บทที่ 7

สรุปผลการวิจัยและข้อเสนอแนะ

จากผลการวิจัย การทดสอบและการทดลองใช้จริง สามารถสรุปผลการวิจัย ปัญหาต่าง ๆ และข้อเสนอแนะดังนี้

สรุปผลการวิจัย

1. การพัฒนาโปรแกรมล็อกอินสำหรับระบบการให้บริการรหัสผ่านแบบใช้ครั้งเดียวได้ยึดหลักความเข้ากันได้ (compatible) กับโปรแกรมล็อกอินแบบเดิม ดังนั้นรูปแบบการขอเข้าใช้ระบบยังคงรูปแบบเดิม

2. ผู้ใช้ที่มีสิทธิเข้าใช้เครื่องแม่ข่ายได้หลาย ๆ เครื่อง ถ้าทุกเครื่องมีชื่อขอเข้าใช้ระบบเป็นชื่อเดียวกันจะสามารถขอเข้าใช้ระบบจากทุก ๆ เครื่องแม่ข่ายโดยใช้รหัสผ่านชุดเดียวกัน

3. การเพิ่มเติมหรือแก้ไขคำสั่งพิเศษสามารถทำได้โดยแก้ไข โปรแกรมให้บริการตรวจสอบรหัสผ่านโดยไม่ต้องทำการแก้ไขโปรแกรมล็อกอิน

ข้อจำกัดและปัญหาที่พบจากการวิจัย

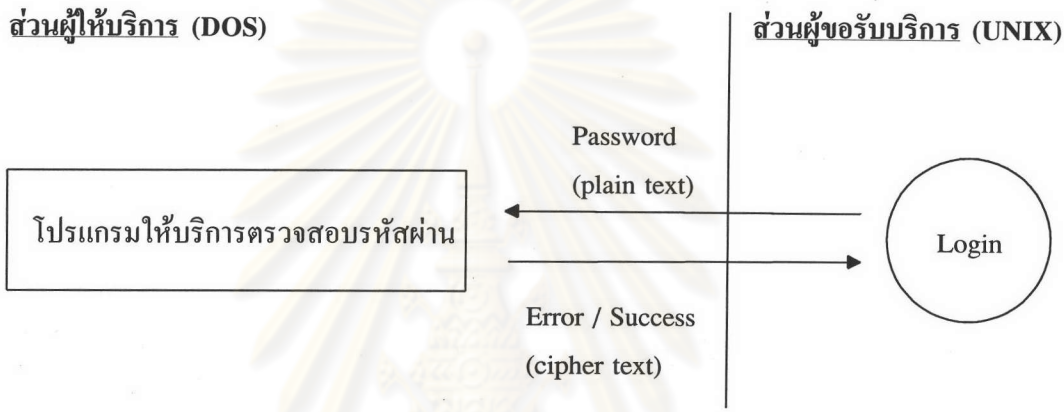
1. ความไม่เป็นมาตรฐานเดียวกันของระบบยูนิกซ์แบบต่าง ๆ ทำให้การเขียนโปรแกรมเพียงโปรแกรมเดียว เพื่อให้สามารถแปลงและทำงานได้ภายใต้ระบบปฏิบัติการยูนิกซ์ต่าง ๆ จะได้โปรแกรมต้นฉบับ (source program) ที่มีขนาดใหญ่และก่อนการแปลจะต้องมีการแก้ไขโปรแกรมต้นฉบับให้เหมาะสมกับระบบที่กำลังจะทำงานด้วยเสียก่อน

2. เนื่องจากใช้เครื่องคอมพิวเตอร์ระดับพีซีเป็นตัวให้บริการตรวจสอบรหัสผ่าน ซึ่งจำเป็นต้องมีไอพีแอดเดรสประจำเครื่อง ปัญหาที่เกิดขึ้นคือ มีเครื่องคอมพิวเตอร์อื่นใช้ไอพีแอดเดรสที่ซ้ำในการติดต่อกับระบบ

3. การส่งรายงานรหัสผ่านให้แก่ผู้ใช้ อาจมีการสูญหาย

ข้อเสนอแนะ

1. ควรพัฒนาขั้นตอนการส่งข้อความที่ใช้ในการติดต่อสื่อสาร โดยทำการเข้ารหัสกลุ่มข้อความก่อนที่จะทำการส่งออกไปยังเน็ตเวิร์ค เพื่อป้องกันการลักลอบเข้าใช้ระบบโดยใช้เครื่องคอมพิวเตอร์ที่เลียนแบบการทำงานของเครื่องคอมพิวเตอร์ที่ให้บริการตรวจสอบรหัสผ่านเครื่องจริงเป็นการหลอกระบบ ในรูปที่ 7.1 เสนอขั้นตอนในการส่งกลุ่มข้อมูลที่ถูกเข้ารหัส



รูป 7.1 ขั้นตอนการส่งรหัสผ่านเพื่อทำการตรวจสอบเมื่อมีการเข้ารหัสกลุ่มข้อความที่จะทำการส่ง

1.1 โปรแกรมล็อกอินส่งรหัสผ่านที่เป็นกลุ่มข้อมูลที่ยังไม่เข้ารหัส (plain text) ไปยังโปรแกรมให้บริการตรวจสอบรหัสผ่าน

1.2 โปรแกรมให้บริการตรวจสอบรหัสผ่านทำการตรวจสอบรหัสผ่าน และส่งผลที่ได้กลับไปยังโปรแกรมล็อกอิน โดยกลุ่มข้อความที่ถูกส่งกลับต้องเป็นกลุ่มข้อมูลที่ถูกเข้ารหัส (cipher text) โดยใช้รหัสผ่านเป็นคีย์

1.3 โปรแกรมล็อกอินทำการถอดรหัสกลุ่มข้อความที่ได้โดยใช้รหัสผ่านเป็นคีย์และทำงานตามผลที่ได้จากการตรวจสอบ

2. ควรพัฒนาวิธีการส่งรายงานรหัสผ่านให้แก่ผู้ใช้ เช่น ทำการส่งรายงานรหัสผ่านโดยใช้จดหมายอีเล็คโทรนิคส์ (electronic mail) โดยทำการเข้ารหัสรายงานรหัสผ่านก่อนที่จะทำการส่ง เมื่อผู้ใช้ได้รับจึงนำรายงานรหัสผ่านไปถอดรหัสตามอัลกอริทึม (algorithm) และคีย์ (key) ที่ได้กำหนดไว้ก่อนแล้ว หรืออีกวิธีหนึ่งคือ พัฒนาเครื่องคิดเลขขนาดเล็กที่สามารถสร้างรหัสผ่านที่ใช้ในการเข้าระบบให้แก่ผู้ใช้แต่ละคน

3. ควรพัฒนาระบบให้บริการรหัสผ่านให้สามารถใช้กับเครื่องแม่ข่ายได้หลาย ๆ เครื่องในเวลาเดียวกัน ปัญหาที่เกิดจากการมีเครื่องแม่ข่ายหลายเครื่อง คือ ผู้ใช้คนเดียวแต่มีชื่อขอเข้าใช้ระบบหลายชื่อ และการที่ผู้ใช้มีชื่อขอเข้าใช้ระบบที่ซ้ำกัน จึงเสนอแนวทางในการแก้ปัญหาโดยทำการสร้างแฟ้มข้อมูลชื่อแฝง (alias file) ใช้เก็บชื่อลงบันทึกเข้าใช้ระบบ ไอพีแอดเดรสของเครื่องแม่ข่าย และหมายเลขที่ใช้อ้างอิงถึงผู้ใช้ เพื่อประโยชน์ในการค้นหาข้อมูลรหัสผ่านของผู้ใช้

ฟิลด์	รูปแบบ	รายละเอียด
LOGIN_NAME	char [8]	ชื่อลงบันทึกเข้าใช้ระบบ
SERVER_IP	char [15]	ไอพีแอดเดรสของเครื่องแม่ข่าย (ถ้าเป็น ALL แสดงว่าเครื่องแม่ข่ายทุกเครื่องใช้ชื่อลงบันทึกเข้าใช้ระบบชื่อเดียวกัน)
ID	int	หมายเลขที่ใช้อ้างอิงถึงผู้ใช้ในระบบ

ตารางที่ 7.1 แสดงรูปแบบของแฟ้มข้อมูลชื่อแฝง

ตัวอย่างข้อมูลที่อยู่ในแฟ้มข้อมูลชื่อแฝง

LOGIN_NAME	SERVER_IP	ID
g36pku	161.200.145.4	001
g36pku	161.200.145.5	001
gcppku	161.200.80.11	001
g36pts	ALL	002
g36tps	161.200.145.5	003
gcptps	161.200.80.11	003

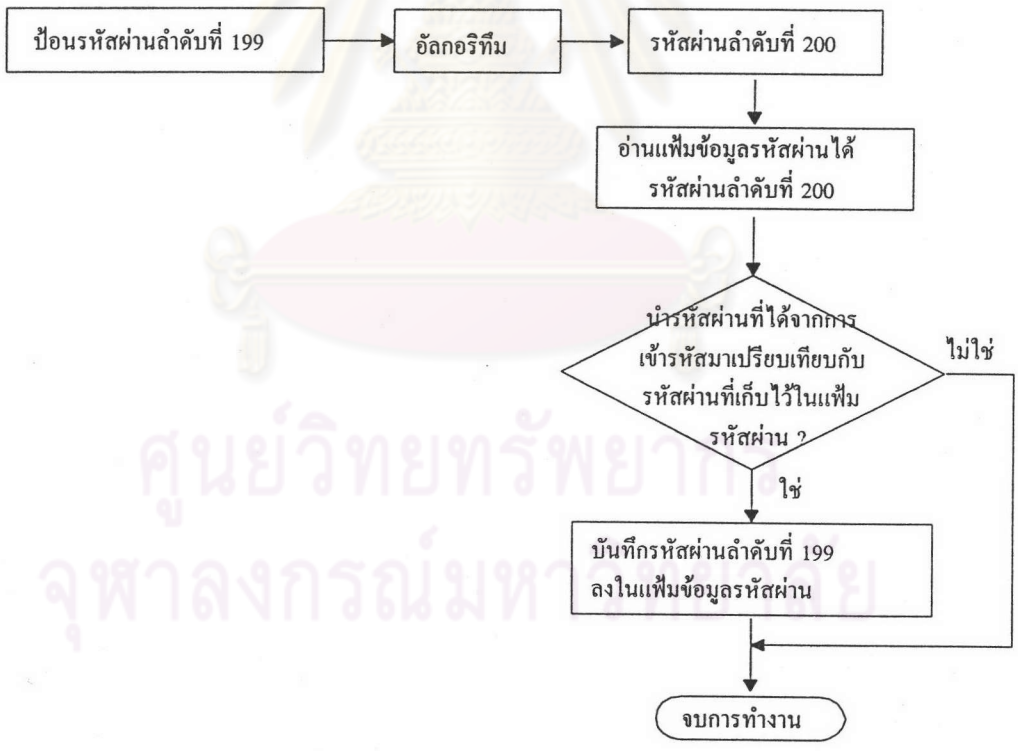
4. กำหนดมาตราการรักษาความปลอดภัยในระดับฟิสิคอล (physical security) ให้แก่เครื่องคอมพิวเตอร์ระดับพีซีที่ใช้เก็บรหัสผ่าน เช่น กำหนดบริเวณที่เครื่องคอมพิวเตอร์ตั้งอยู่เป็นบริเวณที่ผ่านได้เฉพาะผู้ดูแลระบบ

5. ปรับปรุงวิธีสร้างและตรวจสอบรหัสผ่าน โดยใช้อัลกอริทึมที่มีคุณสมบัติดังนี้ คือ เมื่อนำกลุ่มข้อมูลที่ต่างกันมาผ่านอัลกอริทึมนี้สามารถประกันได้ว่ากลุ่มข้อมูลที่ได้จะไม่ซ้ำกัน

และเมื่อทำการเข้ารหัสด้วยอัลกอริทึมนี้พบว่าเป็นการยากที่จะทำการถอดรหัส จากคุณสมบัติทั้งสองข้อทำให้เกิดแนวคิดในการสร้างและตรวจสอบรหัสผ่านแบบใหม่

5.1 วิธีการสร้างรหัสผ่าน รหัสผ่านตัวแรกเกิดจากการสุ่มตัวอักษรจำนวน 6 หลัก ส่วนรหัสผ่านลำดับที่ 2 เกิดจากการเข้ารหัสโดยใช้อัลกอริทึมนี้ 1 ครั้ง และรหัสผ่านลำดับที่ 3 เกิดจากการเข้ารหัส 2 ครั้ง ดังนั้นในแฟ้มข้อมูลรหัสผ่านจึงเก็บรหัสผ่านเพียงตัวเดียวแทนที่จะต้องเก็บรหัสผ่านถึง 200 ตัว

5.2 วิธีตรวจสอบรหัสผ่าน ระบบจะนำรหัสผ่านที่ผู้ใช้ป้อนไปทำการเข้ารหัสโดยใช้อัลกอริทึม 1 ครั้งแล้วนำกลุ่มข้อมูลที่ได้ไปเปรียบเทียบกับรหัสผ่านที่เก็บไว้ในแฟ้มข้อมูลรหัสผ่าน (รหัสผ่านที่เก็บไว้คือ รหัสผ่านที่ถูกใช้ในครั้งที่แล้ว) ถ้าผลการเปรียบเทียบถูกต้องจึงนำรหัสผ่านที่ผู้ใช้ป้อนเข้ามาไปใส่ในแฟ้มข้อมูลรหัสผ่านแทน



รูป 7.2 แสดงขั้นตอนตรวจสอบรหัสผ่านแบบใหม่

จากการสรุปผลการวิจัยทำให้ทราบถึงข้อจำกัดและปัญหาของระบบ จึงได้กล่าวถึงข้อเสนอแนะเพื่อเป็นแนวทางในการพัฒนาระบบต่อไป