บทที่ 1

บทนำ

ที่มาของปัญหา

โปรโตคอลทีซีพี/ไอพี (TCP/IP Protocol) เป็น โปรโตคอลที่มีการใช้งานอย่างแพร่หลาย ทั้งการใช้งานในระดับเครือข่ายท้องถิ่น (Local Area Network) และ ระดับเครือข่ายขนาดใหญ่ (Wide Area Network) โดยโปรโตคอลทีซีพี/ไอพีเป็นโปรโตคอลหลักสำหรับการเชื่อมโยงใน เครือข่ายอินเตอร์เนต (Internet) ซึ่งเป็นเครือข่ายที่ใหญ่ที่สุดในโลก

ข้อมูลที่รับส่งกันใน โปรโตคอลทีซีพี/ไอพี เป็นข้อมูลที่สามารถถูกลักลอบบันทึก (eavedropping หรือ tapping) โดยเครื่องอื่นที่อยู่บนเครือข่าย โดยเฉพาะในระดับเครือข่ายท้องถิ่น เช่น อีเทอร์เนต (Ethernet) หรือ โทกเกนริง (Token Ring) เนื่องจากข้อมูลเป็นข้อความที่สามารถอ่านได้

การลักลอบดักข้อมูลในเครือข่ายทีซีพี/ไอพีนั้น ทำได้โดยการใช้ซอฟต์แวร์พิเศษบางอย่างที่ทำหน้าที่คล้ายกับ ซอฟต์แวร์ที่ตรวจสอบปริมาณการใช้งานเครือข่าย (Traffic Monitor) เช่น โปรแกรมทีซีพีดัมพ์ (tcpdump) หรือ อีเทอร์ไฟน์ (etherfind) ซึ่งทำงานบน เครื่องซัน (Sun workstation) สามารถดักแพกเกต (packet) ที่ส่งไปมาระหว่างเครื่องต่างในๆเครือข่ายอีเทอร์เนตเดียวกันได้

ข้อมูลบางอย่างที่เป็นข้อมูลสำคัญ เช่น รหัสผ่านของเครื่องต่างๆ อาจจะถูกลักลอบบันทึกไปได้ในขณะที่มีการใช้งาน โปรแกรมที่ต้องมีการใส่รหัสผ่านต่างๆ เช่น เทลเนต (telnet) หรือ เอฟทีพี (ftp) เป็นต้น ทำให้ผู้ที่ต้องการทำลายระบบสามารถนำรหัสผ่านของรูตที่ลักลอบบันทึกไปใช้ในทางที่ไม่ดีได้

แนวทางการป้องกันที่สามารถทำได้ แยกได้เป็น 2 ประเภท ได้แก่ การป้องกันทางกายภาพ และ การป้องกันโดยซอฟต์แวร์

1) การป้องกันทางกายภาพ เป็นการป้องกันไม่ให้ผู้อื่น สามารถเข้าถึงอุปกรณ์ต่างๆที่เกี่ยวข้องกับการสื่อสารข้อมูลได้โดยง่าย เช่น

- จำกัดการใช้ขั้วต่อ (connector) เท่าที่จำเป็น
- วางสายสื่อสาร (network cable) ในที่ที่ยากต่อการดักบันทึก
- วางอุปกรณ์ประเภท เราเตอร์ (router) ไว้ในที่ที่ปลอดภัย
- ใช้สายไฟเบอร์ออฟติกเนื่องจากยากต่อการดักบันทึก

2) การป้องกันโดยซอฟต์แวร์ เป็นการใช้วิธีการเข้ารหัสลับข้อมูล (data encryption) เพื่อป้องกันไม่ให้ผู้อื่นสามารถที่ลักลอบดักข้อมูลไปไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้

การเข้ารหัสลับข้อมูลสำหรับโปรโตคอลทีซีพี/ไอพีเพื่อป้องกันการลักลอบบันทึกข้อมูล ได้รับการพัฒนาออกมาในรูปแบบต่างๆ เช่น

- เคอร์เบรอส (Kerberos) ในโครงการ Athena ของ MIT (Cheskwick, 1994; Curry, 1992; Garfinkel, 1991)
- PGP (Pretty Good Privacy) (Garfinkel, 1995)
- CLIPPER (Schneier,1994)
- Secure RPC ของ Sun Microsystem Inc.
- การแก้ไขโปรแกรมต้นฉบับ (source code) สำหรับโปรแกรมให้บริการ (server program) และ โปรแกรมขอรับบริการ (client program) เพื่อเพิ่มเติมหน้าที่สำหรับการเข้ารหัสลับ และถอดรหัสลับข้อมูล (Safford,1993)

สำหรับรูปแบบการป้องกันโดยการเข้ารหัสลับ ตามรูปแบบที่ได้กล่าวมาแม้ว่าจะได้ประสิทธิผลที่ดี แต่ว่ามีผลกระทบต่อโครงสร้างเดิม และยังต้องอาศัยผู้จัดการระบบ (system administrator) ในการติดตั้งให้ ซึ่งทำให้ขาดความยืดหยุ่นในการใช้งานได้

วัตถุประสงค์ของการวิจัย

พัฒนาระบบการเข้ารหัสลับข้อมูล (encryption) และถอดรหัสลับข้อมูล (decryption) เป็นชั้น (layer) ของ โปรโตคอลสแตก (protocol stack) สำหรับโปรโตคอลทีซีพี/ไอพี โดยไม่มีการเปลี่ยนแปลงโปรแกรมต้นฉบับ ของ โปรเซสบริการ และ โปรเซสขอรับบริการ

ขอบเขตการวิจัย

1) พัฒนาระบบการเข้ารหัสลับข้อมูลและถอดรหัสลับข้อมูลสำหรับ โปรโตคอลทีซีพี/ไอพี ระหว่าง โปรแกรมขอรับบริการ บนระบบปฏิบัติการเอ็มเอสดอส กับ โปรแกรมผู้ให้บริการ บนระบบปฏิบัติการยูนิกซ์

2) โปรแกรมขอรับบริการบนระบบปฏิบัติการเอ็มเอสดอส ใช้โปรโตคอลทีซีพี/ไอพี ผ่านทาง แพกเกตไดรเวอร์ ของ บริษัท เอฟทีพีซอฟต์แวร์ (FTP Software packet driver)

3) พัฒนาโปรแกรมให้บริการ ทำหน้าที่เข้ารหัสลับและถอดรหัสลับข้อมูล ให้กับโปรแกรมให้บริการเดิม กับ โปรแกรมขอรับบริการ ซึ่งข้อมูลได้รับการเข้ารหัสลับมาแล้ว

4) พัฒนาโปรแกรมฝังตัว (Terminated and Stay Rresident Program) บน ระบบปฏิบัติการเอ็มเอสดอส ทำหน้าที่เข้ารหัสลับและถอดรหัสลับข้อมูลที่รับส่ง ผ่านทางแพกเกตไดรเวอร์ ของเอฟทีพีซอฟต์แวร์

5) การสื่อสารข้อมูลใช้ อีเทอร์เนต (Ethernet)

6) การเข้ารหัสลับใช้วิธีการเข้ารหัสลับโดยใช้คีย์สาธารณะ (public key encryption)

ประโยชน์ที่คาดว่าจะได้รับ

1) ป้องกันการดักบันทึกข้อมูล ที่รับส่งบนโปรโตคอลทีซีพี/ไอพี โดยเฉพาะอย่างยิ่งข้อมูลที่สำคัญ เช่น รหัสผ่าน เป็นต้น

2) เป็นการพัฒนาระบบความมั่นคง (security system) ที่ไม่กระทบต่อโครงสร้างของระบบเดิม โดยเป็นเพียงการเพิ่มเติมบางส่วนเข้าไปในระบบ

3) ผู้ใช้งานบนระบบปฏิบัติการยูนิกซ์สามารถใช้งานระบบความมั่นคงนี้ได้เอง โดยไม่จำเป็นต้องอาศัยสิทธิของรูต

4) เป็นแนวทางการสำหรับการพัฒนาระบบความมั่นคงบนทีซีพี/ไอพี โปรโตคอล

แนวทางการวิจัย

1) ศึกษาโปรโตคอลทีซีพี/ไอพี, แพกเกตไดร์เวอร์, การเข้ารหัสลับ

2) ศึกษางานวิจัยที่เกี่ยวข้อง

3) ออกแบบระบบสำหรับงานวิจัย

4) พัฒนาต้นแบบของงานวิจัย

5) ปรับปรุงต้นแบบของงานวิจัย

6) ทดสอบและแก้ไขงานวิจัย

7) สรุปผลการวิจัยและเรียบเรียงวิทยานิพนธ์