บทคัดย่อ

งานวิจัยนี้ได้ทำการประเมินประสิทธิภาพระบบตรวจจับการบุกรุกบนอุปกรณ์ฝังตัวสำหรับรักษาความปลอดภัยทางไซเบอร์ โดยเน้นไปทางการตรวจการโจมตีแบบการปฏิเสธการให้บริการที่มุ่งทำลายเครื่องแม่ข่ายที่เปิดให้บริการกับผู้ใช้ ซึ่งจะเป็นผลกระทบอย่างรุนแรงของผู้ประกอบการ โดยได้นำระบบตรวจจับการบุกรุกมาติดตั้งอุปกรณ์ฝังตัวคือราสเบอรรี่ ไพ และได้นำมาทดสอบประสิทธิภาพการบุกรุกในส่วนของการโจทตีผ่านเครือข่ายสาย และไร้สาย เพื่อวิเคราะห์หาประสิทธิภาพการป้องกันการบุกรุกผ่านโปรโตตคอล 3 ชนิดอันได้แก่ TCP UDP และ ICMP ซึ่งจากผลการวิจัยในครั้งนี้พบว่าระบบตรวจจับการบุกรุกเครือข่ายที่ติดตั้งอยู่บนอุปกรณ์ฝังตัวขนาดเล็กสามารถตรวจจับการบุกรุกโดยมีประสิทธิภาพใกล้เคียงกับการติดตั้งบนเครื่องคอมพิวเตอร์ ซึ่งทำให้สามารถลดค่าใช้จ่ายในการนำไปติดตั้งใช้งานจริงกับหน่วยงานที่มีขนาดเล็ก

ABSTRACT

This research has evaluated the intrusion detection system performance on embedded security devices. It focuses on denial of service attacks aimed at destroying servers that are available to users. This will be a serious impact of the operator. The intrusion detection system was installed in Raspberry Pi ,it was tested for intrusion detection through the wireless and wire network to analyze the intrusion prevention performance. There are three types of protocols: TCP, UDP and ICMP. The results of this research show that network intrusion detection systems installed on small embedded devices can detect intrusion effectively as close to the installation on the computer. This makes it possible to reduce the cost of deploying to real-world applications with small enterprise.