ทรงฤทธิ์ ศรีลาศักดิ์ 2552: ระบบตรวจจับและตอบโต้การติดตั้งแอกเซสพอยต์โดยไม่ได้รับอนุญาต ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: รองศาสตราจารย์อนันต์ ผลเพิ่ม, Ph.D. 85 หน้า

โดยทั่วไปพนักงานในองค์กรสามารถเข้าถึงเครื่องแม่ข่ายภายในองค์กรผ่านทางเครือข่ายแลนมีสาย ซึ่งไม่ได้รับความสะดวกเท่ากับการใช้งานผ่านเครือข่ายแลนไร้สาย ได้ไม่สะดวกนัก เนื่องจากหน่วยงานจะมีการกำหนดนโยบายด้านความปลอดภัยซึ่งเป็นสาเหตุหนึ่งที่ทำให้พนักงานมีการนำแอกเซสพอยต์มาติดตั้งในองค์กรโดยไม่ได้แจ้งให้แก่ผู้ดูแลเครือข่ายทราบ ซึ่งส่วนใหญ่ไม่ได้มีการตั้งค่าที่มีความปลอดภัยที่เหมาะสม และ ส่งผลให้เป็นช่องทางให้เกิดการบุกรุก หรือ ดักจับข้อมูลภายในองค์กรได้ นอกจากนี้ยังอาจมีการติดตั้งแอกเซสพอยต์จากผู้บุกรุกภายนอกโดยไม่เชื่อมต่อกับเครือข่ายองค์กร

งานวิจัยนี้เสนอระบบที่มีความสามารถแก้ปัญหาที่เกิดจากแอกเซสพอยต์ที่ติดตั้งโดยไม่ได้รับอนุญาตด้วยการรายการตรวจจับ และ ระงับการเชื่อมต่อแบบอัตโนมัติ ระบบนี้ได้รับการออกแบบให้ทำงานแบบรวมศูนย์ โดยใช้แอกเซสพอยต์ขององค์กรที่มีอยู่ทำหน้าที่ดักจับข้อมูลที่แพร่กระจายในอากาศ ที่มีรูปแบบการสื่อสารตามมาตรฐาน IEEE 802.11 เมื่อแอกเซสพอยต์ได้รับข้อมูลในอากาศจะทำการส่งข้อมูลกลับไปที่เครื่องแม่ข่ายเพื่อทำหน้าที่วิเคราะห์โดยเปรียบเทียบกับฐานข้อมูลแอกเซสพอยต์องค์กร หากพบข้อมูลที่แตกต่างจากฐานข้อมูล ระบบจะทำการส่งคำสั่งควบคุมสวิตช์เพื่อระงับการเชื่อมต่อ จากการทดลอง โดยมีการติดตั้งแอกเซสพอยต์ที่ไม่ได้รับอนุญาตทั้งหมด 4 ประเภททั้งแบบติดตั้งภายในและภายนอกองค์กร เพื่อทดสอบความสามารถในการตรวจจับ พบว่าระบบนี้สามารถตรวจจับแอกเซสพอยต์ได้อย่างถูกต้องในทุกการทดลอง และ มีความสามารถระงับการเชื่อมต่อได้ในแบบอัตโนมัติหากแอกเซสพอยต์นั้นเชื่อมกับเครือข่ายภายในองค์กร

Songrit Srilasak 2009: Rogue Access Point Detection and Counterattack System. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Anan Phonphoem, Ph.D. 85 pages.

Normally a user can access an internal server via wireless LAN with some restriction due to the organization security policy. The user may intentionally install an unregistered access point without administrative awareness for his or her convenient which causes backdoors for eavesdrop or attack from the intruders. The rouge access point may also be installed by the intruder himself without connected to the organization's network.

In this thesis, the rouge access point detection and counterattack system has been proposed. The system is designed as a centralize control by utilizing the existing registered access points to capture the broadcasting data, e.g. the identity of the access point, according to the IEEE802.11 standard. The captured data is then sent to the central server for analysis. If the received data does not match with the registered access point, the system sends control commands to the edge switch for shutting down the port that the unregistered access point is connected to. From the experiment, 4 types of unauthorized access point, both inside and outside the organization, can be correctly detected while the system is able to automatically block the internal rouge access point.