หัวข้อการค้นคว้าแบบอิสระ ระบบวิเคราะห์การบุกรุกเครือข่ายของข้อมูลจราจรทางคอมพิวเตอร์โดยใช้ทฤษฎีต้นไม้การตัดสินใจ

ผู้เขียน นายศักดิ์นริน อินทะจักร์

ปริญญา วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

บทคัดย่อ

งานวิจัยนี้เกี่ยวของกับระบบเครือข่ายคอมพิวเตอร์โดยเริ่มมาจากกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ที่ต้องให้ทุกหน่วยงานเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อเป็นหลักฐานในการใช้งานเครือข่าย งานวิจัยนี้นำการเก็บข้อมูลจราจรทางคอมพิวเตอร์มาใช้ให้เป็นประโยชน์เพิ่มขึ้นโดยการนำข้อมูลมาวิเคราะห์เพื่อหาผู้บุกรุกและภัยคุกคามที่เกิดขึ้นในระบบด้วยทฤษฎีต้นไม้การตัดสินใจ

โดยระบบจะเริ่มจากการนำข้อมูลจราจรทางคอมพิวเตอร์สำหรับการเรียนรู้มาเพื่อเป็นต้นแบบในการวิเคราะห์โดยทฤษฎีต้นไม้การตัดสินใจ สร้างต้นไม้การตัดสินใจขึ้นมาแล้วเมื่ออุปกรณ์ส่งข้อมูลจราจรเข้ามาในระบบจะทำการตรวจสอบว่าเป็นผู้บุกรุกหรือภัยคุกคามหรือไม่ แล้วถ้าพบว่าเป็นผู้บุกรุกจะทำการเก็บไว้เป็นข้อมูลในการสร้างต้นไม้การตัดสินใจ และจะทำการเก็บข้อมูลเรียนรู้ไปเรื่อย ๆ ระบบมีการตรวจสอบที่เร็วขึ้นและคาดเดาว่าเป็นผู้บุกรุกหรือภัยคุกคามได้ดีขึ้นเรื่อยๆ ตามข้อมูลที่อุปกรณ์ส่งเข้ามา

ผลของการดำเนินการวิจัยเป็นไปตามวัตถุประสงค์ และขอบเขตงานวิจัย และจากผลการทดสอบสรุปเป็นกราฟแล้วจะเห็นได้ว่าเมื่อระบบมีการเรียนรู้เพิ่มเติมและปรับโหนดของต้นไม้การตัดสินใจแล้วจะใช้เวลาในการหาผู้บุกรุกหรือภัยคุกคามน้อยลง ทำให้มีประสิทธิภาพที่ดีขึ้น

Independent Study Title	Network Intrusion Analysis System of Computer Traffic Data Using Decision Tree Theory
Author	Mr. Saknarin Intajak
Degree	Master of Science (Computer Science)
Advisor	Assoc. Prof. Dr. Ekkarat Boonchieng

ABSTRACT

This independent study was about computer network systems related to the laws regarding computer-related crime. All sectors collected computer traffic data as evidence for network usability. This independent study made use of computer traffic data by analyzing data to search for the intruders and threats occurring in the system by using decision tree.

Computer traffic data for learning was used as the model which was analyzed by the decision tree. Then, the decision tree was built. When the equipment transferred traffic data into the system, it determind if the data were intruders or threats. If intruders were found, the system kept data for building the decision tree and learning data were continually collected. The system had faster verification and better prediction of intruders and threats according to the data sent by the equipment.

The results of the study were consistent with the objectives and scope of the research. The results were summarized into a graph. It was found that when the system had additional learning and the node of the decision tree was adjusted, less time was taken to detect intruders or threats along with increasing efficiency.