บทที่ 6

สรุปผลการวิจัยและข้อเสนอแนะ

6.1 สรุปผลการวิจัย

การวิจัยนี้เป็นการเสริมความมั่นคงให้แก่ระบบการให้บริการรหัสผ่านแบบใช้ครั้งเดียว ของนายพิษณุ เกริกอำไพสุรกิจ โดยการนำเทคนิคการเข้ารหัสมาใช้ป้องกันการดักฟังและการพิสูจน์ตัวจริงของผู้ให้บริการต่อผู้ขอใช้บริการ และออกแบบระบบใหม่ให้มีประสิทธิภาพมากขึ้น ดังสรุปในตารางที่ 6.1

	ระบบเก่า	ระบบใหม่
OTP Server ผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว	ระบบปฏิบัติการดอส	ระบบปฏิบัติการลินุกซ์
	ทำงานแบบวนซ้ำ (iterative)	ทำงานแบบพร้อมกัน (Concurrent)
	ใช้ยูดีพี/ไอพี (Connection less)	ใช้เอสเอสแอล และ ทีซีพี/ไอพี (Connection Oriented)
	ไม่มีการเข้ารหัส ไม่มีการพิสูจน์ตัวจริง	มีการเข้ารหัส และการพิสูจน์ตัวจริง โดยใช้เอสเอสแอล โพรโตคอล
	โพรโตคอล ผู้ขอให้บริการ → ผู้ให้บริการ ขอใช้บริการ ผู้ขอให้บริการ ← ผู้ให้บริการ แสดงผลการทำงาน	โพรโตคอล ประกอบด้วย 3 ระยะ - ระยะแนะนำตัว - ระยะขอตรวจสอบรหัสผ่าน - ระยะขอปิดการติดตัว
OTP Client ผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว	ระบบปฏิบัติการยูนิกซ์	ระบบปฏิบัติการลินุกซ์
	ใช้ยูดีพี/ไอพี	ใช้เอสเอสแอล และ ทีซีพี/ไอพี
	ไม่มีการเข้ารหัส ไม่มีการพิสูจน์ตัวจริง	มีการเข้ารหัส มีการพิสูจน์ตัวจริง
OTP Maintenance	ให้แฟ้มข้อความ (Text file)	ใช้ฐานข้อมูลเชิงสัมพันธ์ (relational database) ชื่อ "mSQL"

ตารางที่ 6.1 แสดงความแตกต่างระหว่างระบบรหัสผ่านของเก่ากับของใหม่

	ระบบเก่า	ระบบใหม่
ระบบบำรุงรักษาฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียว	ส่วนต่อประสานกับผู้ใช้ (User Interface) แบบเชิงข้อความ (text base)	ส่วนต่อประสานกับผู้ใช้แบบกราฟิก (graphic base)
	บัญชีผู้ใช้ (OTP Account) ใช้งานกับเครื่องแม่ข่ายได้เพียงเครื่องเดียว	บัญชีผู้ใช้ (OTP Account) สามารถใช้งานกับเครื่องแม่ข่ายได้หลาย ๆ เครื่องพร้อมกัน โดยมีการระบุขอบเขต 3 รูปแบบ - <login>+<host>+<domain> - <login>+ALL+<domain> - <login>+ALL+ALL
CA (Certification Authorities) ผู้ออกใบรับรอง	-	CA Server ทำหน้าที่ออกใบรับรอง (Certificate) ให้กับ OTP Server และแจกใบรับรองของตัวเองให้กับทั้ง OTP Server และ OTP Client
เครื่องมือพัฒนาระบบ	Microsoft C/C++ 7.0 Microsoft Assembler 5.0 NCSA Telnet 2.307	GNU C Version 2.7.2.3 SSLeay 0.6.6 b Java Development Kit (JDK) 1.1.6 Mini SQL Version 2.0.8
ผู้ใช้	ต้องจดจำลำดับที่ของรหัสผ่านที่ใช้ต้องใช้คำสั่งในการติดต่อกับ OTP Server นอกเหนือจากการคีย์รหัสผ่าน - เลื่อนลำดับที่ของรหัสผ่าน - เลื่อนไปใช้รหัสผ่านชุดใหม่ - สร้างรหัสผ่านชุดใหม่	ไม่ต้องจดจำเนื่องจากระบบมีการแสดงสถานะเพื่อประกอบการใช้งาน - ชุดรหัสผ่านที่ใช้ - ลำดับที่ของรหัสผ่านปัจจุบัน - เตือนเมื่อรหัสผ่านใกล้หมด - เตือนเมื่อบัญชีผู้ใช้ใกล้หมดอายุ - การสร้างรหัสผ่านชุดใหม่เป็นไปโดยอัตโนมัติ

ตารางที่ 6.1 แสดงความแตกต่างระหว่างระบบรหัสผ่านของเก่ากับของใหม่

จากการเปลี่ยนแปลงดังกล่าวทำให้เกิดผลของการวิจัยสรุปได้ดังนี้

6.1.1 ผู้ให้บริการสามารถทำการพิสูจน์ตัวจริงต่อผู้ขอใช้บริการก่อนการแลกเปลี่ยนคีย์ (key exchange) ที่ใช้ในการเข้ารหัสข้อมูล และเพื่อให้มั่นใจได้ว่ากำลังติดต่ออยู่กับผู้ให้บริการตัวจริง

6.1.2 การแลกเปลี่ยนข้อมูลระหว่างผู้ให้บริการและผู้ขอใช้บริการเป็นการส่งข้อมูลผ่านช่องทางสื่อสารแบบเข้ารหัส เอสเอสแอล (SSL Encrypted Channel) ทำให้สามารถป้องกันการดักฟังได้

6.1.3 ผู้ใช้สามารถเข้าใช้เครื่องแม่ข่ายยูนิกซ์ได้โดยขอลงทะเบียนบัญชีผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว (OTP ACCOUNT) ได้ 3 วิธี

- ระบุให้สามารถเข้าใช้เครื่องแม่ข่ายที่ต้องการเพียงเครื่องเดียว
- ระบุให้เข้าใช้เครื่องแม่ข่ายภายใต้ชื่อโดเมนที่กำหนด
- ระบุให้เข้าใช้เครื่องแม่ข่ายได้ทุกเครื่องที่อยู่ภายใต้ขอบเขต (region) ของผู้ให้บริการ

6.1.4 วิธีการเข้าใช้เครื่องแม่ข่ายยูนิกซ์ ยังคงมีขั้นตอนคล้ายเดิม เพียงแต่ผู้ใช้จะได้รับข้อความพร้อมรับที่มีการบอกถึงรายละเอียดในการใช้รหัสผ่านแบบใช้ครั้งเดียว เช่น วันที่สร้างชุดรหัสผ่าน ลำดับที่ปัจจุบันของรหัสผ่าน เพื่ออำนวยความสะดวกต่อผู้ใช้ และไม่มีความจำเป็นต้องใช้คำสั่งพิเศษเพิ่มเติม นอกเหนือจากการคีย์รหัสผ่าน

6.2 ข้อจำกัดและปัญหาที่พบจากการวิจัย

6.2.1 เนื่องจากขั้นตอนในการลงทะเบียนบัญชีผู้ใช้จะต้องทำการลงทะเบียนทั้งหมด 2 ครั้ง คือ ที่เครื่องผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว และเครื่องแม่ข่ายยูนิกซ์ ทำให้มีขั้นตอนที่ซ้ำซ้อนและอาจเกิดความสับสน เช่น ผู้ใช้ชื่ออุดม ต้องการใช้ระบบนี้สำหรับทุกเครื่องภายใต้โดเมน cp.eng.chula.ac.th ในชื่อล็อกอิน “udom” นอกจากจะต้องลงทะเบียนกับผู้ให้บริการรหัสผ่าน

แบบใช้ครั้งเดียวแล้ว ยังจะต้องขอลงทะเบียนกับเครื่องแม่ข่ายยูนิกซ์ทุกเครื่องภายใต้โดเมน "cp.eng.chula.ac.th" ซึ่งอาจพบว่ามีผู้ใช้คนอื่นใช้ชื่อล็อกอินเดียวกันอยู่ก่อนแล้ว

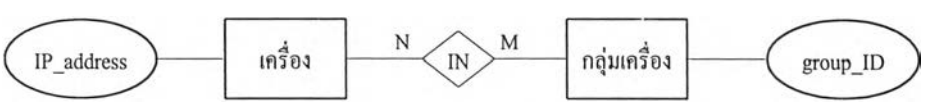
6.2.2 การกำหนดกลุ่มของเครื่องแม่ข่ายมีข้อจำกัดที่ต้องผูกติดอยู่กับชื่อโดเมน เช่น ALL.cp.eng.chala.ac.th หมายถึง ทุกเครื่องภายใต้ชื่อโดเมนที่ระบุ ซึ่งอาจไม่ตรงกับความต้องการที่แท้จริง เช่น กลุ่มเครื่องที่ต้องการเป็นเพียงบางเครื่องภายใต้โดเมนนี้เท่านั้น

6.2.3 ไลบรารีเอสเอสแอลที่ใช้ในการพัฒนาคือ "SSLeay 0.6.6 b" ซึ่งทำงานตามมาตรฐาน SSL 2.0 และสามารถพิสูจน์ตัวจริงเฉพาะทางฝั่งผู้ให้บริการ (Server) เท่านั้น

6.2.4 ระบบฐานข้อมูลเชิงสัมพันธ์ที่ใช้ในปัจจุบันเป็นเพียงรุ่นที่ใช้ทดสอบ (evaluate) ทำให้ขาดความสามารถในการควบคุมการเข้าถึงข้อมูล

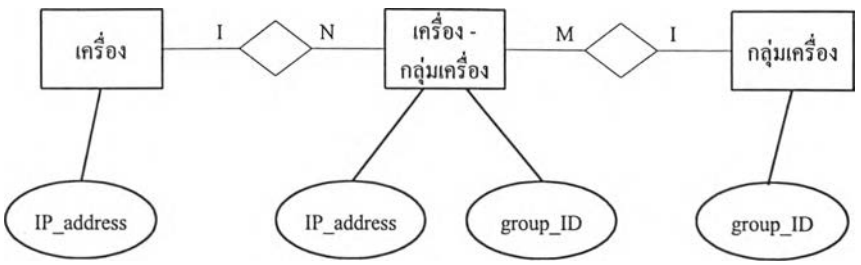
6.3 ข้อเสนอแนะ

6.3.1 ควรพัฒนาให้ระบบมีการระบุกลุ่มของเครื่องที่อิสระจากชื่อโดเมน โดยการออกแบบให้ใช้ชื่อกลุ่มเครื่องแทนและมีชื่อกลุ่มเครื่องพิเศษชื่อ "ALL" หมายถึงทุกเครื่องเช่นเดิม ทำให้



รูปที่ 6.1 แผนผังแสดงความสัมพันธ์ระหว่างเครื่องกับกลุ่มเครื่อง

ยังคงความสามารถในการระบุขอบเขตในระดับโดเมนไว้ดังเดิมด้วย ดังแสดงความสัมพันธ์เครื่องผู้ขอใช้บริการกับกลุ่มเครื่องในรูปที่ 6.1
ซึ่งในการออกแบบสามารถออกแบบความสัมพันธ์ดังกล่าวให้สามารถทำงานโดยอาศัยฐานข้อมูลเชิงสัมพันธ์ ดังแสดงในรูปที่ 6.2 ดังนั้นเครื่องหนึ่งเครื่องสามารถอยู่ได้หลายๆ กลุ่มเครื่องพร้อมๆ กัน และกลุ่มเครื่องสามารถมีสมาชิกได้ไม่จำกัด



รูปที่ 6.2 แผนผังแสดงความสัมพันธ์ระหว่างเครื่องและกลุ่มเครื่อง เมื่อปรับให้เหมาะกับฐานข้อมูลสัมพันธ์

6.3.2 เพิ่มขีดความสามารถในการลงบันทึก (log) การทำงานของผู้ให้บริการ โดยจัดให้มีแฟ้มลงบันทึกเข้าออก (log file) เพื่อนำข้อมูลไปใช้ในการวิเคราะห์การทำงานของระบบในเชิงสถิติและใช้ในระบบเฝ้าสังเกต (monitor system) รายละเอียดของการลงบันทึกประกอบด้วย

- ชื่อผู้ใช้ระบบรหัสผ่านแบบใช้ครั้งเดียว
- ชื่อเครื่องและชื่อโดเมนของเครื่องขอใช้บริการ
- วันที่ เดือน ปี ที่ขอใช้บริการ
- เวลาที่ขอใช้บริการ
- ผลของการขอใช้บริการ เป็นต้น

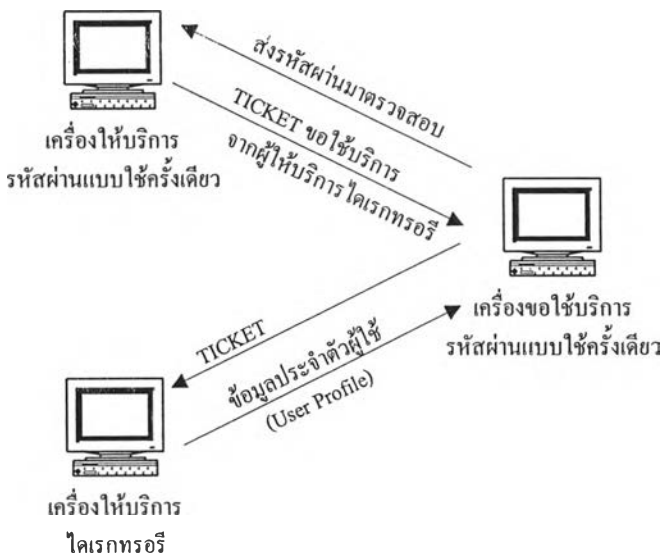
6.3.3 ปรับปรุงวิธีการจัดเก็บรหัสผ่านใหม่ โดยใช้เทคนิคการเข้ารหัสแบบทางเดียว เช่น ฟังก์ชัน crypt() ของยูนิกซ์ ในการเข้ารหัสผ่านทั้งหมดเพื่อป้องกันไม่ให้ผู้ที่ได้แฟ้มรหัสผ่านไปสามารถนำเอารหัสผ่านไปใช้ได้ รวมถึงผู้ที่ดูแลเครื่องให้บริการระบบรหัสแบบใช้ครั้งเดียวเองก็ไม่สามารถทราบถึงรหัสผ่านของผู้ใช้ได้ แต่ทั้งนี้จะต้องปรับปรุงให้การจัดพิมพ์รหัสผ่านให้เป็นความลับด้วย โดยผู้ใช้เท่านั้นที่ได้รับรหัสผ่านที่ไม่เข้ารหัส

6.3.4 ปรับปรุงให้มีการพิสูจน์ตัวจริงได้ทั้งฝั่งผู้ให้บริการและผู้ขอใช้บริการ เพื่อใช้การพิสูจน์ใบรับรองของผู้ขอใช้บริการแทนการตรวจสอบหมายเลขไอพี

6.3.5 ปรับปรุงให้สามารถใช้งานร่วมกับระบบบริการไดเรกทรอรี (Directory Service System) ที่มีอยู่หรือเป็นมาตรฐานในปัจจุบัน เช่น

- LDAP (Lightweight Directory Access Protocol)
- NIS (Network Information Service)
- NDS (Netware Directory Service) เป็นต้น

ซึ่งจะช่วยลดขั้นตอนการลงทะเบียนในส่วนของเครื่องผู้ขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว ดังมีสถาปัตยกรรมดังรูปที่ 6.3



รูปที่ 6.3 แสดงการทำงานร่วมกันระหว่างระบบรหัสผ่านแบบใช้ครั้งเดียว และระบบให้บริการไดเรกทรอรี