STUDY AND IMPLEMENTATION OF MULTI-CRITERION AUTHENTICATION APPROACH TO SECURE MOBILE PAYMENT SYSTEM

Mrs Smita Parte [1],Ms Noumita Dehariya [2]

[1]*Assistant Professor, CSE, TIT College, Bhopal ,MP 462021, India,* ***smita.athanere@gmail.com***
[2]*Assistant Professor, CSE, TIT College, Bhopal, MP 462021, India,* ***ndehariya@gmail.com***

Abstract

Mobile payment (m-payment) is a new and alternative payment mechanism over traditional means of payment like cash, cheque etc. Due to large acceptance of mobile devices users have started using online services such as banking, purchasing etc by their mobile devices. So in commerce related services user can make payment anywhere and anytime. Various security issues are also identified related to mobile payment authentication like user identity theft, virus and man-in-middle attack. Authentication techniques presently available are not adequate to secure financial transaction using mobile devices since they are based on user Id-password approach and only one party who is using the service is validated. Authentication scheme for financial services using mobile devices is highly valuable in terms of security. To protect against identified security threats related to authentication system for mobile payment service, an approach is suggested, use of multiple criteria at multiple levels as authentication keys during the transaction process. I have studied related approaches, added new criteria of authentication, implemented and analyzed this against security issues related to user privacy protection.

Keywords: POS, SET, WAP, SMS, OTP,

---------- *** ----------

1. INTRODUCTION

Nowadays mobile devices are become very popular because of their small size and easy use. People can use these devices anytime and anywhere. By seeing the popularity of mobile devices , services related to commerce, banking are also available in the market as internet based online services available for PCs.

1.1 Motivation

Mobile payment is a kind of service provided by any financial institution or bank. It is a new and easy payment method. Instead of paying with cash, cheques or credit cards a person can use a mobile phone to pay for a wide range of services and goods. Service providers which are offering these kinds of services must provide effective means to authenticate the identity of users, using this service. Whatever web based authentication techniques are available are not adequate for financial transaction since most of them based on user Id-password i.e. single criterion but any financial transaction needs a strong authentication based on multiple criteria since passwords can be hacked and use for further transaction. So we need a strong authentication system which is based on multiple criteria and also authenticate both the parties like user and service provider. To protect against identified security threats related to authentication system for mobile payment service, an approach is suggested, use of multiple criteria at multiple levels as authentication keys during the transaction process. This approach also combines the benefit of simple web based authentication and the wireless technology which results in a very strong authentication mechanism and can raise the faith of users.

1.2 Problem Statement and Objectives

To study the available approach for authentication, this is based on use of multiple criteria at multiple levels to secure Mobile Payment System and implemented it. Objectives are-

(i) Study of mobile payment application and services available in market.
(ii) Identification of security issue of available mobile payment solutions.
(iii) Study and Analysis of available authentication technique of Mobile Payment System which is identified as major security issue.
(iv) Design a solution for identified approach of authentication and user privacy protection.

(v) Implementation of a system for mobile payment which will be more secure against vulnerabilities like phishing, identity theft, man-in-middle attack, session hijacking, mobile device theft.
(vi) Evaluation of performance of developed system.

2. LITERATURE SURVEY

I studied many research woks mentioned as-according to Gao et al. [3], mobile payment refers to wireless-based electronic payment for m-commerce to support point-of-sale/point-of-service (POS) payment transactions using mobile devices. The account based payment systems which can be mobile phone-based, smart card or credit-card m-payment systems [4, 5, 6, 7]. S.S. Manvi, L.B. Bhajantri, M.A. Vijayakumar, "Secure Mobile Payment System in Wireless Environment"[10]. The proposed work introduces alternative ways for providing mobile banking services aimed at J2ME enabled mobile phones over Bluetooth communication. The scope of the proposed solution is the combination of J2EE and J2ME capabilities, means of overcoming the API and technical limitations, as well as security consideration. S. Kungpisdan, B. Srinivasan, and P. Dung Le,"A secure Account-based mobile payment protocol"[11]. In this paper, they had proposed a secure account-based payment protocol which is suitable for wireless networks. M. Hashemi and E. Soroush, "A Secure m-Payment Protocol for Mobile Devices" [12]. In this paper a secure m-payment protocol for mobile devices has been proposed. The Secure Electronic Transaction is a system for ensuring the security of financial transaction on Internet. SET have been designed to operate in a wired infrastructure [8, 9, 18], its transaction flow and implementation of security are very useful because we can apply that flow in wireless scenario. Using SET customer can make credit card payment to any merchant offering web based services.

3. DETAILS OF MOBILE TECHNOLOGY

3.1 Mobile Network Technology

Mobile Network technology have evolved from analog based system to digital based system and from circuit switched technology to packet switched technology. This evolution can be described by different generations of Mobile Technologies -1G, 2G, 2.5G, 3G.

3.2 Mobile Communication Services

SMS (Short Message Service), WAP(Wireless Access Protocol),USSD(Unstructured Supplementary Service Data),Cell Broadcast, SIM Toolkit, Web Clipping, Network Protocol (Infrared) are some Mobile Communication Services

3.3 Mobile Platform

Symbian was formed from Psion Software, by Nokia, Motorola, Psion (UK PDA manufacturer) and Ericsson in June 1398. The Series 60 Platform (Smartphone Platform), designed for Symbian OS, supports mobile browsing, multimedia messaging service (MMS) and content downloading, as well many personal information management and telephony applications. Microsoft has developed a lighter version of its Windows operating system, called Windows CE that has been created especially for small palm-size, hand-held PCs and other consumer electronics devices. Wysdom has recently developed a mobile network operating system called Wysdom MAP-OS.

3.4 Mobile Payment

Mobile Payment is defined as any financial transaction that is carried out via Mobile devices namely besides personal Mobile Phone any mobile instrument such as PDA(personal Digital assistant),Smart Phone, Tablets or merchant operated Mobile terminal could be involved in the Mobile Payment. All the actors are shown in figure 3

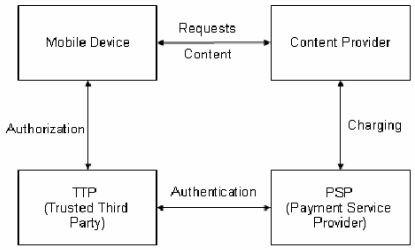

Figure-1: Relationships between all parties in a Mobile Payment System with participation from a Trusted Third Party

3.5 Generic Operations in Mobile Payment

All the interactions among the actors are shown in figure 4. Service Registration, User Registration, Request Service, Request Charging Session, Request Authorization and Authentication, User Authenticated, Provide Content or Service, Charge.

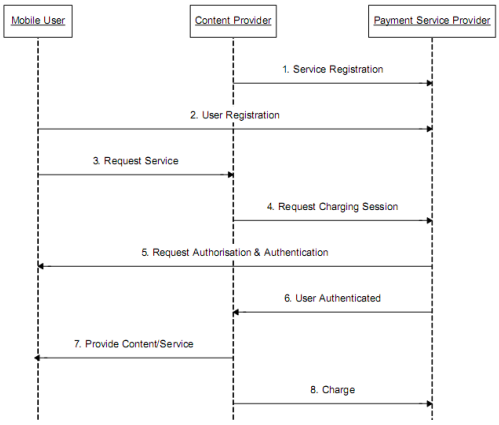

Figure-2: Generic Operations in a Mobile Payment System

3.6 Factor for authentication

3.6.1 Authentication Methodologies

Existing authentication methodologies have basic three "factors" [1]

1) Know: The user knows (password, PIN)
2) Has: The user has (ATM card, smart card)
3) Is: The user is (biometric characteristic such as a fingerprint)

Authentication methods those are based on more than one criterion are more difficult to break and secure than single criterion based methods and hence more secure.

3.6.2 Selection of an Authentication key

Selection of a correct authentication key is one vital feature of securing online services-

(i) **Passwords:** A password is a type of secret authentication data which grants access to only authorized users. The password is known to the only authorized users and unauthorized persons are unaware of this, and user wish to gain access must be tasted to verify the authenticity of the user by checking the password.

(ii) **Hardware tokens:** A hardware token is physical device and it is a hardware implementation of the authentication device attached to an authorized user's computer.

(iii) **Software tokens:** Software tokens are similar to hardware tokens. It is software implementations of hardware tokens.

(iv) **One-time passwords:** The one-time password (OTP) based system is more secure than ordinary password based system, it is difficult break and secured from unauthorized users. In this type of system passwords get updated constantly, for each access user has new password so it reduced the risk.

(v) **Biometrics:** In Biometric authentication human physical and behavioral characteristics are used to verify the identity of the user.

4. SYSTEM REQUIREMENTS

4.1 Functional Requirements

The goal of the project is to construct a system that enables payments very securely. The criteria to be fulfilled by the system in terms of functionality are:

(i) The system should be a secure means of authorization of payments, either on credit or direct debits to avoid phishing and user identity thefts.

(ii) There are six actors that interact with the system: *the merchant, the mobile user, the financial service provide(bank) and the mobile device*

(iii) The system should enable merchants to register payment transaction requests, with details about the payment transaction into the system.

(iv) The system should maintain payment information including the status of the payment transaction requests in the system.

(v) The system should be able to verify the mobile user's validity.

(vi) The system should be able to protect against attack like phishing, user identity theft, session hijacking ,mobile device theft and virus attack

(vii) Multiple mobile users request can be handled.

4.2 Non-Functional Requirement

Scalability, Modularity, Authentication, Authorization, Performance, Usability, Maintainability are some Non-Functional Requirements

5. SYSTEM ARCHITECTURE

We need a strong authentication mechanism when using electronic transfer systems. Authentication based on single criterion is considered to be inadequate for this purpose to secure a financial transaction against user identity theft, session hijacking, virus attack, mobile device theft [25]. Thus, we need authentication based on different factors and also at different level. System architecture diagram is shown in figure 5.

1) Basic user Id-password Authentication: User need to enter his user Id and password to access the system allotted at the time of registration. This is the simple web based authentication.

2) Interactive key interchange: In this, first user makes a request to access system by providing user Id -password. Then System sends a challenge for key1 based on user Id and password information. If key1 is there with the user then it assumes that it is true service provider and then send key2 corresponding to key1. After receiving key2 from user, system once again checks the identity of user whether it is legitimate user or not. If system having key2 then allow user to make payment otherwise not allow further access. In this way communicating parties are validated with intense care to avoid any kind of fraud. Both keys are encrypted make system more secure.

3) Transaction number Validation: This is the technique which is used to identify both the user and the ongoing transaction. Transaction number certifies that the current transaction has been initiated by the right person and it is a valid user who is trying to access his/her account.

4) SMS verification: After the transaction number identification and validation the remaining transaction will proceed. At the end of the transaction the user will get an SMS from the system to confirm his/her financial transaction. By this SMS user can confirm their transaction by responding "yes" or "no". If user chooses yes then transaction would be committed on the server and if the user denied then transaction would be cancelled.

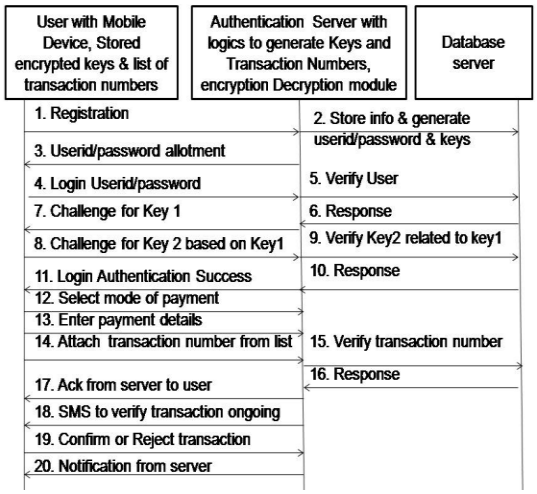

Figure-3: The system architecture

5.1 Algorithm for developed system for authentication

Step 01: Start.
Step 02: Validate user.
Step 03: Is legitimate user? "YES" go to step 4 else go to step 2.
Step 04: Send challenge for key1.
Step 05: Is key1 valid? go to step 6 else go to step 21.
Step 06: User send challenge for key2.
Step 07: Is key2 valid" go to step 8 else go to step 21.
Step 08: Send payment mode selection page.
Step 09: Credit card mode selected.
Step 10: Send credit card provider bank list.
Step 11: Select bank.
Step 12: Send Credit card type selection page.
Step 13: Select Credit card type.
Step 14: Send payment detail form.
Step 15: Fill payment details. If details are valid go to step 16 else go to step 15.Step 16: Attach TIC codes.
Step 17: Is TIC code valid? "YES" go to step 18 else go to step 21.
Step 18: Send waiting message to user.
Step 19: Send SMS confirmation page. If "YES" go to step 20 else go to step 21.
Step 20: Proceed with transaction.
Step 21: Stop.

5.2 Snapshots

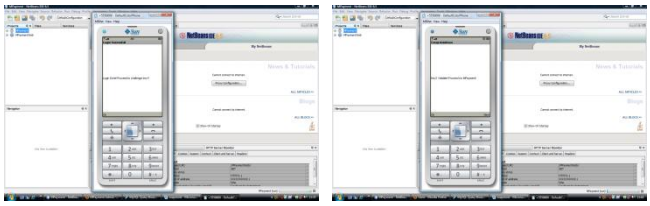

Figure 4: User login successful and do challenge for key1 and key2 form

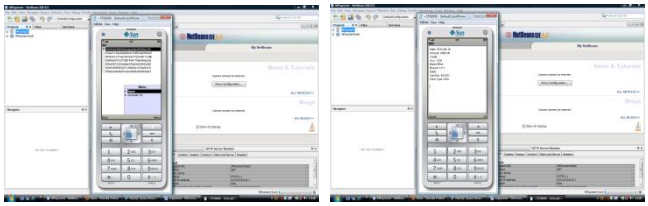

Figure 5: **Transaction Numbers and SMS verification**

6. CONCLUSION & FUTURE WORK

6.1 Conclusion

Security is a major issue in all online payment mechanism. It is very much needed that any financial service provider providing any kind of financial service must provide effective means of authentication scheme so that no fake user can make monetary transaction by hacking user's credential.

The available authentication techniques for mobile payment system are not enough secure since they are susceptible to various kinds of attack like loss of user's confidential information, identity theft, mobile device theft and virus. But an authentication approach based on multiple criterions at multiple levels [1, 2] can provide solution for identified security issue. We have studied this available approach, added a new criterion of authentication, implemented and analyzed the results. With the identified problems in available authentication approach, only one party is validated who initiated the payment request not who providing the service which is mainly responsible for above mentioned attacks. Now both the parties are getting validated properly with suggested authentication criterion

6.2 Future Work

(i) We can focus on developing a new and efficient way for key and transaction number generation logics and transmission from sever to user end.
(ii) We can focus on more strong encryption and decryption algorithms.
(iii) We can add some more criterions to authenticate which will take less time in computation and harder to crack.

REFERENCES

[1] Guidelines: "Guidance on Multi-factor Authentication", e-GIF Operations, State Services Commission, Wellington, Version 1.0, June 2006. (http://www.e.govt.nz)
[2] Website on Authentication: http://www.authenticationkeys.com.
[3] J. Gao, J. Cai, K. Patel, and S.Shim (2005), "Wireless Payment", "*Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05)*", pp. 367-374.
[4] S. Kungpisdan, B. Srinivasan and P.D. Le, (2004), "A Secure Account-Based Mobile Payment Protocol", *Proceedings of the International Conference on Information Technology: Coding and Computing*, IEEE CS press, pp. 35-39.
[5] Y.B. Lin, M.F. Chang, H. C.H. Rao, (2000), "Mobile prepaid phone services", *IEEE Personal Communications*, vol. 7, pp. 6-14.
[6] A. Fourati, H.K.B. Ayed, F. Kamoun, A. Benzekri, (2002), "A SET Based Approach to Secure the Payment in Mobile Commerce", *In Proceedings of 27th Annual IEEE Conference on Local Computer Networks*, pp. 136 – 140.
[7] Huang Z., Chen K., (2002), "Electronic Payment in Mobile Environment", *In Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA'02)*, pp. 413 – 417.
[8] J. Hall, S. Kilbank, M. Barbeau, E. Kranakis (2001), "WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks", *IEEE International Conference on Telecommunications (ICT)*.
[9] V. Pasupathinathan, J. Pieprzyk, H. Wang and J.Y. Cho, (2006), "Formal Analysis of Card-based Payment Systems in Mobile devices", *Fourth Australasian Information Security Workshop, Conferences in Research and Practice in Information Technology*, Vol.54, pp. 213-220.
[10] S.S. Manvi, L.B. Bhajantri, M.A. Vijayakumar, "Secure Mobile Payment System in Wireless Environment", *International Conference on Future Computer and Communication*, 2009 icfcc, pp.31-35S. Kungpisdan, B. Srinivasan, and P. Le. "A secure account-based mobile payment protocol". *In Proceedings of International Conference on Information Technology:Coding and Computing*, 2004.
[11] M. Hashemi, E. Soroush, "A Secure m-Payment Protocol for Mobile Devices", 19th Annual Canadian Conference on Electrical and Computer Engineering, 7-10 May 2006, Ottawa, Canada.
[12] *http://www.w3schools.com/XML/xml_whatis.asp*.
[13] *http://en.wikipedia.org/wiki/XML*.
[14] Latha Srinivasan, Jem Treadwell, "An Overview of Service-Oriented Architecture, Web Services and Grid Computing", *http://h71028.www7.hp.com/ERC/downloads/ SOA-Grid-HP-WhitePaper.pdf*, November 3, 2005.
[15] D. Box, "Simple Object Access Protocol (SOAP) 1.1", *W3C Note 08, World Wide Web Consortium*, *www.w3.org/TR/SOAP/*, May 2000.
[16] E. Christensen, F. Curbera, G. Meredith, S.Weerawarana. "Web Services Description Language (WSDL) 1.1", *W3C Note 15, World Wide Web Consortium, http://www.w3c.org/TR/wsdl*, March 2001.
[17] Jerry Gao, Krishnaveni Edunuru, Jacky Cai, and Simon Shim, "P2P-Paid: A Peer-to-Peer Wireless Payment System", In Proceedings of the Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05), Munich, Germany, pp. 102-111, July 2005.
[18] "OASIS UDDI Version 3.0.*1", UDDI Spec Technical Committee Specification*, *http://uddi.org/pubs/uddi_v3.htm*, 2003.
[19] Teppo Halonen, "A System for Secure Mobile Payment Transactions", Supervisor: Professor Teemupekka

Virtanen, Helsinki University of Technology, Department of Computer Science and Engineering, January 2002.

[20] Peeter Paal, "Java 2 Platform Micro Edition", Helsinki University of technology,Telecommunications Software and Multimedia Laboratory, 2000.

[21] Vartan Proumian , "Wireless J2ME Platform Programming", Sun Micro system Press, Java Series, April 2002.

[22] Lawton G., "Moving Java into Mobile Phones", IEEE Computer, Volume 35 Issue 6, pp. 17- 20, June 2002.

[23] Website on java Servlet: http://java.sun.com/products/servlet

[24] Website on Web Server: http://tomcat.apache.org/

[25] Guidelines : "Authentication in an Internet Banking Environment ", Federal Financial Institutions Examination Council, Arlington, (http://www.ffiec.gov)

.

BIOGRAPHIES

Mrs Smita Parte currently working as Assistant Professor in TIT College Bhopal M P 462021

Ms Noumita Dehariya currently working as Assistant Professor in TIT College Bhopal M P 462021