โพรโทคอลการชำระเงินผ่านเครือข่ายไร้สายผ่านผู้ให้บริการสำหรับธุรกรรมชนิดชำระก่อนและชำระทีหลังบนโพรโทคอล SIP

Mobile Payment Protocol for Prepaid and Postpaid on SIP Protocol

ชาลี ธรรมรัตน์[1] เมฆินทร์ วรศาสตร์[2] เสฏฐ์ศักดิ์ เตรียงตั้ง[3] และ ศุภกร กังพิศดาร[4]
คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร
140 ถนนเชื่อมสัมพันธ์ เขตหนองจอก กรุงเทพมหานคร 10530 โทรศัพท์ 02-988-3655 ต่อ 4111
Emails: [1]chalee@miss.in.th, [2]maykin@miss.in.th, [3]satesak@miss.in.th, [4]supakorn@mut.ac.th

บทคัดย่อ

การทำธุรกรรมจำนวนมากนิยมกระทำผ่านเครือข่ายไร้สายทำให้ผู้ใช้งานได้รับความสะดวกรวดเร็วเพราะสามารถกระทำในขณะเคลื่อนที่อยู่ได้ งานวิจัยจำนวนมากได้นำเสนอโพรโทคอลการชำระเงินผ่านเครือข่ายไร้สายซึ่งยังขาดคุณสมบัติด้านความมั่นคงปลอดภัย บทความวิจัยนี้เสนอวิธีการชำระเงินผ่านโพรโทคอล SIP (Session Initiation Protocol) เพื่อความมั่นคงปลอดภัยที่เพิ่มขึ้น เช่น การรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูล การพิสูจน์ตัวจริง และยังนำเทคนิคการกระจายเซสชันคีย์แบบออฟไลย์ มาใช้งานร่วมด้วยเพื่อการป้องกันการโจมตีในแบบ Man in the middle (MITM)

คำสำคัญ: โพรโทคอลการเข้ารหัสลับ, การชำระเงินผ่านเครือข่ายไร้สาย, โพรโทคอลการชำระเงิน, Session Initiation Protocol, ความมั่นคงปลอดภัยของ SIP, โพรโทคอลความมั่นคงปลอดภัย

Abstract

The number of transactions performed through the wireless network so users can get more convenience because each transaction can be completed while moving. Many mobile payment protocol researches have been proposed but still lack of security feature. Our research proposes mobile payment by using SIP protocol and also enhances more security such as confidentiality, Integrity, authentication and off-line key distribution technique has been used to prevent Man in the middle (MITM)

Keywords: Cryptography Protocol, Mobile Payment Protocol, Payment Protocol, Session Initiation Protocol, SIP Security Protocol, Security Protocol

1. บทนำ

ปัจจุบันโพรโทคอล SIP ถูกนำมาใช้งานอย่างแพร่หลายและเป็นโพรโทคอลที่มีขนาดเล็ก มีการติดต่อสื่อสารที่ไม่ซับซ้อน ซึ่งนำไปใช้ในการติดต่อสื่อสารผ่านเครื่อข่ายอินเทอร์เน็ต เช่น VoIP การส่งข้อความ สื่อมัลติมีเดีย และการประชุมทางไกล (Video Conference) นอกจากนี้ยังสามารถนำมาประยุกต์ใช้กับการทำธุรกรรมผ่านโทรศัพท์มือถือ หรือการชำระเงินผ่านระบบโทรศัพท์มือถือ ซึ่งโทรศัพท์มือถือในปัจจุบันมีความสามารถนอกจากการใช้เป็นอุปกรณ์โทรศัพท์พกพา แต่ยังสามารถนำมาใช้ในการส่งข้อมูลผ่านเครือข่ายการสื่อสารโทรศัพท์เคลื่อนที่ยุคที่ 3 หรือยุคของ 3G ที่ได้รับความนิยมอย่างมาก เนื่องจากมีต้นทุนต่ำและเร็วกว่าการทำธุรกรรมผ่าน SMS

งานวิจัยที่มีอยู่ [1, 2, 3, 4] ได้นำเสนอการชำระเงินผ่านข้อความสั้น (Short Message Service หรือ SMS) ที่มีความมั่นคงปลอดภัยแต่ยังไม่เพียงพอและงานวิจัย [12, 13] ได้นำเสนอช่องโหว่ของโพรโทคอล SIP ในการคิดค่าใช้จ่ายจากการโจมตีแบบ MITM

งานวิจัยที่นำเสนอนี้ได้เพิ่มความมั่นคงปลอดภัย ในด้านการรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูล การพิสูจน์ตัวจริง และรูปแบบการเข้ารหัสลับแบบสมมาตรเป็นส่วนใหญ่ การเข้ารหัสลับจึงมีน้ำหนักเบา เหมาะสำหรับการทำธุรกรรมบนเครือข่ายไร้สายที่มีทรัพยากรจำกัด และยังสามารถป้องกันการโจมตีแบบ MITM ได้โดยใช้เทคนิคการกระจายเซสชันคีย์แบบออฟไลน์

โครงสร้างของงานวิจัยฉบับนี้มีดังต่อไปนี้ บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 แสดงงานวิจัยที่นำเสนอ บทที่ 4 เสนอการวิเคราะห์ความมั่นคงปลอดภัยของโพรโทคอลที่นำเสนอ บทที่ 5 สรุปผลการวิจัย

2. ทฤษฎีที่เกี่ยวข้อง

2.1 การชำระเงินผ่านเครือข่ายไร้สาย

ระบบการชำระเงินทั่ว [9] ไปประกอบด้วย 5 ฝ่าย คือ Client (ลูกค้า) Merchant (พ่อค้า) Payment Gateway (หรือ PG) Issuer (สถาบันการเงินของลูกค้า) และ Acquirer (สถาบันการเงินของร้านค้า)

การดำเนินการของ issuer และ acquirer กระทำผ่านอินเทอร์เน็ต การตัดเงินจากการชำระเงินกระทำภายในเครือข่ายระหว่างธนาคาร โดยธุรกรรมดังกล่าวนั้นมี 3 ลักษณะ คือ การชำระเงิน การหักเงิน และการเพิ่มเงิน

การชำระเงิน (Payment) เป็นปฏิสัมพันธ์ที่เกิดขึ้นเมื่อลูกค้าต้องการซื้อสินค้าหรือบริการกับพ่อค้า รวมถึงพ่อค้าส่งใบเสร็จรับเงินการชำระเงินให้ลูกค้า การตัดเงินเกิดขึ้นที่ฝั่งลูกค้า โดยส่งคำขอไปยัง PG (ในนามของ (Issuer) เพื่อหักเงินตามจำนวนที่ต้องการชำระออกจากบัญชีของลูกค้า และแจ้งลูกค้าว่าจำนวนเงินที่ต้องการถูกหักจากบัญชีของลูกค้าแล้ว การเพิ่มเงินทำโดยพ่อค้า โดยการร้องขอ PG (ในนามของ Acquirer) เพื่อขอโอนเงินไปยังบัญชีของพ่อค้า แล้วแจ้งพ่อค้าว่ามีการโอนเข้าบัญชีพ่อค้าเรียบร้อยแล้ว มีธุรกรรมในหลายโพรโทคอลการชำระเงิน [3, 4] 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)
โดย C, M, PG คือ ลูกค้า พ่อค้า และ Payment Gateway

2.2 Session Initiation Protocol

โพรโทคอล SIP [11] ทำหน้าที่ในการสร้างการเชื่อมต่อ ยกเลิกการเชื่อมต่อของ VoIP และเป็นโพรโทคอลที่อยู่ในระดับชั้นแอพพลิเคชั่น (Application Layer) โพรโทคอล SIP มีลักษณะเป็น text-based protocol มีการใช้ส่วนประกอบร่วมกับโพรโทคอล HTTP และโพรโทคอล SMTP (Simple Mail Transfer Protocol) การส่งข้อมูลของโพรโทคอล SIP มีพื้นฐานมาจากการรับส่งข้อมูลของโพรโทคอล HTTP โดยมีการส่งข้อความ HTTP Request แล้วจึงรับการตอบกลับด้วยข้อมูล HTTP Response จาก HTTP Server โพรโทคอล SIP ได้นำเฮดเดอร์ และการแปลงค่าต่างๆ และ Response code เกือบทั้งหมดของโพรโทคอล HTTP มาปรับใช้ในรูปแบบของโพรโทคอล SIP

2.3 Harb *et al.*

Harb *et al.* [3] ได้เสนอ SecureSMSPay เป็นระบบการชำระเงินโดยมีการเข้ารหัสลับแบบสมมาตร ระบบนี้ประกอบด้วย 5 ฝ่าย คือ ผู้รับ (Payee) ผู้ชำระเงิน (Payer) ธนาคารผู้รับเงิน (Payee's Bank) ธนาคารของผู้ชำระเงิน (Payer's Bank) และ PG ผู้รับเงินเปิดบัญชีกับธนาคารของตน ส่วนผู้ชำระเงินก็เปิดกับธนาคารของตน โดยที่ PG ทำหน้าที่เป็นคนกลางระหว่างธนาคาร ในการโอนเงินทำจากธนาคารของผู้ชำระเงินไปที่ธนาคารของผู้รับเงินผ่านทาง PG

อย่างไรก็ตาม ระบบดังกล่าวมีข้อบกพร่อง โดยที่ไม่มีมีการเข้ารหัสลับข้อมูล เช่น หมายเลขโทรศัพท์มือถือ และสถานะก็สามารถแก้ไขได้โดยผู้โจมตีนอกจากนี้การรักษาความปลอดภัยของระบบขึ้นอยู่กับการเข้ารหัสลับแบบสมมาตรที่ใช้คีย์ร่วมกัน การเปลี่ยนคีย์ของระบบ ได้มาจากค่าแฮชจากการเลื่อนบิตของเซสชันคีย์ปัจจุบัน สังเกตได้ว่าคีย์ที่สร้างจากฟังก์ชันแฮชมีความยาวคงที่ ไม่ได้เพิ่มความมั่นคงปลอดภัยจากการโจมตีแบบ Brute-force แต่อย่างใด

2.4 Toorani *et al.*

Toorani *et al.* [2] เสนอ SSMS โดยใช้การเข้ารหัสลับแบบ Elliptic-curve มีคุณสมบัติการรักษาความลับของข้อมูล คงสภาพของข้อมูล การพิสูจน์ตัวจริง และการไม่สามารถปฏิเสธความรับผิดชอบได้ โพรโทคอลนี้ยังมีความสามารถในการตรวจสอบคีย์สาธารณะของแต่ละฝ่าย และมีคุณสมบัติการส่งต่อความลับ ซึ่งเป็นระบบที่ใช้การเข้ารหัสแบบคีย์สาธารณะ จึงจำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้ทำหน้าที่เป็นผู้รับรอง

2.5 Hashemi *et al.*

Hashemi *et al.* [4] นำเสนอเทคนิคการชำระเงินผ่านมือถือ โดยอธิบายความสัมพันธ์ระหว่าง SMS gateway และ Short Message Service Center (หรือ SMSC) และภาพรวมของการชำระเงินด้วย SMS แบบต่างๆ โดยใช้ Advanced Encryption Standard (AES) ซึ่งเป็นวิธีการเข้ารหัสลับแบบสมมาตรซึ่งคีย์ที่ใช้ระหว่างลูกค้าและธนาคารมีการกระจายในเฉพาะกรณีที่ลูกค้าลงทะเบียนใช้บริการครั้งแรก แต่อย่างไรก็ตาม ไม่มีการกล่าวถึงการปรับเปลี่ยนคีย์ในบทความนี้

2.6 Kungpisdan *et al.*

Kungpisdan *et al.* [5] ได้นำเสนอวิธีการสร้างและกระจายคีย์แบบออฟไลน์ ซึ่งมีการสร้างและกระจายเซสชันคีย์โดยที่ไม่ต้องมีการส่งคีย์ดังกล่าวผ่านเครือข่าย [10] มีจุดเด่นเหนือเทคนิคการกระจายคีย์แบบออนไลน์ โดยเทคนิคการสร้างและกระจายคีย์แบบต่างๆ ถูกนำเสนอ [5, 6, 8, 9] โดยที่ Kungpisdan et al. ได้แนะนำเทคนิคการสร้างคีย์แบบออฟไลน์ที่มีความมั่นคงปลอดภัยจากการโจมตีได้เป็นอย่างดี

2.7 Zhang *et al.*

Zhang *et al.* [12] นำเสนอตัวอย่างการโจมตีของ Man-in-the-Middle (MITM) โดยนำเสนอรูปแบบการโจมตีของ MITM บนโพรโทคอล SIP ที่เกิดขึ้นกับผู้ให้บริการ VoIP Service ในปัจจุบัน 4 รูปแบบ Fake Busy Billing Attack, Invite Replay Billing Attack, Bye Delay Billing Attack Bye Drop Billing Attack ทำให้การคิดค่าใช้จ่ายของผู้ให้บริการมีความผิดพลาด

3. งานวิจัยที่นำเสนอ

เพื่อแก้ปัญหาและข้อจำกัดของงานวิจัยที่มีอยู่ งานวิจัยฉบับนี้นำเสนอโพรโทคอลใหม่สำหรับการชำระค่าสินค้าและบริการบนโพรโทคอล SIP โดยนำเทคนิคการสร้างและกระจายเซสชันคีย์แบบออฟไลน์มาใช้ เพื่อความมั่นคงปลอดภัยมากยิ่งขึ้น

3.1 นิยามและสมมติฐาน

ลูกค้า (Client หรือ *C*) คือ ผู้ที่สั่งซื้อสินค้าหรือบริการ, พ่อค้า (*Merchant* หรือ *M*) คือ ผู้ที่ขายสินค้าหรือบริการ, Mobile Operator (หรือ *O*) คือ ผู้ให้บริการโทรศัพท์มือถือ โดยที่ *C* ใช้อุปกรณ์มือถือที่ติดตั้งซอฟต์แวร์ที่นำเสนอ และ *M* จดทะเบียนเป็นผู้ค้ากับ *O* ซึ่ง *O* ตั้งตัวเองเป็นเซิร์ฟเวอร์ เรียกว่า Payment Server *(PS)* เพื่อให้บริการการชำระเงินกับ *C* และ *M*

- SK_{ABj} โดยที่ $j=1...m$ คือ เซสชันคีย์ใช้ร่วมกันระหว่าง *A* กับ *B*
- $\{m\}_K$ การเข้ารหัสลับแบบสมมาตรของข้อความ m ด้วยคีย์ *K*
- *h(m)* คือค่าแฮชของข้อความ *m*
- *h(m, K)* เป็นรหัสพิสูจน์ตัวจริงข้อความ (MAC) ของข้อความ *m* ที่ใช้คีย์ *K*
- *C* เปิดบัญชีกับ *O* สำหรับใช้บริการโทรศัพท์และใช้ข้อมูล

3.2 การลงทะเบียนของลูกค้า

อุปกรณ์มือถือต้องติดตั้งซอฟต์แวร์การชำระเงิน เมื่อซอฟต์แวร์ถูกดาวน์โหลดไปยังเครื่องของลูกค้า ลูกค้าต้องเข้าสู่ระบบการลงทะเบียนซึ่งดำเนินการผ่านช่องทางที่มีความมั่นคงปลอดภัย เช่น WTLS (Wireless Transaction Layer Security) ซึ่งวัตถุประสงค์ของการลงทะเบียน คือ การแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ ระหว่างลูกค้าและผู้ให้บริการ หลังจากการแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กัน ทั้งลูกค้าและผู้ให้บริการ สามารถสร้างเซสชันคีย์ SK_{COj} เมื่อ $j=1...m$ โดยใช้เทคนิค [6]

3.3 การพิสูจน์ตัวจริง (Authentication Protocol)

ก่อนที่ *C* จะชำระค่าสินค้าหรือบริการ *C* แลกเปลี่ยน $\{K_{CP}, DK_{CP}, m_{CP}\}$ แล้วทั้ง *C* และ *P* สร้างเซสชันคีย์ SK_{CPj} เมื่อ $j=1...m$ โดยใช้เทคนิคการสร้างคีย์ที่แสดงในส่วน 2.6 และเพื่อขอ Username, Password ใช้พิสูจน์ตัวจริงกับ *P* โดย *C* ส่งข้อความดังนี้

C→P (INVITE)

From: *Alice,* $\{Alice\}_{SKCO}$, *h{Alice,* SK_{CP}*}@domain1.com*

To: $\{Bob, \{Bob\}_{SKCO}\}_{SKCP}$*@domain1.com*

P→C (407 Authentication)

P ส่งข้อความ 407 Proxy Authentication Required กลับไปยัง C เพื่อร้องขอการพิสูจน์ตัวจริง

C→P (INVITE)

From: *Alice,* $\{Alice\}_{SKCO}$, *h(Alice,* SK_{PC}*)@domain1.com*

To: $\{Bob, \{Bob\}_{SKCO}\}_{SKCP}$*@domain1.com*

Body: $h(nonce, Username, Password, SK_{CPj+1})$

P→O (INVITE)

From: $\{Alice\}_{SKCO}$*@domain1.com*

To: Bob, $\{Bob\}_{SKCO}$*@domain1.com*

O→P (180 Ringing)

From: *Bob,* $\{Bob\}_{SKCO}$, *h(Bob,* SK_{CP}*)@domain1.com*

To: *{Alice,* $\{Alice\}_{SKCO}\}_{SKPO}$*@domain1.com*

P→C (Ringing)

From: $\{Bob\}_{SKCO}$*@domain1.com*

To: *Alice,* $\{Alice\}_{SKCO}$*@domain1.com*

โดยที่ *P* คือ Proxy Server ของผู้ให้บริการโทรศัพท์เคลื่อนที่

3.4 การร้องขอวงเงิน

โดยสมมติฐานว่าผู้ให้บริการโทรศัพท์เคลื่อนที่มีสินค้า หรือบริการ เช่น เสียงเรียกเข้า เพลง และดาวน์โหลดซอฟต์แวร์ ซึ่งลูกค้าจะถูกเรียกเก็บเงินตามสิ่งที่ซื้อจากบัญชีของตน โดยทำการเติมเงินได้ 2 รูปแบบ คือ แบบลงทะเบียน (Postpaid) และแบบจ่ายเงินล่วงหน้า (Prepaid)

3.4.1 การเติมเงินแบบจ่ายเงินล่วงหน้า (Prepaid)

หลังจากซื้อบัตรและเติมเงินเรียบร้อยแล้ว *C* เปิดโปรแกรมในมือถือของตนเองและกรอกข้อมูลที่จำเป็น แล้วส่งไปให้ผู้ให้บริการ *O* ดังนี้

C→P (INVITE)

From: *Alice,* $\{Alice\}_{SKCOj+1}$, $h(Alice, SK_{CPj+1})$*@domain1.com*

To: $\{Bob, \{Bob\}_{SKCOj+1}\}_{SKCPj+1}$*@domain1.com*

Body: $ID_C, T_1, \{CL_T, h(CL_T, T_1, SK_{COj+1})\}_{SKCOj+1}$

P→O (INVITE)

From: $\{Alice\}_{SKCOj+1}$*@domain1.com*

To: *Bob,* $\{Bob\}_{SKCOj+1}$*@domain1.com*

Body: $ID_C, T_1, \{CL_T, h(CL_T, T_1, SK_{COj+1})\}_{SKCOj+1}$

O→P (180 Ringing)

From: *Bob,* $\{Bob\}_{SKCOj+1}$, $h(Bob, SK_{POj+1})$*@domain1.com*

To: $\{Alice, \{Alice\}_{SKCOj+1}\}_{SKPOj+1}$*@domain1.com*

Body: $T_1, T_2, h(CL_R, T_1, T_2, SK_{COj+1})$

P→C (180 Ringing)

From: $\{Bob\}_{SKCOj+1}$*@domain1.com*

To: *Alice,* $\{Alice\}_{SKCOj+1}$*@domain1.com*

Body: $T_1, T_2, h(CL_R, T_1, T_2, SK_{COj+1})$

C→P (200 OK)

From: *Alice, {Alice}$_{SKCOj+1}$, h{Alice, SK$_{CPj+1}$}@domain1.com*

To: *{Bob, {Bob}$_{SKCOj+1}$}$_{SKCP}$@domain1.com*

P→O (200 OK)

From: *{Alice}$_{SKCOj+1}$@domain1.com*

To: *Bob, {Bob}$_{SKCOj+1}$@domain1.com*

โดยที่ *SN* คือ หมายเลขบัตรเติมเงินใช้อ้างอิงวงเงิน *(CL$_T$)* ที่ *C* ใช้อ้างอิงการซื้อขายสิ้นค้าหรือบริการและ *C* จะถูกเรียกเก็บเงินจาก *O* ทุกสิ้นเดือนเมื่อการทำธุรกรรมสมบรูณ์

3.4.2 การเติมเงินแบบลงทะเบียน (Postpaid)

ถ้า *C* ทำธุรกรรมที่มีราคามากกว่าจำนวนเงินที่มีอยู่ในบัญชี *C* จะต้องทำการร้องขอวงเงินจากผู้ให้บริการโทรศัพท์เคลื่อนที่ และการขอวงเงินจะไม่เกินวงเงินของการให้แต่ละเดือน ดังนี้

C→P (INVITE)

From: *Alice, {Alice}$_{SKCOj+1}$, h(Alice,SK$_{CPj+1}$)@domain1.com*

To: *{Bob, {Bob}$_{SKCOj+1}$}$_{SKCPj+1}$@domain1.com*

Body: *ID$_C$, T$_1$, SN, h(CL$_T$, SN, SK$_{COj+1}$)*

P→O (INVITE)

From: *{Alice}$_{SKCOj+1}$@domain1.com*

To: *Bob, {Bob}$_{SKCOj+1}$@domain1.com*

Body: *ID$_C$, T$_1$, SN, h(CL$_T$, SN, SK$_{COj+1}$)*

O→P (180 Ringing)

From: *Bob,{Bob}$_{SKCOj+1}$, h(Bob, SK$_{POj+1}$)@domain1.com*

To: *{Alice,{Alice}$_{SKCOj+1}$}$_{SKPOj+1}$@domain1.com*

Body: *T$_1$, T$_2$, h(T$_1$, T$_2$, SK$_{COj+1}$)*

P→C (180 Ringing)

From: *{Bob}$_{SKCOj+1}$@domain1.com*

To: *Alice, {Alice}$_{SKCOj+1}$@domain1.com*

Body: *T$_1$, T$_2$, h(T$_1$, T$_2$, SK$_{COj+1}$)*

C→P (200 OK)

From: *Alice, {Alice}$_{SKCOj+1}$, h(Alice, SK$_{CPj+1}$@domain1.com*

To: *{Bob, {Bob}$_{SKCOj+1}$}$_{SKCPj+1}$@domain1.com*

P→O (200 OK)

From: *{Alice}$_{SKCOj+1}$@domain1.com*

To: *Bob, {Bob}$_{SKCOj+1}$@domain1.com*

โดยที่ *CL$_T$* คือจำนวนเงินที่ร้องขอ, *CL$_R$* คือจำนวนเงินคงเหลือในบัญชี,*T$_1$* คือเวลาที่ร้องขอวงเงิน,*T$_2$* คือเวลาที่ออกวงเงินให้ลูกค้าและ *C* จะถูกเรียกเก็บเงินจาก *O* ทันทีที่การทำธุรกรรมสมบรูณ์

3.5 การชำระเงิน

3.5.1 การชำระเงินกับผู้ให้บริการ

หลังจาก *C* เลือกสินค้าหรือบริการเรียบร้อยแล้ว *C* สามารถชำระเงินโดยส่งข้อความต่อไปนี้ให้ *O*

C→P (INVITE)

From: *Alice, {Alice}$_{SKCOj+1}$, h(Alice, SK$_{CPj+1}$@domain1.com*

To: *{Bob, {Bob}$_{SKCOj+1}$}$_{SKCP}$@domain1.com*

Body: *ID$_C$, {T$_P$, OI}$_{SKCOj+1}$, h(ID$_C$, T$_P$, OI, SK$_{COj+1}$)*

P→O (INVITE)

From: *{Alice}$_{SKCOj+1}$}@domain1.com*

To: *Bob, {Bob}$_{SKCOj+1}$@domain1.com*

Body: *ID$_C$, {T$_P$, OI}$_{SKCOj+1}$, h(ID$_C$, T$_P$, OI, SK$_{COj+1}$)*

O→P (180 Ringing)

From: *Bob,{Bob}$_{SKCOj+1}$, h(Bob, SK$_{POj+1}$@domain1.com*

To: *{Alice,{Alice}$_{SKCOj+1}$}$_{SKPOj+1}$@domain1.com*

Body: *Yes/No, h(Yes/No, CL$_{RM}$, h(T$_P$, OI,ID$_C$, SK$_{COj+1}$), SK$_{CO\ j+1}$)*

P→C (180 Ringing)

From: *{Bob}$_{SKCOj+1}$@domain1.com*

To: *Alice, {Alice}$_{SKCOj+1}$@domain1.com*

Body: *Yes/No, h(Yes/No, CL$_{RM}$, h(T$_P$, OI,ID$_C$, SK$_{COj+1}$), SK$_{COj+1}$)*

C→P (200 OK)

From: *Alice, {Alice}$_{SKCOj+1}$, h(Alice, SK$_{CPj+1}$@domain1.com*

To: *{Bob, {Bob}$_{SKCOj+1}$}$_{SKCPj+1}$@domain1.com*

PO→ (200 OK)

From: *{Alice}$_{SKCOj+1}$@domain1.com*

To: *Bob, {Bob}$_{SKCOj+1}$@domain1.com*

โดยที่ T_P คือ เวลาขณะร้องขอเพื่อชำระเงิน, *OI* คือ *{TID, Price, OD}* *TID* คือหมายเลขของการทำรายการ, CL_{RM} คือ จำนวนเงินคงเหลือหลังจากทำธุรกรรมสมบูรณ์ *Price* คือ ราคาของสินค้าหรือบริการ และ *OD* คือรายละเอียดของสินค้า เมื่อ *O* ได้รับคำร้องขอ *O* จะตรวจสอบจำนวนเงินในบัญชีของ *C* กับราคาของสินค้าหรือบริการ ถ้าจำนวนเงินในบัญชีของ *C* พอจะตอบ *Yes* กลับไป แต่ถ้าไม่พอจะตอบ *No* กลับไป ถ้า *C* ต้องการทำรายการต่อ *C* ต้องกลับไปร้องขอวงเงินตามหัวข้อแบบลงทะเบียนหรือแบบจ่ายเงินล่วงหน้าต่อไป

3.5.2 การชำระเงินให้พ่อค้าโดยผ่านผู้ให้บริการ

ส่วนนี้กล่าวถึงผู้บริการเป็นผู้ที่ช่วยให้ลูกค้าดำเนินธุรกรรมการชำระเงินกับพ่อค้าได้ ซึ่งมีสมมติฐานดังต่อไปนี้ *C* และ *M* เปิดบัญชีกับ *O* แล้ว *C* ได้รับอนุมัติวงเงินจากผู้ให้บริการ โปรแกรมในฝั่งลูกค้าทำหน้าที่ 2 ส่วน คือ การค้นหาสินค้าและการชำระเงิน โดยที่พ่อค้าหมายถึงผู้ที่ขายสินค้าหรือบริการบนมือถือ ดำเนินการโดยผู้ให้บริการ รายละเอียดดังนี้

1) หลังจากตัดสินใจเลือกใช้บริการการชำระเงินแล้ว *C* สร้างเซสชันโดยใช้ WTLS และแลกเปลี่ยน $\{K_{CO}, DK_{CO}, m_{CO}\}$ กับ *O* จากนั้น *C* และ *O* จะสร้างเซสชันคีย์ SK_{COj} โดยที่ j = 1...m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.6

2) M แลกเปลี่ยน $\{K_{MO}, DK_{MO}, m_{MO}\}$ กับ *O* ทั้ง 2 ฝ่ายสร้างเซสชันคีย์ SK_{MOj} โดยที่ j = 1...m โดยใช้เทคนิคการสร้างคีย์ในส่วนที่ 2.6

3) *C* เปิดโปรแกรมในมือถือของตน เพื่อเรียกดูสินค้าหรือบริการ เมื่อเลือกสินค้าหรือบริการแล้ว *C* ดำเนินการขอสั่งซื้อสินค้าหรือบริการ ดังต่อไปนี้

4) *P1* และ *P2* ลงทะเบียนขอใบรับรองดิจิทัล (Digital Certificate) จากองค์กรที่ให้บริการ (Certificate Authority หรือ CA) ที่น่าเชื่อถือ *P1* และ *P2* แลกเปลี่ยนพับบลิคคีย์ซึ่งกันและกัน

C→P1 (INVITE)

From: *Alice,* $\{Alice\}_{SKCMj+1}$*@domain1.com*

To: $\{Bob\}_{PubZ}$*@domain2.com*

Body: $ID_C, T, \{ID_M, OI, T, h(OI, SK_{CM})\}_{SKCOj+1}$

P1→P2 (INVITE)

From: $\{Alice\}_{SKCMj+1}$*@domain1.com*

To: $\{Bob\}_{PubP2}$*@domain2.com*

Body: $\{OI, h(OI, SK_{CM}), h(OI, SK_{COj+1}), T\}_{SKMOj+1}, \{Alice\}_{PriP1}$

P2→M (INVITE)

From: $\{Alice\}_{SKCM}$*@domain1.com*

To: *Bob@domain2.com*

Body: $\{OI, h(OI, SK_{CMj+1}), h(OI, SK_{COj+1}), T\}_{SKMOj+1}$

M→P2 (180 Ringing)

From: *Bob,* $\{Bob\}_{SKCMj+1}$*@domain2.com*

To: $\{Alice\}_{PubP1}$*@domain1.com*

Body: $\{Yes/No, h(Yes/No, OI, SK_{CMj+1})\}_{SKMOj+1}$

P2→P1 (180 Ringing)

From: $\{Bob\}_{SKCMj+1}$*@domain2.com*

To: $\{Alice\}_{PubP1}$*@domain1.com*

Body: $\{Yes/No, CL_{RM}, h(Yes/No, OI, SK_{CMj+1}), h(OI, SK_{MOj+1})\}_{SKCOj+1}, \{Bob\}_{PriP2}$

P1→C (180 Ringing)

From: $\{Bob\}_{SKCMj+1}$*@domain2.com*

To: *Alice@domain1.com*

Body: $\{Yes/No, CL_{RM}, h(Yes/No, OI, SK_{CMj+1}), h(OI, SK_{MOj+1})\}_{SKCOj+1}$

C→P1 (200 OK)

From: *Alice,*$\{Alice\}_{SKCMj+1}$*@domain1.com*

To: $\{Bob\}_{PubP2}$*@domain2.com*

P1→P2 (200 OK)

From: *Alice,*$\{Alice\}_{SKCMj+1}$*@domain1.com*

To: $\{Bob\}_{PubP2}$*@domain2.com*

Body: $\{Alice\}_{PriP1}$

P2→M (200 OK)

From: $\{Alice\}_{SKCMj+1}$*@domain1.com*

To: *Bob@domain2.com*

โดยที่ P1 คือ Proxy Server ของลูกค้าและ P2 คือ Proxy Server ของผู้ให้บริการโทรศัพท์เคลื่อนที่

เมื่อ *T* คือการประทับเวลา (Timestamp) หลังจาก *C* คลิกปุ่มทำการชำระเงินมีเซสชันใหม่เกิดขึ้นระหว่าง C และ M ชุดของคีย์ $\{K_{CM}, DK_{CM}, m_{CM}\}$ ถูกใช้งานร่วมกัน ทั้งสองฝ่ายสามารถสร้างเซสชันคีย์ SK_{CMj} โดยที่ *j=1...m* โดยใช้เทคนิคขการสร้างและการจายคีย์แบบออฟไลน์ จากข้อความข้างต้น สังเกตได้ว่า *O* ไม่สามารถสร้างข้อความแรกได้ เพราะมี $h(OI, SK_{CMj})$ รวมอยู่ ซึ่ง SK_{CMj} ถูกใช้ร่วมกันระหว่าง *C* และ *M* เท่านั้น

4. การวิเคราะห์คุณสมบัติความมั่นคงปลอดภัย

4.1 การรักษาความลับของข้อมูล

เนื่องจากการเข้ารหัสลับด้วยเซสชันคีย์ในแต่ละครั้งผู้ที่มีเซสชันคีย์ที่ตรงกันเท่านั้นที่จะสามารถถอดรหัสลับข้อมูลได้ และการสร้างเซสชันคีย์แบบออฟไลน์ คือไม่มีการส่งเซสชันคีย์ผ่านทางเครือข่าย จะทำให้การดักจับคีย์ไปทำการวิเคราะห์เป็นไปได้ยาก

4.2 การต้านทานการโจมตีแบบ Brute Force Attack

การโจมตีชนิด Brute Force Attack เพื่อค้นหาคีย์ที่ถูกต้องนั้นในโพรโทคอลที่นำเสนอนั้นทำได้ยากเนื่องจากมีการเปลี่ยนแปลงค่าของเซสชันคีย์ในทุกๆ ครั้งที่มีการทำธุรกรรม นอกจากนี้การนำเอาเทคนิคการสร้างและการกระจายคีย์แบบออฟไลน์ ทำให้การค้นหาคีย์ตั้งต้น ในการสร้างชุดของเซสชันคีย์ทั้งหมดทำได้ยากขึ้น จึงทำให้การโจมตีแบบ Brute Force Attack ประสบความสำเร็จยากขึ้นตามไปด้วย

4.3 การต้านทานการโจมตีแบบ Replay Attack

การโจมตีแบบ Replay Attack โดยการปลอมตัวเป็นไคลเอนท์แล้วส่งข้อมูลที่ดักจับได้อีกครั้งจะประสบความสำเร็จได้น้อยเนื่องจากการเปลี่ยนเซสชันคีย์ทุกครั้งที่มีการติดต่อสื่อสารอย่างสมบูรณ์

4.4 ความคงสภาพของข้อมูล

การใช้ฟังก์ชันแฮชทำให้สามารถตรวจสอบได้ว่าข้อมูลที่ส่งมานั้นระหว่างทางถูกเปลี่ยนแปลงข้อมูลจากบุคคลอื่นมาก่อนหรือไม่

4.5 การพิสูจน์ตัวจริงของผู้ส่งข้อความ (Party Authentication)

คุณสมบัตินี้เป็นการพิสูจน์ตัวจริงของผู้ส่งข้อความ โพรโทคอลที่นำเสนอมีคุณสมบัตินี้ในทุกๆ ข้อความ เพราะจากโพรโทคอลที่นำเสนอมีการนำเอา Message Authentication Code มาประยุกต์ใช้ ทำให้ผู้รับมั่นใจได้ว่าผู้ส่งเป็นผู้ส่งข้อความมาจริง

4.6 การโจมตีชนิด Man in the middle attack

ผู้โจมตีไม่สามารถปลอมตัวเป็นผู้ที่มีความเกี่ยวข้องหรือดักฟังข้อความของได้เนื่องจากมีการใช้กลุ่มของเซสชันคีย์ใน ซึ่งมีการเปลี่ยนคีย์ทุกครั้งในการสื่อสาร และใช้การเข้ารหัสลับที่เหมาะสม

5. สรุปผลการวิจัย

งานวิจัยฉบับนี้ได้นำเสนอโพรโทคอลที่มีความมั่นคงปลอดภัยสำหรับการทำธุรกรรมบนโพรโทคอล SIP และนำเทคนิคการสร้างเซสชันคีย์แบบออฟไลน์มาใช้งานทำให้ป้องกันการโจมตีแบบ Man-in-the-Middle ทั้งยังมีคุณสมบัติของการรักษาความลับของข้อมูล ความคงสภาพของข้อมูล การพิสูจน์ตัวจริงผู้ส่งและผู้รับข้อมูลและมีความรวดเร็วกว่าการส่งข้อมูลผ่าน SMS อีกด้วย โดยขั้นตอนต่อไปผู้วิจัยจะพัฒนาระบบต้นแบบทั้งด้านความสะดวกในการใช้งานและให้มีประสิทธิภาพมากที่สุด

6. เอกสารอ้างอิง

[1] เมฆินทร์ วรศาสตร์ และ ศุภกร กังพิศดาร, "การรักษาความมั่นคงปลอดภัยของการชำระเงินผ่านเครือข่ายไร้สายโดยใช้ข้อความสั้นผ่านผู้ให้บริการ", Proceedings of the 3rd National Conference on Information Technology (NCIT2010), Bangkok, Thailand, pp. 59-64

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

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

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

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

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

[7] S. Kungpisdan, P.D. Le, and B. Srinivasan, "A Limited-Used Key Generation Scheme for Internet Transactions", LNCS, Vol. 3325, 2005.

[8] Li, Y. and Zhang, X., 2004. "A Security-enhanced One-time Payment Scheme for Credit Card". International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications.

[9] S. Kungpisdan, B. Srinivasan, and P.D. Le, "Lightweight Mobile Credit-card Payment Protocol", LNCS, Vol. 2904, 2003, pp. 295-308.

[10] A. D. Rubin and R.N. Wright, "Off-line Generation of Limited-Use Credit Card Numbers", LNCS, Vol. 2339, 2002, pp. 196.

[11] IETF Standard, "SIP: Session Initiation Protocol", IETF RFC 3261, Jun. 2002.

[12] Ruishan Zhang, Xinyuan Wang, Xiaohui Yang, Xuxian Jiang, "Billing Attacks on SIP Based VoIP Systems 2010", This work was partially supported by NSF grant CNS-0524286.

[13] Narendra M. Shekokar, and Satish R. Devane, "A Novel Approach to Avoid Billing Attack on VOIP System", World Academy of Science, Engineering and Technology 62 2010.

[14] อธิพัฒน์ ทองย่อน และ ศุภกร กังพิศดาร, "A Security Protocol Preserving User Privacy for Session Initiation Protocol", 15th ICSEC, Bangkok, Thailand, 2011, pp. 97-102

[15] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[16] อธิพัฒน์ ทองย่อน และ ศุภกร กังพิศดาร, "การออกแบบโพรโทคอลชำระเงินบนโพรโทคอล SIP ที่คงคุณสมบัติความเป็นส่วนตัวของผู้ใช้", 34th EECON 2011, Nov. 30 - Dec. 2, 2011, pp. 1041-1044.