

**SECURE ONLINE TRADING SYSTEM**

**KAYTIP OJAKA**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT  
OF THE REQUIREMENTS FOR  
THE DEGREE OF MASTER OF SCIENCE  
(COMPUTER SCIENCE)  
FACULTY OF GRADUATE STUDIES  
MAHIDOL UNIVERSITY  
2003**

**ISBN 974-04-3762-1  
COPYRIGHT OF MAHIDOL UNIVERSITY**

ระบบรักษาความปลอดภัยทางการค้าออนไลน์ (SECURE ONLINE TRADING SYSTEM )

กฤษฎิ์ โອชะกะ 4137842 SCCS/M

วท.ม. (วิทยาการคอมพิวเตอร์)

คณะกรรมการควบคุมวิทยานิพนธ์ : คำรัส วงศ์สว่าง, Ph.D., สุทธิญา พงษ์สุภาพ, Ph.D.

### บทคัดย่อ

ปัจจุบันพาณิชย์อิเล็กทรอนิกส์มีการพัฒนาและมีการใช้อย่างแพร่หลาย ผู้ใช้สามารถใช้ ณ สถานที่ และเวลาใดก็ได้ จึงกลายเป็นส่วนหนึ่งในชีวิตประจำวัน เพราะใช้ง่าย สะดวก รวดเร็ว ระบบพาณิชย์อิเล็กทรอนิกส์เป็นระบบเปิด ดังนั้นการติดต่อสื่อสารระหว่างผู้ใช้ระบบ ยังไม่มีระบบรักษาความปลอดภัยและการบริการที่ดีทำให้มีจุดอ่อนและผู้ไม่หวังดีคุกคามระบบ เพื่อต้องการรู้หมายเลขบัตรเครดิต, การแก้ไขหรือเปลี่ยนแปลงข้อมูลการสั่งซื้อสินค้าและข้อมูลการชำระเงิน, ปลอมแปลงเป็นผู้อื่นเข้ามาใช้ระบบและกรณีระบบเครือข่ายไม่สามารถใช้งานได้ ทำให้ขาดความเชื่อถือในการส่งหมายเลขบัตรเครดิตผ่านระบบอินเทอร์เน็ต อย่างไรก็ตามการเข้ารหัสบัตรเครดิตเพียงอย่างเดียว ยังไม่เพียงพอที่จะรับรองความปลอดภัยของระบบพาณิชย์อิเล็กทรอนิกส์

วิทยานิพนธ์ฉบับนี้ได้เสนอโครงสร้างและรูปแบบการทำงาน เรียกว่า “ระบบรักษาความปลอดภัยทางการค้าออนไลน์” (SOT) เพื่อแก้ปัญหาที่อาจเกิดขึ้นกับพาณิชย์อิเล็กทรอนิกส์ เน้นถึงระบบความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต โดยใช้การจัดการความปลอดภัยแบบศูนย์กลาง เพื่อให้บริการความปลอดภัย ประกอบด้วย ปกปิดข้อมูล, ความถูกต้องของข้อมูล, การพิสูจน์ตัวจริง, ผู้รับ-ผู้ส่งไม่สามารถปฏิเสธการรับ-ส่งข้อมูล, ร้านค้าได้รับเงินจากลูกค้าและลูกค้าได้รับสินค้าหลังจากที่สั่งซื้อ นอกจากนี้ ระบบสามารถเปลี่ยนกลไกเพื่อพัฒนาให้เป็นปัจจุบัน แนวความคิดนี้ สามารถปรับปรุงความปลอดภัยในระบบพาณิชย์อิเล็กทรอนิกส์ ต้นแบบของ SOT ถูกสาธิตและทดลองเพื่อพิสูจน์ความปลอดภัย วิทยานิพนธ์ได้นำเสนอรายละเอียดโครงสร้างและการวิเคราะห์ของ SOT ตลอดจนนำผลลัพธ์ที่ได้จากการทดลองมาวิเคราะห์ อภิปรายและสรุปผลพร้อมทั้งคำแนะนำเพื่อพัฒนางานในอนาคต

SECURE ONLINE TRADING SYSTEM.

KAYTIP OJAKA 4137842 SCCS/M

M.Sc.(COMPUTER SCIENCE)

THESIS ADVISORS : DAMRAS WONGSAWANG, Ph.D. , SUKANYA  
PHONGSUPHAP, Ph.D.

## **ABSTRACT**

Nowadays, E-commerce is rapidly developing and used extensively. E-commerce can be accessed 24 hours per day and 365 days in a year. E-commerce has become a part of daily life, because it is simple, convenient, and fast. Given the openness of today's networks for communication, very little attention has been given to the need for security when sharing personal details on an open network. E-commerce is susceptible to interception by unwanted parties and exchanged information can be accessed at numerous stages in the communication. Hacking is the term used for people who gain unauthorized access to material. Credit card details, order information, address and payment information are all useful material for the hacker who is able to manipulate these for his own benefit. Obviously such problems must be overcome if users are to have the confidence to trade on an open network. Some methods have been tried to make the system more secure such as encrypting credit card details.

This thesis proposed a model, called the "Secure Online Trading System" (SOT), in an attempt to further enhance security with E-commerce. The SOT focus was on security when conducting E-commerce via any public network. It employed the concept of central security control, which provides a variety of security services to users including confidentiality, integrity, authentication and non-repudiation. The SOT, which is made up of secured encryption, authentication and other security mechanisms is very flexible. It can be adapted and upgraded when new technology or systems are available to add to it. This approach helps improve the security in the E-commerce system. The SOT prototype was implemented and tested. It proved to be secure against passive attacks. This thesis presented a detailed structure and analysis of SOT. The experimental results were also analysed, discussed and conclusions reached. Finally, future research benefit to further enhance of the SOT system were also suggested.

**KEY WORDS : SECURE E-Commerce SYSTEM / AUTHENTICATION  
MESSAGE AUTHENTICATION / MESSAGE PRIVACY**

144 P. ISBN 974-04-3762-1