บทที่ 6

สรุปการวิจัย และข้อเสนอแนะ

สำหรับในบทนี้จะเป็นการกล่าวสรุปการวิจัย โดยจะเริ่มจากสรุปการวิจัยในการตรวจจับการบุกรุก การทำงานของระบบตรวจจับการบุกรุก ปัญหาและข้อจำกัดของระบบตรวจจับการบุกรุก และในหัวข้อสุดท้ายจะกล่าวถึงข้อเสนอแนะในการพัฒนาระบบตรวจจับการบุกรุกให้ทำงานได้มีประสิทธิภาพมากยิ่งขึ้นต่อไป

6.1 สรุปการวิจัยระบบตรวจจับการบุกรุก

วิทยานิพนธ์ชิ้นนี้เป็นการพัฒนาระบบตรวจจับการบุกรุกโดยใช้เทคนิคการแยกประเภท (classification) ของการทำเหมืองข้อมูล (data mining) มาใช้งานกับการตรวจสอบแบบผสมซึ่งนำวิธีการตรวจจับแบบ misuse detection และ anomaly detection มาใช้ร่วมกันเพื่อตรวจสอบการบุกรุกบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0 ซึ่งจากการทดสอบระบบตรวจจับการบุกรุกที่กล่าวมาแล้วในบทที่ 5 นั้นจะเห็นได้ว่าการตรวจจับการบุกรุกด้วยเทคนิคที่ใช้ในวิทยานิพนธ์ให้ผลการทดสอบเป็นที่น่าพอใจ นั่นคือระบบตรวจจับการบุกรุกสามารถแยกแยะการทำงานแบบปกติและการบุกรุกระบบได้ อีกทั้งยังช่วยลดปริมาณความเสียหายที่จะเกิดขึ้นต่อระบบด้วย

อย่างไรก็ตามไม่มีระบบตรวจจับการบุกรุกใดที่สามารถทำงานได้ครอบคลุมประเภทการบุกรุกทุกประเภทหรืออาจกล่าวอีกนัยหนึ่งได้ว่า ไม่มีระบบตรวจจับการบุกรุกใดที่สามารถทำงานได้อย่างสมบูรณ์แบบเนื่องจากลักษณะของการบุกรุกมีหลากหลาย เครื่องมือที่ใช้ตรวจจับการบุกรุกได้รับการพัฒนาขึ้นตามลักษณะของการบุกรุกแบบนั้น ๆ อีกทั้งผู้บุกรุกได้พัฒนาเครื่องมือที่ใช้สำหรับบุกรุกระบบอยู่เสมอเช่นเดียวกัน ในส่วนถัดไปจะกล่าวถึงการใช้งานระบบตรวจจับการบุกรุก การนำไปใช้งาน รวมทั้งปัญหาข้อจำกัดและข้อเสนอแนะ

6.2 การใช้งานระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุกนี้สามารถนำไปใช้งานได้จริงบนระบบปฏิบัติลินุกซ์เรด-แฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0 ซึ่งระบบตรวจจับการบุกรุกประกอบด้วยสารบบและแฟ้มข้อมูลในการทำงานดังที่กล่าวไว้ในบทที่ 4 เมื่อต้องการใช้โปรแกรมตรวจจับการบุกรุก

ให้ทำการแก้ไขแฟ้ม /etc/rc.d/rc.local เพื่อเพิ่มบรรทัดให้มีการเรียกใช้โปรแกรม phids.pl ให้ทำงานอยู่เบื้องหลังหลังจากที่บริการอื่น ๆ ของระบบได้ทำงานแล้ว สำหรับผลที่ได้จากการตรวจจับสามารถใช้เป็นข้อมูลให้กับผู้ดูแลระบบได้ เมื่อเกิดปัญหาเกี่ยวกับระบบผู้ดูแลระบบสามารถใช้แฟ้มบันทึกข้อมูลการบุกรุกเป็นหลักฐานในการสืบหาสาเหตุของการเกิดปัญหานั้นได้ อีกทางหนึ่งถ้าหากว่าปัญหาที่เกิดขึ้นเกิดจากการบุกรุกที่ระบบตรวจจับการบุกรุกครอบคลุมอยู่

6.3 ปัญหาและข้อจำกัด

จากขั้นตอนการทำงานของระบบตรวจจับการบุกรุกที่เริ่มต้นการทำงานเมื่อผู้ใช้ได้รับเชลล์มาแล้ว การทำงานในส่วนนี้ยังคงเป็นข้อจำกัดเนื่องจากยังมีโปรเซสอื่น ๆ ภายในระบบที่ยังไม่ได้ตรวจสอบการทำงานซึ่งโปรเซสที่ยังไม่ได้รับการตรวจสอบเหล่านั้นอาจถูกใช้เป็นเครื่องมือของผู้บุกรุกโดยไม่คาดการณ์ไว้ล่วงหน้า ระบบตรวจจับการบุกรุกที่สร้างขึ้นค่อนข้างใช้ทรัพยากรของระบบอย่างสิ้นเปลือง โดยที่ความสิ้นเปลืองส่วนใหญ่เกิดขึ้นจากการค้นหาเชลล์ของผู้ใช้ภายในระบบ ปัญหาที่สำคัญอีกอย่างหนึ่งคือหากนำระบบตรวจจับการบุกรุกนี้ไปใช้งานกับระบบปฏิบัติการที่มีงานภายในระบบมากจะทำให้เวลาทำงานส่วนใหญ่ของซีพียูหมดไปกับการสลับงานเข้าไปและออกมาจากหน่วยความจำ นอกจากนี้ยังมีปัญหาในเรื่องของความล่าช้าในการตรวจจับเพราะการทำงานของระบบตรวจจับการบุกรุกจะต้องเปิดปิดแฟ้มข้อมูลบ่อย ๆ อีกทั้งระบบที่พัฒนาขึ้นนำความถี่ของซิสเท็มคอลจากการเรียกใช้ของโปรเซสมาใช้งานในการตรวจจับ ฉะนั้นการทำงานในแต่ละครั้งของระบบตรวจจับการบุกรุกจะเป็นการตรวจจับภายหลังจากการทำงานของโปรเซสสิ้นสุดลงไปแล้ว ถึงแม้ว่าระบบตรวจจับการบุกรุกจะสามารถตรวจจับพฤติ-กรรมที่เข้าข่ายการบุกรุกได้ แต่ในเรื่องของการตอบสนองต่อพฤติกรรมเหล่านั้นจะเป็นเพียงการยับยั้งพฤติกรรมเสี่ยงที่จะเกิดตามมาจากพฤติกรรมที่ตรวจจับได้ และบันทึกข้อมูลที่มีก็เพื่อให้ผู้ดูแลระบบสามารถแก้ไขความเสียหายหรือเป็นแนวทางในการป้องกันครั้งต่อไปซึ่งถ้าหากสามารถตรวจจับการบุกรุกได้ก่อนที่โปรเซสนั้นจะทำงานได้สำเร็จก็จะเป็นการช่วยป้องกันพฤติกรรมที่เข้าข่ายการบุกรุกไม่ให้เกิดขึ้นได้ ปัญหาอื่น ๆ ที่มีผลกระทบต่อความถูกต้องในการตรวจจับคือการทำงานของระบบปฏิบัติการ เนื่องจากระบบปฏิบัติการลินุกซ์เรดแฮ็ทสร้างแฟ้มข้อมูลแบบ flush memory เมื่อในระบบมีโปรเซสเป็นจำนวนมากจะมีผลกระทบกับการสร้างแฟ้มข้อมูลซึ่งเป็นข้อ-มูลนำเข้าของระบบตรวจจับการบุกรุก เมื่อระบบตรวจจับการบุกรุกเปิดแฟ้มข้อมูลเพื่อนับความถี่ของซิสเท็มคอลจะทำให้ได้ความถี่น้อยกว่าปกติจึงมีผลต่อความผิดพลาดทางบวกและความผิดพลาดทางลบในการทำงาน

6.4 ข้อเสนอแนะ

ระบบตรวจจับการบุกรุกที่ได้รับการพัฒนาขึ้นนี้ยังเป็นเพียงต้นแบบของระบบตรวจจับการบุกรุกซึ่งควรจะได้รับการปรับปรุงเพื่อแก้ไขปัญหาและข้อจำกัดที่มีอยู่ เพื่อให้ได้ระบบตรวจจับการบุกรุกที่มีประสิทธิภาพในการทำงานมากขึ้นทั้งในส่วนการทำงานของระบบตรวจจับการบุกรุกเอง และในส่วนของผลกระทบต่อประสิทธิภาพในการทำงานของระบบปฏิบัติการ ดังนั้นการปรับปรุงระบบตรวจจับการบุกรุกจึงอยู่ในประเด็นต่อไปนี้

- ขยายขอบเขตการตรวจสอบกิจกรรมภายในระบบให้ครอบคลุมทุกกิจกรรม โดยการติดตามการทำงานของโปรเซส initd ซึ่งเป็นโปรเซสเริ่มต้นของระบบปฏิบัติการ
- ปรับปรุงการทำงานของระบบตรวจจับการบุกรุกให้สามารถใช้งานซีพียูและหน่วยความจำให้เกิดประโยชน์อย่างคุ้มค่า ในเบื้องต้นควรศึกษาการติดตามโปรเซสของโปรแกรม top เนื่องจากโปรแกรม top สามารถติดตามการทำงานของโปรเซสที่เกิดขึ้นในระบบทุกโปรเซส อีกทั้งยังมีการใช้งานซีพียูและหน่วยความจำได้อย่างมีประสิทธิภาพ หรืออาจเปลี่ยนกระบวนการของระบบตรวจจับการบุกรุกให้ทำงานที่ระดับของเคอร์เนลซึ่งเป็นศูนย์กลางที่คอยประสานการทำงานระหว่างส่วนต่าง ๆ ในระบบปฏิบัติการแทน
- ลดการทำงานที่เกี่ยวข้องกับการใช้แฟ้มข้อมูล นอกจากนี้ควรหาวิธีการตรวจจับการบุกรุกให้ทำงานในแบบ real-time เพื่อให้ระบบมีความปลอดภัยมากยิ่งขึ้น
- ระบบตรวจจับการบุกรุกที่พัฒนาขึ้นอาจถูกฝึกสอนโดยผู้ประสงค์ร้ายต่อระบบได้ ดังนั้นจึงควรเก็บค่าช่วงเวลาในการใช้งานซิสเท็มคอลด้วย
- ในการแยกประเภทข้อมูลโดยใช้โปรแกรม TiMBL จะต้องเรียนรู้ข้อมูลจากแฟ้มข้อมูลฝึกสอนระบบทุกครั้งซึ่งเป็นส่วนหนึ่งที่ทำให้ระบบทำงานล่าช้า ดังนั้นจึงควรปรับเปลี่ยนมาใช้ neural network แทนเพราะ neural network สามารถทำนายเหตุการณ์ต่าง ๆ ได้เองเมื่อผ่านการฝึกสอนระบบเรียบร้อยแล้ว

ระบบตรวจจับการบุกรุกที่พัฒนาขึ้นนี้สามารถใช้เป็นแนวทางเพื่อพัฒนาระบบตรวจจับการบุกรุกแบบผสมต่อไปในอนาคต เนื่องจากวิธีการบุกรุกระบบสามารถเปลี่ยนแปลงได้อยู่ตลอดเวลาและอาจมีการผสมผสานการบุกรุกด้วย ดังนั้นการที่ระบบตรวจจับการบุกรุก

สามารถรู้จักพฤติกรรมการบุกรุกได้มาก และมีกระบวนการเรียนรู้พฤติกรรมการบุกรุกจะทำให้ระบบตรวจจับการบุกรุกนั้นทำงานได้อย่างมีประสิทธิภาพ