทคอล เอสเอสแอล 22
รูปที่ 3.2 แสดงลำดับการทำงานของระบบรหัสผานแบบใช้ครั้งเดียว 24
รูปที่ 3.3 โครงสร้างส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว 27
รูปที่ 3.4 โครงสร้างของโปรแกรมให้บริการตรวจสอบรหัสผ่าน 28
รูปที่ 3.5 ผังงานแสดงการทำงานของโปรแกรมให้บริการตรวจสอบรหัสผ่าน 29
รูปที่ 3.6 โครงสร้างโปรแกรมบำรุงรักษาฐานข้อมูลระบบรหัสผ่าน 30
รูปที่ 3.7 ผังงานแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลบัญชีผู้ใช้ 31
รูปที่ 3.8 ผังแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลรหัสผ่านของผู้ใช้ 32
รูปที่ 3.9 ผังงานแสดงการทำงานของโปรแกรมปรับปรุงข้อมูลเครื่องขอใช้บริการ 33

รูปที่ 3.10 โครงสร้างส่วนขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว 34
รูปที่ 3.11 โครงสร้างโปรแกรมตรวจสอบประเภทของผู้ใช้ 35
รูปที่ 3.12 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบประเภทของผู้ใช้ 36
รูปที่ 3.13 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบรหัสผ่านแบบยูนิกซ์ 37
รูปที่ 3.14 โครงสร้างโปรแกรมตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว 37
รูปที่ 3.15 ผังงานแสดงการทำงานของโปรแกรมตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว 38
รูปที่ 3.16 ผังงานแสดงการทำงานของโปรแกรมจัดสภาพแวดล้อม
การใช้งานสำหรับผู้ใช้ยูนิกซ์ 39
รูปที่ 3.17 แสดงลำดับการทำงานในระยะแนะนำตัว 40
รูปที่ 3.18 แสดงลำดับการทำงานในระยะตรวจสอบรหัสผ่าน 41
รูปที่ 3.19 แสดงลำดับการทำงานในระยะปิดการติดต่อ 42
รูปที่ 3.20 แสดงลำดับการทำงานของโพรโทคอลชั้นการสื่อสารประยุกต์
เพื่อการบริการรหัสผ่านแบบใช้ครั้งเดียว 43
รูปที่ 3.21 รูปแบบของกลุ่มข้อมูล 44
รูปที่ 3.22 รูปแบบรหัสแสดงผลลัพธ์การทำงาน 45
รูปที่ 3.23 ผังสถานะการทำงานของผู้ให้บริการและผู้ขอใช้บริการ 46
รูปที่ 3.24 รูปแบบรหัสของเขตข้อมูล flag 48
รูปที่ 3.25 แผนผังแสดงความสัมพันธ์ของเอนทิตี 51
รูปที่ 4.1 ลำดับชั้นการสื่อสารของผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว 54
รูปที่ 4.2 สถาปัตยกรรมของส่วนให้บริการรหัสผ่านแบบใช้ครั้งเดียว 54
รูปที่ 4.3 แสดงลำดับชั้นการสื่อสารและความสัมพันธ์ของทั้งผู้ให้บริการและผู้ขอใช้บริการ . 55
รูปที่ 4.4 สถาปัตยกรรมของโปรแกรมทั้งหมดที่ทำงานอยู่ภายใน
เครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว 56
รูปที่ 5.1 ใบรับรองของผู้ออกใบรับรอง 82
รูปที่ 5.2 คีย์ส่วนตัวของผู้ออกใบรับรอง 82
รูปที่ 5.3 คีย์ส่วนตัวของผู้ให้บริการรหัสผ่าน 83
รูปที่ 5.4 ใบรับรองของผู้ให้บริการที่ถูกออกโดยผู้ออกใบรับรอง 85
รูปที่ 5.5 แสดงการเริ่มดำเนินงานของโปรแกรมจัดการฐานข้อมูล 86
รูปที่ 5.6 หน้าจอที่ใช้ในการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์ 87

รูปที่ 5.7 หน้าจอที่ใช้ในการเพิ่มบัญชีผู้ใช้เข้าสู่ระบบรหัสผ่านแบบใช้ครั้งเดียว 87
รูปที่ 5.8 แสดงการเริ่มดำเนินงานของโปรแกรมให้บริการรหัสผ่าน 88
รูปที่ 5.9 แสดงการล็อกอินของผู้ใช้ประเภทที่ใช้รหัสผ่านแบบยูนิกซ์ 89
รูปที่ 5.10 แสดงการล็อกอินของผู้ใช้ประเภทรหัสผ่านแบบใช้ครั้งเดียว
และคีย์รหัสผ่านถูกต้อง 90
รูปที่ 5.11 แสดงการทำงานของ OTP Server กรณีที่มีการขอตรวจสอบรหัสผ่าน
และรหัสผ่านถูกต้อง 91
รูปที่ 5.12 แสดงการล็อกอินเมื่อคีย์รหัสผ่านผิด 91
รูปที่ 5.13 แสดงการทำงานของ OTP Server กรณีที่มีผู้ใช้คีย์รหัสผ่านผิด 92
รูปที่ 5.14 แสดงการล็อกอินของผู้ใช้ที่ถูกสั่งระงับการใช้ 92
รูปที่ 5.15 แสดงการทำงานของ OTP Server กรณีบัญชีผู้ใช้ถูกระงับการใช้ 93
รูปที่ 5.16 แสดงการล็อกอินของผู้ใช้กรณีบัญชีผู้ใช้หมดอายุการใช้ 93
รูปที่ 5.17 แสดงการทำงานของ OTP Server กรณีที่บัญชีผู้ใช้หมดอายุ 94
รูปที่ 5.18 แสดงการเตือนให้ผู้ใช้ทราบว่าจำนวนรหัสผ่านใกล้หมด 94
รูปที่ 5.19 แสดงการทำงานของ OTP Server เมื่อจำนวนรหัสผ่านของผู้ใช้ใกล้หมด 95
รูปที่ 5.20 แสดงการเตือนให้ผู้ใช้ทราบว่าบัญชีผู้ใช้ใกล้หมดอายุ 95
รูปที่ 5.21 แสดงการทำงานของ OTP Server เมื่อบัญชีผู้ใช้ใกล้หมดอายุ 96
รูปที่ 5.22 แสดงการทำงานของ OTP Server ในการตรวจจับผู้ใช้บริการที่ไม่ได้ลงทะเบียน 96
รูปที่ 5.23 แสดงการถูกปิดการติดต่อเนื่องจากเครื่องแม่ข่ายยูนิกซ์ไม่ได้ลงทะเบียน 97
รูปที่ 5.24 แสดงการทำงานของ OTP Client ในการตรวจสอบใบรับรองพบว่า
ไม่ใช่ของผู้ให้บริการตัวจริง 97
รูปที่ 5.25 แสดงการทำงานของ OTP Client ในการตรวจสอบใบรับรอง
พบว่าออกโดยผู้รับรองที่ไม่น่าเชื่อถือ 98
รูปที่ 5.26 แสดงการส่งข้อความ “Hello World” ของโปรแกรม cli 99
รูปที่ 5.27 แสดงการรับข้อความ “Hello World” ของโปรแกรม serv-1 99
รูปที่ 5.28 แสดงการรับข้อความ “Hello World” ของโปรแกรม serv-2 100
รูปที่ 6.1 แผนผังแสดงความสัมพันธ์ระหว่างเครื่องและกลุ่มเครื่อง 104
รูปที่ 6.2 แผนผังแสดงความสัมพันธ์ระหว่างเครื่องและกลุ่มเครื่อง
เมื่อปรับให้เหมาะกับฐานข้อมูลสัมพันธ์ 105

รูปที่ 6.3 แสดงการทำงานร่วมกันระหว่างระบบรหัสผ่านแบบใช้ครั้งเดียว
และระบบให้บริการไดเรกทรอรี 106
รูปที่ ก.1 ค่าเริ่มต้นของโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียว 111
รูปที่ ก.2 ค่าเริ่มต้นของโปรแกรมขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว 113
รูปที่ ข.1 หน้าต่างหลักของโปรแกรมบำรุงรักษาฐานข้อมูลรหัสผ่าน 114
รูปที่ ข.2 หน้าต่างการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์ 115
รูปที่ ข.3 หน้าต่างการเพิ่มเครื่องแม่ข่ายยูนิกซ์ 115
รูปที่ ข.4 หน้าต่างการแก้ไขเครื่องแม่ข่ายยูนิกซ์ 116
รูปที่ ข.5 หน้าต่างการจัดการข้อมูลบัญชีผู้ใช้ 117
รูปที่ ข.6 หน้าต่างการเพิ่มข้อมูลบัญชีผู้ใช้ 117
รูปที่ ข.7 หน้าต่างการแก้ไขข้อมูลบัญชีผู้ใช้ 118
รูปที่ ข.8 หน้าต่างการจัดการข้อมูลรหัสผ่าน 119
รูปที่ ข.9 หน้าต่างการพิมพ์ใบรายงานรหัสผ่าน 119