บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

การพัฒนาให้ระบบการรับส่งไฟล์สามารถรองรับการใช้รหัสผ่านแบบใช้ครั้งเดียวสำหรับระบบยูนิกซ์ เป็นอีกวิธีหนึ่งที่สามารถป้องกันเหตุร้ายอันเกิดจากการลักลอบเข้าใช้บริการถ่ายโอนแฟ้มจากผู้ที่ไม่มีสิทธิที่ทราบรหัสผ่านของผู้ใช้คนอื่น เนื่องจากการรองรับระบบรหัสผ่านแบบใช้ครั้งเดียวทำให้รหัสผ่านที่ผู้ไม่มีสิทธิได้รับไปนั้นไม่สามารถนำมาใช้ได้อีกในครั้งต่อไป เพราะโปรแกรมให้บริการถ่ายโอนแฟ้มถามความถูกต้องจากส่วนให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวซึ่งจะทำการเปลี่ยนรหัสผ่านทุกครั้งที่มีการเข้าใช้ระบบสำเร็จและรหัสผ่านเหล่านั้น มีเพียงผู้ใช้ที่มีสิทธิและส่วนให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวเท่านั้นที่ทราบ โดยรหัสผ่านจะถูกเก็บไว้ในฐานข้อมูลบนเครื่องให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวและถูกพิมพ์ส่งไปให้ผู้ใช้

เนื่องจากงานวิจัยชิ้นนี้จะต้องมีการปรับปรุงส่วนให้บริการถ่ายโอนแฟ้ม ซึ่งจะต้องเป็นไปตาม อาร์เอฟซี 959โพรโทคอลถ่ายโอนแฟ้ม (RFC 959 FILE TRANSFER PROTOCOL) (Postel and Reynolds, 1985) รวมทั้งจะต้องสามารถรองรับระบบรักษาความปลอดภัยในระบบยูนิกซ์แบบต่างๆ ที่มีอยู่ได้แก่

- แบบมาตรฐาน
- Shadow
- HP-Trusted-System
- Digital Enhanced C2
- Standard AIX
- ระบบรักษาความปลอดภัยรหัสผ่านแบบใช้ครั้งเดียวของจุฬาลงกรณ์มหาวิทยาลัย (พิษณุ เกริกอำไพสุรกิจ, 2539)

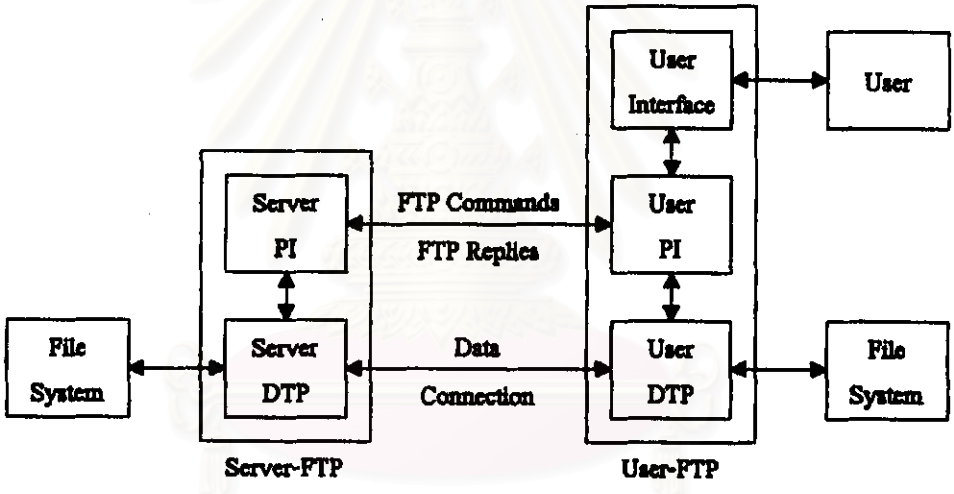
ผู้บริหารระบบสามารถที่จะเลือกได้ว่า จะใช้ระบบรักษาความปลอดภัยรหัสผ่านแบบใช้ครั้งเดียวหรือไม่ ในบทนี้จะกล่าวถึง โพรโทคอลถ่ายโอนแฟ้ม ระบบรักษาความปลอดภัยในระบบยูนิกซ์ และ ระบบรหัสผ่านแบบใช้ครั้งเดียวของจุฬาลงกรณ์มหาวิทยาลัย

หอสมุดกลาง สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

2.1 โพรโทคอลถ่ายโอนแฟ้ม

โพรโทคอลถ่ายโอนแฟ้ม (File Transfer Protocol, FTP) (Postel and Reynold, 1985) เป็นโพรโทคอลที่ถูกพัฒนาขึ้นโดย Advance Research Project Agency (ARPA) มีจุดประสงค์หลักเพื่อ

- สนับสนุนการใช้งานแฟ้มร่วมกัน
- สนับสนุนไม่ว่าจะทางตรงหรือทางอ้อมในการใช้งานคอมพิวเตอร์ที่อยู่ห่างไกล
- แยกผู้ใช้ออกจากความซับซ้อนของระบบแฟ้มต่างเครื่อง
- รับส่งข้อมูล อย่างปลอดภัย และ มีประสิทธิภาพ



รูปที่ 2.1 แสดงแบบจำลองการทำงานของโพรโทคอลถ่ายโอนแฟ้ม

Server-FTP คือ กระบวนการ (process) หรือ กลุ่มของกระบวนการที่มีหน้าที่ในการถ่ายโอนแฟ้มและทำงานร่วมกับ User-FTP ประกอบไปด้วย PI และ DTP

Server-PI คือ ตัวแปลความหมายโพรโทคอล ซึ่งจะคอยสัญญาณเดิดต่อสื่อสารจาก User-PI และทำการติดต่อสื่อสารกัน โดยใช้ คำสั่งมาตรฐานของโพรโทคอลถ่ายโอนแฟ้ม แล้วนำคำสั่งที่แปลได้ไปใช้ในการจัดการกับ Server DTP

Server-DTP คือ กระบวนการในการรับส่งข้อมูลโดยรับคำสั่งจาก Server-PI เพื่อส่งและรับข้อมูลลงระบบแฟ้ม

User-FTP คือ กระบวนการ หรือ กลุ่มของกระบวนการที่มีหน้าที่ในการถ่ายโอนแฟ้ม และทำงานร่วมกับหนึ่ง หรือ หลาย Server-PI

User-PI คือ ตัวแปลความหมายโพรโทคอล ซึ่งจะเป็นฝ่ายเริ่มต้นติดต่อสื่อสารกับ Server-PI โดยใช้ คำสั่งมาตรฐานของโพรโทคอลถ่ายโอนแฟ้ม แล้วนำคำสั่งที่แปลได้ไปใช้ในการจัดการกับ Server DTP

User-DTP คือ กระบวนการในการรับส่งข้อมูลโดยรับคำสั่งจาก User-PI เพื่อส่งและรับข้อมูลลงระบบแฟ้ม และจะมีสถานะปิดการทำงานเมื่อเป็นการถ่ายโอนแฟ้มระหว่าง Server-PI ด้วยกัน

การติดต่อสื่อสารข้ามเครื่องในระดับต่ำจะใช้มาตรฐานของโพรโทคอลเทลเน็ตโดยในมาตรฐานของโพรโทคอลถ่ายโอนแฟ้มจะกล่าวถึงเฉพาะระดับคำสั่งที่เกี่ยวกับการถ่ายโอนแฟ้ม

2.2 ระบบรักษาความปลอดภัยในระบบยูนิกซ์

ระบบรักษาความปลอดภัยในระบบยูนิกซ์มีหลายวิธี หนึ่งในวิธีเหล่านั้นคือ การใช้รหัสผ่าน ซึ่งรหัสผ่านและข้อมูลที่สำคัญอื่นๆ เช่น หมายเลขผู้ใช้ หมายเลขกลุ่ม สารบบบ้าน(home directory) ฯลฯ จะถูกเก็บไว้ในแฟ้มชื่อ /etc/passwd (Stevens, 1994: 24-25)โดยจะมีรูปแบบดังนี้

login-name:encrypted-password:user-id:group-id:miscellany:login-directory:shell

เช่น

g39ssk:u0ud5eOq2MpaZ:224:5:Sommart Srikitticha:/grad/g39ssk:/bin/ksh

login-name	คือ อักขระที่ใช้ในการบันทึกเข้า
encrypted-password	คือ รหัสผ่านที่ได้รับการเข้ารหัสแล้ว
user-id และ group-id	คือ หมายเลขผู้ใช้ และ หมายเลขกลุ่มผู้ใช้
miscellany	คือ เบ็ดเตล็ดแต่โดยส่วนใหญ่จะเก็บชื่อ และนามสกุล รวมทั้งข้อมูลอื่นๆ ของผู้ใช้
login-directory	คือ สารบบเริ่มต้น หรือ สารบบบ้าน
shell	คือ โปรแกรมที่ทำหน้าที่เป็นเปลือกระบบ

แม้ว่าแฟ้มรหัสผ่านจะมีการเข้ารหัสรหัสผ่านไว้แล้วก็ตาม แต่ผู้ไม่ประสงค์ดีอาจจะทำการคัดลอกแฟ้มรหัสผ่านเพื่อนำไปทำกรรมวิธีการใดๆก็ตามเพื่อหารหัสผ่าน โดยเฉพาะผู้ใช้โดยทั่วไปมักจะนำคำที่ใช้ในชีวิตประจำวันมาใช้ในการตั้งรหัสผ่าน ทำให้การเดาและนำมาเข้ารหัสเพื่อเปรียบเทียบทำได้ง่ายขึ้น

วิธีการในการจัดการกับรหัสผ่านดังกล่าวได้ถูกพัฒนาเพิ่มขึ้นอีกโดยการแยกรหัสผ่านที่ได้รับการเข้ารหัสแล้วมาเก็บไว้ในอีกแฟ้มหนึ่ง ชื่อ /etc/shadow โดยเปลี่ยนค่า encrypted-password ที่อยู่ในแฟ้ม /etc/passwd ให้เป็นเครื่องหมายดอกจัน และจะอนุญาตให้อ่านได้เฉพาะผู้ใช้ที่มีสิทธิสูงเท่านั้นพร้อมทั้งมีการเพิ่มเติมส่วนของอายุการใช้งานของรหัสผ่านด้วย (password aging) เริ่มมีการนำวิธีนี้มาใช้ตั้งแต่ ระบบยูนิกซ์ System V รุ่น 3.2 เรียกวิธีนี้ว่ารหัสผ่านแบบชาโดว์(shadow password)(Stevens, 1994: 25) โดยมีเขตข้อมูลดังต่อไปนี้(SunSoft, 1995: 19-20)

username:password:lastchg:min:max:warn:inactive:expire

เช่น

rimmer:86Kg/MNT/dGu.:8882:0::5:20:8978

username	คือ ชื่อบัญชีผู้ใช้
password	คือ รหัสผ่านที่ได้รับการเข้ารหัสแล้ว
lastchg	คือ วันที่ที่มีการเปลี่ยนรหัสผ่านครั้งล่าสุด คิดเป็นจำนวนวัน เทียบกับวันที่ 1 มกราคม พ.ศ. 2513
min	คือ จำนวนวันหลังจากเปลี่ยนรหัสผ่านครั้งล่าสุดที่จะอนุญาตให้เปลี่ยนรหัสผ่านได้
max	คือ อายุการใช้งานรหัสผ่าน หรือ จะต้องเปลี่ยนรหัสผ่านภายในจำนวนวันของเขตข้อมูลนี้
warn	คือ จำนวนวันก่อนหมดอายุการใช้งานรหัสผ่านที่จะเริ่มมีการเตือน
inactive	คือ จำนวนวันหลังจากหมดอายุการใช้งานรหัสผ่าน หากพ้นจำนวนวันนี้แล้วบัญชีผู้ใช้จะถูกปิดทาง (disable) ไม่ให้ใช้งาน
expire	คือ วันที่ที่หมดอายุการใช้งานของบัญชีผู้ใช้

ในระบบยูนิกซ์ HP-UX รุ่น 10 เป็นต้นไปสามารถติดตั้งระบบรักษาความปลอดภัยได้ 2 แบบ ได้แก่ แบบมาตรฐานดังได้กล่าวมาแล้ว และ แบบ Trusted ซึ่งปรับปรุงระบบรักษาความปลอดภัยให้เป็นไปตามมาตรฐาน ซีทู (C2) ของ กระทรวงกลาโหมสหรัฐอเมริกา เรียกวิธีนี้ว่า HP-UX Trusted System (Jerbic, n.d.d.) และในส่วนของการเก็บรักษารหัสผ่านจะเปลี่ยนไปเก็บในสารบบ /tob/files/auth แทนโดยมีเขตข้อมูลที่เกี่ยวกับรหัสผ่านและโยงไปถึงการอนุญาตหรือ ไม่อนุญาตให้บันทึกเข้า (login) ได้แก่

u_name	คือ ชื่อบัญชีผู้ใช้
u_id	คือ หมายเลขผู้ใช้
u_pwd	คือ รหัสผ่านที่ได้รับการเข้ารหัสแล้ว
u_minchg	คือ จำนวนวินาทีหลังจากเปลี่ยนรหัสผ่านครั้งล่าสุดที่จะอนุญาตให้เปลี่ยนรหัสผ่านได้
u_exp	คือ อายุการใช้งานรหัสผ่าน เป็นวินาที
u_life	คือ อายุการใช้งานรหัสผ่านที่หากเลยจากวินาทีนี้ไปแล้วบัญชีผู้ใช้จะถูกปิดทาง
u_succhg	คือ วันและเวลาที่มีการเปลี่ยนรหัสผ่านครั้งล่าสุด คิดเป็นจำนวนวินาที เทียบกับวันที่ 1 มกราคม พ.ศ. 2513
u_acct_expire	คือ วันและเวลาที่หมดอายุการใช้งานของบัญชีผู้ใช้ คิดเป็นจำนวนวินาทีเทียบกับวันที่ 1 มกราคม พ.ศ. 2513
u_tod	คือ วันและเวลาที่อนุญาตให้บันทึกเข้า
u_unsuclog	คือ จำนวนครั้งในการบันทึกเข้าผิดพลาด
u_maxtries	คือ จำนวนครั้งที่ยอมให้บันทึกเข้าผิดพลาด หากมากกว่านี้บัญชีผู้ใช้จะถูกปิดทาง
u_lock	คือ อนุญาต หรือ ไม่อนุญาตให้ผู้ใช้บันทึกเข้า ฯลฯ

หากไม่มีการกำหนดค่าเหล่านี้จะใช้ค่าที่อยู่ในเขตข้อมูลของแฟ้ม/tob/files/auth/system/default ซึ่งจะเก็บค่าโดยปริยายเอาไว้ (Hewlett Packard, 1995: Section 3-221 – Section 3-222)

ในระบบยูนิกซ์ Digital Unix รุ่น 4.0 มีการนำระบบรักษาความปลอดภัยที่ตรงตามมาตรฐาน ซีทู เช่นเดียวกับระบบยูนิกซ์ HP-UX Trusted System รวมทั้งยังมีรายละเอียดเหมือนกันหลายประการเช่น สารบบที่ใช้ในการเก็บรักษารหัสผ่าน และ ข้อมูลเกี่ยวกับรหัสผ่านของผู้

ใช้ในสารบบ /tcb/files/auth การเก็บค่าโดยปริยายของผู้ใช้ไว้ในแฟ้ม /tcb/files/auth/system/default (Digital Equipment Corperation, 1996)

ในระบบยูนิกซ์ AIX รุ่น 4.3 มีระบบรักษาความปลอดภัยโดยเฉพาะของตัวเอง โดยจะทำการจัดเก็บรหัสผ่านไว้ใน สารบบ /etc/security/passwd (IBM, 1997c)รวมถึงข้อมูลอื่นๆ เช่น วันและเวลาที่มีการเปลี่ยนแปลงรหัสผ่านครั้งสุดท้าย นอกจากนั้นยังมีแฟ้มอื่นๆ เช่น

- /etc/security/user (IBM, 1997d) สำหรับเก็บข้อมูลต่างๆของผู้ใช้ เช่น
  - account_locked คือ การอนุญาตหรือไม่อนุญาตให้บันทึกเข้า
  - expires คือ วันที่หมดอายุการใช้งานของบัญชีผู้ใช้
  - logintimes คือ วันและเวลาที่อนุญาตให้บันทึกเข้า
  - loginretries คือ จำนวนครั้งที่อนุญาตให้บันทึกเข้าผิดติดต่อกัน
  - maxage คือ อายุการใช้งานของรหัสผ่าน
  - maxexpired คือ จำนวนวันหลังจากหมดอายุการใช้งานรหัสผ่าน หากพ้นจำนวนวันนี้แล้วบัญชีผู้ใช้จะถูกปิดทาง (disable) ไม่ให้ใช้งาน
  - minage คือ จำนวนวันหลังจากเปลี่ยนรหัสผ่านครั้งล่าสุดที่จะอนุญาตให้เปลี่ยนรหัสผ่านได้
  - pwdwarntime คือ จำนวนวันก่อนหมดอายุการใช้งานรหัสผ่านที่จะเริ่มมีการเตือน

  ฯลฯ
- /etc/security/lastlog (IBM, 1997c) สำหรับเก็บข้อมูลของการบันทึกเข้าครั้งสุดท้ายเช่น
  - unsuccessful_login_count คือ จำนวนครั้งในการบันทึกเข้าผิดพลาดติดต่อกัน

  ฯลฯ

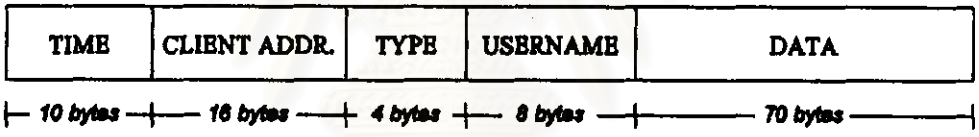
สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

2.3 ระบบรหัสผ่านแบบใช้ครั้งเดียวของจุฬาลงกรณ์มหาวิทยาลัย(พิษณุ เกริกอำไพสุรกิจ, 2539)

ระบบรหัสผ่านแบบใช้ครั้งเดียวของจุฬาลงกรณ์มหาวิทยาลัยเป็นระบบรักษาความปลอดภัยที่ถูกพัฒนาขึ้นโดย พิษณุ เกริกอำไพสุรกิจ ในปี พ.ศ. 2539 เพื่อให้รหัสผ่านรหัสผ่านที่ถูกลักลอบนำไปใช้โดยผู้ใช้อื่นไม่สามารถนำกลับมาใช้ในการเข้าสู่ระบบครั้งต่อไปได้

2.3.1 รูปแบบในการติดต่อสื่อสาร

เนื่องจากระบบรหัสผ่านแบบใช้ครั้งเดียวจะต้องประกอบด้วย 2 ส่วนดังที่กล่าวมาแล้วจึงต้องมีการติดต่อสื่อสารกันระหว่างทั้ง 2 ส่วน โดยโพรโทคอลที่ใช้ในการติดต่อสื่อสารคือ โพรโทคอลทีซีพี/ไอพี และใช้ช่องทาง (port) สื่อสารหมายเลข 6669 ในการติดต่อสื่อสาร



รูปที่ 2.2 แสดงรูปแบบของกลุ่มข้อมูลในการติดต่อสื่อสาร

TYPE คือ ชนิดของกลุ่มข้อมูล

- PASSWD หมายถึง กลุ่มข้อมูลชนิดรหัสผ่าน
- RESULT หมายถึง กลุ่มข้อมูลชนิดผลลัพธ์
- ERROR หมายถึง เกิดความผิดพลาดในการติดต่อสื่อสาร
- SEND_SUCCESS หมายถึง มีการเปลี่ยนแปลงลำดับรหัสผ่านอย่างถูกต้อง

DATA คือ ข้อมูล ที่ส่งระหว่าง โปรแกรมให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียว และ โปรแกรมบนระบบยูนิกซ์

- PASSWORD ส่งจาก โปรแกรมบนระบบยูนิกซ์ ไปยัง โปรแกรมให้บริการตรวจสอบรหัสผ่านแบบใช้ครั้งเดียวเพื่อทำการตรวจสอบว่าถูกต้องหรือไม่