

การปรับปรุงความสามารถระบบรหัสผ่านแบบใช้ครั้งเดียว
ให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง

นายจักรกฤษณ์ นันทพนิต



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตรคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2541

ISBN 974-331-486-5

ลิขสิทธิ์ของบัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย

IMPROVEMENT OF ONE-TIME PASSWORD SYSTEM
FOR USERS ON MULTIPLE SERVERS

MR. JUGKRIT NUNTAPINIT

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

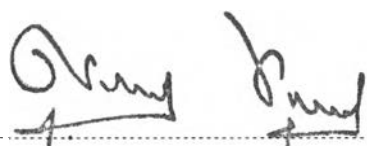
Academic Year 1998

ISBN 974-331-486-5

หัวข้อวิทยานิพนธ์ การปรับปรุงความสามารถระบบรหัสผ่านแบบใช้ครั้งเดียวให้ครอบคลุมผู้ใช้
เซิร์ฟเวอร์หลายเครื่อง

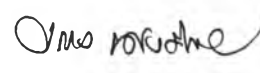
โดย นายจักรกฤษณ์ นันทพินิต
ภาควิชา วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา อาจารย์ ดร. ยรรยง เต็งอำนาจ

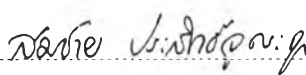
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่ง
ของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

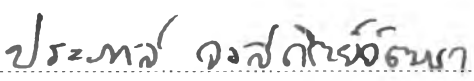

..... คณบดีบัณฑิตวิทยาลัย
(ศาสตราจารย์ นายแพทย์ ศุภวัฒน์ ชูติวงศ์)

คณะกรรมการสอบวิทยานิพนธ์


..... ประธานกรรมการ
(อาจารย์ จารุมাত্র ปิ่นทอง)


..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร. ยรรยง เต็งอำนาจ)


..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. สมชาย ประสิทธิ์จตุระกุล)


..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ประภาส จงสถิตย์วัฒนา)

จักรกฤษณ์ นันทพินิต : การปรับปรุงความสามารถระบบรหัสผ่านแบบใช้ครั้งเดียวให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง (IMPROVEMENT OF ONE-TIME PASSWORD SYSTEM FOR USERS ON MULTIPLE SERVERS) อาจารย์ที่ปรึกษา : อาจารย์ ดร. ยรรยง เต็งอำนาจ, 49 หน้า. ISBN 974-331-486-5

การพัฒนาระบบการให้บริการรหัสผ่านแบบใช้ครั้งเดียวสำหรับระบบยูนิกซ์ เป็นแนวทางหนึ่งที่ถูกพัฒนาขึ้นมาเพื่อเสริมความปลอดภัยให้กับระบบคอมพิวเตอร์ที่ใช้รหัสผ่านเพื่อการพิสูจน์ตัวตน โดยการเปลี่ยนรหัสผ่านทุกครั้งหลังจากผลการพิสูจน์ตัวตนถูกต้อง ซึ่งสามารถลดปัญหาที่เกิดจากการขโมยรหัสผ่านเพื่อนำกลับไปใช้ได้

วิทยานิพนธ์ฉบับนี้จัดทำขึ้นโดย การศึกษางานวิจัย ปัญหา ข้อจำกัด สรุปผลการวิจัยและข้อเสนอแนะจากระบบเดิม รวมทั้งทฤษฎีต่าง ๆ ที่เกี่ยวข้อง เพื่อปรับปรุงความสามารถระบบรหัสผ่านแบบใช้ครั้งเดียวให้ครอบคลุมผู้ใช้เซิร์ฟเวอร์หลายเครื่อง รวมถึงการขยายเพื่อรองรับพัฒนาการของระบบรหัสผ่านแบบใช้ครั้งเดียวต่อไปในอนาคต

ภาควิชา วิศวกรรมคอมพิวเตอร์
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์
ปีการศึกษา 2541

ลายมือชื่อนิติ
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

พิมพ์ต้นฉบับบทคัดย่อวิทยานิพนธ์ภายในกรอบสี่เหลี่ยมนี้เพียงแผ่นเดียว

C818586 : MAJOR COMPUTER SCIENCE

KEY WORD: ONE TIME PASSWORD / PASSWORD / LOGIN / SECURITY

JUGKRIT NUNTAPINIT : IMPROVEMENT OF ONE-TIME PASSWORD SYSTEM

FOR USERS ON MULTIPLE SERVERS. THESIS ADVISOR :

YUNYONG TENG-AMNUAY, PH.D. 49 pp. ISBN 974-331-486-5

Development of a PC-based one-time password service system for UNIX system is to supplement security to a computer system. The computer system will use a password for authentication and will change password every time after a user correctly identifying himself. With this method, it will reduce a problem of larceny of password.

This thesis studies the previous work and related theories and aims to improve a one-time password system for users on multiple servers including the development of a one-time password system in the future.

ภาควิชา.....วิศวกรรมคอมพิวเตอร์.....

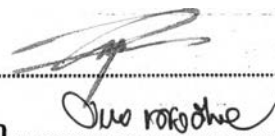
สาขาวิชา.....วิทยาศาสตร์คอมพิวเตอร์.....

ปีการศึกษา..... 2541.....

ลายมือชื่อนิสิต.....

ลายมือชื่ออาจารย์ที่ปรึกษา.....

ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....



กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลือของอาจารย์ ดร. ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำและข้อคิดเห็นต่าง ๆ ในการวิจัยมาด้วยดี ตลอด และเนื่องจากทุนการวิจัยครั้งนี้บางส่วนได้รับมาจากทุนอุดหนุนการวิจัยของบัณฑิตวิทยาลัย จึงขอขอบพระคุณบัณฑิตวิทยาลัยมา ณ ที่นี้ด้วย

ท้ายนี้ ผู้วิจัยใคร่ขอกราบขอบพระคุณ บิดาและมารดา ซึ่งสนับสนุนและให้กำลังใจแก่ผู้วิจัย เสมอมาจนสำเร็จการศึกษา



สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	ง
บทคัดย่อภาษาอังกฤษ.....	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญ.....	ช
สารบัญตาราง.....	ซ
สารบัญรูป.....	ณ
บทที่ 1 บทนำ	
ความเป็นมาและความสำคัญของปัญหา.....	1
วัตถุประสงค์ของการวิจัย.....	1
ขอบเขตของวิทยานิพนธ์.....	1
ขั้นตอนและวิธีการดำเนินงาน.....	2
ประโยชน์ที่คาดว่าจะได้รับ.....	2
บทที่ 2 แนวคิดและทฤษฎีที่เกี่ยวข้อง	
ระบบรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ.....	3
วิทยาการเข้ารหัสลับ.....	7
บทที่ 3 การวิเคราะห์และออกแบบระบบ	
ข้อจำกัดของระบบเดิม.....	11
การแก้ไขข้อจำกัดและปรับปรุงเพิ่มเติม.....	15
รูปแบบกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร.....	25
สรุปผลการวิเคราะห์และออกแบบระบบ.....	26
บทที่ 4 การพัฒนาโปรแกรม	
การพัฒนาส่วนขอใช้บริการรหัสผ่าน.....	28
การพัฒนาส่วนให้บริการรหัสผ่าน.....	32

บทที่ 5	การทดสอบโปรแกรม	
	ขั้นตอนการติดตั้งโปรแกรม	37
	สภาวะที่ใช้ทดสอบโปรแกรม.....	37
	เงื่อนไขที่ใช้ทดสอบ	39
	ผลการทดสอบ.....	40
บทที่ 6	สรุปผลการวิจัยและข้อเสนอแนะ	
	สรุปผลการวิจัย.....	41
	ปัญหาและข้อจำกัดที่พบจากการวิจัย	41
	ข้อเสนอแนะ.....	42
	รายการอ้างอิง	43
	ภาคผนวก.....	44
	ประวัติผู้เขียน.....	49

สารบัญตาราง

ตารางที่	หน้า
2.1	แสดงถึงรูปแบบของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร 6
2.2	แสดงข้อมูลที่เกี่ยวข้อง..... 6
2.3	แสดงชนิดของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสาร 7
3.1	แสดงชื่อลงบันทึกเข้าใช้และชื่อบัญชีผู้ใช้ในระบบของคุณพิษณุ 13
3.2	แสดงชื่อลงบันทึกเข้าใช้แต่ละเซิร์ฟเวอร์กับชื่อบัญชีผู้ใช้ 16
3.3	รูปแบบของข้อมูลที่ใช้กำหนดชื่อบัญชีผู้ใช้บนเครื่องให้บริการรหัสผ่าน 17
3.4	รูปแบบของข้อมูลที่ใช้เพื่อระบุชนิดของอัลกอริทึม..... 18
3.5	รูปแบบของข้อมูลที่ใช้เพื่อระบุชนิดของการเข้ารหัส 18
3.6	รูปแบบของข้อมูลที่ใช้เพื่อบอกประเภทของคำร้องขอและการตอบกลับ 19
3.7	รูปแบบของข้อมูลที่ใช้เพื่อบอกรุ่นควบคุม..... 21
3.8	รูปแบบของข้อมูลที่ใช้รองรับข้อมูลที่สอดคล้องกับวัตถุประสงค์ 21
3.9	รูปแบบของกลุ่มข้อมูลที่ใช้ในการติดต่อสื่อสารที่ได้รับการปรับปรุง..... 25
3.10	แสดงการเปรียบเทียบระบบก่อนและหลังปรับปรุง 26
4.1	แสดงรูปแบบของแฟ้มข้อมูลการกำหนดบัญชีผู้ใช้ระบบ 36
ก.1	รูปแบบของแฟ้มข้อมูล otpacct..... 46
ก.2	รูปแบบของแฟ้มข้อมูล userinfo..... 47
ก.3	รูปแบบของแฟ้มข้อมูลรหัสผ่าน 48

สารบัญรูป

รูปที่		หน้า
2.1	แผนภูมิการทำงานของระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียว.....	4
2.2	แสดงขั้นตอนการทำงานของโปรแกรมล็อกอินในระบบของคุณพิษณุ.....	5
2.3	การเข้ารหัสข้อมูล	7
2.4	การเข้ารหัสโดยใช้คีย์ส่วนตัว.....	9
2.5	การเข้ารหัสโดยใช้คีย์สาธารณะ	9
2.6	การถอดรหัสโดยใช้คีย์สาธารณะ.....	10
3.1	ความสัมพันธ์ของส่วนที่เกี่ยวข้องในระบบของคุณพิษณุ.....	12
3.2	แสดงประกอบตัวอย่างชื่อลงบันทึกเข้าใช้บนแต่ละเซิร์ฟเวอร์	12
3.3	ขั้นตอนการสื่อสารในระบบของคุณพิษณุ	15
3.4	ความสัมพันธ์ระหว่างผู้ใช้ ชื่อลงบันทึกเข้าใช้ และเซิร์ฟเวอร์	15
3.5	ความสัมพันธ์ระหว่างชื่อลงบันทึกเข้าใช้ของแต่ละเซิร์ฟเวอร์กับชื่อบัญชีผู้ใช้	16
3.6	ขั้นตอนการสื่อสารในระบบของคุณพิษณุที่ได้รับการปรับปรุง	19
3.7	ขั้นตอนการทำงานของกระบบรหัสผ่านแบบใช้ครั้งเดียวบนระบบเน็ตเวิร์ก.....	23
4.1	ระบบให้บริการรหัสผ่านแบบใช้ครั้งเดียวของคุณพิษณุ.....	27
4.2	ขั้นตอนการทำงานบางส่วนของโปรแกรมล็อกอินที่ได้รับการปรับปรุง	29
4.3	ขั้นตอนการทำงานของส่วนให้บริการตรวจสอบรหัสผ่านที่ได้รับการปรับปรุง	33
4.4	แสดงรายละเอียดขั้นตอนการขอหมายเลขลำดับรหัสผ่านปัจจุบัน	34
5.1	แสดงเครื่องที่ใช้ในการทดสอบระบบ	38