# บทที่ 7
# บทสรุป ปัญหาและข้อเสนอแนะ

## 7.1 บทนำ

สำหรับบทนี้จะกล่าวถึงบทสรุปและข้อเสนอแนะที่ได้จากการดำเนินการทำวิทยานิพนธ์ตลอดจนปัญหาและอุปสรรคที่เกิดขึ้นขณะทำวิทยานิพนธ์และในหัวข้อสุดท้ายเป็นการให้ข้อเสนอแนะแก่ผู้สนใจจะนำวิทยานิพนธ์ชุดนี้ไปพัฒนาต่อไป

## 7.2 สรุปผลการทำวิทยานิพนธ์

วิทยานิพนธ์ชุดนี้เป็นการเพิ่มสมรรถนะทางด้านความปลอดภัยให้แก่ระบบปฏิบัติการโดยการแก้ไขซิซเท็มคอลของระบบปฏิบัติการเพื่อเพิ่มกลไกการตรวจจับการบุกรุกซึ่งพัฒนาตามแนวคิดของการตรวจจับการบุกรุก กลไกดังกล่าวประกอบไปด้วย 3 ส่วนหลักได้แก่

1. **source** หมายถึงแหล่งข้อมูลที่ใช้สำหรับการตรวจสอบกิจกรรมว่าเป็นการบุกรุกโดยพิจารณาจากค่า user credential ชื่อซิซเท็มคอลและค่าพารามิเตอร์ของซิซเท็มคอลของโปรเซสที่กำลังทำงานในขณะนั้นโดยอ่านมาจากโครงสร้างข้อมูลของระบบปฏิบัติการใน kernel space
2. **analysis** หมายถึงวิธีการวิเคราะห์ พิจารณากิจกรรมโดยกำหนดนโยบายของการตรวจสอบกิจกรรมด้วยวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะซึ่งแทนกิจกรรมของระบบปฏิบัติการให้อยู่ในรูปแบบของสถานะหลังจากนั้นตรวจสอบการเปลี่ยนแปลงสถานะและพิจารณากิจกรรมนั้นด้วยกฎสนับสนุน
3. **response** เป็นการการตอบสนองต่อเหตุการณ์บุกรุกโดยการทำลายโปรเซสบุกรุกและโปรเซสอื่นๆ ที่มีเจ้าของคนเดียวกันกับโปรเซสบุกรุกโดยพิจารณาจากค่า UID

แนวคิดของการศึกษาและพัฒนากลไกการตรวจจับการบุกรุกของวิทยานิพนธ์ชุดนี้ครอบคลุมเฉพาะระบบปฏิบัติการยูนิกซ์เท่านั้นซึ่งทดสอบแนวคิดบนระบบปฏิบัติการเน็ทบีเอสดี ผลการทดสอบความแม่นยำของการตรวจจับการบุกรุก สรุปได้ว่ากลไกการตรวจจับการบุกรุกชุดนี้สามารถตรวจจับการบุกรุกได้ทุกกรณีที่ขัดต่อกฎสนับสนุน เช่นการพยายามเปลี่ยนสิทธิ์ของผู้บุกรุกเป็น root ปัญหาการล้นของบัฟเฟอร์ โปรแกรมโทรจันและโปรแกรม rootkits เป็นต้น แต่

ไม่สามารถตรวจจับการเกิด race condition ช่องโหว่ของระบบปฏิบัติการที่เกิดจากการปรับแต่งระบบปฏิบัติการที่ผิดพลาดได้ นอกจากนี้กระบวนการตรวจสอบสามารถทำงานได้ทั้งที่ทรัพยากรของระบบเหลืออยู่น้อย หรือมีจำนวนโปรเซสบุกรุกเกิดขึ้นมากกว่าหนึ่งโปรเซส

ในบางกรณีที่กฎสนับสนุนไม่ครอบคลุม ผู้บุกรุกอาจจะบุกรุกระบบได้สำเร็จ ระบบปฏิบัติการจำเป็นต้องได้รับการติดตั้งเครื่องมืออื่นๆ เพื่อเป็นการเสริมประสิทธิภาพทางด้านความปลอดภัยแก่ระบบปฏิบัติการ เช่น ติดตั้งโปรแกรม Tripwire เพื่อคอยตรวจสอบการเปลี่ยนแปลงของแฟ้มของระบบ หมั่นตรวจหา sniffer ที่ถูกติดตั้งไว้ในหรือติดตั้งโปรแกรม antisniffer หรือติดตั้งระบบวิเคราะห์ล็อกไฟล์ของ ศุภโชค [ศุภโชค, 2548]

ทางด้านผลกระทบของการตรวจจับการบุกรุกที่มีต่อระบบปฏิบัติการนั้นสรุปได้ว่า เฉพาะคำสั่ง su เท่านั้นที่ได้รับผลกระทบ ซึ่งในขณะนี้คำสั่งดังกล่าวจะถูกยกเลิกชั่วคราวจนกว่าจะออกแบบและพัฒนาโปรแกรมดังกล่าวขึ้นมาใหม่ สำหรับกิจกรรมอื่นที่ดำเนินการบนระบบปฏิบัติการชุดนี้ไม่ได้รับผลกระทบ

ประสิทธิภาพของระบบปฏิบัติการหลังจากได้รับการแก้ไขถือว่ายอมรับได้เนื่องจากเวลาที่เพิ่มขึ้นของซิซเท็มคอลน้อยกว่าร้อยละ 5 ซิซเท็มคอลที่ได้รับการแก้ไขส่วนใหญ่ใช้เวลาในการทำงานเพิ่มขึ้นเพียงเล็กน้อยซึ่งไม่เกินร้อยละ 1 ยกเว้นซิซเท็มคอล open() ได้ใช้เวลาเพิ่มจากเดิมถึงร้อยละ 3 แต่ก็ถือว่ายอมรับได้ โดยสรุปแล้วกลไกการตรวจจับการบุกรุกที่พัฒนาในวิทยานิพนธ์ชุดนี้มีคุณลักษณะดังต่อไปนี้

1. กลไกของการตรวจจับการบุกรุกสามารถทำงานได้ตลอดเวลาเนื่องจากถูกพัฒนาให้เป็นส่วนหนึ่งของระบบปฏิบัติการซึ่งแตกต่างกับระบบตรวจจับการบุกรุกแบบอื่นที่ทำงานในระดับโปรแกรมประยุกต์
2. กลไกของการตรวจจับการบุกรุกชุดนี้มีความคงทนต่อการก่อกวน และสามารถดำเนินงานต่อไปได้อย่างถูกต้อง อีกทั้งไม่มีการสร้างฐานความรู้เพื่อใช้การพิจารณากิจกรรม แต่อาศัยผลของการศึกษาและวิเคราะห์การบุกรุกที่เกิดขึ้นในอดีตมาออกแบบนโยบายเพื่อเป็นแนวทางในการตรวจสอบกิจกรรม
3. กลไกของการตรวจจับการบุกรุกจะไม่ถูกทำลายหรือเปลี่ยนแปลงโดยโปรเซสอื่น เพราะระบบทำงานในระดับระบบปฏิบัติการไม่ใช่ระดับของโปรเซส เว้นแต่ผู้ดูแลระบบได้คอมไพล์ระบบปฏิบัติการใหม่เพื่อยกเลิกกลไกดังกล่าว

4. กลไกของการตรวจจับการบุกรุกได้รับการทดสอบทางด้านผลกระทบของการทำงาน และทดสอประสิทธิภาพของระบบ ปฏิบัติการแล้วว่า โดยภาพรวมแล้วกลไกการตรวจจับการบุกรุกไม่ก่อให้เกิดผลกระทบแก่ผู้ใช้ทั่วไป ยกเว้นคำสั่ง su ซึ่งเรียกใช้โดยผู้ดูและระบบ สำหรับโปรแกรมที่จะนำมาติดตั้งใหม่นั้นต้องมั่นใจว่าได้รับการพัฒนามาอย่างถูกต้องและมีความปลอดภัย น่าเชื่อถือโดยเฉพาะอย่างยิ่งโปรแกรมแบบ setuidในขณะที่ประสิทธิภาพของระบบปฏิบัติการเปลี่ยนแปลงไปในระดับที่ยอมรับได้
5. เมื่อศึกษาถึงการจัดอนุกรมวิธานของการบุกรุกจึงแสดงให้เห็นว่าช่องทางของการบุกรุกมีไม่กี่ช่องทาง อีกทั้งกลไกการตรวจจับการบุกรุกชุดนี้ได้ทำงานในระดับของซิซเท็มคอลซึ่งเป็นช่องทางเดียวที่โปรเซสของใช้สามารถเข้าถึงได้ ดังนั้นไม่ว่าผู้บุกอาศัยช่องทางใดเข้ามาในระบบจะต้องผ่านกระบวนการตรวจสอบเสมอ

## 7.3 ผลที่ได้จากการทำวิทยานิพนธ์ชุดนี้

ผู้ทำวิทยานิพนธ์ได้ศึกษาและวิเคราะห์วิธีการตรวจจับการบุกรุกด้วยการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซสโดยติดตามการเปลี่ยนแปลงค่า user credential เพื่อที่จะนำแนวคิดที่ได้นั้นไปพัฒนาในระดับของระบบปฏิบัติการโดยการแก้ไขซิซเท็มคอล (รายละเอียดในหัวข้อที่ 3.3 และ 3.4) แต่ก่อนที่จะแก้ไขซิซเท็มคอลนั้นได้ทดสอบแนวคิดนั้นในระดับโปรแกรมประยุกต์ให้เพื่อแน่ใจว่าแนวคิดนั้นมีความแม่นยำและไม่มีผลกระทบต่อระบบปฏิบัติการ เมื่อมั่นใจแล้วว่าแนวคิดที่ได้มาทำงานได้จริงจึงแก้ไขซิซเท็มคอลตามวิธีการที่ได้มา (รายละเอียดในบทที่ 4) ท้ายที่สุดทำการทดสอบความถูกต้องและประสิทธิภาพของระบบปฏิบัติการภาพหลังการแก้ไขซึ่งสรุปได้ว่า กลไกการตรวจจับการบุกรุกสามารถทำงานได้อย่างถูกต้อง แม้ว่าการแก้ไขระบบปฏิบัติการจะก่อให้เกิดการเปลี่ยนแปลงทางด้านประสิทธิภาพของระบบปฏิบัติการ เมื่อทดสอบประสิทธิภาพแล้วพบว่าการเปลี่ยนแปลงองประสิทธิภาพอยู่ในระดับที่ยอมรับได้ (รายละเอียดในบทที่ 5 และ 6)

ผลที่ได้จากการทำวิทยานิพนธ์ชุดนี้คือ ระบบปฏิบัติการเน็ทบีเอสดีที่มีความปลอดภัยยิ่งขึ้นโดยการแก้ไขระบบปฏิบัติการโดยเพิ่มกลไกการตรวจจับการบุกรุก และแนวทางของการเพิ่มสมรรถนะทางด้านความปลอดภัยบนระบบปฏิบัติการยูนิกซ์ตระกูลอื่นๆ เช่น ระบบปฏิบัติการฟรีบีเอสดี (FreeBSD) ระบบปฏิบัติการโซลารีส (Solaris) และ ระบบปฏิบัติการลินุกซ์ (Linux) เป็นต้น

## 7.4 ปัญหาและอุปสรรคของการทำวิทยานิพนธ์

ปัญหาและอุปสรรคของวิทยานิพนธ์ชุดนี้แบ่งออกเป็น 2 ส่วนได้แก่ ปัญหาทางด้านการทำวิทยานิพนธ์ และปัญหาทางด้านผู้ทำวิทยานิพนธ์เอง รายละเอียดของปัญหาต่างๆ จะกล่าวตามลำดับดังนี้

1. **ปัญหาทางด้านการทำวิทยานิพนธ์** ในส่วนของการทดสอบระบบ เนื่องจากโปรแกรมบุกรุกที่ดาวน์โหลดจากอินเทอร์เน็ตนั้นจะจำเพาะเจาะจงกับโปรแกรมเป้าหมายและรุ่นของโปรแกรมเป้าหมาย อีกทั้งระบบปฏิบัติการในตระกูลบีเอสดีนั้นหายากกว่าโปรแกรมบุกรุกบนระบบปฏิบัติการวินโดวส์ หรือระบบปฏิบัติการลินุกส์ (Linux)
2. **ปัญหาทางด้านผู้ทำวิทยานิพนธ์** ผู้วิจัยมีทักษะทางภาษาอังกฤษไม่ดีทั้งด้านการฟัง พูด อ่านและเขียนซึ่งก่อให้เกิดปัญหาในการศึกษางานวิจัยอื่นๆ อีกทั้งทักษะการเขียนรายงานเชิงวิชาการไม่ดีเช่นกันจึงใช้เวลาในการเขียนรายงานและ manuscript ค่อนข้างนาน

## 7.5 ข้อเสนอแนะ

งานวิจัยชุดนี้เป็นเพียงการเริ่มต้นศึกษาและทดสอบแนวคิดของการพัฒนาระบบตรวจจับการบุกรุกในระดับของระบบปฏิบัติการเท่านั้น ซึ่งครอบคลุมเฉพาะการรักษาความปลอดภัยของคอมพิวเตอร์บางส่วนเท่านั้นยังไม่ครอบคลุมความถึงความปลอดภัยของเครือข่ายคอมพิวเตอร์ ผู้สนใจควรศึกษาถึงการบุกรุกระบบเครือข่ายแล้วปรับปรุงกฎสนับสนุนเพื่อหาแนวทางสำหรับการแก้ไขซิซเท็มคอลที่เกี่ยวข้องอื่นๆ ต่อไป อีกทั้งงานวิจัยชุดนี้ได้พัฒนาและทดสอบแนวคิดนี้บนระบบปฏิบัติการเน็ทบีเอสดีเท่านั้นแต่ยังไม่ได้ทดสอบแนวคิดนี้บนระบบปฏิบัติการยูนิกซ์ตระกูลอื่น เช่น ระบบปฏิบัติการลีนุกซ์ ระบบปฏิบัติการโซลารีส (Solaris) เป็นต้น