ชื่อวิทยานิพนธ์	การจัดทำโปรแกรมตรวจจับการบุกรุกบนระบบปฏิบัติการยูนิกซ์
ผู้เขียน	นางสาวพัฒนาวดี ศิวดิณฑุโก
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
ปีการศึกษา	2547

บทคัดย่อ

วิทยานิพนธ์นี้เสนอการพัฒนาเครื่องมือช่วยในการตรวจจับการบุกรุกบนระบบปฏิบัติการยูนิกซ์ ซึ่งใช้หลักการของการติดตามการทำงานของโปรเซสโดยการเรียกใช้ system call และการวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซสร่วมกับกฎที่ใช้สนับสนุนการตรวจจับการบุกรุก ตัวระบบประกอบด้วย 3 ส่วนได้แก่ การติดตามการทำงานของโปรเซส (process monitoring module) การวิเคราะห์การเปลี่ยนแปลงสถานะของโปรเซส (state transition analysis module) และการตรวจจับการบุกรุก (detection module) โดยที่ในส่วนของการติดตามการทำงานของโปรเซสนั้นจะติดตามการเรียกใช้ system call และสถานะของโปรเซสในขณะนั้น ข้อมูลจากส่วนนี้จะถูกส่งไปยังส่วนที่สองคือการวิเคราะห์การเปลี่ยนแปลงสถานะหากตัวระบบพบว่าในขณะนั้นสถานะที่เกิดขึ้นเป็นสถานะที่ต้องห้ามสำหรับผู้ใช้โดยทั่วไปขั้นตอนของการตรวจจับการบุกรุกจะถูกเรียกใช้ นอกจากความสามารถในการตรวจจับการบุกรุกได้ตามวัตถุประสงค์หลักแล้วเทคนิคในการตรวจจับการบุกรุกที่เลือกใช้สำหรับวิทยานิพนธ์นี้ยังช่วยลดผลกระทบที่สำคัญของระบบตรวจจับการบุกรุกในเรื่องของการตัดสินผิดทางบวกอีกด้วย

Thesis Title	Implementation of an Approach to Intrusion Detection on Unix Hosts
Author	Miss Pattanawadee Siwatintuko
Major Program	Computer Engineering
Academic Year	2004

Abstract

This thesis presents an intrusion detection system tool on Unix hosts implemented using system call tracing and a state transition analysis technique. The system consists of three modules, process monitoring, state transition analysis, and detecting module. The process monitoring module monitors system call usage and the user credentials of processes. The state transition technique takes its input from the monitoring module to analyze and define process state at a particular time. If the underlying process changes its state into a forbidden state, then it is flagged as a suspicious activity and the detection module is called. This technique also decreases false positives.