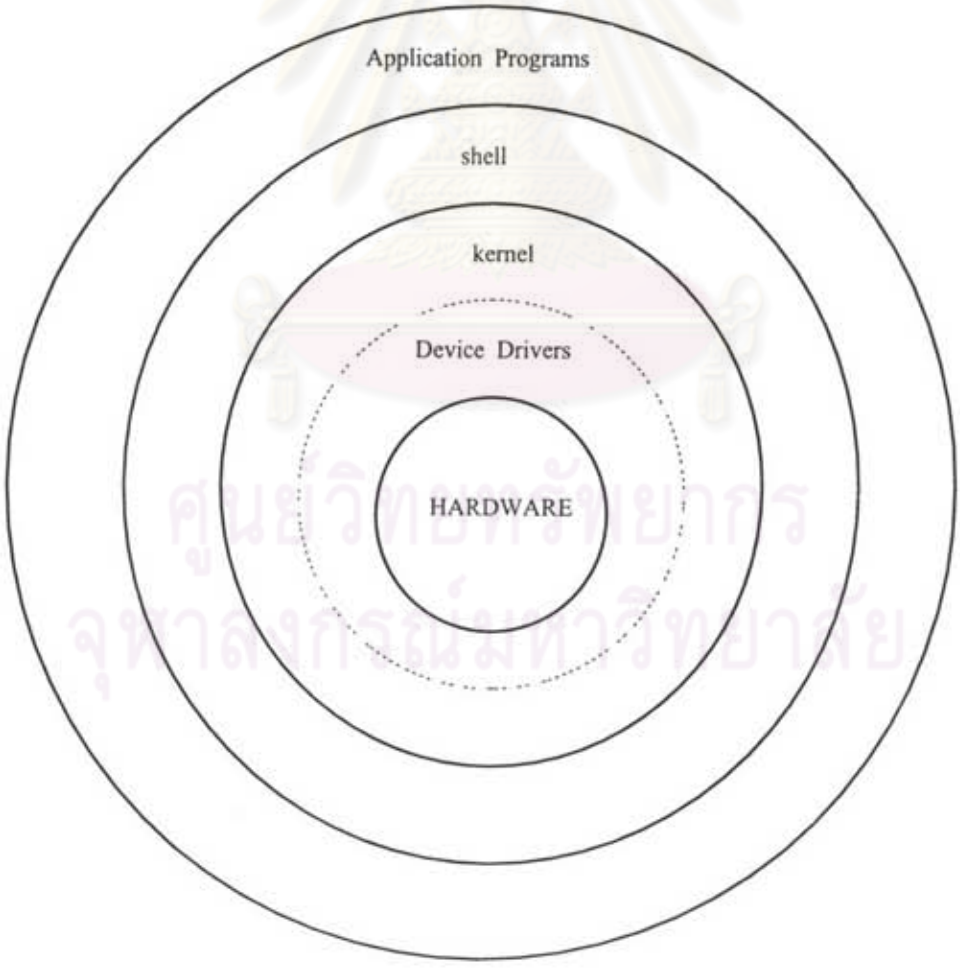
บทที่ 2

แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1 โครงสร้างพื้นฐานของระบบปฏิบัติการโอเอสเอฟวัน

ระบบปฏิบัติการโอเอสเอฟวัน มีรากฐานพัฒนามาจากยูนิกซ์ตระกูล BSD 4.3 มาปรับปรุงเพื่อสนับสนุนการทำงานของระบบคอมพิวเตอร์ที่มีได้หลายโปรเซสเซอร์ และมีบางอย่างที่รับมาจากยูนิกซ์ตระกูล System V R4



รูปที่ 2.1 แสดงชั้นของระบบปฏิบัติการ

2.1.1 โครงสร้างของระบบปฏิบัติการโอเอสเอฟวันประกอบด้วยส่วนต่าง ๆ ดังนี้

2.1.1.1 ส่วนของฮาร์ดแวร์

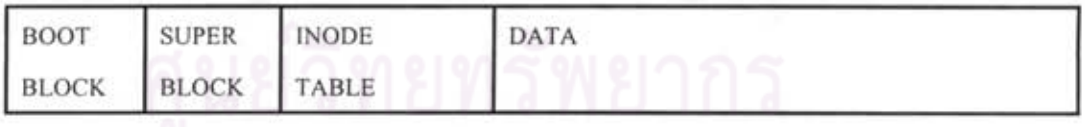
2.1.1.2 ตัวขับอุปกรณ์ (Device driver) เป็นชุดคำสั่งสำหรับติดต่อกับอุปกรณ์ภายนอก

2.1.1.3 แก่น (Kernel) เป็นส่วนที่สำคัญที่สุดของระบบปฏิบัติการ เป็นส่วนที่รับผิดชอบในการใช้ทรัพยากรของระบบ เช่น หน่วยความจำ หน่วยประมวลผลกลาง และอุปกรณ์สำหรับการประมวลผล ระบบปฏิบัติการโอเอสเอฟวันมีแก่นแบบมัค ซึ่งเป็นแก่นขนาดเล็ก และออกแบบมาสำหรับการทำงานในสภาวะแวดล้อมแบบขนานและกระจาย

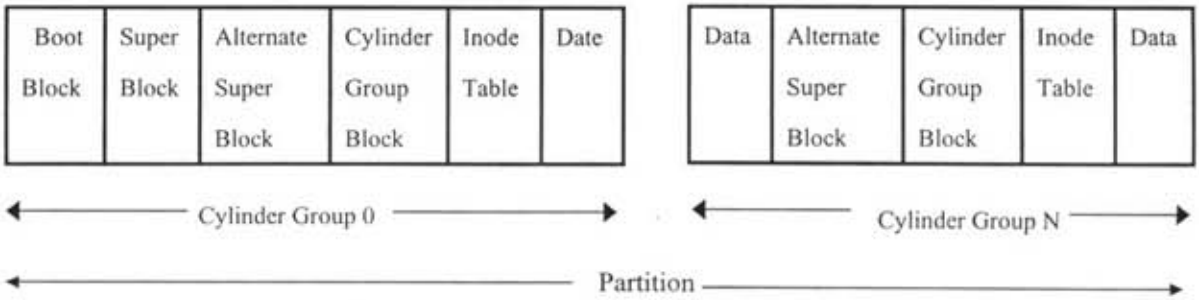
2.1.1.4 เชลล์ (shell) เป็นส่วนการให้บริการเรียกใช้ระบบ (system call)

2.1.1.5 โปรแกรมอรรถประโยชน์หรือโปรแกรมประยุกต์อื่น ๆ

2.1.2 โครงสร้างระบบไฟล์ (File system) ระบบปฏิบัติการโอเอสเอฟวัน สามารถใช้งานร่วมกับระบบไฟล์แบบ System V R2 ระบบไฟล์จาก BSD 4.3 และระบบไฟล์ NFS ได้ โดยที่ระบบไฟล์ของระบบปฏิบัติการโอเอสเอฟวันมีโครงสร้างเป็นระดับขั้น (Hierachy) ประกอบด้วยไดเรกทอรีและไฟล์ โดยเริ่มต้นที่รูทไดเรกทอรี และแต่ละไดเรกทอรี ประกอบด้วยทั้งไฟล์และไดเรกทอรีอยู่ภายใน แต่ละระบบไฟล์จะแยกกันอยู่ ไม่มีส่วนที่ซ้อนกันและอยู่ในขอบเขตของพาร์ติชัน ไม่มีการข้ามพาร์ติชันนอกจากจะมีการทำโวลุมแบบลอจิก (Logical Volumn) โดยที่ตัวจัดการโวลุมแบบลอจิก เป็นการจัดการให้ระบบไฟล์ สามารถแบ่งข้ามมาอีกโวลุม สามารถขยายขนาด รวมทั้งสามารถนำมาทำในลักษณะดิสต์กระจก (disk mirroring) ได้



รูปที่ 2.2 (ก) แสดงรูปแบบของระบบไฟล์แบบ System V



รูปที่ 2.2 (ข) แสดงรูปแบบของระบบไฟล์ยูนิกซ์

2.2 คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน

ความมั่นคงของระบบปฏิบัติการโอเอสเอฟวันนี้ ได้มีการออกแบบไว้ในระดับขั้น C2 ตามมาตรฐานของกระทรวงกลาโหม สหรัฐอเมริกา (Department of Defence 5200.28-STD) จากหนังสือสีส้ม (Orange Book) โดยมีคุณสมบัติดังนี้

2.2.1 คุณสมบัติด้านการตรวจสอบ

2.2.1.1 สามารถส่งรายการการตรวจสอบ (Audit log) ให้กับคอมพิวเตอร์แม่ข่ายระยะไกล (remote host)

2.2.1.2 มีประเภทของเหตุการณ์การตรวจสอบดังนี้

ก. การระบุที่ตั้งในการใช้ระบบ

ข. การเรียกใช้ระบบ

ค. เหตุการณ์ที่เกิดขึ้นเป็นประจำ

ง. การใช้งานประยุกต์

2.2.1.3 การเลือกก่อนอย่างละเอียดของเหตุการณ์ของระบบ โปรแกรมงานประยุกต์ และเหตุการณ์ในการกำหนดที่ตั้ง

2.2.1.4 การขยายหลังการตัดทอนของเหตุการณ์ของระบบ โปรแกรมงานประยุกต์ และเหตุการณ์ในการกำหนดที่ตั้ง

2.2.1.5 การระบุการเชื่อมโยงเวลาของระบบตรวจสอบย่อย

2.2.1.6 การตรวจสอบ .profile ของผู้ใช้แต่ละคน

โดยที่บนระบบปฏิบัติการโอเอสเอฟวัน มีเครื่องมือหรือคำสั่งที่ใช้ในการตรวจสอบดังนี้

`-audit_setup` ใช้ในการตั้งค่าสภาวะแวดล้อมในการตรวจสอบระบบ

`-auditmask` ใช้ในการเลือกเหตุการณ์ในรายการตรวจสอบ

`-audgen` ใช้ในการสร้างรายการตรวจสอบ ที่ระบุข้อความได้

`-auditd` เป็นการสั่งหรือกระตุ้นให้โปรแกรมการตรวจสอบระบบทำงาน

`-audit_tool` ใช้ในการเลือกหรือกรองข้อมูลที่เก็บอยู่ในรายการตรวจสอบ มาแสดงในรูปแบบที่ต้องการได้

2.2.2 คุณสมบัติด้านการแสดงตนและการพิสูจน์ตน (I&A) มีดังนี้คือ

2.2.2.1 การควบคุมที่รหัสผ่าน

ก. ตั้งความยาวของรหัสผ่าน สามารถให้ตั้งได้สูงสุด 80 ตัวอักษร

ข. ตั้งอายุของรหัสผ่าน

ค. การเปลี่ยนแปลงความยาวต่ำสุดของรหัสผ่าน อาจใช้ตามแนวทางจากหนังสือสีเขียว (Department of Defense Password Management Guideline) หรือขึ้นอยู่กับผู้ดูแลระบบในการตั้งอายุหรือความยาวต่ำสุดให้กับรหัสผ่าน

ง. มีการบันทึกผู้ที่เข้ามาทำการเปลี่ยนรหัสผ่าน ที่ไม่ใช่ผู้ใช้ที่เป็นเจ้าของ

จ. มีการเก็บประวัติการใช้รหัสผ่าน (0-9 รหัสผ่านที่ใช้ก่อนหน้านี้)

2.2.2.2 การควบคุมการเข้ามาใช้งาน

ก. บันทึกเครื่องและเวลาการเข้ามาใช้งานครั้งหลังสุด และการพยายามเข้ามาใช้งานแต่ไม่สำเร็จ

ข. ปิดกั้นบัญชีผู้ใช้อัตโนมัติ หลังจากการที่พยายามเข้ามาใช้งานติดต่อกัน ไม่ได้หลายครั้ง ตามจำนวนที่ระบุไว้ ในกรณีที่ฐานข้อมูลของระบบเกิดติดขัด รูท (root) สามารถเข้าสู่ระบบที่จอคอลโซล (console) ได้

ค. มีการตั้งเวลาของการพยายามเข้ามาใช้งานติดต่อกันไว้ที่เทอร์มินอลแต่ละตัว และตั้งเวลาสูงสุดของการพยายามในแต่ละครั้งก่อนที่จะแสดงออกมาว่าการพยายามนั้นล้มเหลว

ง. มีการตั้งจำนวนครั้งสูงสุดในการพยายามเข้ามาใช้ระบบติดต่อกันที่เทอร์มินอลแต่ละตัว ก่อนที่จะล็อคการเข้าถึงอีกครั้งจากเทอร์มินอลนั้น ๆ

2.2.2.3 ไม่ว่าจะเป็นบัญชีผู้ใช้ที่โดนปลด (retires) หรือถูกล็อค จะมีพื้นฐานเหมือนกันคือ จะพยายามยืนกรานในการเข้าถึงระบบ แต่ต่างกันที่การจัดการ คือมีการปลดโดยอัตโนมัติ สำหรับบัญชีผู้ใช้ที่หมดอายุ

2.2.2.4 ค่าโดยปริยายของระบบสำหรับคุณสมบัติการแสดงตนและการพิสูจน์ตน เช่นเวลาที่ใช้เตือนก่อนที่รหัสผ่านจะหมดอายุ ต้องไม่สามารถเปลี่ยนโดยโปรไฟล์ (profile) ของแต่ละผู้ใช้ได้

คำสั่ง passwd จะถูกนำมาใช้ในคุณสมบัติด้านการแสดงตนและการพิสูจน์ตนในการควบคุมการตั้งรหัสผ่าน และการควบคุมการใช้งาน

2.2.3 คุณสมบัติด้านความถูกต้องเชื่อถือได้

ในด้านความมั่นคงของระบบ มีการจัดเตรียมให้ระบบสามารถทำงานได้ถูกต้องทั้งทาง ด้านฮาร์ดแวร์ เฟิร์มแวร์และซอฟต์แวร์ของทีซีบี โดยที่ตัวเฟิร์มแวร์จะอยู่ในหน่วยความจำแบบ EEPROM และสามารถป้องกันการเขียนทางกายภาพ โดยสามารถนำมาเปรียบเทียบหรือนำเข้ามาใหม่ จากสื่อต้นฉบับภายนอกได้

เครื่องมือหรือคำสั่งที่ใช้ในการตรวจสอบความถูกต้องเชื่อถือได้ มีดังนี้คือ

- fverify ใช้ในการตรวจพิสูจน์ซอฟต์แวร์ที่ใช้ในระบบ
- authck ใช้ในการตรวจสอบโครงสร้างรวมของฐานข้อมูลที่เกี่ยวข้องในการป้องกันระบบ

โดยที่ ฐานข้อมูลที่เกี่ยวข้องในการป้องกันระบบ ได้แก่

1. ฐานข้อมูลที่เกี่ยวข้องในการป้องกันรหัสผ่านของผู้ใช้ในระบบ (Protected Password Database) อยู่ภายใต้ ไดเรกทอรี /tcb/files/auth ตามด้วยไดเรกทอรีที่ขึ้นต้นด้วยตัวอักษรตัวแรกของรหัสผู้ใช้ หรือตามรูปแบบ /tcb/files/auth/<a-z>/*username* เช่น รหัสผู้ใช้ที่เป็นรูท (root) จะมีไฟล์ที่ใช้ในการพิสูจน์ตน (authentication profile) อยู่ที่ไดเรกทอรี /tcb/files/auth/r และดูได้ที่ไฟล์ชื่อ root หรือรหัสผู้ใช้ที่ชื่อ took จะมีไฟล์ที่ใช้ในการพิสูจน์ตน อยู่ที่ /tcb/files/auth/t/took ซึ่งไฟล์ที่ใช้ในการพิสูจน์ตนนี้จะประกอบด้วยค่าต่าง ๆ ที่ทีซีบีจะนำไปใช้ โดยไฟล์นี้จะเป็นไฟล์เฉพาะของแต่ละรหัสผู้ใช้ ตัวอย่างเช่น ไฟล์ /tcb/files/auth/t/took เก็บข้อมูลดังต่อไปนี้คือ

```
took:u_name=took:u_id#206:\
     :u_pwd=PkpQiFIXTDzq6:\
     :u_pwdict=BrT4ukzHm9j.A, VStvwNmAzlZh6,  Nologin:\
     :u_suclog#839432554:u_suctty=ttyp0:u_lock@:\
     :chkent:
```

จากตัวอย่างค่าฟิลด์ต่าง ๆ ในที่นี้เช่น

u_name หมายถึงรหัสชื่อผู้ใช้ (username)

u_id มาจาก user ID

u_pwd หมายถึงรหัสผ่านของผู้ใช้ที่เข้ารหัสแล้ว (Encrypted password)

u_pwdict จะเก็บรายการประวัติของรหัสผ่านเก่า ๆ ที่เคยใช้ ซึ่งจะเก็บประวัติไว้ตามจำนวนเท่าไรนั้น ขึ้นอยู่กับค่า u_pwdepth ที่ตั้งไว้

u_suclog หมายถึง เวลาที่เข้าสู่ระบบสำเร็จครั้งหลังสุด

u_suctty หมายถึง เทอร์มินอลที่ใช้เข้าสู่ระบบสำเร็จครั้งหลังสุด

u_lock@ เป็นการระบุว่ารหัสผู้ใช้นี้สามารถเข้ามาใช้งานได้ ไม่ถูกล็อคโดยระบบ

chkent เป็นการระบุว่าค่าที่ตั้งไว้ต่าง ๆ หมดแล้ว

ซึ่งค่าที่ตั้งต่าง ๆ นี้ยังมีค่าอื่น ๆ อีกขึ้นอยู่กับการกำหนดให้เฉพาะแต่ละผู้ใช้ อ้างอิงดูได้ที่ prpasswd แต่โดยทั่วไปจะประกอบด้วยฟิลด์ รหัสชื่อผู้ใช้, UID, รหัสผ่านที่เข้ารหัสแล้ว , จำนวนครั้งของการเข้าสู่ระบบสำเร็จหรือไม่สำเร็จ และเทอร์มินอลที่ใช้ เป็นต้น

2. ฐานข้อมูลค่าโดยปริยายของระบบ (System Defaults Database) ไฟล์นี้จะเก็บค่าโดยปริยายต่าง ๆ ในระบบเพื่อใช้ในกรณีที่ผู้ดูแลระบบไม่ได้ตั้งค่าไว้ในฐานข้อมูลที่เกี่ยวข้องในการป้องกันรหัสผ่านของผู้ใช้ในระบบ, ฐานข้อมูลควบคุมเทอร์มินอล และฐานข้อมูลกำหนดค่าอุปกรณ์ โดยฐานข้อมูลนี้จะเก็บอยู่ที่ `/etc/auth/system/default`

3. ฐานข้อมูลควบคุมเทอร์มินอล (Terminal Control Database) ผู้ดูแลระบบสามารถควบคุมการล็อกอินเข้าสู่ระบบของแต่ละเทอร์มินอลที่ต่อเข้าสู่ระบบ ซึ่งข้อมูลที่ใช้ควบคุมเทอร์มินอลนี้ประกอบไปด้วย ชื่ออุปกรณ์เทอร์มินอล, เลขประจำตัวผู้ใช้ (UID) และ เวลาที่พยายามเข้าสู่ระบบโดยเทอร์มินอลนั้นๆ พร้อมทั้งบอกได้ว่าเข้าสู่ระบบได้สำเร็จหรือไม่ เป็นต้น โดยข้อมูลนี้จะเก็บอยู่ที่ `/etc/auth/system/ttys`

4. ฐานข้อมูลในการควบคุมไฟล์ (File Control Database) ประกอบด้วยข้อมูลที่ใช้ปกป้องคุณสมบัติของไฟล์ของระบบ (attributes of system file) ช่วยในการป้องกันความมั่นคงให้กับทีซีบี โดยจะประกอบด้วยข้อมูลต่าง ๆ ดังนี้คือ เส้นทางแบบเต็มรูปแบบของไฟล์ เจ้าของและกลุ่มของไฟล์ โหมดและประเภทของไฟล์ ฐานข้อมูลในการควบคุมไฟล์นี้เก็บอยู่ที่ `/etc/auth/system/files`

5. ฐานข้อมูลกำหนดค่าอุปกรณ์ (Device Assignment Database) เก็บข้อมูลเกี่ยวกับอุปกรณ์ที่ใช้แลกเปลี่ยนข้อมูลกับผู้ใช้ ระบบจะใช้ฐานข้อมูลนี้ช่วยในการจำกัดขอบเขตความปลอดภัยของข้อมูลในการรับ-ส่งผ่านอุปกรณ์ของระบบ โดยฐานข้อมูลนี้ประกอบด้วยข้อมูลที่เกี่ยวกับอุปกรณ์ เช่น เส้นทางชื่ออุปกรณ์ ประเภทของอุปกรณ์ รวมถึงชื่อเส้นทางที่อ้างอิงอยู่กับอุปกรณ์จริงทางกายภาพ ฐานข้อมูลกำหนดค่าอุปกรณ์นี้จะเก็บอยู่ที่ `/etc/auth/system/devassign`

2.3 แนวคิดด้านความมั่นคง

2.3.1 นิยามของระบบที่ไว้ใจได้

หนังสือสีส้มได้เขียนเกี่ยวกับระบบที่ไว้ใจได้ (trusted) มากกว่าระบบที่มั่นคง (secure) ซึ่งคำทั้งสองนี้จะไม่เหมือนกันทีเดียวนัก เนื่องจากว่าจะไม่มีระบบใดเลยที่มีความมั่นคงอย่างสมบูรณ์ ทุกระบบสามารถที่จะถูกเจาะได้ถ้ามีเครื่องมือและให้เวลาที่เพียงพอ แต่สามารถที่จะไว้ใจในระบบได้ คือจะเป็นไปได้ในสิ่งที่เราต้องการหรือคาดหวังให้เกิด

ในวิทยานิพนธ์นี้ จึงขอใช้คำว่า ความมั่นคง (security) การป้องกัน (prevention) การคุ้มครอง (protection) การไว้ใจได้ (trusted) ในความหมายนัยเดียวกันว่า ระบบที่มีการป้องกันหรือได้รับการคุ้มครอง ถือว่าเป็นการสร้างความมั่นคงให้กับระบบ ระบบนั้นก็ย่อมเป็นที่ไว้ใจได้

ในหนังสือสีส้มได้นิยาม **"ระบบที่ไว้ใจได้คืออะไร"** ไว้ว่า เป็นระบบที่มีการวัดความเชื่อถือได้ในการใช้ฮาร์ดแวร์และซอฟต์แวร์อย่างเพียงพอ เพื่อสำหรับทำการประมวลผลข้อมูลที่มีความไหว (sensitive) ได้ในเวลาเดียวกันสำหรับผู้ใช้ที่มีความหลากหลาย โดยปราศจากการรบกวนสิทธ์ของกันและกันในหนังสือสีส้ม ได้ให้มุมมองของการไว้ใจจาก

2.3.1.1 นโยบายด้านความมั่นคง (Security Policy)

ในนโยบายด้านความมั่นคง ได้เน้นถึง กฎที่บังคับด้วยคุณลักษณะของระบบความมั่นคง ตัวอย่างเช่น กฎในการให้ผู้ใช้แต่ละคนมีสิทธิในการใช้ข้อมูลในแต่ละชิ้นได้ต่างกัน สังเกตได้จาก ระบบที่มีความมั่นคงในระดับสูง (คือระบบที่เริ่มตั้งแต่ขั้น B1 ขึ้นไป) มีคุณสมบัติด้านความมั่นคงสูงกว่าในระบบที่มีความมั่นคงในระดับต่ำ (เช่น ระบบขั้น C1 หรือ C2) แต่ในระบบที่มีความมั่นคงระดับสูงด้วยกัน จะมีคุณสมบัติด้านความมั่นคงแตกต่างกันเพียงเล็กน้อย โดยเน้นในเรื่องของการประกัน (assurance)

2.3.1.2 การประกัน (Assurance)

การประกันเป็นการสร้างความไว้ใจที่ใส่ในระบบที่สามารถนำไปพิสูจน์ทดสอบ อ้างอิงและสามารถส่งให้กับลูกค้าได้ ในระบบที่มีความมั่นคงระดับสูงมีคุณสมบัติด้านความมั่นคงแตกต่างกันเพียงเล็กน้อย แต่จะมุ่งในเรื่องระดับของการประกัน ซึ่งผู้ใช้สามารถนำมาใส่ให้กับโครงสร้างของระบบหรือนำมาเสริมในโยบายด้านความมั่นคง

2.3.2 พื้นฐานความไว้ใจในคอมพิวเตอร์ (Trusted Computing Base - ทีซีบี)

แนวคิดในเรื่องทีซีบี ถูกรวมไว้เข้ากับแนวคิดของระบบที่ไว้ใจได้ ในหนังสือสีส้มได้อ้างว่าทีซีบีเป็นกลไกในการบังคับความมั่นคงในระบบ โดยนิยามทีซีบีไว้ดังนี้ คือ เป็นการรวมกลไกในการปกป้องระบบคอมพิวเตอร์ ซึ่งจะประกอบด้วยฮาร์ดแวร์ เฟิร์มแวร์ และซอฟต์แวร์ ซึ่งการประสานกันในการทำงานนี้เป็นไปในบังคับตามนโยบายด้านความมั่นคง โดยมีการสร้างสภาวะการปกป้องพื้นฐานและเตรียมรับระบบคอมพิวเตอร์ที่ไว้ใจได้ที่เพิ่มเข้ามาตามความต้องการของผู้ใช้ ไม่เพียงแต่ทุกส่วนของระบบปฏิบัติการ ที่ต้องการความไว้ใจ ยังมีส่วนอื่น ๆ ที่สำคัญในการประเมินระบบคอมพิวเตอร์ เช่น สถาปัตยกรรม กลไกของการรับประกันและคุณสมบัติด้านความมั่นคงที่รวมถึงทีซีบี ซึ่งทีซีบีต้องสามารถแสดงให้เห็นว่าสามารถป้องกันการเข้ามารบกวนไม่ว่าจะเป็นโดยอุบัติเหตุหรือตั้งใจ

2.3.3 นโยบายด้านความมั่นคง (Security Policy)

นโยบายด้านความมั่นคง เป็นกฎหรือข้อปฏิบัติที่องค์กรใช้ในการจัดการป้องกันกระจายข้อมูลที่มีความไหวโดยสม่ำเสมอ ซึ่งเป็นเค้าโครงหรือโครงร่างที่ระบบได้จัดเตรียมความไว้ใจได้ไว้ นโยบายด้านความมั่นคง มักจะเน้นในเทอมของตัวกระทำ (subject) และตัวถูกกระทำ (object) โดยที่ตัวกระทำหมายถึงบางสิ่งบางอย่างที่เป็นผู้กระทำอยู่ในระบบ เช่นผู้ใช้งาน โปรเซส หรือโปรแกรม ส่วนตัวถูกกระทำหมายถึงบางสิ่งบางอย่างที่ถูกกระทำโดยตัวผู้กระทำ เช่น ไฟล์ ไดเรคทอรี อุปกรณ์ ซ็อคเก็ต (socket) หรือหน้าต่าง (windows) เป็นต้น

2.3.4 แบบจำลองของความมั่นคง (Security Model)

กลไกที่จำเป็นในการบังคับใช้นโยบายด้านความมั่นคง มักระบุอยู่ในรูปของแบบจำลองของความมั่นคง โดยที่แบบจำลองนี้ต้องแสดงความมั่นคงของระบบได้อย่างละเอียดและไม่สับสน ซึ่งแบบจำลองของความมั่นคงนี้ได้ถูกพัฒนาขึ้นมาหลากหลายรูปแบบ โดยแบบจำลองของระบบที่ต้องการความมั่นคงสูงมักแสดงในรูปทางคณิตศาสตร์และมักใช้ทฤษฎีในการอธิบายกฎในการเข้าถึงระบบ

2.3.5 แก่นของความมั่นคง (Security Kernel)

แก่นของความมั่นคง หมายถึงกลไกของระบบปฏิบัติการที่พัฒนาโดยอาศัยแนวคิดในเรื่องของการจับตามองการทำงาน (reference monitor) ซึ่งแก่นของความมั่นคงนี้เป็นหัวใจของทีซีบี โดยหนังสือสีส้มได้ให้นิยามแก่นของความมั่นคง ไว้ดังนี้

ส่วนประกอบทางฮาร์ดแวร์ เฟิร์มแวร์และซอฟต์แวร์ของทีซีบี ได้มีการพัฒนาจากแนวคิดในเรื่องของการจับตามองการทำงาน ซึ่งสามารถเข้าถึงได้อย่างทันทีทันการ ป้องกันการมาเปลี่ยนแปลงแก้ไข และสามารถตรวจสอบความถูกต้องได้ โดยมากมักใส่ไว้ในระบบที่ต้องการความไว้ใจได้สูง

2.3.6 ขอบเขตของความมั่นคง (Security Perimeter)

เป็นสิ่งสำคัญมากในการเชื่อมต่อข้ามเขตของความมั่นคง (คือมีหลายวิธีที่ผู้ใช้หลายคนสามารถเลือกใช้แนวทางด้านความมั่นคงได้หลายทาง) จึงต้องมีการกำหนดอย่างละเอียดและบังคับให้เป็นไปตามเกณฑ์ของระบบ

2.4 ระดับขั้นของความมั่นคง

เนื่องจากความแตกต่างขององค์กร ความแตกต่างของข้อมูลสารสนเทศ ความต้องการในเรื่องความมั่นคงของข้อมูลก็ย่อมที่จะแตกต่างกัน หนังสือสีส้มจึงเกิดมาจากสามัญสำนึกของความต้องการความมั่นคงที่เพิ่มมากขึ้น จากทั้งภาครัฐบาลและภาคอุตสาหกรรม ซึ่งต้องการหามาตรฐานในการเลือกซื้อหรือใช้คอมพิวเตอร์ที่สามารถทำการต่อเชื่อมเข้าด้วยกัน

ในหนังสือสีส้มได้มีการกำหนดชั้นส่วนของการป้องกันความมั่นคง โดยในแต่ละส่วนประกอบด้วย 1 หรือมากกว่า 1 ขั้น (CLASS) ซึ่งตัวเลขที่มีค่ามาก หมายถึง ความมั่นคงที่สูงกว่า ตัวอย่างเช่น ในส่วน C จะประกอบด้วย 2 ขั้น (C2 จะมีความ มั่นคง มากกว่า C1) และในส่วน B จะประกอบด้วย 3 ขั้น (โดยที่ B3 จะมีความมั่นคงมากกว่า B2 และมากกว่า B1) ในส่วน A ในปัจจุบันนี้มีอยู่เพียง 1 ขั้น โดยลำดับของความไว้ใจได้จากน้อย ไปหามากดังนี้

2.4.1 ระดับขั้น D: ความมั่นคงในระดับขั้นต่ำสุด (Minimal security)

เป็นระบบที่ไม่มีความมั่นคงเลย เช่น คอมพิวเตอร์ส่วนบุคคลที่ใช้ระบบปฏิบัติการดอส (DOS) เครื่องคอมพิวเตอร์แมคอินทอช

2.4.2 ระดับขั้น C หมายถึงการป้องกันที่ผ่านการไตร่ตรองอย่างรอบคอบ (Discretionary protection)

2.4.2.1 ระดับขั้น C1: การป้องกันโดยใช้ดุลยพินิจ (Discretionay security protection) ผู้ใช้สามารถป้องกันไฟล์ หรือทรัพยากรของตน ที่จะเข้าถึงโดยผู้อื่น

2.4.2.2 ระดับขั้น C2: การป้องกันโดยการควบคุมการเข้าถึง (Controlled access protection) ครอบคลุมในระดับขั้น C1 ผู้ใช้ต้องมีการใส่รหัสผ่าน และถูกตรวจสอบ ซึ่งระบบปฏิบัติการยูนิกซ์โดยทั่วไปจะมีความมั่นคงในระดับขั้นนี้

2.4.3 ระดับขั้น B หมายถึงการป้องกันที่อยู่ภายใต้อาณัติ (Mandatory protection)

2.4.3.1 ระดับขั้น B1: การป้องกันความมั่นคงโดยการใช้ป้ายชื่อ (Labeled security protection) ครอบคลุมในระดับขั้น C2 แต่มีป้ายชื่อของข้อมูลเข้ามาเกี่ยวข้อง ถ้าข้อมูลที่มีความไหวถูกสั่งพิมพ์ออกมา ต้องมีกลไกการเตือน มีการควบคุมการเข้าถึงภายใต้นโยบายเข้มงวด (เอ็มเอซี) ผู้จัดการความมั่นคงให้กับระบบต้องสามารถระบุได้ว่าตัวถูกกระทำตัวใด จะมีสิทธิใช้โดยใครบ้าง

2.4.3.2 ระดับขั้น B2: การป้องกันโครงสร้าง (Structured protection) ครอบคลุมระดับขั้น B1 และมีการทดสอบ ซึ่งตัวถูกกระทำทุกตัวต้องมีการควบคุมการเข้าถึงอย่างเคร่งครัด ทุกรูโหว่หรือช่องทางที่จะเข้าสู่ระบบ จะถูกหาพบแล้วกำจัดทิ้ง มีการตรวจสอบ ซึ่งเหตุการณ์ที่ทำให้เกิดคำถามหรือชวนสงสัย จะต้องถูกรายงานให้กับผู้จัดการระบบ ตัวอย่างเช่น คำสั่งยูนิกซ์ "สลับเปลี่ยนผู้ใช้" ('su' Switch User) ต้องมีคำเตือนมาที่หน้าจอควบคุมของระบบ เพื่อที่ดูว่ามาจากใคร เป็นผู้ดูแลระบบหรือไม่ สิ่งที่เป็นปัญหาในการที่จะนำระบบมาสู่ขั้น B2 นั้น จะเป็นเรื่องของการจัดแบ่งเป็นส่วนเป็นตอน (Modularity) ซึ่งการจัดแบ่งเป็นส่วนเป็นตอนนี้เป็นการที่แก่น (Kernel) ของมันเองต้องเล็กและปรับเปลี่ยนโครงสร้างใหม่ได้ แต่ปัญหานี้แทบไม่ใช่ปัญหาของยูนิกซ์รุ่นใหม่ ๆ ที่ใช้แก่นแบบมัค ซึ่งจะเป็นแก่นแบบเพรียวลม (stream lined kernel) อยู่แล้ว

2.4.3.3 ระดับขั้น B3: ขอบเขตความมั่นคง (Security domains) ครอบคลุมระดับขั้น B2 เป็นสุดยอดของความมั่นคง ปัจจุบันยังไม่มียูนิกซ์รุ่นไหนเลยที่มีความมั่นคงถึงขั้นนี้ ส่วนหนึ่งเนื่องจากว่า จะขึ้นอยู่กับส่วนประกอบทางฮาร์ดแวร์แล้วมีการพิสูจน์ด้วย ต้องมีผู้ดูแลด้านความมั่นคง เขตขั้นความมั่นคงในระดับสูง จะมีความสัมพันธ์กันน้อย ซึ่งต้องสามารถตรวจสอบพิสูจน์ได้ และมีรายละเอียดของการฟื้นฟูสภาพอยู่ด้วย ในขณะที่ขั้น B2 มีการตรวจสอบระบบ ขั้น B3 จะตรวจสอบข้อชวนสงสัยของเหตุการณ์ที่ละเมิดในสิทธิของผู้จัดการระบบ และถ้าจำเป็นจริง ๆ ก็จะทำการปิดระบบหรือปิดเครื่องเพื่อป้องกันการคุกคามความมั่นคง

2.4.4 ระดับขั้นA การป้องกันที่สามารถจะพิสูจน์ได้ (Verified protection)

ระดับขั้น A1: การออกแบบที่พิสูจน์ได้ (Verified design) เป็นระดับสูงสุด นโยบายทางความมั่นคง จะถูกทดสอบและตรวจสอบ

ซึ่งแต่ละขั้นถูกกำหนดด้วยเกณฑ์หรือบรรทัดฐานโดยเฉพาะ โดยที่เกณฑ์ หรือบรรทัดฐานนี้ แบ่งได้เป็น 4 กลุ่มหลัก คือ นโยบายด้านความมั่นคง (Security Policy) การชี้แจงรายการ (Accountability) การประกัน (Assurance) และการจัดการเอกสาร (Documentation) ซึ่งการวัดเกณฑ์นี้มาจากจุดประสงค์พื้นฐาน 3 ข้อคือ

- การวัด (Measurement)

เพื่อจัดมาตราการวัดระดับความไว้ใจในระบบคอมพิวเตอร์ สำหรับความมั่นคงของการประมวลผลที่แตกต่างกันหรือสำหรับข้อมูลสารสนเทศที่มีความสำคัญมาก ๆ ตัวอย่างเช่น ผู้ใช้สามารถที่วางใจในระบบที่มีความมั่นคงในระดับขั้นB2 มากกว่าระบบที่มีความมั่นคงระดับขั้น C2

- คำแนะนำ (Guidance)

โดยมีคำแนะนำให้กับผู้ทำงานเพื่อเสมือนเป็นการสร้างความเชื่อมั่นของงานที่ทำที่มีความละเอียดอ่อน

- การได้มาหรือเข้าถือสิทธิ (Acquisition)

เป็นการเตรียมขั้นพื้นฐานสำหรับระบุในเรื่องความมั่นคงในผู้ที่มีการระบุว่ามีสิทธิแทนที่จะกำหนดให้โดยรวม ๆ แล้วคอยมาจัดสรรเป็นส่วน ๆ

Criteria	C1	C2	B1	B2	B3	A1
Security Policy						
Discretionary Access Control	⊗	⊗	⇒	⇒	⊗	⇒
Object Reuse	■	⊗	⇒	⇒	⇒	⇒
Labels	■	■	⊗	⊗	⇒	⇒
Label Integrity	■	■	⊗	⇒	⇒	⇒
Exportation of Labeled Information	■	■	⊗	⇒	⇒	⇒
Exportation of Multilevel Devices	■	■	⊗	⇒	⇒	⇒
Exportation of Single-Level Devices	■	■	⊗	⇒	⇒	⇒
Labeling Human-Readable Output	■	■	⊗	⇒	⇒	⇒
Subject Sensitivity Labels	■	■	■	⊗	⇒	⇒
Device Labels	■	■	■	⊗	⇒	⇒
Mandatory Access Control	■	■	⊗	⊗	⇒	⇒
Accountability						
Identification and Authentication	⊗	⊗	⊗	⇒	⇒	⇒
Audit	■	⊗	⊗	⊗	⊗	⇒
Trusted Path	■	■	■	⊗	⊗	⇒
Assurance						
System Architecture	⊗	⊗	⊗	⊗	⊗	⇒
System Integrity	⊗	⇒	⇒	⇒	⇒	⇒
Covert Channel Analysis	■	■	■	⊗	⊗	⊗
Trusted Facility Management	■	■	■	⊗	⊗	⇒
Trusted Recovery	■	■	■	■	⊗	⇒
Security Testing	⊗	⊗	⊗	⊗	⊗	⊗
Design Specification and Verification	■	■	⊗	⊗	⊗	⊗
Configuration Management	■	■	■	⊗	⇒	⊗
Trusted Distribution	■	■	■	■	■	⊗
Documentation						
Security Features User's Guide	⊗	⇒	⇒	⇒	⇒	⇒
Trusted Facility Manual	⊗	⊗	⊗	⊗	⊗	⇒
Test Documentation	⊗	⇒	⇒	⊗	⇒	⊗
Design Documentation	⊗	⇒	⊗	⊗	⊗	⊗

■ No requirements for this class

⊗ New or enhanced requirements for this class

⇒ Same requirements as previous class

รูปที่ 2.3 แสดงเกณฑ์ของระบบคอมพิวเตอร์ที่ไว้ใจได้

2.5 การประเมินค่าของระบบที่มั่นคง

2.5.1 ความต้องการของนโยบายด้านความมั่นคง (Security Policy Requirements)

- การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ (Discretionary Access Control - ดีเอซี)
- การนำตัวถูกกระทำมาใช้ใหม่ (Object reuse)
- ป้ายชื่อ (Labels)
- การควบคุมการเข้าถึงภายใต้อาณัติ (Mandatory access control)

2.5.1.1 การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ

เป็นวิธีที่เข้มงวดวิธีหนึ่งในการเข้าถึงไฟล์หรือตัวถูกกระทำของระบบอื่น โดยขึ้นอยู่กับการตรวจดูว่าเป็นตัวผู้ใช้หรืออยู่ในกลุ่มที่เป็นเจ้าของไฟล์ ซึ่งดีเอซีนี้เป็นกลไกที่ใช้ ควบคุมการเข้าถึงในระบบที่ไว้ใจได้โดยทั่วไป ผู้ใช้หรือเจ้าของไฟล์ต้องป้องกันไฟล์ของตนโดยสามารถระบุให้ใครสามารถใช้ได้บ้างและให้ใช้ได้ในระดับใด เช่น ให้อ่านได้อย่างเดียวหรือ อ่านได้แล้วแก้ไขได้ เป็นต้น

2.5.1.2 การนำตัวถูกกระทำมาใช้ใหม่

ต้องสามารถทำการป้องกันไฟล์ หน่วยความจำ และตัวถูกกระทำอื่นๆในระบบที่อาจเกิดจากการเข้าถึงระบบของผู้ใช้ที่ไม่มีสิทธิ ได้โดยบังเอิญ โดยลักษณะนี้จึงต้องมีการเก็บแอดเดรส (address) ที่เกิดขึ้นเมื่อมีการกำหนดค่าใหม่ให้กับตัวถูกกระทำ การนำตัวถูกกระทำมาใช้ใหม่นี้มีในระบบที่มีความมั่นคงตั้งแต่ระดับขั้น C2 เป็นต้นไป พิจารณาตัวอย่างที่จะกล่าวต่อไปนี้ ถ้าไม่มีคุณสมบัติในข้อนี้ ในระบบที่ไว้ใจได้จะเป็นอย่างไร สมมติว่าเมื่อมีการสร้างไฟล์ใหม่ ระบบจะทำการจองเนื้อที่สำหรับไฟล์ เพื่อสามารถเก็บข้อมูลในไฟล์ ป้องกันได้อย่างแน่นหนา เมื่อใช้งานเสร็จแล้ว ลบทิ้ง แต่จริง ๆ แล้วระบบไม่ได้ลบข้อมูลออกจากเนื้อที่ในจานบันทึกจริง เพียงแต่ทำการเขียนที่หัวไฟล์ระบุว่าเป็นไฟล์ที่ลบแล้ว ซึ่งมีหลายวิธีที่สามารถทำการผ่านเข้ามาในระบบแบบไม่ธรรมดา แล้วสามารถอ่านข้อมูลนั้นไปจากจานบันทึกได้

หรืออีกตัวอย่าง สมมติให้นาย JACK J. HACKE มีรหัสชื่อผู้ใช้ในการล็อกอิน คือ JJH ได้ออกจากงานไป และในปีต่อมา นางสาว JUNE J. HACKE มาทำงานแทน ผู้ดูแลระบบ (administrator) ได้กำหนดรหัสชื่อผู้ใช้ในการล็อกอิน ให้นางสาว JUNE เป็น JJH (ซึ่งใช้ของเก่าของนาย JACK) อันตรายก็คือว่ารหัสชื่อผู้ใช้ของนาย JACK อาจจะยังมีค้างอยู่ที่ไหนสักแห่ง ใน

ระบบ เช่นอยู่ในเอซีแอล (Access Control Lists) ที่แสดงว่ามีผู้ใช้ใดเข้ามาใช้ไฟล์ ซึ่งเมื่อนำ รหัสเดิมมากำหนดใหม่ ให้ นางสาว JUNE ทำให้เธอกลายเป็นผู้ใช้ข้อมูล ซึ่งแท้จริงแล้วเป็นนาย JACK

คุณสมบัติของการนำตัวถูกกระทำมาใช้ใหม่นี้ได้มีมาตรการความมั่นคง โดยสร้างความมั่นใจให้ว่า เมื่อไรที่ตัวถูกกระทำ เช่น รหัสชื่อล็อกอิน ถูกกำหนดให้ใช้ใหม่ กำหนดที่หรือย้ายที่ ตัวถูกกระทำนี้จะไม่เก็บข้อมูลที่มีการใช้ในก่อนหน้านี้ เช่นในตัวอย่างแรก ข้อมูลเมื่อสั่งลบจะต้องถูกเขียนทับ ซึ่งทำให้ไม่มีใครสามารถดึงข้อมูลจากจานบันทึกได้ และในตัวอย่างที่สอง คุณสมบัติของการนำตัวถูกกระทำมาใช้ใหม่ ต้องทำการปรับปรุงไฟล์ที่เก็บรหัสของผู้ใช้เมื่อมีการลบออกจากระบบ เมื่อมีการเพิ่มผู้ใช้ใหม่เข้ามาในระบบ ระบบต้องทำการตรวจดูไฟล์นี้เพื่อความแน่ใจว่ารหัสนี้จะไม่ซ้ำกับการที่กำหนดไปแล้วก่อนหน้านี้

คุณสมบัติของการนำตัวถูกกระทำมาใช้ใหม่ ที่มีอยู่ในระบบที่ไว้ใจได้จะประกอบไปด้วย

- การลบบล็อค (block) หรือเพจ (page) ออกจากหน่วยความจำ ก่อนที่จะถูกใช้โดยโปรแกรม
- ทำการลบบล็อคจากจานบันทึก เมื่อมีการลบไฟล์หรือก่อนที่บล็อคนั้นจะถูกนำไปใช้ โดยไฟล์
- ทำให้พ้นจากอำนาจแม่เหล็ก เมื่อไม่จำเป็นต้องใช้เทปหรือจานแม่เหล็กนั้นอีก
- ทำการลบตัวถูกกระทำที่เป็นเอ็กซ์วินโดว์ ก่อนที่จะไปกำหนดให้ผู้ใช้อื่น
- ลบบัฟเฟอร์ของรหัสผ่าน (password buffer) หลังจากทำการเข้ารหัส
- ลบเพจ เอกสารหรือหน้าจอที่ค้างอยู่ ในหน่วยความจำของ เทอร์มินอล หรือเครื่องพิมพ์ที่ใช้งาน

2.5.1.3 ป้ายชื่อ

เริ่มที่ระดับขั้น B1 ในหนังสือสีส้มได้ระบุว่า ทุก ๆ ตัวกระทำ (เช่น ผู้ใช้, โปรเซส) และ ตัวถูกกระทำที่เก็บข้อมูล (เช่น ไฟล์ ไดเรกทอรี หน้าต่าง ซ็อคเก็ต) เกี่ยวข้องกับป้ายความไหว (sensitivity label) สำหรับระบบที่มีความมั่นคงตั้งแต่ขั้น B2 ขึ้นไป ทรัพยากรของระบบทั้งหมด เช่น อุปกรณ์ รอม (ROM) ต้องมีป้ายความไหว ป้ายความไหวหมายถึงป้ายชื่อที่แสดงถึง ระดับความมั่นคงของตัวถูกกระทำหนึ่ง ๆ โดยบ่งบอกถึง ความลับ หรือความสำคัญ ของข้อมูลในตัวถูกกระทำนั้น ๆ ส่วนป้ายความไหวของผู้ใช้ (user's sensitivity label) จะระบุถึงระดับของความไว้ใจได้ ซึ่งขึ้นอยู่กับผู้ใช้ โดยมักเรียกกันว่า "ข้อกระจ่าง (clearance)" ป้ายความไหวของไฟล์ระบุระดับของความไว้ใจได้ของผู้ใช้ที่มีความสามารถในการเข้าถึงไฟล์

2.5.1.4 การควบคุมการเข้าถึงภายใต้อาณัติ

เป็นนโยบายด้านความมั่นคงขั้นสุดท้าย ซึ่งควบคุมการเข้าถึงตัวถูกกระทำของระบบอย่างเข้มงวด โดยขึ้นอยู่กับความไหวของข้อมูลในตัวถูกกระทำนั้น ซึ่งแสดงโดยป้ายของตัวถูกกระทำ และการตรวจสอบตัวกระทำ มักแสดงโดยข้อกระจ่างของผู้ใช้ ภายใต้อาณัติ หมายถึงระบบที่ถูกบังคับโดยนโยบาย ซึ่งผู้ใช้ไม่สามารถที่จะใช้ดุลยพินิจที่จะทำการแบ่งหรือร่วมกันใช้ไฟล์ของตน ซึ่งจะต่างจากดีเอซี

2.5.2 ความต้องการในการชี้แจงรายการ (Accountability Requirement)

การชี้แจงรายการเป็นแนวหนึ่งที่นำมาใช้ในเรื่องของความมั่นคงของระบบ เป็นแนวคิดที่ระบบใช้ตรวจดูว่า ผู้ใช้คือใครและกำลังทำอะไร ซึ่งระบบต้องสามารถพิสูจน์ แยกแยะผู้ใช้ได้ทั้งหมด ต้องสามารถพิสูจน์ได้ด้วยว่าผู้ใช้นั้นๆ มีสิทธิถูกต้องในการเข้าถึงข้อมูล และต้องเก็บการกระทำต่าง ๆ ที่เกี่ยวกับความมั่นคงของระบบโดยการชี้แจงรายการจะต้องมีคุณลักษณะในเรื่องดังนี้

- การพิสูจน์ตนและการแสดงตน (Identification and Authentication)
- เส้นทางการไว้ใจได้ (Trusted path)
- การตรวจสอบ (Audit)

2.5.2.1 การพิสูจน์ตนและการแสดงตน

การพิสูจน์ตนและการแสดงตนนี้ เป็นสิ่งที่จะต้องมีในทุกระดับของความมั่นคงของระบบ ในหนังสือสีส้มได้ระบุว่า ผู้ใช้ต้องมีการแสดงตนก่อนที่จะกระทำการใด ๆ ที่เกี่ยวพันกับทีซีบี เช่น สั่งโปรแกรมทำงาน อ่านไฟล์หรือเกี่ยวข้องกับฟังก์ชันใด ๆ ที่ระบบจำเป็นต้องดูว่าผู้ใช้นั้นมีสิทธิหรือไม่ ซึ่งส่วนมากระบบที่มีผู้ใช้หลายคนในเวลาเดียวกัน จะมีการให้แสดงตนต่อระบบตอนล็อกอินเข้าสู่ระบบ แล้วตามด้วยการใส่รหัสผ่าน ซึ่งหนังสือสีส้มแนะนำว่า รหัสผ่านต้องมีการป้องกัน โดยมีสิ่งตีพิมพ์ที่เป็นทางการ 2 เล่ม (The Department of Defense Password Management Guideline "the Green Book" กับ FIPS PUB 112 - Password Usage) ได้ให้ข้อมูลสนับสนุน เกี่ยวกับคุณสมบัติไว้ดังนี้

- ผู้ใช้ควรสามารถเปลี่ยนรหัสผ่านได้ด้วยตัวเอง
- รหัสผ่านควรเกิดจากการสร้างของเครื่องแทนที่จะให้ผู้ใช้สร้าง
- ตัวตรวจสอบ (เช่น วันที่และเวลาหลังจากล็อกอิน) ควรตั้งโดยระบบให้กับผู้ใช้

2.5.2.2 เส้นทางการไว้ใจได้

เส้นทางการไว้ใจได้ มีไว้สำหรับจัดเตรียมวิธีที่ไม่ยอมให้เกิดข้อผิดพลาดขึ้นกับผู้ใช้ในการติดต่อโดยตรงกับทีซีบี เพื่อจะได้ไม่ต้องผ่านส่วนของโปรแกรมประยุกต์หรือ ส่วนชั้นอื่น ๆ ของระบบปฏิบัติการ ที่อาจจะไว้ใจไม่ได้ ซึ่งเส้นทางการไว้ใจได้นี้ มีในระบบที่มีความมั่นคงตั้งแต่ระดับขั้น B2 ขึ้นไป

2.5.2.3 การตรวจสอบ

การตรวจสอบ หมายถึงการเก็บบันทึก การทดสอบ การทบทวนดูการกระทำที่เกี่ยวข้องกับความมั่นคงของระบบ ซึ่งจะรวมถึงการกระทำใด ๆ ที่ตัวกระทำเข้าถึงตัวถูกกระทำ ในเทอมของการตรวจสอบ การกระทำใด ๆ จะเรียกว่า "เหตุการณ์" (EVENT) และการตรวจสอบเอง จะเรียกว่า "การบันทึกเหตุการณ์" (Event Logging) เหตุการณ์ที่สำคัญ ๆ จะประกอบด้วย

- การเข้าสู่ระบบ (Logon) ไม่ว่าจะเข้าสู่ระบบได้สำเร็จหรือไม่สำเร็จ
- การออกจากระบบ (Logout)
- การเข้าถึงระบบจากทางไกล (Remote Access)
- การเปิด ปิด เปลี่ยนชื่อ และการลบไฟล์
- การเปลี่ยนสิทธิระดับหรือคุณสมบัติด้านความมั่นคงของระบบ เช่น เปลี่ยนป้ายความไหวของไฟล์ (file's sentivity label) หรือของผู้ใช้

เหตุผลที่มีการตรวจสอบในสิ่งเหล่านี้ เพราะว่าความมั่นคงในระบบนั้นไม่มั่นคงสามารถที่จะถูกโจมตีได้

การตรวจสอบจึงมีการจัดเตรียมวิธีในการทดสอบในรูปแบบต่าง ๆ ของการโจมตีที่อาจเกิดขึ้นได้เริ่มต้นที่ระดับขั้น C2 ซึ่งในหนังสือสีส้มระบุว่าต้องมีการตรวจสอบ รหัสของผู้ใช้ต้องมีความสัมพันธ์กับการกระทำที่ผู้ใช้นั้นกระทำและตรวจสอบได้ หมายความว่า เมื่อใดที่ผู้ใช้พยายามที่จะล็อกอินเข้า (ไม่ว่าจะสำเร็จหรือไม่) หรือ ผู้ใช้ที่พยายามจะเข้าถึงไฟล์ที่ป้องกันไม่ให้ผู้ใช้นั้นเห็น หรือการที่ผู้ใช้นั้นพยายามที่จะทำตนเป็นผู้ดูแลระบบ สิ่งเหล่านี้ทั้งหมด ระบบจะต้องตรวจสอบได้

การตรวจสอบนี้ทำให้เกิดการกระทำ 2 อย่างที่เป็นประโยชน์ ในด้านความมั่นคงของระบบ ก็คือการระมัดระวัง (surveillance) และการสร้างโครงสร้างใหม่ (reconstruction) การระมัดระวังนี้ เป็นการเฝ้าดูการกระทำต่าง ๆ ของผู้ใช้ ซึ่งการตรวจสอบนี้ สามารถช่วยป้องกันการก่อกวนความมั่นคงของระบบที่อาจเกิดขึ้นได้ เพราะผู้ใช้รู้ว่ามีการจับตามองอยู่ ส่วนการสร้างโครงสร้างใหม่ มาจากการนำเหตุการณ์ที่ก่อกวนความมั่นคงของระบบ การเก็บสิ่งที่เกิดขึ้น หรือ

สิ่งที่จำเป็นต้องแก้ไขเข้าไว้ด้วยกันและดูว่าใครควรรับผิดชอบ ซึ่งการตรวจสอบ เหตุการณ์ครั้งหนึ่งระบบจะเขียนข้อมูลต่อไปนี้ไว้ที่แนวการตรวจสอบ (audit trail)

- วันที่และเวลาของเหตุการณ์
- รหัสของผู้ใช้ที่สร้างเหตุการณ์
- ประเภทของเหตุการณ์
- สำเร็จหรือล้มเหลว
- ต้นกำเนิดที่ก่อให้เกิด เช่น หมายเลขของเทอร์มินอล
- ชื่อของตัวถูกกระทำที่เกี่ยวข้อง เช่น ไฟล์ที่ถูกลบ
- รายละเอียดของการแก้ไขฐานข้อมูลความมั่นคง

2.5.3 ความต้องการในด้านการประกัน

ความต้องการในด้านของการประกัน การประกันเป็นสิ่งที่ยืนยันว่านโยบายความมั่นคงของระบบที่ไว้ใจได้นั้น ได้มีการวางไว้อย่างถูกทาง ในหนังสือสีส้มได้แบ่งการประกันเป็น 2 ประเภทคือ การประกันทางการปฏิบัติ (operational assurance) และการประกันแบบวงจรชีวิต (life-cycle assurance) โดยการประกันในทางปฏิบัติ ได้เน้นในแง่ของพื้นฐานทางสถาปัตยกรรมและคุณลักษณะของระบบ ส่วนการประกันแบบวงจรชีวิต มุ่งเน้นในแง่ของการควบคุม และสร้างมาตรฐานในการสร้างและปรับปรุงระบบ โดยหนังสือสีส้ม ได้แยกลักษณะแต่ละส่วนของการประกัน ไว้ดังนี้

2.5.3.1 การประกันในทางปฏิบัติ ได้แก่

- สถาปัตยกรรมของระบบ (System architecture)
- ความเป็นเอกภาพของระบบ (System integrity)
- การวิเคราะห์ช่องทางลับ (Covert channel analysis)
- การจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ (Trusted facility management)
- การฟื้นฟูการไว้ใจได้ (Trusted recovery)

2.5.3.2. การประกันแบบวงจรชีวิต ได้แก่

- การทดสอบความมั่นคง (Security testing)
- การออกแบบลักษณะเฉพาะและทำการพิสูจน์ (Design specification and verification)

- การจัดการรูปร่าง (Configuration management)
- การกระจายความไว้ใจ (Trusted distribution)

2.5.4 ความต้องการในแง่เอกสาร

2.5.4.1. คำแนะนำสมบัติของความมั่นคงสำหรับผู้ใช้ (Security Features User's Guide) ใช้สำหรับผู้ใช้โดยทั่ว ๆ ไป ซึ่งจะบอกทุกสิ่งที่ผู้ใช้ต้องการรู้เกี่ยวกับความมั่นคงของระบบ รวมทั้งการป้องกันต่าง ๆ

2.5.4.2. คู่มืออำนวยความสะดวก (Trusted Facility Manual) ใช้สำหรับผู้ดูแลความมั่นคงหรือผู้จัดการของระบบ ซึ่งจะอธิบายทุกสิ่งเกี่ยวกับ การติดตั้งความมั่นคงให้กับระบบ การติดต่อกับความต้องการของผู้ใช้ มีคำเตือนเกี่ยวกับฟังก์ชันหรือสิทธิพิเศษ ที่ใช้ควบคุมระบบที่ไว้ใจได้ แต่งานของผู้ดูแลระบบจะซับซ้อนขึ้น และกฎโดยทั่วไปอาจไม่ครอบคุมสถานการณ์ทั้งหมดที่อาจเกิดขึ้น

2.5.4.3. เอกสารทดสอบ (Test documentation) เอกสารทดสอบที่ดี โดยมากมักมีปริมาณมาก และย่อมไม่ดีต่อระบบที่มีความมั่นคงในขั้น C1 หรือ C2 แต่ที่ต้องมีเหมือน ๆ กันในทุกระดับคือ แสดงกลไกวิธีการในการทดสอบความมั่นคง และผลของการทดสอบจากกลไกเหล่านั้น ในเอกสารการทดสอบต้องมีแผนการทดสอบ การตั้งสมมติฐานของสภาพแวดล้อมในการทดสอบ ทดสอบส่วนย่อย ผลที่คาดว่าจะเกิดและผลลัพธ์ที่ได้จริง

2.5.4.4. เอกสารการออกแบบ (Design documentation) เอกสารการออกแบบเป็นข้อคิด ในการสร้างเอกสารเกี่ยวกับส่วนภายในของระบบฮาร์ดแวร์ ซอฟต์แวร์และเฟิร์มแวร์ ซึ่งจุดรวมของการออกแบบเอกสารนี้คือ ปรัชญาของการป้องกัน และปรัชญาที่ว่านี้ก็จะถูกแปลงไปอยู่ในรูปของทีซีบี

2.6 ความมั่นคงของระดับขั้น B3

ระดับขั้น B3 ส่วนของทีซีบีต้องมีการรายงานการเข้าถึงในการกระทำต่าง ๆ ที่เกี่ยวข้องของทั้งตัวผู้กระทำและตัวถูกกระทำ ซึ่งในส่วนนี้โครงสร้างของทีซีบีอาจไม่เพียงพอต่อนโยบายด้านความมั่นคงในการป้องกันระบบ ต้องมีผู้จัดการด้านความมั่นคงมาช่วย เช่นในการ ตรวจสอบกลไกต่าง ๆ แล้วนำมาขยายแปลงเป็นสัญญาณในรูปเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงหรือการทำ

การฟื้นฟูระบบ ระบบจะต้องมีความต้านทานสูงต่อการถูกเจาะ ความต้องการอย่างต่ำของระบบในระดับขั้น B3 มีดังนี้

2.6.1 นโยบายด้านความมั่นคง (Security Policy)

2.6.1.1 การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ ทีซีบีจะกำหนด และควบคุมการเข้าถึงระหว่างชื่อผู้ใช้และชื่อของตัวถูกกระทำ (เช่น ไฟล์ หรือโปรแกรมต่างๆ) กลไกในการป้องกัน (เช่น เอซีแอล) จะอนุญาตให้ผู้ใช้สามารถระบุและ ควบคุมการแบ่งกันใช้ตัวถูกกระทำเหล่านั้นได้ รวมทั้งควบคุมการจำกัดสิทธิในการเข้าถึง กลไก ดีเอซีนี้ ผู้ใช้สามารถตั้งกำหนดขึ้นมาเอง หรือใช้จากค่าโดยปริยายของระบบ ซึ่งจัดให้มีการป้องกัน การเข้าถึงจากผู้ใช้ที่ไม่มีสิทธิ โดยการควบคุมการเข้าถึงนี้ สามารถระบุให้เฉพาะตัวถูกกระทำแต่ละตัว หรือสามารถระบุเป็นกลุ่มในโหมดของการใช้งานในตัวถูกกระทำนั้น ๆ ได้ และในทาง กลับกัน ก็สามารถระบุเฉพาะตัวหรือระบุเป็นกลุ่มในการไม่ยอมให้มีการเข้าถึงตัวถูกกระทำนั้น ๆ ได้เช่นกัน ซึ่งการอนุญาตในการเข้าถึงตัวถูกกระทำนี้ ต้องกำหนดโดยผู้ใช้ที่มี สิทธิเท่านั้น

2.6.1.2 การนำตัวถูกกระทำมาใช้ใหม่ หมายถึง การมีสิทธิในการใช้ข้อมูลต่างๆ ที่เก็บอยู่ในตัวถูกกระทำ จะต้องนำมาลบล้างหรือถอนสิทธิออก ก่อนที่จะมีการนำมาใช้ใหม่ โดยอาจมีการโยกย้ายตำแหน่งที่อยู่ของตัวกระทำในทีซีบี ไปในส่วนที่เป็นตัวถูกกระทำที่ไม่ใช้ แล้วไม่ให้เหลือข้อมูล รวมทั้งข้อมูลที่มีการเข้ารหัสไว้ ที่เกิดจากการสร้างของตัวกระทำในก่อนหน้านี้ ต้องลบล้างออกจากระบบให้หมด

2.6.1.3 ป้ายชื่อ หรือหมายถึง ป้ายความไหวเกี่ยวข้องกับทรัพยากรของระบบ เช่น ตัวกระทำ ที่เก็บตัวถูกกระทำ หน่วยความจำ เป็นต้น ซึ่งเป็นการเข้าถึงโดยตัวกระทำทั้งทางตรงและทางอ้อม ถูกดูแลรักษาโดยทีซีบี โดยใช้ป้ายชื่อนี้ เป็นพื้นฐานในการตัดสินใจในการควบคุมการเข้าถึงภายใต้อาณัติ แทนที่จะรับข้อมูลที่ไม่มีป้ายชื่อเข้ามา ทีซีบีจะร้องขอและรับจากผู้ใช้ที่มีสิทธิในการใช้ข้อมูล และการกระทำต่าง ๆ จะถูกตรวจสอบโดยทีซีบี

2.6.1.3.1 ความเป็นเอกภาพของป้ายชื่อ (Label Integrity) ต้องทำให้มั่นใจได้ว่าป้ายความไหวต้องเกี่ยวข้องสัมพันธ์กันอย่างถูกต้องระหว่างตัวกระทำและตัวถูกกระทำ สมมติเช่น ผู้ใช้มีการแก้ไขไฟล์ลับสุดยอด (TOP SECRET) โดยทำการลบข้อมูลลับทั้งหมดเสีย

เหลือแต่ข้อมูลที่ไม่มีการแยกแยะไว้ (UNCLASSIFIED) และจากนั้นทำการเปลี่ยนป้ายการรับรู้เป็นว่าไม่มีการแยกแยะ ถ้าระบบเกิดการขัดข้องขึ้น ต้องทำให้มั่นใจได้ว่าป้ายชื่อนั้นจะไม่ถูกเขียนลงจานแม่เหล็กก่อนที่ไฟล์จะถูกเปลี่ยนแปลง ถ้าหากเกิดเหตุการณ์เช่นนี้ขึ้น ต้องมีวิธีการกอบกู้ข้อมูลลับสุดยอดนั้น จากไฟล์ป้ายชื่อที่ไม่มีการแยกแยะได้

2.6.1.3.2 การส่งออกข้อมูลที่มีป้ายชื่อ (Exportation of labeled Infor - mation) ระบบที่ไว้ใจได้นั้น ต้องทำให้มั่นใจได้ว่า เมื่อข้อมูลถูกเขียนออกโดยระบบแล้ว ข้อมูลนั้นต้องคงได้รับการป้องกันอยู่ มี 2 ทางที่สำคัญในการส่งข้อมูลออกคือ การกำหนดระดับความมั่นคงให้กับอุปกรณ์ผลลัพธ์ และการใส่ป้ายความไหวให้กับข้อมูล โดยที่อุปกรณ์ในการส่งผลลัพธ์ มีการกำหนดไว้ 2 อย่างคือ

ก. การส่งออกไปที่อุปกรณ์หลายระดับ (Exportation to Multi-level devices) อุปกรณ์หลายระดับหรือช่องสื่อสารหลายระดับนี้ ใช้เขียนข้อมูลที่มีความไหวได้หลายระดับที่ต่างกัน ระบบต้องมีวิธีการในการระบุระดับของความมั่นคง เช่นต่ำสุด (ไม่มี การแยกแยะเลย) หรือสูงสุด (ลับสุดยอด) ให้สำหรับข้อมูลที่จะเขียนผ่านอุปกรณ์นั้น ๆ โดยกลไกในการจัดการจะแตกต่างกันในระบบที่ต่างกัน หรือชนิดของอุปกรณ์ที่ต่างกัน ไฟล์ต่าง ๆ ที่เขียนที่อุปกรณ์เหล่านั้นต้องมีระดับของความไหวอยู่ด้วย (โดยมากมักเก็บไว้ที่หัวระเบียนแรกก่อนถึงตัวข้อมูลในไฟล์) ซึ่งแบบนี้เป็นการป้องกันไม่ให้ผู้ใช้ผ่านข้ามการควบคุมของระบบ ในการทำสำเนาคัดลอกไฟล์ไปอย่างง่าย ๆ ไปไว้ที่อื่น ซึ่งแน่นอนว่าต้องมีระบบควบคุมการใช้อุปกรณ์เหล่านั้นและอะไรจะเกิดขึ้นกับข้อมูลที่ถูกถ่ายเทไปแล้ว ป้ายความไหวของไฟล์นี้ ไม่สามารถป้องกันได้ถ้าผู้ใช้สามารถนำแผ่นดิสต์เก็ตกลับบ้านได้ หรือสามารถที่จะส่งไฟล์ไปยังไปรษณีย์อิเล็คทรอนิคซึ่งในระบบที่ไว้ใจได้ส่วนใหญ่ จานแม่เหล็กเท่านั้นที่จัดว่าเป็นอุปกรณ์หลายระดับ

ข. การส่งออกไปที่อุปกรณ์ระดับเดี่ยว (Exportation to Single-level devices) อุปกรณ์ระดับเดี่ยวหรือช่องทางการสื่อสารระดับเดี่ยว ใช้สำหรับเขียนข้อมูลที่มีความไหวได้ระดับเดี่ยว เช่น เทอร์มินอล เครื่องพิมพ์ เครื่องขับเทป และพอร์ทของการสื่อสาร เป็นต้น ระดับที่สามารถระบุให้กับอุปกรณ์ได้นั้น จึงขึ้นอยู่กับที่ตั้งทางกายภาพ หรือธรรมชาติของความมั่นคงของอุปกรณ์นั้น ๆ ตัวอย่างเช่น ในการติดตั้งเครื่องพิมพ์ในห้องคอมพิวเตอร์หรือห้องต่าง ๆ ในสำนักงาน ต้องมีระดับของความไหวให้ เพื่อตอบสนองการใช้งานของบุคลากรซึ่งการติดตั้งในที่สาธารณะอาจระบุแบบไม่มีการแยกแยะไว้ ในขณะที่เครื่องพิมพ์อีกเครื่องหนึ่งอาจอยู่ในสำนักงานที่มีการป้องกันสูงใช้สำหรับงานลับสุดยอด และเมื่อติดตั้งอุปกรณ์ใน ลักษณะนี้ระบบต้องสามารถส่งข้อมูลที่มีระดับความสำคัญ ให้ถูกต้องสัมพันธ์กับอุปกรณ์นั้น ๆ ด้วย

ค. ป้ายชื่อของสิ่งพิมพ์ (Labeling Human-Readable Output) ต้องมีวิธีการระบุว่าสิ่งพิมพ์ที่จะพิมพ์ออกมานั้น ต้องมีป้ายระบุว่าเป็นของใคร อาจระบุไว้ที่ส่วนบนหรือส่วนล่างของหน้ากระดาษ ซึ่งการควบคุมทางกายภาพเป็นสิ่งจำเป็นมาก ในการจัดการสิ่งพิมพ์ พนักงานดูแลควรสังเกตและ ตรวจตราข้อมูลที่มีความไหวเหล่านั้นก่อนที่จะส่งไปยังเครื่องพิมพ์ และก็ไม่ควรกองไว้ที่ไหน เพื่อที่ใคร ๆ ก็สามารถดูได้

2.6.1.3.3 ป้ายความไหวของตัวกระทำ (Subject Sensitivity Labels) เป็นสภาวะที่ระบบต้องสังเกตุผู้ใช้เทอร์มินอลที่มีการเปลี่ยนแปลงระดับความมั่นคงในขณะใช้งานอยู่ แนวคิดของเรื่องนี้มีอยู่ว่า ผู้ใช้จะต้องรู้ระดับของความมั่นคงที่ใช้งานอยู่ ระบบที่ไว้ใจได้จะแสดงทำให้เกิดข้อกระจ่าง ในขณะที่ผู้ใช้ล็อกอินเข้าระบบ และจะแสดงเมื่อมีการเปลี่ยนระดับของความมั่นคงโดยอัตโนมัติหรือตามความต้องการของผู้ใช้

2.6.1.3.4 ป้ายชื่อของอุปกรณ์ (Device Labels) เป็นสภาวะที่อุปกรณ์ภายนอกที่ต่ออยู่กับระบบต้องถูกกำหนดระดับความมั่นคงที่สูงสุดและต่ำสุดให้ ซึ่งระดับความมั่นคงนี้ถูกนำมาใช้ในการบังคับการติดตั้งอุปกรณ์เหล่านั้นในสภาพแวดล้อมที่เหมาะสม

2.6.1.4 การควบคุมการเข้าถึงภายใต้อาณัติ ทีซีบีใช้การควบคุมแบบนี้จัดการกับทรัพยากรทั้งหมดในระบบ ที่ตัวกระทำภายนอกสามารถเข้าถึงทีซีบี ได้ทั้งทางตรงและทางอ้อม ซึ่งทั้งตัวกระทำและตัวถูกกระทำ ถูกกำหนดป้ายความไหวไว้ โดยมี การแบ่งแยกเป็นลำดับขั้นความสำคัญไว้ด้วย เพื่อเป็นพื้นฐานในการตัดสินใจในการใช้ควบคุมการเข้าถึง เช่น ตัวกระทำสามารถอ่านตัวถูกกระทำได้ ถ้าระดับความมั่นคงของตัวกระทำนั้น มีค่าสูงกว่า หรือเท่ากับตัวถูกกระทำ และตัวกระทำ สามารถเขียนตัวถูกกระทำได้ ถ้าระดับความมั่นคงของตัวกระทำมีค่าน้อยกว่าหรือเท่ากับของตัวถูกกระทำ

2.6.2 การชี้แจงรายการ (Accountability)

เป็นแนวคิดที่ระบบใช้ตรวจดูว่า ผู้ใช้คือใครและกำลังทำอะไร ซึ่งระบบต้องสามารถพิสูจน์แยกแยะผู้ใช้ได้ทั้งหมด ต้องสามารถพิสูจน์ได้ด้วยว่า ผู้ใช้นั้น ๆ มีสิทธิถูกต้องในการเข้าถึงข้อมูล และต้องเก็บการกระทำต่าง ๆ ที่เกี่ยวกับความมั่นคงของระบบ โดยการชี้แจงรายการจะต้องมีคุณลักษณะในเรื่องดังนี้

2.6.2.1 การพิสูจน์ตนและการแสดงตน การพิสูจน์ตนและการแสดงตนนี้ ทีซีบีกำหนดให้ผู้ใช้ต้องมีการแสดงตนก่อนที่จะกระทำการใด ๆ ที่เกี่ยวพันกับทีซีบี (เช่น การสั่งโปรแกรมทำงาน อ่านไฟล์หรือเกี่ยวข้องกับฟังก์ชันใด ๆ ที่ระบบ จำเป็นต้องดูว่าผู้ใช้นั้นมีสิทธิหรือไม่) ซึ่งส่วนมากระบบที่มีผู้ใช้หลายคนในเวลาเดียวกัน จะมีการให้แสดงตนต่อระบบ ในขณะล็อกอินเข้าสู่ระบบ แล้วตามด้วยการใส่รหัสผ่าน ผู้ใช้แต่ละคนต้องมีรหัสชื่อผู้ใช้โดยเฉพาะ ซึ่งรหัสชื่อผู้ใช้จะต้องไม่ซ้ำกันด้วย ไม่ใช่เป็นบริษัท แผนก กลุ่ม หรือหมายเลขเทอร์มินอลทั้งสิ้น และเมื่อผู้ใช้เข้าสู่ระบบได้แล้ว ระบบจะใช้รหัสที่ล็อกอินเข้ามากับแฟ้มที่เก็บข้อมูลความมั่นคง เพื่อใช้ในการพิจารณาให้ผู้ใช้มีสิทธิในการเข้าถึงข้อมูลเพียงใด อย่างเช่นถ้ามีผู้ใช้ที่พยายามใช้ไฟล์ที่มีความไหว ระบบจะนำรหัสผู้ใช้นั้นไปตรวจดูว่าเป็นผู้ใช้ที่ถูกต้องมีสิทธิ ในการแก้ ข้อมูลไฟล์นั้นหรือไม่ นอกจากนี้ระบบสามารถนำรหัสของผู้ใช้ เพื่อตรวจสอบดูกระทำ หากมีผู้ใช้ที่ไม่มีสิทธิ ทำการละเมิด ระบบสามารถตรวจสอบได้

2.6.2.2 เส้นทางการไว้ใจได้ มีไว้สำหรับจัดเตรียมวิธีที่ไม่ยอมให้เกิดข้อผิดพลาดขึ้นได้ ให้กับผู้ใช้ในการติดต่อโดยตรงกับทีซีบี เพื่อจะได้ ไม่ต้องผ่านส่วนของโปรแกรมประยุกต์หรือส่วนชั้นอื่น ๆ ของระบบปฏิบัติการที่อาจไว้ใจไม่ได้

2.6.2.3 การตรวจสอบ หมายถึงการเก็บบันทึก การทดสอบ การทบทวน ดูการกระทำที่เกี่ยวข้องกับความมั่นคงของระบบ ซึ่งรวมถึงการกระทำต่าง ๆ ที่ตัวกระทำเข้าถึงตัวถูกระทำ เหตุการณ์ที่สำคัญ ๆ ประกอบด้วย การล็อกอินเข้าสู่ระบบ ไม่ว่าจะเข้าสู่ระบบได้สำเร็จหรือไม่ การออกจากระบบ การเข้าถึงระบบจากทางไกล การเปิด ปิด เปลี่ยนชื่อ และการลบไฟล์ การเปลี่ยนสิทธิระดับ หรือคุณสมบัติด้านความมั่นคงของระบบ เช่น การเปลี่ยนป้ายความไหว การตรวจสอบเหตุการณ์ครั้งหนึ่ง ๆ ระบบจะบันทึกข้อมูลต่อไปนี้ไว้ที่ไฟล์แนวทางการตรวจสอบได้แก่ วันที่และเวลาของเหตุการณ์ รหัสของผู้ใช้ที่สร้างเหตุการณ์ ประเภทของ เหตุการณ์ สำเร็จหรือล้มเหลว ต้นกำเนิดที่ก่อให้เกิด เช่น หมายเลขเทอร์มินอล ชื่อของตัวถูกกระทำที่เกี่ยวข้อง เช่น ไฟล์ที่ถูกลบ รายละเอียดของการแก้ไขฐานข้อมูลความมั่นคง ระบบต้องสามารถเฝ้าดูเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง โดยมีกลไกใน การแจ้งต่อผู้ดูแลระบบ เช่น มีเสียงสัญญาณหรือข้อความมาเตือน เป็นต้น

2.6.3 การประกัน (Assurance)

2.6.3.1 การประกันในทางปฏิบัติ

2.6.3.1.1 สถาปัตยกรรมของระบบ ทีซีบีจะป้องกันสิ่งที่อยู่ในขอบเขตการดูแลจากการก่อกวนจากภายนอก เช่น การแก้ไขเปลี่ยนแปลง โครงสร้างของข้อมูล และจะดูแลโปรเซสให้ทำงานอยู่ภายใต้เนื้อที่ควบคุม คุณสมบัติด้าน ฮาร์ดแวร์ เช่น การจัดแบ่งเซกเมนต์ (Segmaentation) จะถูกนำมาใช้ในการแบ่งพื้นที่ในหน่วยความจำในทางตรรกภาพ โดยอาศัยคุณลักษณะต่าง ๆ เช่น ชื่อ ความสามารถในการอ่าน ความสามารถในการเขียนได้ เป็นต้น ทีซีบีจะถูกออกแบบให้มีโครงสร้างที่สมบูรณ์ มีกลไกในการ ป้องกันอย่างละเอียดอ่อน ซึ่งกลไกที่ว่านี้เป็นศูนย์กลางในการควบคุมบังคับโครงสร้างภายในของทีซีบีและระบบ ซึ่งทีซีบีจะอาศัยความสัมพันธ์ของนัยสำคัญของระดับชั้น (Layering) การซ่อนข้อมูลสำคัญของระบบทางวิศวกรรมจะลดความซับซ้อนของทีซีบี และป้องกันจากโมดูล ทีซีบีที่ไม่สำคัญ

2.6.3.1.2 ความเป็นเอกภาพของระบบ คุณสมบัติทั้ง ทางด้านฮาร์ดแวร์และซอฟต์แวร์ ต้องจัดให้ใช้ทำงานได้อย่างถูกต้องกับ ส่วนประกอบทางด้านฮาร์ดแวร์ และเฟริม์แวร์ ของทีซีบี

2.6.3.1.3 การวิเคราะห์ช่องทางลับ นักพัฒนาและผู้ดูแลระบบควรตรวจหาช่องทางลับทั้งหมดในระบบและทำการประเมินค่าความกว้างของแบนวิธ (band width) ของแต่ละช่องทาง

2.6.3.1.4 การจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ ทีซีบีจะเป็นตัวสนับสนุนการแบ่งการทำงานของผู้ดูแลระบบกับ ผู้ปฏิบัติการ

2.6.3.1.5 การฟื้นฟูการไว้ใจได้ ต้องมีชุดขั้นตอนคำสั่ง หรือกลไกในการจัดการระบบหลังการล้มเหลว

2.6.3.2 การประกันแบบวงจรชีวิต (Life-Cycle Assurance)

2.6.3.2.1 การทดสอบความมั่นคง กลไกความมั่นคงต้องนำมาทดสอบให้ทำงานคล้องกับที่อ้างไว้ในเอกสารของระบบ โดยต้องมีทีมงานที่ตั้งขึ้นมาโดยเฉพาะ และต้องเป็นผู้ที่เข้าใจจุดมุ่งหมายของทีซีบี ต้องทำการทั้งวิเคราะห์และทดสอบในเอกสาร ที่ออกแบบมา ชุดคำสั่ง (source code) รวมทั้งชุดคำสั่งในการทำงาน (object code) ด้วย โดยมีวัตถุประสงค์คือ ทำความเข้าใจ กับสิ่งที่ออกแบบขึ้นมาทั้งหมด และจัดการกับช่องโหว่ ที่ยอมให้ ตัวกระทำภายนอกทีซีบี สามารถอ่าน แก้ไข หรือลบข้อมูลที่ไม่สมควรจะลบได้ ภายใต้การควบคุมของนโยบายด้านความมั่นคงโดยใช้ดุลยพินิจ หรือภายใต้อาณัติของทีซีบี โดยต้องทำให้แน่ใจได้ว่าต้องไม่มีตัวกระทำอื่นที่ไม่มีสิทธิสามารถเข้ามาทำให้ทีซีบีอยู่ในสภาวะที่ ไม่สามารถตอบสนองการสื่อสารกับผู้ใช้อื่น ๆ ได้ ทีซีบีต้องคงทนทานต่อการถูกเจาะ และช่องโหว่ต่าง ๆ ที่พบต้องได้รับการแก้ไข มีการทดสอบทีซีบีใหม่ เพื่อแสดงว่าได้กำจัดช่องโหว่ได้จริง และจะไม่มีช่องโหว่เกิดขึ้นอีก

2.6.3.2.2 การออกแบบลักษณะเฉพาะและทำการพิสูจน์ หมายถึงรูปแบบของนโยบายด้านความมั่นคงโดยทั่วไปที่สนับสนุนทีซีบี ต้องได้รับการดูแลตลอดวงจรชีวิตของระบบ ซึ่งสามารถพิสูจน์ความเหนียวแน่นของระบบได้ในตัวเอง โดยที่สัณฐานระดับสุดยอดของทีซีบีต้องได้รับการดูแลรักษาไว้ให้สมบูรณ์และถูกต้อง ซึ่งในเอกสารการออกแบบ อาศัยการพิสูจน์ทางคณิตศาสตร์มาอธิบายทีซีบี

2.6.3.2.3 การจัดการสัณฐาน ในระหว่าง การพัฒนาและดูแลรักษาทีซีบี การจัดการสัณฐานของระบบ ต้องสร้างความมั่นใจในการจัดการระบบให้เป็นไปตามนโยบายด้านความมั่นคง มีการกำหนดค่าสัณฐานลงในเอกสารทั้งหมด รวมทั้งระบุความสัมพันธ์ที่เกี่ยวข้องกันของรุ่นทีซีบีที่ใช้อยู่ในปัจจุบัน

2.6.4 เอกสารสำหรับการวิจัย (Documentation)

2.6.4.1 คำแนะนำคุณสมบัติของความมั่นคงสำหรับผู้ใช้ เป็นบทสรุปคู่มือ หรือเอกสารที่บอกอธิบายกลไกในการป้องกันต่าง ๆ ที่ทีซีบีมีให้ มีคำแนะนำในการใช้งานและความสัมพันธ์ที่เกี่ยวข้องกับส่วนอื่น ๆ

2.6.4.2 คู่มืออำนวยความสะดวกที่ไว้ใจได้ เป็นคู่มือที่แสดงถึงข้อความ คำเตือน เกี่ยวกับงานและสิทธิต่าง ๆ ที่ต้องมีการควบคุมในขณะเรียกใช้ สิ่งอำนวยความสะดวกด้านความมั่นคง มีชุดขั้นตอนสำหรับการทดสอบ และรักษาไฟล์ตรวจสอบ ต่าง ๆ ที่ใช้ เหตุการณ์การตรวจสอบในแต่ละรูปแบบ ในคู่มือจะอธิบายฟังก์ชันงานของผู้ปฏิบัติการกับผู้ดูแลระบบ ที่เกี่ยวข้องในด้านความมั่นคง ประกอบด้วยการเปลี่ยนแปลง คุณสมบัติด้านความมั่นคงของผู้ใช้ มีคำแนะนำในการใช้คุณสมบัติของการป้องกันระบบอย่างมีประสิทธิภาพ การเชื่อมโยง การสร้างทีซีบีใหม่อย่างมั่นคง และขั้นตอนอำนวยความสะดวกต่าง ๆ คำเตือน และสิทธิ ต่าง ๆ ที่จำเป็นต้องมีการควบคุมในการใช้สิ่งอำนวยความสะดวกด้านความมั่นคง ทีซีบีที่เก็บกลไกอ้างอิง ต้องมีการพินิจพิเคราะห์แสดงตน และเมื่อเริ่มทำงาน ต้องทำให้ระบบอยู่ในสภาวะอาการที่มั่นคง

2.6.4.3 เอกสารทดสอบ นักพัฒนาระบบควรจัดเอกสารการประเมิน เพื่อใช้อธิบายแผนการทดสอบ ขั้นตอนการทดสอบที่แสดงกลไก วิธีการทดสอบ ด้าน ความมั่นคง และผลของการทดสอบจากกลไกเหล่านั้น ซึ่งอาจประกอบด้วย ผลของการทดสอบ จากวิธีที่มีประสิทธิภาพเพื่อใช้ลดแบนวิธของช่องทางลับ

2.6.4.4 เอกสารการออกแบบ เอกสารนี้ควรต้องมีอยู่ เพื่อใช้ในการอธิบายถึงปรัชญาในการดำเนินการของการป้องกันและอธิบายปรัชญานี้มาอยู่ในรูปของทีซีบี มีคำอธิบายการเชื่อมโยงโมดูลระหว่างทีซีบี มีคำอธบายที่เป็นทางการของนโยบายด้านความมั่นคงที่บังคับโดยทีซีบี และกลไกการป้องกันที่ระบุที่ทีซีบีต้องได้รับการพิสูจน์และอธิบาย ให้เห็นได้ว่าเป็นรูปร่างที่น่าพอใจ เอกสารต้องอธิบายถึงแนวคิดในการเฝ้ามอง การก่อกวนระบบ ที่ไม่สามารถข้ามไปได้ และจัดการได้อย่างถูกต้อง

2.7 ตัวอย่างของการคุกคามที่มีต่อระบบ

2.7.1 การเปิดเผยของข้อมูล (Data disclosure)

ผลของการคุกคามที่ข้อมูลถูกเปิดเผยจะเกิดขึ้นเมื่อผู้ใช้พยายามที่จะเข้าถึงข้อมูลที่ผู้ใช้นั้นไม่จำเป็นที่จะต้องรู้ ซึ่งขอบเขตของการจำเป็นที่จะต้องรู้ ถูกควบคุมโดยคุณสมบัติดีเอซีของระบบ ซึ่งขึ้นอยู่กับผู้ใช้ที่เป็นเจ้าของ ยอมให้ข้อมูลของตน เข้าถึงโดยผู้ใช้อื่นได้หรือไม่

2.7.2 การสูญเสียความถูกต้องของข้อมูล (Loss of data integrity)

การคุกคามแบบนี้ เกิดขึ้นโดยผู้ใช้หรือเมื่อข้อมูลของระบบถูกเขียนทับไม่ว่าโดยตั้งใจหรือไม่ตั้งใจ ซึ่งการสูญเสียความถูกต้องของข้อมูลนี้ อาจเกิดจากการเสียหรือล้มเหลวของฮาร์ดแวร์ เมื่อเกิดการสูญเสียของข้อมูลขึ้น ก็จะเป็นโอกาสของผู้ใช้ที่ไม่มีสิทธิ์เข้ามาทำการสร้างหรือเปลี่ยนแปลงข้อมูลที่มีผลต่อการทำงานของระบบโดยรวม

2.7.3 การสูญเสียความถูกต้องของทีซีบี (Loss of TCB integrity)

ทีซีบีซึ่งเป็นตัวควบคุมนโยบายความมั่นคงของระบบ เมื่อเกิดการสูญเสียความถูกต้องของโปรแกรมหรือไฟล์ของทีซีบี จะมีผลไปถึงการควบคุมความมั่นคงของระบบด้วย

2.7.4 การปฏิเสธการให้บริการ (Denial of service)

เพื่อประโยชน์ในการทำงาน ระบบต้องตอบสนองต่อการขอใช้บริการ มีวิธีเป็นไปได้ที่จะสร้างปัญหาให้กับระบบเพื่อให้ทำงานล้มเหลว ไม่สามารถรับผิดชอบต่องานได้ เมื่อมีการปฏิเสธ การให้บริการ ผู้ใช้จะสูญเสียความสามารถในการเข้าถึงข้อมูลของตน ซึ่งจะไปสัมพันธ์ กับการคุกคามที่กล่าวมาแล้วข้างต้น