International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 18-22

DESIGN AND ANALYSIS OF SECURE MOBILE TRANSACTION AND PROTOCOL

[1]Narinder Bali, [2]Dr Raghav Mehra
[1] Phd scholar , [2]Associate professor
[1,2] Department of computer sciences, Bhagwant University, Ajmer Rajasthan
balinarinder7@gmail.com

***Abstract*— Mobile phones are getting smarter and people have been using them for many different proposes. 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 development. The aim of this research paper is to study and design a mobile transaction processing systems, focusing on versatile data sharing mechanisms in volatile mobile environments. The worldwide rapid increase of the Internet has led to the emergence of an Substantial range of service one of the most popular being electronic commerce Mobile e-commerce is a natural extension of e-commerce and represents a new way for conducting commerce .M-commerce transactions are conducted through a mobile device by wireless networks. Mobile payment is defined as any payment transaction involving the purchase of goods or services that is completed with a wireless device. M-payments facilitate m-commerce were users make online purchases from their mobile devices remotely at any time In this paper let us have a brief survey on security issues when designing implementing, and deploying secure m-payment systems with a focus on threats, vulnerabilities, and risk. In the future as m-payment systems become fully integrated with other emerging technologies such as fifth-generation mobile networks (5G) and cloud computing. This article considers M-payment classification based on several other criteria, Based on Payment, or how the money is transferred; payment medium to be used to realize the payment; Timing payment, or when it occurs; payment amount conveyed from the customer to the merchant; and payment location—that is, where the payment takes place.. Generally, an m- payment system consists of four main entities:**

theclient, the merchant, the merchant's financial institution (called the acquirer) and the client's financial institution (called the issuer). The client and the merchant can be connected through a short-range link or the Internet using wired, wireless, or cellular communication technologies that are offered by a mobile-phone operator (such as General Packet Radio Service (GPRS), Enhanced Data Rates for Global System for Mobile Communications(GSM) Evolution, Evolution-Data Optimized, or High Speed Downlink Packet Access (HSDPA).

***Index Terms*— Mobile phones, mobile payments, M-commerce, wireless networks.**

I. INTRODUCTION

Recent developments of communications technologies and business models raised concerns about mobile payment systems in terms of usability and security. Rising smart mobile devices with variety of usage and privacy and easy access to communication protocols have provided the potentials for growing development of mobile commerce. Furthermore, new business models in daily activities have increased the need of comprehensive mobile e-commerce system. Protocols that enable secure communication over un trusted network constitute an important part of the current computing infrastructure. Common examples of such protocols are SSL [53], TLS [44], Kerberos [106], and the IPSec [73]. SSL and TLS are used by internet browsers and web servers to allow secure transactions in applications like online banking. The IPSec protocol suite provides confidentiality and integrity at the IP layer and is widely used to secure corporate VPNs. It provides data protection and integrity in wireless local area networks, while Kerberos is used for network authentication. A Mobile Payment System (MPS) defined as any payment system that enables financial transactions to be made securely from one organization or individual to another over a mobile network. Mobile Payment System provide attractive opportunities to, merchants financial, and users. These opportunities were simplicity and ease of an m-payment transaction for the user and they also enable merchants to access customer information and target specific customer groups through various incentive programs, such as discount coupons and rewards programs. The growth of Mobile Payment transactions over the last decade has been largely enabled by increasing speeds of mobile-network connections, the rapid proliferation of portable devices and the worldwide penetration of mobile-cellular subscriptions. In fact, the global worldwide m-payment market will reach over 450 million users and a transaction value of over US$721 billion by 2017.Thrive Analytics surveyed the, consumers in Asia-Pacific region and the results showed that there are about 950 million people who have used mobile phones as of July 2016 . Thrive Analytics also found that46 % haven't used a mobile phone to pay for goods and services because they concern about security and privacy. 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 12 years in three aspects: methodology, security and performance. The structure of the paper is organized as follows.

Section 1 provides an overview and the background of mobile payments. Section 2 classifies the technology of mobile payment systems. Section 3 presents the properties of security and cryptographic concept. Section4 analyzes the existing secure mobile payment protocols.

Section 5 concludes the paper.

. Basically, m-payment process may be implemented in different scenarios, but it includes some fundamental steps: registration, payment submission, authentication and authorization of parties by system service provider, and the final confirmation. In order to provide a secure and comprehensive m-payment, the payment scenario should be designed so that it performs fast and simple for the end-user, but secure and comprehensive for the provider. An efficient payment scenario takes efficient steps in performance. The critical items in each step are the payment messages containing critical information being transferred between participating parties. These messages are objects to which security should be applied. Applying security to messages, to transfer and process payment messages should be done to fulfill a desired fast, secure, integrated and comprehensive transaction. Authentication, secure communication, including confidentiality and integrity of messages, authenticity of sender and recipient, key exchange protocols and non-repudiation should enhance an atomic payment transaction with security. To establish the desired implementation of convenient m-commerce operations, a need of a mobile application is being felt. With rising new smart phones available in markets, the facilities of smart mobile devices could be exploited to develop an application to perform required m-commerce operations. Current smart phones with different operating systems provide an extensive environment to develop desired applications based on business and users needs. This project basically followed the potential to overcome specific financial access problems in some developing markets by accommodating unbanked users. Then, design and implementing a mobile application is conducted according to some defined business and professional needs. This report brings a comprehensive overview about its potentials starting form supporting back-end systems, up to design and implementation of account-based payment scenarios used in m-commerce and traditional transactions and evaluating and analyzing of the results against the essential and probable business needs, keeping in mind a perspective for further development And research potentials.

II. Components of Mobile Payment

We analyze the components of mobile payments from the existing researches related to mobile payment protocols. Fun, Beng and Razali stated that the components of mobile payment scheme consist of seven main actors: Financial Service Providers (FSPs), Payment Service providers (PSPs), Payee, Payer, Mobile Network Operator (MNOs), Device Manufacturers, and Regulators. However, Fun, Beng, Roslan and Habeeb stated that mobile payment protocols are composed of five principals which include client, merchant, issuer (client's financial institution), acquirer (merchant's financial institution) and payment gateway (PG) . Kungpisdan, Srinivasan and Le also defined that five parties on mobile payment protocols are client, merchant, payment gateway, issuer and acquirer. Singh and Shahazad stated that the components of mobile payment protocol consist of three participants: payee, payer and financial institution. McKitterick and P. Pukkasenung and R. Chokngamwong Dowling stated that the components of mobile payment protocols are composed of four parts: customer, merchant, payment service provider and trust third party (TTP) . The number of components mentioned above by researchers is different due to the design of payment protocols. However, we conclude that the components of mobile payment protocols, in general, consist of only three main parts: buyer, payment channel and seller.

A. Background and Basic Concepts

Sufficient background information is given to the reader to understand the context and significance of the problem of the undertaken research Basic Concepts Mobile Payment As mobile devices have been transforming into personal trust devices, mobile payment is recognized as interactions between parties in a e-payment system with specific context (e.g. business models, player relationships) and capabilities (mobile device capabilities) so that there is at least one party as a mobile user .Basically, the context of m-payments includes any payment in which a mobile device is used in order to "initiate, activate, and confirm" the payment].. Mobile payment systems evolve with new technologies, since they are free of limitations usually applied to bank-anchored services. There are three initiatives that could be considered to best suit mobile payments. First, mobile device is the most convenient and possible payment technology for mobile context and service purchases. Second, the diminishing use of cash provides the potentials to develop new substitute payment approaches for low value transactions using financial service stations. Third, need of a cost-effective means to charge macro-payments in m-commerce environment. Purposed, like exchanging digital goods, tickets or coupons.

B. Methodology for Establishing System Requirements

This section describes system requirements being considered in order to evaluate if the purpose of the paper is successfully met. Initially, technical, business, and user requirements should be considered for a payment system presenting an interoperable, modular, integrated, extendible and mobile payment architecture that provides the potentials for deploying security extensions. Secondly, according to the specified system requirements, a financial system appropriate for mobile applications has been chosen. Considering fundamental system requirements of mobile payment systems, the architecture of the system has been evaluated as well as the interactions between internal components and external components of the system. The third step will be identifying

potentials of the payment model of the system for security enhancement along with preserving system behavior including protocols, services, transactions and message structure. Next, an interface has been designed which is used to interact with the adopted financial system. Development of mobile applications is required to provide required mobile commerce services for corresponding users. Identifying potentials points of interactions between mobile applications and back-bone system in applying security constrains was the starting point to employ security arrangements. According to all information related to evaluating system security potentials, security requirement specifications have been determined, so that the system can proceed persistently along with predicted security circumstances. Based on possible security requirement specifications, some of them should be adopted which are feasible in terms of design, implementation and deployment in an efficient way. Finally, a methodology for security design and implementation will be planned

C. Methodology for Design and Implementation

This section describes a methodology for design and implementation of the system described in this paper. A qualitative case study methodology has been conducted in order to provide tools to study existing phenomena within the research context, for revealing and understanding multiple facets of the phenomenon. A case study design is considered in this report, this study focuses on answering "how all steps of mobile payments should be considered in applying security" and "why it is required to design and employ a security method of payment transactions"; Also the behavior of involved components in the study could not be manipulated. Moreover, it is required to include contextual conditions relevant to the phenomenon under study. Here, the contextual conditions could be financial system infrastructure and mobile interfaces. Next, in order to determine the case of analysis, it is required to analyze the process of mobile payment in adopted environment.

D. Methodology for Data Acquisition

This section describes the complimentary methodology for data acquisition in order to make conclusion of the current work. Using different data sources enhances data credibility for this research paper. Potential data sources in this paper include extensive study and analysis of related works and technology, direct observations, and participant-observation. By data acquisition in integration with qualitative approach, within a case study research, data integration and collection can facilitate reaching a holistic understanding of the phenomenon under study. Mobile payment methods have always been critical, since they are dealing with credits or money. So, providing an adequate security would be mandatory and an inevitable aspect of mobile payments. On the other hand, there has been an issue to preserve a trade-off between usability and security of mobile payments, so that providing maximum security can affect or even violate the usability of mobile payments in practice. In order to provide a secure and comprehensive m-payment, the payment scenario should be designed so that it performs fast and simple for the end-user, but secure and comprehensive for the provider. An efficient payment scenario takes efficient steps in performance. The critical items in each step are the payment messages containing critical information being transferred between participating parties. These messages are objects to which security should be applied. Applying security to messages, to transfer and process payment messages should be done to fulfill a desired fast, secure, integrated andcomprehensive transaction. Authentication, secure communication, including confidentiality and integrity of messages, authenticity of sender and recipient, key exchange protocols and non-repudiation should enhance an atomic payment transaction with security. To establish the desired implementation of convenient m-commerce operations, a need of a mobile application is being felt.

III. 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 designed the SET protocol (Secure Electronic Transfer Protocol). This protocol is using a cryptographic technique by using public key and digital signature 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 designed the iKP protocol (i-Key-Protocol) 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 designed the KSL protocol (Kungpisdan Logic) which focuses on client processing for decreasing the computational cost on the mobile wireless network. The protocol applied a symmetric 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. developed the Kungpisdan Protocol (Account-based Mobile Payment) 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 Review and Comparison of Mobile Payment Protocol 15 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. designed the LMPP protocol (Lightweight Mobile Payment Protocol). This protocol is using only the symmetric key but the performance is better than the SET, iKP and Kungpisdan protocols. Shedid adjusted the MSET Protocol (Modified SET Protocol) by decreasing the number of operational cryptographic for increasing the performance. Dizaj et al. designed the MPCP2 Protocol (Mobile Pay Center Protocol 2) 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 numberof operation of the other protocols. Isaac and Zeadally designed PCMS Protocol (Payment Centric Model Using Symmetric Cryptography). The protocol focuses on Payment gateway centric model. All parties must connect via the payment gateway for authorization. Sekhar and Sarvabhatla designed the SLMPP Protocol (Secure Lightweight Mobile Payment Protocol). 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 designed the LPMP Protocol (Lightweight Protocol For Mobile Payment) 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 designed the SAMPP Protocol (Secure Account-based Mobile Payment Protocol) by using asymmetric key and digital signature. The authentication technique is using a multifactor authentication with a biometric and private key. The performance 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 original protocol, SET, was formed in 1996 and the latest protocol, SAMPP, was formed in 2016. 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.

IV. Security Mechanism

During a payment transaction, the system transfers the transaction message attached with the digital signature's public key over an unsecured network link. In order to protect transaction messages from third party eavesdropping, both signature and encryption layers are used to process messages. Digital signature layer ensures that the message is sent from the right client to he right server. Hence, they combined the SIM (Subscriber Identifier Module Number), PHID (mobile phone serial number) and ACCID (user's bank account number) as the Client ID, then Due to the J2ME limitations, ECDSA has been adopted because of its low computational cost, higher performance, a fast signature generation, and short key size. Elliptic Curve Digital Signature Algorithm (ECDSA) is adopted to implement Digital Signature Algorithm (DSA). When Java applications are being compiled, class files are generated in machine language so; this process makes it difficult to understand details of the private key. The RMS (Record Management System) APIs provides the ability to manipulate records between different applications and shares records within an application, so that access to these records is strictly prohibited. The key pair will eventually expire, and the banking server detects if any renewal of the key-pair in needed then, initiates the renewal of a key pair by notifying mobile device to generate a new one.

References

[1] S. Kungpisdan, Securing Mobile Payments: Modelling, Design, and Analysis: Discovering a New Way to Perform Secure Payment Transactions Over Wireless Networks, LAP Lambert Acad, 2010.

[2] P.-L. Chatain, Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks of Money Laundering and Terrorist Financing, World Bank Publications, 2008.

[3] D. M. K. Finkenzeller, Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, John Wiley and Sons, 2010.

[4] M. D. Marina Yue Zhang, High-tech entrepreneurship in Asia : innovation, industry and institutional dynamics in mobile payments, Cheltenham, Edward Elgar, 2007.

[5] B. Unhelkar, Handbook of Research in Mobile Business: Technical, Methodological, and Social Perspectives, IGI Global Snippe, 2009.

[6] K. Petrova, Mobile Payment: Towards a Customer-Centric Model, Springer, 2008.

[7] N. N. Tabandehjooy, "A Lighweight and Secure Protocol for Mobile Payments Via Wireless Internet in Mcommerce," in e-Education, e-Business, e-Management, and e-Learning, International Conference, Shiraz Univ., Shiraz, Iran, 2010.

[8] 9Secure Element Evaluation Kit for the Android platform," Open source, [Online]. Available: http://code.google.com/p/seek-for-android/. [Accessed 10 12 2012].

[9] RSA Laboratories," RSA, [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2132. [Accessed 10 12 2012].

[10] S. Cimato. Design of an authentication protocol for GSM javacards. Lecture Notes in Computer Science, 2288:355–368, 2002. [Com04] Commonwealth Bank Group. EFTPOS, 2004. http://www.commbank.com.au/ Last accessed January 30, 2005. 272 [Dat04]

[11] C. S. P. D. Morley, Understanding Computers: Today and Tomorrow, Introductory, Cengage Learning, 2010

[12] F. Zhang, "Secure Applications for Financial Environments (SAFE) System," School of Information

and Communication Technologies, Royal Institute of Technolog, 2008.

[13]. E. C. Limited, Business Knowledge for IT in Retail Banking: The Complete Handbook for IT Professionals, Essvale Corporation Limited, 2007.

[14] M. Yung, "On the Evolution of User Authentication: Non-bilateral Factors," in Information Security and Cryptology, Springer Berlin Heidelberg, 2008.

[15] A. Kondoro, "Location based authentication," 2011.

[16] D. Ortiz-Arroyo, "Intelligence and Security Informatics," in European Conference, EuroISI, 2008. R. Chbeir, Emergent Web Intelligence: Advanced Information Retrieval, Springer, 2010

[17] Google, "Android development," Google, [Online]. Available: http://developer.android.com/index.html. [Accessed 10 12 2012].

[18] Oracle, "Oracle Java documents," Oracle, [Online]. Available: http://docs.oracle.com/cd/E21043_01/apirefs.1111/e10674/oracle/security/crypto/cert/Ce rtificateRequest.html. [Accessed 10 12 2012].

[19] "RSA Laboratories," RSA, [Online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2129. [Accessed 10 12 2012].

[20] "certicom," [Online]. Available: http://www.certicom.com/index.php/an-introduction-to-the-uses-of-eccbased-certificates. [Accessed 01 01 2013].