

การออกแบบและพัฒนาระบบแสดงตนของบัตรเครดิตในพาณิชย์อิเล็กทรอนิกส์



นางสาว ชนิษฐา พรหมสุข

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2543

ISBN 974-13-0843-4

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

3 ก.ย. 2546

119694118

DESIGN AND DEVELOPMENT OF CREDIT CARD AUTHENTICATION
IN ELECTRONIC COMMERCE

Miss Khanittha Promsook

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Computer Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2000

ISBN 974-13-0843-4

นางสาวชนิษฐา พรหมสุข : การออกแบบและพัฒนาระบบการแสดงผลของบัตรเครดิตในระบบพาณิชย์อิเล็กทรอนิกส์. (DESIGN AND DEVELOPMENT OF CREDIT CARD AUTHENTICATION IN ELECTRONIC COMMERCE) อ. ที่ปรึกษา : รศ.ดร.วันชัย ธีวไพบูลย์, อ. ที่ปรึกษาร่วม : ดร.อมฤต เหล่ารักพงษ์, 85 หน้า. ISBN 974-13-0843-4.

เมื่อระบบการค้าอิเล็กทรอนิกส์ได้รับความนิยมมากขึ้นเรื่อย ๆ การใช้งานจำเป็นต้องมีประสิทธิภาพมากที่สุด ระบบการค้าอิเล็กทรอนิกส์อาจเกิดปัญหาได้หากผู้ใช้ไม่มีความเชื่อมั่น โดยเฉพาะอย่างยิ่งการชำระเงินด้วยบัตรเครดิตบนระบบการค้าอิเล็กทรอนิกส์ บัตรเครดิตซึ่งมีพื้นฐานมาจากการไว้วางใจกัน มีหลักการรักษาความปลอดภัยที่สำคัญคือการตรวจสอบความถูกต้องของลายมือชื่อของผู้ถือบัตรที่ปรากฏบนบัตร และลายมือชื่อที่ผู้ถือบัตรลงนามลงบนเอกสารการชำระเงิน แต่บนระบบการค้าอิเล็กทรอนิกส์ที่ผู้ขายและผู้ซื้อแทบจะไม่มีโอกาสพบกันเลยนั้น การตรวจสอบจึงไม่สะดวกที่จะทำตามวิธีพื้นฐาน ปัจจุบันมีหลายองค์กรที่ทำการศึกษารองความปลอดภัยของการใช้บัตรเครดิตบนระบบการค้าอิเล็กทรอนิกส์ แต่ในเชิงพาณิชย์ค่าใช้จ่ายที่เกิดขึ้นและความเหมาะสมกับองค์กรจึงเป็นเรื่องที่ผู้ใช้ระบบต้องพิจารณา

การวิจัยนี้ทำขึ้นเพื่อศึกษารูปแบบการใช้งานของระบบในเชิงพาณิชย์ที่มีในปัจจุบัน ศึกษาข้อเด่นและข้อด้อย ทดลองสร้างระบบขึ้นใช้เองโดยการสร้างโปรแกรมประยุกต์ที่ใช้แนวคิดการเข้ารหัส (Cryptography) และเปรียบเทียบผลการทดลองจากระบบตัวอย่างที่สร้างขึ้นกับระบบที่มีอยู่ วิเคราะห์จุดเด่นและจุดด้อยของระบบที่น่าเสนอ เพื่อหาระบบที่มีประสิทธิภาพและมีค่าใช้จ่ายต่ำ สำหรับเป็นทางเลือกอีกทางของผู้ใช้ และยังเป็นประโยชน์ต่อการศึกษาต่อไปในอนาคตอีกด้วย

ภาควิชา วิศวกรรมศาสตร์คอมพิวเตอร์
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์
ปีการศึกษา 2543

ลายมือชื่อนิสิต วนิษฐา พรหมสุข
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

4071407621 : MAJOR COMPUTER SCIENCE

KEY WORD: AUTHENTICATION / ELECTONIC COMMERCE / CREDIT CARD / SECURITY / CRYPTOGRAPHY

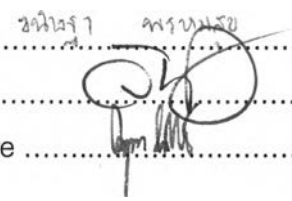
KHANITTHA PROMSOOK : DESIGN AND DEVELOPMENT OF CREDIT CARD AUTHENTICATION IN ELECTRONIC COMMERCE. (DESIGN AND DEVELOPMENT OF CREDIT CARD AUTHENTICATION IN ELECTRONIC COMMERCE) THESIS ADVISOR : ASSOC. PROF.WANCHAI REIPAIBOON,Ph.D., THESIS COADVISOR : AMARIT LAORAKPONG,D.Eng. , 85 pp. ISBN 974-13-0843-4.

An electronic commerce is in the growth time. It has to have a very strong efficiency. The system will not work if user does not trust on it. The main topic is payment by credit card. Normally credit card concept is based on confidence. When a card holder use his credit card, a merchant will check by comparing the signature on card and the signature on receipt. In electronic commerce , card holder and merchant are not in the same place, so the system cannot use the traditional method. Nowadays there are many commercial products have been created to protect this problem, but these products spend a lot of cost and these products may not suitable for any organizations.

Studies on payment by credit card on electronic commerce try to study the way some commercial products work to know their strength and weakness and to create a new application program using cryptography knowledge to be a new effective choice for user .

Department Computer Engineering
Field of study Computer Science
Academic year 2000

Student's signature
Advisor's signature
Co-advisor's signature



กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของอาจารย์ที่ปรึกษาทั้ง 2 ท่าน คือ รองศาสตราจารย์ ดร.วันชัย รั้วไพบูลย์ และ ดร.อมฤต เหล่ารักพงษ์ และกรรมการสอบวิทยานิพนธ์อีก 2 ท่าน คือ อาจารย์ ดร.อาทิตย์ ทองทัช และอาจารย์ ดร.บุญเสริม กิจศิริกุล และกรรมการสอบความก้าวหน้า รวมถึงคณาจารย์ทุกท่านในภาควิชาวิศวกรรมคอมพิวเตอร์ที่ได้ให้ความรู้ตลอดหลักสูตร ซึ่งทุกท่านได้ให้โอกาส และคำแนะนำเป็นอย่างดี จึงขอขอบพระคุณมา ณ ที่นี้

ชนิษฐา พรหมสุข

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ฉ
สารบัญ	ช
สารบัญตาราง	ฅ
สารบัญภาพ	ญ
บทที่	
1. บทนำ	
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	3
1.3 ขอบเขตของการวิจัย	4
1.4 ข้อจำกัดของการวิจัย	5
1.5 ประโยชน์ที่คาดว่าจะได้รับ	6
1.6 วิธีดำเนินการวิจัย	6
2. เอกสารและงานวิจัยที่เกี่ยวข้อง	
2.1 แนวคิดและทฤษฎี	7
2.1.1 ความรู้ทั่วไปเกี่ยวกับบัตรเครดิต	7
2.1.2 ประเภทของการค้าอิเล็กทรอนิกส์	12
2.1.3 ความทั่วไปว่าด้วยการเข้ารหัส (Cryptography)	14
2.1.4 ลายมือชื่อดิจิทัล (Digital signature) และ ลายมือชื่ออิเล็กทรอนิกส์อื่น ๆ	15
2.1.5 CyberCash Credit Card Protocol Version 0.8	17
2.1.6 Transaction Security Protocol.....	18
2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง	24
2.2.1 การปกป้องข้อมูลบนอินเทอร์เน็ต.....	24
2.2.2 คริปโตกราฟฟีคัลลอรี่ทิม.....	25
2.2.3 อเทนท์ซิเคชัน และลายเซ็นดิจิทัล.....	26
2.2.4 การเข้ารหัสลับ.....	30

	หน้า
2.2.5 หลักการเข้ารหัสข้อมูลบนอินเทอร์เน็ตแบบอาร์ เอส เอ (RSA)...	40
3 วิธีดำเนินการวิจัย	46
4 ผลการทดลอง.....	66
5 สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ	81
รายการอ้างอิง	83
ประวัติผู้เขียนวิทยานิพนธ์.....	84

สารบัญตาราง

ตาราง	หน้า
ตารางที่ 1.1 ตารางแสดงปัญหาของผู้ซื้อและผู้ขายในการชำระเงินด้วยบัตรเครดิตบนระบบออนไลน์.....	3
ตารางที่ 2.1 ตารางแสดงบริการด้านความปลอดภัยพื้นฐานของระบบ SSL.....	20
ตารางที่ 2.2 ตารางสรุปข้อเปรียบเทียบระหว่าง SSL กับ SET.....	22
ตารางที่ 2.3 ตารางแสดงเวลาที่ใช้สำหรับแยกตัวประกอบของระบบ RSA.....	45
ตารางที่ 3.1 เพิ่มข้อมูลสำหรับเก็บข้อมูลผู้ถือบัตรที่ลงทะเบียน.....	50
ตารางที่ 3.2 เพิ่มข้อมูลสำหรับเก็บข้อมูลรหัสของผู้ถือบัตรที่ลงทะเบียน.....	50
ตารางที่ 3.3 เพิ่มข้อมูลสำหรับเก็บข้อมูลร้านค้ารับบัตรที่ลงทะเบียน.....	51
ตารางที่ 3.4 เพิ่มข้อมูลสำหรับเก็บข้อมูลรหัสของร้านค้ารับบัตรที่ลงทะเบียน.....	51
ตารางที่ 3.5 เพิ่มข้อมูลสำหรับเก็บข้อมูลรายการค้า (รายการซื้อ / ขายสินค้า).....	52
ตารางที่ 3.6 ตารางแสดงรายชื่อโปรแกรม หน้าจอ ส่วนจำเพาะ (module) ของระบบทดลองส่วนของบริษัทผู้ให้บริการบัตรเครดิต.....	53
ตารางที่ 3.7 ตารางแสดงรายชื่อโปรแกรม หน้าจอ ส่วนจำเพาะ (module) ของระบบทดลองส่วนของร้านค้ารับบัตร.....	54
ตารางที่ 3.8 ตารางแสดงการเรียกใช้งานหน้าจอ.....	54
ตารางที่ 4.1 ตารางสรุปข้อเปรียบเทียบระหว่างระบบที่ทำการทดลองกับ SET.....	72

สารบัญภาพ

ภาพประกอบ	หน้า
รูปที่ 1.1 รูปแสดงขอบเขตงานของระบบ.....	5
รูปที่ 2.1 รูปแสดงความสัมพันธ์ของกลุ่มผู้ที่เกี่ยวข้องกับการใช้บัตรเครดิต.....	10
รูปที่ 2.2 แบบข้อความที่ส่งของ CyberCash.....	18
รูปที่ 2.3 ภาพแสดงตำแหน่งของ SSL Protocol บนมาตรฐาน OSI.....	19
รูปที่ 2.4 แสดงวิธีตรวจสอบข้อความโดยใช้รหัสรับรองข้อความ.....	27
รูปที่ 2.5 แสดงการเข้ารหัสโดยใช้คีย์ที่ต่างกัน.....	28
รูปที่ 2.6 แสดงการดำเนินการเข้ารหัสลับและการดำเนินการถอดรหัสลับ.....	32
รูปที่ 2.7 การเข้ารหัสแบบกุญแจสมมาตร.....	33
รูปที่ 2.8 การเข้ารหัสแบบกุญแจสมมาตร.....	34
รูปที่ 2.9 การเข้ารหัสแบบกุญแจผสม.....	35
รูปที่ 2.10 แสดงข้อมูลบนบัตรประจำตัวดิจิทัล.....	36
รูปที่ 2.11 การส่งข้อความไปพร้อมกับลายเซ็นดิจิทัล และ การตรวจสอบข้อความด้วยลายเซ็นดิจิทัล.....	37
รูปที่ 2.12 แสดงขั้นตอนการเข้ารหัสแบบ RSA.....	42
รูปที่ 3.1 Data Flow Diagram Level 0 – Context Diagram.....	47
รูปที่ 3.2 Data Flow Diagram Level 1.....	47
รูปที่ 3.3 ภาพรวมของระบบที่ทำการทดลอง (System Overview).....	48
รูปที่ 3.4 Data Model.....	49
รูปที่ 3.5 หน้าจอสำหรับการลงทะเบียนของผู้ถือบัตร.....	55
รูปที่ 3.6 หน้าจอสำหรับการลงทะเบียนของร้านค้ารับบัตร.....	58
รูปที่ 3.7 หน้าจอสำหรับการส่งข้อมูลการสั่งซื้อ.....	61
รูปที่ 3.8 หน้าจอสำหรับการบันทึกข้อมูลทางการเงินของผู้ถือบัตร.....	63
รูปที่ 4.1 หน้าจอสำหรับการลงทะเบียนของผู้ถือบัตร.....	66
รูปที่ 4.2 หน้าจอสำหรับการลงทะเบียนของร้านค้ารับบัตร.....	67
รูปที่ 4.3 หน้าจอสำหรับการส่งข้อมูลการสั่งซื้อ.....	68
รูปที่ 4.4 หน้าจอสำหรับการบันทึกข้อมูลทางการเงินของผู้ถือบัตร.....	70
รูปที่ 4.5 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้ารับบัตร.....	75
รูปที่ 4.6 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นผู้ถือบัตร.....	76

สารบัญญภาพ (ต่อ)

ภาพประกอบ	หน้า
รูปที่ 4.7 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้า และการปลอมเป็นผู้ถือบัตร	77
รูปที่ 4.8 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นบริษัทผู้ออกบัตร.....	78
รูปที่ 4.9 ระบบที่ทำการทดลองเมื่อมีการปลอมเป็นร้านค้า และการปลอมเป็นบริษัทผู้ออกบัตร.....	79
รูปที่ 4.10 ระบบที่ทำการทดลองเมื่อมีการส่งรายการที่ไม่ถูกต้อง จากร้านค้ารับบัตรที่ลงทะเบียนอย่างถูกต้อง.....	80