ชื่อวิทยานิพนธ์ ต้นแบบระบบตรวจจับการบุกรุกแบบผสมโดยใช้วิธีการทำเหมืองข้อมูลส่วนคำสั่งที่เรียกใช้บริการของระบบปฏิบัติการ

ผู้เขียน นายคุณชิต สุขพัฒนศรีกุล

สาขาวิชา วิทยาการคอมพิวเตอร์

ปีการศึกษา 2548

บทคัดย่อ

วิทยานิพนธ์นี้เสนอการพัฒนาต้นแบบของเครื่องมือช่วยในการตรวจจับการบุก-รุกบนระบบปฏิบัติการลินุกซ์เรดแฮ็ท โดยใช้วิธีการตรวจจับการบุกรุกแบบการตรวจจับความผิดปกติ (anomaly detection) และการใช้งานที่ไม่ถูกต้อง (misuse detection) ร่วมกัน และใช้เทคนิคการแยกประเภท (classification) ของการทำเหมืองข้อมูล (data mining) เพื่อแยกประเภทการทำงานของโปรเซสด้วยความถี่ของการเรียกใช้ส่วนคำสั่งที่เรียกใช้บริการของระบบปฏิบัติการ (system call) ตัวระบบประกอบด้วยกระบวนการทำงานหลัก 2 ส่วนคือ การติดตามการทำงานของเชลล์ผู้ใช้ และการตรวจสอบความปลอดภัย โดยเมื่อมีโปรเซสเกิดขึ้นจะมีการสร้างแฟ้มข้อมูลเพื่อติดตามและบันทึกการทำงานของโปรเซสนั้นไว้ และในส่วนของการตรวจสอบความปลอดภัยทำการตรวจสอบการทำงานของโปรเซสเพื่อหาว่าเป็นการบุกรุกระบบหรือไม่โดยใช้ข้อมูลจากแฟ้มข้อมูลนั้นมาพิจารณานับความถี่ของการเรียกใช้ system call แล้วแยกประเภทคลาสการทำงาน หากการทำงานที่เกิดจากโปรเซสนั้นทำให้การแยกประเภทได้คลาสการทำงานที่ “ผิดปกติ (abnormal)” ก็ถือว่าเป็นการบุกรุกระบบ

Thesis Title	A Prototype of a Hybrid Intrusion Detection System based on System Calls Mining Technique
Author	Mr.Kunnachit Sukpatthanasikun
Major Program	Computer Science
Academic Year	2005

ABSTRACT

This thesis proposes the development of an instrument model to detect intrusion into RedHat Linux versions 6.1, 7.0 and 9.0. The model uses a combination of anomaly and misuse detection methods, with data mining classification technique to classify system calls usages. There are two main modules : the tracing shell and the safety check. The tracing shell will track user's shells. When a process is created, a new file is also created to record all of process activities. This file is examined regardless whether there is a threat to the system. The safety check counts frequencies and classifies the types of activities base on frequency of system call usage. If a process execution is classified as abnormal, a threat to the system can be suspected. The intrusion detection system developed satisfies the goals of thesis research.