SECURE ELECTRONIC MAIL

URAIWUN THAIGUN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(COMPUTER SCIENCE)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2001

ISBN 974-04-0369-7

4137864 SCCS/M : MAJOR : COMPUTER SCIENCE ; M.Sc.(COMPUTER SCIENCE)
KEY WORDS : SECURE E-MAIL SYSTEM / AUTHENTICATION MESSAGE AUTHENTICATION / MESSAGE PRIVACY
URAIWUN THAIGUN : SECURE ELECTRONIC MAIL. THESIS ADVISORS: DAMRAS WONGSAWANG, Ph.D., CHOMTIP PORNPANOMCHAI, Ph.D. 103 P. ISBN 974-04-0369-7

Modern technological advancements as well as the availability of networks to use the e-mail is a great help to commercial utilities and communications. E-mail has become a part of everyday life, because it is simple, convenient and fast. The standard method of sending and receiving e-mail over the internet, the one commonly used, has almost no security features built into it and no capability for necessary services. E-mail is susceptible to interception and review by unauthorized or unintended parties at numerous stages of the communication. These can be serious problems causing a decrease in e-mail usage. E-mail encryption is not enough to ensure the security of messages. The system should also ensure that e-mails received are authentic.

This thesis proposed a new model, called the "Secure Electronic Mail" (SEM), to solve security problems with e-mail. The SEM focuses on security of transferring e-mail via any public network. It employs the concept of central security control, which provides a variety of security services to users such as integrity, privacy, authentication, self-destruction, anonymity, non-repudiation, audit, and accounting. The SEM was made up of secured encryption, authentication and other security mechanisms that can be replaced for current development. This approach helps improve the security in the e-mail system. The prototype of SEM was implemented and tested. It proved to be secure against passive attacks. This thesis presented a detailed structure and analysis of SEM. The experimental results were also analysed, discussed and concluded. Finally, future work for further development are suggested.

4137864 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม. (วิทยาการคอมพิวเตอร์)

อุไรวรรณ์ ไทยกรรณ์ : ไปรษณีย์อิเล็กทรอนิกส์ที่มีความปลอดภัย (SECURE ELECTRONIC MAIL). คณะกรรมการควบคุมวิทยานิพนธ์ : ดำรัส วงศ์สว่าง, Ph.D., ชมทิพ พรพนมชัย, Ph.D. 103 หน้า. ISBN 974-04-0369-7

ในปัจจุบันพัฒนาการทางเทคโนโลยีและการที่มีเครือข่ายการสื่อสารใช้อย่างแพร่หลาย ทำให้การใช้จดหมายอิเล็กทรอนิกส์ ถูกนำมาใช้ในเชิงพาณิชย์และในการสื่อสารอย่างกว้างขวาง จนกลายเป็นส่วนหนึ่งในชีวิตประจำวันของคนทั่วไป เพราะใช้งานง่าย สะดวก และรวดเร็ว ระบบการส่งและการรับจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเตอร์เน็ตที่ใช้อยู่นั้น ส่วนใหญ่ยังไม่มีระบบความปลอดภัยและการบริการที่จำเป็น ทำให้มีจุดอ่อนให้ผู้ไม่หวังดีคุกคาม ทั้งในเรื่องการปลอมแปลงจดหมาย การแก้ไขจดหมาย หรือการแอบคัดลอกจดหมาย ซึ่งเป็นสาเหตุหลักที่ทำให้ผู้ใช้ลดความน่าเชื่อถือในการใช้งาน การเข้ารหัสจดหมายอิเล็กทรอนิกส์เพียงอย่างเดียวยังไม่พอที่จะรับรองความปลอดภัยของข้อความ ระบบควรจะทำให้มั่นใจด้วยว่าจดหมายที่ผู้รับได้รับนั้นเป็นของจริง

วิทยานิพนธ์ฉบับนี้ได้เสนอตัวแบบใหม่ เรียกว่า "ไปรษณีย์อิเล็กทรอนิกส์ที่มีความปลอดภัย" (SEM) เพื่อแก้ปัญหาที่อาจเกิดขึ้นกับจดหมายอิเล็กทรอนิกส์ ซึ่งเน้นถึงระบบความปลอดภัยในการส่งจดหมายผ่านเครือข่ายสื่อสารสาธารณะ โดยใช้แนวคิดของการควบคุมระบบความปลอดภัยแบบศูนย์กลาง เพื่อให้บริการความปลอดภัยหลายรูปแบบแก่ผู้ใช้เช่น ความคงสภาพของจดหมาย การปกปิดจดหมาย การรับรองจดหมายเป็นของจริง จดหมายที่ทำลายตัวเองเมื่อผู้รับอ่าน จดหมายไม่ประสงค์ออกนาม ผู้รับและผู้ส่งไม่สามารถปฏิเสธการรับและส่งจดหมาย การตรวจสอบ และการทำสถิติการใช้ระบบ SEM ได้ถูกสร้างขึ้นด้วยการเข้ารหัสที่ให้ความปลอดภัย การรับรองว่าเป็นของจริง และสามารถเปลี่ยนกลไกการทำงานความปลอดภัยแบบอื่นได้เพื่อการพัฒนาให้เป็นปัจจุบันอย่างเหมาะสม โดยแนวความคิดนี้สามารถช่วยปรับปรุงความปลอดภัยในระบบจดหมายอิเลคทรอนิกส์ได้อย่างดี ต้นแบบของ SEM ถูกสาธิตและทดลองเพื่อสามารถพิสูจน์ความปลอดภัยถึงการป้องกันจากผู้ไม่ประสงค์ดี วิทยานิพนธ์ฉบับนี้ได้นำเสนอรายละเอียดโครงสร้างและการวิเคราะห์ของ SEM ตลอดจนนำผลลัพธ์ที่ได้จากการทดลองมาวิเคราะห์ อภิปราย และสรุปผล พร้อมทั้งคำแนะนำสำหรับพัฒนางานในอนาคต