ชื่อวิทยานิพนธ์ การเพิ่มสมรรถนะระบบปฏิบัติการด้วยฟังก์ชันการตรวจจับและการป้องกันการบุกรุกบนระบบปฏิบัติการเน็ทบีเอสดี

ผู้เขียน นายชัยยุทธ จันแดง

สาขาวิชา วิทยาการคอมพิวเตอร์

ปีการศึกษา 2548

บทคัดย่อ

วิทยานิพนธ์นี้เป็นการเสนอแนวคิดของการเพิ่มสมรรถนะทางด้านความปลอดภัยแก่ระบบปฏิบัติการ โดยทดสอบแนวคิดบนระบบปฏิบัติการเน็ทบีเอสดี สำหรับวิธีการเพิ่มสมรรถนะแก่ระบบปฏิบัติการเป็นการนำวิธีการตรวจจับการบุกรุกมาพัฒนาในระดับระบบปฏิบัติการ โดยเลือกการตรวจจับการบุกรุกด้วยวิธีการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซสมาพิจารณากิจกรรมของโปรเซส เนื่องจากการแก้ไขระบบปฏิบัติการเป็นเรื่องที่ละเอียดอ่อนจึงจำเป็นต้องทดสอบวิธีการตรวจจับการบุกรุกโดยการพัฒนาโปรแกรมตรวจจับการบุกรุกเพื่อทดสอบแนวคิด หาขั้นตอนวิธีและฟังก์ชันที่จำเป็นต้องได้รับการแก้ไข ต่อมานำขั้นตอนวิธีที่ได้ไปแก้ไขฟังก์ชันของระบบปฏิบัติการ หลังจากนั้นทดสอบประสิทธิภาพของกลไกการตรวจจับการบุกรุกทางด้านความแม่นยำและความคงทนในการทำงาน อีกทั้งทดสอบเพื่อหาผลกระทบของกลไกการตรวจจับการบุกรุกที่มีผลต่อคำสั่งของระบบปฏิบัติการ ท้ายที่สุดเมื่อแก้ไขระบบปฏิบัติการแล้ว ประสิทธิภาพการทำงานของระบบปฏิบัติอาจจะเปลี่ยนแปลงไป และลดลงไม่เกินร้อยละ 5

Thesis Title	Operating System Enhancement with Intrusion Detection and Prevention Functionality Based on NetBSD System
Author	Mr. Chaiyut Jundang
Major Program	Computer Science
Academic Year	2005

ABSTRACT

This thesis proposes an concept for a operating system security enhancement based on the NetBSD system. This concept implements an intrusion detection approach named Process State Transition Analysis Technique (Nuansri, 1999) in the kernel level. As modifying the kernel is complicated, we must test the approach in the application level for obtaining the algorithm and discovering the system functions that have to be modified. After the system function is modified, the performance of the intrusion detection mechanism is tested for both accuracy and robustness, and to verify the covert operation of system commands. Finally, we test the performance of the operating system, with the result being only 5% lower than the original operating system.