SECURITY INFORMATION EVENT MANAGEMENT WITH LATENT SEMANTIC ANALYSIS TECHNIQUE FOR THREAT IDENTIFICATION

PAVARIT DAIRINRAM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (COMPUTER SCIENCE) FACULTY OF GRADUATE STUDIES MAHIDOL UNIVERSITY 2014

Copyright by Mahidol University

COPYRIGHT OF MAHIDOL UNIVERSITY

SECURITY INFORMATION EVENT MANAGEMENT WITH LATENT SEMANTIC ANALYSIS TECHNIQUE FOR THREAT IDENTIFICATION

PAVARIT DAIRINRAM 5237679 ITCS/M

M.Sc. (COMPUTER SCIENCE)

THESIS ADVISORY COMMITTEE: DAMRAS WONGSAWANG, Ph.D., VASAKA VISOOTTIVISETH, Ph.D.

ABSTRACT

Security in a heterogeneous and complex network is one of the most significant challenges for administrators. A lot of devices are needed to handle and perform the protection and prevention in order to secure the network resources and assets from the threats, which are growing rapidly. The Security Information and Event Management (SIEM) is the major tool that helps administrators attend to the current situation. It is deployed to manage and identify the threats. Besides these, it is able to initiate the actions for protection and prevention of the network and also generate a report, which is conforms to the security standard. On the other hand, the amount of data from devices is significantly large, and the variation of threats is also a major concern for identifying them. To mitigate these problems, Latent Semantic Analysis (LSA) was proposed in this research. LSA is one of the most powerful tools that can provide efficiency in the exact matching, commonly used in information retrieval. LSA improves its performance by reducing the amount of unnecessary data generated from network devices. Additionally, it can be used to identify a similar threat pattern from the similarity between events and threats. The experiments showed that the LSA approach could help improve the threat identifying process by eliminating an amount of unnecessary data without a degradation in accuracy.

KEY WORDS: SECURITY INFORMATION EVENT MANAGEMENT / LATENT SEMANTIC ANALYSIS / THREAT IDENTIFICATION / NETWORK SECURITY

89 pages

Copyright© by Mahidol University

การจัดการสารสนเทศและเหตุการณ์ของความมั่นคงด้วยเทคนิคการวิเคราะห์ความหมายแฝง สำหรับการระบุภาวะคุกคาม

SECURITY INFORMATION EVENT MANAGEMENT WITH LATENT SEMANTIC ANALYSIS TECHNIQUE FOR THREAT IDENTIFICATION

ปวริศ ด้ายรินรัมย์ 5237679 ITCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์ : ดำรัส วงศ์สว่าง, Ph.D., วัสกา วิสุทธิวิเศษ, Ph.D.

บทคัดย่อ

ระบบความมั่นคงในระบบเครือข่ายที่มีความหลากหลาย และ สลับซับซ้อนถือเป็นอุปสรรค์สำหรับ ผู้ดูแลระบบในการรักษาความมั่นคงต่อ ระบบเครือข่ายและ สินทรัพย์ภายในระบบเครือข่าย ผู้ดูแลระบบต้องทำการบริหารจัดการ อุปกรณ์ภายในเครือข่ายให้มีความสามารถป้องกันและป้องปรามจากภาวะคุกคามต่าง ๆ ที่มีจำนวนมากได้ อุปกรณ์จัดการสารสนเทศและเหตุการณ์ของความมั่นคง หรือ SIEM เป็นอีกอุปกรณ์หนึ่ง ที่อำนวยความสะดวกให้ผู้ดูแลระบบสามารถแก้ไขปัญหา และบริหารจัดการ อีกทั้งช่วยระบุภัยคุกคามที่กำลังโจมตี และเสนอแนะแนวทางการปฏิบัติ พร้อมการดำเนินการป้องกันและป้องปราม หลังจากที่ทำการระบุภัยคุกคามได้อย่างถูกต้อง อีกทั้งสร้างรายงาน ที่อ้างอิงตามมาตรฐานความมั่นคง ต่อผู้ดูแลระบบได้ ทั้งนี้ข้อมูลที่ได้จากอุปกรณ์ต่างๆ ในเครือข่ายนั้นอาจมีขนาดใหญ่ รวมไปถึงการผันแปรของภัยคุกคาม ประเด็นเหล่านี้อาจส่งผลต่อเวลาและความถูกต้องในการระบุภัยคุกคามได้ ดังนั้น การใช้เทคนิคการวิเคราะห์ความหมายแฝง หรือ LSA ได้ถูกนำเสนอในการวิจัยนี้ เพื่อบรรเทาปัญหาข้างต้นลง โดยเทคนิคนี้ช่วยให้ลด จำนวนของข้อมูลที่ไม่จำเป็นออก เพื่อให้การวิเคราะห์นั้นมีประสิทธิภาพที่ดีขึ้น อีกทั้งเทคนิคนี้สามารถวิเคราะห์คล้ายคลึงของภัยคุกคามที่มีความเป็นไปได้จากข้อมูลของภัยคุกคามและข้อมูลเหตุการณ์ที่มีอยู่ในฐานข้อมูล โดยจากการทำลองในการวิจัยนี้พบว่า การใช้เทคนิค LSA ในอุปกรณ์ SIEM นั้นช่วยในการปรับปรุงขั้นตอนการระบุภัยคุกคามโดยการลดจำนวนของข้อมูลที่ไม่จำเป็นออกไป โดยที่การระบุยังคงความแม่นยำ เช่นเดียวกับก่อนการลดจำนวนของข้อมูล

Copyright by Mahidol University

89 หน้า