บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ระบบยูนิกซ์ (UNIX system) เป็นระบบปฏิบัติการที่ผู้ใช้สามารถเข้าใช้งานบนระบบได้จากระยะทางไกล (remote access) โดยใช้โปรแกรมจำลองเทอร์มินอล (terminal emulator program) หรือโปรแกรมเทลเนตผู้ขอรับบริการ (telnet client program) เสนอขอรับบริการไปยังเครื่องที่ให้บริการ (remote host) โดยมีโปรแกรมเทลเนตผู้ให้บริการ (telnet server program) ทำงานอยู่ เพื่อการใช้งานบนระบบโดยผ่านการติดต่อสื่อสารด้วยโปรโตคอลทีซีพีไอพี (TCP/IP connection)

ในการเข้าใช้งานระบบ ผู้ใช้ต้องมีสิทธิ์บนระบบนั้น โดยมีข้อมูลของผู้ใช้ (account) บันทึกอยู่บนระบบ เพื่อใช้ในการตรวจสอบเมื่อต้องการเข้าใช้งาน ข้อมูลสำคัญที่ผู้ใช้ต้องใช้แสดงตนในการเข้าใช้งานได้คือ รหัสผู้ใช้ (user id) และรหัสผ่าน (password) ผู้ใช้ต้องพิมพ์รหัสผู้ใช้และรหัสผ่าน เพื่อลงบันทึกการเข้าใช้งานทุกครั้งที่เริ่มต้นการใช้งานระบบ

การใช้งานระบบจากระยะทางไกลโดยใช้โปรแกรมประยุกต์เทลเนตนี้ ข้อมูลต่างๆที่สื่อสารระหว่างผู้ใช้กับระบบ ถูกส่งผ่านเข้าไปในระบบเครือข่าย (network system) ในรูปแบบปกติ (plain text) สิ่งนี้เป็นปัญหาที่สำคัญ โดยเฉพาะข้อมูลที่มีความสำคัญมาก เช่น รหัสผู้ใช้และรหัสผ่าน ที่ต้องพิมพ์เพื่อแสดงตนในการเข้าใช้งานทุกครั้ง ถ้าการสื่อสารข้อมูลอยู่ในระบบเครือข่ายที่ไม่น่าเชื่อถือหรือไว้ใจได้ มีความเป็นไปได้ง่ายที่ข้อมูลเหล่านี้สามารถถูกลอบดัก (eavesdropped) เพื่อนำไปใช้ประโยชน์โดยบุคคลอื่น และอาจทำให้เกิดความเสียหายแก่เจ้าของข้อมูลได้ในภายหลัง

เพื่อสร้างช่องทางการสื่อสารที่น่าเชื่อถือ (reliable channel) และสร้างความปลอดภัยให้กับข้อมูล (secure channel) กล่าวคือ ข้อมูลที่ส่งผ่านเข้าไปในระบบเครือข่ายถึงผู้รับได้อย่างถูกต้องและครบถ้วนแล้ว ต้องมีวิธีที่ทำให้แน่ใจได้ว่าการส่งผ่านข้อมูลเข้าไปในเครือข่ายนั้น ข้อมูลจะไม่ถูกลักลอบนำไปใช้ประโยชน์ โดยผู้ที่ไม่มีส่วนเกี่ยวข้องได้

ระบบการเข้ารหัสข้อมูล (cryptography system) ใช้วิธีการเข้ารหัสข้อมูล (data encrytion) เปลี่ยนข้อมูลที่อยู่ในรูปปกติ (plain text) เป็นข้อมูลในรูปที่ไม่สามารถเข้าใจได้ (cipher text) เพื่อป้องกันไม่ให้บุคคลอื่นที่ไม่มีส่วนเกี่ยวข้องสามารถลอบนำข้อมูลไปใช้ประโยชน์ได้ และใช้วิธีการถอดรหัส (data decryption) เปลี่ยนข้อมูลกลับมาอยู่ในรูปปกติตามเดิม เมื่อส่งถึงจุดหมายและนำไปใช้ประโยชน์ต่อไป

ภายในมหาวิทยาลัยมีการใช้งานโปรแกรมประยุกต์เทลเนตอย่างกว้างขวาง ในการเข้าใช้งานบนระบบจากระยะไกล ความไม่ปลอดภัยของข้อมูลเกิดขึ้นได้ดังที่ได้กล่าวมาแล้ว ปัจจุบันมีการสร้างระบบความปลอดภัยของข้อมูลให้กับโปรแกรมประยุกต์เทลเนต โดยการป้องกันข้อมูลของการตรวจสอบสิทธิ์การเข้าใช้งาน (authentication) คือรหัสผู้ใช้และรหัสผ่าน แต่หลังจากนั้นในส่วนของข้อมูลที่ส่งผ่านระหว่างผู้ใช้และระบบยังคงอยู่ในรูปแบบปกติ

การออกแบบและพัฒนาโปรแกรมเทลเนตที่สร้างช่องทางการสื่อสารที่ปลอดภัยอย่างสมบูรณ์ให้กับข้อมูล และนำโปรแกรมที่ได้รับการพัฒนามาใช้ให้เกิดประโยชน์ เพราะข้อมูลของผู้ใช้ที่ส่งผ่านระบบเครือข่ายตลอดระยะเวลาการใช้งานมีความสำคัญทั้งสิ้น โดยใช้การเข้ารหัสข้อมูลทั้งหลายก่อนส่งผ่านระบบเครือข่าย เป็นการสร้างความมั่นใจให้กับข้อมูลของผู้ใช้ในการใช้งานผ่านระบบเครือข่ายได้เป็นอย่างดีทางหนึ่ง

วัตถุประสงค์ของการวิจัย

พัฒนาแนวทางเพื่อเพิ่มประสิทธิภาพให้กับโปรแกรมเทลเนตผู้ขอรับบริการที่ทำงานบนระบบปฏิบัติการดอส (DOS) และโปรแกรมเทลเนตผู้ให้บริการที่ทำงานบนระบบปฏิบัติการยูนิกซ์ โดยการเพิ่มระบบการเข้ารหัสข้อมูลเข้าไปในโปรแกรม เพื่อสร้างช่องทางการสื่อสารข้อมูลที่ปลอดภัยในการใช้งานระบบจากระยะไกล

ขอบเขตของการวิจัย

1. การพัฒนาเพื่อเพิ่มประสิทธิภาพให้กับโปรแกรมเทลเนตผู้ขอรับบริการ โดยใช้โปรแกรมเทลเนตผู้ขอรับบริการ เวอร์ชั่น 2.3.08 ของ NCSA : National Center for Supercomputing Application

2. ทำการพัฒนาโดยเพิ่มระบบการเข้ารหัสข้อมูล ให้กับโปรแกรมเอ็นซีเอสเอเทลเนต และสามารถใช้งานบนระบบปฏิบัติการดอส (DOS) ได้

3. การพัฒนาเพื่อเพิ่มประสิทธิภาพ ให้กับโปรแกรมเทลเนตผู้ให้บริการ โดยใช้โปรแกรมเทลเน็ตผู้ให้บริการที่ได้รับการพัฒนาโดย University of California, Berkeley

4. ทำการพัฒนาโดยเพิ่มระบบการเข้ารหัสข้อมูล ให้กับโปรแกรมเทลเนตผู้ให้บริการ และสามารถใช้งานบนระบบปฏิบัติการยูนิกซ์ ทั้งแบบ BSD 4.3 และ SYSTEM V Release 4 ได้

5. ทำการพัฒนาโปรแกรมเทลเนตผู้ขอรับบริการ ที่เพิ่มระบบการเข้ารหัสข้อมูล ให้สามารถรับและส่งข้อมูลที่มีความปลอดภัยกับโปรแกรมเทลเนตผู้ให้บริการที่เพิ่มระบบการเข้ารหัสข้อมูลได้อย่างถูกต้องตรงกัน และสามารถใช้งานกับโปรแกรมเทลเนตผู้ให้บริการบนเครื่องอื่น ในการส่งข้อมูลแบบปกติระหว่างกันได้ด้วยเช่นกัน

6. ทำการพัฒนาโปรแกรมเทลเนตผู้ให้บริการที่เพิ่มระบบการเข้ารหัสข้อมูล ให้สามารถรับและส่งข้อมูลที่มีความปลอดภัยกับโปรแกรมเทลเนตผู้ขอรับบริการ ที่เพิ่มระบบการเข้ารหัสข้อมูลได้อย่างถูกต้องตรงกัน และสามารถใช้งานกับโปรแกรมเทลเนตผู้ขอรับบริการอื่น ในการส่งข้อมูลแบบปกติระหว่างกันได้ด้วย

7. ภาษาที่ใช้ในการพัฒนาโปรแกรมใช้ภาษาซี

ลำดับขั้นตอนการวิจัย

1. ศึกษารายละเอียดและข้อกำหนดของโปรโตคอลเทลเนต (telnet protocol) ประกอบด้วยขั้นตอนการทำงาน การส่งผ่านคำสั่ง และการเจรจาทางเลือกต่างๆ ระหว่างโปรแกรมเทลเนตผู้ขอรับบริการ และโปรแกรมเทลเนตผู้ให้บริการ

2. ศึกษารายละเอียดของโปรแกรมเทลเนตผู้ขอรับบริการ ที่ทำงานบนระบบระบบปฏิบัติการดอส และโปรแกรมเทลเนตผู้ให้บริการ ที่ทำงานบนระบบปฏิบัติการยูนิกซ์

3. ศึกษาระบบการเข้ารหัส (cryptography system)

4. ออกแบบการเจรจาทางเลือกสำหรับการเข้ารหัส (option negotiation for data encryption) ระหว่างโปรแกรมเทลเนตผู้ขอรับบริการ และโปรแกรมเทลเนตผู้ให้บริการ เพื่อการเข้าสู่ระบบการเข้ารหัสข้อมูลของโปรแกรมทั้งสอง และทำการเข้ารหัสข้อมูลและถอดรหัสข้อมูลได้ถูกต้องตรงกัน

5. ออกแบบระบบการเข้ารหัส

6. พัฒนาโปรแกรม
7. ทดสอบและแก้ไขโปรแกรม
8. สรุปผลการวิจัย และเรียบเรียงวิทยานิพนธ์

ประโยชน์ที่คาดว่าจะได้รับ

1. โปรแกรมเทลเนตผู้ขอรับบริการและโปรแกรมเทลเนตผู้ให้บริการ ที่ได้พัฒนาขึ้นมาสามารถใช้งานแทนโปรแกรมเดิมที่มีการใช้งานกันมาก โดยมีข้อดีของการสร้างความปลอดภัยให้กับข้อมูลที่ส่งผ่านเครือข่าย ผู้ใช้โปรแกรมเทลเนตในการเข้าใช้งานระบบจากระยะไกล มีความมั่นใจในความปลอดภัยของข้อมูล ไม่สามารถถูกลอบนำไปใช้ประโยชน์โดยบุคคลอื่นได้

2. โปรแกรมเทลเนตผู้ขอรับบริการและโปรแกรมเทลเนตผู้ให้บริการที่ได้พัฒนาขึ้นมา ผู้ใช้สามารถใช้งานได้ตามปกติเหมือนเช่นการใช้งานบนโปรแกรมเดิม โดยไม่ต้องมาเรียนรู้วิธีการใช้งานใหม่อีก

3. มีโปรแกรมต้นฉบับ (source program) ที่เป็นของภาควิชาวิศวกรรมคอมพิวเตอร์และของมหาวิทยาลัย เพื่อการพัฒนาและปรับปรุงในการใช้ประโยชน์สำหรับโปรแกรมประยุกต์อื่นๆ ได้ต่อไป