บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบรักษาความมั่นคง (security) ที่ถูกใช้มากที่สุดในระบบคอมพิวเตอร์ในปัจจุบัน คือ ระบบบรหัสผ่าน (password) เนื่องจากเป็นระบบที่มีความสะดวกและปลอดภัยพอสมควร ปัญหาสำคัญของการใช้รหัสผ่าน คือ

- การดักฟัง (eavesdropping) รหัสผ่านบนระบบเครือข่าย (network system)
- การขโมยแฟ้มรหัสผ่าน (password file) ทั้งที่ไม่มีการเข้ารหัสและมีการเข้ารหัส (cryptography)
- การคาดเดารหัสผ่านโดยการทดลองซ้ำ ๆ (off-line password guessing)

ปัญหาแต่ละแบบจะมีวิธีการแก้ปัญหาที่แตกต่างกัน เช่น

- ปัญหาการดักฟังรหัสผ่านบนระบบเครือข่ายสามารถแก้ไขได้โดยการส่งข้อมูลผ่านช่องทางสื่อสารแบบเข้ารหัส (encryption channel)
- ปัญหาการขโมยแฟ้มรหัสผ่านสามารถแก้ไขได้โดย การควบคุมการเข้าถึงแหล่งข้อมูล (access control)
- ปัญหาการคาดเดารหัสผ่านโดยการทดลองซ้ำ ๆ สามารถแก้ไขได้โดยนำเอาระบบรหัสผ่านแบบใช้ครั้งเดียว (one-time password system) มาใช้แทนระบบรหัสผ่านแบบเดิม

ระบบรหัสผ่านแบบใช้ครั้งเดียวมีหลักการทำงานเบื้องต้น คือ ระบบจะทำการเปลี่ยนรหัสผ่านทุกครั้งที่มีการล็อกอิน (login) ไม่ว่าการเข้าใช้บริการจะสำเร็จหรือไม่ ผู้ใช้ (user) จะต้องป้อนรหัสผ่านชุดใหม่ที่ถูกกำหนดไว้ล่วงหน้าทุกครั้งที่ล็อกอิน ดังนั้นไม่สามารถคาดเดารหัสผ่านโดยการทดลองซ้ำได้อีก[5,6]

ระบบรหัสผ่านแบบใช้ครั้งเดียวที่ถูกพัฒนาขึ้นโดยก่อนหน้านี้ มีข้อบกพร่องบางประการดังนี้[1]

- การส่งผ่านรหัสผ่านทางเครือข่ายในรูปแบบที่อ่านได้ (plain text)
- การเก็บแฟ้มรหัสผ่านแบบใช้ครั้งเดียวในเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว (one-time password server) ไม่มีการเข้ารหัสและการควบคุมการเข้าถึง
- การติดต่อสื่อสารระหว่างเครื่องที่ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว (client) กับเครื่องให้บริการรหัสผ่านแบบใช้ครั้งเดียว (server) ขาดการพิสูจน์ตัวจริง (authentication)

ดังนั้นจึงควรมีการปรับปรุงระบบรหัสผ่านแบบใช้ครั้งเดียวให้มีความปลอดภัยมากขึ้น ซึ่งการปรับปรุงสามารถทำได้หลายแนวทาง แนวทางหนึ่งที่ถูกเลือกมาใช้ในวิทยานิพนธ์นี้คือการใช้วิธีการเข้ารหัส (cryptography) และการพิสูจน์ตัวจริงมาใช้ในแก้ปัญหาดังที่กล่าวมา

1.2 วัตถุประสงค์

เพื่อนำเทคนิคการเข้ารหัสและการพิสูจน์ตัวจริงมาใช้เสริมประสิทธิภาพของระบบรหัสผ่านแบบใช้ครั้งเดียว

1.3 ขอบเขตของการวิจัย

1.3.1 ปรับปรุงโปรแกรมการล็อกอิน (login) บนระบบปฏิบัติการยูนิกซ์ โดยอาศัยระบบรหัสผ่านแบบใช้ครั้งเดียวสำหรับระบบยูนิกซ์ ของนายพิษณุ เกริกอำไพสุรกิจ[1] ให้สามารถทำการเข้ารหัส เพื่อป้องกันการดักฟังและสามารถพิสูจน์ตัวจริงในระบบผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว

1.3.2 ปรับปรุงโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียวให้สามารถทำงานร่วมกับโปรแกรมการล็อกอินที่มีการเข้ารหัสและการพิสูจน์ตัวจริง

1.3.3 ขั้นตอนการล็อกอินตั้งแต่การป้อนชื่อ (login name) และรหัสผ่าน (password) จะไม่มีการเปลี่ยนแปลงหรือถ้าเปลี่ยนแปลงจะไม่ส่งผลกระทบต่อผู้ใช้

1.3.4 การพัฒนาการเข้ารหัสอาศัยโปรแกรมไลบรารีที่มีอยู่ในสาธารณะ (public program library)

1.4 ขั้นตอนและวิธีการดำเนินการวิจัย

1.4.1 ศึกษาการทำงานของระบบรหัสผ่านแบบใช้ครั้งเดียวที่มีอยู่แล้ว

1.4.2 ศึกษาการทำงานของโปรแกรมที่ทำงานภายใต้ระบบปฏิบัติการยูนิกซ์

1.4.3 ศึกษาการทำงานของโปรแกรมไลบรารี่สาธารณะของการเข้ารหัสแบบคีย์ลับเฉพาะและการเข้ารหัสแบบคีย์สาธารณะ

1.4.4 ศึกษาการทำงานของโปรแกรมไลบรารีสาธารณะของการพิสูจน์ตัวจริง

1.4.5 พัฒนาต้นแบบการเข้ารหัสและการพิสูจน์ตัวจริงโดยอาศัยไลบรารีที่มีอยู่ในสาธารณะ

1.4.6 ปรับปรุงโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียวให้มีการเข้ารหัสและการพิสูจน์ตัวจริง

1.4.7 ปรับปรุงโปรแกรมการล็อกอินให้มีการเข้ารหัสและการพิสูจน์ตัวจริง

1.4.8 ทดสอบการทำงาน ปรับปรุงและแก้ไขโปรแกรม

1.4.9 สรุปผลวิจัยและข้อเสนอแนะ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

เพิ่มความมั่นคงให้แก่ระบบรหัสผ่านแบบใช้ครั้งเดียวเพื่อป้องกันการดักฟังและการปลอมตัวระหว่างเครื่องที่ให้บริการรหัสผ่านแบบใช้ครั้งเดียว