RESEARCH ARTICLE OPEN ACCESS

Comparison of Mobile Payment Protocol Security

[1]R Chitti Raja,
[1]Asst Prof in Rajamahendri institute of Engineering and Technology, Rajahmundry, Affiliated to JNTUK,
[2]Ksnv Jyotsna Devi,
[2]Asst Prof in Rajamahendri Institute of Engineering and Technology, Rajahmundry, Affiliated to JNTUK,
[3]K Nagaraju
[3]Assoc Prof in Gayatri Vidya Parishad College of Engineering for Women, Vizag, Affiliated to JNTUK.
Corresponding Author: R Chitti Raja

ABSTRACT
Mobile phones are getting smarter and people have been using them for many different proposes. Recently, more and more people have begun using their mobile phones as a method of payment for online shopping and banking. Mobile payments have become easier than ever. Present security issues of mobile payments, however, still require improvement. This paper aims to summarize the idea of mobile payments and analyze the research of existing secure mobile payment protocols by using MPPS (Mobile Payment Protocol Security) framework. As a result, this paper will give researchers tools to standardize current protocol and share new developments.
***Keywords*:** Mobile payment protocol Secure mobile payment

---

Date of Submission: 02-11-2017 Date of acceptance: 11-11-2017

I. INTRODUCTION

Mobile devices have become a popular method for businesses in the digital world because of their convenience for payments of goods and services. The payers can access the payment system via web browsers or applications on mobile devices. More people nowadays are willing to pay for goods or services using their mobile devices. Gartner Inc., the world's leading information technology, reports that the market worth of worldwide mobile payment transactions grew to $235 billion in 2013 and will reach $721 billion by 2017 [1]. Thrive Analytics surveyed the consumers in Asia-Pacific region and the results showed that there are about 800 million people who have used mobile phones as of June 2014 [2]. Thrive Analytics also found that 46 % haven't used a mobile phone to pay for goods and services because they concern about security and privacy [2]. Thus, the study concluded that the mobile payments have both advantages and disadvantages. The researchers are trying to find ways to deal with privacy and security issues by designing a protocol for mobile payments to be more effective and secure.

This paper analyzed the mobile payment protocols dating back 10 years in three aspects: methodology, security and performance. The structure of the paper is organized as follows.
Section 2 provides an overview of the background of mobile payments.
Section 3 classifies the technology of mobile payment systems.
Section 4 presents the properties of security and cryptographic concept.
Section 5 analyzes the existing secure mobile payment protocols.
Section 6 concludes the paper.

II. BACKGROUND AND RELATED WORK

This section provides the background and related works of the mobile payment.

2.1 Primitive Payment Transaction

Conceptually, the primitive mobile payment is composed of three basic steps [3,4]: Payment—Client makes a payment to the merchant, Value Subtraction—Client requests to the payment gateway for his debit, and Value Claim—Merchant requests to the payment gateway to credit transaction amount into his account.

2.2 Mobile Payment Procedure

Type of payments based on location

- **Remote Transactions:** These transactions are conducted regardless of the user's location. Location distances don't limit the users.
- **Proximity/Local Transactions**: These transactions are where the device communicates locally to perform close proximity payments. This involves the use of short range messaging protocol such as Bluetooth infrared, RFID and contact less chips to pay for goods and services in short distances.

Type of payments based on value

- **Micro-Payments**: These are low value payments less than US$1 [5].
- **Macro-Payments**: These are large value payments more than US$10 [5].

Type of payments based on charging method

- **Post-paid:** This is the most common payment method used in e-commerce transactions today. This consists of account-based and token-based method. Account-based method is used by banks, and the credit card industry. Consumers with a bank account or credit card can pay using the account-based method [7]. Token-based method is the charge method for goods and service such as e-money, e-wallet by mobile network operator [9.10].
- **Pre-paid**: This is the most common charging method used by mobile network operators as well as third-party service providers. This method can only be used by consumers capable of paying immediately.

III. TECHNOLOGY OF MOBILE PAYMENT

We studied and assessed technologies in mobile payment systems from the existing researches as described below [11].

- **SMS**—Short Messaging Service is a text messaging service used to send and receive short text messages. The maximum length of messages is less than 160 alphanumeric characters, to and from mobile phones.
- **WAP**—Wireless Application Protocol is a technology which provides a mechanism for displaying internet information on a mobile phone.
- **NFC**—Near Field Communication is the communication between contactless smart cards and mobile phones.
- **RFID**—Radio Frequency Identification is a method of identifying an item wirelessly using radio waves
- **Smart Card**—Smart cards and plastic cards normally appear in the same shape as credit cards are embedded with a chip or microprocessor that can handle and store 10–100 times more information than traditional magnetic-stripe cards [12].
- **Internet**—The internet is a publicly accessible, globally interconnected network. It uses the internet protocol to enable the exchanging and sharing of data among computers in the network
- **USSD**—Unstructured Supplementary Services Data is a mechanism of transmitting information via a GSM network. Unlike SMS, it offers a real-time connection during a session
- **IVR**—Interactive Voice Response is a telephony technology where the users can interact with the database of a system without any human interaction
- **Magnetic**—Data is stored in a magnetic stripe on a plastic card. It is read by swiping the card in a magnetic card reader.

IV. SECURITY OF MOBILE PAYMENT

This section presents security properties, and cryptographic techniques.

4.1 Security Properties

A secure mobile payment system must have the following properties [13].

- **Confidentiality**—The system must ensure that private or confidential information will not be made available or disclosed to unauthorized individuals.
- **Integrity**—The system must ensure that only authorized parties are able to modify computer system assets and transmitted information.
- **Authentication**—The system must ensure that the origin of a message is correctly identified, with an assurance that the identity is not false.
- **Non-repudiation**—The system must ensure that the user cannot deny that he/she has performed a transaction and he/she must provide proof if such a situation occurs.
- **Availability**—The system must be accessible for authorized users at any time.
- **Authorization**—The system must verify if the user is allowed to make the requested transaction.

4.2 Cryptography Concept

Cryptography is a technique used to secure data protection from the hacker, which can be classified into the following three groups:

- **Symmetric Key Cryptography**—It is the encryption methods in which both the sender and receiver share the same key. The algorithms, in general, consist of DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advance Encryption Standard)
- **Asymmetric Key Cryptography**—It is also known as public key cryptography, a class of cryptographic algorithms which requires two separate keys. One key is secret and the other key is public. The algorithms are RSA (Rivest, Shamir and Adleman) and ECC (Elliptic Curve Cryptography).
- **Hash Function**—It is a public one-way function that maps a message of any length into a fixed-length, which serves as the authenticator. A variety of ways of a hash code can be used to provide message authentication.

V. ANALYSIS OF EXISTING SECURE MOBILE PAYMENT PROTOCOLS

We analyzed the existing researches on 11 secure mobile payment protocols that focus on lightweight protocol and high level of security. Bellare and Wang [14] designed the SET protocol (Secure Electronic 14Transfer Protocol) in 1996. This protocol is using a cryptographic technique by using public key and digital sig-nature to protect information on mobile payment via a credit card that gives three important properties of information security: confidentiality, integrity and authorization. Bellare and Garay [15] designed the iKP protocol (i-Key-Protocol) in 2000 that is adjusted from the SET protocol by using pair "i". If it is high, it shows a high level of security. This protocol provided the properties of security similar to the SET protocol. Kungpisdan and Srinivasan [16] designed the KSL protocol (Kungpisdan Logic) in 2003 which focuses on client processing for decreasing the computational cost on the mobile wireless network. The protocol applied a sym-metric key cryptography. The comparison shows that it has better performance over the SET and iKP protocols and also provides the non-repudiation property. Kungpisdan et al. [4] developed the Kungpisdan Protocol (Account-based Mobile Payment) in 2004 that is improved from KSL protocol by using symmetric key for all the parties. This protocol creates a secret shared key between two parties which support high level of four security properties: confidentiality, integrity, authentication and non-repudiation. The performance, when compared with the SET and iKP protocol, showed that the computation time at the client is relatively faster.

Fun et al. [17] designed the LMPP protocol (Lightweight Mobile Payment Protocol) in 2008. This protocol is using only the symmetric key but the performance is better than the SET, iKP and Kungpisdan [16] protocols. Shedid [18] adjusted the MSET Protocol (Modified SET Protocol) in 2010 by decreasing the number of operational cryptographic for increasing the performance. Dizaj et al. [19] designed the MPCP2 Protocol (Mobile Pay Center Protocol 2) in 2011 for decreasing the number of cryptographic operations between all engaging parties. By using symmetric cryptography all parties exchange key offline by Diffie-Hellman method. When compared with the SET, iKP, KSL and Kungpisdan protocols, the performance showed that the number of operation at the client is less than the number of operation of the other protocols. Isaac and Zeadally [20] designed PCMS Protocol (Payment Centric Model Using Symmetric Cryptography) in 2012. The protocol focuses on Payment gateway centric model. All parties must connect via the payment gateway for authorization.

Sekhar and Sarvabhatla [21] designed the SLMPP Protocol (Secure Lightweight Mobile Payment Protocol) in 2012. This protocol focuses on end-to-end encryption by using symmetric key cryptography in order to decrease the number of operation at the client side. The comparison with the SET, iKP and Kungpisdan protocols found that this protocol has less number of operations. The authors concluded that this protocol is suitable for mobile wireless network. Tripathai [22] designed the LPMP Protocol (Lightweight Protocol For Mobile Payment) in 2012 focusing on the number of cryptographic operations. It is compared with the SET, iKP, KSL and MSET protocols, and found that the LPMP use only the cryptographic operations on the client side which all processes are less than the others. Auala and Arora [23] designed the SAMPP Protocol (Secure Account-based Mobile Payment Protocol) in 2013 by using asymmetric key and digital signature. The authentication technique is using a multifactor authentication with a biometric and private key. The per-romance is better when compared with the SET and iKP protocols.

The analyses of the relationship between all secure mobile payment protocols from the past to present showed that almost all protocols are compared in performance with SET and iKP. Subordinates of SET and iKP are Kungpisdan, KSL, LMPP and MSET. The relationship of the secure mobile payments protocols from the past 10 years is depicted. The original protocol, SET, was formed in 1996 and the latest protocol, SAMPP, was formed in 2013. Security protocols can be divided into three aspects: methodology, security and performance. These three aspects are key factors to the success of secure mobile payment protocol and are the core of research on mobile payment security. The concept of MPPS framework is depicted.

Number of reference	[14]	[15]	[16]	[4]	[17]	[18]	[19]	[20]	[21]	[22]
Confidentiality	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Integrity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Authenticaton	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Non-repudiation	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Id protect from payee	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Id protection from	N	N	N	N	Y	Y	Y	-	Y	Y
Eavesdropper	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Transaction privacy	N	N	N	N	Y	Y	Y	Y	Y	Y

The detailed analysis of secure mobile payment protocol is as follows:

5.1 Methodology Aspect

Secure mobile payment protocols such as SET, iKP, KSL and SAMPP use the asymmetric key cryptography technique to support security. The others use sym-metric key cryptography. The processes of encryption have the following objectives:

- Encryption/Decryption—This ensures that the data is confidential and is encrypted secretly and privately.
- Hash Function—This ensures that the data is sent correctly and the sent data matches the original data. HMAC (Hash Message Authentication Code): pro-vides an easy mechanism for verifying both user authenticity and that a message hasn't been tampered with of message; it protects the integrity and the authenticity of the message.
- Key generation—This ensures the non-repudiation property by confirming the corresponding data before beginning a transaction order to prevent disclaimers.

5.2 Security Aspect

After analyzing 11 protocols of mobile payments, we found that almost all proto-cols support features of security in four key areas: confidentiality, integrity, authentication and non-repudiation. But, two protocols SET and iKP do not support non-repudiation. Moreover, the protocols KSL, LMPP, MSET, MPCP2, SLMPP, LPMP and SAMPP provided all privacy properties that the others could not. The security properties and features of the different protocols are summarized in Table 1.

Table 1 Security Properties of Protocol

REFERENCES

[1] Gartner.com (2013) Gartner Says worldwide mobile payment transaction value to surpass $235 billion in 2013. http://www.gartner.com/newsroom/id/2504915

[2] Richter F Consumers wary of mobile payment security. http://www.statistica.com

[3] Fun TS, Beng LY, Roslan R, Habeeb HS (2008) Privacy in new mobile payment protocol. World Acad Sci Eng Technol 2:198–202

[4] Kungpisdan S, Srinivasan B, Le PD (2004) A secure account-based mobile payment protocol In: Proceedings of the international conference on information technology: coding and computing (ITCC 2004)

[5] Fun TS, Beng LY, Razali MN (2013) Review of mobile macro-payments schemes. J Adv Comput Netw 1(4)

[6] Kungpisdan S, Srinivasan B, Le PD (2003) Lightweight mobile credit-card payment protocol. Lect Notes Comput Sci 2904:295–230

[7] Singh A, Shahazad KS (2012) A review: secure payment system for electronic transaction. Int J Adv Res Comput Sci Softw Eng 2(3)

[8] McKitterick D, Dowlin J State of the art review of mobile payment technology. https://www.scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf

[9] Ahamad SS, Udgata SK, Nair M (2014) A secure lightweight and scalable mobile payment framework. In: FICTA 2013. Advances in intelligent system and computing, vol 247. Springer International Publishing, Switzerland

[10] Ferreira C, Dahab R (1998) A scheme for analyzing electronic payment systems. In: Computer security applications conference, proceedings. 14th Annual, 1998

[11] Mathew M, Balakrishnan N, Pratheeba S (2010) A study on the success potential of multiple mobile payment technologies. In: Technology management for global economic growth (PICMET), Proceedings of PICMET '10

[12] Smart Card Alliance (2008) Proximity mobile payments business scenario: research report on stakeholder perspectives

[13] Computer Fraud & Security (2007) Analysis of mobile payment security measures and different standards

[14] Li Y, Wang Y Secure electronic transaction. http://people.dsv.su.se/*matei/courses/IK2001SJE/li-wang_SET.pdf

[15] Bellare M, Garay JA (2000) Design implementation, and deployment of the ikp secure electronic payment system. IEEE J Sel Areas Commun 18(4)

[16] Kungpisdan S, Srinivasan B, Le PD (2003) Lightweight mobile credit-card payment protocol. Lect Notes Comput Sci 2904:295–308

[17] Fun TS, Beng LY, Likoh J, Roslan R (2008) A lightweight and private mobile payment protocol by using mobile network operator. In: Proceedings of the international conference on computer and communication engineering 2008 May 13–15, Kuala Lumpur, Malaysia, 2008

[18] Shedid SM (2010) Modified SET protocol for mobile payment. Proc Int Conf J Comput Sci Netw Secur 10(7):289–295

[19] Alizadeh Dizaj MV, Moghaddam RA, Momenebellah S (2011) New mobile payment protocol: Mobile Pay Center Protocol 2 (MPCP2) by using new key agreement protocol: VAM. In: 3rd

international conference on electronics computer technology (ICECT)
[20] Isaac JT, Zeadally S (2012) An anonymous secure payment protocol in a payment gateway centric model. In: The 9th international conference on mobile web information system (MobiWIS). Elsevier
[21] Sekhar VC, Sarvabhatla M (2012) Secure lightweight mobile payment protocol using symmetric key techniques. In: International conference on computer communication and informatics (ICCCI), pp 1–6, 10–12 Jan 2012
[22] Tripathi DM, Ojha A (2012) LPMP: an efficient lightweight protocol for mobile payment. In: 3rd national conference on emerging trends and applications in computer science (NCETACS)
[23] Auala PS, Arora H (2013) A secure account based mobile payment protocol with public key cryptography and biometric characteristics. In: International journal of science and research (IJSR), vol 2(3), India online ISSN: 2319-7064

Mr. R Chittiraja working as Asst Prof in Department of Computer Science and Engineering in RIET in Rajahmundry. He had 9+years experience in various repeatated Technological Institutes in India. I completed my graduation and post graduation in Institute Affiliated to JNTU-H.

Mrs. I KSNV Jyotsna Devi working as Asst prof in Computer Science and Engineering in RIET. She had 2 years Experience in repeatated Technological Institutes in India.

Mr.K Nagaraju working as Assoc Prof in Computer Science and Engineering in GVP Engineering College. He had 10 Years Experience in repeatated Technological Institutes in India.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

R Chitti Raja. "Comparison of Mobile Payment Protocol Security." International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 11, 2017, pp. 72–76.