การรักษาความมั่นคงปลอดภัยของการชำระเงินผ่านเครือข่ายไร้สาย โดยใช้ข้อความสั้นผ่านผู้ให้บริการ

เมฆินทร์ วรศาสตร์[1] และ ศุภกร กังพิศดาร[2]

คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร

Emails: [1] maykin@webmaster.in.th, [2]supakorn@mut.ac.th

บทคัดย่อ

การชำระเงินผ่านอุปกรณ์สื่อสารไร้สาย ทำให้ผู้ใช้งานสามารถซื้อสินค้าหรือบริการในขณะที่กำลังเคลื่อนที่อยู่ได้ ปัจจุบันการทำธุรกรรมบนอุปกรณ์ไร้สาย ส่วนใหญ่จะทำผ่านข้อความสั้น (Short Message Service หรือ SMS) ที่ผ่านมามีการนำเสนอโพรโทคอลสำหรับการชำระเงินผ่าน SMS จำนวนมาก แต่อย่างไรก็ตาม โพรโทคอลดังกล่าวยังขาดคุณสมบัติทางด้านความมั่นคงปลอดภัย ในบทความนี้ผู้วิจัยนำเสนอโมเดลสำหรับการชำระค่าสินค้าหรือบริการผ่าน SMS และยังได้เสนอโพรโทคอลชำระเงินผ่าน SMS ที่ช่วยให้ผู้ใช้งานสามารถชำระเงินโดยตรงกับโอเปอเรเตอร์ หรือชำระเงินให้พ่อค้าผ่านโอเปอเรเตอร์ได้ นอกจากธุรกรรมที่ทำจะมีคุณสมบัติด้านความมั่นคงปลอดภัยแล้ว ยังมีความง่ายและเข้ากันได้กับโครงสร้างพื้นฐานของระบบ SMS ที่มีอยู่ในปัจจุบัน

คำสำคัญ— Mobile payment, SMS payment, mobile commerce, payment protocols, cryptographic protocols

1. บทนำ

โทรศัพท์มือถือในปัจจุบันมีความสามารถมากกว่าการใช้เป็นอุปกรณ์โทรศัพท์ แต่ยังสามารถนำมาใช้ในการส่งข้อมูลผ่านเครือข่ายการสื่อสาร เช่น GPRS (General Packet Radio Service), EDGE (Enhanced Data Rate for GSM Evolution) หรือ HSPDA (High-Speed Downlink Packet Access) ซึ่งผู้ใช้งานสามารถเชื่อมต่ออินเทอร์เน็ต และใช้งานโปรแกรมบนอุปกรณ์มือถือได้ แม้ว่ารูปแบบของการส่งข้อมูลจะมีอยู่หลากหลาย อันเนื่องมาจากความรวดเร็วของการส่งข้อมูล แต่ข้อความสั้น (SMS) กลับได้รับความนิยมมากที่สุด เนื่องจากมีต้นทุนต่ำ และเป็นคุณสมบัติที่มีอยู่ในมือถือที่มีราคาต่ำ ในปัจจุบันมีการใช้ SMS เพื่อวัตถุประสงค์หลายอย่าง เช่น ส่ง SMS ไปยังสมาชิก ซึ่งเป็นส่วนหนึ่งของแคมเปญโฆษณา หรือการส่ง SMS เพื่อขอใช้บริการเสริมต่างๆ

ในปัจจุบันมีการใช้ SMS สำหรับการทำธุรกรรมการชำระเงิน เช่น การซื้อเสียงรอสาย (Ringtones) เพลง หรือรูปภาพจากผู้ประกอบการมือถือ โดยเรียกธุรกรรมในลักษณะนี้ว่า Mobile Payment ซึ่งหมายถึงการทำธุรกรรมการชำระเงินระหว่างบุคคลผ่านเครือข่ายไร้สายในขณะที่กำลังเคลื่อนที่ โดยผู้ชำระเงินโอนยอดเงินให้ผู้รับเงิน แล้วรับสินค้าหรือบริการจากผู้รับเงิน การชำระเงินด้วยมือถือจึงไม่ได้เป็นแค่เพียงทางเลือกการชำระเงินอิเล็กทรอนิกส์ ด้วยพื้นฐานของการสื่อสารไร้สาย จึงนำมาซึ่งปัญหาที่เกิดขึ้นใหม่เกี่ยวกับธุรกรรมการรักษาความมั่นคงปลอดภัยและประสิทธิภาพของการชำระเงินมือถือ ข้อมูลที่ส่งผ่านเครือข่ายไร้สายถูกดักจับได้ง่าย แม้ว่าเครือข่าย GSM มีการเข้ารหัสลับข้อมูลที่ส่งระหว่างอุปกรณ์เคลื่อนที่และสถานีฐานที่อาศัยเทคนิคการเข้ารหัสลับ A5/1 และ A5/2 ซึ่งมีรายงานถึงความอ่อนและช่องโหว่ตาม [1] ดังนั้นการรักษาความมั่นคงปลอดภัยของเครือข่าย GSM ที่ชั้นดาต้าลิงก์ (Data-link layer) จึงไม่เพียงพอ จำเป็นต้องมีช่องทางสำหรับการสื่อสารที่มั่นคงปลอดภัยบนเครือข่ายไร้สายที่ชั้นแอพลิเคชัน (Application layer) ในการใช้งานจริงนั้นสามารถทำได้โดยใช้การเข้ารหัสลับ

เพื่อสร้างความมั่นคงปลอดภัยให้กับการชำระเงินผ่านมือถือโดยใช้ SMS นั้น มีโพรโทคอลสำหรับการชำระเงินมือถือจำนวนมากถูกนำเสนอ [1, 2, 3] โดย Toorani *et al.* [1] เสนอระบบ SSMS ซึ่งใช้วิทยาการเข้ารหัสลับแบบ Elliptic-curve (Elliptic-curve Cryptography) ที่ให้คุณสมบัติทางด้านความมั่นคงปลอดภัยมากมาย เช่น การรักษาความลับของข้อมูล (Data Confidentiality) ความคงสภาพของข้อมูล (Data Integrity) การพิสูจน์ตัวตน (Authentication) และการไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation) นอกจากนี้ยังมีความความสามารถในการตรวจสอบพับบลิคคีย์ (Public key) ของแต่ละฝ่าย และส่งต่อความลับ เนื่องจากเป็นระบบที่ใช้การเข้ารหัสลับแบบพับบลิคคีย์จึงจำเป็นต้องใช้บุคคลที่สามที่เชื่อถือได้ ทำหน้าที่เป็นผู้รับรอง

นอกจากนี้ Hashemi *et al.* [3] เสนอกรอบการทำงาน สำหรับการชำระเงินมือถือที่มีความปลอดภัยโดยใช้ SMS ที่อธิบายความสัมพันธ์ระหว่าง SMS gateway และ SMSC (Short Message Service Center) และยังอธิบายถึงภาพรวมของกรอบการทำงานของการชำระเงินที่เหมาะสมสำหรับ SMS โดยใช้การเข้ารหัสลับแบบ AES (Advanced Encryption Standard) เพื่อความมั่นคงปลอดภัยของธุรกรรมที่เกิดขึ้น ซึ่งเป็นวิธีการเข้ารหัสลับแบบสมมาตร (Symmetric Cryptography) โดยที่คีย์ (Key) ที่ใช้ร่วมกันระหว่างลูกค้าและ

ธนาคารมีการกระจายเฉพาะตอนที่ลูกค้าลงทะเบียนใช้บริการเป็นครั้งแรก แต่ไม่มีการแลกเปลี่ยนเซสชันคีย์ (Session key) ระหว่างกัน

ต่อมา Harb *et al.* [2] เสนอ SecureSMSPay ซึ่งเป็นระบบการชำระเงินระหว่างผู้ชำระเงินและผู้รับเงิน โดยการโอนเงินทำจากธนาคารของผู้ชำระเงิน ผ่านทาง Payment gateway แต่ระบบนี้จำเป็นต้องรู้หมายเลขโทรศัพท์มือถือของผู้ชำระเงินและผู้รับเงิน นอกจากนี้การรักษาความมั่นคงปลอดภัยของระบบจะขึ้นอยู่กับการเข้ารหัสลับแบบสมมาตรที่ต้องใช้คีย์ร่วมกัน การเปลี่ยนเซสชันคีย์นั้นระบบใช้ค่าแฮช (Hash value) ของการหมุนเวียนของเซสชันคีย์ ซึ่งเสี่ยงต่อการถูกโจมตี

บทความวิจัยฉบับนี้เสนอโมเดลสำหรับการชำระค่าสินค้าหรือบริการผ่านข้อความสั้นหรือ SMS เพื่อแสดงให้เห็นถึงแนวทางการสร้างความเข้าใจถึงสภาพแวดล้อมของการชำระเงิน ลักษณะการทำธุรกรรมภายในระบบ รวมทั้งคุณสมบัติทางด้านความมั่นคงปลอดภัยที่จำเป็น นอกจากนี้ยังได้เสนอโพรโทคอลใหม่สำหรับการชำระเงินที่ปลอดภัยบนมือถือด้วย SMS ที่เรียกว่า SMS-based Operator-assisted Mobile Payment (SOMP) ที่มีแนวทางการทำงานตามโมเดลที่นำเสนอ นอกจากนี้โพรโทคอลนี้ยังมีน้ำหนักเบาเนื่องจากใช้เพียงการเข้ารหัสลับแบบสมมาตรและฟังก์ชันแฮช โพรโทคอลนี้ทำให้ลูกค้าสามารถชำระเงินให้สินค้าบริการให้แก่ผู้ให้บริการ หรือชำระให้กับร้านค้าผ่านผู้ให้บริการ ซึ่งทำให้โพรโทคอลนี้สามารถนำไปใช้ในธุรกิจได้จริง รวมถึงยังมีคุณสมบัติในการรักษาความมั่นคงปลอดภัยของการทำธุรกรรมที่จำเป็นที่เป็น คือ ความลับข้อมูล ความคงสภาพ และการพิสูจน์ตัวตนของผู้ใช้ นอกจากนี้ยังใช้การสร้างเซสชันคีย์ที่มีการใช้งานจำกัด และเทคนิคการกระจายคีย์ตาม [8] เพื่อป้องกันการใช้งานซ้ำของเซสชันคีย์ ซึ่งโพรโทคอลที่เสนอยังเข้ากันได้กับโครงสร้างพื้นฐานของ SMS ที่มีอยู่

บทความวิจัยฉบับนี้มีโครงสร้างดังนี้ บทที่ 2 กล่าวถึงพื้นฐานที่เกี่ยวข้อง บทที่ 3 เสนอโมเดลสำหรับการชำระเงินผ่าน SMS บทที่ 4 เสนอโพรโทคอลอย่างละเอียด บทที่ 5 วิเคราะห์ความมั่นคงปลอดภัยของโพรโทคอล บทที่ 6 สรุปผลการวิจัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 การชำระเงินผ่านเครือข่ายไร้สาย

สืบเนื่องจาก [14] ระบบการชำระเงินทั่วไปประกอบด้วย 5 ฝ่ายคือ Client (ลูกค้า), Merchant (พ่อค้า), Payment Gateway (หรือ PG), Issuer (สถาบันการเงินของลูกค้า) และ Acquirer (สถาบันการเงินของร้านค้า) การดำเนินการของ issuer และ acquirer กระทำบนอินเทอร์เน็ต ขณะที่การตัดเงินจากการชำระเงินกระทำภายในเครือข่ายระหว่างธนาคาร ในการทำธุรกรรรมนั้น มี 3 รายการพื้นฐาน คือ สั่งซื้อชำระเงิน การหักเงิน และการเพิ่มเงิน

การชำระเงิน (Payment) เป็นปฏิสัมพันธ์ที่เกิดขึ้นเมื่อลูกค้าต้องการซื้อสินค้าหรือบริการกับพ่อค้า รวมถึงพ่อค้าส่งใบเสร็จรับเงินการชำระเงินให้ลูกค้า การตัดเงินเกิดขึ้นที่ฝั่งลูกค้า โดยส่งคำขอไปยัง PG (ในนามของ Issuer) เพื่อหักยอดเงินที่ต้องการชำระจากบัญชีของลูกค้า และแจ้งลูกค้าว่าจำนวนเงินที่ต้องการถูกหักจากบัญชีของลูกค้าแล้ว การเพิ่มเงินทำที่พ่อค้าโดยร้องขอ PG (ในนามของ Acquirer) เพื่อขอโอนเงินไปยังบัญชีของพ่อค้า โดยจะทำรายการที่ PG (ในนามของ Acquirer) แล้วแจ้งพ่อค้าว่ามีการโอนเข้าบัญชีพ่อค้าแล้ว มีธุรกรรมในหลายโพรโทคอลสำหรับการชำระเงิน [11, 12, 13] เป็นไปตามขั้นตอนต่อไปนี้

C → M: *Payment (Request), Debit (Request)*

M → PG: *Debit (Request), Credit (Request)*

PG → M : *Credit (Response), Debit (Response)*

M → C: *Payment (Response), Debit (Response)*

เมื่อ C, M, PG หมายถึง ลูกค้า พ่อค้า และ PG ตามลำดับ อย่างไรก็ตามโพรโทคอลชำระเงินจำนวนไม่น้อยที่ทำงานแตกต่างออกไป ในบางระบบการชำระเงินมี PG เป็นศูนย์กลางที่ต้องทำธุรกรรมผ่านระหว่างลูกค้า ตัวอย่างที่ชัดเจนสำหรับประเภทของระบบการชำระเงิน คือ ระบบธนาคารอินเทอร์เน็ต (Internet Banking) ซึ่งการทำธุรกรรมกระทำผ่านคนกลาง คือ PG กระบวนการนี้น่าจะเหมาะสมกับระบบการชำระเงินโดยใช้ SMS ในปัจจุบันที่ผู้ให้บริการมือถือ ทำหน้าที่เป็น PG อยู่แล้วกล่าวคือลูกค้าสามารถสมัครรับบริการกับผู้ให้บริการมือถือ เช่น การชำระเงินค่าสินค้าหรือบริการรวมถึง เสียงรอสาย เพลง คลิปวิดีโอ ฯลฯ ซึ่งลูกค้าจะได้รับสิทธิ์ในการสั่งซื้อสินค้าหรือบริการภายในวงเงินที่มี จากนั้นผู้ให้บริการมือถือจะโอนเงินดังกล่าวให้พ่อค้า

2.2 งานวิจัยที่มีอยู่

ที่ผ่านมามีงานวิจัยมากมายได้นำเสนอแนวทางการรักษาความมั่นคงปลอดภัยให้แก่ระบบชำระเงินผ่านข้อความสั้น ดังเช่น Harb *et al.* [2] ได้เสนอ SecureSMSPay ซึ่งเป็นระบบการชำระเงินโดยมีการเข้ารหัสลับแบบสมมาตร ระบบนี้ประกอบด้วย 5 ฝ่ายคือ ผู้รับ (Payee) ผู้ชำระเงิน (Payer) ธนาคารผู้รับเงิน (Payee's Bank) ธนาคารของผู้ชำระเงิน (Payer's Bank) และ PG ผู้รับเงินเปิดบัญชีกับธนาคารของตน ส่วนผู้ชำระเงินก็เปิดกับธนาคารของตน มี PG ทำหน้าที่เป็นคนกลางระหว่างธนาคาร การโอนเงินทำจากธนาคารของผู้ชำระเงินที่ธนาคารผู้รับเงินของการชำระเงินผ่านทาง PG

อย่างไรก็ตาม ระบบดังกล่าวมีข้อบกพร่อง คือบางข้อความจะถูกส่งในแบบข้อความที่ไม่มีมีการเข้ารหัสลับ เช่น หมายเลขโทรศัพท์มือถือ และสถานะก็สามารถแก้ไขได้โดยผู้โจมตี นอกจากนี้การรักษาความปลอดภัยของระบบจะขึ้นอยู่กับการเข้ารหัสลับแบบสมมาตรที่ใช้คีย์ร่วมกัน การเปลี่ยนคีย์ของระบบ ได้มาจากค่าแฮชจากการเลื่อนบิตของเซสชันคีย์ปัจจุบัน จะสังเกตได้ว่าคีย์ที่สร้างจากฟังก์ชันแฮชมีความยาวคงที่ ไม่ได้เพิ่มความปลอดภัยจากการโจมตีแบบ Brute-force แต่อย่างใด

นอกจากนี้ Toorani *et al.* [1] เสนอ SSMS โดยใช้การเข้ารหัสแบบ Elliptic-curve ซึ่งให้คุณสมบัติ ความลับของข้อมูล ความคงสภาพของข้อมูล การพิสูจน์ตัวตน รวมถึงการไม่สามารถปฏิเสธความรับผิดชอบได้ นอกจากนั้นโพรโทคอลนี้ยังมีความสามารถในการตรวจสอบคีย์สาธารณะของแต่ละฝ่าย และการส่งต่อความลับได้ ซึ่งเป็นระบบที่ใช้การเข้ารหัสแบบคีย์สาธารณะ จึงจำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้ทำหน้าที่เป็นผู้รับรอง

Hashemi *et al.* [3] เสนอกรอบการชำระเงินมือถือโดยใช้ SMS ที่อธิบายความสัมพันธ์ระหว่าง SMS gateway และ Short Message Service Center (หรือ SMSC) และภาพรวมของเค้าร่างการชำระเงินด้วย SMS แบบต่างๆ โดยใช้ Advanced Encryption Standard (หรือ AES) เพื่อเพิ่มความปลอดภัยให้กับธุรกรรม ซึ่งเป็นวิธีการเข้ารหัสแบบสมมาตร ซึ่งคีย์ที่ใช้ร่วมกันระหว่างลูกค้าและธนาคารมีการกระจายเฉพาะในกรณีที่ ลูกค้าลงทะเบียนใช้บริการครั้งแรก แต่อย่างไรก็ตาม ไม่มีการกล่าวถึงการปรับเปลี่ยนคีย์ในบทความนี้

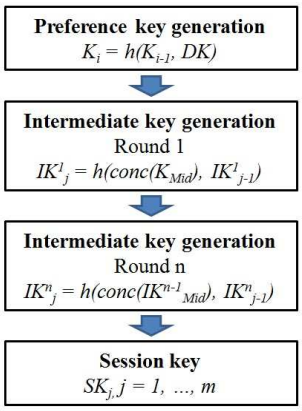
2.3 การสร้างเซสชันคีย์แบบจำกัด และการกระจาย

การสร้างและกระจายคีย์ สามารถแบ่งได้เป็น 2 ประเภท คือ เทคนิคแบบออนไลน์และแบบออฟไลน์ สำหรับการกระจายคีย์แบบออนไลน์จำเป็นต้องมีการส่งคีย์ผ่านเครือข่าย ถึงแม้ว่าจะมีการเข้ารหัสเอาไว้ แต่ก็ยังสามารถถูกดักจับได้ การสร้างและกระจายคีย์แบบออฟไลน์และเทคนิคการสร้างคีย์ครั้งใหม่ไม่จำเป็นต้องมีการส่งในเครือข่าย จึงดักจับไม่ได้แม้กระทั่งบนสายสื่อสารจากข้างต้น เทคนิคการสร้างและกระจายคีย์ได้รับการเสนอ [8, 9, 10, 13, 14, 15] ซึ่ง Kungpisdan *et al.* ได้แนะนำเทคนิคการสร้างคีย์ที่ไม่เพียงแต่มีความปลอดภัยจากการโจมตีเท่านั้น แต่ยังสามารถทำงานได้แบบออฟไลน์ นอกจากนี้ยังมีการนำไปใช้เพื่อเพิ่มความปลอดภัยต่อการทำธุรกรรมทางอินเทอร์เน็ตอีกด้วย

วิธีของ Kungpisdan *et al.*

กำหนดให้อลิซ และบ๊อบใช้ $\{K_{AB}, DK, m\}$ ร่วมกัน ซึ่งคีย์ K_{AB} เป็นคีย์ระยะยาว (Long term key) ระหว่างอลิซและบ๊อบ DK เป็นคีย์กระจาย (Distributed key) และ m เป็นเลขสุ่ม ใช้ m ในการระบุจำนวนคีย์ที่จะสร้าง ซึ่งขึ้นอยู่กับการสุ่มระหว่างคู่ที่แตกต่างกัน $conc(M_1, M_2, M_3)$ แสดงการต่อกันของข้อความ M_1, M_2 และ M_3 ตามลำดับ กระบวนการสร้างคีย์ แสดงดังรูปที่ 1

หลังจากแลกเปลี่ยน $\{K_{AB}, DK, m\}$ กัน อลิซและบ๊อบจะสร้างคีย์ที่ใช้ในการตั้งค่า (preference key) K_i โดยที่ $i = 1$ ถึง m ดังนี้ $K_i = h(K_{i-1}, DK)$, โดยที่ $K_0 = K_{AB}$. ซึ่ง K_i จะถูกใช้เป็นข้อมูลสำหรับการสร้างเซสชันคีย์ต่อไปในกรณีที่จำเป็น หลังจากสร้าง K_i แล้ว สามารถลบ K_{AB} และ DK ออกจากระบบได้



รูปที่ 1: กระบวนการสร้างเซสชันคีย์

ทั้งอลิซและบ๊อบสร้างคีย์กลาง (Intermediate key) เพื่อเพิ่มความยากสำหรับการทำ Cryptanalysis ซึ่งเป็นการเพิ่มความยากในการหาคีย์ที่ใช้ในการตั้งค่าในกรณีที่เซสชันคีย์ถูกดักจับได้ โดยคีย์กลางจะถูกสร้างตามจำนวนรอบที่สูงสุด ซึ่งให้ความปลอดภัยที่สูงกว่า ซึ่งการสร้างคีย์กลางทำได้ดังนี้ $IK^x_j = h(conc(IK^{x-1}_{Mid}), IK^x_{j-1})$, เมื่อ x คือจำนวนรอบ j คือจำนวนของคีย์กลางที่สร้างโดยที่ $j = 1$ ถึง m และ IK^{x-1}_{Mid} คือชุดของ $\{IK^{x-1}_{Mid1}, IK^{x-1}_{Mid2}, IK^{x-1}_{Mid3}\}$ โดยที่ $IK^x_{Mid1} = mid(IK^x_1, IK^x_{rm})$ และ rm คือจำนวนของคีย์กลางที่เหลืออยู่ ในชุด IK^x_j. $IK^x_{Mid2} = mid(IK^x_{Mid1}, IK^x_{rm})$. $IK^x_{Mid3} = mid(IK^x_1, IK^x_{Mid2})$. $IK^1_{Mid1} = K_{Mid1}$, $IK^1_{Mid2} = K_{Mid2}$, และ $IK^1_{Mid3} = K_{Mid3}$ ในการสร้าง K_{Mid1}, K_{Mid2}, และ K_{Mid3} จะเหมือนกันกับการสร้าง IK^x_{Mid1}, IK^x_{Mid2}, IK^x_{Mid3} ตามลำดับ $IK^x_{j-1} = \phi$ คือผลลัพธ์สุดท้ายของการสร้างคีย์กลาง ซึ่งใช้เป็นเซสชันคีย์ SK_j, โดยที่ $j = 1$ ถึง m ซึ่งแสดงได้ดังนี้ $IK^n_1 = SK_1$, $IK^n_2 = SK_2$, ... , $IK^n_m = SK_m$ ซึ่งอลิซและบ๊อบสามารถใช้ SK_j เพื่อความมั่นคงปลอดภัยของการทำธุรกรรม เช่น ใช้เป็นคีย์ในการเข้ารหัส หรือใช้เป็นคีย์สำหรับ Message Authentication Code

เซสชันคีย์ดังกล่าวถูกสร้างขึ้นแบบออฟไลน์ โดยที่แต่ละฝ่ายสามารถสร้างคีย์ที่ใช้ในการรักษาความปลอดภัยของการติดต่อสื่อสารระหว่างกัน โดยไม่ต้องมีการส่งข้อมูลใดผ่านเครือข่าย เมื่อเซสชันคีย์ไม่ต้องมีการส่งผ่านเครือข่ายจะไม่สามารถถูกดักจับ จึงช่วยเพิ่มความมั่นคงปลอดภัยให้แก่การเข้ารหัสแบบสมมาตร

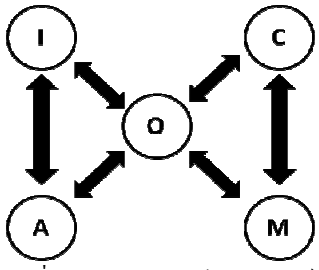
3. โมเดลสำหรับการชำระเงินผ่านข้อความสั้น

เพื่อเป็นการทำความเข้าใจอย่างถ่องแท้ถึงแนวทางการพัฒนาระบบชำระเงินผ่านข้อความสั้น (SMS) นั้น บทความวิจัยฉบับนี้เสนอโมเดลสำหรับการชำระเงินอย่างปลอดภัยผ่านข้อความสั้น ดังแสดงในรูปที่ 2

ระบบชำระเงินผ่านข้อความสั้นประกอบด้วยผู้ที่เกี่ยวข้องจำนวน 5 ส่วน คือ ลูกค้า (Client หรือ *C*), พ่อค้า (Merchant หรือ *M*), ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Operator หรือ *O*), สถาบันการเงินของลูกค้า (Issuer หรือ *I*) และสถาบันการเงินของพ่อค้า (Acquirer หรือ *A*) ภายในระบบ *C* และ *M* เปิดบัญชีกับ *I* และ *A* ตามลำดับ โดยที่การทำธุรกรรมทั้งหมด

กระทำผ่าน *O* ในรูปของการชำระเงินผ่านเว็บไซต์ที่ถูกออกแบบเฉพาะสำหรับโทรศัพท์เคลื่อนที่ การทำธุรกรรมภายในระบบมีทั้งสิ้น 5 ประเภทคือ

1) **Payment Request/Response** เป็นธุรกรรมระหว่าง *C* และ *M* เพื่อร้องขอซื้อ/ขายสินค้าหรือบริการระหว่างกัน ธุรกรรมดังกล่าวสามารถทำผ่าน *O* หรือกระทำระหว่างกันโดยตรงก็ได้
2) **Debit Request/Response** เป็นธุรกรรมระหว่าง *C* และ *I* โดยที่ *C* ร้องขอให้ *I* หักเงินในบัญชีของ *C* เป็นจำนวนเท่ากับค่าสินค้าหรือบริการ
3) **Credit Request/Response** เป็นธุรกรรมที่ *M* ร้องขอให้ *A* นำเงินที่ได้จากการขายสินค้าหรือบริการเข้าสู่บัญชีของ *M* ที่เก็บไว้ที่ *A*
4) **Payment Clearing Request/Response** เป็นธุรกรรมระหว่าง *I* และ *A* เพื่อโอนเงินจากบัญชีของ *C* ไปยังบัญชีของ *M*



รูปที่ 2: กระบวนการสร้างเซสชันคีย์

จากรูปที่ 2 พบว่า ธุรกรรมที่เกิดขึ้นระหว่าง *C* และ *M* จะกระทำผ่าน *O* ในบางกรณี *O* อาจเป็นทั้ง *I* และ *A* ได้ในกรณีที่ *C* และ *M* มีบัญชีที่ *O* เช่น *C* เป็นลูกค้าที่ใช้โทรศัพท์รายเดือน ในขณะที่ *M* ลงทะเบียนและเปิดบัญชีกับ *O* เพื่อเป็นพ่อค้าภายในระบบ ธุรกรรมภายในระบบสามารถแสดงได้ดังนี้

C → O: *Payment Request, Debit Request*

O → M: *Payment Request, Approved/Reject*

M → O: *Payment Response, Credit Request*

O → C: *Payment Response, Debit Response*

O → M: *Credit Response*

แนวทางการทำธุรกรรมข้างต้นจะถูกนำไปใช้ในการออกแบบโพรโทคอลชำระเงินผ่านข้อความสั้นภายในงานวิจัยฉบับนี้ต่อไป

4. โพรโทคอลสำหรับการชำระเงินผ่านข้อความสั้นที่นำเสนอ

4.1 นิยามและสมมติฐาน

โพรโทคอลสำหรับการชำระเงินมือถือโดยใช้ SMS มีสมมติฐานดังต่อไปนี้

- ในระบบประกอบด้วย 3 ฝ่าย คือ ลูกค้า (*C*) พ่อค้า (*M*) และผู้ให้บริการมือถือ (*O*) โดยที่ *C* ใช้มือถือที่ติดตั้งซอฟต์แวร์ที่นำเสนอ และ *M* จดทะเบียนเป็นผู้ค้ากับ *O* ซึ่ง *O* ตั้งตัวเองเป็นเซิร์ฟเวอร์ เรียกว่า SMS Payment Server (SPS) เพื่อให้บริการการชำระเงินกับ *C* และ *M*
- *C* เปิดบัญชีกับ *O* สำหรับใช้บริการโทรศัพท์และใช้ข้อมูล โดยที่ *C* จะถูกเรียกเก็บเงินจาก *O* ทุกสิ้นเดือน
- *{A, B}* คือผู้ที่ติดต่อสื่อสารกัน ขณะที่ *S* หมายถึงเซิร์ฟเวอร์ส่งข้อความ
- ID_A คือสิ่งที่ระบุว่าเป็น *A*
- $\{DK_{AB}, K_{AB}, m_{AB}\}$ เป็นตัวแปรในการสร้างและกระจายเซสชันคีย์ ซึ่งถูกใช้ร่วมกันระหว่าง *A* กับ *B*
- SK_{ABj} โดยที่ $j = 1$ ถึง m คือ เซสชันคีย์ที่ใช้ร่วมกันระหว่าง *A* กับ *B*
- *n* เป็น nonce ใช้เพื่อป้องกันการส่งข้อมูลซ้ำ
- $\{m\}_K$ เป็นข้อความที่เข้ารหัสสมมาตรของข้อความ *m* ด้วยคีย์ *K*
- *h(m)* คือค่าแฮชของข้อความ *m*
- *h(m, K)* เป็นรหัสตรวจสอบข้อความ (MAC) ของข้อความ *m* ที่ใช้คีย์ *K*

4.2 การลงทะเบียนของลูกค้า

อุปกรณ์มือถือต้องติดตั้งซอฟต์แวร์การชำระเงินด้วย SMS ตามโพรโทคอลที่นำเสนอ เมื่อซอฟต์แวร์ถูกดาวน์โหลดไปยังเครื่องของลูกค้า ลูกค้าต้องเข้าสู่ระบบของ SPS เพื่อลงทะเบียน การลงทะเบียนดำเนินการผ่านช่องทางที่ปลอดภัย เช่น TLS (Transport Layer Security) โดยที่ TLS ใช้เพื่อความปลอดภัยในการสื่อสารไร้สาย เรียกว่า WTLS (Wireless Transaction Layer Security) วัตถุประสงค์ของการลงทะเบียน คือ การแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ ระหว่างลูกค้าและผู้ให้บริการ ซึ่งโทรศัพท์มือถือของลูกค้าแต่ละรายอาจติดตั้ง SIM Application Toolkit (หรือ SAT) ซึ่งมีคีย์ที่ใช้ร่วมกับผู้ให้บริการโทรศัพท์มือถืออยู่แล้ว ซึ่งหลังจากการแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กัน ทั้งลูกค้าและผู้ให้บริการ สามารถสร้างเซสชันคีย์ SK_{COj} เมื่อ $j = 1$ ถึง m โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.3

4.3 การชำระเงินโดยตรงกับผู้ให้บริการ

ในส่วนนี้ ผู้วิจัยเสนอโพรโทคอลที่เหมาะสำหรับการชำระเงินระหว่างลูกค้าและให้บริการโทรศัพท์เคลื่อนที่ผ่าน SMS โดยมีสมมติฐานว่าผู้ให้บริการโทรศัพท์เคลื่อนที่ *O* มีผลิตภัณฑ์และบริการให้แก่ลูกค้า เช่น เสียงเรียกเข้าเพลง ดาวน์โหลดซอฟต์แวร์ ซึ่งลูกค้าจะถูกเรียกเก็บเงินตามสิ่งที่ซื้อจากบัญชีของตนที่จะเรียกเก็บเงิน ณ สิ้นเดือน สำหรับโพรโทคอลนี้ การทำธุรกรรมการชำระเงินทำได้ทั้งที่เป็นแบบเติมเงินและจดทะเบียน โดยดำเนินการตามรายละเอียดต่อไปนี้ ในการชำระเงินเติมเงิน ลูกค้าจะต้องซื้อบัตรเงินสด ที่มีขายอยู่ในร้านสะดวกซื้อ แล้วเติมเงินเข้าบัญชีของตน จากนั้นลูกค้าจะสามารถทำธุรกรรมได้ ดังนี้

การร้องขอวงเงิน (Purchase Credit Request)

หลังจากซื้อบัตรและเติมเงินแล้ว ลูกค้า *C* เปิดโปรแกรมขึ้นในมือถือของตน กรอกข้อมูลที่จำเป็น และส่งต่อไปยังผู้ให้บริการ *O*

C → O: $ID_C, T_1, h(SN, CL_1, T_1, SK_{CO}), SN$

โดยที่

- *SN* คือหมายเลขของบัตรเติมเงิน *SN* จะอ้างอิงถึงวงเงิน (CL_T) ที่ลูกค้าสามารถใช้ในการซื้อสินค้าหรือบริการจากผู้ให้บริการ
- ID_C คือส่งที่ใช้ระบุตัวลูกค้า ซึ่งใช้หมายเลขโทรศัพท์มือถือของลูกค้าก็ได้
- T_1 คือเวลาที่ร้องขอวงเงิน

จากข้อมูลข้างต้น ลูกค้าส่ง *SN* ร่วมกับคำร้องขอวงเงิน CL_T จาก *O* ซึ่ง *O* จะพิจารณาวงเงินของลูกค้าจาก *SN* ซึ่งผู้โจมตีไม่สามารถแก้ไข *SN* ได้ แม้ว่าจะถูกส่งในแบบไม่เข้ารหัสก็ตาม เพราะมีการใช้คีย์แฮช $h(SN, CL_T, T_1, SK_{COj})$ ซึ่งเป็นตัวตรวจสอบข้อความกับ SK_{COj} ซึ่งใช้ร่วมกันระหว่าง *C* และ *O* โดยหลังจาก *O* ได้รับคำขอจาก *C* แล้ว *O* จะเพิ่มวงเงิน CL_T เข้าบัญชีของ *C* และส่งข้อความต่อไปนี้ให้ *C*

O → C: $T_1, T_2, h(CL_T, T_{S1}, T_2, SK_{COj+1})$

เมื่อ T_2 เป็นการประทับเวลา ขณะออกวงเงินให้ลูกค้า จากข้อความข้างต้น *O* เพิ่มวงเงินให้กับบัญชีของ *C* ตาม CL_T.

การชำระเงิน (Making Payment)

หลังจากเรียกดูสินค้าหรือบริการแล้ว *C* สามารถชำระเงินโดยการส่งข้อความต่อไปนี้ให้ *O*

C → O: $ID_C, \{T_1, OI\}_{SKcoj}, h(T_1, OI, ID_C, SK_{COj})$

เมื่อ

- T_1 หมายถึง timestamp เมื่อร้องขอเพื่อชำระเงิน
- *OI* คือ *{TID, Price, OD}* *TID* คือ หมายถึงหมายเลขของการทำรายการ *Price* คือราคาของสินค้าหรือบริการ และ *OD* หมายถึงคำสั่งที่มีคำอธิบายรายละเอียดของผลิตภัณฑ์หรือบริการที่ซื้อ

หลังจากได้รับคำขอ *O* จะตรวจสอบวงเงินที่มีอยู่ของ *C* และเปรียบเทียบกับราคา ถ้า *C* มีเงินเพียงพอ *O* ข้อความ *Yes* กลับไปยัง *C* แต่ถ้าไม่ จะตอบสนองด้วยข้อความ *No* ดังนี้

O → C: $Yes/No, h(Yes/No, CL_{RM}, h(T_1, OI, ID_C, SK_{COj}), SK_{COj+1})$

CL_{RM} เป็นเงินคงเหลือในบัญชี ทั้งนี้สำหรับการชำระเงินของระบบลงทะเบียน (postpaid) สามารถดำเนินการได้ในลักษณะเดียวกับการชำระเงินระบบจ่ายล่วงหน้า (prepaid) โดยไม่ต้องมีโพรโทคอลเพิ่มเติม เนื่องจากลูกค้าได้รับวงเงิน CL_T จำกัด จากผู้ให้บริการอยู่แล้ว

4.4 SMS-based Operator-Assisted Mobile Payment Protocol

ตามรูปแบบที่นำเสนอในส่วนที่ 2.1 ในส่วนนี้ผู้วิจัยเสนอโพรโทคอล SMS-based operator-assisted mobile payment (SOMP) โดยที่ในโพรโทคอลนี้ ผู้ให้บริการจะเป็นผู้ที่ช่วยให้ลูกค้าดำเนินธุรกรรมการชำระเงินกับพ่อค้าได้ ซึ่งมีสมมติฐานดังต่อไปนี้ คือ ระบบประกอบด้วยลูกค้า (*C*) พ่อค้า (*M*) และผู้ให้บริการ (*O*) ลูกค้าและพ่อค้าเปิดบัญชีกับ *O* แล้ว *C* ได้รับอนุมัติวงเงินจากผู้ให้บริการ ซึ่งลูกค้าจะถูกเรียกเก็บเงินในตอนสิ้นเดือนโดยผู้ให้บริการสำหรับสินค้าหรือบริการที่ซื้อไป โปรแกรมในฝั่งลูกค้าทำหน้าที่ 2 ส่วน คือ การค้นหาสินค้าและการชำระเงิน โดยที่ พ่อค้า หมายถึงผู้ที่ขายสินค้าหรือบริการบนมือถือ ซึ่งดำเนินการโดยผู้ให้บริการมือถือ รายละเอียดของ SOMP มีดังนี้

1) หลังจากตัดสินใจเลือกใช้บริการการชำระเงินแล้ว *C* สร้างเซสชันโดยใช้ WTLS และแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กับ *O* จากนั้น *C* และ *O* จะสร้างเซสชันคีย์ K_{COj} โดยที่ $j = 1$ ถึง m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.3
2) *M* แลกเปลี่ยน $\{K_{MO}, DK_{MO}, m_{MO}\}$ กับ *O* ทั้ง 2 ฝ่ายสร้างเซสชันคีย์ K_{MOj} โดยที่ $j = 1$ ถึง m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.3
3) *C* เปิดโปรแกรมในมือถือของตน เพื่อเรียกดูสินค้าหรือบริการ เมื่อเลือกสินค้าหรือบริการแล้ว *C* ดำเนินการขอสั่งซื้อสินค้าหรือบริการ ดังต่อไปนี้

C → O: $ID_C, T, \{ID_M, OI, T, h(OI, K_{CMj})\}_{KCOj}$

O → M: $\{OI, h(OI, K_{CMj}), h(OI, K_{COj+1}), T\}_{KMOj}$

M → O: $\{Yes/No, h(Yes/No,OI, K_{CMj+1})\}_{KMOj+1}$

O → C: $\{Yes/No, CL_{RM}, h(Yes/No, OI, K_{CMj+1}), h(OI, K_{MOj+1})\}_{KCOj+1}$

เมื่อ *T* คือการประทับเวลา ซึ่งหลังจาก *C* คลิกปุ่มเช็คเอาต์จะมีเซสชันใหม่เกิดขึ้นระหว่าง *C* และ *M* ชุดของคีย์ $\{K_{CM}, DK_{CM}, m_{CM}\}$ จะถูกใช้งานร่วมกัน ทั้งสองฝ่ายสามารถสร้างเซสชันคีย์ SK_{CMj} โดยที่ $j = 1$ ถึง m ได้โดยใช้เทคนิคของการสร้างและการจายคีย์แบบออฟไลน์ จากข้อความข้างต้นจะสังเกตว่า *O* ไม่สามารถสร้างข้อความแรกได้ เพราะมี $h(OI, K_{CMj})$ รวมอยู่ ซึ่งถูกใช้ร่วมกันระหว่าง *C* และ *M* เท่านั้น

5. การวิเคราะห์คุณสมบัติความมั่นคงปลอดภัย

5.1 การเข้ากันได้กับระบบการส่งข้อความสั้นที่มีอยู่

โพรโทคอลที่เสนอ ถูกออกแบบมาโดยให้ความสำคัญเรื่องความเข้ากันได้กับโครงสร้างพื้นฐานของ SMS ที่มีอยู่ ซึ่งข้อความถูกจำกัดอยู่ที่ 160 ตัวอักษร (หรือ 160 ไบต์) จึงพยายามลดขนาดของข้อความโดยการใช้ฟังก์ชันแฮชและรหัสตรวจสอบข้อความ ที่ลดขนาดไป 20 ไบต์ (SHA - 1) นอกจากนี้ การใช้การเข้ารหัสแบบสมมาตรเพื่อสร้างข้อความตามแบบของผู้วิจัย ไม่มีข้อความในโพรโทคอลที่เสนอที่มีขนาดใหญ่กว่า 160 ไบต์

นอกจากนี้ มีการใช้การเข้ารหัสแบบสมมาตร หรือฟังก์ชันแฮชในการสร้างผลลัพธ์ออกมาในรูปแบบไบนารี ดังนั้น เพื่อให้แต่ละข้อความที่ใช้ร่วมกับโครงสร้างพื้นฐานของ SMS ที่มีอยู่ อัลกอริทึม Binary - to - ASCII เช่น BASE64 จึงถูกนำไปใช้ก่อนส่งข้อความ

5.2 ความมั่นคงปลอดภัยของระบบ

ประเด็นหลักที่แสดงให้เห็นว่า การทำธุรกรรมทางการเงินผ่านมือถือมีความปลอดภัย คือโพรโทคอลการชำระเงินมือถือนั้น ควรมีคุณสมบัติในการรักษาความปลอดภัยที่จำเป็น เช่น การรักษาความลับข้อมูล ความคงสภาพของข้อมูล การพิสูจน์ตรวจสอบ และการส่งต่อความลับ

โพรโทคอลที่เสนอ ใช้การเข้ารหัสลับแบบสมมาตรที่มีเฉพาะบุคคลที่มีคีย์ร่วมกันเท่านั้นที่สามารถถอดรหัสลับได้ ส่วนความคงสภาพของ

ข้อความใช้รหัสการตรวจสอบข้อความ (MAC) เพื่อตรวจสอบว่าผู้โจมตีจะไม่สามารถแก้ไขข้อความได้โดยที่ไม่ถูกตรวจพบ ซึ่งมีเฉพาะบุคคลที่รู้คีย์ MAC เท่านั้น ที่สามารถตรวจสอบความคงสภาพของข้อความได้ ในการตรวจสอบข้อความนั้นใช้ทั้งการเข้ารหัสลับสมมาตร รหัสตรวจสอบข้อความ นอกจากนี้งานวิจัยนี้ยังให้ความสำคัญเกี่ยวกับความปลอดภัยของเซสชันคีย์ ซึ่งไม่ควรนำกลับมาใช้ใหม่ ตามโพรโทคอลที่เสนอ ใช้เทคนิคการสร้างและกระจายคีย์แบบจำกัด เพื่อให้แต่ละข้อความใช้เซสชันคีย์ใหม่ ไม่มีการส่งเซสชันคีย์เดิมในการส่งข้อความ ซึ่งจะช่วยลดโอกาสที่จะถูกโจมตีได้

โพรโทคอลที่เสนอ สามารถตอบสนองในเรื่องการส่งต่อความลับได้ หมายถึงระบบยังคงมีความปลอดภัยอยู่ แม้เซสชันคีย์จะถูกดักจับได้ และแกะรหัสสำเร็จจนกระทั่งได้ SK_{CM1} ซึ่งใช้ร่วมกันระหว่าง C กับ M ผู้โจมตีก็ไม่สามารถใช้ SK_{CM1} สำหรับถอดรหัสข้อความใด ๆ เพราะคีย์นั้นใช้ได้เพียงครั้งเดียว ซึ่งเป็นไปตามเทคนิคที่นำเสนอใน [8] คือ ผู้โจมตีไม่สามารถสร้าง SK_{CM2} จาก SK_{CM1} ได้

5.3 การวิเคราะห์ค่าใช้จ่าย

เมื่อมีการเพิ่มการเข้ารหัสลับเข้ามา มีผลให้ขนาดของข้อมูลที่ส่งยาวมากขึ้น ทำให้ค่าใช้จ่ายในการส่ง SMS เพิ่มขึ้นเป็นสองเท่า แต่เนื่องจากในปัจจุบันค่าบริการส่ง SMS มีการแข่งขันจนราคาถูกมาก จึงทำให้ค่าใช้จ่ายที่เกิดขึ้นนี้ถือว่าไม่สูงเกินไป

6. สรุปผลงานวิจัย

ในบทความนี้ ผู้วิจัยพบว่า SMS เป็นช่องทางสื่อสารระหว่างผู้ใช้กับผู้ใช้ และระหว่างผู้ใช้กับผู้ให้บริการมือถือ มากที่สุด แต่วิธีที่ใช้รักษาความปลอดภัยในการทำธุรกรรมการชำระเงินผ่าน SMS ไม่เพียงพอ เพราะยังขาดทั้งคุณสมบัติการรักษาความปลอดภัยและประสิทธิภาพ บทความนี้ผู้วิจัยเสนอโพรโทคอลการชำระเงินมือถือด้วย SMS ที่เรียกว่า SOMP ซึ่งช่วยให้ผู้ใช้ซื้อสินค้าหรือบริการจากผู้ให้บริการมือถือ และร้านค้าได้ โดยโพรโทคอลนี้ไม่เพียงแต่ให้คุณสมบัติด้านความปลอดภัยที่จำเป็นเท่านั้น แต่ยังเข้ากันได้กับโครงสร้างพื้นฐานของ SMS ที่มีอยู่ในปัจจุบันอีกด้วย

เอกสารอ้างอิง

[1] M. Toorani and A. A. B. Shirazi, SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems, Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC'08), Marrakech, July 6-9, 2008, pp. 700-705.

[2] H. Harb, H. Farahat, and M. Ezz, SecureSMSPay: Secure SMS Mobile Payment Model, Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification 2008, Guiyang, Aug 20-23, 2008, pp. 11-17.

[3] M. R. Hashemi and E. Soroush, A Secure m-Payment Protocol for Mobile Devices, Proceedings of the Canadian Conference on Electrical and Computer Engineering 2006 (CCECE'06), May 2006, Ottawa, Ont., pp. 294-297.

[4] P. Soni, M-Payment Between Banks Using SMS, Proceedings of the IEEE, Vol. 98(6), June 2010, ISSN: 0018-9219, pp. 903-905.

[5] S. Kungpisdan, Accountability in Centralized Payment Environments, Proceedings of the 9th International Symposium on Communications and Information Technology 2009, Sept 28-30, 2009, Incheon, pp. 1022-1027.

[6] S. Kungpisdan and T. Thai-udom, Securing Micropayment Transactions Over Session Initiation Protocol, Proceedings of the 9th International Symposium on Communications and Information Technology 2009, Sept 28-30, 2009, Incheon, pp. 187-192.

[7] X. Wu, O. Dandash, and P. D. Le, The Design and Implementation of A Smartphone Payment System Based on Limited-used Key Generation Scheme, Journal of Theoretical and Applied Electronic Commerce Research, Vol. 1(2), Aug 2006, pp. 1-11.

[8] S. Kungpisdan and S. Metheekul, A Secure Offline Key Generation With Protection Against Key Compromise, Proceedings of the 13th World Multi-conference on Systemics, Cybernetics, and Informatics 2009, Orlando, USA.

[9] O. Dandash *et al.*, Fraudulent Internet Banking Payments Prevention using Dynamic Key, Journal of Networks, Vol.3(1), Academy Publisher, pp. 25-34, 2008.

[10] S. Kungpisdan, P.D. Le, and B. Srinivasan, "A Limited-Used Key Generation Scheme for Internet Transactions", Lecture Notes in Computer Science, Vol. 3325, 2005.

[11] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, and M. Waidner, Design, "Implementation, and Deployment of the *i*KP Secure Electronic Payment System", *IEEE Journal of Selected Areas in Communications*, 2000.

[12] Mastercard and Visa, "SET Protocol Specifications", 1997. http://www.setco.org/set_specifications.html

[13] Li, Y. and Zhang, X., 2004. A Security-enhanced One-time Payment Scheme for Credit Card. *Proc. of the Int'l Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications*,

[14] S. Kungpisdan, B. Srinivasan, and P.D. Le, Lightweight Mobile Credit-card Payment Protocol, Lecture Notes in Computer Science, Vol. 2904, 2003, pp. 295-308.

[15] A. D. Rubin and R.N. Wright, Off-line Generation of Limited-Use Credit Card Numbers, Lecture Notes in Computer Science, Vol. 2339, 2002, pp. 196