บทที่ 7

บทสรุปและข้อเสนอแนะ

สำหรับบทนี้จะกล่าวถึงบทสรุปและข้อเสนอแนะที่ได้จากการดำเนินการวิจัย ตลอดจนปัญหาและอุปสรรคที่เกิดขึ้นขณะทำการวิจัยและในหัวข้อสุดท้ายเป็นการให้ข้อเสนอแนะแก่ผู้สนใจจะนำงานวิจัยนี้ไปพัฒนาต่อไป

7.1 สรุปผลการวิจัย

แบบจำลองที่พัฒนานี้ใช้วิธีการวิเคราะห์ข้อมูลของกิจกรรมของระบบหรือข้อมูลล็อกเพื่อตรวจจับการบุกรุก สามารถนำพัฒนาเพื่อใช้งานกับระบบปฏิบัติการยูนิกซ์เท่านั้น ไม่สามารถนำไปใช้กับระบบปฏิบัติการวินโดวส์ ซึ่งผลการทดสอบการทำงานของระบบการตรวจจับการบุกรุกที่พัฒนาในเครือข่ายที่จัดทำขึ้นสำหรับการทดสอบพบว่าความสามารถในการตรวจจับการบุกรุกจะขึ้นอยู่กับกฎที่ใช้ในส่วน Prefiltering และ Misuse Detection Engine เป็นหลัก ระบบสามารถตรวจจับการบุกรุกและแจ้งเตือนสำหรับเหตุการณ์การบุกรุกที่ทำให้เกิดล็อกตามเงื่อนไขที่กำหนดไว้ในกฎได้อย่างทันท่วงที และยังสามารถตรวจจับการบุกรุกรูปแบบใหม่ได้ หากเหตุการณ์บุกรุกนั้นทำให้เกิดล็อกที่ไม่เหมือนล็อกของเหตุการณ์ปกติ ตามที่ระบุไว้ในกฎสำหรับกระบวนการ Prefiltering แต่ผู้ดูแลระบบจะต้องตรวจสอบข้อมูลล็อกในไฟล์ที่ใช้เก็บส่วนของ unknown message ด้วยตนเอง นอกจากนี้จากการทดสอบยังพบว่าการบุกรุกบางวิธีจะไม่ปรากฏร่องรอยหรือล็อกของเหตุการณ์นั้นขึ้นในล็อกไฟล์ เช่น การเกิดเหตุการณ์ buffer overflow เป็นต้น ทั้งนี้เนื่องจากระบบไม่มีกลไกหรือเครื่องมือที่คอยตรวจจับการเกิดเหตุการณ์และบันทึกข้อมูลล็อกของเหตุการณ์ลงในล็อกไฟล์ ซึ่งเทคนิคที่เหมาะสำหรับการตรวจจับการบุกรุกในลักษณะนี้คือ State Transition Analysis โดยตัวอย่างงานวิจัยที่ใช้เทคนิคนี้ได้แก่ การจัดทำโปรแกรมตรวจจับการบุกรุกบนปฏิบัติการยูนิกซ์ [พัฒนาวดี ศิวติณทุโก, 2548] สำหรับกลไกหรือเครื่องมือที่ติดตั้งเพิ่มเติมเพื่อบันทึกกิจกรรมของระบบเพิ่มเติมจากเดิมพบว่าในกรณีของไวรัสควรติดตั้งโปรแกรม MailScanner และโปรแกรมค้นหาไวรัส และผู้ดูแลระบบจะต้องควรปรับปรุงข้อมูลไวรัสของโปรแกรมค้นหาไวรัสอย่างสม่ำเสมอ เพื่อผลการตรจจับไวรัสที่ดี และในกรณีที่ต้องการตรวจจับการบุกรุกที่เป็นการโจมตีผ่านระบบเครือข่ายควรจะติดตั้งโปรแกรม Snort เพิ่มเข้าไปในระบบด้วย นอกจากนี้ในกรณีที่ต้องการตรวจสอบหรือติดตามข้อมูลรายละเอียดของผู้บุกรุกเช่น ผู้บุกรุกมาจากหมายเลข IP ใดบ้างหรือจำนวนเหตุการณ์การบุกรุกในแต่ละวิธีเป็นเท่าใด ผู้ดูแลระบบสามารถตรวจสอบได้จากข้อมูลล็อคได้ด้วยตนเองหรืออาจจะพัฒนาโปรแกรมส่วนนี้เพิ่มเติม

สำหรับผลการศึกษาวิเคราะห์และนำเสนอระดับของการบันทึกเหตุการณ์ของ syslog บนเครื่อง ratree.psu.ac.th ศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ สรุปได้ว่าควรกำหนดค่า priority ในการบันทึกข้อมูลของ syslog ในระดับ information ขึ้นไปเนื่องจากการทดสอบการบุกรุกพบว่าข้อมูลร่องรอยส่วนใหญ่ที่เกิดขึ้นจะบันทึกลงในล็อกไฟล์ อยู่ในระดับนี้และข้อมูลล็อกที่ได้ก็มีรายละเอียดที่เหมาะสมสำหรับการนำวิเคราะห์เพื่อตรวจจับการบุกรุกได้เป็นอย่างดี โดยใช้พื้นที่ในการจัดเก็บข้อมูลล็อกประมาณวันละ 31 MB

ระบบที่พัฒนาขึ้นเมื่อเปรียบเทียบกับคุณลักษณะของระบบตรวจจับการบุกรุกที่ดีที่ได้กล่าวไว้ในหัวข้อที่ 3.7 ดังนี้

1. ทำงานอยู่ตลอดเวลาได้เองโดยไม่ต้องมีการควบคุมของผู้ดูแลระบบ และระบบต้องมีความน่าเชื่อถือที่เพียงพอที่จะทำงานในลักษณะอยู่เบื้องหลัง (background process) แต่ผู้ดูแลระบบต้องสามารถตรวจสอบการทำงานจากภายนอกได้
   ระบบที่พัฒนา : ทำงานในลักษณะอยู่เบื้องหลัง
2. เป็นระบบที่เป็น fault tolerant ในความหมายที่ว่ายังคงสามารถที่จะทำงานต่อไปได้ในกรณีที่ระบบคอมพิวเตอร์เกิดปัญหาหรือมีข้อผิดพลาดเกิดขึ้นและไม่ต้องมีการสร้างฐานข้อมูลความรู้ (knowledge-base) ทุกครั้งที่เริ่มระบบ
   ระบบที่พัฒนา : เก็บฐานข้อมูลความรู้ไว้ในไฟล์และไม่ต้องสร้างใหม่ทุกครั้งที่เริ่มระบบใหม่
3. มีความสามารถในการตรวจสอบตัวเองเพื่อไม่ให้ถูกลบ ทำลาย แก้ไข หรือถูกแทนที่ด้วยโปรแกรมอื่นได้
   ระบบที่พัฒนา : ไม่มี
4. ส่งผลกระทบกับการทำงานของระบบคอมพิวเตอร์น้อยที่สุด นั่นคือในการทำงานของระบบตรวจจับจะต้องใช้ทรัพยากรของระบบคอมพิวเตอร์น้อยที่สุดเท่าที่จะทำได้ เพราะถ้าหากทำให้ระบบคอมพิวเตอร์ทำงานช้าลงแล้วก็จะส่งผลให้ไม่มีการใช้งานระบบตรวจจับการบุกรุก
   ระบบที่พัฒนา : ใช้หน่วยความจำค่อนข้างน้อยในระหว่างที่ทำงาน
5. ตรวจสอบการทำงานที่ผิดไปจากรูปแบบการทำงานปกติได้
   ระบบที่พัฒนา : มีส่วนที่ทำหน้าที่ตรวจจับการทำงานที่ผิดปกติและการบุกรุก
6. ปรับเปลี่ยนหรือแก้ไขให้เข้ากับระบบคอมพิวเตอร์ได้ง่าย เนื่องจากแต่ละระบบคอมพิวเตอร์จะมีรูปแบบการใช้งานและกลไกในการป้องกันที่ต่างกัน
   ระบบที่พัฒนา : ระบบสามารถนำไปประยุกต์ใช้กับระบบที่ใช้ระบบปฏิบัติการยูนิกซ์ได้ง่าย แต่ไม่สามารถนำไปใช้กับระบบปฏิบัติการวินโดวส์ได้

7. ปรับการทำงานให้สอดคล้องกับการเปลี่ยนแปลงพฤติกรรมการใช้งานของระบบได้ เช่นเมื่อมีการติดตั้งโปรแกรมใหม่ ระบบ IDS ก็ต้องสามารถปรับเปลี่ยนการทำงานให้เข้ากับระบบที่เปลี่ยนไปได้
   ระบบที่พัฒนา : ระบบสามารถปรับเปลี่ยนการทำงานให้เข้าการเปลี่ยนแปลงระบบได้ง่าย โดยการแก้ไขข้อมูลกฎต่าง ๆ ที่เก็บอยู่ในไฟล์
8. มีความผิดพลาดในการทำงานน้อยที่สุด
   ระบบที่พัฒนา : ระบบสามารถสามารถตรวจจับได้อย่างถูกต้อง ภายใต้เงื่อนไขที่กฎต่าง ๆ ที่กำหนดไว้จะต้องมีความถูกต้องและมีข้อมูลล็อกส่งมาให้ระบบทำการวิเคราะห์เพื่อตรวจจับการบุกรุก

7.2 ปัญหาและอุปสรรคในการวิจัย

1. เนื่องจากบางเหตุการณ์ที่เกิดขึ้น ไม่มีกลไกในการตรวจจับการเกิดเหตุการณ์และบันทึกข้อมูลลงในล็อกไฟล์ ดังนั้นจึงต้องอาศัยโปรแกรมอื่น ๆ เช่น snort มาใช้เป็นเครื่องมือในการตรวจจับการเกิดเหตุการณ์โจมตีทางเครือข่ายและบันทึกข้อมูลลงในล็อกไฟล์ เพื่อจะให้ได้ข้อมูลมาใช้ในการวิเคราะห์ ดังนั้นจึงต้องใช้เวลาในการศึกษาเครื่องมือและกลไกที่ใช้ในการตรวจจับบางเหตุการณ์และบันทึกข้อมูลลงล็อกไฟล์ด้วย
2. การทดสอบการทำงานของระบบตรวจจับการบุกรุกที่พัฒนาขึ้น บางโปรแกรมจะส่งผลให้ระบบปฏิบัติการของเครื่องที่ใช้เป็นเป้าหมายของการโจมตีมีความเสียหาย ทำให้ไม่สามารถใช้ได้ จึงทำให้ต้องเสียเวลาในการติดตั้งระบบปฏิบัติการให้เครื่องดังกล่าวใหม่

7.3 ข้อเสนอแนะ

1. ควรพัฒนาโปรแกรมส่วนที่ใช้วิเคราะห์ข้อมูลการบุกรุกที่ไม่สามารถระบุได้เพิ่มเติม ซึ่งข้อมูลถูกเก็บอยู่ในไฟล์ unknown messages โดยอาจจะเป็นการรวบรวมและสรุปข้อมูลล็อกที่มีลักษณะคล้ายกันเป็นกลุ่มเดียวกัน ทั้งนี้เพื่อจะได้ง่ายสำหรับการตรวจสอบในภายหลัง
2. ควรเพิ่มเติมโปรแกรมส่วนที่ใช้ตรวจสอบความถูกต้องของกฎต่าง ๆที่เขียนเพื่อใช้ในการตรวจจับการบุกรุกด้วย เนื่องจากหากมีการเขียนกฎที่ไม่ถูกต้องอาจจะส่งผลกระทบต่อการทำงานของโปรแกรมได้

3. โปรแกรมที่พัฒนานี้เป็นการวิเคราะห์ข้อมูลล็อกทีละบรรทัดเท่านั้น ยังขาดความสามารถในการวิเคราะห์ล็อกในลักษณะหลายบรรทัดและการจัดลำดับของการเกิดเหตุการณ์ ความสัมพันธ์ของแต่ละเหตุการณ์ของการบุกรุกในแต่ละรูปแบบ เนื่องจากในการบุกรุกแต่ละรูปแบบอาจจะประกอบด้วยข้อมูลล็อกมากกว่า 1 รายการ