TRUSTED ELECTRONIC MAIL SYSTEM ON INTERNET

PEERAWIT WANNAWITTAYAPA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE
IN COMPUTER SCIENCE FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
1999

ISBN 974-662-552-7

3837890 SCCS/M : MAJOR : Computer Science : M.Sc. (Computer Science)
KEY WORDS : SECURE E-MAIL/ INFORMATION THEORY
PEERAWIT WANNAWITTAYAPA: TRUSTED ELECTRONIC MAIL SYTEM ON INTERNET. THESIS ADVISOR: DAMRAS WONGSAWANG Ph.D., SUPACHAI TANGWONGSAN Ph.D. 94 P. ISBN 974-662-552-7

Normally, sending E-mail via Internet system uses Simple Mail Transfer Protocol (SMTP) to manage transferring data. This protocol has been designed for general application and it is not adequate for use in applications requiring high level security. Thus, problems often occurred regarding security issues, for example, reading, imitating, modifying E-mails by unauthorized people. These are serious problems causing decrease in E-mail usage. Presently, new systems of sending E-mail have been developed and implemented for higher security, such as S/MIME, PEM, and PGP. However, these systems lack management, inspection, and verification.

This thesis proposed the secure E-mail system, called S-mail, having very high level security. S-mail focus on security of transferring E-mail via Internet. It used the concept of central security control, which provides better security than the distributed one. Namely, a server will manage security of the system, including communication services to users. Then, it encodes data by symmetric and asymmetric cryptosystems. This approach helps improve the management, inspection, and verification of security in the emailing system. This will increase confidence of sending importance messages. S-mail provides many security services such as self-destruct E-mail, anonymous E-mail, etc. These services are not provided in other systems. Experimentally, S-mail is one of the highest security E-mail systems. This system can be used for practical application.This thesis presents the model and structure of S-mail in detail. The implementation and experimentation are also presented. The results are discussed and evaluated and the improvements are suggested.

3837890 SCCS/M : สาขาวิชา : วิทยาการคอมพิวเตอร์ ; วท.ม. (วิทยาการคอมพิวเตอร์)
คำสำคัญ : ระบบไปรษณีย์อิเลคโทรนิคที่มีความปลอดภัย

พีรวิชญ์ วรรณวิทยาภา : ระบบไปรษณีย์อิเลคโทรนิคที่มีความปลอดภัยบนอินเตอร์เน็ต (TRUSTED ELECTRONIC MAIL SYSTEM ON INTERNET) คณะกรรมการควบคุมวิทยานิพนธ์: ดำรัส วงศ์สว่าง, Ph.D., ศุภชัย ตั้งวงศ์ศานต์, Ph.D., 94 หน้า. ISBN 974-662-552-7

โดยปกติการส่งจดหมายอิเลคโทรนิคผ่านระบบเครือข่ายอินเตอร์เน็ต จะใช้ Simple Mail Transfer Protocol (SMTP) เป็นตัวจัดการในการรับส่งข้อมูล ซึ่งเป็นโปรโตคอลที่ถูกออกแบบมานาน และไม่ได้ออกแบบมาสำหรับการใช้งานทั่วไป ที่ไม่มีระบบความปลอดภัยที่ดี ทำให้เกิดปัญหาขึ้นบ่อยครั้งทางด้านความปลอดภัยในการรับส่งจดหมายในปัจจุบันทั้งในเรื่องการปลอมจดหมาย การแก้ไขจดหมาย หรือการขโมยจดหมาย ซึ่งเป็นสาเหตุหลักอย่างหนึ่งที่ทำให้ผู้ใช้ลดความเชื่อถือในการใช้งาน แต่ปัจจุบันก็มีผู้ที่คิดค้นและพัฒนาระบบการรับส่งจดหมายอิเลคโทรนิคให้มีความปลอดภัยมากยิ่งขึ้น เช่น S/MIME , PEM, PGP แต่อย่างไรก็ตามระบบเหล่านี้ยังขาดการทางด้านการจัดการ การควบคุม การตรวจสอบ การติดตามในกรณีที่ผิดพลาด

งานวิจัยฉบับนี้ได้เสนอระบบไปรษณีย์อิเลคโทรนิคที่ปลอดภัย เรียกว่า S-mail ที่มีระบบความปลอดภัยสูง โดยเน้นถึงระบบความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายอินเตอร์เน็ต โดยใช้หลักการของการจัดการความปลอดภัยแบบศูนย์กลาง ซึ่งจะให้ความปลอดภัยที่ดีกว่าแบบกระจาย คือ มี Server ที่ทำหน้าที่ในการจัดการระบบความปลอดภัยของระบบ พร้อมทั้งให้บริการทางด้านการสื่อสารข้อมูลต่างๆแก่ผู้ใช้ และใช้หลักการเข้ารหัสข้อมูลในการป้องกันข้อความที่ส่งผ่านเครือข่าย โดยนำหลักการของ Symmetric และ Asymmetric cryptosystems มาประยุกต์ใช้ โดยแนวความคิดนี้จะสามารถช่วยในการจัดการ การตรวจสอบ การติดตาม ทางด้านความปลอดภัยระบบจดหมายอิเลคโทรนิกระทำได้ง่ายขึ้น ให้ความน่าเชื่อถือในการรับส่งข้อมูลสูง สามารถที่จะให้บริการระบบความปลอดภัยในหลายรูปแบบเช่น จดหมายที่ทำลายตัวเองเมื่อผู้รับอ่าน จดหมายไม่ประสงค์ออกนาม เป็นต้น ซึ่งบริการต่างๆ เหล่านี้ไม่มีอยู่ในระบบอื่น จากการทดสอบพบว่า S-mail เป็นระบบที่ให้ความปลอดภัยสูง และสามารถนำไปใช้งานได้จริง วิทยานิพนธ์ฉบับนี้จะได้นำเสนอโมเดล และโครงสร้างของ S-mail การนำไปประยุกต์ใช้งาน พร้อมทั้งนำเสนอการทดสอบ ผลการทดสอบ พร้อมทั้งอภิปรายผล และข้อเสนอแนะสำหรับการปรับปรุง