ชื่อเรื่องการค้นคว้าแบบอิสระ ลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บ

ผู้เขียน นายภูริพงษ์ อำนาจ

ปริญญา วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

บทคัดย่อ

การค้นคว้าแบบอิสระเรื่องลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บมีวัตถุประสงค์ เพื่อศึกษาและพัฒนาระบบอีเมลที่ส่งผ่านบนเว็บที่สามารถแนบลายเซ็นอิเล็กทรอนิกส์ ตรวจสอบลายเซ็นอิเล็กทรอนิกส์ และระบบสำหรับสร้างกุญแจส่วนบุคคลและกุญแจสาธารณะ ที่ใช้สำหรับการทำลายเซ็นดิจิทัล

ระบบงานลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บ พัฒนาขึ้นโดยใช้ขั้นตอนวิธีอาร์เอสเอ ทำงานร่วมกับขั้นตอนวิธีแฮชในการทำข้อความฉบับย่อเพื่อสะดวกในการทำลายเซ็นอิเล็กทรอนิกส์ สำหรับการส่งข้อมูลระหว่างเครื่องแม่ข่ายและเครื่องลูกข่าย ข้อมูลจะถูกเข้ารหัสด้วยซ็อกเก็ตซีเคียวร์เลเยอร์โพรโทคอล

ในการสร้างและกำหนดค่ากุญแจส่วนบุคคลและกุญแจสาธารณะให้กับผู้ใช้จะเป็นหน้าที่ของผู้ดูแลระบบ ผู้ใช้สามารถเพิ่มลายเซ็นอิเล็กทรอนิกส์ระหว่างการส่งอีเมล ตรวจสอบลายเซ็นอิเล็กทรอนิกส์ได้ในระหว่างการอ่านอีเมล ส่งต่ออีเมล ส่งไฟล์เอกสาร ลบอีเมล มีระบบบัญชีรายชื่อผู้ใช้ในการเก็บข้อมูลสำหรับการติดต่อตลอดจนเก็บข้อมูลของกุญแจสาธารณะเพื่อใช้สำหรับการตรวจสอบลายเซ็นอิเล็กทรอนิกส์

ระบบงานลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บ พัฒนาขึ้นโดยใช้โปรแกรมภาษาพีเอชพี จาวาสคริปท์ เพิร์ล เชลสคริปท์ และสร้างฐานข้อมูลเชิงสัมพันธ์ด้วยระบบจัดการฐานข้อมูลมายเอสคิวแอล เพื่อทำงานได้บนระบบเครือข่าย

ระบบงานลายเซ็นดิจิทัลสำหรับอีเมลที่ส่งผ่านบนเว็บ ได้ทำการทดสอบโดยส่งอีเมลจำนวน 50 ฉบับ ภายในอินทราเน็ตเวิร์ก ซึ่งในอีเมล 5 ฉบับมีการเปลี่ยนแปลงข้อความภายในจดหมายที่ฝั่งผู้รับ 5 ฉบับมีแก้ไขเปลี่ยนค่ากุญแจส่วนบุคคลในการส่ง ผลปรากฏว่าระบบสามารถแจ้งได้ว่าอีเมล 10 ฉบับนี้ไม่ผ่านการตรวจสอบ

Independent Study Title Digital Signature for Web-Based E-mail

Author Mr. Phuripong Amnart

Degree Master of Science (Computer Science)

Independent Study Advisor Assoc. Prof. Dr.Ekkarat Boonchieng

ABSTRACT

The objectives of this independent study entitled, "Digital Signature for Web-Based E-mail" are to study and develop a web-based email system which enables email user to attach and verify digital signatures, as well as private and public key generation for creating digital signatures.

The digital signature system for web-based email was developed by using RSA algorithm, which integrated into the email message hashing process. As a result, the data was encrypted before sending between client and server machines via Secured Socket Layer (SSL) Protocol.

The system administrator is responsible for generating private and public keys for users. The user can include his/her digital signature when sending emails, verify digital signatures attached to the received emails, together with other common operations such as forwarding emails, file attachments, and deletion emails. There is a user database system for storing information used in data communication, as well as information on public keys for verifying digital signatures.

The system was developed by using a variety of computing languages: PHP, javascript, Perl, and Shell script. MySql was used as database management system (DBMS).

Finally, the system was tested by sending/receiving 50 emails within the intranet; five of which have their email messages edited at the receiver side, another five of which have their private key modified during email transmission. The system was able to identify all tampered emails during the verification process.