บทที่ 5

สรุปการวิจัยและข้อเสนอแนะ

การเปรียบเทียบเกณฑ์ความมั่นคงในระดับขั้น B3 กับระบบที่ออกแบบ

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
1. นโยบายด้านความมั่นคง	
1.1 การควบคุมการเข้าถึงโดยใช้ดุลยพินิจ (Discretionary Access Control ดีเอซี) ทีซีบีจะกำหนดและควบคุมการเข้าถึงระหว่างชื่อผู้ใช้และชื่อของตัวถูกกระทำ กลไกในการป้องกัน จะอนุญาตให้ผู้ใช้สามารถระบุและควบคุมการแบ่งกันใช้ตัวถูกกระทำเหล่านั้นได้ รวมทั้งควบคุมการจำกัดสิทธิในการเข้าถึง กลไก ดีเอซีนี้ผู้ใช้สามารถตั้งกำหนดขึ้นมาเอง หรือใช้จากค่าโดยปริยายของระบบ ซึ่งจัดให้มีการป้องกันการเข้าถึงจากผู้ใช้ที่ไม่มีสิทธิ โดยการควบคุมการเข้าถึงนี้ สามารถระบุให้เฉพาะตัวถูกกระทำแต่ละตัว หรือสามารถระบุเป็นกลุ่มในโหมดของการใช้งานในตัวถูกกระทำนั้น ๆ ได้ และในทางกลับกันสามารถระบุเฉพาะตัวหรือระบุ เป็นกลุ่มในการไม่ยอมให้มีการเข้าถึงตัวถูกกระทำนั้น ๆ ได้เช่นกัน ซึ่งการอนุญาตในการเข้าถึงตัวถูกกระทำนี้ ต้องกำหนดโดยผู้ใช้ที่มีสิทธิเท่านั้น	คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน มีคุณสมบัติครบตามในข้อนี้แล้ว

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
1.2 การนำตัวถูกกระทำมาใช้ใหม่ (Object Reuse) การมีสิทธิในการใช้ข้อมูลต่างๆ ที่เก็บอยู่ในตัวถูกกระทำจะต้องนำมาลบล้างหรือถอนสิทธิออกก่อนที่จะมีการนำมาใช้ใหม่ โดยการโยกย้ายตำแหน่งที่อยู่ของตัวกระทำในทีซีบี ไปในส่วนที่เป็นตัวถูกกระทำที่ไม่ใช้ แล้ว ไม่ให้เหลือข้อมูล รวมทั้งข้อมูลที่มีการเข้ารหัสไว้ ที่เกิดจากการสร้างของตัวกระทำในก่อนหน้านี้ ต้องลบล้างออกจากระบบให้หมด	คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน มีคุณสมบัติครบตามในข้อนี้แล้ว
1.3 ป้ายชื่อ (Labels) ป้ายความไหวเกี่ยวข้องกับทรัพยากรของระบบ ซึ่งเป็นการเข้าถึงโดยตัวกระทำทั้งทางตรงและทางอ้อม โดยใช้ป้ายชื่อเป็นพื้นฐานในการตัดสินใจในการ ควบคุมการเข้าถึงภายใต้อาณัติสิทธิในการใช้ข้อมูล และการกระทำต่าง ๆ จะถูกตรวจสอบโดยทีซีบี	**โมดูลในการควบคุมการใช้งานในระบบ** ได้อธิบายแนวทางในการใช้งานป้ายชื่อ หรือป้ายความไหว มาระบุให้กับตัวกระทำและตัวถูกกระทำในระบบ
1.3.1 ความเป็นเอกภาพของป้ายชื่อ (Label Integrity) ต้องทำให้มั่นใจว่าป้ายความไหวต้องเกี่ยวข้องสัมพันธ์กันอย่างถูกต้องระหว่างตัวกระทำและตัวถูกกระทำ	**โมดูลในการควบคุมการใช้งานในระบบ** มีการตรวจสอบป้ายความไหวของทั้งตัวกระทำและตัวถูกกระทำ ก่อนที่จะอนุญาติให้ตัวกระทำเข้าถึงตัวถูกกระทำ
1.3.2 การส่งออกข้อมูลที่มีป้ายชื่อ (Exportation of labeled Information) ระบบที่ไว้ใจได้นั้น ต้องทำให้มั่นใจได้ว่า เมื่อข้อมูลถูกเขียนออกโดยระบบแล้ว ข้อมูลนั้นต้องคงได้รับการป้องกันอยู่ มี 2 ทางที่สำคัญในการส่งข้อมูลออกคือ การกำหนดระดับความมั่นคงให้กับอุปกรณ์ผลลัพธ์ และการใส่ป้ายความไหวให้กับข้อมูล	**โมดูลในการควบคุมการใช้งานในระบบ** มีการตรวจสอบป้ายความไหวของข้อมูลกับป้ายความไหวของอุปกรณ์ปลายทาง ถ้าอุปกรณ์ปลายทางมีป้ายความไหวของข้อมูลต่ำกว่าป้ายความไหวของข้อมูลที่จะส่งออก ก้จะไม่ยอมให้ทำงานได้

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
1.3.2.1 การส่งออกไปที่อุปกรณ์หลายระดับ (Exportation to Multi-level devices) ใช้เขียนข้อมูลที่มีความไหวได้หลายระดับที่ต่างกัน ระบบต้องมีวิธีการในการระบุระดับของความมั่นคง ให้สำหรับข้อมูลที่จะเขียนผ่านอุปกรณ์นั้น ๆ โดยกลไกในการจัดการจะต่างกันในระบบที่ต่างกัน หรือชนิดของอุปกรณ์ที่ต่างกัน ไฟล์ต่าง ๆ ที่เขียนที่อุปกรณ์เหล่านั้นต้องมีระดับของความไหวอยู่ด้วย ซึ่งเป็นการป้องกันไม่ให้ผู้ใช้ผ่านข้ามการควบคุมของระบบ ในการทำสำเนาคัดลอกไฟล์ไปอย่างง่ายไปไว้ที่อื่น **1.3.2.2 การส่งออกไปที่อุปกรณ์ระดับเดี่ยว (Exportation to Single-level devices)** อุปกรณ์ระดับเดี่ยว หรือช่องทางสื่อสารระดับเดียว สำหรับเขียนข้อมูลที่มีความไหวได้ระดับเดี่ยวเช่น เทอร์มินอล เครื่องพิมพ์ เครื่องขับเทป และพอร์ทของการสื่อสาร ระดับที่สามารถระบุให้กับอุปกรณ์ได้นั้น ขึ้นอยู่กับที่ตั้งทางกายภาพหรือธรรมชาติของความมั่นคงของอุปกรณ์นั้น ๆ ระบบต้องสามารถส่งข้อมูล ที่มีระดับความสำคัญให้ถูกต้องสัมพันธ์ กับ อุปกรณ์นั้น ๆ ด้วย **1.3.2.3. ป้ายชื่อของสิ่งพิมพ์ (Labeling Human - Readable Output)** ต้องมีวิธีการระบุว่าสิ่งพิมพ์ที่จะพิมพ์ออกมานั้นต้องมีป้ายระบุว่าเป็นของใคร อาจระบุไว้ที่ส่วนบนหรือส่วนล่างของหน้ากระดาษ ซึ่งการควบคุมทางกายภาพเป็นสิ่งจำเป็นมาก ในการจัดการสิ่งพิมพ์	**โมดูลในการควบคุมการใช้งานในระบบ** การส่งออกข้อมูล ถ้าอุปกรณ์ปลายทางมีป้ายความไหวของข้อมูลต่ำกว่าป้ายความไหวของข้อมูลที่จะส่งออก จะไม่ยอมให้ทำงานได้ เช่น ถ้าอุปกรณ์ปลายทางเป็นจอ เทอร์มินอล ก็จะทำการล็อคเทอร์มินอลนั้น หรือถ้าพิมพ์ข้อมูลที่มีป้ายความไหวสูงไปยังเครื่องพิมพ์ที่มีป้ายความไหวสูงเช่นกัน หมายถึงเครื่องพิมพ์นั้นจะต้องถูกติดตั้งไว้ในที่ที่มีความปลอดภัยสูง มีการควบคุมการเข้าถึงทางกายภาพ ระบบจะยอมให้พิมพ์ข้อมูลนั้นได้ โดยสิ่งพิมพ์ที่ได้มีการระบุ ป้ายความไหวของข้อมูลนั้นด้วย รวมทั้งมีการระบุชื่อและป้ายความไหวของเครื่องพิมพ์ วันที่-เวลา หมายเลขหน้า และจำนวนรวมของหน้าที่พิมพ์ คือระบุว่าพิมพ์หน้าที่เท่าไรของจำนวนหน้าทั้งหมด ถ้าอุปกรณ์ปลายทางเป็นดิสต์ ให้เปรียบเทียบป้ายความไหวของข้อมูลกับป้ายความไหวของดิสต์ ถ้าป้ายความไหวของดิสต์สูงกว่าป้ายความไหวของข้อมูลระบบยอมให้ดิสต์นั้นเก็บข้อมูลได้

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
1.3.3 ป้ายความไหวของตัวกระทำ (Subject Sensitivity Labels) เป็นสภาวะที่ระบบต้องสังเกตผู้ใช้เทอร์มินอลที่มีการเปลี่ยนแปลงระดับความมั่นคงในขณะใช้งานอยู่ ผู้ใช้จะต้องรู้ระดับของความมั่นคงที่ใช้งานอยู่ ระบบที่ไว้ใจได้จะแสดงทำให้เกิดข้อกระจ่าง ในขณะที่ผู้ใช้ลงบันทึกเข้า และจะแสดงเมื่อมีการเปลี่ยนระดับของความมั่นคงโดยอัตโนมัติหรือตามความต้องการของผู้ใช้	**โมดูลในการควบคุมการใช้งานในระบบ** มีการกำหนดป้ายความไหวให้กับตัวกระทำในระบบ ซึ่งมีการแบ่งระดับความสำคัญของข้อมูล และมีการกำหนดกลุ่มของขอบเขตข้อมูลในป้ายความไหวไว้ ซึ่งสามารถใช้เปรียบเทียบถ้าตัวกระทำมีการเข้าถึงตัวถูกกระทำ โดยถ้าป้ายความไหวของตัวกระทำเปลี่ยนไป ก็จะมีการเก็บบันทึกไว้ตรวจสอบได้
1.3.4 ป้ายชื่อของอุปกรณ์ (Device Labels) เป็นสภาวะที่อุปกรณ์ ภายนอกที่ต่ออยู่กับระบบต้องถูกกำหนดระดับความมั่นคงที่สูงสุดและต่ำสุดให้ ซึ่งระดับความ มั่นคงนี้ถูกนำมาใช้ในการบังคับการติดตั้งอุปกรณ์เหล่านั้นในสภาพแวดล้อมที่เหมาะสม	**โมดูลในการควบคุมการใช้งานในระบบ** ได้ออกแบบให้มีการกำหนดป้ายความไหวให้กับอุปกรณ์ โดยที่ป้ายความไหวของอุปกรณ์มีการแบ่งระดับความสำคัญของข้อมูล และมีการกำหนดกลุ่มของขอบเขตข้อมูลไว้
1.4 การควบคุมการเข้าถึงภายใต้อาณัติ (Mandatory Access Control) ทีซีบีใช้การควบคุมแบบนี้กับทรัพยากรทั้งหมดในระบบ ที่ตัวกระทำภายนอกสามารถเข้าถึงทีซีบีได้ทั้งทางตรงและทางอ้อม ทั้งตัวกระทำและตัวถูกกระทำ ถูกกำหนดป้ายความไหวไว้โดยมี การแบ่งแยกเป็นลำดับขั้นความสำคัญไว้เพื่อเป็นพื้นฐานในการตัดสินใจในการใช้ควบคุมการเข้าถึง เช่น ตัวกระทำสามารถอ่านตัวถูกกระทำได้ถ้าระดับความมั่นคงของตัวกระทำนั้นมีค่าสูงกว่า หรือเท่ากับตัวถูกกระทำ และตัวกระทำสามารถเขียนตัวถูกกระทำได้ถ้าระดับความมั่นคงของตัว กระทำมีค่าน้อยกว่าหรือเท่ากับของตัวถูกกระทำ	**โมดูลในการควบคุมการใช้งานในระบบ** มีการกำหนดป้ายความไหวให้กับตัวกระทำและตัวถูกกระทำ ในเรื่องของการอ่านและเขียนข้อมูล ถ้าหากผู้ใช้เกิดการประมาณในการส่งข้อมูล ที่มีความสำคัญสูง ไปยังเครื่องพิมพ์ในที่สาธารณะ ระบบจะเปรียบเทียบป้ายความไหวของตัวข้อมูลกับเครื่องพิมพ์นั้น ซึ่งระบบก็จะไม่ยอมให้มีการพิมพ์ข้อมูลนั้นได้

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
2. การชี้แจงรายการ	
2.1 การพิสูจน์ตนและการแสดงตน (Identification and Authentication) ทีซีบีกำหนดให้ผู้ใช้ต้องมีการแสดงตนก่อนที่จะกระทำการใด ๆ ที่เกี่ยวพันกับทีซีบี เช่น การอ่านไฟล์หรือเกี่ยวข้องกับฟังก์ชันใด ๆ ที่ระบบจำเป็นต้องดูว่าผู้ใช้นั้นมีสิทธิหรือไม่ซึ่งส่วนมากระบบที่มีผู้ใช้หลายคนในเวลาเดียวกัน จะมีการให้แสดงตนต่อระบบตอนลงบันทึกเข้า แล้วตามด้วยการใส่รหัสผ่าน ผู้ใช้แต่ละคนต้องมีรหัสโดยเฉพาะ และเมื่อผู้ใช้ เข้าสู่ระบบได้แล้ว ระบบจะใช้รหัสที่เข้ามา กับแฟ้มที่เก็บข้อมูลความมั่นคง เพื่อใช้ในการ พิจารณาให้ผู้ใช้มีสิทธิในการเข้าถึงข้อมูลเพียงใด และระบบสามารถนำรหัสของผู้ใช้ เพื่อตรวจสอบดูกระทำหากมีผู้ใช้ที่ไม่มีสิทธิทำการละเมิดระบบ ก็สามารถตรวจสอบได้	คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน มีคุณสมบัติครบตามในข้อนี้แล้ว **โมดูลในการแสดงตนและการพิสูจน์ตน** ได้กำหนดแนวทางการป้องกันไว้สำหรับผู้ใช้ทั่วไปและผู้ดูแลระบบ ในการติดตั้งสภาวะแวดล้อมของการใช้งานในระบบ ให้มีความมั่นคงยิ่งขึ้น
2.2 เส้นทางการไว้ใจได้ (Trusted Path) ไว้สำหรับเตรียมวิธีที่ไม่ยอมให้เกิดข้อผิดพลาดกับผู้ใช้ในการติดต่อโดยตรงกับทีซีบี เพื่อจะได้ไม่ต้องผ่านส่วนของโปรแกรมประยุกต์ หรือส่วนอื่น ๆ ของระบบปฏิบัติการที่อาจไว้ใจไม่ได้	**โมดูลในการป้องกันผู้ใช้พิเศษ** ได้มีการกำหนดการเข้ามาใช้ระบบได้ของผู้ใช้พิเศษ ซึ่งป้องกันการปลอมแปลงเข้ามาใช้งานเป็นผู้ใช้พิเศษได้ในระดับหนึ่ง **โมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ** เมื่อผู้ใช้ มีการเข้าสู่ระบบ ระบบจะมีการตรวจสอบโปรเซสในขณะนั้นว่ามีโปรเซสใดที่ใช้พอร์ท telnet อยู่บ้าง ซึ่งระบบจะทำการจัดการกำจัดให้

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
2.3 การตรวจสอบ (Audit) การเก็บบันทึก การทดสอบ การทบทวนดูการกระทำที่เกี่ยวข้องกับความมั่นคงของระบบ ซึ่งรวมถึงการกระทำต่าง ๆ ที่ตัวกระทำเข้าถึง ตัวถูกกระทำ เหตุการณ์ที่สำคัญ ๆ ประกอบด้วย การเข้าสู่ระบบ ไม่ว่าจะเข้าสู่ระบบได้ สำเร็จหรือไม่ การออกจากระบบ การเข้าถึงระบบจากทางไกล การเปิด ปิด เปลี่ยนชื่อ และลบไฟล์ การเปลี่ยนสิทธิระดับ หรือคุณสมบัติด้านความมั่นคงของระบบ เช่น เปลี่ยนป้ายความไหว การตรวจสอบเหตุการณ์ครั้งหนึ่ง ๆ ระบบจะเขียนข้อมูลต่อไปนี้ไว้ที่แนวการตรวจสอบ ได้แก่ วันที่และเวลาของเหตุการณ์ รหัสของผู้ใช้ที่สร้างเหตุการณ์ ประเภทของเหตุการณ์ สำเร็จหรือล้มเหลว ต้นกำเนิดที่ก่อให้เกิด เช่น หมายเลขเทอร์มินอล ชื่อของตัวถูกกระทำที่เกี่ยวข้อง เช่น ไฟล์ที่ถูกลบ รายละเอียดของการแก้ไขฐานข้อมูลความมั่นคง ระบบต้องสามารถเฝ้าดูเหตุการณ์ที่เกี่ยวข้องกับความมั่นคง โดยมีกลไกใน การแจ้งต่อผู้ดูแลระบบ เช่น มีเสียงสัญญาณหรือข้อความมาเตือน เป็นต้น	**โมดูลในการตรวจสอบระบบ** ระบบปฏิบัติการ โอเอสเอฟวัน สามารถจัดหรือติดตั้งสภาวะแวดล้อม ให้มีการบันทึกการตรวจสอบสิ่งต่าง ๆ ดังต่อไป นี้คือ วัน-เวลาที่เกิดเหตุการณ์ ผู้ใช้หรือผู้กระทำที่เกี่ยวข้อง ประเภทของเหตุการณ์ที่เกิด เหตุการณ์นั้นทำได้ สำเร็จหรือล้มเหลว แหล่งกำเนิดหรือต้นทางที่เป็นที่มาของเหตุการณ์ มีกลไกในการเฝ้าติดตามและรายงานเหตุการณ์ที่ใกล้จะเป็นอันตรายต่อความมั่นคงของระบบ ซึ่งรายงานนี้จะรายงานให้ผู้ดูแลระบบทราบโดยทันที และมีการใส่กลไกเพื่อหยุดเหตุการณ์นั้นด้วย และมีกลไกในการป้องกันการเกิดการล้นของข้อมูลขึ้น โดยกลไกที่ว่านี้สามารถ เลือกการจัดการเมื่อเกิดการล้นของข้อมูลขึ้น โดยสามารถเปลี่ยนที่จัดเก็บรายการตรวจสอบได้ไหม่ **โปรแกรมในการป้องกันผู้ใช้พิเศษ และ โมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ** ได้มีการเก็บบันทึกการเข้าสู่ระบบของผู้ใช้ทั้งหมด ซึ่งสามารถนำมาตรวจสอบได้ ถ้าหากมีผู้ที่ไม่มีสิทธิพยายามปลอมเข้ามาสู่ระบบ โดยตรวจได้ด้วยว่าพยายามเข้าสู่ระบบมาจากที่ไหน **โมดูลในการควบคุมการใช้งานในระบบ** ในการส่งข้อมูลออกข้อมูล ถ้ามีการพยายามส่งข้อมูลที่มีป้ายความไหวเหนือกว่าป้ายความไหวของอุปกรณ์ที่จะส่งออก จะมีการบันทึกไว้และสามารถนำมาตรวจสอบได้

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับชั้น B3	ระบบที่ออกแบบ
3. การประกัน	
3.1 สถาปัตยกรรมของระบบ (System Architecture) ทีซีบีจะป้องกันสิ่งที่อยู่ในขอบเขตการดูแลจากการก่อกวนจากภายนอก เช่น การเปลี่ยนแปลงโครงสร้างของข้อมูล และจะดูแลโปรเซสให้ทำงานอยู่ภายใต้เนื้อที่ควบคุม คุณสมบัติด้านฮาร์ดแวร์ เช่นการจัดแบ่งเซกเมนต์ จะถูกนำมาใช้ในการแบ่งพื้นที่ในหน่วยความจำในทางตรรกภาพโดยอาศัยคุณลักษณะต่าง ๆ เช่น ชื่อความสามารถในการอ่าน ความสามารถในการเขียนได้ เป็นต้น ทีซีบีจะถูกออกแบบให้มีโครงสร้างที่สมบูรณ์ มีกลไกการป้องกันอย่างละเอียดอ่อน ซึ่งกลไกที่ว่านี้เป็นศูนย์กลางในการควบคุมบังคับโครงสร้างภายในของทีซีบีและระบบ	**โมดูลการออกแบบสถาปัตยกรรมระบบ** มีแนวทางในการออกแบบในส่วนของระบบปฏิบัติการ ซึ่งสามารถสร้างความมั่นคงระดับ B3 ให้กับระบบได้
3.2 ความเป็นเอกภาพของระบบ (System Integrity) คุณสมบัติทั้ง ทางด้านฮาร์ดแวร์และซอฟต์แวร์ต้องจัดให้ใช้ทำงานได้อย่างถูกต้อง กับส่วนประกอบทางด้าน ฮาร์ดแวร์และเฟิร์มแวร์ของทีซีบี	คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน มีคุณสมบัติครบตามในข้อนี้แล้ว
3.3 การวิเคราะห์ช่องทางลับ (Covert Channel Analysis) นักพัฒนาระบบควรตรวจหาช่องทางลับทั้งหมดในระบบและทำการประเมินค่าแบนวิธของแต่ละช่องทาง	**โมดูลการออกแบบการวิเคราะห์ช่องทางลับ** อธิบายการตรวจหาช่องทางลับต่าง ๆ ภายในเครื่องคอมพิวเตอร์ ซึ่งต่ออยู่กับเครือข่าย

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
3.4 การจัดการสิ่งอำนวยความสะดวกในการสร้าง ความมั่นใจ (Trusted Facility Management) ทีซีบีจะเป็นตัวสนับสนุนการแบ่งการทำงานกันของผู้ดูแลระบบกับผู้ปฏิบัติการ	**โมดูลใน การจัดการสิ่งอำนวยความสะดวกในการ สร้าง ความมั่นใจ** ได้มีการออกแบบแนวทางการ การจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจในเกณฑ์ความมั่นคงไว้ในด้านต่าง ๆ
3.5 การฟื้นฟูการไว้ใจได้ (Trusted Recovery) ต้องมีชุดขั้นตอน หรือกลไกในการจัดการระบบหลังการล้มเหลว	**โมดูลในการจัดการระบบหลังการล้มเหลว** มีแนวทางในการแก้ไขหลังจากระบบล้มเหลว สามาถทำการฟื้นฟูระบบได้ โดยอาศัยการทำสำเนา
3.6 การทดสอบความมั่นคง (Security Testing) กลไกความมั่นคงต้องนำมาทดสอบให้ทำงานสอดคล้องกับที่อ้างไว้ในเอกสารของระบบ โดยต้องมีทีมงานที่ตั้งขึ้นมาโดยเฉพาะเป็นผู้ที่เข้าใจจุดมุ่งหมายของทีซีบี ต้องทำการทั้งวิเคราะห์และทดสอบในเอกสารที่ออกแบบมา ชุดคำสั่ง (source code) รวมทั้งชุดคำสั่งในการทำงาน (object code) ด้วย โดยมีวัตถุ ประสงค์คือ ทำความเข้าใจกับสิ่งที่ออกแบบขึ้นมาทั้งหมด และจัดการกับช่องโหว่ ที่ยอมให้ตัวกระทำภายนอกทีซีบี สามารถอ่าน แก้ไข หรือลบข้อมูลที่ไม่สมควรจะลบได้ ภายใต้การควบคุมของนโยบายด้านความมั่นคงโดยใช้ดุลยพินิจหรือภายใต้อาณัติของทีซีบี โดยต้องทำให้แน่ใจได้ว่าต้องไม่มีตัวกระทำอื่นที่ไม่มีสิทธิสามารถเข้ามาทำให้ทีซีบีอยู่ในสภาวะที่ ไม่สามารถตอบสนองการสื่อสารกับผู้ใช้อื่น ๆ ได้ ทีซีบีต้องคงทนทานต่อการถูกเจาะ และช่องโหว่ต่าง ๆ ที่พบต้องได้รับการแก้ไข มีการทดสอบทีซีบีใหม่เพื่อแสดงว่าได้กำจัดช่องโหว่ได้จริง	**โมดูลในการทดสอบระบบ** มีการกำหนดเป็นแนวทางให้นักพัฒนาระบบและผู้ดูแลระบบ ทำการทดสอบความมั่นคงของระบบในทุก ๆ ด้านและมั่นใจได้ว่าระบบทำงานเป็นไปตามที่อธิบายไว้ในเอกสารการทดสอบ

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
3.7 การออกแบบลักษณะเฉพาะและการพิสูจน์ (Design Speci -fication and Verification) รูปแบบของนโยบายด้านความมั่นคงโดยทั่วไปที่สนับสนุนทีซีบี ต้องได้ รับการดูแลตลอดวงจรชีวิตของระบบ ซึ่งสามารถพิสูจน์ความคงทนของระบบได้ในตัวเอง โดยที่สัญฐานระดับสุดยอดของทีซีบี ต้องได้รับการดูแลรักษาไว้ให้สมบูรณ์และถูกต้อง ซึ่งในเอกสารการออกแบบอาศัยการพิสูจน์ทางคณิตศาสตร์มาอธิบายทีซีบี	**โมดูลในการออกแบบลักษณะเฉพาะและทำการพิสูจน์** มีการกำหนดแนวทางในการออกแบบเฉพาะ เช่น การออกแบบเอกสารด้านนโยบายความมั่นคง แนวทางการออกแบบเอกสารในการป้องกันทีซีบี และเอกสารในการจัดการกับช่องทางลับ โดยอาศัยทฤษฎีทางคณิตศาสตร์ มาอธิบายนโยบายด้านความมั่นคงของระบบ ในเอกสารการออกแบบ ต้องมีรูปแบบจำลองของนโยบายความมั่นคงอย่างเป็นทางการ โดยประกอบด้วย ตัวกระทำ ตัวถูกกระทำ โหมดของการเข้าถึง คุณสมบัติของความมั่นคง และการแปลงจากสภาวะเริ่มต้นของระบบไปสู่สภาวะที่ระบบมีความมั่นคง
3.8 การจัดการสัญฐาน (Configuration Management) ในระหว่าง การพัฒนาและการดูแลรักษาทีซีบี การจัดการสัญฐานของระบบ ต้องสร้างความมั่นใจในการจับคู่ของเอกสารทั้งหมดกับรหัสที่มีความเกี่ยวข้องกันของรุ่นทีซีบีที่ใช้อยู่ปัจจุบัน	**โมดูลในการออกแบบการจัดการสัญฐาน** มีการออกแบบแนวทางในการจัดการกับสัญฐานต่าง ๆ ในระบบ พร้อมทั้งการติดตามการเปลี่ยนแปลง ของสัญฐานที่จะมีผลต่อความมั่นคงของระบบ
4. เอกสารสำหรับการวิจัย	
4.1 คำแนะนำคุณสมบัติของความมั่นคงสำหรับผู้ใช้ (Security Features User 's Guide) เป็นบทสรุปคู่มือหรือเอกสารที่อธิบายกลไกในการป้องกันต่าง ๆ ที่ทีซีบีมีให้ มีคำแนะนำการใช้งานและความสัมพันธ์ที่เกี่ยวข้องกับส่วนอื่น	คุณสมบัติด้านความมั่นคงของระบบปฏิบัติการโอเอสเอฟวัน มีคุณสมบัติครบตามในข้อนี้แล้ว

คุณสมบัติตามเกณฑ์ความมั่นคงในระดับขั้น B3	ระบบที่ออกแบบ
4.2 คู่มืออำนวยความสะดวกที่ไว้ใจได้ (Trusted Facility Manual) เป็นคู่มือที่แสดงถึงคำเตือนเกี่ยวกับงานและสิทธิต่าง ๆ ที่ต้องมีการควบคุมในขณะเรียกใช้ สิ่งอำนวยความสะดวกด้านความมั่นคง มีขั้นตอนสำหรับการทดสอบ และรักษาไฟล์ตรวจสอบ ในคู่มือจะอธิบายฟังก์ชันงานของผู้ปฏิบัติการกับผู้ดูแลระบบที่เกี่ยวข้องในด้านความมั่นคง ประกอบด้วยการเปลี่ยนแปลงคุณสมบัติด้านความมั่นคงของผู้ใช้ มีคำแนะนำในการใช้คุณสมบัติของการป้องกันระบบอย่างมีประสิทธิภาพ การเชื่อมโยง การสร้างทีซีบีใหม่	**โมดูลในการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ** ได้มีการกำหนดแนวทางการออกแบบเอกสารหรือคู่มืออำนวยความสะดวกที่ไว้ใจได้ไว้แล้ว
4.3 เอกสารทดสอบ (Test Documentation) นักพัฒนาระบบควรจัดเอกสาร การประเมิน เพื่อใช้อธิบายแผนการทดสอบพร้อมทั้งขั้นตอนการทดสอบที่แสดงกลไก วิธีการทดสอบด้านความมั่นคง และผลของการทดสอบจากกลไกเหล่านั้น ซึ่งประกอบด้วยผลของการทดสอบจากวิธีที่มีประสิทธิภาพ เพื่อใช้ลดความกว้างของช่องทางลับ	**โมดูลในการทดสอบระบบ** ได้มีการกำหนดแนวทางการออกแบบเอกสารทดสอบไว้
4.4 เอกสารออกแบบ (Design Documentation) ใช้ในการอธิบายถึงปรัชญาการป้องกันในรูปทีซีบี มีคำอธิบายการเชื่อมโยงโมดูลระหว่างทีซีบี มีคำ อธิบายที่เป็นทางการของนโยบายด้านความมั่นคงที่บังคับโดยทีซีบี และกลไกการป้องกัน ที่ระบุที่ทีซีบีต้องได้รับการพิสูจน์ และอธิบายให้เห็นได้ว่าเป็นรูปร่างที่น่าพอใจ ต้องมีแนวคิดในการเฝ้ามองการก่อกวนระบบ ที่ไม่สามารถข้ามไปได้ และจัดการได้อย่างถูกต้อง	**โมดูลในการออกแบบลักษณะเฉพาะและทำการพิสูจน์** ได้มีการกำหนดแนวทางในการออกแบบเอกสารต่าง ๆ ไว้ เช่น เอกสารด้านนโยบายความมั่นคง เอกสารกลไกในการป้องกันทีซีบี เอกสารของช่องทางลับ

ข้อจำกัดและแนวทางการพัฒนาต่อ

ในวิทยานิพนธ์นี้ ได้กำหนดแนวทางการออกแบบระบบรักษาความมั่นคงให้ได้เกณฑ์ความมั่นคงในด้านต่าง ๆ เพื่อให้ระบบสามารถเป็นไปตามเกณฑ์ในระดับขั้น B3 ซึ่งในบางด้านระบบปฏิบัติการโอเอสเอฟวันในรุ่นปัจจุบัน (V. 4.0) ไม่เอื้ออำนวยต่อการทำ จึงขอสรุปแยกกันดังนี้

โมดูลที่สามารถนำไปพัฒนาต่อ เพื่อให้ระบบปฏิบัติการโอเอสเอฟวัน มีความมั่นคงมากขึ้น ได้แก่

- โมดูลในการป้องกันผู้ใช้พิเศษ
- โมดูลในการป้องกันผู้ใช้ให้เข้าสู่ระบบได้อย่างมั่นใจ
- โมดูลในการตรวจสอบระบบ
- โมดูลในการควบคุมการใช้งานในระบบ
- โมดูลในการแสดงตนและการพิสูจน์ตน
- โมดูลในการจัดการระบบหลังการล้มเหลว

โมดูลที่สามารถพัฒนาต่อได้ ถ้าโมดูลที่กล่าวข้างต้น ได้มีการพัฒนาขึ้นมาแล้ว มีดังนี้

- โมดูลในการจัดการสิ่งอำนวยความสะดวกในการสร้างความมั่นใจ
- โมดูลในการทดสอบระบบ
- โมดูลในการออกแบบลักษณะเฉพาะและทำการพิสูจน์
- โมดูลในการออกแบบการจัดการสัณฐาน
- โมดูลในการออกแบบการวิเคราะห์ช่องทางลับ

โมดูลที่ไม่สามารถทำได้ นอกจากการแก้ที่โครงสร้างของระบบปฏิบัติการ ได้แก่

- โมดูลในการออกแบบสถาปัตยกรรมของระบบ

ข้อเสนอแนะ

ระบบปฏิบัติการโอเอสเอฟวัน สามารถที่จะสร้างความมั่นคงให้ได้ในระดับขั้น B3 นั้น จะต้องมีการจัดสภาวะแวดล้อมการใช้งานไว้ให้เหมาะสม เช่น การควบคุมการเข้าถึงทางกายภาพ รวมถึงการให้บริการใช้งานได้เฉพาะหน่วยงานในระดับแผนก ที่ไม่ได้ต่อเข้ากับเครือข่ายภายนอก สามารถควบคุมการเข้ามาใช้งานของผู้ใช้ในระบบ

วิทยานิพนธ์นี้ ถือเป็นแนวทางการสร้างระบบรักษาความมั่นคงให้กับระบบปฏิบัติการยูนิกซ์อื่น ๆ ได้ ซึ่งผู้ดูแลระบบหรือผู้ดูแลด้านความมั่นคงสามารถนำวิธีการที่กล่าวถึง ไปประยุกต์ใช้กับระบบที่ตนรับผิดชอบได้