มหคม อร่ามเสรีวงศ์ : การออกแบบและพัฒนาระบบป้องกันการบุกรุกเครือข่ายโดยอัตโนมัติโดยใช้เครือข่ายแอ็กทีฟ เพื่อรับมือกับการโจมตีจากเครือข่ายภายในที่ถูกผู้บุกรุกยึดครอง. (A DESIGN AND DEVELOPMENT OF AN AUTOMATIC NETWORK-INTRUSION DEFENSE SYSTEM USING ACTIVE NETWORK FOR HANDLING ATTACKS FROM COMPROMISED INTERNAL NETWORKS) อ. ที่ปรึกษา : อ.ดร.เฉลิมเอก อินทนากรวิวัฒน์, 151 หน้า. ISBN 974-53-2529-5.

วิทยานิพนธ์ฉบับนี้ได้พัฒนาระบบป้องกันการบุกรุกเครือข่าย ที่มีอุปกรณ์ป้องกันการบุกรุกเครือข่ายหลายตัวทำงานร่วมกันโดยใช้เครือข่ายแอ็กทีฟในการพัฒนา ทำให้สามารถปรับเปลี่ยนโปรแกรมควบคุมการทำงานของอุปกรณ์ได้ตลอดเวลา ระบบนี้มีความสามารถในการตรวจสอบ ค้นหาที่มา และหยุดการบุกรุกให้อยู่เฉพาะในเครือข่ายย่อยได้ งานวิจัยนี้ยังได้นำเสนอวิธีตรวจสอบการบุกรุกแบบกระจาย โดยที่อุปกรณ์หลายตัวจะช่วยกันตรวจสอบการบุกรุก เป็นการกระจายภาระในการตรวจสอบ อีกทั้งอุปกรณ์แต่ละตัวไม่ต้องตรวจสอบการบุกรุกทุกรูปแบบที่มีอยู่ แต่ตรวจสอบเฉพาะการบุกรุกที่มุ่งโจมตีเครื่องที่อยู่ในเครือข่ายย่อยที่ดูแลเท่านั้น จากผลการทดสอบพบว่าวิธีการนี้ให้อัตราการส่งผ่านข้อมูลดีขึ้น เมื่อเทียบกับการใช้วิธีตรวจสอบแบบทั่วไป

This thesis presents a network-intrusion prevention system that is a collaboration among multiple intrusion prevention devices. By using Active Networks, a control program can be dynamically loaded into any intrusion prevention devices. This system can detect, traceback, and stop intruders at theirs sub-networks. In addition, we propose "distributed detection" for multiple detectors to co-operate in detecting intrusion and to share the detection load. Each device does not have to detect all intrusion signatures, but only the signatures that are known to be feasible attacks on the host platform in its sub-network. Our experimental results indicate that the throughput of this new detection method is more than that of the general approach.