รายการอ้างอิง

1. พิษณุ เกริกอำไพสุรกิจ. **ระบบรหัสผ่านแบบใช้ครั้งเดียวสำหรับระบบยูนิกซ์**. วิทยานิพนธ์ปริญญามหาบัณฑิตภาควิชาวิศวกรรมศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2538.
2. ราชบัณฑิตยสถาน. **ศัพท์คอมพิวเตอร์ ฉบับราชบัณฑิตยสถาน**. กรุงเทพมหานคร : โรงพิมพ์มหาจุฬาลงกรณราชวิทยาลัย, 2540.
3. Bruce Schneier. **Applied Cryptography Protocols, Algorithms and Source Code in C**. U.S.A. : John Wiley & Sons, Inc., 1994.
4. Charlie Kaufman, Radia Perlman, Mike Speciner. **Network Security Private Communication in a PUBLIC World**. New Jersey : Prentice-Hall, Inc., 1995.
5. Chris Hare, Karanjit Siyan. **Internet Firewalls and Network Security**. Indianapolis, U.S.A. : New Rider Publishing, 1996.
6. Larry J. Hughes, Jr. **Actually Usefull Internet Security Techniques**. Indianapolis, U.S.A. : New Rider Publishing, 1995.
7. William Stallings. **Cryptography and Network Security Principles and Practice**. New Jersey : Prentice Hall International, Inc., 1999.
8. David A. Curry. **UNIX Systems Programming**. CA : O'Reilly & Associates, Inc., 1996.
9. W. Richard Stevens. **UNIX Network Programming**. Singapore : Prentic-Hall International, Inc., 1994.

ภาคผนวก ก.

คู่มือการติดตั้งระบบ

ก.1 การติดตั้งโปรแกรมเอสเอสแอลอีเอวาย รุ่น 0.6.6 b

ก.1.1 บรรจุลง (download) โปรแกรมจาก ยูอาร์แอล (URL : Universal Resource Locator)

ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/SSLeay-0.6.6b.tar.gz

ก.1.2 ขยายออก (unpack) แฟ้มข้อมูล SSLeay-0.6.6b.tar.gz ด้วยคำสั่ง zcat และ tar ดังนี้

```
$ zcat SSLeay-0.6.6b.tar.gz | tar xvf -
```

ซึ่งจะได้แฟ้มข้อมูลที่ขยายออกมาทั้งหมดอยู่ภายใต้ไดเรกทรอรี "SSLeay-0.6.6b"

ก.1.3 กำหนดเส้นทางไดเรกทรอรีที่อ่านโปรแกรม "perl" เช่น ถ้าโปรแกรม "perl" เก็บอยู่ที่ไดเรกทรอรี "/usr/bin" ให้คีย์คำสั่งดังนี้

```
$ perl util/perlpath.pl /usr/bin
```

ก.1.4 กำหนดตำแหน่งไดเรกทรอรีที่ใช้ลงโปรแกรม เช่น ถ้ากำหนดให้โปรแกรมเอสเอสแอลอีเอวายถูกเก็บอยู่ภายใต้ไดเรกทรอรี "/usr/local/ssl" ให้คีย์คำสั่งดังนี้

```
$ perl util/ssldir.pl /usr/local/ssl
```

ก.1.5 สร้างลิงค์ไฟล์ (link file) ด้วยคำสั่ง

```
$ make  -f Makefile.ssl links
```

ก.1.6 ปรับแต่งบทคำสั่ง (script) การแปลโปรแกรม (compile) ตามประเภทของระบบปฏิบัติการและฮาร์ดแวร์ที่ใช้ ในที่นี้ใช้ระบบปฏิบัติการลินุกซ์ ดังนั้นคำสั่งที่ใช้คือ

```
$ ./Configure 'linux  -elf'
```

ก.1.7 ทำการแปลโปรแกรม (compile) ตามขั้นตอนดังนี้

```
$ make clear
$ make
$ make rehash
$ make test
```

ก.1.8 ติดตั้งโปรแกรมเอสเอสแอลอีเอวาย โดยขั้นตอนนี้จะต้องใช้สิทธิของ “root” ในการติดตั้ง

```
$ su
# make install
```

ก.2 การสร้างชุดคีย์สาธารณะ

ชุดคีย์สาธารณะจะถูกแยกออก 2 ส่วนคือ

- คีย์ส่วนตัว (private key)
- ใบคำร้องขอใบรับรอง (request) ซึ่งจะประกอบด้วยชื่อผู้ขอใบรับรองและคีย์สาธารณะของผู้ขอ

การสร้างชุดคีย์ดังกล่าวสามารถทำได้ด้วยคำสั่ง “ssleay” ที่ได้จากการติดตั้งโปรแกรมเอสเอสแอลอีเอวาย ดังนี้

```
$ ssleay reg  -new  -keyout <keyfile.pem>  -out <reqfile.pem>
```

ความหมายของทางเลือก (options)

-new	สร้างใบคำร้องขอใบรับรอง
-keyout <keyfile.pem>	กำหนดชื่อแฟ้มข้อมูลที่ใช้เก็บคีย์ส่วนตัวที่มีนามสกุลเป็น “.pem”
-out <reqfile.pem>	กำหนดชื่อแฟ้มข้อมูลที่ใช้เก็บใบคำร้องขอใบรับรองที่มีนามสกุลเป็น “.pem”

ชุดคีย์สาธารณะที่ได้เป็นชุดคีย์สาธารณะที่ใช้วิธีการเข้ารหัสแบบอาร์เอสเอ (RSA : Rivest, Shamir, and Adleman) โดยแฟ้มข้อมูลคีย์ส่วนตัวที่ได้จะถูกเก็บเป็นความลับด้วยการเข้ารหัสแบบดีอีเอส (DES : Data Encryption Standard) ส่วนใบคำร้องขอใบรับรองจะถูกส่งให้ผู้ออกใบรับรองทำการลงลายเซ็นอิเล็กทรอนิกส์ออกเป็นใบรับรอง

ก.3 การติดตั้งระบบบริหารใบรับรองและออกใบรับรอง

หลังจากการติดตั้งโปรแกรมเอสเอสแอลอีเอวายแล้ว เราจะได้ชุดโปรแกรมสำหรับบริหารใบรับรองขั้นพื้นฐานมาพร้อมกัน ซึ่งชุดโปรแกรมดังกล่าวถูกติดตั้งลงบนเครื่องออกใบรับรอง โดยมีขั้นตอนดังนี้

ก.3.1 ติดตั้งชุดโปรแกรมบริหารใบรับรอง

```
$ CA .sh  -newca
```

คำสั่งนี้จะสร้างไดเรกทรอรีชื่อ “demoCA” ภายใต้ไดเรกทรอรีปัจจุบัน พร้อมติดตั้งแฟ้มข้อมูลต่างๆ ที่ใช้ในการออกใบรับรอง

ก.3.2 สร้างคีย์ส่วนตัวและใบรับรองของผู้อกใบรับรอง

```
$ ssleay req   -new   -X509  -keyout ./demoCA/private/cakey.pem
                  -out ./demoCA/cacert.pem
```

ความหมายของทางเลือก (options)

-X509 กำหนดให้ใช้โครงสร้างการเก็บใบรับรองเป็นแบบ X509

คำสั่งนี้จะสร้างแฟ้มข้อมูลคีย์ส่วนตัวของผู้ออกใบรับรอง ชื่อ “cakey.pem” ภายใต้ไดเรกทรอรี “./demoCA/private” และแฟ้มข้อมูลใบรับรองของผู้ออกใบรับรองชื่อ “cacert.pem” ภายใต้ไดเรกทรอรี “./demoCA”

ก.3.3 การลงลายเซ็นอิเล็กทรอนิกส์บนใบคำร้องขอใบรับรอง

```
$ ssleay  ca   -policy   policy_anything  -out <certfile.pem>  -infiles <reqfile.pem>
```

ความหมายของทางเลือก (options)

-policy <policyname>	กำหนดนโยบายในการออกใบรับรอง
-out <certfile.pem>	กำหนดชื่อแฟ้มข้อมูลที่ใช้เก็บใบรับรองที่ผ่านการลงลายเซ็นอิเล็กทรอนิกส์
-infiles <reqfile.pem>	กำหนดชื่อแฟ้มข้อมูลที่เก็บใบคำร้องขอใบรับรองที่ต้องการให้ผู้ออกใบรับรองลงลายเซ็นอิเล็กทรอนิกส์

คำสั่งนี้เป็นการนำเอาใบคำร้องขอใบรับรองมาลงลายเซ็นอิเล็กทรอนิกส์ เพื่อสร้างเป็นใบรับรอง

ก.4 การติดตั้งโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียว

ก.4.1 สร้างแฟ้มข้อมูลค่าเริ่มต้น (default value file) ของผู้ให้บริการชื่อ "sslserv.conf" ภายใต้ไดเรกทรอรี "/etc" ดังแสดงในรูปที่ ก.1

```
serv_port=4444
ca_path=/usr/home/anu/demoCA
ca_file=/usr/home/anu/demoCA/cacert.pem
certify=/usr/home/anu/server/servcert.pem
key_file=/usr/home/anu/server/servkey.pem
cipher=RC4-MD5
depth=0
timeout=180
debug=0
```

รูปที่ ก.1 ค่าเริ่มต้นของโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียว

ความหมายของค่าเริ่มต้น

serv_port	หมายเลขพอร์ตของโปรแกรมให้บริการรหัสผ่านแบบใช้ครั้งเดียว
ca_path	เส้นทางไดเรกทรอรีที่ใช้เก็บใบรับรองของผู้ออกใบรับรอง

ca_file	เส้นทางสมบูรณ์ของแฟ้มข้อมูลที่ใช้เก็บใบรับรองของผู้ออกใบรับรอง
key_file	เส้นทางสมบูรณ์ของแฟ้มข้อมูลที่ใช้เก็บคีย์ส่วนตัวของผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว
cipher	วิธีการเข้ารหัสและการจำแนกข้อความ (message digest)
depth	จำนวนชั้นของผู้ออกใบรับรองในการยอมรับการพิสูจน์ใบรับรอง
timeout	เวลาที่ผู้ให้บริการรอคอยการตอบสนองจากผู้ขอใช้บริการก่อนที่จะตัดการติดต่อ (หน่วยเป็นวินาที)
debug	กำหนดให้ทำงานแบบแสดงจุดบกพร่อง (debug mode)

ก.4.2 ติดตั้งใบรับรองที่ผ่านการลงลายเซ็นอิเล็กทรอนิกส์จากผู้ออกใบรับรองและใบรับรองของผู้ออกใบรับรองเองลงในชื่อแฟ้มข้อมูลและตำแหน่งไดเรกทรอรีตามที่กำหนดในค่าเริ่มต้น

ก.4.3 ติดตั้งโปรแกรม "otpserv" ภายใต้ไดเรกทรอรี "/usr/local/bin" หลังจากนั้นการสั่งให้โปรแกรม "otpserv" ดำเนินงานสามารถทำได้ 2 วิธี คือ

- สั่งให้ดำเนินงานภายใต้โปรแกรมเชลล์ (shell program)
- สั่งให้ดำเนินงานโดยอัตโนมัติด้วยการเพิ่มคำสั่งให้ดำเนินงานโปรแกรม "otpserv" ในบทคำสั่งเริ่มต้นของยูนิกซ์ (rc script)

ก.5 การติดตั้งโปรแกรมขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

ก.5.1 สร้างแฟ้มข้อมูลค่าเริ่มต้น (defalut value file) ของผู้ขอใช้บริการชื่อ "sslcli.conf" ภายใต้ไดเรกทรอรี "/etc"

```
serv_ip=199.199.199.44
serv_port=4444
serv_subj=/C=TH/SP=Bangkok/O=Chulalongkorn University/OU=Computer Engineering
Department/CN=OTPserver
ca_path=/usr/home/anu/client
ca_file=/usr/home/anu/client/cacert.pem
cipher=
depth=0
timeout=300
debug=0
```

รูปที่ ก.2 ค่าเริ่มต้นของโปรแกรมขอใช้บริการรหัสผ่านแบบใช้ครั้งเดียว

ความหมายของค่าเริ่มต้น

serv_ip	หมายเลขไอพีของผู้ให้บริการรหัสผ่านแบบใช้ครั้งเดียว
serv_subj	ชื่อเจ้าของใบรับรองของผู้ให้บริการรหัสผ่านตัวจริง

ก.5.2 ติดตั้งใบรับรองของผู้ออกใบรับรองลงในชื่อแฟ้มข้อมูลและตำแหน่งไดเรกทรอรีที่กำหนดในค่าเริ่มต้น

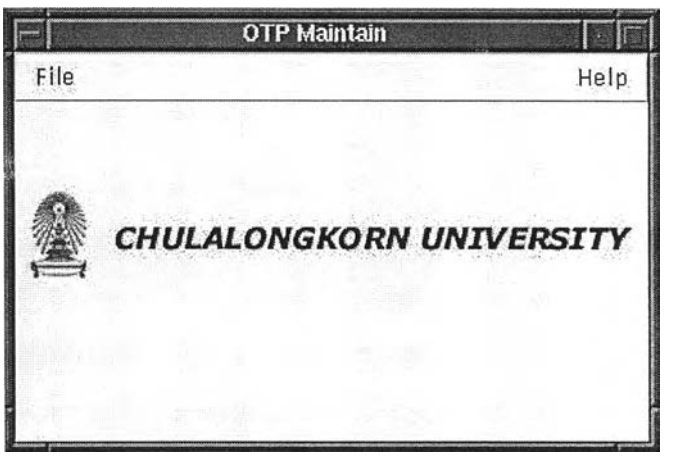
ก.5.3 ติดตั้งโปรแกรม “otpcli” แทนที่โปรแกรม login ในไดเรกทรอรี “/bin”

ภาคผนวก ข.

คู่มือการใช้โปรแกรมบำรุงรักษาฐานข้อมูลรหัสผ่านแบบใช้ครั้งเดียว

ข.1 การเรียกโปรแกรมบำรุงรักษาฐานข้อมูล

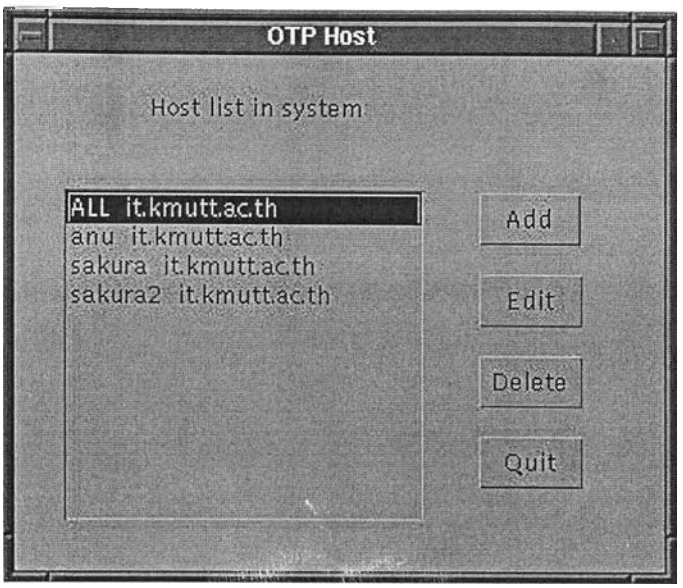
$ java MainFrame -H 127.0.0.1



รูปที่ ข.1 หน้าต่างหลักของโปรแกรมบำรุงรักษาฐานข้อมูลรหัสผ่าน

ข.2 การลงทะเบียนเครื่องแม่ข่ายยูนิกซ์

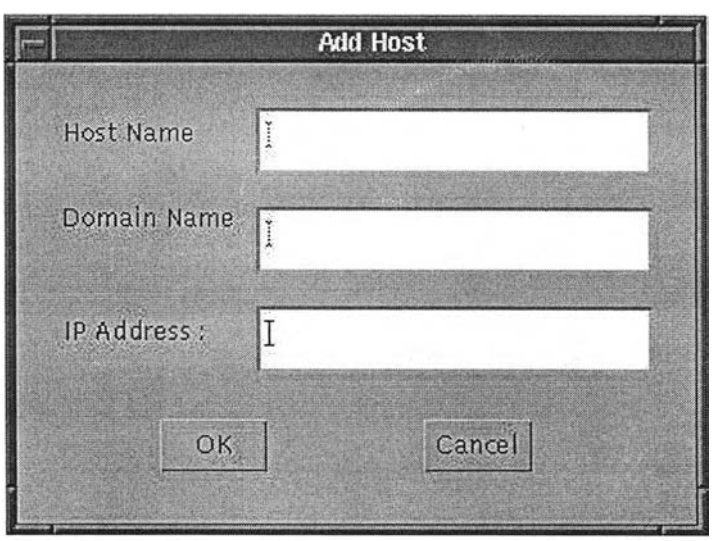
- เลือกเมนู File → Host จากหน้าต่างหลัก



รูปที่ ข.2 หน้าต่างการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์

ข.2.1 การเพิ่มเครื่องแม่ข่ายยูนิกซ์ในระบบทะเบียน

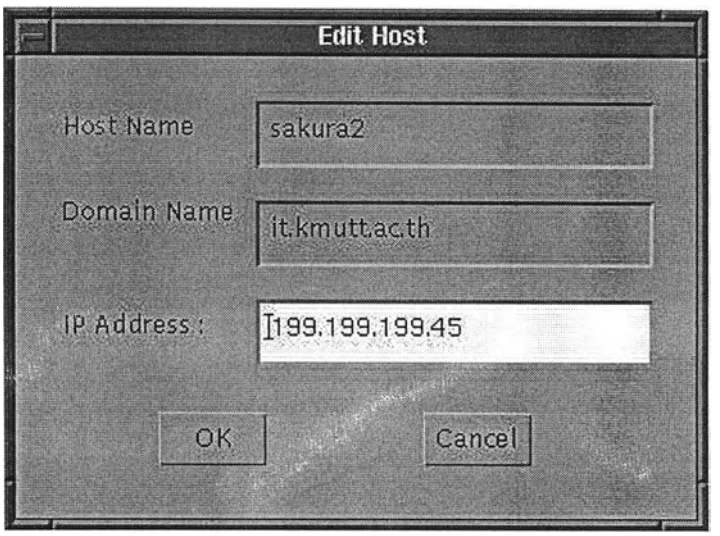
- กดปุ่ม Add ในหน้าต่างการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์ รูปที่ ข.2



รูปที่ ข.3 หน้าต่างการเพิ่มเครื่องแม่ข่ายยูนิกซ์

ข.2.2 การแก้ไขข้อมูลเครื่องแม่ข่ายยูนิกซ์

- กดปุ่ม Edit ในหน้าต่างการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์ รูปที่ ข.2



รูปที่ ข.4 หน้าต่างการแก้ไขเครื่องแม่ข่ายยูนิกซ์

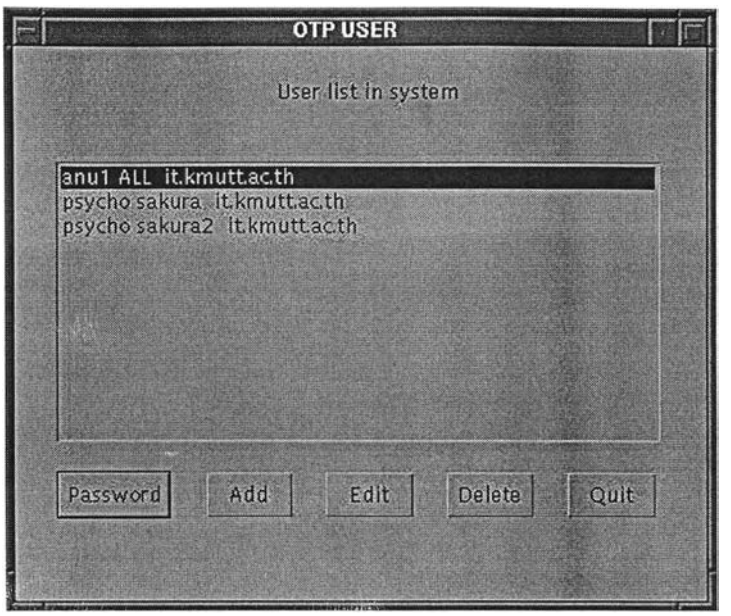
ข.2.3 การลบเครื่องแม่ข่ายยูนิกซ์ออกจากระบบทะเบียน

ในหน้าต่างการลงทะเบียนเครื่องแม่ข่ายยูนิกซ์ รูปที่ ข.2

- เลือกรายการเครื่องแม่ข่ายที่ต้องการลบ
- กดปุ่ม Delete

ข.3 การจัดการข้อมูลบัญชีผู้ใช้

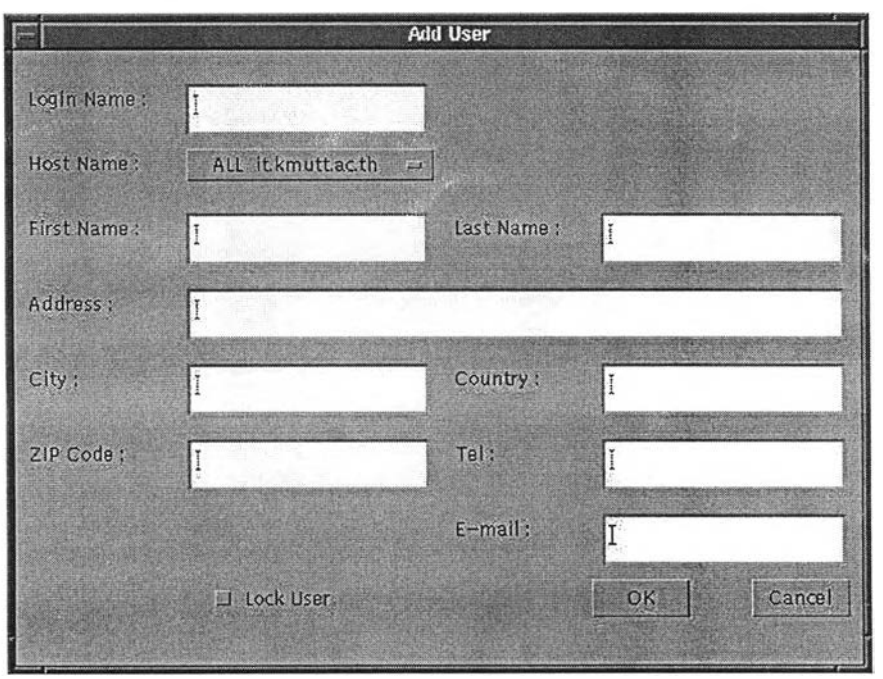
- เลือกเมนู File → User ในหน้าต่างหลัก รูปที่ ข.1



รูปที่ ข.5 หน้าต่างการจัดการข้อมูลบัญชีผู้ใช้

ข.3.1 การเพิ่มข้อมูลบัญชีผู้ใช้

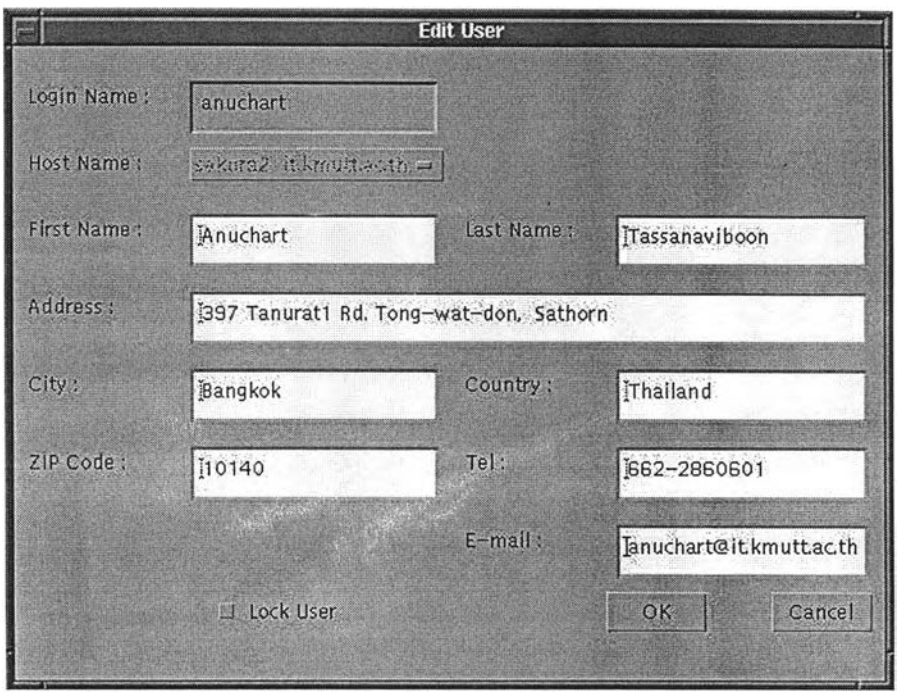
– กดปุ่ม Add ในหน้าต่างการจัดการข้อมูลบัญชีผู้ใช้ รูปที่ ข.5



รูปที่ ข.6 หน้าต่างการเพิ่มข้อมูลบัญชีผู้ใช้

ข.3.2 การแก้ไขข้อมูลบัญชีผู้ใช้

- กดปุ่ม Edit ในหน้าต่างการจัดการข้อมูลบัญชีผู้ใช้ รูปที่ ข.5



รูปที่ ข.7 หน้าต่างการแก้ไขข้อมูลบัญชีผู้ใช้

ข.3.3 การลบข้อมูลบัญชีผู้ใช้

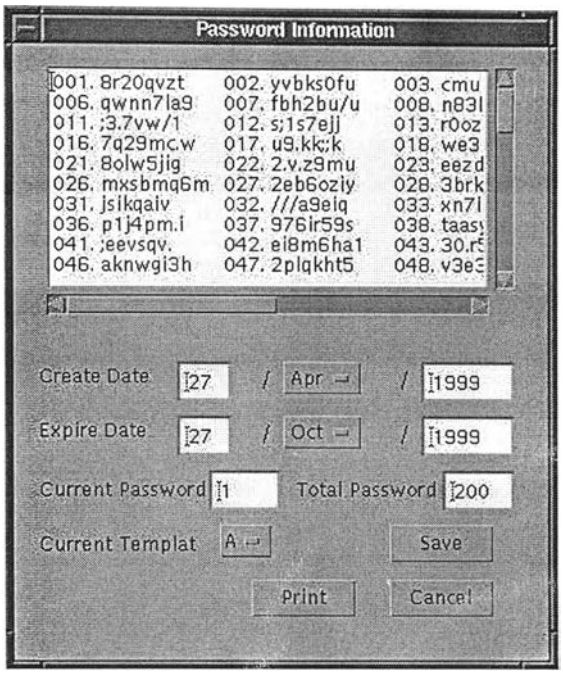
ในหน้าต่างการจัดการข้อมูลบัญชีผู้ใช้ รูปที่ ข.5

- เลือกรายการบัญชีผู้ใช้ที่ต้องการลบ
- กดปุ่ม Delete

ข.3.4 การจัดการข้อมูลรหัสผ่านของผู้ใช้

ในหน้าต่างการจัดการข้อมูลบัญชีผู้ใช้ รูปที่ ข.5

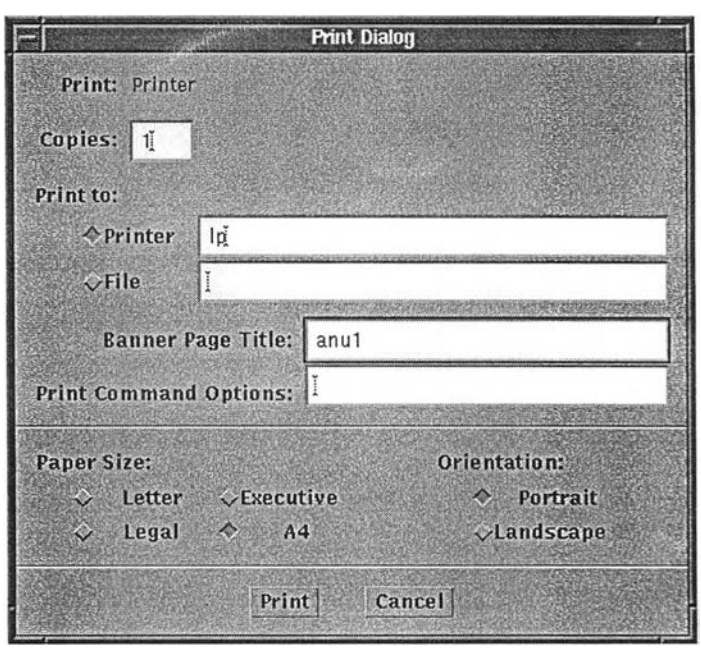
- เลือกรายการบัญชีผู้ใช้ที่ต้องการ
- กดปุ่ม Password



รูปที่ ข.8 หน้าต่างการจัดการข้อมูลรหัสผ่าน

ข.3.4.1 การพิมพ์ใบรายงานรหัสผ่าน

- กดปุ่ม Print ในหน้าต่างการจัดการข้อมูลรหัสผ่าน รูปที่ ข.8



รูปที่ ข.9 หน้าต่างการพิมพ์ใบรายงานรหัสผ่าน

ประวัติผู้วิจัย

นาย อนุชาติ ทัศนวิบูลย์ เกิดเมื่อวันที่ 23 สิงหาคม พ.ศ. 2507 จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีวิศวกรรมศาสตรบัณฑิต (วิศวกรรมไฟฟ้า) คณะวิศวกรรมศาสตร์ จากสถาบันเทคโนโลยีพระจอมเกล้าธนบุรี เมื่อปีการศึกษา 2531 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต ที่จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2538 ปัจจุบันทำงานที่มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี