TRUST MANAGEMENT APPLIED TO LOG ACCESS

KHOMDRAD BOONTAE

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2007

การจัดการความน่าเชื่อถือที่ประยุกต์ใช้กับการเข้าถึงข้อมูลที่บันทึกระบบ
(TRUST MANAGEMENT APPLIED TO LOG ACCESS)

คมเดช บุญแท้ 4537066 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์: สุดสงวน งามสุริยโรจน์, Ph.D., ดำรัส วงศ์สว่าง, Ph.D.

บทคัดย่อ

Log File เป็นเครื่องมือที่ทำหน้าที่ในการบันทึกลำดับเหตุการณ์ต่างๆที่เกิดขึ้นในระบบ ซึ่งข้อมูลใน log เป็นบันทึกที่สำคัญ สามารถนำมาใช้ในการตรวจสอบเหตุการณ์ต่างๆที่เกิดขึ้นแล้วภายในระบบว่ามีความผิดพลาดหรือไม่ และอย่างไรได้ในภายหลัง ปัจจุบัน Log file ของระบบเครือข่ายขนาดใหญ่ จะมีผู้ดูแลระบบหลายคนและสังกัดส่วนงานที่แตกต่างกัน รวมถึงมีหน้าที่และความรับผิดชอบที่แตกต่างกันด้วย ทำให้เกิดปัญหาในเรื่องของสิทธิในการเข้าถึง Log file ของระบบต่างๆว่า ผู้ใดมีสิทธิในการเข้าไปทำการตรวจสอบ Log file ของระบบใดได้บ้าง ซึ่งสิทธิต่างๆเหล่านี้ต้องเป็นไปตามนโยบายความปลอดภัย (Security Policy) ขององค์กร ดังนั้นประเด็นเรื่องสิทธิในการเข้าถึง Log ของระบบงานต่างๆจึงเป็นประเด็นที่จะต้องมีการบริหารจัดการ

ในงานวิจัยนี้เราออกแบบและพัฒนาระบบ Trusted Framework เพื่อการบริหารจัดการสิทธิในการเข้าถึง Log file ใน Distributed Environment โดยระบบ Trusted Framework นี้จะทำงานตามนโยบายความปลอดภัยขององค์กรที่กำหนดไว้ว่าผู้ดูแลระบบงานใดสามารถเข้าถึงข้อมูล Log ของระบบงานใดได้บ้าง และเป็นไปตาม domain ต่างๆ ซึ่งผลการทดลองแสดงให้เห็นว่าระบบ Trusted Framework ที่ได้พัฒนาขึ้น สามารถช่วยบริหารจัดการสิทธิการเข้าถึง Log file ใน 4 สถานการณ์ที่จำลองขึ้นเพื่อการทดสอบได้เป็นอย่างดี

124 หน้า.

TRUST MANAGEMENT APPLIED TO LOG ACCESS

KHOMDRAD BOONTAE 4537066 SCCS/M

M.Sc. (COMPUTER SCIENCE)

THESIS ADVISORS: SUDSANGUAN NGAMSURIYAROJ, Ph.D., DAMRAS WONGSAWANG, Ph.D.

ABSTRACT

The log file is the main instrument for recording all sequential events that have happened in any computer system. It contains the important records that can be used to investigate what abnormal behavior occurred in the past, and how it happened. Currently, log files of enterprise networks have several responsible administrators residing across departments in an organization. They have different roles and responsibilities as well. The security policy of the organization will identify who has the authorization to access which log file of all systems. How the authorization of accessing log files is designed and implemented would be a significant issue, and that would be our research focus.

In this thesis, we designed and implemented a trusted framework for managing log file accesses in a distributed environment. The framework is enforced by the organization's security policy that specifies which administrators can access which log files at what time. The experimental results in the four sample scenarios show that the developed trusted framework would help us manage the log access authorization very well.

KEY WORDS: TRUST MANAGEMENT / CERTIFICATE AUTHORITY / PUBLIC KEY INFRASTRUCTURE / LOG ACCESS /

124 pp.