บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของงานวิจัย

คอมพิวเตอร์เป็นอุปกรณ์หนึ่งที่มีความสำคัญในชีวิตของมนุษย์ในปัจจุบันนี้เป็นอย่างยิ่ง เนื่องจากความสามารถของคอมพิวเตอร์ได้อำนวยความสะดวกให้มนุษย์มากขึ้น งานที่เคยสิ้นเปลืองเวลาจำนวนมากสามารถลดระยะเวลาลงให้เหลือเพียงน้อยนิด มีความถูกต้องในการทำงานเพิ่มขึ้น อีกทั้งสามารถปรับปรุงเปลี่ยนแปลงการทำงานเพื่อให้ได้ผลลัพธ์ที่ต้องการได้ง่าย ด้วยเหตุนี้เองจึงทำให้คอมพิวเตอร์ได้เข้ามามีบทบาทสำคัญในการทำงานภายในองค์กรทั้งของรัฐบาลและของเอกชน ความแพร่หลายและประโยชน์ของคอมพิวเตอร์ได้ทำให้เกิดกิจกรรมที่สำคัญซึ่งทำให้องค์กรได้รับประโยชน์ และพัฒนาก้าวหน้าไปอย่างรวดเร็ว แต่การนำคอมพิวเตอร์มาใช้งานอย่างแพร่หลายนั้นก็ทำให้เกิดกิจกรรมที่ไม่พึงประสงค์ตามมาด้วยเช่นกัน นั่นคือการบุกรุกระบบคอมพิวเตอร์ การบุกรุกระบบคอมพิวเตอร์มีอยู่ด้วยกันหลายรูปแบบ ทั้งการบุกรุกจากภายนอกและภายในองค์กร อาทิเช่น พนักงานในองค์กรที่ต้องการรู้ข้อมูลที่เป็นความลับขององค์กรพยายามหาช่องทางที่จะนำเอาข้อมูลที่เป็นความลับนั้นออกมา หรือผู้ใช้งานในองค์กรนั้นพยายามใช้สิทธิเกินจากที่ได้รับจากผู้ดูแลระบบโดยวิธีการต่าง ๆ กัน ตัวอย่างเช่น เปลี่ยนแปลงสิทธิของตนเองให้มีสิทธิเทียบเท่ากับผู้ใช้ที่มีสิทธิสูงกว่าตนเอง ซึ่งพฤติกรรมเหล่านี้อาจจะก่อให้เกิดความเสียหายต่อระบบ ทำให้สูญเสียข้อมูล ข้อมูลไม่เป็นความลับหรืออาจจะทำให้การทำงานของระบบต้องหยุดชะงักลง และเสียค่าใช้จ่ายในการปรับปรุงและฟื้นฟูระบบ ตัวอย่างเหล่านี้เป็นเพียงส่วนหนึ่งที่ทำให้ผู้ดูแลระบบคอมพิวเตอร์ต้องมีภาระงานเพิ่มขึ้นในการตรวจสอบพฤติกรรมซึ่งอาจจะก่อให้เกิดความเสียหายเหล่านี้นอกเหนือไปจากการให้บริการทั่ว ๆ ไปที่ต้องปฏิบัติเป็นกิจวัตรอยู่แล้ว จากปัญหาเหล่านี้ทำให้ต้องมีการค้นหาวิธีการรักษาความปลอดภัยสำหรับระบบคอมพิวเตอร์ให้มากยิ่งขึ้น

งานวิจัยนี้ได้เสนอแนวทางในการสร้างต้นแบบระบบตรวจจับการบุกรุกแบบใหม่ ซึ่งเป็นการผสมผสานวิธีการตรวจจับการบุกรุกแบบการตรวจจับความผิดปกติ (anomaly detection) และการตรวจจับการใช้งานที่ไม่ถูกต้อง (misuse detection) เข้าไว้ด้วยกันเพื่อใช้ตรวจสอบการทำงานของคำสั่งและโปรแกรมที่ถูกเรียกใช้งานผ่านเชลล์ของระบบปฏิบัติการลินุกซ์เรด-แฮ็ท (RedHat) เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0 โดยอาศัยข้อมูลระบบซึ่งเป็นความถี่ของซิสเท็มคอล (system call) ที่เกิดจากการร้องขอทรัพยากรของระบบเพื่อใช้งานระบบปฏิบัติ

การเป็นเครื่องมือในการระบุลักษณะการทำงานว่าเป็นแบบการทำงานทั่วไปของลินุกซ์เรดแฮ็ท หรือเป็นการบุกรุกระบบ โดยนำวิธีการแยกประเภท (classification) ทางด้านการทำเหมืองข้อมูล (data mining) มาใช้ในการตรวจจับการบุกรุก

1.2 วัตถุประสงค์

1. เพื่อจัดทำต้นแบบระบบตรวจจับการบุกรุกแบบผสม (anomaly detection และ misuse detection) โดยใช้วิธีการทำเหมืองข้อมูลความถี่ของซิสเท็มคอลที่ถูกเรียกใช้งานบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท โดยให้ต้นแบบระบบตรวจจับการบุกรุกตรวจสอบคำสั่งพื้นฐานของระบบปฏิบัติการลินุกซ์ที่ถูกเรียกใช้งานเพื่อเป็นกรณีตัวอย่างของการตรวจจับการบุกรุก
2. พยายามลดความผิดพลาดที่เกิดขึ้นกับต้นแบบระบบตรวจจับการบุกรุกแบบผสม

1.3 ขอบเขตการวิจัย

1. สร้างข้อมูลฝึกสอนระบบ (training data) ซึ่งเป็นความถี่ของซิสเท็มคอลที่ได้มาจากการเรียกใช้งานคำสั่งพื้นฐานและโปรแกรมที่ทำงานบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท
2. พัฒนาต้นแบบระบบตรวจจับการบุกรุกแบบผสมที่นำเอาวิธีการตรวจจับความผิดปกติรวมกับวิธีตรวจจับการทำงานที่ไม่ถูกต้อง เพื่อใช้แยกประเภทข้อมูลที่เกิดขึ้นภายในระบบว่าเป็นแบบการทำงานทั่วไปของลินุกซ์เรดแฮ็ทหรือเป็นการบุกรุกระบบนี้ ได้เลือกคำสั่งพื้นฐานของระบบปฏิบัติการลินุกซ์เรดแฮ็ทมาใช้เป็นกรณีตัวอย่างเพื่อทดสอบการทำงานระบบตรวจจับการบุกรุกที่สร้างขึ้นสำหรับใช้งานกับระบบปฏิบัติการลินุกซ์เรดแฮ็ท เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0

1.4 ขั้นตอนการดำเนินงาน

1. ศึกษางานวิจัยและเอกสารที่เกี่ยวข้องและทำความเข้าใจกับเอกสารและงานวิจัยเกี่ยวกับระบบตรวจจับการบุกรุกโดยใช้ซิสเท็มคอลและการนำวิธีการทำเหมืองข้อมูลมาใช้งานร่วมกับการตรวจจับการบุกรุก
2. ศึกษาความถี่ของซิสเท็มคอลซึ่งเกิดจากการเรียกใช้งานของคำสั่งพื้นฐานแล้วนำมาสร้างเป็นข้อมูลฝึกสอนระบบ
3. ศึกษาเทคโนโลยีและเครื่องมือสำหรับการทำงานวิจัย ค้นหาเครื่องมือที่ช่วยในการทำวิจัย ศึกษาและทดลองใช้เครื่องมือนั้น

4. สร้างต้นแบบระบบตรวจจับการบุกรุกแบบผสมเพื่อใช้ทำนายกลุ่มผลลัพธ์จากข้อมูลที่ต้องการทดสอบ และฝึกสอนระบบจากชุดข้อมูลที่ได้รวบรวมไว้

5. ทดสอบและติดตั้งการใช้งาน ทำการทดสอบต้นแบบระบบตรวจจับการบุกรุกกับชุดข้อมูลจริงเพื่อทดสอบประสิทธิภาพในการทำงานโดยรวมของระบบ

6. จัดทำเอกสารประกอบระบบและรายงานวิทยานิพนธ์

1.5 ระยะเวลาในการดำเนินงาน

ตาราง 1.1 ระยะเวลาดำเนินงาน

ขั้นตอน	2546			2547												2548							
	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8
1																							
2																							
3																							
4																							
5																							
6																							

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ต้นแบบระบบตรวจจับการบุกรุกแบบผสมที่ใช้วิธีการทำเหมืองข้อมูลเพื่อใช้ตรวจสอบความถี่ของซิสเท็มคอลซึ่งถูกเรียกใช้งานโดยโปรแกรมต่าง ๆ บนระบบปฏิบัติการลินุกซ์เรด-แฮ็ท

2. เป็นแนวทางในการสร้างระบบตรวจจับการบุกรุกที่นำแนวคิดของการผสมผสานวิธีการตรวจจับทั้งสองอย่างคือ การตรวจจับความผิดปกติและการใช้งานที่ไม่ถูกต้องเข้าไว้ด้วยกันเพื่อพัฒนาความสามารถของระบบตรวจจับการบุกรุกต่อไปในอนาคต

1.7 สถานที่ทำการวิจัย

ห้องปฏิบัติการคอมพิวเตอร์ M105 ตึกคณิตศาสตร์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

1.8 เครื่องมือและอุปกรณ์ที่ใช้

1.8.1 ฮาร์ดแวร์

1. เครื่องไมโครคอมพิวเตอร์ ซีพียู Intel Pentium III 950 เมกะเฮิรตซ์ หน่วยความจำ 128 เมกะไบต์ ระบบปฏิบัติการ Red Hat Linux เวอร์ชัน 6.1 เวอร์ชัน 7.0 และเวอร์ชัน 9.0

2. เครื่องไมโครคอมพิวเตอร์ ซีพียู Intel Pentium III 439 เมกะเฮิรตซ์ หน่วยความจำ 256 เมกะไบต์ ระบบปฏิบัติการ Microsoft Windows XP Professional เวอร์ชัน 2002

1.8.2 ซอฟต์แวร์

1. ตัวแปลภาษาเพิร์ล เวอร์ชัน 5.00503 (RedHat เวอร์ชัน 6.1) เวอร์ชัน 5.6.0 (RedHat เวอร์ชัน 7.0) เวอร์ชัน 5.8.6 (RedHat เวอร์ชัน 9.0)

2. โปรแกรม TiMBL (Tiburg Memory-Based Learner) เวอร์ชัน 4.3

3. โปรแกรม EditPlus เวอร์ชัน 2.11