บทที่ 4

สรุปแนวทางการออกแบบและการพิสูจน์ระบบงาน

4.1 โมดูลในการป้องกันผู้ใช้พิเศษ

โมดูลนี้สามารถบันทึกรายการการตรวจสอบในการกระทำที่เกิดจากผู้ใช้พิเศษหรือรูทของระบบ รวมทั้งเป็นการสร้างเส้นทางการไว้ใจได้ของการเข้าใช้งานของผู้ดูแลระบบ

แนวทางการพิสูจน์

1. กำหนดข้อมูลในไฟล์ /etc/securettys ให้มีค่าดังนี้ /dev/console หมายถึง ถ้าจะเข้าสู่ระบบโดยการเป็นรูท (root) ให้เข้าได้ที่คอลโซลเท่านั้น

2. กำหนดให้คำสั่งrunacct ทำงานเพื่อเป็นการเก็บคำสั่งที่ผู้ใช้ทั้งหมดในระบบสั่งทำงาน ซึ่งผลของการใช้คำสั่งจะมีการจัดเก็บไว้ที่ /var/adm/pacct และต้องใช้คำสั่ง lastcomm ในการเรียกดู

3. กำหนดรายชื่อผู้ใช้ที่สามารถทำหน้าที่เป็นรูทได้ ไว้ในไฟล์ /etc/group โดยระบุให้มีชื่อที่กลุ่ม system เช่นตัวอย่างในไฟล์ /etc/group มีดังนี้

```
system:*:0:root,took
```

หมายถึง กำหนดสิทธิให้ผู้ใช้ชื่อ took สามารถใช้คำสั่ง su ในการเป็นรูทได้

4. สร้างคำสั่งเสมือน (alias)ของคำสั่ง /bin/su ด้วยคำสั่ง /bin/su - เพื่อต้องการให้ผู้ใช้ที่ใช้ คำสั่ง su แล้วมาทำงานภายใต้สภาวะแวดล้อม ของรูท เช่นมาทำงานภายใต้คำสั่งที่อยู่ใน /.profile

5. กำหนดให้คำสั่งใน /.profile ทำงานดังต่อไปนี้

5.1 เมื่อ su เข้ามาแล้ว ให้ใช้คำสั่ง echo $LOGNAME ภายในเวลา 10 วินาที มิฉะนั้นจะถูกให้ล็อคเอาท์ออกจากการเป็นรูทและมีข้อความมาเตือนที่หน้าจอคอลโซลว่า ขณะนี้มีการ su ได้สำเร็จโดยเป็นรูทปลอม และมีการบันทึกไว้ว่าใครเป็นผู้ su และพยายามจะใช้คำสั่งอะไรมาทำอะไรในระบบ แต่ถ้า echo แล้วให้ทำงานภายใต้สภาวะของรูทได้ตามปกติ ตัวอย่างในไฟล์ /var/adm/sialog เมื่อเข้าสู่ระบบจากนั้น su ได้สำเร็จ จะมีการบันทึกไว้ดังนี้

```
SIA:EVENT Mon Sep 16 20:20:40 1996
Successful authentication for took on /dev/ttyp4
SIA:EVENT Mon Sep 16 20:20:42 1996
Successful authentication for su from took to root
```

พร้อมกับมีการบันทึกไว้ที่ไฟล์ /var/adm/syslog.dated/16-SEP-12:00/auth.log ดังนี้

```
Sep 16 20:20:42 kmitnb04 su: su took on /dev/ttyp4
```

และในไฟล์ /var/adm/syslog.dated/16-SEP-12:00/daemon.log จะเก็บข้อมูลไว้ดังนี้

```
Sep 16 20:20:40 kmitnb04 netacl[2713]:permit host=unknow/202.44.41.9
service=telnetd  execute=/usr/sbin/telnetd
```

เป็นการอ้างอิงได้ว่า มีผู้ใช้ชื่อ took เข้าสู่ระบบจากเครื่องที่มีหมายเลขไอพีแอสเดรส 202.44.41.9 ถ้าผู้ใช้ชื่อ took ไม่สั่ง echo $LOGNAME ภายใน 10 วินาที จะให้มีการเก็บบันทึกลงในไฟล์ /var/adm/fsu.log พร้อมทั้งแสดงที่หน้าจอคอลโซล โดยให้มีข้อมูลดังนี้

```
Sep 16 20:20:40 kmitnb04 netacl[2713]:permit host=unknow/202.44.41.9
service=telnetd  execute=/usr/sbin/telnetd
SIA:EVENT Mon Sep 16 20:20:42 1996
Successful authentication for su from took to root
```

5.2 จากนั้นให้มีการสั่ง `echo exit | cat >> ~took/.profile` เพื่อที่ ถ้าผู้ใช้ชื่อ took จะล็อกอินเข้าสู่ระบบอีกครั้ง ก็จะถูกสั่งให้ออกทันที

5.3 ถ้า su แล้วไม่สั่ง echo และพยายามใช้คำสั่งในกลุ่มต่อไปนี้

cat .profile more .profile pg .profile lpr .profile vi .profile rm .profile mv .profile <fn> cp .profile <fn> cp <fn> .profile chmod .profile chgrp .profile chown .profile จะทำการนำไฟล์ .profile ของปลอมขึ้นมาให้ถูกกระทำแทน หรือ ถ้าสั่งคำสั่ง passwd , rm .... จะไม่ยอมให้คำสั่งเหล่านี้ทำงานได้

4.2 โมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ

โมดูลนี้สนับสนุนในเรื่องของนโยบายความมั่นคง ในด้านการควบคุมการเข้าถึงโดยใช้ดุลยพินิจ และการชี้แจงรายการในเรื่องของการพิสูจน์ตนและการแสดงตน มีเส้นทางการไว้ใจได้ในการเข้าสู่ระบบ และมีการบันทึกในรายการตรวจสอบ

แนวทางการพิสูจน์

ให้มีการสร้างโปรแกรมที่ทำงานตลอดเวลา ในการตรวจสอบการใช้งานที่พอร์ท เทลเนต เพื่อตรวจดูว่า มีโปรเซสอื่น มาใช้งานที่พอร์ทนี้หรือไม่ เมื่อมีผู้ใช้เข้ามาใช้งาน ก็จะทำงานตามโมดูลในผังงาน ตามรูปที่ 3.2 ซึ่งทำให้สามารถตรวจสอบจากไฟล์ที่เก็บรายการตรวจสอบได้ว่าผู้ใช้ใดหรือโปรเซสใดกำลังจะละเมิดความมั่นคงของระบบ

4.3 โมดูลในการตรวจสอบระบบ

โมดูลนี้ชี้แจงการจัดเก็บรายการตรวจสอบต่าง ๆ ที่สามารถบันทึกได้ในระบบปฏิบัติการโอเอสเอฟวัน รวมทั้งการแก้ไขปัญหาถ้าเนื้อที่ในการจัดเก็บรายการตรวจสอบเต็ม

4.4 โมดูลในการควบคุมการใช้งานในระบบ

โมดูลนี้ใช้ควบคุมการกระทำต่าง ๆ ในการใช้งานในระบบ โดยอาศัยเกณฑ์ในเรื่องของป้ายชื่อมาใช้ ได้แก่การสร้างความเป็นเอกภาพของป้ายชื่อ การส่งออกข้อมูลที่มีป้ายชื่อ ทั้งการส่งออกไปที่อุปกรณ์หลายระดับและอุปกรณ์ระดับเดียว การจัดการป้ายชื่อของสิ่งพิมพ์ การกำหนดป้ายความไหวของตัวกระทำและป้ายชื่ออุปกรณ์ รวมทั้งการควบคุมการเข้าถึงภายใต้อาณัติ

แนวทางการพิสูจน์

การควบคุมการอ่านและการเขียน โดยมีการแบ่งระดับความมั่นคงของตัวถูกกระทำ รวมทั้งมีการระบุกลุ่มของขอบเขตในการเข้าถึงข้อมูลนั้น สามารถใช้แบบจำลองของการไหลของข้อมูล คือ แบบจำลองเบลลาปาดูลา (Bell-LaPadula Model) มาอธิบายได้

4.5 โมดูลในการแสดงตนและการพิสูจน์ตน

โมดูลนี้เขียนเป็นแนวทางการสร้างความมั่นคงในด้านการแสดงตนและการพิสูจน์ตน เป็นแนวทางการทำงานของผู้ดูแลระบบหรือผู้ดูแลด้านความมั่นคง รวมทั้งผู้ใช้ในระบบ

4.6 โมดูลในการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ

โมดูลนี้เขียนเป็นแนวทางการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ ตามเกณฑ์ของคุณสมบัติด้านความมั่นคงในด้านต่าง ๆ โดยมีการแยกหน้าที่กันของผู้ดูแลระบบกับผู้ดูแลด้านความมั่นคงของระบบ และหน้าที่ของผู้ปฏิบัติงาน

4.7 โมดูลในการจัดการระบบหลังการล้มเหลว

โมดูลนี้เขียนเป็นแนวทางการจัดการระบบหลังการล้มเหลว เป็นแนวทางการทำงานในการป้องกันถ้าหากต้องทำการฟื้นฟูระบบ

4.8 โมดูลในการทดสอบระบบ

โมดูลนี้เขียนเป็นแนวทาง การทดสอบระบบ และแนวทางของเอกสารที่ใช้ในการทดสอบรวมถึงคำสั่งที่ใช้ทดสอบหรือตรวจสอบไฟล์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงบนระบบปฏิบัติการโอเอสเอฟวัน

4.9 โมดูลในการออกแบบลักษณะเฉพาะและทำการพิสูจน์

โมดูลนี้เขียนเป็นแนวทาง ในการออกแบบลักษณะเฉพาะและทำการพิสูจน์ รวมถึงแนวทางการสร้างเอกสารการออกแบบในระบบที่ไว้ใจได้

4.10 โมดูลในการออกแบบการจัดการสัณฐาน

โมดูลนี้เขียนเป็นแนวทางในการออกแบบการจัดการสัณฐานของระบบ

4.11 โมดูลในการออกแบบสถาปัตยกรรมของระบบ

โมดูลนี้เขียนเป็นแนวทางของการออกแบบสถาปัตยกรรมของระบบปฏิบัติการถ้าต้องการให้มีความมั่นคงในระดับขั้น B3

4.12 โมดูลในการออกแบบการวิเคราะห์ช่องทางลับ

โมดูลนี้ ใช้เป็นแนวทางในการป้องกันช่องทางลับที่มีอยู่ในระบบได้ในระดับหนึ่ง