บทที่ 3

การออกแบบระบบ

เนื่องจากความต้องการด้านการติดต่อสื่อสารระหว่างคอมพิวเตอร์ ซึ่งมีการเชื่อมต่อกันเป็นเครือข่ายนั้น การออกแบบความมั่นคงเฉพาะของระบบปฏิบัติการโอเอสเอฟวัน ย่อมไม่เพียงพอต่อการป้องกัน และแก้ปัญหาด้านความมั่นคง เนื่องจากการคุกคามอาจเกิดมาจากภายนอก ซึ่งระดับการป้องกันจะต้องป้องกันในระดับของการสื่อสาร ดังนั้นการออกแแบบจะถูกแบ่งเป็น 2 ส่วนคือ

- ส่วนที่เกี่ยวกับระบบโดยตรง
- ส่วนที่เกี่ยวข้องกับหน้าที่ของผู้บริหารระบบหรือผู้ดูแลด้านความมั่นคงของระบบ

3.1 การออกแบบโมดูลที่เกี่ยวกับระบบโดยตรง

3.1.1 การออกแบบโมดูลในการป้องกันผู้ใช้พิเศษ

โมดูลนี้ออกแบบเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้าน การตรวจสอบและการสร้างเส้นทางไว้ใจได้

<u>วัตถุประสงค์</u>

เนื่องจากผู้ใช้พิเศษหรือรูท (root) จะเป็นผู้ที่มีอภิสิทธิมากที่สุดในระบบ เพราะฉะนั้น นักเจาะระบบทั้งหลาย นิยมที่จะเจาะรหัสผ่านของผู้ใช้พิเศษนี้ จึงจำเป็นต้องมีมาตรการในการป้องกันระบบ ถ้ารหัสผ่านของผู้ใช้พิเศษนี้รั่วไหล ผู้ดูแลระบบจะต้องรู้และ สามารถป้องกันการเสียหายที่อาจเกิดจากการปลอมแปลงเป็นรูท โดยนักเจาะระบบเข้ามาได้สำเร็จ

<u>ปัญหาที่พบ</u>

พวกนักเจาะระบบพยายามที่จะล็อกอินเข้าสู่ระบบ โดยใช้รหัสบัญชีชื่อ รูท โดยตรงหรือใช้คำสั่ง su ในการเป็นรูท แล้วใส่รหัสผ่าน รหัสผ่านของรูท ที่รั่วไหล อาจเกิดจากหลายสาเหตุด้วยกัน เช่น

- ในกรณีที่มีผู้บริหารระบบอยู่หลายคน เมื่อมีการเปลี่ยนรหัสผ่านของรูท จะต้องมีการแจ้งให้ผู้บริหารระบบทุกคนทราบ โดยวิธีการแจ้ง อาจใช้การส่งจดหมายอิเล็คทรอนิกส์ วิธีนี้มีจุดอ่อนที่ จดหมายนี้จะถูกส่งไปในเครือข่าย และระหว่างเส้นทางในเครือข่าย อาจมีโปรแกรมกับดักประเภทตรวจสอบหัวจดหมายวางอยู่ เมื่อโปรแกรมนี้ตรวจสอบที่หัวจดหมายและพบคำเกี่ยวกับ 'รหัสผ่าน' ก็จะทำการเปิดจดหมายนั้น โดยทั้งที่ผู้รับและผู้ส่งไม่ทราบว่าจดหมายนี้ได้รั่วไหลแล้ว

- เกิดจากการตั้งรหัสผ่านของรูท ไม่ดี เช่นใช้คำศัพท์ที่มีความหมาย ซึ่งสามารถใช้โปรแกรมแกะรหัสผ่านได้ง่าย โดยอาศัยคำศัพท์จากพจนานุกรม หรือใช้ชื่อหรือข้อมูลส่วนตัวของผู้ดูแลระบบ ซึ่งสามารถเดาได้ง่าย

<u>แนวทางการออกแบบการป้องกันและการแก้ไข</u>

เนื่องจากรูท มีสิทธิทุกอย่างในระบบ แม้กระทั่งการลบร่องรอยการตรวจสอบของระบบ เพราะฉะนั้นจำเป็นต้องมีการตั้งนโยบายด้านความมั่นคง ของการใช้รหัสผู้ใช้พิเศษนี้ในองค์กรขึ้นเอง โดยอาจกำหนดเป็นแนวทางได้ดังนี้

1. ระบุให้ผู้ใช้พิเศษ หรือรูทนี้สามารถล็อกอินเข้าสู่ระบบได้โดยตรงเฉพาะที่คอลโซลเท่านั้น นอกนั้นถ้าจะเป็นผู้ใช้พิเศษให้ใช้คำสั่ง su ที่เทอร์มินอลเข้ามาได้ โดยที่ระบบปฏิบัติการโอเอสเอฟวันนี้ มีไฟล์ที่เก็บว่าสามารถล็อกอินรูทได้ที่ใดบ้าง อยู่ที่ไฟล์ /etc/securettys และมีไฟล์ที่เก็บการล็อกอินและการ su อยู่ที่ไฟล์ /var/adm/sialog

ตัวอย่างไฟล์ /etc/securettys

```
/dev/console
```

หมายถึงระบุให้ รูท ล็อกอินได้โดยตรงที่คอลโซลเท่านั้น

ตัวอย่างไฟล์ /var/adm/sialog

```
บรรทัดที่ 1: SIA:EVENT Thu Sep 12  13:17:13 1996
บรรทัดที่ 2: Successful session authentication for root on /dev/console
บรรทัดที่ 3: SIA:EVENT Mon Sep 16 20:20:42 1996
บรรทัดที่ 4: Successful authentication for su from took to root
บรรทัดที่ 5: SIA:ERROR Thu Sep  19 15:30:20 1996
บรรทัดที่ 6: Failure on authentication for su from field to root
```

จากตัวอย่าง

บรรทัดที่ 1-2 แสดงว่า รูทสามารถล็อกอินได้สำเร็จที่คอนโซล ณ วันพฤหัสที่ 12 กย. (ปี คศ. 1996) เวลา 13.17 น.

บรรทัดที่ 3-4 แสดงว่า รหัสผู้ใช้ที่ชื่อ took สามารถ su เป็นรูทได้สำเร็จ ณ วันจันทร์ที่ 16 กย. เวลา 20.20 น.

บรรทัดที่ 5-6 แสดงว่า รหัสผู้ใช้ที่ชื่อ field พยายาม su เป็นรูท แต่ไม่สำเร็จ ณ วันที่ 19 กย. เวลา 15.30 น.

2. กำหนดให้คำสั่ง su ในระบบเป็น su - เสมอ เพื่อที่เวลาเรียกใช้คำสั่ง su แล้วจะได้ทำงาน ภายใต้สภาพแวดล้อมของรูท ซึ่งในที่นี้ต้องการให้ su แล้วมาทำงานตามคำสั่งที่กำหนดไว้ที่ไฟล์ /.profile ของรูท

3. กำหนดให้คำสั่งใน /.profile ทำงานดังต่อไปนี้

- เมื่อ su เข้ามาแล้ว ให้ใช้คำสั่ง echo $LOGNAME ภายในเวลา 10 วินาที มิฉะนั้นจะถูกให้ล็อกเอาท์ออกจากการเป็นรูทและมีข้อความมาเตือนที่หน้าจอคอลโซลว่า ขณะนี้มีการ su ได้สำเร็จโดยเป็นรูทปลอม และมีการบันทึกไว้ว่าใครเป็นผู้ su และพยายามจะใช้คำสั่งอะไรมาทำอะไรในระบบ แต่ถ้า echo แล้วให้ทำงานภายใต้สภาวะของรูทได้ตามปกติ

- ถ้า su แล้วไม่สั่ง echo และพยายามใช้คำสั่งในกลุ่มต่อไปนี้

cat .profile more .profile pg .profile lpr .profile vi .profile

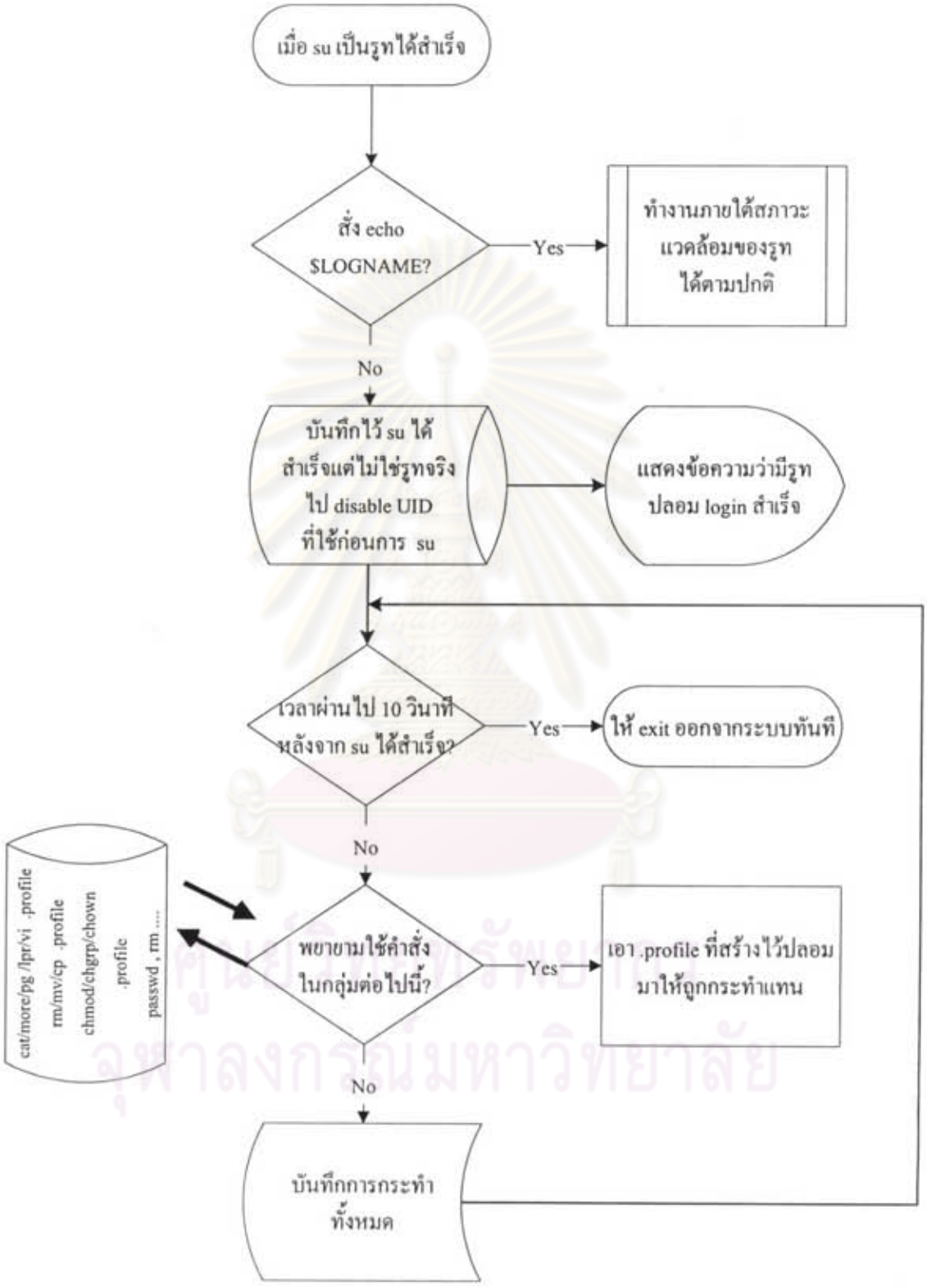
rm .profile mv .profile cp .profile <fn> cp <fn> .profile

chmod .profile chgrp .profile chown .profile

จะทำการนำไฟล์ .profile ของปลอมขึ้นมาให้ถูกกระทำแทน

หรือ ถ้าสั่งคำสั่ง passwd , rm .... จะไม่ยอมให้คำสั่งเหล่านี้ทำงานได้

จากแนวทางการออกแบบนี้ การสั่งคำสั่ง echo $LOGNAME ภายใน 10 วินาทีนั้นสามารถเปลี่ยนเป็นการสั่งให้ทำงานอย่างอื่นก็ได้ โดยขึ้นอยู่กับนโยบายของหน่วยงาน หรือตามความเห็นชอบของกลุ่มผู้ดูแลระบบ ที่จะตกลงร่วมกัน



รูปที่ 3.1 โมดูลในการป้องกันผู้ใช้พิเศษ

3.1.2 การออกแบบโมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ

โมดูลนี้ออกแบบมาเพื่อให้ได้ตามเกณฑ์ความมั่นคง ในด้านการควบคุมการเข้าถึง โดยใช้คุลยพินิจ การแสดงตนและการพิสูจน์ตน เส้นทางการไว้ใจได้ และการตรวจสอบ

วัตถุประสงค์

ผู้ใช้ที่จะเข้าสู่ระบบนั้น จะต้องมีบัญชีชื่อผู้ใช้อยู่ในระบบ และต้องมีการใส่รหัสผ่านในการแสดงตนและพิสูจน์ตนก่อนที่จะเข้ามาใช้ระบบได้ ในทางกลับกันระบบจะต้องได้รับการตรวจสอบด้วยว่าไม่มีโปรแกรมปลอมมาทำงานแอบดักจับ และปลอมแปลงรหัสผ่านของผู้ใช้ ที่เข้ามาใช้งาน ในระบบ เป็นการสร้างความมั่นใจให้กับผู้ใช้

ปัญหาที่พบ

การสร้างโปรแกรมในการเข้าสู่ระบบหรือล็อกอินปลอมขึ้นมา เพื่อดักจับรหัสผ่านของผู้ใช้ ก่อนที่ผู้ใช้ สามารถเข้าสู่ระบบได้ เป็นอีกวิธีหนึ่งที่นักเจาะระบบนิยมกระทำ โดยสรุปมีดังนี้ นักเจาะระบบจะทำการรันโปรแกรมการเข้าสู่ระบบที่ปลอมขึ้นมา ไว้ที่ตามเทอร์มินอลหรือศูนย์บริการคอมพิวเตอร์ ซึ่งโปรแกรมที่ว่านี้ จะแสดงหน้าจอและการทำงานเหมือนโปรแกรมการเข้าสู่ระบบจริง มีการขึ้น LOGIN PROMPT เพื่อให้ผู้ใช้ใส่บัญชีชื่อผู้ใช้ และขึ้น PASSWORD PROMPT เพื่อรอรับรหัสผ่านของผู้ใช้ ซึ่งเมื่อผู้ใช้เรียกใช้งาน โปรแกรมนี้ก็จะทำงานและจะเก็บคีย์ที่ผู้ใช้พิมพ์เข้ามา ก่อนที่จะให้ผู้ใช้เข้าสู่โปรแกรมการเข้าสู่ระบบที่แท้จริงได้ โดยที่ผู้ใช้เองไม่ทราบว่ารหัสผ่านของตนถูกดักจับไปแล้ว

แนวทางการออกแบบและการป้องกันแก้ไข

1. สำหรับตัวผู้ใช้ ต้องมีการสังเกตวันที่- เวลาครั้งล่าสุดของตัวผู้ใช้เอง ถ้าหากว่าไม่ตรงกับความเป็นจริง ต้องรีบแจ้งให้ผู้ดูแลระบบทราบว่า บัญชีชื่อผู้ใช้ของตนถูกใช้ โดยผู้อื่น และให้ทำการตรวจสอบข้อมูลภายในไดเรกทอรีของตนว่า มีสิ่งผิดปกติหรือไม่ พร้อมกันนั้นให้ทำการเปลี่ยนรหัสผ่านใหม่

2. สำหรับผู้ดูแลระบบ จะต้องทำการตรวจสอบว่ามีการปลอมแปลงการเข้าสู่ระบบมาจากที่ไหน และเข้ามาทำอะไรบ้าง โดยที่ระบบปฏิบัติการโอเอสเอฟวัน จะมีไฟล์ที่เก็บข้อมูลการเข้ามาใช้งานของผู้ใช้ และคำสั่งที่ผู้ใช้สั่งให้ทำงานอยู่ที่ไฟล์ /var/adm/wtmp และ ไฟล์ /var/adm/pacct ตามลำดับ ซึ่งผู้ดูแลระบบจะต้องใช้คำสั่งในการดูไฟล์ /var/adm/wtmp ด้วยคำสั่ง last และใช้คำสั่ง lastcomm ในการดู ไฟล์ /var/adm/pacct ตัวอย่างผลของการเรียกดูไฟล์ทั้งสองมีดังนี้

ตัวอย่างการเรียกดูไฟล์ /var/adm/wtmp โดยใช้คำสั่ง last

```
gl          ttyp2      202.44.41.100    Thu Jan 16 18:51   still logged in
took        ttyp1      202.44.34.124    Thu Jan 16 16:49   still logged in
gl01        ttyp1      202.44.33.133    Thu Jan 16 15:23 - 16:14  (00:51)
gl02        ttyp2      202.44.33.130    Thu Jan 16 14:39 - 16:16  (01:36)
nui         ttyp3      202.44.41.10     Thu Jan 16 12:06 - 12:14  (00:08)
gl          ttyp2      202.44.41.100    Thu Jan 16 12:02 - 12:51  (00:48)
ent1        ttyp1      202.44.41.100    Thu Jan 16 11:07 - 12:51  (01:43)
took        ttyp1      202.44.41.100    Thu Jan 16 11:06 - 11:06  (00:00)
noi         ttyp1      202.44.41.14     Thu Jan 16 09:10 - 09:16  (00:05)
```

ตัวอย่างการเรียกดูไฟล์ /var/adm/pacct โดยใช้คำสั่ง lastcomm

```
sreport     gl         ttyp2      0.25 secs Thu Jan 16 19:12
vi          gl         ttyp2      0.08 secs Thu Jan 16 19:12
gl3.exe     gl         ttyp2      0.16 secs Thu Jan 16 19:12
sh          gl         ttyp2      0.01 secs Thu Jan 16 19:12
report      gl         ttyp2      0.09 secs Thu Jan 16 19:12
sreport     gl         ttyp2      0.27 secs Thu Jan 16 19:12
vi          gl         ttyp2      0.09 secs Thu Jan 16 19:11
gl3.exe     gl         ttyp2      0.16 secs Thu Jan 16 19:11
sh          gl         ttyp2      0.01 secs Thu Jan 16 19:11
report      gl         ttyp2      0.09 secs Thu Jan 16 19:11
lastcomm    took       ttyp0      0.01 secs Thu Jan 16 19:11
sreport     gl         ttyp2      0.27 secs Thu Jan 16 19:11
vi          gl         ttyp2      0.17 secs Thu Jan 16 19:09
```

3. หลังจากทำการตรวจสอบการเข้ามาใช้งานแล้ว ผู้ดูแลระบบจะต้องทำการตรวจสอบทั้งระบบว่า โปรแกรมการล็อกอินที่ปลอมแปลงการเข้ามาใช้งานนั้น วางอยู่ที่ไดเรกทอรีใด ให้ทำการกำจัดทิ้ง โดยอาจตรวจสอบดูว่ามีโปรแกรมใดที่มาทำการเรียกใช้บริการพอร์ทเบอร์ 23 บ้าง ซึ่งพอร์ทเบอร์นี้มักใช้เป็นค่าโดยปริยายของการเทลเนต (telnet)

4. นอกจากการเทลเนตเข้าสู่ระบบแล้ว ผู้ใช้สามารถติดต่อกับเครื่องคอมพิวเตอร์ที่ให้บริการ โดยผ่านเข้ามาทางโมเด็ม เพื่อเพิ่มความมั่นคงให้กับระบบ และความมั่นใจให้กับผู้ใช้ ว่าจะไม่มีการดักจับรหัสผ่านทางสายโทรศัพท์ ซึ่งกรณีนี้สามารถแก้ไขได้ โดยการทำการเข้ารหัสก่อนที่จะมีการส่งข้อมูลออกมาที่สายโทรศัพท์

รูปที่ 3.2 โมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ

3.1.3 การออกแบบโมดูลในการตรวจสอบระบบ

โมดูลนี้ออกแบบมาเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการตรวจสอบ

วัตถุประสงค์

ในการออกแบบให้ระบบมีความมั่นคงในระดับขั้น B3 ระบบจะต้องมีคุณสมบัติดังนี้คือ

1. ทีซีบีจะต้องมีกลไกดูแลและป้องกันการแก้ไข หรือทำลายตัวกระทำที่มีอยู่จากผู้ใช้ที่ไม่มีสิทธิโดยชอบธรรม

2. ทีซีบีจะต้องสามารถบันทึกเหตุการณ์ดังต่อไปนี้ได้แก่

2.1 การแสดงตนและการพิสูจน์ตนของผู้ใช้ที่เข้าสู่ระบบ

2.2 การกระทำของผู้ใช้ที่มีต่อตัวถูกกระทำ เช่นการเปิดหรือการลบไฟล์

2.3 การกระทำหรือเหตุการณ์ที่ทำโดยผู้ใช้พิเศษ

2.4 การกระทำหรือเหตุการณ์ที่มีผลต่อด้านความมั่นคงของระบบ

3. การบันทึกการตรวจสอบจะต้องมีการบันทึกสิ่งต่าง ๆ ดังต่อไปนี้คือ วัน-เวลาที่เกิดเหตุการณ์ ผู้ใช้หรือผู้กระทำที่เกี่ยวข้อง ประเภทของเหตุการณ์ที่เกิด เหตุการณ์นั้นทำได้สำเร็จหรือล้มเหลว แหล่งกำเนิดหรือต้นทางที่เป็นที่มาของเหตุการณ์ เช่น หมายเลขเทอร์มินอลหรือหมายเลขเครื่องที่ใช้ ชื่อของตัวถูกกระทำ เช่น ชื่อไฟล์ที่ถูกเปิดหรือลบ เป็นต้น

4. ทีซีบีสามารถตรวจสอบสิ่งพิมพ์ หรือผลลัพธ์ที่ออกมาในรูปแบบที่สามารถอ่านออกได้ โดยระบุว่าตัวกระทำที่ถูกผู้ใช้ใช้นั้น มีระดับขั้นความมั่นคงในระดับใด

5. ทีซีบีจะต้องมีการตรวจสอบเหตุการณ์ที่เข้ามาใช้ประโยชน์ จากช่องเก็บทางลับที่มีค่าแบนวิธสูงกว่า 1 บิตใน 10 วินาที

6. ทีซีบีจะต้องมีกลไกในการเฝ้าติดตาม และรายงานเหตุการณ์ ที่กำลังจะเป็นอันตรายต่อความมั่นคงของระบบ ซึ่งรายงานนี้จะต้องรายงานให้ผู้ดูแลระบบทราบโดยทันที และอาจใส่กลไกเพื่อหยุดเหตุการณ์นั้นด้วย

ตัวอย่างการบันทึกเหตุการณ์ตรวจสอบ ในระบบปฏิบัติการโอเอสเอฟวัน โดยสามารถระบุส่วนที่ต้องการตรวจสอบ และ ระดับของเหตุการณ์ เก็บไว้ที่ไฟล์ /etc/syslog.conf

ตัวอย่างไฟล์ syslog.conf

```
# @(#)$RCSfile: syslog.conf,v $ $Revision: 4.1.4.2 $ (DEC)
# $Date: 1992/03/18 14:58:45
# syslogd config file
# facilities: kern user mail daemon auth syslog lpr binary
# priorities: emerg alert crit err warning notice info debug
kern.debug          /var/adm/syslog.dated/kern.log
user.debug          /var/adm/syslog.dated/user.log
mail.debug          /var/adm/syslog.dated/mail.log
daemon.debug        /var/adm/syslog.dated/daemon.log
auth.debug          /var/adm/syslog.dated/auth.log
syslog.debug        /var/adm/syslog.dated/syslog.log
lpr.debug           /var/adm/syslog.dated/lpr.log
msgbuf.err          /var/adm/crash/msgbuf.savecore
kern.debug          /var/adm/messages
kern.debug          /dev/console
*.emerg                 *
```

โดยที่ facilities หมายถึงส่วนที่เราต้องการตรวจสอบ เช่น kern หมายถึง การตรวจสอบที่แก่นของระบบปฏิบัติการ user หมายถึงผู้ใช้ทั่วไป auth หมายถึงการตรวจดูการใช้สิทธิในการเข้าสู่ระบบ เช่นการ login และการใส่รหัสผ่าน รวมทั้งการใช้คำสั่ง su และ priorities หมายถึงระดับการบันทึก เหตุการณ์ที่เกิดขึ้น เช่น emerg หมายถึงให้บันทึกเมื่อมีเหตุการณ์ฉุกเฉิน เช่น ระบบ crash โดยกระทันหัน ซึ่งจะต้องมีการประกาศไปยังผู้ใช้ทุกคน alert หมายถึงระดับเหตุการณ์ที่ควรจะต้องมีการแก้ไขในทันที เช่นการเสียหายของฐานข้อมูลของระบบ crit หมายถึงเหตุการณ์ที่วิกฤติ เช่น การทำงานผิดพลาดของฮาร์ดแวร์ เป็นต้น

ซึ่งในส่วนคอลัมน์แรกเป็นการเลือกส่วนและระดับเหตุการณ์ในการบันทึก และในคอลัมน์ด้านขวาจะเป็นการระบุไฟล์ที่ใช้เก็บการตรวจสอบ โดยที่จะมีการแยกไดเรกทอรีเป็นรายวันในการเก็บ log ไฟล์ต่าง ๆ เช่น

ตัวอย่างไฟล์ kern.log

```
Jan 30 12:30:25 kmitnb04 vmunix: fork/procdup: task_create failed. Code: 0x11
```

ตัวอย่างไฟล์ syslog.log

```
Jan 30 00:34:06 kmitnb04 syslogd: restart
```

ตัวอย่างไฟล์ daemon.log

```
Jan 28 22:58:55 kmitnb04 netacl[2713]:permit host=unknow/202.44.41.9
service=telnetd  execute=/usr/sbin/telnetd
Jan 28 23:41:05 kmitnb04 netacl[2650]:deny host=kmitnb5/202.44.32.2
service=rlogind  execute=/usr/sbin/rlogind
```

ตัวอย่างไฟล์ /var/adm/syslog.dated/auth.log เก็บข้อมูลดังนี้

```
บรรทัดที่ 1    Jan 31 10:54:58 kmitnb04 su: BADSU ingres on /dev/ttyp3
บรรทัดที่ 2    Jan 31 10:55:23 kmitnb04 su: SU took on /dev/ttyp4
บรรทัดที่ 3    Jan 31 11:02:10 kmitnb04 su: BADSU ingres on /dev/ttyp3
บรรทัดที่ 4    Jan 31 11:02:24 kmitnb04 su: BADSU ingres on /dev/ttyp3
บรรทัดที่ 5    Jan 31 11:02:46 kmitnb04 su: BADSU took on /dev/ttyp4
บรรทัดที่ 6    Jan 31 11:02:52 kmitnb04 su: SU took on /dev/ttyp4
```

จากตัวอย่างไฟล์ auth.log ของวันที่ 31 Jan จะสัมพันธ์กับไฟล์ /var/adm/sialog ดังนี้

ตัวอย่างไฟล์ /var/adm/sialog

```
SIA:ERROR Fri Jan 31 10:54:58 1997
Failure on authentication for su from ingres to root
SIA:EVENT Fri Jan 31 10:55:23 1997
Successful authentication for su from took to root
SIA:ERROR Fri Jan 31 11:02:10 1997
Failure on authentication for su from ingres to root
SIA:ERROR Fri Jan 31 11:02:24 1997
Failure on authentication for su from ingres to took
SIA:ERROR Fri Jan 31 11:02:46 1997
Failure on authentication for su from took to root
SIA:EVENT Fri Jan 31 11:02:52 1997
Successful authentication for su from took to root
```

ปัญหาที่พบ

มักพบว่าผู้ใช้ที่มีความมุ่งร้ายต่อระบบ มักจะพยายามซ่อนตนต่อการถูกตรวจสอบ โดยพยายามที่จะหลีกเลี่ยงหรือลบหลักฐานต่าง ๆ ที่มีการบ่งบอกว่าตนเป็นผู้กระทำ และกระทำสิ่งใดลงไป

แนวทางในการออกแบบการตรวจสอบ

1. กลไกการตรวจสอบจะต้องมีการป้องกันไม่ให้ผู้ใช้ใด ๆ ในระบบหรือแม้แต่บุคคลภายนอก ผ่านพ้นหรือละเมิดกลไกการป้องกันความมั่นคงของระบบไปได้

2. กลไกการตรวจสอบจะต้องแสดงหรือบอกได้ว่า มีผู้ใช้พยายามใช้สิทธิในการกระทำบางอย่างนอกเหนือจากสิทธิที่ได้รับ

3. กลไกการตรวจสอบ ต้องสามารถป้องกันขับยั้งพวกเจาะระบบที่พยายามผ่านข้ามหรือหลบจากกลไกการป้องกันระบบ

4. สามารถที่จะเลือกกลไกการตรวจสอบว่า สามารถเลือกเหตุการณ์ก่อนหรือหลังจากการเกิดเหตุการณ์มาทำการตรวจสอบ เช่นถ้าไม่มีกลไกแบบเลือกเหตุการณ์ตรวจสอบไว้ก่อน ดังนั้นเหตุการณ์ทั้งหมดจะถูกนำมาไว้ที่รายการการตรวจสอบ ซึ่งกฎเกณฑ์ในการเลือกกลไกนี้จะขึ้นอยู่กับผู้ดูแลระบบว่า สามารถที่จะพิสูจน์ตัวผู้ใช้หรือผู้กระทำ หรือสามารถจัดจำแนกตัวถูกกระทำได้หรือไม่

<u>การออกแบบการตรวจสอบ</u>

โดยคำนึงถึงสิ่งต่อไปนี้

1. แหล่งที่เก็บรายการข้อมูลตรวจสอบ บนระบบปฏิบัติการโอเอสเอฟวันมีโปรแกรมติดตั้ง การตรวจสอบ ซึ่งสามารถใช้ระบุได้ว่าต้องการเก็บรายการตรวจสอบไว้ที่ใด โดยปริยายมักจะเก็บไว้ที่ `/var/adm/auditlog.nnn` ซึ่ง *nnn* หมายถึง ตัวเลขที่เพิ่มขึ้นของรายการตรวจสอบในแต่ละครั้ง เนื่องจากรายการข้อมูลตรวจสอบอาจมีจำนวนมาก ทำให้ต้องใช้เนื้อที่อย่างมาก ในการจัดเก็บ และต้องมีกลไกในการป้องกันการเกิดการล้นของข้อมูลขึ้น โดยกลไกที่ว่านี้ สามารถ เลือกการจัดการเมื่อเกิดการล้นของข้อมูลขึ้น โดยสามารถเลือกการทำงานได้ดังนี้ คือ

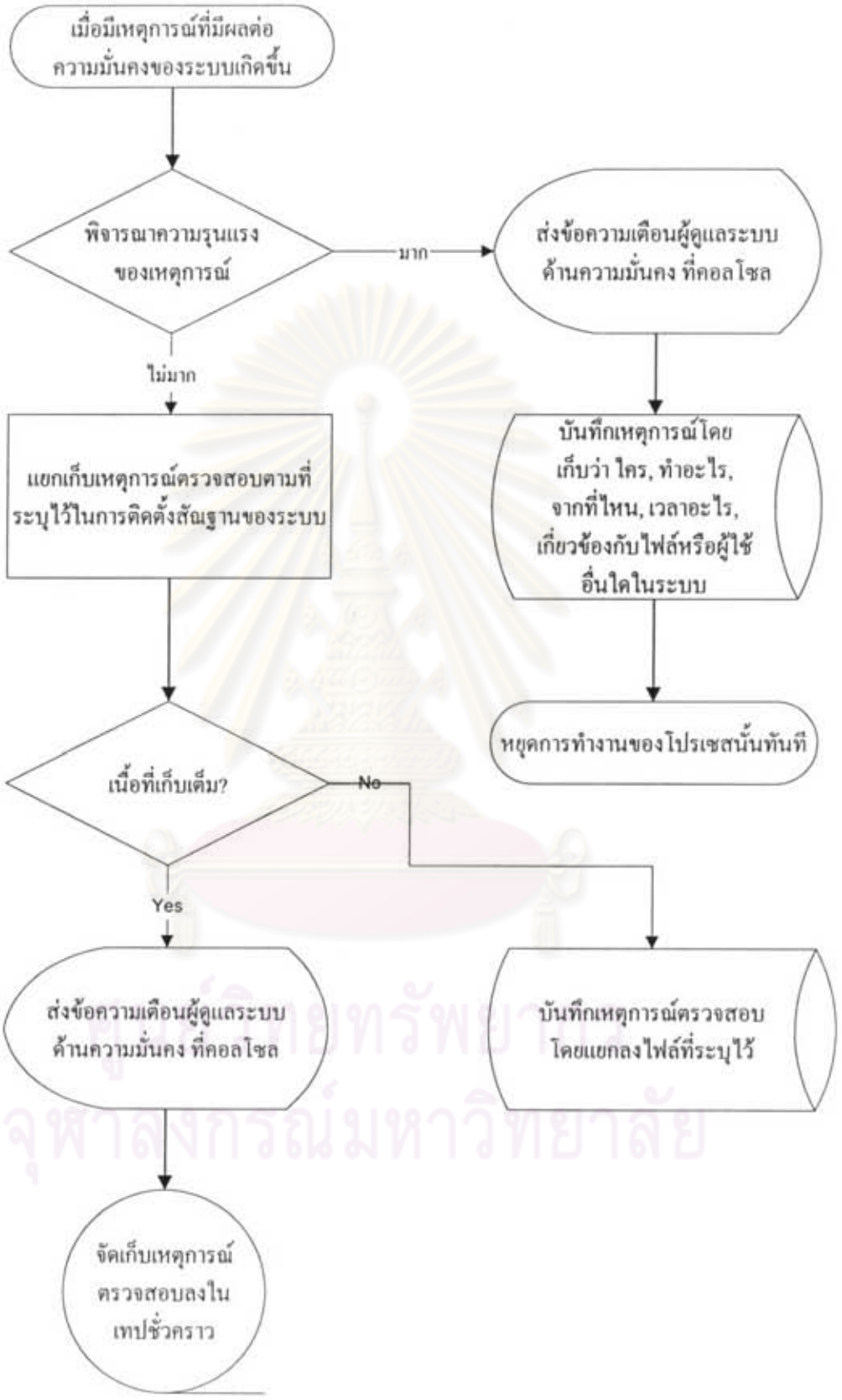
1.1 สามารถเปลี่ยนที่จัดเก็บรายการตรวจสอบได้ใหม่

1.2 หยุดเก็บรายการตรวจสอบชั่วคราว

1.3 เขียนทับรายการตรวจสอบเดิมที่มีอยู่ โดยเขียนทับไปยังรายการตรวจสอบแรก ในลักษณะคิวแบบวงกลม

2. ถ้ามีเครื่องคอมพิวเตอร์ที่ต่อเชื่อมอยู่ด้วยกัน โดยใช้โปรโตคอลทีซีพีไอพี (TCP/IP) ก็สามารถที่จะนำรายการ ตรวจสอบไปไว้ที่เครื่องคอมพิวเตอร์เครื่องอื่นได้ โดยคำนึงถึงเครื่องคอมพิวเตอร์นั้นเป็นหลักว่า จะต้องอยู่ในที่ตั้งที่มีความปลอดภัย

3. ประสิทธิภาพการทำงานของระบบ บนระบบปฏิบัติการโอเอสเอฟวันระบุรายการการตรวจสอบ ไว้ที่ `/etc/sec/audit_events` ซึ่งสามารถระบุเลือกเหตุการณ์การตรวจสอบได้ เช่น การ ตรวจสอบโดยระบุหมายเลขโปรเซส การตรวจสอบโดยระบุบัญชีชื่อผู้ใช้เฉพาะรายบุคคล โดยขึ้นอยู่กับดุลยพินิจของผู้ดูแลระบบ



รูปที่ 3.3 การออกแบบการจัดเก็บรายการตรวจสอบ

3.1.4 การออกแบบโมดูลในการควบคุมการใช้งานในระบบ

โมดูลนี้ออกแบบมาเพื่อให้ได้ตามเกณฑ์ความมั่นคงในเรื่องเกี่ยวกับป้ายชื่อหรือป้ายความไหว ได้แก่ การสร้างความเป็นเอกภาพของป้ายชื่อ การส่งออกข้อมูล การจัดการป้ายชื่อของสิ่งพิมพ์ ป้ายชื่ออุปกรณ์ รวมทั้งการควบคุมการเข้าถึงภายใต้อาณัติ

วัตถุประสงค์

เนื่องจากระบบปฏิบัติการโอเอสเอฟวันออกแบบมาเพื่อสำหรับ ให้ผู้ใช้หลาย ๆ คนเข้ามาใช้งานได้ในเวลาเดียวกัน และผู้ใช้ในระบบนั้นมีระดับความสำคัญที่แตกต่างกัน รวมทั้งการใช้ข้อมูลที่มีความสำคัญต่างกันด้วย จึงจำเป็นต้องมีการจัดแบ่งแยกระดับ หรือกำหนดระดับขั้นความสำคัญหรือความมั่นคงให้กับผู้ใช้ในระบบให้มีความต่างกัน รวมทั้งการระบุหรือกำหนดความสำคัญของข้อมูลว่าอนุญาตให้ผู้ใช้ใดใช้ได้ ซึ่งจะต้องมีการควมคุมการใช้งานอย่างเข้มงวด เพื่อทำให้ระบบมีความมั่นคงและไว้ใจได้มากขึ้น

ปัญหาที่พบ

ปัญหาส่วนใหญ่มักเกิดจากตัวผู้ใช้เอง โดยความประมาทหรือความรู้เท่าไม่ถึงการณ์ หรือการพยายามละเมิดสิทธิที่ได้รับ เช่น การสั่งพิมพ์ข้อมูลลับไปออกที่เครื่องพิมพ์ที่ใช้ในที่สาธารณะ การนำข้อมูลส่วนตัวเช่นจดหมายไปไว้ที่ /tmp ซึ่งสามารถอ่านได้โดยผู้ใช้ทั่วไป

แนวทางการออกแบบการป้องกันและการแก้ไข

ไฟล์ในระบบปฏิบัติการโอเอสเอฟวัน สามารถเพิ่มข้อมูลเข้าไปที่ส่วนหัวของไฟล์ ซึ่ง ข้อมูลที่เก็บนี้คือค่าระดับความสำคัญหรือป้ายชื่อความไหวของไฟล์ โดยแบ่งเป็น 2 ส่วน คือ ระดับความสำคัญของข้อมูลและเก็บกลุ่มของขอบเขตข้อมูล ที่อนุญาตให้ผู้ใช้เข้ามาใช้งานได้

ตัวอย่างการแบ่งระดับความสำคัญของข้อมูล เช่นข้อมูลในวงการราชการ อาจแบ่งระดับความสำคัญเป็น ลับสุดยอด ลับ หนังสือเวียน หรือในวงการธุรกิจอาจแบ่งข้อมูลออกเป็นข้อมูล สำหรับผู้บริหารระดับสูง ข้อมูลสำหรับเจ้าหน้าที่เฉพาะด้าน ข้อมูลทั่วไปที่ใช้ เฉพาะภายในบริษัท และข้อมูลที่เผยแพร่สู่สาธารณชนภายนอกได้ เป็นต้น ให้ขึ้นอยู่กับสภาพแวดล้อมในการนำไปใช้ และนโยบายของหน่วยงาน

กลุ่มของขอบเขตข้อมูล ไม่มีการแบ่งระดับขั้นความสำคัญ แต่ให้ระบุขอบเขตการเข้าใช้ ซึ่งจะเป็นข้อมูลในระบบหรือในหน่วยงานนั้น ๆ เช่น ฝ่ายบัญชี ฝ่ายบุคลากร ฝ่ายการตลาด ฝ่ายขาย ฝ่ายซ่อมบำรุง ฝ่ายบริการ เป็นต้น จะได้รูปแบบของป้ายชื่อความไหวของไฟล์ ดังนี้

ระดับความสำคัญของข้อมูล [กลุ่มของขอบเขต]
เช่น ลับสุดยอด [ฝ่ายบัญชี , ฝ่ายบุคลากร]

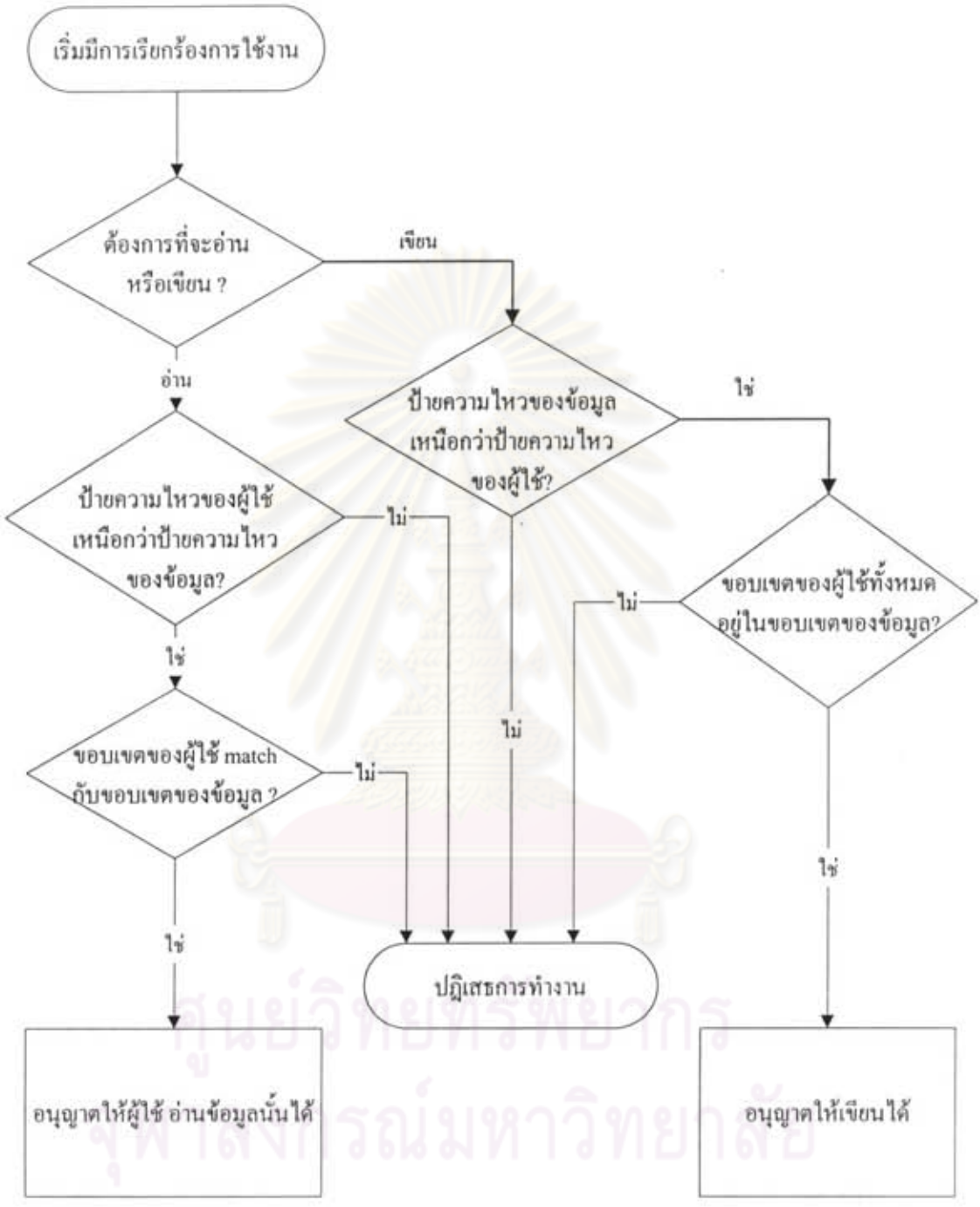
โดยระบบจะมีการควบคุมการเข้าใช้ข้อมูลอย่างเข้มงวด การอนุญาตหรือการปฏิเสธการให้ใช้งาน ขึ้นอยู่กับ 3 สิ่งคือ ป้ายความไหวของตัวกระทำหรือผู้ใช้ ป้ายความไหวของตัวถูกกระทำ เช่น ไฟล์ข้อมูล และความต้องการในการเข้าใช้งาน โดยแบ่งการเข้าใช้งานเป็นดังนี้

1. การอ่าน ในการที่ผู้ใช้จะอ่านข้อมูลได้นั้น ป้ายความไหวของตัวผู้ใช้จะต้องเหนือกว่าหรือเท่ากับป้ายความไหวของตัวข้อมูล เพื่อเป็นการบังคับว่าข้อมูลที่มีความสำคัญสูงถูกอ่านได้โดยผู้ใช้ที่มีความสำคัญสูงเช่นกัน ไม่ยอมให้ผู้ใช้ทั่วไปอ่านได้

2. การเขียน ในการเขียนข้อมูล ป้ายความไหวของตัวข้อมูล จะต้องเหนือกว่าหรือเท่ากับป้ายความไหวของผู้ใช้ เพื่อไม่ต้องการให้ผู้ใช้ที่อยู่ในระดับความสำคัญสูงเขียนข้อมูลหรือเปลี่ยนแปลงข้อมูลที่มีความสำคัญน้อยกว่าเพราะเป็นการทำให้ข้อมูลถูกลดเกรดความสำคัญลง แต่ในขณะเดียวกันผู้ใช้ในระดับทั่วไป ระบบอนุญาตให้เขียน ข้อมูลไปที่หน่วยความจำที่เป็นความลับได้ แต่จากนั้นไม่อนุญาตให้อ่านหน่วยความจำลับนั้นได้ ซึ่งกฎในการเขียนนี้ จะเป็นการเพิ่มและลดเกรดความสำคัญของข้อมูล

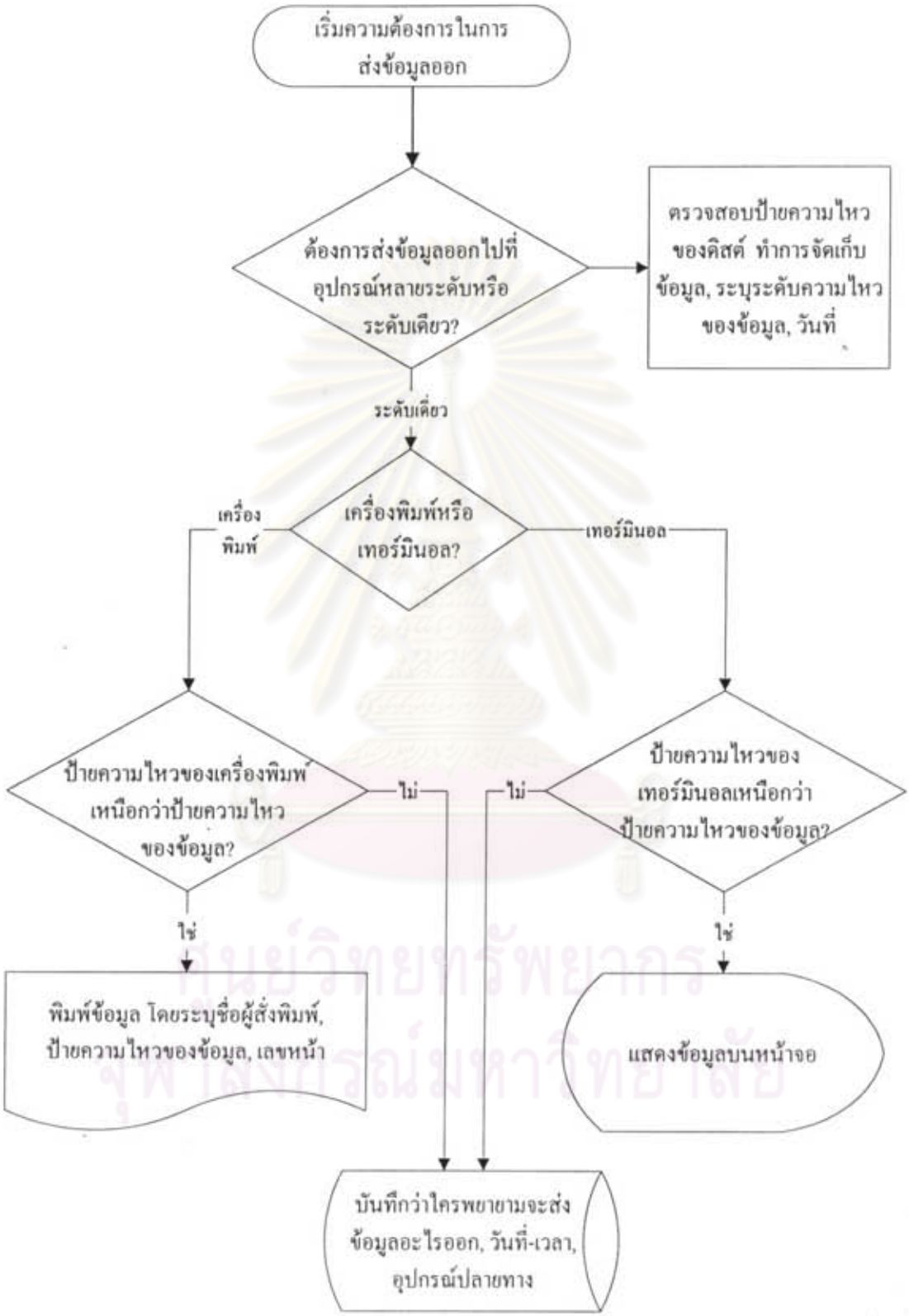
3. การส่งออกข้อมูล ถ้าอุปกรณ์ปลายทางมีป้ายความไหวของข้อมูลต่ำกว่าป้ายความไหวของข้อมูลที่จะส่งออก จะไม่ยอมให้ทำงานได้ เช่น ถ้าอุปกรณ์ปลายทางเป็นจอเทอร์มินอลจะทำ การล็อคเทอร์มินอลนั้น หรือถ้าพิมพ์ข้อมูลที่มีป้ายความไหวสูงไปยังเครื่องพิมพ์ที่มีป้ายความไหวสูงเช่นกัน หมายถึงเครื่องพิมพ์นั้นจะต้องถูกติดตั้งไว้ในที่ที่มีความปลอดภัยสูง มีการควบคุมการเข้าถึงทางกายภาพ ระบบจะยอมให้พิมพ์ข้อมูลนั้นได้ โดยสิ่งพิมพ์ที่ได้มีการระบุป้ายความไหวของข้อมูลนั้นด้วย รวมทั้งมีการระบุชื่อและป้ายความไหวของเครื่องพิมพ์ วันที่-เวลา หมายเลขหน้า และจำนวนรวมของหน้าที่พิมพ์ คือระบุว่าพิมพ์หน้าที่เท่าไรของจำนวนหน้าทั้งหมด

ถ้าอุปกรณ์ปลายทางเป็นดิสก์ ให้เปรียบเทียบป้ายความไหวของข้อมูลกับป้ายความไหวของดิสก์ ถ้าป้ายความไหวของดิสก์สูงกว่าป้ายความไหวของข้อมูลระบบยอมให้ดิสก์นั้นเก็บข้อมูลได้



รูปที่ 3.4 (ก) โมดูลการควบคุมการใช้งานในระบบ

การควบคุมการอ่านและเขียน



รูปที่ 3.4 (ข)โมดูลการควบคุมการใช้งานในระบบ

การส่งข้อมูลออก

3.2 ส่วนที่เกี่ยวข้องกับหน้าที่ของผู้บริหารระบบ/ผู้ดูแลด้านความมั่นคงของระบบ

3.2.1 โมดูลในการแสดงตนและการพิสูจน์ตน

โมดูลนี้เขียนเป็นแนวทางเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการแสดงตนและการพิสูจน์ตน

วัตถุประสงค์

ในการออกแบบให้ระบบมีความมั่นคงในระดับขั้น B3 ทีซีบีจะต้องมีกลไกให้ผู้ใช้แสดงตนและพิสูจน์ได้ว่าเป็นผู้ใช้ที่มีสิทธิถูกต้องในการเข้าใช้ตัวกระทำนั้น ๆ ได้ และทีซีบีจะต้องสามารถป้องกันข้อมูลส่วนตัวของผู้ใช้หนึ่ง ๆ ไม่ให้ใครจากภายนอกหรือผู้ใช้ในระบบเองละเมิดหรือปลอมแปลงไปได้

ปัญหาที่พบ

คุณสมบัติด้านการแสดงตนและการพิสูจน์ตนของระบบปฏิบัติการโอเอสเอฟวันในรุ่นปัจจุบัน มีความมั่นคงในระดับขั้น C2 ซึ่งจุดอ่อนของความมั่นคงในระดับนี้พบว่า ระบบมีการตรวจสอบการแสดงตนและการพิสูจน์ตนของผู้ใช้ โดยเก็บข้อมูลของผู้ใช้ไว้ที่ไฟล์ /etc/passwd แต่นักเจาะระบบสามารถเจาะระบบโดยเข้าทางไฟล์ที่เก็บรหัสผ่านได้ โดยวิธีทางที่ทำได้มีดังนี้คือ

1. นำไฟล์ที่เก็บรหัสผ่าน มาผ่านโปรแกรมในการถอดรหัส ซึ่งการนำไฟล์รหัสผ่านมาได้นั้น ถ้าเป็นผู้ใช้คนหนึ่งในระบบนั้นเองก็สามารถทำการคัดลอกสำเนา (copy) ได้โดยตรง แต่ถ้าเป็นผู้เจาะระบบจากภายนอก สามารถที่จะนำไฟล์รหัสผ่านไปได้ โดยมากมักอาศัยบัญชีผู้ใช้ที่ชื่อว่า anonymous, ftp เข้ามาทำการคัดลอกสำเนาโดยอาศัยผ่านทางช่องทางสื่อสารของเครือข่ายคอมพิวเตอร์ ซึ่งเมื่อนำไฟล์รหัสผ่านมาผ่านโปรแกรมในการถอดรหัสแล้ว ก็จะทราบรหัสผ่านของผู้ใช้บางคนที่อยู่ในระบบนั้น ผู้เจาะระบบก็สามารถที่จะเข้าสู่ระบบได้ โดยอาศัยรหัสผ่านที่เจาะมาได้

2. เจาะระบบโดยอาศัยชื่อบัญชีผู้ใช้ที่ยอดนิยม (well-known account) เช่น Guest, Demo, Games, Mail, root, Admin, Fund หรือ vendor account เช่น field (เป็นชื่อบัญชีผู้ใช้ที่เป็นที่ตกลงกันของบริษัทดิจิตอล ที่ใช้ในการเข้ามาดูเครื่องและบริการลูกค้า) โดยที่นักเจาะระบบอาจอาศัยการเดารหัสผ่านของบัญชีรายชื่อเหล่านี้แล้วสามารถเข้าสู่ระบบได้ โดยที่ระบบไม่สามารถตรวจสอบได้ว่าแท้จริงใครเป็นผู้เข้ามาในระบบ

แนวทางการออกแบบการป้องกันและการแก้ไข

การป้องกันจุดอ่อนเหล่านี้ สามารถทำได้ดังนี้คือ

1. ผู้ดูแลระบบ ควรนำชุดโปรแกรมคำสั่งในการถอดรหัสมาใช้ในการตรวจจับเพื่อหาว่าผู้ใช้ใดในระบบ ไม่มีการใส่รหัสผ่าน หรือใส่รหัสผ่านที่โดนเจาะได้ง่าย ซึ่งเมื่อตรวจพบก็ทำการจัดการให้ผู้ใช้นั้นๆ ทราบและให้ผู้ใช้นั้นๆ ใส่รหัสผ่านใหม่

2. การตั้งรหัสผ่านของผู้ใช้ ผู้ดูแลระบบควรสร้างกลไกในการตั้งรหัสผ่านที่มั่นคงไว้ เป็นการบังคับให้ผู้ใช้ทำตาม เช่น

2.1 การบังคับการตั้งความยาวของรหัสผ่าน ซึ่งต้องไม่สั้นหรือยาวเกินไปเพราะถ้าสั้นเกินไป รหัสผ่านก็สามารถที่จะถูกเดาได้ง่าย หรือถ้ายาวเกินไปผู้ใช้มักจะจำไม่ได้ แล้วอาจจดไว้บนสิ่งที่อยู่ใกล้ตัว หรือผู้ใช้ต้องใช้เวลาในการพิมพ์รหัสผ่านนาน รหัสผ่านก็อาจถูกสังเกตหรือจดจำโดยผู้อื่นได้

2.2 การบังคับอายุของรหัสผ่าน เนื่องจากว่าถ้าไฟล์รหัสผ่านถูกนำไปผ่านโปรแกรมในการถอดรหัส ซึ่งถ้ารหัสผ่านมีความยาวมากพอ การรันโปรแกรมถอดรหัสก็จะใช้เวลามากด้วย แต่ก็เป็นไปได้ที่จะสามารถถอดรหัสได้สำเร็จ ซึ่งถ้ามีการบังคับอายุของรหัสผ่านให้ผู้ใช้ในระบบเปลี่ยนรหัสผ่านตามระยะเวลา โอกาสที่นักเจาะระบบจะรันโปรแกรมถอดรหัสจากไฟล์รหัสผ่านที่นำไปได้สำเร็จนั้น ก็จะไม่สามารถนำรหัสผ่านที่เจาะได้มาใช้ เพราะผู้ใช้มีการตั้งรหัสผ่านใหม่แล้ว

2.3 ทำการบันทึกผู้ที่เข้ามาทำการเปลี่ยนรหัสผ่าน ที่ไม่ใช่ผู้ใช้ที่เป็นเจ้าของ

2.4 มีการเก็บประวัติการใช้รหัสผ่านของผู้ใช้ ซึ่งเมื่อรหัสผ่านหมดอายุ ต้องบังคับให้ผู้ใช้ตั้งรหัสผ่านใหม่ และห้ามไม่ให้ผู้ใช้กลับมาใช้รหัสผ่านเดิม

3. การตรวจสอบโครงสร้างของไฟล์รหัสผ่านและไฟล์ที่เกี่ยวข้อง เช่น /etc/passwd, /etc/passwd.pag, /etc/utmp, /etc/wtmp, /etc/group เพราะไฟล์เหล่านี้เก็บข้อมูลของผู้ใช้ที่มีสิทธิที่เข้ามาใช้ในระบบ

4. การป้องกันการคัดลอกหรือสำเนาไฟล์รหัสผ่าน จากผู้ใช้ในระบบเองหรือจากบุคคลภายนอก โดยการระบุโหมดสิทธิในการใช้ไฟล์รหัสผ่าน หรือตรวจจับการใช้ FTP กับไฟล์รหัสผ่าน

5. การป้องกันในฐานะผู้ใช้พิเศษ เนื่องจากผู้ดูแลระบบสามารถใช้คำสั่งในการ 'สลับเปลี่ยนผู้ใช้' หรือคำสั่ง su เพื่อใช้บัญชีผู้ใช้ที่ชื่อรูท ซึ่งเป็นผู้ใช้ที่มีอำนาจสิทธิสูงที่สุดในระบบ จึงมักเป็นที่ท้าทายของนักเจาะระบบทั้งหลายในการพยายามที่จะเป็นรูท เข้ามาในระบบ ซึ่งบัญชีผู้ใช้นี้จะต้องได้รับการป้องกันให้ปลอดภัยที่สุด โดยมีแนวทางดังนี้

5.1 อย่าใส่ไดเรกทอรีปัจจุบัน (.) และไดเรกทอรี bin ของผู้ใช้ ไว้ในเส้นทางการค้นหาของรูท เพราะว่าเมื่อรูท มีการเปลี่ยนไปยังไดเรกทอรีของผู้ใช้ในระบบ และเรียกใช้โปรแกรมอรรถประโยชน์หรือคำสั่งของระบบเอง อาจเป็นการไม่ปลอดภัยถ้าผู้ใช้นั้น ได้สร้างโปรแกรมเลียนแบบโปรแกรมอรรถประโยชน์หรือคำสั่งของระบบปลอมแปลงขึ้นมา แล้วมีโปรแกรมประเภทม้าโทรจันซ่อนอยู่

5.2 ในการใช้คำสั่ง su เพื่อเป็นผู้ใช้พิเศษในระบบ ควรเรียกใช้คำสั่งที่ /bin/su แทนที่จะเรียก su เพียงอย่างเดียว เนื่องจากอาจมีการสร้างโปรแกรม su ปลอมขึ้นมาเป็นโปรแกรมประเภทม้าโทรจัน ที่อาจมีการดักจับรหัสผ่านของผู้ใช้พิเศษได้

5.3 ไม่ควรที่จะรันโปรแกรมของผู้ใช้ในขณะที่เป็นรูท เนื่องจากอาจติดกับดักโปรแกรมประเภทม้าโทรจัน

5.4 ไม่ควรที่จะทิ้งเชลล์ในฐานะผู้ใช้พิเศษหรือรูทไว้ที่หน้าจอ ในขณะที่ไม่อยู่แม้แต่ เสี้ยวนาที หรือปล่อยให้ผู้อื่นมาใช้งานในขณะที่เป็นผู้ใช้พิเศษอยู่

5.5 ควรมีการเปลี่ยนรหัสผ่านของรูทบ่อย ๆ

5.6 ในการก่อนที่จะใช้บัญชีผู้ใช้ รูท ให้เข้าสู่ระบบด้วยบัญชีผู้ใช้ธรรมดาก่อน แล้วถึงใช้คำสั่ง su ในการสลับเปลี่ยนมาเป็นผู้ใช้พิเศษนี้

3.2.2 โมดูลในการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ

โมดูลนี้เขียนเป็นแนวทางเพื่อให้ได้ความมั่นคงในด้านการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ พร้อมด้วยแนวทางของคู่มืออำนวยความสะดวกที่ไว้ใจได้

วัตถุประสงค์

1. เพื่อแยกการทำงานของผู้ปฏิบัติการกับผู้ดูแลระบบ
2. เพื่อทำการแยกกันทางตรรกภาพและกายภาพของฐานข้อมูลที่เกี่ยวข้องกับงานต่าง ๆ
3. เพื่อเพิ่มความมั่นคงโดยการให้สิทธิที่น้อยที่สุด ตามความจำเป็นในการใช้ฐานข้อมูล

ปัญหาที่พบ

จุดอ่อนของด้านนี้อยู่ที่ บทบาทในการดูแลและจัดการระบบ แบ่งเป็น 3 รูปแบบได้แก่

1. การแก้ไขฮาร์ดแวร์หรือซอฟต์แวร์ของผู้ไม่มีสิทธิ หรือการแก้สภาวะแวดล้อมของระบบ
2. การเจาะระบบโดยแทรกแซงหน้าที่ของผู้ดูแลระบบ
3. การใช้อำนาจหน้าที่ของผู้ดูแลระบบในทางที่ผิด

แนวทางการออกแบบการป้องกันและการแก้ไข

การจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ มีการกำหนดความต้องการของเกณฑ์ความมั่นคงต่าง ๆ ดังนี้

1. นโยบายด้านความมั่นคง

ในคู่มืออำนวยความสะดวกที่ไว้ใจได้ ต้องระบุนโยบายด้านความมั่นคงไว้ดังนี้

1.1 การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ มีการกำหนดโหมดของสิทธิในการใช้งานไว้ที่ตัวกระทำ และกำหนดคุณสมบัติของผู้ใช้ไว้ที่ไฟล์ /etc/passwd ดังนี้

รูปแบบโหมดของไฟล์ -rwxrwxrwx หมายถึงสิทธิในการอ่าน เขียน และทำงาน ได้ ของเจ้าของไฟล์ กลุ่มผู้ใช้เดียวกับเจ้าของไฟล์ และผู้ใช้อื่น ตามลำดับ ในการใช้ไฟล์นี้ได้

รูปแบบของไฟล์ /etc/passwd มี 7 เขตข้อมูลดังนี้

```
user_account:encrypted_passwd:UID:GID:user_info:home_dir:login-shell
```

user_account	หมายถึงบัญชีชื่อผู้ใช้
encrypted_passwd	หมายถึงรหัสผ่านของผู้ใช้
UID	หมายถึงเลขรหัสประจำตัวผู้ใช้
GID	หมายถึงเลขรหัสกลุ่มของผู้ใช้
user_info	หมายถึงข้อมูลของตัวผู้ใช้
home_dir	หมายถึงไดเรกทอรีที่ผู้ใช้ครอบครอง
login-shell	หมายถึงเชลล์ที่ผู้ใช้ทำงานในการเข้าสู่ระบบ

1.2 การควบคุมการเข้าถึงภายใต้อาณัติ

มีการกำหนดการแบ่งระดับของความมั่นคง ให้กับตัวถูกกระทำและตัวกระทำ โดยมีการระบุป้ายความไหวให้ทั้งตัวถูกกระทำและตัวกระทำ โดยที่ป้ายความไหวมีดังนี้

ระดับความสำคัญของข้อมูล [กลุ่มของขอบเขต]

2. การชี้แจงรายการ

2.1 การแสดงตนและพิสูจน์ตน

มีคำสั่งที่เกี่ยวข้องในการจัดการได้แก่ คำสั่ง passwd , chfn ใช้ในการเปลี่ยนข้อมูลเกี่ยวกับผู้ใช้ รวมทั้งการเข้าสู่ระบบของผู้ใช้

2.2 การตรวจสอบ

ในคู่มืออำนวยความสะดวกที่ไว้ใจได้ ต้องระบุกลไกการตรวจสอบและการจัดการรายการตรวจสอบ คำอธิบายเหตุการณ์ในรายการตรวจสอบ ตัวอย่างเช่น

ตัวอย่างไฟล์ syslog.conf

```
# syslogd config file
# facilities: kern user mail daemon auth syslog lpr binary
# priorities: emerg alert crit err warning notice info debug


kern.debug          /var/adm/syslog.dated/kern.log
user.debug          /var/adm/syslog.dated/user.log
mail.debug          /var/adm/syslog.dated/mail.log
daemon.debug        /var/adm/syslog.dated/daemon.log
auth.debug          /var/adm/syslog.dated/auth.log
syslog.debug        /var/adm/syslog.dated/syslog.log
lpr.debug           /var/adm/syslog.dated/lpr.log
msgbuf.err          /var/adm/crash/msgbuf.savecore
kern.debug          /var/adm/messages
kern.debug          /dev/console
*.emerg                 *
```

facilities หมายถึงส่วนที่เราต้องการตรวจสอบ เช่น

kern หมายถึง การตรวจสอบที่แก่นของระบบปฏิบัติการ

user หมายถึงผู้ใช้ทั่วไป

auth หมายถึง การตรวจดูการใช้สิทธิในการเข้าสู่ระบบ รวมทั้งการใช้คำสั่ง su

priorities หมายถึงระดับการบันทึกเหตุการณ์ที่เกิดขึ้น เช่น

emerg หมายถึงให้บันทึกเมื่อมีเหตุการณ์ฉุกเฉิน เช่น ระบบขัดข้องอย่างกระทันหัน ซึ่งจะต้องมีการประกาศไปยังผู้ใช้ทุกคน

alert หมายถึง ระดับเหตุการณ์ที่ควรจะต้องมีการแก้ไขในทันที เช่น การเสียหายของฐานข้อมูลของระบบ

crit หมายถึง เหตุการณ์ที่วิกฤติ เช่น การทำงานผิดพลาดของฮาร์ดแวร์

ซึ่งในส่วนคอลัมน์แรกเป็นการเลือกส่วนและ ระดับเหตุการณ์ในการบันทึก และในคอลัมน์ด้านขวาจะเป็นการระบุไฟล์ที่ใช้เก็บการตรวจสอบ โดยที่จะมีการแยกไดเรกทอรีเป็นรายวัน ในการเก็บไฟล์รายการตรวจสอบต่าง ๆ เช่น

ตัวอย่างไฟล์ kern.log

```
Jan 30 12:30:25 kmitnb04 vmunix: fork/procdup: task_create failed. Code: 0x11
```

ตัวอย่างไฟล์ syslog.log

```
Jan 30 00:34:06 kmitnb04 syslogd: restart
```

ตัวอย่างไฟล์ daemon.log

```
Jan 28 22:58:55 kmitnb04 netacl[2713]:permit host=unknow/202.44.41.9
service=telnetd  execute=/usr/sbin/telnetd
Jan 28 23:41:05 kmitnb04 netacl[2650]:deny host=kmitnb5/202.44.32.2
service=rlogind  execute=/usr/sbin/rlogind
```

ตัวอย่างไฟล์ /var/adm/syslog.dated/auth.log เก็บข้อมูลดังนี้

```
บรรทัดที่ 1     Jan 31 10:54:58 kmitnb04 su: BADSU ingres on /dev/ttyp3
บรรทัดที่ 2     Jan 31 10:55:23 kmitnb04 su: SU took on /dev/ttyp4
บรรทัดที่ 3     Jan 31 11:02:46 kmitnb04 su: BADSU took on /dev/ttyp4
```

จากตัวอย่างไฟล์ auth.log ของวันที่ 31 Jan จะสัมพันธ์กับไฟล์ /var/adm/sialog ดังนี้

ตัวอย่างไฟล์ /var/adm/sialog

```
SIA:ERROR Fri Jan 31 10:54:58 1997
Failure on authentication for su from ingres to root
SIA:EVENT Fri Jan 31 10:55:23 1997
Successful authentication for su from took to root
SIA:ERROR Fri Jan 31 11:02:46 1997
Failure on authentication for su from took to root
```

โดยมีคำสั่งที่ใช้จัดการกับการตรวจสอบ ดังนี้

-audit_setup ใช้ในการตั้งค่าสภาวะแวดล้อมในการตรวจสอบระบบ

-auditmask ใช้ในการเลือกเหตุการณ์ในรายการตรวจสอบ

-audgen ใช้ในการสร้างรายการตรวจสอบ ที่ระบุข้อความได้

-auditd เป็นการสั่งหรือกระตุ้นให้โปรแกรมการตรวจสอบระบบทำงาน

-audit_tool ใช้ในการเลือกหรือกรองข้อมูลที่เก็บอยู่ในรายการตรวจสอบมาแสดงในรูปแบบที่ต้องการได้

3. การประกันในทางปฏิบัติ

3.1 สถาปัตยกรรมของระบบ

โปรแกรมทีซีบีและโครงสร้างข้อมูลจะต้องสนับสนุนการทำงานดูแลระบบ

และโครงสร้างทีซีบี มักจะเป็นสิ่งที่มองไม่เห็น การซ่อนของข้อมูลและลำดับชั้น จะต้องประยุกต์เข้ากับการทำงานของทีซีบีที่ใช้พัฒนาบทบาทของการดูแลและจัดการระบบ

3.2 การจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ

การทำงานของการดูแลและจัดการระบบจะแยกกันอย่างเด็ดขาดในส่วนที่เกี่ยวข้องกับความมั่นคงกับส่วนที่ไม่เกี่ยวข้อง งานในส่วนที่สัมพันธ์เกี่ยวข้องกับความมั่นคงต้องมีการจำกัดทำงานเฉพาะในส่วนที่จำเป็นจริง ๆ ทุกการกระทำของบุคคลที่เกี่ยวข้องกับความมั่นคงจะต้องมีการบันทึกไว้ตรวจสอบ การทำงานของผู้ดูแลระบบด้านความมั่นคงกับบุคลากรต่าง ๆ ต้องมีการแยกจากกันในระหว่างผู้เขียนโปรแกรมระบบ ผู้ดูแลระบบด้านความมั่นคง ผู้ตรวจสอบ ผู้ปฏิบัติการด้าน ความมั่นคง โดยแยกทั้งสิทธิ และฐานข้อมูลที่ใช้ มีการตั้งระดับของการไว้ใจได้ให้แตกต่างกันสำหรับบุคลากรต่าง ๆ โดยขึ้นอยู่กับ ส่วนที่มีผลต่อความมั่นคงของระบบ

3.3 การฟื้นฟูการไว้ใจได้

จะสนับสนุนการทำงานของทีซีบีที่มีต่อบทบาทของการดูแลและจัดการระบบ

4. การประกันแบบวงจรชีวิต

4.1 การทดสอบความมั่นคง

การทดสอบความต้องการด้านความมั่นคงทั้งหมดของระดับขั้น B3 ที่มีต่อทีซีบี จะเน้นการติดต่อกับบทบาทของผู้ดูแลระบบ

4.2 การออกแบบลักษณะเฉพาะและทำการพิสูจน์

จะเน้นการติดต่อกับบทบาทของผู้ดูแลระบบ

4.3 การจัดการสัณฐาน

ไม่มีความต้องการเพิ่มเติม

5. เอกสารสำหรับการวิจัย

5.1 คู่มืออำนวยความสะดวกที่ไว้ใจได้ ประกอบด้วยสิ่งต่อไปนี้ คือ

- มีการอ้างถึงการดูแลและจัดการระบบ ซึ่งจะมีคำเตือนเมื่อมีการทำงานที่มีผลต่อความมั่นคงของระบบ
- มีวิธีการในการทดสอบและรักษาไฟล์ตรวจสอบ
- มีรายละเอียดและโครงสร้างของเหตุการณ์ตรวจสอบทั้งหมด
- อธิบายถึงหน้าที่และการทำงานของผู้ปฏิบัติการและผู้ดูแลระบบ ในส่วนที่เกี่ยวข้องกับความมั่นคง ซึ่งจะรวมถึงการเปลี่ยนคุณสมบัติด้านความมั่นคงของผู้ใช้ด้วย
- มีคำแนะนำในการใช้กลไกการป้องกันระบบอย่างมีประสิทธิภาพ

- มีคำอธิบายคุณสมบัติของการป้องกันที่มีต่อระบบ

- มีคำแนะนำ อำนวยความสะดวกในการใช้งาน คำเตือน และสิทธิต่าง ๆ ที่จำเป็นต้องอยู่ในความควบคุม ในการปฏิบัติให้ระบบอยู่ภายใต้ความมั่นคง

- แยกแยะโมดูลของทีซีบี ที่เก็บกลไกในการอ้างอิงความเที่ยงตรงของระบบ

- อธิบายขั้นตอน สำหรับการสร้างทีซีบีขึ้นมาใหม่ หลังจากที่มีการเปลี่ยนแปลงโมดูลใด ๆ ในทีซีบี

- ขั้นตอนที่ทำให้สามารถมั่นใจได้ว่า การเริ่มต้นระบบให้อยู่ในสถานะที่มั่นคง และมีชุดขั้นตอนที่สรุปได้ว่าการปฏิบัติการต่อระบบไม่ว่าจะผ่านไปนานเพียงใด ระบบยังคงต้องมีความมั่นคงอยู่

ตัวอย่างการแยกหน้าที่ของผู้ดูแลระบบในคู่มืออำนวยความสะดวก ในระบบที่มีความมั่นคงในระดับสูงจะต้องมีผู้ดูแลระบบและผู้ดูแลด้านความมั่นคงของระบบทำหน้าที่แยกกันดังนี้

1. บทบาทและหน้าที่ของผู้ดูแลระบบ

- สร้างหรือเพิ่มรายชื่อผู้ใช้ในระบบ โดยมีการตั้งค่าหรือคุณสมบัติให้กับบัญชีชื่อผู้ใช้ เป็นค่าโดยปริยาย โดยที่ในระบบปฏิบัติการโอเอสเอฟวันมีโปรแกรมชื่อ adduser ใช้สำหรับทำการเพิ่มบัญชีชื่อผู้ใช้ให้โดยอัตโนมัติ

- สร้างหรือเพิ่มรายชื่อกลุ่ม รายชื่อกลุ่มจะถูกนำไปใช้ในกลไกของการเข้าถึงข้อมูลโดยใช้ ดุลยพินิจหรือดีเอซี คำสั่งที่ใช้ในการเพิ่มกลุ่มในระบบปฏิบัติการโอเอสเอฟวันคือ addgroup

- สร้างหรือเพิ่มระบบไฟล์ใหม่ โดยใช้คำสั่ง newfs และทำการตรวจสอบระบบไฟล์ โดย ใช้คำสั่ง fsck

- ถ้ามีการลบไฟล์ของระบบหรือไฟล์ของผู้ใช้โดยบังเอิญ ต้องทำการสร้างกลับมาใหม่ได้

2. บทบาทและหน้าที่ของผู้ดูแลความมั่นคงของระบบ

- ทำการกำหนดค่าให้กับอุปกรณ์ในระบบเช่น เทอร์มินอล เครื่องพิมพ์ จานหรือเทป แม่เหล็ก โดยต้องกำหนดค่าพารามิเตอร์ต่าง ๆ ให้กับอุปกรณ์ให้ถูกต้อง คำสั่งที่ใช้ในการกำหนดค่าอุปกรณ์คือ คำสั่ง devassign

- กำหนดค่าโดยปริยายของระบบ เช่นการกำหนดค่าพารามิเตอร์ของรหัสผ่านของผู้ใช้ หรือค่าเริ่มต้นเมื่อผู้ใช้เข้าสู่ระบบ คำสั่งที่ใช้กำหนดค่าโดยปริยายคือ คำสั่ง default

- การเปลี่ยนแปลงหรือแก้ไขบัญชีผู้ใช้ เช่นการสร้างโปรไฟล์ (Profile) ของการพิสูจน์ตน หรือการเพิ่มสิทธิของผู้ใช้ มีคำสั่งที่ใช้ในการจัดการคือ คำสั่ง prpasswd หรือ prpwd

- ตรวจสอบการทำงานของระบบ โดยเลือกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงของระบบ การตั้งค่าพารามิเตอร์ที่ใช้ในการตรวจสอบ การสร้างรายงานการตรวจสอบ

- ตรวจสอบความถูกต้องเชื่อถือได้ของระบบ โดยใช้คำสั่ง authck ในการตรวจสอบ โครงสร้างรวมของฐานข้อมูลที่เกี่ยวข้องในการป้องกันระบบ

3. บทบาทและหน้าที่ของผู้ปฏิบัติการ

- ดูแลและจัดการเกี่ยวกับเครื่องพิมพ์

- เปิดและปิดเครื่อง หรือระบบ ทำการบูธ (Boot) หรือเปลี่ยนระดับการทำงานของระบบ

- การต่อ (mount) และการเลิกต่อ (unmount) ระบบไฟล์

- การทำสำเนาและการสร้างข้อมูลกับมาใหม่

5.2 เอกสารทดสอบ ใช้ทดสอบฟังก์ชันงานของทีซีบี และการเชื่อมต่อกับบทบาทของการดูแลระบบ

5.3 เอกสารการออกแบบ ในเอกสารจะประกอบด้วยรายละเอียด ดังนี้

- การติดต่อกันของโมดูลต่าง ๆ ในทีซีบีที่เกี่ยวกับบทบาทการดูแลระบบ

- ระบุ กลไกในการป้องกันทีซีบี ที่ใช้สำหรับแยกบทบาทในการดูแลระบบ

- อธิบายรายละเอียดของโมดูลทีซีบีที่ใช้ติดต่อกับบทบาทการดูแลระบบ

- กฎของการใช้สิทธิอย่างน้อยสุด ในการทำงานและติดต่อของทีซีบีที่ใช้ในการพัฒนาบทบาทการดูแลระบบ

- การบันทึกการตรวจสอบบทบาทของการดูแลระบบ

3.2.3 โมดูลในการจัดการระบบหลังการล้มเหลว

โมดูลนี้เขียนเป็นแนวทางเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการฟื้นฟูการไว้ใจได้

วัตถุประสงค์

การฟื้นฟูสภาพระบบหลังการล้มเหลว เพื่อสามารถทำให้ระบบทำงานได้อีกครั้ง โดยข้อมูลและสภาพแวดล้อมต่าง ๆ ของระบบต้องกลับคืนสู่ในสภาวะปกติก่อนเกิดการล้มเหลว

ปัญหาที่พบ

ระบบ มักอาจเกิดการล้มเหลว ไม่สามารถทำงานได้ โดยอาจเกิดจากสาเหตุทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ เช่น ไฟฟ้าลัดวงจร ดิสต์พัง แหล่งจ่ายไฟไม่ทำงาน การเจาะระบบของนักเจาะระบบที่เข้ามาวางกับดักไว้ตามโปรแกรมที่ทำงานแล้วมีผลต่อฐานข้อมูลของระบบ หรือโปรแกรมประเภทไวรัส เป็นต้น

แนวทางการออกแบบการป้องกันและการแก้ไข

กลไกการจัดการระบบหลังการล้มเหลว การฟื้นฟูสภาพจำเป็นต้องอาศัยข้อมูลหรือสภาวะแวดล้อมของระบบต่าง ๆ ที่มีอยู่ก่อนหน้านี้มาใช้ ซึ่งสิ่งที่จำเป็นและสำคัญในการนี้คือการทำสำเนาข้อมูล โดยส่วนใหญ่มักอาศัยสื่อข้อมูลภายนอกมาใช้ในการทำสำเนา เช่น เทป ต้องมีการสร้างตารางการทำสำเนาที่ดีรวมทั้งระบุระดับในการทำสำเนาด้วย เพื่อประโยชน์ในการสร้างข้อมูลใหม่กลับคืนมา โดยสรุปเป็นแนวทางได้ดังนี้

1. การนำเทปสำเนามาซ่อมแทนที่
2. ตรวจสอบไฟล์ที่เกี่ยวข้องในการให้ระบบเริ่มทำงานใหม่ ดังนี้

   2.1 `/tcb/files/auth/r/root`

ถ้าฐานข้อมูลในการรักษารหัสผ่านของผู้ใช้ เสียหาย โดยเฉพาะข้อมูลของผู้ใช้ พิเศษ (root) ไม่อยู่ในสภาพอันควร ให้ทำการเริ่มระบบใหม่โดยเข้าสู่โหมดของผู้ใช้คนเดียว จากนั้นให้จัดการแก้ไขไฟล์ `/tcb/files/auth/r/root` ให้มีค่าโดยปริยายดังนี้

```
root:u_name=root:u_id#0:\
    :u_pwd=encrypted_password:\
    :u_minchg#0:u_pickpw:u_nullpw:u_restrict@:\
    :u_maxtries#100:u_lock@:chkent:
```

2.2 /etc/auth/system/ttys

การตรวจดูฐานข้อมูลควบคุมจอเทอร์มินอล โดยเฉพาะข้อมูลของจอคอลโซลของระบบ ต้องมีการตั้งค่าไฟล์ /etc/auth/system/ttys ดังนี้

```
console:t_devname=console:chkent:
```

2.3 /etc/auth/system/default

ฐานข้อมูลค่าโดยปริยายของระบบ จะต้องตั้งค่าเริ่มต้นเป็นค่าโดยปริยาย ดังนี้

```
default:\
      :d_name=default:\
      :d_boot_authenticate@:\
      :d_audit_enable@:\
      :d_pw_expire_warning#3456000:\
      :u_pwd=*:\
      :u_minchg#0:u_maxlen#20:u_exp#157248000:\
      :u_life#31449600:\
      :u_pickpw:u_genpwd:u_restrict@:u_nullpwd@:\
      :u_genchars:u_genletters:u_maxtries#5:u_lock@:\
      :t_logdelay#1:t_maxtries#5:t_lock@:\
      :t_login_timeout#60:\
      :chkent:
```

2.4 /etc/auth/system/devassign

ถ้าข้อมูลสำหรับจอคอลโซลไม่เที่ยงตรง ก็จะไม่มีโปรแกรมประยุกต์ใดสามารถทำงานได้ จะต้องมาทำการกำหนดค่าฟิลด์แรกของฐานข้อมูลกำหนดค่าอุปกรณ์ ด้วยคำว่า console พร้อมทั้งมีการระบุค่าตามนี้

```
console:v_devs=/dev/console:v_type=terminal:\
      :chkent:
```

2.5 /etc/passwd

ฐานข้อมูลเก็บข้อมูลของผู้ใช้ จะต้องมีข้อมูลตามรูปแบบที่ถูกต้อง คือมีฟิลด์ครบ ดังนี้

```
useraccount:*:UID:GID:user-infomation:home-directory: login-shell
```

ซึ่งสามารถใช้คำสั่ง /tcb/bin/authck มาช่วยในการตรวจสอบ

2.6 /etc/group

ฐานข้อมูลกลุ่ม จะต้องจัดให้อยู่ในรูปแบบที่ถูกต้อง

2.7 /etc/auth/system/pw_id_map

ฐานข้อมูลในการผูกชื่อผู้ใช้ให้เข้ากับหมายเลข

2.8 /etc/auth/system/gr_id_map

ฐานข้อมูลในการผูกชื่อกลุ่มให้เข้ากับหมายเลข

2.9 /sbin/rc[023]s

เป็นไฟล์ ที่ใช้สำหรับเริ่มต้นให้ระบบทำงานเรียกใช้โดย init ในการเปลี่ยนระหว่างระดับของการทำงาน ซึ่งควรมีการทำสำเนาไฟล์เหล่านี้ไว้หลังจากการติดตั้งระบบเสร็จสมบูรณ์

2.10 /dev/console

เป็นไฟล์ที่ระบุคุณสมบัติของอุปกรณ์ที่เกี่ยวข้องกับจอคอลโซลของระบบ

2.11 /dev/tty*,/dev/pty*,/dev/ptm*,/dev/pts/*

เป็นไฟล์อุปกรณ์เทอร์มินอลเสมือน ใช้สำหรับติดต่อสื่อสารกันระหว่างโปรเซส

2.12 /sbin/sh

เป็นเชลล์ในการเปลี่ยนไปสู่สถานะของโหมดผู้ใช้คนเดียว

2.13 /vmunix

เป็นไฟล์อุปมาของระบบปฏิบัติการ ใช้ในการบูธระบบ

3.2.4 โมดูลในการทดสอบระบบ

โมดูลนี้เขียนเป็นแนวทาง เพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการทดสอบความมั่นคง และแนวทางการเขียนเอกสารทดสอบ

วัตถุประสงค์

เพื่อให้นักพัฒนาระบบทดสอบความมั่นคงของระบบในทุก ๆ ด้าน และมั่นใจได้ว่าระบบทำงานเป็นไปตามที่อธิบายไว้ในเอกสารการทดสอบ

ปัญหาที่พบ

มักเกิดจากผู้ดูแลระบบ ที่ไม่ได้ตรวจสอบระบบโดยถี่ถ้วน ซึ่งผู้ดูแลระบบอาจไม่มีความรู้เพียงพอ หรืออาจเกิดจากเอกสารที่ขาดความชัดเจน

แนวทางการออกแบบ

1. การทดสอบกลไกความมั่นคงในด้านต่าง ๆ ประกอบด้วย การทดสอบการควบคุมการเข้าถึงโดยใช้ดุลยพินิจ การทดสอบที่เกี่ยวข้องกับป้ายชื่อ การควบคุมการเข้าถึงภายใต้อาณัติ การทดสอบด้านการแสดงตนและพิสูจน์ตน การทดสอบเส้นทางการไว้ใจได้ และการทดสอบกลไกการตรวจสอบต่าง ๆ

2. การทดสอบในการอินเทอร์เฟส เป็นการทดสอบ การทำงานของผู้ใช้ทั้งหมดที่เกี่ยวข้อง กับความมั่นคงของระบบ หรือการทำงานที่เกี่ยวข้องกับทีซีบี

3. เอกสารการทดสอบต้องมีการระบุ ขั้นตอน ในการทดสอบความมั่นคงของกลไกต่าง ๆ รวมทั้งผลของการทดสอบที่ได้ด้วย มีแผนการณ์การทดสอบ สมมติฐานของสภาวะแวดล้อมในการทดสอบ ผลที่คาดว่าจะได้รับและผลที่แท้จริง

4. แนวทางการตรวจสอบระบบปฏิบัติการโอเอสเอฟวัน

4.1. การตรวจสอบไฟล์รายการตรวจสอบ โดยมากไฟล์เหล่านี้มักเก็บอยู่ภายใต้ /var/adm

4.2. ไฟล์หลบซ่อนในระบบ นักเจาะระบบมักมีความรอบครอบในการลบร่องรอยและหลบซ่อนการกระทำของตน ซึ่งผู้ดูแลระบบควรทำการตรวจตราไฟล์หลบซ่อนต่าง ๆ ทั้งระบบ เช่น ไฟล์ที่ขึ้นต้นด้วย . (จุด) หรือ '...' (จุด จุด จุด) หรือ '.. ' (จุด จุด ช่องว่าง 2 ตำแหน่ง) หรืออาจใช้พวกตัวอักขระควบคุมเช่น '..^G' (จุด จุด คอนโทรลจี) เป็นต้น

4.3. การตรวจสอบเอซีแอลของไฟล์ ,ไดเรกทอรีและไฟล์อุปกรณ์ เช่นตรวจหาไฟล์ที่สามารถเขียนโดยผู้ใช้ใด ๆ ก็ได้ในระบบ โดยการใช้คำสั่งดังนี้

```
# find / -perm -2 ! \(  -type l  -o  -type p  -o  -type s \)  -print
```

หรือการตรวจหาไฟล์ที่ มีสิทธิการใช้งานเป็น root (SUID ไฟล์และ SGID ไฟล์) โดยใช้คำสั่ง

```
# find  / \(  -perm  -002000  -o  -perm  -004000  \)  -print
```

4.4. ตรวจสอบไฟล์ไบนารี่ของระบบ เช่นไฟล์ `login,su,telnet,ls,du, netstat,ifconfig,find,df,libc,sync` และไฟล์อื่น ๆ ที่อ้างอิงในไฟล์ /etc/inetd.conf

4.5. ตรวจสอบไฟล์ทั้งหมดที่ถูกนำไปใช้งานโดยคำสั่ง `cron` หรือ `at` โดยมากนักเจาะระบบจะสร้างประตูกล (back doors) ไว้ในไฟล์ที่ถูกนำไปใช้งานโดยคำสั่ง `cron` หรือ `at` ซึ่งเทคนิคนี้ ทำให้นักเจาะระบบสามารถกลับเข้าสู่ระบบได้ หลังจากที่ถูกเขี่ยออกจากระบบ โดยผู้ดูแลระบบแล้วก็ตาม

4.6. ตรวจสอบไฟล์ /etc/inetd.conf เนื่องจากไฟล์นี้เป็นไฟล์ฐานข้อมูลที่เก็บค่าโดยปริยายเกี่ยวกับสัณฐานของระบบ ควรจะต้องทำการตรวจสอบระวังดูว่าอาจมีโปรแกรมประเภทม้าโทรจันซ่อนอยู่

4.7. ไฟล์สัณฐานของระบบและเครือข่าย เช่นการตรวจดูที่ไฟล์ /etc/hosts.equiv ต้องดูว่าไม่ควรมี เครื่องหมาย + (บวก) ในไฟล์นี้ รวมทั้งตรวจหาไฟล์ .rhosts ทั่วทั้งระบบ

4.8. ตรวจสอบไฟล์ /etc/passwd เช่นอาจใช้คำสั่งดังนี้ ในการตรวจดูว่ามีบัญชีผู้ใช้รายใดที่มีข้อมูลไม่ครบ 7 ฟิลด์

```
#awk -F:'NF !=7 || $3==0 || $2== " " {print $1 " " $2 " " $3}'\ <  /etc/passwd
```

4.9. ใช้คำสั่ง `/tcb/bin/authck` เพื่อตรวจสอบ ความถูกต้องอันควรของฐานข้อมูลที่เกี่ยวข้องในการป้องกันระบบ ได้แก่ไฟล์ `/etc/passwd, /tcb/files/auth/*/* , /tcb/auth/system/files, /etc/auth/system/ttys, /etc/auth/system/files` และ `/etc/auth/system/default`

3.2.5 โมดูลในการออกแบบลักษณะเฉพาะและทำการพิสูจน์

โมดูลนี้เขียนเป็นแนวทางมาเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการออกแบบลักษณะเฉพาะและทำการพิสูจน์ รวมถึงแนวทางการสร้างเอกสารการออกแบบ

วัตถุประสงค์

เพื่อทำการสร้างเอกสารและทำการพิสูจน์การออกแบบระบบความมั่นคงของระบบว่าเป็นไปตามเกณฑ์บรรทัดฐานหรือไม่ โดยอาศัยทฤษฎีทางคณิตศาสตร์ นอกจากนี้ยังเป็นการกระตุ้นให้ผู้ค้าฮาร์ดแวร์ได้เห็นความสำคัญของเอกสารด้านความมั่นคงของระบบ ตลอดวงจรของการใช้งาน รวมถึงการสร้างคู่มือในการสร้างความเข้าใจพื้นฐานระหว่างผู้ค้าฮาร์ดแวร์ และผู้พัฒนาระบบ

แนวทางการออกแบบ

1. อาศัยทฤษฎีทางคณิตศาสตร์ มาอธิบายนโยบายด้านความมั่นคงของระบบ

2. ในเอกสารการออกแบบ ต้องมีรูปแบบจำลองของนโยบายความมั่นคงอย่างเป็นทางการ โดยประกอบด้วย ตัวกระทำ ตัวถูกกระทำ โหมดของการเข้าถึง คุณสมบัติของความมั่นคง และการแปลงจากสภาวะเริ่มต้นของระบบไปสู่สภาวะที่ระบบมีความมั่นคง

3. มีการจับคู่ของคุณสมบัติด้านความมั่นคงเข้ากับนโยบายด้านความมั่นคง รวมทั้งอธิบายแนวคิดของการพัฒนาการจับตาดูระบบของทีซีบี ซึ่งต้องระบุไว้ในเอกสารการออกแบบ

4. ต้องแสดงการจับคู่ระหว่าง (Descriptive Top Level Specification) และ ทีซีบี โดยต้องแสดงให้เห็นด้วยว่า DTLS นั้น มีความเที่ยงตรงในแบบจำลองของนโยบายความมั่นคงอย่างเป็นทางการไว้ในเอกสารการออกแบบ

5. ความต้องการในการออกแบบเอกสาร ให้ได้ระดับขั้นความมั่นคงในขั้น B3

5.1. อธิบายหลักการกว้าง ๆ ของการป้องกัน

5.2. อธิบายรายละเอียดในการแปลงหลักการในการป้องกันมาอยู่ในรูปของทีซีบี

5.3. อธิบายถึงการแบ่งเป็นโมดูลของทีซีบี

5.4. อธิบายการติดต่อระหว่างโมดูลของทีซีบี

5.5. อธิบายการป้องกันตัวเองของทีซีบี

5.6. มีการแถลงนโยบายด้านความมั่นคงของระบบ

5.7. มีรูปแบบจำลองของนโยบายด้านความมั่นคงอย่างเป็นทางการ หรือไม่เป็นทางการ ที่บังคับโดยทีซีบี

5.8. อธิบายถึงแบบจำลองของนโยบายด้านความมั่นคงที่เพียงพอ ในการบังคับนโยบายด้าน ความมั่นคง

5.9. แยกแยะและอธิบายกลไกการป้องกันของทีซีบี

5.10. อธิบายกลไกของทีซีบีที่เป็นไปตาม แบบจำลองของนโยบาย ด้านความมั่นคง

5.11. มีการอธิบายอย่างเป็นทางการของแบบจำลองของนโยบายด้านความมั่นคง

5.12. มีการพิสูจน์ว่า แบบจำลองของนโยบายด้านความมั่นคง เพียงพอในการบังคับนโยบายด้าน ความมั่นคง

5.13. อธิบายการทำงานของทีซีบีในแนวความคิดของการจับตามองระบบ รวมทั้งกฎการห้ามละเมิดกลไกนี้

5.14. นำเสนอวิธีการการวิเคราะห์ช่องทางลับ

5.15. จำแนกเหตุการณ์การตรวจสอบที่เกี่ยวเนื่องกับช่องทางลับ

<u>แนวทางการออกแบบเอกสาร</u>

1. เอกสารด้านนโยบายความมั่นคง

อธิบายปรัชญาและแนวทางการป้องกันระบบ กลไกทั้งหมดของทีซีบี โดยเริ่มที่การกำหนดขอบเขตของระบบ และส่วนที่เกี่ยวข้องกับความมั่นคง โดยกลไกการป้องกันนั้นสามารถนำเสนอมาในรูปแบบที่เป็นทางการประกอบด้วย ตัวกระทำ ตัวถูกกระทำ โหมดของการเข้าถึง คุณสมบัติของความมั่นคง และการแปลงจากสภาวะเริ่มต้นของระบบไปสู่สภาวะที่ระบบมีความมั่นคง มีการจับคู่ของคุณสมบัติด้านความมั่นคงเข้ากับนโยบายด้านความมั่นคง รวมทั้งอธิบายแนวคิดของการพัฒนาการจับตาดูระบบของทีซีบี และต้องแสดงการจับคู่ระหว่าง (Descriptive Top Level Specification) และ ทีซีบี โดยต้องแสดงให้เห็นด้วยว่า DTLS นั้นมีความเที่ยงตรงในแบบจำลองของนโยบายความมั่นคงอย่างเป็นทางการ

2. เอกสารกลไกในการป้องกันทีซีบี

2.1 อธิบายกลไกในการป้องกันทีซีบี เช่นนโยบายในการควบคุมการเข้าถึง การแสดงตนและการพิสูจน์ตน

2.2 อธิบายการทำงานในการสนับสนุนส่วนของสถาปัตยกรรมของระบบที่เพิ่มขึ้นมาสำหรับการ แยกการทำงานของโปรเซส โดยที่กลไกการแยกการทำงานของโปรเซสสามารถป้องกันผู้กระทำ ต่าง ๆ จากการเข้าถึงในการใช้พื้นที่ทำงานแยกจากกัน

2.3 อธิบายถึงหลักการของแนวคิดในการเฝ้ามองและติดตามการเข้าถึงของตัวกระทำที่กระทำการใด ๆ ต่อตัวถูกกระทำ โดยห้ามมีการข้ามผ่านการตรวจสอบ ในการเฝ้ามองนี้สำหรับเฟิร์มแวร์ ต้องอธิบายถึงการทำงานอย่างน้อยในระดับของการทำอินเทอร์รัพท์ คำสั่งที่เกี่ยวข้องกับ I/O รวมทั้งการอธิบายการเชื่อมโยงกับสิ่งต่าง ๆ ที่อยู่ภายในทีซีบี แต่อยู่นอกเหนือจากการเฝ้ามอง เช่น ตัวควบคุมดิสต์ เครื่องพิมพ์ เป็นต้น

2.4 ใส่รายละเอียดแยกการทำงานสำหรับผู้ดูแลระบบ ผู้ดูแลความมั่นคงของระบบและผู้ตรวจสอบระบบ

3. เอกสารของช่องทางลับ

3.1 ในเอกสารควรมีการนำเสนอ ผลของการวิเคราะห์ช่องทางลับและวิธีการที่ใช้ โดยมีภาพรวม ของการวิเคราะห์ช่องเก็บลับ ขั้นตอนและผลของการทดสอบ

3.2 รายการตรวจสอบทั้งหมดที่ได้ควรมีการจำแนกและอธิบายถึงช่องเก็บลับทั้งหมดที่ยังไม่ได้ กำจัดออกจากระบบ

3.3 ในเอกสารควรอธิบายถึงการกระทำต่าง ๆ และผลในการลดประสิทธิภาพการทำงานของระบบ เมื่อมีการจำแนกช่องทางลับที่อาจกระทำการบางอย่างแล้วมีผลกับแบนวิธของช่องทางนั้น ๆ

3.4 ในเอกสารควรมีการแนะนำช่องเวลาลับ การวิเคราะห์ ขั้นตอน รวมทั้งผลของการทดสอบ

3.2.6 โมดูลในการออกแบบการจัดการสัณฐาน

โมดูลนี้เขียนเป็นแนวทางเพื่อให้ได้ตามเกณฑ์ความมั่นคงในด้านการจัดการสัณฐาน

<u>วัตถุประสงค์</u>

1. เพื่อควบคุมการดูแลรักษาระบบตลอดการใช้งานในวงจรชีวิต เป็นการสร้างความมั่นใจว่าระบบนั้นมีนโยบายด้านความมั่นคง
2. ทำให้สามารถกลับคืนไปใช้ระบบในรุ่นก่อนหน้านี้ได้ ถ้าหากพบว่ามีปัญหาด้านความมั่นคงที่พบในรุ่นที่ใช้งานอยู่ในปัจจุบัน

<u>แนวทางการออกแบบการป้องกันและการแก้ไข</u>

1. การกำหนดค่าเอกสิทธิให้กับข้อมูลสัณฐานแต่ละตัว ซึ่งทำให้สามารถติดตามส่วนประกอบของแต่ละสัณฐานได้โดยเฉพาะ เช่น ส่วนประกอบทางด้านฮาร์ดแวร์ โปรแกรม หรือข้อมูลผู้ใช้ เป็นต้น
2. วางแผนการพัฒนาการจัดการสัณฐาน มีการกำหนดการติดตามข้อมูลสัณฐานแต่ละตัวอย่างชัดเจน เช่น ใครเป็นผู้เสนอ ประเมินค่า และรับรองหรือไม่รับรองการเปลี่ยนแปลง และความเร่งด่วนในเรื่องของเวลาที่ใช้ในการเปลี่ยนแปลงให้สำเร็จ
3. เก็บบันทึกการเปลี่ยนแปลงข้อมูลสัณฐานทั้งหมด เพื่อเป็นแนวทางในการตรวจสอบข้อมูลเหล่านั้นเมื่อมีการพิสูจน์
4. จัดตั้งคณะการควบคุมสัณฐาน โดยแบ่งตามขอบเขตของการพัฒนาระบบ เช่น ด้านวิศวกรรมระบบ ด้านการประกันคุณภาพ ด้านการสนับสนุนทางด้านเทคนิค เอกสารทางเทคนิค กลุ่มวิศวกรรมด้านความมั่นคง และกลุ่มผู้ใช้ เป็นต้น ควรมีการประชุมร่วมกัน ถ้าหากว่าต้องการทำการเปลี่ยนแปลงสัณฐาน ซึ่งการเปลี่ยนแปลงนั้น ต้องได้รับการรับรองหรือยอมรับในการนำมาปรับเปลี่ยนระบบได้

3.2.7 โมดูลการออกแบบสถาปัตยกรรมของระบบ

ความต้องการของสถาปัตยกรรมของระบบเพื่อให้ได้ระดับขั้นความมั่นคงในขั้น B3 มีดังนี้

1. มีการป้องกันการทำงานของฟังก์ชันต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงของระบบให้อยู่ภายใต้ขอบเขต ตัวอย่างเช่น โปรแกรมที่มีสิทธิสูง ๆ เช่น โปรแกรมที่เกี่ยวกับการเก็บรายการตรวจสอบความมั่นคงของระบบ ต้องไม่สามารถรบกวนโดยโปรแกรมของผู้ใช้โดยทั่วไปได้ ซึ่งในลักษณะนี้ สถาปัตยกรรมแบบวงแหวน สามารถช่วยแยกขอบเขตระหว่างโปรแกรมของผู้ใช้ทั่วไปกับโปรแกรมของระบบได้ โดยมากแล้วทีซีบีหรือแก่นความมั่นคงของระบบจะอยู่ที่วงแหวนในสุด และโปรแกรมของผู้ใช้จะอยู่ที่วงนอกสุด และวงต่าง ๆ ที่อยู่ระหว่างนี้ จะเป็นส่วนโปรเซส การให้บริการของระบบปฏิบัติการหรือโปรแกรมในการจัดการระบบต่าง ๆ

2. มีการป้องกันทรัพยากรในการควบคุมการเข้าถึงและการตรวจสอบ ซึ่งรวมถึงการป้องกันทรัพยากรต่าง ๆ ที่มีผลต่อความมั่นคง เช่นวิธีการใส่รายการการควบคุมการเข้าถึงลงในไฟล์รหัสผ่าน ซึ่งเป็นการป้องกันไฟล์ของผู้ใช้จากการเข้าถึงโดยผู้ใช้อื่นโดยเจตนาหรือไม่ก็ตาม

3. การแยกกันอย่างชัดเจนของโปรเซสในแต่ละพื้นที่ใช้งาน ซึ่งเป็นการสร้างความมั่นใจว่าเมื่อมีโปรเซสหลาย ๆ โปรเซสทำงานในขณะเดียวกันจะไม่รบกวนซึ่งกันและกัน เช่น การไปเขียนในหน่วยความจำของโปรเซสอื่น หรือการไปเปลี่ยนคำสั่งการทำงานของโปรเซสอื่น นอกจากนี้ยังต้องทำให้มั่นใจได้ว่าระบบสามารถเก็บลู่ทางการทำงานของทุกสิ่งที่จำเป็น เช่น รีจิสเตอร์ สถานะของข้อมูล ไว้ได้ ในการที่จะสลับไปทำโปรเซสอื่น ซึ่งเทคนิคของการใช้หน่วยความจำเสมือน มักถูกนำมาใช้ในการจัดเก็บการทำงานของโปรเซสหลาย ๆ โปรเซส ที่ทำงานพร้อมกัน โดยแต่ละโปรเซสจะมีที่อยู่เสมือนของตัวเองและปราศจากการรบกวนจากโปรเซสอื่น ๆ

4. การแบ่งโมดูลของทีซีบีในการบังคับการใช้สิทธิพิเศษให้น้อยที่สุด หมายถึงโมดูลที่จำเป็นต้องใช้สิทธิพิเศษของระบบจริง ๆ จะสามารถมาอยู่ในส่วนหรือขอบเขตของแก่นความมั่นคงได้

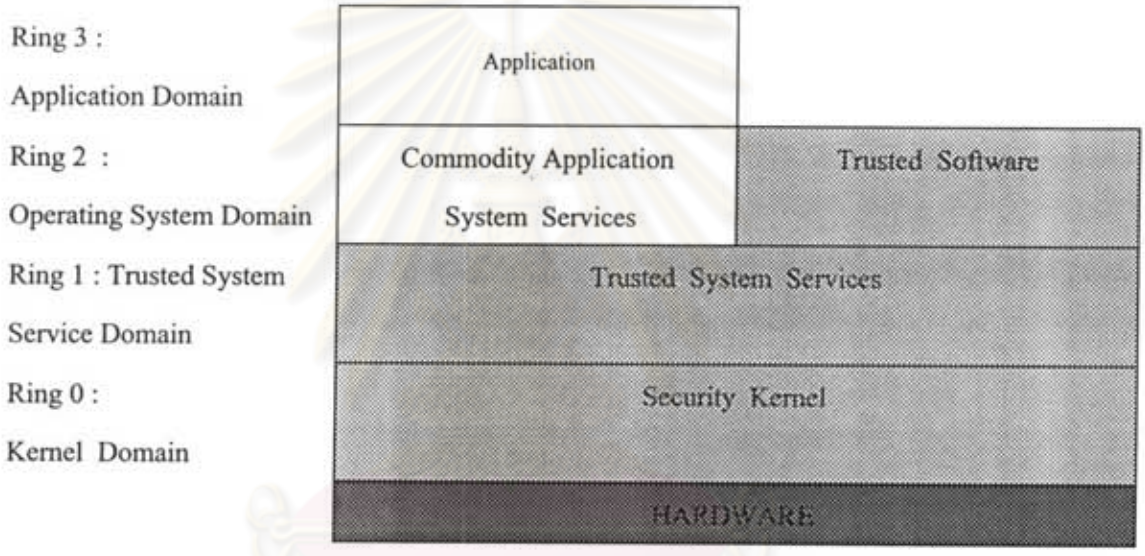
5. มีคุณสมบัติทางด้านฮาร์ดแวร์ในการแบ่งเซกเมนต์ โดยระบบสามารถแบ่งหน่วยความจำเสมือนออกเป็นเซกเมนต์ ซึ่งโปรเซสหนึ่ง ๆ อาจครอบครองได้หลายเซกเมนต์ตามความจำเป็นในการใช้งาน แต่มีข้อแม้ว่าโปรเซสของผู้ใช้ทั่วไปต้องไม่สามารถเข้าถึงหน่วยความจำที่ระบบปฏิบัติการใช้งานอยู่ได้

6. มีกลไกการป้องกันที่ละเอียดอ่อนในการบังคับให้มีคุณสมบัติบางอย่าง เช่น การแบ่งลำดับขั้นนัยสำคัญ การซ่อนของข้อมูล ซึ่งการแบ่งเป็นลำดับขั้นนี้ ลำดับขั้นต่ำสุดจะเป็น

การทำงานของฟังก์ชันพื้นฐาน ส่วนในลำดับขั้นที่สูงกว่าจะทำงานที่มีฟังก์ชันงานซับซ้อนมากกว่า และมีการกำหนดอย่างชัดเจนในการติดต่อสื่อสารกันในระหว่างลำดับขั้น ส่วนการซ่อนของข้อมูล หมายถึง จะไม่สามารถเข้าถึงข้อมูลที่อยู่นอกเหนือจากลำดับขั้นเดียวกัน

แนวทางการออกแบบ

สถาปัตยกรรมของระบบ ควรแบ่งเป็นวงแหวน โดยแบ่ง 4 วงดังนี้



1. แก่นความมั่นคง ให้บริการพื้นฐานของระบบปฏิบัติการ การบริหารทรัพยากรของระบบ การจัดตารางเวลาของโปรเซส การควบคุมการอินเทอร์รัพ การตรวจสอบ และการควบคุมการใช้นโยบายความมั่นคงทั้งการเข้าถึงโดยใช้ดุลยพินิจและการเข้าถึงภายใต้อาณัติสำหรับควบคุมโปรเซสและอุปกรณ์ต่าง ๆ

2. ส่วนการบริการของระบบที่ไว้ใจได้ ได้แก่ การจัดการเกี่ยวกับ I/O การบริการเครือข่าย การจัดการระบบไฟล์ การบังคับใช้นโยบายการควบคุมการเข้าถึงโดยใช้ดุลยพินิจสำหรับตัวกระทำที่เป็นไฟล์ ส่วนนี้ไม่สามารถเปลี่ยนแปลงหรือเรียกใช้โดยผู้ใช้ได้

3. ซอฟต์แวร์ที่ไว้ใจได้ ประกอบด้วยฟังก์ชันการทำงานทั้งหมด ที่เกี่ยวข้องกับความมั่นคง ซึ่งมีการทำงานแยกกันอย่างอิสระ กับ ส่วนการบริการติดต่อกับโปรแกรมประยุกต์ ในวงแหวนนี้จะเป็นขอบเขตของระบบปฏิบัติการ

4. ขอบเขตของโปรแกรมประยุกต์ ไว้สำหรับโปรเซสของผู้ใช้ทั่วไป

สำหรับระบบปฏิบัติการโอเอสเอฟวัน ไม่สามารถทำการเปลี่ยนแปลงในส่วนของสถาปัตยกรรมของระบบได้ แนวทางในการป้องกันควรทำในลักษณะการจัดการโดยผู้ดูแลระบบ หมายความว่าเมื่อไรก็ตามที่มีเหตุการณ์ มาละเมิดความมั่นคงในส่วนโครงสร้างของสถาปัตยกรรมของระบบแล้ว จะต้องมีข้อความขึ้นเตือนที่หน้าจอคอลโซล จนกว่าผู้ดูแลระบบจะจัดการกับการละเมิดความมั่นคงนั้นเสีย ถึงจะยอมให้ระบบทำงานต่อได้

3.2.8 โมดูลการออกแบบการวิเคราะห์ช่องทางลับ

ช่องทางลับหมายถึงช่องทางการสื่อสารของข้อมูลที่ไม่ธรรมดา ซึ่งสามารถหลีกเลี่ยงการตรวจจับของกลไกการป้องกันในระบบไปได้ ซึ่งช่องทางลับมีอยู่สองชนิดคือ ช่องทางที่เก็บ กับช่องทางเวลา ช่องทางที่เก็บทำงานรับส่งข้อมูลโดยการเปลี่ยนแปลงที่เก็บข้อมูลระบบบางอย่าง ส่วนช่องทางเวลา ทำงานรับส่งข้อมูลโดยมีผลกับสภาวะการทำงานของ ระบบหรือเกี่ยวข้องในการเปลี่ยนแปลงเวลาโดยการใช้ทรัพยากรของระบบในการวัดการทำงานบางอย่าง

<u>วัตถุประสงค์</u>

1. ต้องมีการพิสูจน์ช่องทางลับต่าง ๆ ในทีซีบี โดยการค้นหาทุก ๆ ตัวแปรที่อยู่ในทีซีบี เพราะอย่างน้อยต้องมีตัวแปรหนึ่งตัวที่ใช้เป็นตัวติดต่อ ซึ่งยอมให้มีการเปลี่ยนแปลงค่า หรือเป็นการสังเกตุค่าของตัวแปรที่มีผลต่อการไหลของข้อมูล โดยทั้งช่องทางที่เก็บและช่องทาง เวลานี้ใช้ตัวแปรอย่างน้อย 1 ตัวสำหรับการรับส่งข้อมูลระหว่างผู้รับและผู้ส่ง ซึ่งตัวแปรของช่องทางลับนี้สามารถเป็นได้ทั้งฮาร์ดแวร์ ซอฟต์แวร์หรือเฟิร์มแวร์

2. การประมาณค่าแบนวิธที่สูงสุดของแต่ละช่องทาง ค่าแบนวิธ หมายถึง อัตราการส่งของข้อมูลที่ผ่านช่องทาง

3. การทดสอบการจัดการช่องทางลับ มีเอกสารในการทดสอบการจัดการกับช่องทางลับ เช่น เงื่อนไขการทดสอบ สภาวะแวดล้อมที่ติดตั้งในการทดสอบ ข้อมูลทดสอบ และผลที่คาดว่าจะได้รับ เป็นต้น

ปัญหาที่พบ

การที่คอมพิวเตอร์ต่าง ๆ มีการเชื่อมโยงต่อเข้าถึงกันเป็นเครือข่ายนั้น นักเจาะระบบที่อยู่ ภายนอกสามารถใช้โปรแกรมประเภทตรวจจับข้อมูลที่วิ่งอยู่บนเครือข่าย มาดักจับชื่อผู้ใช้และ รหัสผ่านไปได้ หรือจากการเข้ามาฝังโปรแกรมประเภทม้าโทรจัน โดยอาศัยชื่อผู้ใช้ที่อยู่ในระบบ นั้นทำงาน เช่นโปรแกรมที่ว่านี้อาจตั้งชื่อว่า ftp ซึ่งถ้าใช้คำสั่งดูโปรเซสจะเห็นว่าเป็นการส่งไฟล์ แต่จริง ๆ แล้วโปรแกรมนี้ทำการเก็บข้อมูลและรหัสผ่านของผู้ใช้ต่าง ๆ ภายในเครือข่ายนั้นอยู่ ซึ่งโหมดของไฟล์นี้ มีการตั้ง SUID ไว้ โดยถ้าผู้ดูแลระบบไม่ทันสังเกตุก็จะเข้าใจว่า เป็นโปรแกรมส่งไฟล์ธรรมดา

แนวทางป้องกันแก้ไข

1. การค้นหาช่องทางลับทั้งหมดในระบบ อยู่ที่การหมั่นตรวจตราระบบเป็นประจำของผู้ดูแลระบบหรือผู้ตรวจสอบระบบ โดยทำการตรวจหาไฟล์ทุกไดเรกทอรีที่มีอยู่ในระบบที่มีการ ตั้งโหมดว่ามี SUID หรือ SGID คือเป็นไฟล์ที่ทำงานแล้วกลายเป็นการทำงานของผู้ใช้พิเศษขึ้นมา

2. การติดตั้งโปรแกรมประเภทกำแพงไฟ เพื่อตรวจสอบข้อมูลที่วิ่งผ่านเข้าออกเครือข่าย สังเกตที่อยู่หรือแอดเดรสปลายทางที่มีการติดต่อบ่อย ๆ หรือสังกตุโปรเซสที่มีการทำงานค้างไว้เป็นระยะเวลานาน