บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของหัวข้อวิจัย

ปัจจุบันเทคโนโลยีเครือข่ายคอมพิวเตอร์มีการเจริญเติบโตอย่างรวดเร็วเป็นเหตุให้บริษัท องค์กรหรือหน่วยงานจำนวนมากหันมาใช้เครือข่ายภายในองค์กร (intranet) และเครือข่ายอินเตอร์เน็ต (Internet) เป็นเครื่องมือในการสื่อสารมากขึ้นตามไปด้วย นั่นหมายความถึงจำนวนกิจกรรมที่จำเป็นในการใช้งานบนเครือข่ายคอมพิวเตอร์มีจำนวนสูงขึ้นเช่นเดียวกันกับกิจกรรมที่ไม่ได้รับอนุญาตหรือการยอมรับจากเจ้าของทรัพยากรก็มีจำนวนสูงขึ้นด้วยตัวอย่างเช่น การบุกรุกระบบคอมพิวเตอร์ ซึ่งสามารถจำแนกออกได้เป็นสองกลุ่มใหญ่คือการบุกรุกจากภายนอก (external intrusion) และการบุกรุกภายใน (internal intrusion) อาทิเช่น พนักงานในบริษัทที่ต้องการจะได้ข้อมูลที่เป็นความลับของบริษัทพยายามที่จะบุกรุกหาช่องทางที่จะเอาข้อมูลที่เป็นความลับนั้นออกมา หรือผู้ใช้ของระบบนั้นพยายามที่จะใช้สิทธิเกินจากที่ได้รับจากผู้ดูแลระบบโดยวิธีการต่าง ๆ กัน เช่น เปลี่ยนแปลงสิทธิของตนเองให้มีสิทธิเทียบเท่ากับผู้ใช้ที่มีสิทธิสูงกว่าตนเอง ซึ่งพฤติกรรมเหล่านี้อาจจะก่อให้เกิดความเสียหายต่อระบบ ทำให้สูญเสียข้อมูล ข้อมูลไม่เป็นความลับหรืออาจจะทำให้การใช้งานระบบต้องหยุดชะงักและเสียค่าใช้จ่ายในการปรับปรุงและฟื้นฟู ผู้ดูแลระบบต้องมีภาระงานเพิ่มขึ้นในการตรวจสอบพฤติกรรมซึ่งอาจจะก่อให้เกิดความเสียหายเหล่านี้นอกเหนือไปจากการให้บริการทั่วๆไปที่ต้องปฏิบัติเป็นกิจวัตรอยู่แล้ว จากปัญหาเหล่านี้ทำให้ต้องมีการค้นหาวิธีการหรือมาตรการต่าง ๆ เพื่อช่วยในการรักษาความปลอดภัยในระบบคอมพิวเตอร์ให้มากขึ้น

โดยทั่วไปการรักษาความปลอดภัยของคอมพิวเตอร์อาจจะแบ่งออกได้เป็นสองลักษณะใหญ่ ๆ คือ การป้องกันการบุกรุกและการตรวจสอบการบุกรุก สำหรับกระบวนการป้องกันที่มีใช้กันอยู่ในปัจจุบันนั้นระบบคอมพิวเตอร์ส่วนใหญ่จะมีบริการที่สามารถใช้สำหรับตรวจสอบและยืนยันสิทธิของผู้ใช้ในการเข้าใช้ทรัพยากรของระบบอย่างเช่น การที่ผู้ใช้จะต้องใส่ชื่อ (login) และรหัสผ่าน (password) ก่อนเข้าใช้ทรัพยากรในระบบ ก็เพื่อยืนยันว่าเป็นผู้ใช้ตัวจริงที่มีอยู่ในระบบ ซึ่งกระบวนการนี้เรียกว่าเป็นการรับรองว่าเป็นผู้ใช้ตัวจริง (authentication) หลังจากนั้นเมื่อผู้ใช้แต่

ละคนร้องขอใช้ทรัพยากรต่าง ๆ เช่น การอ่านหรือเขียนแฟ้มข้อมูล ระบบจะตรวจสอบว่าผู้ใช้มีสิทธิที่จะเข้าใช้ทรัพยากรเหล่านั้นหรือไม่ในระดับใดและอย่างไร กระบวนการนี้เรียกว่าการตรวจสอบสิทธิของผู้ใช้ (authorization) กระบวนการป้องกันอีกรูปแบบหนึ่งที่ใช้กันแพร่หลายได้แก่การเข้ารหัสข้อมูล (data encryption) ซึ่งเป็นการป้องกันไม่ให้ผู้ที่ไม่มีสิทธินำข้อมูลไปใช้

อย่างไรก็ตามจนกระทั่งปัจจุบันวิธีการป้องกันการบุกรุกที่กล่าวมาทั้งในส่วนของการตรวจสอบสิทธิของผู้ใช้และการเข้ารหัสข้อมูลยังไม่สามารถป้องกันการบุกรุกได้อย่างสมบูรณ์ เมื่อพิจารณากระบวนการป้องกันที่ใช้ชื่อและรหัสผ่าน เพื่อตรวจสอบผู้ใช้งานของระบบ ผู้บุกรุกเองก็มีวิธีการที่จะให้ได้มาซึ่งชื่อและรหัสผ่านของผู้ใช้ในระบบบางคนหรือทั้งหมด เพื่อที่จะเข้าใช้ทรัพยากรภายในระบบ ซึ่งแม้จะไม่ง่ายนักแต่ในปัจจุบันวิธีการที่จะให้ได้ข้อมูลเหล่านั้นมาเพื่อเข้าใช้ระบบสามารถกระทำได้ไม่ยาก เช่น เมื่อผู้บุกรุกได้รหัสผ่านของผู้ใช้ซึ่งอยู่ในรูปแบบของการเข้ารหัส ผู้บุกรุกก็จะพยายามทำการถอดรหัสนั้น ๆ โดยอาจจะใช้โปรแกรมที่สามารถเปรียบเทียบตัวอักษรตามพจนานุกรมแล้วทำการวนซ้ำในแต่ละตำแหน่งจนได้คำที่ตรงกับที่ผู้ใช้ใช้เป็นรหัสผ่าน การกระทำในลักษณะนี้ประสบความสำเร็จในระดับหนึ่งโดยเฉพาะในกรณีที่ผู้ใช้ละเลยเรื่องความสำคัญของการกำหนดรหัสผ่าน เช่น การใช้คำง่าย ๆ หรือคำที่มีความหมายซึ่งมีอยู่ในพจนานุกรมและรหัสผ่านที่มีความยาวไม่กี่ตัวอักษร พฤติกรรมเหล่านี้ช่วยให้ผู้บุกรุกสามารถถอดเอารหัสผ่านได้ในเวลาอันสั้น ตัวอย่างการบุกรุกที่เกิดจากผู้ใช้ในระบบเองที่เห็นได้ชัดอีกประการหนึ่งคือ การที่ผู้ใช้ภายในระบบพยายามเปลี่ยนแปลงสิทธิในการใช้ทรัพยากรของตนเองให้เทียบเท่ากับผู้ดูแลระบบซึ่งมีสิทธิในการใช้ทรัพยากรต่าง ๆ ทั้งหมด การกระทำดังกล่าวนี้สามารถกระทำได้โดยไม่ยากนัก โดยเฉพาะในกรณีที่ระบบเป้าหมายมีช่องโหว่ของตัวระบบเองหรือโปรแกรมประยุกต์ที่ใช้ จะเห็นได้ว่ากระบวนการการป้องกันไม่สามารถใช้แก้ปัญหาเกี่ยวกับความปลอดภัยในระบบความพิวเตอร์ได้ทั้งหมด ฉะนั้นปราการด่านที่สองในการรักษาความปลอดภัยซึ่งมีความสำคัญอีกด่านหนึ่งในกรณีที่ผู้บุกรุกสามารถเข้ามาในระบบได้แล้วก็คือการตรวจจับการบุกรุก (intrusion detection) ในส่วนของกระบวนการการตรวจจับนี้จะช่วยให้ผู้ดูแลระบบทราบว่ามีเหตุการณ์ผิดปกติหรือการบุกรุกเกิดขึ้นกับระบบและเกิดขึ้นอย่างไร โดยสามารถแบ่งอย่างคร่าวๆได้เป็นสองลักษณะคือ

1. การพิจารณาจากแฟ้มที่บันทึกการทำงานในระบบหรือแฟ้มบันทึกข้อมูลการบุกรุก (log file) โดยทั่วไประบบปฏิบัติการจะบันทึกเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบไว้ตามที่ผู้ดูแลระบบกำหนดและเมื่อเกิดเหตุการณ์ผิดปกติ หรือระบบไม่สามารถใช้งานได้ ผู้ดูแลระบบสามารถ

วิเคราะห์สืบหาร่องรอยการกระทำที่ก่อให้เกิดความผิดปกติหรือเสียหายแก่ระบบจากแฟ้มบันทึกข้อมูลการบุกรุกได้ และใช้ข้อมูลหรือความรู้ที่ได้จากการวิเคราะห์นี้ใช้ในการป้องกันการกระทำอันจะทำให้ระบบเสียหายในครั้งต่อไปได้ แต่เนื่องจากในปัจจุบันผู้บุกรุกระบบอาจจะเป็นผู้ที่มีความรู้ดีเท่าเทียมหรือดีกว่าผู้ดูแลระบบ ผู้บุกรุกสามารถทำลายหลักฐานโดยการแก้ไขหรือลบข้อมูลในแฟ้มบันทึกข้อมูลการบุกรุก เพื่อป้องกันไม่ให้ผู้ดูแลระบบสามารถสืบหาสาเหตุที่ทำให้เกิดความเสียหายของระบบได้

2. การตรวจสอบการบุกรุกที่กำลังเกิดขึ้นในขณะหนึ่ง ๆ ซึ่งถือว่าเป็นระบบการรักษาความปลอดภัยที่มีประโยชน์มากกว่าระบบการรักษาความปลอดภัยวิธีอื่น เนื่องจากเป็นวิธีที่สามารถตรวจสอบผู้บุกรุกที่กำลังทำการโจมตีระบบในขณะนั้น และทำการแจ้งเตือนผู้ดูแลระบบเพื่อให้หาทางป้องกันหรือแก้ไขทันเวลาได้ จะเห็นได้ว่าวิธีการตรวจสอบการบุกรุกในลักษณะนี้ช่วยลดหรือป้องกันความเสียหายที่เกิดจากการบุกรุกได้มากกว่าวิธีการแรก เนื่องจากผู้ดูแลระบบได้ทราบถึงการบุกรุกและมีโอกาสที่จะป้องกันหรือแก้ไขความเสียหายเหล่านั้นได้ทันก่อนที่ผู้บุกรุกจะกระทำความเสียหายแก่ระบบได้สำเร็จ

ระบบปฏิบัติการยูนิกซ์เป็นเป้าหมายหนึ่งของการบุกรุก เนื่องจากระบบนี้ได้ถูกนำมาใช้สำหรับการให้บริการสำคัญ ๆ ของระบบเครือข่ายเช่น การให้บริการจดหมายอิเล็คทรอนิก การให้บริการเว็บ เป็นต้น และในระบบปฏิบัติการยูนิกซ์มีผู้ใช้ที่มีสิทธิสูงสุด (root) ซึ่งสามารถควบคุมการทำงานและทรัพยากรทุกอย่างบนระบบได้อย่างเต็มที่ดังนั้นเป้าหมายหลักของผู้บุกรุกในระบบปฏิบัติการยูนิกซ์ส่วนใหญ่ก็คือต้องการะเป็นผู้ใช้ที่มีสิทธิสูงสุด

ระบบตรวจจับการบุกรุกที่มีอยู่ในปัจจุบันไม่สามารถใช้ได้กับภัยการบุกรุกทั้งหมด เนื่องจากภัยการบุกรุกในปัจจุบันเพิ่มขึ้นอย่างรวดเร็วและมีหลายรูปแบบระบบตรวจจับการบุกรุกแต่ละระบบจะมีการทำงานที่เฉพาะในแต่ละปัญหาขึ้นกับวัตถุประสงค์ของระบบตรวจจับการบุก-รุกนั้น ๆ สำหรับระบบตรวจจับการบุกรุกในงานวิจัยชิ้นนี้ใช้หลักการของการวิเคราะห์การเปลี่ยนแปลงสถานะของค่าประจำตัวของผู้ใช้ของโปรเซส (รายละเอียดถูกนำเสนอในบทที่2) ซึ่งช่วยลดปัญหาในเรื่องของการตัดสินผิด หรือ “false positive” ซึ่งเป็นปัญหาที่พบมากที่สุดปัญหาหนึ่งในเรื่องของการตรวจจับการบุกรุกเนื่องจากการเปลี่ยนแปลงสถานะในแต่ละขั้นของกระบวนการจะมีลักษณะที่แน่นอนทำให้ความผิดพลาดในการวิเคราะห์เหตุการณ์ที่เข้าข่ายการบุกรุกเป็นไปได้น้อยมาก ประกอบกับงานวิจัยของ ดร. นิษฐิดา นวลศรี [1] ได้เสนอแนวคิดในการตรวจจับการบุกรุก

โดยการตรวจสอบการเรียกใช้งาน system call ที่ถูกเรียกใช้โดยโปรแกรมต่าง ๆ บนระบบปฏิบัติการยูนิกซ์ โดยอาศัยรูปแบบของการวิเคราะห์การเปลี่ยนสถานะ (state transition analysis) พร้อมทั้งกฎที่ใช้สนับสนุนการพิจารณาการบุกรุก (supporting rules for intrusion detection) ฉะนั้นงานวิทยานิพนธ์ชิ้นนี้ได้เลือกเอาแนวคิดดังกล่าวมาพัฒนาเครื่องมือเพื่อใช้ในการตรวจจับการบุกรุกในขณะที่ผู้บุกรุกกำลังกระทำการบุกรุกบนระบบปฏิบัติการยูนิกซ์ ซึ่งคาดว่าผลที่ได้จะช่วยแก้ปัญหาในส่วนของการรักษาความปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้น

1.2 การตรวจเอกสาร

ถึงแม้ว่าในปัจจุบันระบบการตรวจจับการบุกรุกได้ถูกพัฒนาขึ้นมาก แต่ก็ยังไม่มีระบบใดในปัจจุบันที่สามารถทำงานได้อย่างถูกต้องแน่นอน และไม่มีการรับประกันความถูกต้องของการตัดสินใจ ดังนั้นการนำระบบเหล่านี้มาใช้ต้องคำนึงถึงความเหมาะสมหลายๆด้านประกอบกัน อาทิ เช่น ความเหมาะสมของระบบปฏิบัติการที่ใช้อยู่ วัตถุประสงค์ที่ใช้ รายละเอียดเกี่ยวกับระบบตรวจจับการบุกรุกและประเภทของระบบตรวจจับการบุกรุกจะกล่าวอย่างละเอียดอีกครั้งในบทที่ 2 สำหรับในหัวข้อนี้จะกล่าวถึงตัวอย่างระบบการตรวจจับการบุกรุกที่เป็นระบบตรวจจับเฉพาะตน

- ComputerWatch [2] ระบบนี้พัฒนาขึ้นเพื่อใช้งานบนระบบปฏิบัติการ System V/MLS เป็นระบบผู้เชี่ยวชาญที่ตรวจจับพฤติกรรมที่ผิดปกติ มีการทำงานแบบวิเคราะห์สถิติการทำงานของผู้ใช้และรายงานโดยการใช้ภาษาเอสคิวแอล (SQL-based query language)
- Discovery พัฒนาขึ้นโดยใช้ภาษาโคบอลและทำงานบนระบบไอบีเอ็ม เป็นระบบตรวจจับการบุกรุกบนระบบจัดการฐานข้อมูลขนาดใหญ่ มีการทำงานเป็นระบบผู้เชี่ยวชาญและใช้เทคนิคการวิเคราะห์สถิติของการใช้งานระบบฐานข้อมูล [3]
- HAYSTACK [4] พัฒนาขึ้นโดยใช้ภาษาซี ทำงานบนเครื่องคอมพิวเตอร์เมนเฟรม Unisys 1100/2000 และพีซีซึ่งใช้ระบบปฏิบัติการดอส และยังสามารถนำไปใช้งานกับระบบฐานข้อมูล ออราเคิล ข้อมูลที่ถูกวิเคราะห์แล้วจะถูกส่งจากเมนเฟรมไปยังพีซีโดยผ่านเครือข่ายคอมพิวเตอร์ระบบนี้จะตรวจจับการบุกรุกโดยอาศัยสถิติการใช้งาน
- IDES (Intrusion Detection Expert System) [5] ใช้วิธีการตรวจจับการบุกรุกจากสถิติที่มีโครงสร้างซับซ้อนและอาศัยระบบผู้เชี่ยวชาญสำหรับการตรวจจับความผิดปกติโดยมีการทำงานเป็นแบบเวลาจริง

- ISOA (Information Security Officer's Assistant) [6] การทำงานของระบบจะพิจารณาสถานะของผู้ใช้งานและสถิติของผู้ใช้แต่ละคน เมื่อมีการบุกรุกจะมีการตัดสินใจว่าการกระทำดังกล่าวถือเป็นการบุกรุกหรือไม่ โดยใช้หลักทางสถิติ ระบบนี้เป็นการทำงานแบบเวลาจริงบนระบบปฏิบัติการลีนุกซ์
- MIDAS (Multics Intrusion Detection and Alerting System) [7] เป็นระบบผู้เชี่ยวชาญทำงานแบบเวลาจริงบนระบบปฏิบัติการ Multics ใช้เทคนิคการเปรียบเทียบพฤติกรรมของผู้ใช้งาน และตรวจจับการบุกรุกผ่านจุดอ่อนของระบบ
- Wisdom and Sense [8] ถูกพัฒนาขึ้นที่ห้องปฏิบัติการลอสอาลามอส สหรัฐอเมริกา ทำงานบนระบบปฏิบัติการยูนิกซ์โดยรับข้อมูลที่จะวิเคราะห์จากสถานีงานระบบปฏิบัติการ VAX/VMS ระบบนี้วิเคราะห์การบุกรุกแบบทั่วไปเช่น ไวรัส, ม้าโทรจัน เป็นต้น

1.3 วัตถุประสงค์

นำเอาแนวคิดในการตรวจจับการบุกรุกจากงานวิจัยโดยใช้หลักการ state transition analysis และ supporting rules โดยอาศัยข้อมูลจากการเรียกใช้งาน system call มาใช้ในการออกแบบ และสร้างโปรแกรมตรวจจับการบุกบนระบบปฏิบัติการยูนิกซ์ เพื่อให้สามารถใช้งานได้จริง

1.4 ขอบเขตของการวิจัย

สร้างโปรแกรมตรวจจับการบุกรุกบนระบบปฏิบัติการยูนิกซ์โดยใช้วิธีการตรวจสอบการเรียกใช้ system call โดยอาศัยรูปแบบการวิเคราะห์การเปลี่ยนแปลงสถานะ พร้อมทั้งกฎที่ใช้สนับสนุนการพิจารณาการบุกรุก โดยระบบปฏิบัติการที่ใช้เป็นระบบปฏิบัติการ NetBSD ภาษาที่ใช้ในการโปรแกรมคือ ภาษาซี ลักษณะการทำงานของระบบตรวจจับการบุกรุกนี้จะคอยติดตามการทำงานของโปรเซสต่าง ๆ บนระบบคอมพิวเตอร์เมื่อโปรเซสอยู่ในสถานะที่เรียกว่า สถานะที่มีสิทธิพิเศษ system call ที่ถูกเรียกใช้ในขณะที่โปรเซสอยู่ในสถานะนี้จะถูกนำมาพิจารณาตามกฎที่ตั้งไว้ เมื่อตรวจพบการกระทำที่ถือว่าเป็นการบุกรุกจะหยุดกระบวนการทำงานนั้นให้เร็วที่สุดเพื่อป้องกันการกระทำต่อเนื่องที่จะสร้างความเสียหายแก่ระบบมากขึ้น ผลที่ได้จากการตรวจจับจะถูกบันทึกเป็นแฟ้มบันทึกข้อมูลการบุกรุก เพื่อที่ผู้ดูแลระบบสามารถใช้เป็นข้อมูลในการป้องกัน หรือซ่อมแซมส่วนที่เสียหายได้ต่อไป

1.5 ขั้นตอนและวิธีการดำเนินการวิจัย

1.5.1 ศึกษาการทำงานของเครื่องมือที่สามารถใช้ติดตามกระบวนการทำงานของโปรแกรมที่มีอยู่ในระบบปฏิบัติการที่ใช้ทำการวิจัย

1.5.2 วิเคราะห์ผลที่ได้จากโปรแกรมในข้อ 1.5.1

1.5.3 ศึกษาทำความเข้าใจกฎที่ใช้สนับสนุนการตรวจจับการบุกรุกทั้งหกข้อ

1.5.4 ศึกษาในเรื่องของ "process" บนระบบปฏิบัติการยูนิกซ์

1.5.5 ออกแบบและสร้างโปรแกรมพื้นฐานเพื่อตรวจจับการบุกรุกสำหรับกฎทั้งหกข้อ

1.5.6 ทดสอบและแก้ไขโปรแกรมพื้นฐานที่สร้างขึ้นในข้อ 1.5.5

1.5.7 พัฒนาและปรับปรุงโปรแกรมเพิ่มเพื่อให้โปรแกรมพื้นฐานที่โปรแกรมไว้สามารถใช้งานร่วมกันได้จริง

1.5.8 ทดสอบและนำโปรแกรมที่สร้างขึ้นใช้งานจริงในระบบ

1.5.9 สรุปและเขียนวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ได้ระบบสำหรับตรวจจับการบุกรุกบนระบบคอมพิวเตอร์

1.6.2 สร้างทางเลือกในการรักษาความปลอดภัยบนระบบปฏิบัติการยูนิกซ์