บทที่ 5

สรุปการวิจัยและข้อเสนอแนะ

ข้อจำกัดของการวิจัย

ข้อจำกัดของวิทยานิพนธ์ที่สำคัญ คือไม่สามารถใช้ไดรเวอร์ภาษาไทยกับโปรแกรมเทลเนตผู้ขอรับบริการได้ ในบทที่ 2 ที่กล่าวถึงแนวคิดและทฤษฎี ได้อธิบายข้อกำหนดของโปรโตคอลเทลเนต ที่ใช้การสมมาตรข้อมูลแทนรูปแบบข้อมูลสำหรับเทอร์มินอลของผู้ใช้ เปลี่ยนเป็นรูปแบบข้อมูลของเนตเวิร์คเวอร์ชวลเทอร์มินอล หรือ NVT ก่อนส่งข้อมูลผ่านระบบเครือข่ายทีซีพีไอพี ดังที่ได้กล่าวแล้วว่า NVT ใช้การแทนข้อมูลด้วยรหัสแอสกีเพียง 7 บิต โดยบิตที่ 8 มีค่าเป็น 0 สำหรับไดรเวอร์ภาษาไทยใช้รหัสแอสกี ครบทั้ง 8 บิต ในการแทนข้อมูลตัวอักษรภาษาไทย ทำให้โปรโตคอลเทลเนตไม่สามารถส่งผ่านข้อมูลภาษาไทยระหว่างโปรแกรมผู้ให้บริการและโปรแกรมผู้ขอรับบริการได้ เพราะบิตที่ 8 ของรหัสแอสกีที่แทนข้อมูลภาษาไทย 1 ตัวอักษร ถูกกำหนดค่าให้เป็น 0 ทำให้ข้อมูลเปลี่ยนไป

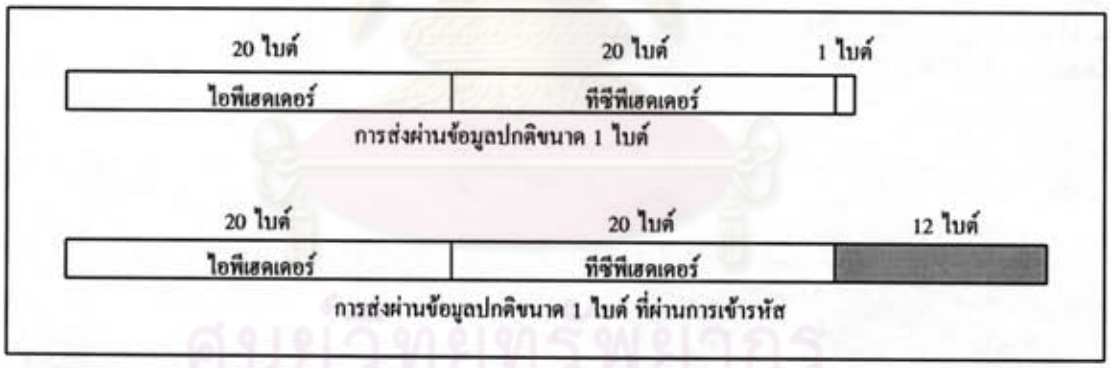
ข้อสรุป

การวิจัยสามารถพัฒนาระบบงานได้ตามวัตถุประสงค์ของงานวิจัยที่กำหนดไว้ คือ โปรแกรมเทลเนตผู้ให้บริการ และโปรแกรมเทลเนตผู้ขอรับบริการ สามารถเข้ารหัสข้อมูลก่อนส่งผ่านระบบเครือข่าย โดยรูปแบบการทำงานในการเข้ารหัส และถอดรหัสเป็นแบบบล็อคไซเฟอร์ และการแลกเปลี่ยนคีย์เซสชั่นคีย์เป็นแบบการเข้ารหัสข้อมูลด้วยคีย์สาธารณะ

การเข้ารหัสข้อมูลแบบบล็อคไซเฟอร์ มีความปลอดภัยในการป้องกันข้อมูลได้ดี เพราะการลอบดักข้อมูล เพื่อนำไปถอดรหัสทำได้ค่อนข้างยากถ้าไม่สามารถถอดเซสชั่นคีย์ เพื่อนำไปใช้ในการถอดรหัสข้อมูลได้ ในขั้นตอนการแลกเปลี่ยนเซสชั่นคีย์ มีกระบวนการป้องกันคีย์ไม่ให้ถูก

ลอบดัก โดยการแลกเปลี่ยนคีย์ใช้วิธีการเข้ารหัสข้อมูลแบบคีย์สาธารณะก่อนส่งผ่านคีย์ไปยังอีกฝ่าย เป็นการป้องกันคีย์ได้เป็นอย่างดี เพราะการนำข้อมูลที่ถูกเข้ารหัสด้วยคีย์สาธารณะไปถอดรหัสข้อมูล เป็นงานที่ยากเช่นกัน

โดยส่วนใหญ่ข้อมูลที่ส่งผ่านระหว่างโปรแกรมเทลเนตผู้ขอรับบริการ และโปรแกรมเทลเนตผู้ให้บริการมีขนาด 1 ตัวอักษร ข้อมูลแต่ละตัวที่ผู้ใช้พิมพ์ผ่านเทอร์มินอล ถูกส่งผ่านไปยังเครื่องผู้ให้บริการ เพื่อผ่านกระบวนการของผู้ให้บริการและได้ผลลัพธ์ส่งคืนกลับไปยังเทอร์มินอลผู้ขอรับบริการ ในชั้นของโปรแกรมประยุกต์เทลเนต รูปแบบข้อมูลดังที่ได้กล่าวแล้วว่าประกอบด้วยข้อมูลจริงของผู้ใช้ ข้อมูลส่วนหัวที่บอกจำนวนของข้อมูลที่ผ่านขั้นตอนการเข้ารหัสในแต่ละชุด และข้อมูลแพดดิ้งครบบล็อค (ในกรณีที่ข้อมูลบล็อคสุดท้ายของชุดข้อมูลไม่ครบบล็อคของกระบวนการเข้ารหัส) ถ้าการส่งข้อมูล 1 ไบต์ เมื่อผ่านกระบวนการเข้ารหัส ข้อมูลมีขนาดเพิ่มขึ้นเป็น 12 ไบต์ เมื่อข้อมูลถูกส่งผ่านไปยังชั้นต่างๆ ตามมาตรฐานการสื่อสาร คือชั้นทรานสปอร์ตและชั้นเนตเวิร์ค ตามโปรโตคอลทีซีพีไอพี ข้อมูลผ่านการเข้ารหัส (encapsulation) ประกอบด้วย ทีซีพีเฮดเดอร์ (tcp header) ขนาด 20 ไบต์ และ ไอพีเฮดเดอร์ (ip header) ขนาด 20 ไบต์



รูปที่ 5.1 แสดงรูปแบบข้อมูลเปรียบเทียบระหว่างการส่งผ่านข้อมูลปกติ และข้อมูลที่เข้ารหัสตามโปรโตคอลทีซีพีไอพี

การทำงานของโปรแกรมเทลเนตที่เพิ่มระบบการเข้ารหัสข้อมูล ใช้เวลาในการทำงานเพิ่มขึ้นจากกระบวนการเข้ารหัสข้อมูลก่อนส่งออกไป และถอดรหัสข้อมูลเมื่อรับเข้ามา โดยเกิดขึ้นทั้งในโปรแกรมเทลเนตผู้ขอรับบริการ และโปรแกรมเทลเนตผู้ให้บริการ เวลาที่เพิ่มขึ้นวัดจากอัตราความเร็วในการเข้ารหัสข้อมูล ทดสอบการทำงานบนเครื่อง 486 DX ความเร็วของ CPU 33 Mhz เข้ารหัสข้อมูลได้ในอัตราประมาณ 1,000 Kbps

โปรแกรมเทลเนตผู้ขอรับบริการ และโปรแกรมเทลเนตผู้ให้บริการ เมื่อทำการแก้ไขเพิ่มระบบการเข้ารหัสข้อมูลก่อนส่งผ่านเครือข่าย โปรแกรมทั้งสองมีขนาดเปลี่ยนแปลงเพิ่มขึ้นโดยเมื่อเปรียบเทียบกับโปรแกรมเดิม แสดงได้ดังตารางที่ 5.1

Client program	size (byte)	Server program	size (byte)
telbin.exe	253,302	telnetd	90,112
cryptel.exe	288,442	crypteld	114,688

ตารางที่ 5.1 เปรียบเทียบขนาดของโปรแกรมเทลเนตเดิมกับโปรแกรมใหม่

ข้อเสนอแนะ

ในวิทยานิพนธ์นี้ ได้พัฒนาระบบการเข้ารหัสข้อมูล โดยใช้โปรแกรมเทลเนตผู้ขอรับบริการที่ได้รับการพัฒนาจาก National Center for Supercomputing Application ที่มีขั้นตอนการทำงานตรงตามข้อกำหนดของโปรโตคอลเทลเนตอย่างถูกต้อง เพราะข้อกำหนดในการสมมาตรข้อมูลของเนตเวิร์คเวอร์ชวลเทอร์มินอลหรือ NVT เป็นข้อจำกัดในการพัฒนาเพื่อใช้งานกับไดรเวอร์ภาษาไทย ในการใช้ภาษาไทยบนโปรแกรมเทลเนตผู้ขอรับบริการ

การพัฒนาระบบการเข้ารหัสข้อมูลสำหรับโปรแกรมเทลเนตผู้ขอรับบริการ ให้สามารถใช้งานภาษาไทยได้ โดยการนำโปรแกรมเลียนแบบเทอร์มินอลภาษาไทยที่เป็นผลงานวิจัยของคุณเสกสรรค์ ตัณฑารักษ์ มาพัฒนาระบบการเข้ารหัสข้อมูลก่อนส่งผ่านระบบเครือข่าย เป็นแนวทางที่ทำให้สามารถใช้งานภาษาไทยบนโปรแกรมเทลเนตผู้ขอรับบริการ และสร้างความปลอดภัยให้กับข้อมูลก่อนส่งผ่านเครือข่าย เพิ่มความมั่นใจในการใช้งานสำหรับผู้ใช้ได้เป็นอย่างดี