บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของวิทยานิพนธ์

ปัจจุบันระบบคอมพิวเตอร์และทรัพยากรภายในระบบมีความเสี่ยงต่อภัยคุกคามตลอดเวลา รายงานของ Computer Emergency Response Team หรือ CERT เรื่องจุดอ่อนในระบบคอมพิวเตอร์ได้อธิบายถึงช่องทางของการโจมตีระบบปฏิบัติการต่างๆ ตั้งแต่ปี ค.ศ. 1996 จนถึงปี ค.ศ. 2004 และมีรายงานเกี่ยวกับการโจมตีจำนวน 164 รายการ [CERT, 2004] เมื่อจำแนกช่องทางที่ก่อให้เกิดการบุกรุกเหล่านั้นตามแนวคิดของ Landwehr [Landwehr, 1994] พบว่าช่องทางเหล่านั้นเกิดจากความผิดพลาดในกระบวนการผลิตซอฟต์แวร์มีถึงร้อยละ 85.97 จากรายงานทั้งหมด ความผิดพลาดในกระบวนการผลิตซอฟต์แวร์ก่อให้เกิดการโจมตีด้วยวิธีการที่เรียกว่า การล้นของบัฟเฟอร์ (buffer overflow) ถึงร้อยละ 39.00 เป็นจุดอ่อนและช่องทางในการบุกรุกที่ไม่ระบุวิธีการอีกร้อยละ 57.44

นอกจากนี้ CERT รายงานถึงความสูญเสียทางเศรษฐกิจที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2003 รวมมูลค่าประมาณ 666 ล้านเหรียญสหรัฐ [CERT, 2003] โดยมีองค์กรต่างๆ ที่ได้รับผลกระทบเป็นผู้ให้ข้อมูล จากจำนวนองค์กรทั้งหมดมีองค์กรคิดเป็นร้อยละ 43 รายงานว่าอาชญากรรมทางคอมพิวเตอร์มีจำนวนเพิ่มขึ้นจากปีที่ผ่านมา องค์กรร้อยละ 70 ประสบกับอาชญากรรมทางคอมพิวเตอร์อย่างน้อยหนึ่งเหตุการณ์ จากจำนวนขององค์กรที่ประสบเหตุการณ์นั้นมีองค์กรร้อยละ 56 ได้รับผลกระทบทางด้านการดำเนินงาน ร้อยละ 25 ประสบปัญหาทางด้านการเงิน และร้อยละ 12 ได้รับผลกระทบอื่นๆ จากองค์กรที่ประสบปัญหา มีองค์กรร้อยละ 30 ขาดประสบการณ์ในการจัดการ ร้อยละ 25 พอที่จะทราบและมีแนวทางในการแก้ไข นอกจากนี้มีรายงานว่าการบุกรุกเกิดจากภายนอกองค์กรถึงร้อยละ 71 และเกิดจากการโจมตีจากภายในองค์กรร้อยละ 29 จากปัญหาทั้งหมดที่เกิดขึ้นองค์กรเหล่านั้นได้แก้ไขและป้องกันปัญหาโดยใช้วิธีการต่างๆ เช่น ติดตั้งไฟร์วอลล์ (firewall) การรักษาความปลอดภัยของระบบทางกายภาพ นอกจากนี้ยังป้องกันข้อมูลขององค์กรโดยการเข้ารหัส (encryption) แม้ว่าในแต่ละองค์กรมีวิธีการจัดการกับปัญหาที่เกิดขึ้นแต่ก็ไม่สามารถแก้ปัญหาได้ทั้งหมด จำเป็นต้องมีระบบที่ช่วยในการตรวจจับการบุกรุกมาช่วยอีกทางหนึ่ง นักวิจัยได้ศึกษาเกี่ยวกับการตรวจจับและป้องกันการบุกรุกระบบคอมพิวเตอร์โดยวิธีการต่างๆ และพัฒนาโปรแกรมเช่น โปรแกรมป้องกันและตรวจจับไวรัส โปรแกรมไฟร์วอล และระบบตรวจจับการบุกรุก (intrusion detection system หรือ IDS) เป็นต้น

Bace [Bace, 2001] ได้ให้คำนิยามของระบบตรวจจับการบุกรุกไว้ว่า ระบบตรวจจับการบุกรุกคือระบบที่ประกอบด้วยฮาร์ดแวร์หรือซอฟต์แวร์สำหรับตรวจสอบเหตุการณ์ที่เกิดขึ้นในระบบคอมพิวเตอร์เพื่อวิเคราะห์หาร่องรอยของการบุกรุกโดยอัตโนมัติ และได้ให้นิยามของการบุกรุก (intrusion) ไว้ว่า การบุกรุกคือ ความพยายามหรือการกระทำที่ส่งผลกระทบต่อความบูรณภาพ (integrity) ความลับ (confidentiality) และความพร้อมใช้งาน (availability) ของทรัพยากรหรือการกระทำเพื่อข้ามผ่านมาตรการในการควบคุมความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

ในหลายปีที่ผ่านมานักวิจัยเล็งเห็นความสำคัญของระบบความปลอดภัยของคอมพิวเตอร์จึงมีการศึกษาวิจัยทั้งในทางป้องกันและตรวจสอบปัญหาที่จะมีผลต่อความปลอดภัยของระบบคอมพิวเตอร์ จุดมุ่งหมายของการวิจัยทางด้านระบบตรวจจับการบุกรุกจะเน้นส่วนของระเบียบวิธีการตรวจจับ การปรับปรุงประสิทธิภาพและกลไกของความปลอดภัย ดังจะได้เห็นจากโปรแกรมตรวจจับการบุกรุกในปัจจุบัน เช่น Snort [Martin, 1999] USTAT [Ilgun, 1993] Firestorm [Leach, 2005] และ Tripwire [Donowan, 2005] เป็นต้น

จากการศึกษาถึงระบบตรวจจับการบุกรุกสรุปได้ว่าแต่ละระบบมีวิธีการทำงานที่หลากหลาย แตกต่างกันทั้งในด้านวิธีการตรวจจับการบุกรุกและสถาปัตยกรรมของระบบ แต่อย่างไรก็ตาม ระบบส่วนใหญ่มีความเหมือนกันคือ ต่างก็ทำงานในระดับของโปรแกรมของระบบปฏิบัติการ ดังนั้นโปรแกรมเหล่านี้จึงมีสถานะเทียบเท่ากับโปรแกรมประยุกต์ และอาจจะเป็นเป้าหมายการโจมตีของผู้บุกรุกได้โดยตรง เช่นโปรแกรม Snort รุ่น 1.6.x จนถึง 2.0beta เนื่องจากมีจุดอ่อนที่เป็นช่องทางให้ผู้บุกรุกโจมตีระบบ และเมื่อผู้บุกรุกสามารถทำการบุกรุกสำเร็จจะได้รับสิทธิ์ของผู้ดูแลระบบ [CA-2003-13, 2003] นอกจากนี้โปรแกรมตรวจจับการบุกรุกส่วนใหญ่ไม่มีการป้องกันตัวเองจากการถูกโจมตี ดังนั้นผู้บุกรุกสามารถกระทำการต่างๆ เพื่อที่จะขัดขวางการทำงานของระบบตรวจจับการบุกรุกได้ เนื่องจากระบบตรวจจับการบุกรุกส่วนใหญ่ถูกเรียกใช้งานโดย root ซึ่งมีสิทธิ์สูงสุดในระบบ ถ้าหากผู้บุกรุกสามารถโจมตีโปรแกรมเป้าหมายสำเร็จแล้วผู้บุกรุกจะได้รับสิทธิ์ของ root เพื่อควบคุมระบบ

ดังนั้นวิทยานิพนธ์ชุดนี้จึงเสนอว่า การตรวจจับการบุกรุกควรเป็นส่วนหนึ่งของระบบปฏิบัติการเช่นเดียวกับฟังก์ชันเกี่ยวกับการจัดสรรทรัพยากร ฟังก์ชันการจัดการโปรเซส หรือฟังก์ชันอื่นๆ ของระบบปฏิบัติการ แต่อย่างไรก็ตามการแก้ไขดัดแปลงระบบปฏิบัติการต้องกระทำด้วยความระมัดระวัง มีการตรวจสอบถึงผลที่จะตามมาภายหลังอย่างถี่ถ้วน และไม่ทำให้ประสิทธิภาพของระบบปฏิบัติการลดลงมากนัก วิทยานิพนธ์ชุดนี้ได้เสนอวิธีการเพิ่มความสามารถของระบบของระบบปฏิบัติการโดยเพิ่มขั้นตอนการตรวจจับการบุกรุกลงในฟังก์ชันของระบบปฏิบัติการที่เป็นระบบปฏิบัติการแบบเปิดซึ่งเปิดเผยสถาปัตยกรรม ขั้นตอนวิธี และรหัสต้นฉบับ (source

code) เช่น ระบบปฏิบัติการเน็ทบีเอสดี ระบบปฏิบัติการลินุกซ์ (Linux) เป็นต้น

ก่อนที่จะแก้ไขระบบปฏิบัติการ ข้าพเจ้าได้ศึกษาและพัฒนาโปรแกรมตรวจจับการบุกรุกตามแนวคิดของ Nuansri [Nuansri , 1999] ซึ่งเสนอแนวทางในการตรวจจับการบุกรุกด้วยวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซส เมื่อพัฒนาโปรแกรมตรวจจับการบุกรุกและทดสอบได้ว่าการตรวจจับการบุกรุกตามแนวคิดดังกล่าวได้ผลลัพธ์ที่ถูกต้อง ผลที่ตามมาด้วยคือฟังก์ชันของระบบปฏิบัติการที่ควรจะได้รับการแก้ไขเพื่อเพิ่มกลไกการตรวจจับการบุกรุก จากนั้นจึงทำการแก้ไขฟังก์ชันเหล่านั้นแล้วทดสอบประสิทธิภาพของระบบระบบปฏิบัติการชุดใหม่ทั้งความแม่นยำในการตรวจจับการบุกรุกและความคงทนของระบบโดยรวม ทดสอบหาผลกระทบของการเพิ่มกลไกการตรวจจับการบุกรุกที่อาจจะมีผลต่อชุดคำสั่งของระบบปฏิบัติการ และท้ายที่สุดเปรียบเทียบประสิทธิภาพของระบบปฏิบัติการเดิมกับระบบที่แก้ไขใหม่โดยวัดเวลาการทำงานผลต่างของเวลาที่เกิดขึ้นควรอยู่ในระดับที่ยอมรับได้

1.2 การตรวจเอกสาร

งานวิจัยที่สำคัญและเป็นรากฐานของการศึกษาและพัฒนาระบบตรวจจับการบุกรุกเสนอโดย Anderson [Anderson, 1980] เรื่อง “Computer Security Threat Monitoring and Surveillance” โดยเสนอแนวความคิดพื้นฐานว่าพฤติกรรมปกติของผู้ใช้สามารถอธิบายได้โดยวิเคราะห์กิจกรรมต่างๆ ในล็อกไฟล์และการบุกรุกระบบคอมพิวเตอร์สามารถตรวจจับได้โดยการใช้ข้อมูลที่ได้มาจากลักษณะของพฤติกรรมทั่วไป ในลำดับถัดมาได้มีการศึกษาและพัฒนาระบบตรวจจับการบุกรุกเพิ่มขึ้นและเสนอแนวคิดอื่นๆ เพื่อใช้สำหรับการตรวจจับการบุกรุก เช่น การวิเคราะห์เชิงสถิติ การวิเคราะห์รูปแบบของกิจกรรม การวิเคราะห์การเปลี่ยนแปลงสถานะ ระบบผู้ชำนาญการ และโครงข่ายประสาทเทียม เป็นต้น ตัวอย่างระบบตรวจจับการบุกรุก เช่น

- กระประยุกต์ระบบผู้ชำนาญการ (expert system) เพื่อใช้สำหรับการตรวจจับการบุกรุกโดยแทนกิจกรรมของระบบปฏิบัติการด้วยโครงสร้างข้อมูลแบบต้นไม้ (tree data structure) และพิจารณาเหตุการณ์ที่เกิดขึ้นด้วยระบบผู้ชำนาญการและการค้นหาข้อมูลแบบ heuristic โดยหาผลเฉลยที่เหมาะสมที่สุด เพื่อตัดสินว่ากิจกรรมที่กำลังตรวจสอบเป็นการบุกรุกระบบหรือไม่ เช่น งานวิจัยของ Reichelt [Reichelt, 1992]

- การประยุกต์โครงข่ายประสาทเทียม (neuron network) สำหรับการพัฒนาระบบตรวจจับการบุกรุก มีรูปแบบการดำเนินการคล้ายคลึงกับระบบผู้ชำนาญการ แต่เปลี่ยนกระบวนการพิจารณากิจกรรมของระบบปฏิบัติการโดยนำรูปแบบของการโจมตีระบบมาสอน (train) ให้แก่สถาปัตยกรรมโครงข่ายประสาทเทียม เพื่อให้เป็นฐานความรู้สำหรับการตรวจสอบกิจกรรมที่เกิดขึ้นใหม่ เช่น ระบบตรวจจับการบุกรุกชื่อ Shukla [Tan, 1995]
- วิธีการวิเคราะห์การเปลี่ยนแปลงสถานะ (state transition analysis technique) เป็นการแทนกิจกรรมของระบบปฏิบัติการด้วยสถานะหลังจากนั้นติดตามการเปลี่ยนแปลงสถานะ ตัวอย่างการประยุกกต์ใช้วิธีการนี้ได้แก่ Ilgun [Ilgun, 1992] ได้ให้สมติฐานไว้ว่า การบุกรุกบนระบบปฏิบัติการยูนิกซ์สามารถแทนให้อยู่ในรูปแบบของสถานะได้ เนื่องจากการบุกรุกระบบนั้นเป็นการเรียกใช้คำสั่งของระบบปฏิบัติการเพื่อดำเนินการต่างๆ ให้การบุกรุกประสบความสำเร็จ เมื่อนำรูปแบบการบุกรุกที่เกิดขึ้นในอดีตมาแทนให้อยู่ในรูปแบบของสถานะ และคอยตรวจสอบกิจกรรมที่เกิดขึ้นว่าตรงกับรูปแบบที่เคยเก็บไว้หรือไม่ หากตรงกันถือว่ากิจกรรมนั้นเป็นการบุกรุกระบบ

1.3 วัตถุประสงค์ของวิทยานิพนธ์

เพื่อเพิ่มสมรรถนะทางด้านความปลอดภัยให้เกิดระบบปฏิบัติการเน็ทบีเอสดีโดยเพิ่มส่วนของการตรวจสอบการบุกรุกในฟังก์ชันของระบบปฏิบัติการ

1.4 ขอบเขตและวิธีดำเนินการการทำวิทยานิพนธ์

วิทยานิพนธ์ชุดนี้แบ่งการทำงานออกเป็นสามส่วนคือ การออกแบบและพัฒนาโปรแกรมตรวจจับการบุกรุก การปรับปรุงระบบปฏิบัติการด้วยกระบวนการตรวจจับการบุกรุกและการทดสอบประสิทธิภาพของระบบปฏิบัติการที่ได้รับการปรับปรุง ดังมีรายละเอียดในหัวข้อที่ 1.2.1, 1.2.2 และ 1.2.3 ตามลำดับ

1.4.1 การออกแบบและพัฒนาโปรแกรมตรวจจับการบุกรุก

ศึกษา ออกแบบและพัฒนาวิธีการตรวจจับการบุกรุกในระดับโปรแกรมประยุกต์ตามวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะโดยติดตามและวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซสในระบบปฏิบัติการซึ่งเสนอโดย Nuansri [Nuansri, 1999] เพื่อหาวิธีการพัฒนากลไกการตรวจจับการบุกรุก และฟังก์ชันของระบบปฏิบัติการที่ควรจะได้รับการแก้ไขต่อไป

1.4.2 การปรับปรุงระบบปฏิบัติการด้วยกลไกการตรวจจับการบุกรุก

แก้ไขฟังก์ชันของระบบปฏิบัติการยูนิกซ์ โดยเพิ่มกลไกการตรวจจับการบุกรุกไว้ในฟังก์ชันเหล่านั้นพร้อมทั้งทดสอบความแม่นยำและความคงทนของกลไกการตรวจจับการบุกรุกในระดับระบบปฏิบัติการ

1.4.3 การทดสอบประสิทธิภาพของระบบปฏิบัติการที่ได้รับการแก้ไข

หลังจากที่แก้ไขระบบปฏิบัติการตามวิธีการที่กล่าวมาข้างต้นแล้ว การแก้ไขดังกล่าวอาจจะก่อให้เกิดผลกระทบต่อการทำงานระบบปฏิบัติการ เช่น ผลกระทบต่อชุดคำสั่งของระบบปฏิบัติการ เวลาในการประมวลผลของระบบปฏิบัติการอาจจะเพิ่มขึ้น แต่อย่างไรก็ตามเวลาที่แตกต่างนั้นควรอยู่ในระดับที่ยอมรับได้

1.5 ขั้นตอนและระยะเวลาการดำเนินการ

1.5.1 ขั้นตอนการดำเนินการ

เพื่อให้กระบวนการทำวิทยานิพนธ์สำเร็จลุล่วงและบรรลุตามวัตถุประสงค์และขอบเขตดังกล่าว จึงดำเนินการทำวิทยานิพนธ์ตามขั้นตอนต่างๆ ดังต่อไปนี้

1. ศึกษาและค้นคว้าเอกสารที่เกี่ยวข้อง โดยแบ่งหมวดหมู่ของการศึกษาออกเป็นหัวข้อดังนี้
   1.1. **รูปแบบการบุกรุกระบบ** ศึกษาถึงรูปแบบ วิธีการและผลกระทบที่เกิดจากการบุกรุกระบบที่เกิดขึ้นในอดีต รวมถึงวิธีการจัดจำแนกอนุกรมวิธาน (taxonomy) ของการบุกรุก เพื่อออกแบบและพัฒนาวิธีการตรวจจับการบุกรุกในระดับของระบบปฏิบัติการ

1.2. **วิธีการตรวจจับการบุกรุก** ศึกษาถึงวิธีการตรวจจับการบุกรุกต่างๆ หลังจากนั้นเลือกวิธีการที่เหมาะสมในการพัฒนาระบบการตรวจจับการบุกรุกในระดับปฏิบัติการ (ผลการศึกษาจะกล่าวถึงในหัวข้อที่ 2.4.3)

1.3. **ระบบปฏิบัติการยูนิกซ์** ศึกษาถึงสถาปัตยกรรมของระบบ การทำงานของโปรแกรมต่างๆ ของระบบปฏิบัติการเพื่อหาแนวทางการแก้ไขและปรับปรุงฟังก์ชันของระบบปฏิบัติการให้สามารถตรวจจับการบุกรุกได้

2. วิเคราะห์และออกแบบโปรแกรมตรวจจับการบุกรุกเพื่อหาแนวคิดและวิธีการแก้ไขระบบปฏิบัติการ โดยทดสอบแนวคิดดังกล่าวในระดับของโปรแกรมประยุกต์ ซึ่งแบ่งการดำเนินงานออกเป็นส่วนๆ ดังนี้
   2.1. ศึกษาและวิเคราะห์วิธีการตรวจจับการบุกรุกตามวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซส
   2.2. ออกแบบและพัฒนาโปรแกรมตรวจจับการบุกรุก
   2.3. ทดสอบความแม่นยำของโปรแกรมตรวจจับการบุกรุก
   2.4. ทดสอบหาผลกระทบที่เกิดขึ้นจากโปรแกรมตรวจจับการบุกรุกที่มีผลต่อชุดคำสั่งของระบบ

3. แก้ไขระบบปฏิบัติการ โดยเพิ่มขั้นตอนการตรวจจับการบุกรุกลงในฟังก์ชันระบบปฏิบัติการตามแนวคิดที่ได้จากการศึกษา วิเคราะห์และพัฒนาวิธีการตรวจจับการบุกรุก

4. การทดสอบระบบงาน เมื่อแก้ไขระบบปฏิบัติการแล้วจึงทดสอบระบบปฏิบัติการตามประเด็นต่างๆ ดังต่อไปนี้
   4.1. ทดสอบความแม่นยำของการตรวจจับการบุกรุกของระบบปฏิบัติการ
   4.2. ศึกษาและแก้ไขผลกระทบที่เกิดขึ้นเมื่อแก้ไขระบบปฏิบัติการ
   4.3. ทดสอบประสิทธิภาพของระบบปฏิบัติการหลังจากที่ได้รับการแก้ไขแล้ว

5. จัดทำเอกสารรายงานผลการทำวิทยานิพนธ์

1.5.2 ระยะเวลาการดำเนินการ

กรกฎาคม 2547 – มีนาคม 2549

ขั้นตอน	2547						2548												2549		
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
1																					
2																					
3																					
4																					
5																					

1.6 สถานที่และเครื่องมือที่ใช้ในวิทยานิพนธ์

สถานที่

ห้องปฏิบัติการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่

เครื่องมือที่ใช้

<u>ด้านฮาร์ดแวร์</u>

- เครื่องคอมพิวเตอร์ส่วนบุคคล ความเร็ว 1.5 กิกะเฮิร์ซ หน่วยความจำ 256 เมกะไบต์ ฮาร์ดดิสก์ความจุ 40 กิกะไบต์ จำนวน 2 ชุด เพื่อใช้สำหรับพัฒนาและทดสอบระบบ

<u>ด้านซอฟต์แวร์</u>

- ระบบปฏิบัติการยูนิกซ์ NetBSD 3.0
- ระบบปฏิบัติการ Microsoft Window XP Professional

1.7 ประโยชน์ที่คาดว่าจะได้รับ

ระบบปฏิบัติการยูนิกซ์ที่เพิ่มประสิทธิภาพให้มีความสามารถในการตรวจจับและการป้องกันการบุกรุก ในขณะที่ประสิทธิภาพของระบบปฏิบัติการไม่เปลี่ยนแปลงหรือเปลี่ยนแปลงในระดับที่ยอมรับได้