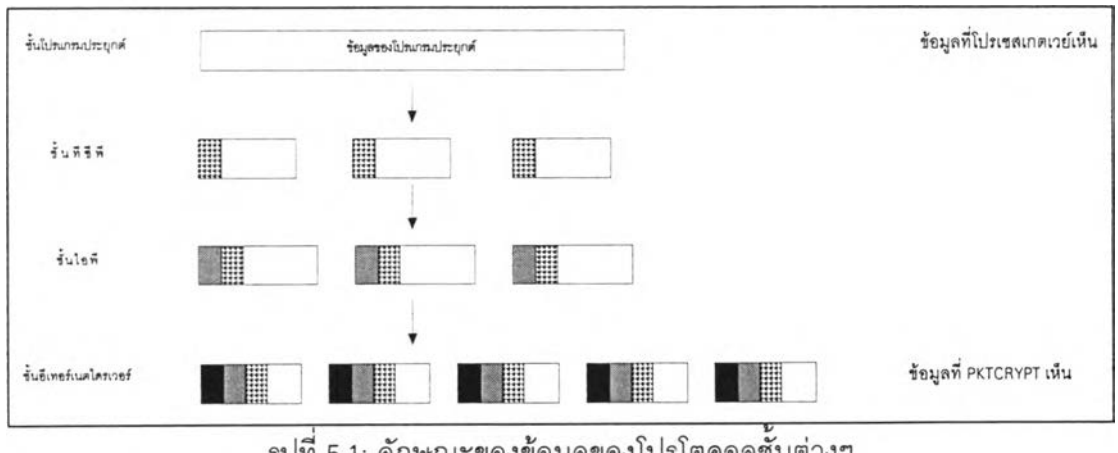
บทที่ 5

สรุปการวิจัยและข้อเสนอแนะ

ข้อจำกัดของการวิจัย

ข้อจำกัดสำหรับวิทยานิพนธ์ที่สำคัญ ได้แก่ การไม่สามารถเข้ารหัสลับข้อมูลแบบบล็อก ระหว่างโปรเซสเกตเวย์สำหรับการเข้ารหัสลับ ซึ่งทำงานบนระบบปฏิบัติการยูนิกซ์ และโปรแกรม PKTCRYPT เนื่องจากการทำงานของทั้ง 2 เป็นการทำงานต่างชั้นกันใน โปรโตคอลแสตก กล่าวคือ โปรเซสเกตเวย์สำหรับการเข้ารหัสลับบนยูนิกซ์ เป็นการทำงานในชั้นของโปรแกรมประยุกต์ ส่วน PKTCRYPT ทำงานในชั้นดาตาลิงค์ โดยทั้ง 2 จะมองรูปแบบของข้อมูลที่แตกต่างกัน

รูปแบบของข้อมูลที่โปรเซสเกตเวย์เป็นการมองข้อมูลแบบตรรก (logical data) นั่นคือข้อมูลมีขนาดความยาวเป็นขนาดจริง สำหรับ ข้อมูลที่ PKTCRYPT นั้นมองข้อมูลในรูปแบบของเฟรมอีเทอร์เนต ข้อมูลจะมีขนาดจำกัดเพื่อใช้ในการรับส่งกับเครือข่าย โดยข้อมูลที่โปรเซสเกตเวย์มองเห็น อาจจะถูกระบบโปรโตคอลตัดข้อมูลออกเป็นส่วนๆ ก่อนที่จะส่งลงไปในระดับล่างลงไป ลักษณะดังภาพ



รูปที่ 5.1: ลักษณะของข้อมูลของโปรโตคอลชั้นต่างๆ

การใช้วิธีการเข้ารหัสลับแบบบล็อก (block encryption) เช่น DES, IDEA จะไม่สามารถที่จะทำได้ เนื่องจากการเข้ารหัสลับแบบนี้จะต้องใส่เฮดเดอร์สำหรับการเข้ารหัสลับลงไปในข้อมูล ซึ่งถ้าหากกระทำในต่างชั้นกัน จะทำให้ข้อมูลไม่มีความเป็นในรูปแบบที่ถูกต้อง (non integrity) ของโปรโตคอล

ข้อจำกัดอีกอย่างหนึ่งคือ โปรแกรมขอรับบริการที่ใช้งานในระบบการทำงานนี้ไม่สามารถใช้ระบบการกำหนดที่อยู่ของไอพีแบบไดนามิก (dynamic IP address) ประเภท BOOTP หรือ RARP เป็นต้น เนื่องจากในระบบจะต้องมีการเก็บข้อมูลของคีย์โดยอ้างอิงกับที่อยู่ของไอพี จึงทำให้จะต้องกำหนดแบบระบุแน่นอน

ข้อสรุป

การวิจัยตามวิทยานิพนธ์นี้สามารถพัฒนาระบบงานที่เป็นไปตามวัตถุประสงค์ที่กำหนดไว้ คือสามารถทำการเข้ารหัสลับของข้อมูลในระบบโปรโตคอลทีซีพี/ไอพี โดยไม่จำเป็นจะต้องแก้ไขโปรแกรมต้นฉบับใดๆ และ ยังสามารถให้ผู้ใช้งานระบบยูนิกซ์ สามารถใช้งานระบบนี้ได้

การเข้ารหัสลับจะเป็นเพียงการเข้ารหัสลับในระดับไบต์ ซึ่งทำให้ข้อมูลที่ได้รับการเข้ารหัสลับ อาจจะถูกจับวิธีการเข้ารหัสลับ (cryptography) โดยการใช้วิธีการตรวจสอบรูปแบบของข้อมูลจำนวนมากได้ แต่อย่างไรก็ตามการรับส่งคีย์ก็ยังคงมีความปลอดภัยในระดับที่ดีพอสมควร เนื่องจากเป็นการรับส่งโดยการเข้ารหัสลับแบบใช้คีย์สาธารณะ

ข้อเสนอแนะ

ในวิทยานิพนธ์นี้ตามที่ได้กล่าวใน ข้อจำกัดของการวิจัย ที่ไม่สามารถทำการเข้ารหัสลับแบบบล็อก ซึ่งมีความปลอดภัยมากกว่าการเข้ารหัสลับแบบไบต์ โดยการแก้ไขระบบใหม่กล่าวคือ ให้แก้ไขในโปรแกรมต้นฉบับของโปรแกรมขอรับบริการโดยตรง จะทำให้ทั้งโปรเซสเกตเวย์ และโปรแกรมขอรับบริการมองข้อมูลในรูปตรรกเหมือนกัน การจะใช้วิธีการเข้ารหัสลับแบบบล็อกก็ย่อมทำได้

นอกจากการเปลี่ยนแปลงระบบการเข้ารหัสลับแล้ว อาจจะมีการเก็บข้อมูลคีย์ในลักษณะที่ดีกว่าในวิทยานิพนธ์นี้ ซึ่งเก็บข้อมูลในรูปของไฟล์ เพื่อให้การเก็บข้อมูลคีย์ของโปรเซสให้บริการคีย์ทำงานได้ดีกว่า อาจจะทำการเก็บข้อมูลคีย์ในระบบฐานข้อมูล (database) ซึ่งจะทำให้

ใช้ความสามารถของระบบฐานข้อมูลต่างๆ เช่น ความสามารถในการเรียกค้นข้อมูล, การกำหนดสิทธิการใช้งาน เป็นต้น แต่ทั้งนี้ในเครื่องที่เก็บข้อมูลคีย์ก็จะต้องมีระบบฐานข้อมูลอยู่ด้วย