A Secure Account based Mobile Payment Protocol with Public Key Cryptography and Biometric Characteristics

Pawandeep Singh Aujla[1], Harneet Arora[2]

Department of Computer Science & Engineering, Sri Guru Granth Sahib World University
Fatehgarh Sahib, India

gillharman888@gmail.com
harneet159@gmail.com

Abstract: ***The way people do the business and transactions are changing drastically with the advent of Information Technology. The customer wants to access information, goods and services any time and in any place on his mobile device. Receiving financial data, trade on stock exchanges, accessing\balances, paying bills and transfer funds using SMS are done through mobile phones. Due to involvement of valuable financial and personal information, the mobile phones are vulnerable to numerous security threats. Most common activity in M-Commerce is the payment to the merchant using a mobile phone. In this paper we present a secure account–based payment protocol which is suitable for M-commerce to transfer the payment from wireless networks based on public key cryptography. Based on author knowledge, this is a first kind of protocol which applies public key cryptography to mobile network and satisfies all the security requirements of the properties provided by standard protocols for wired networks such as SET and iKP.***

Keywords: Electronic commerce protocol, Mobile payment, Wireless payment, Credit card payment, Cryptographic Protocol, Account Based protocol, Finger print Scanner.

1. Introduction

Mobile commerce is a powerful technology which is a result of combining two strongly emerging trends: electronic commerce and wireless computing. Internet + Wireless + E-Business = M-Commerce. M-Commerce represents extended application of e-commerce in which user uses a mobile phone or PDA to do business. Mobile phones are most common devices to do business and commerce today and the trend is increasing due to involvement of huge financial and personal data transferring (PIN, Band Account no). The rapid use of M-Commerce demands the means for secure mobile payments. Lack of efficient protocols makes the security issue of mobile networks more challenging. In this paper, we present an account-based payment protocol for wireless networks based on public key cryptography. The public key cryptography can provide the Authentication, Confidentiality, Integrity and non-repudiation.

A. General Model for Payment Transactions

A general account–based payment model [4] involves 4 parties. Buyer(who makes the actual payment through mobile phone), Seller(who receives payment), Issuer (Bank or Buyer financial institution) , Acquirer (Bank or Seller financial institution). An additional party called Payment Gateway which acts an interface between the mobile payment world and existing payment infrastructure. Payment Gateway plays a major role between Issuer and Acquirer for the settlement of the transaction. The complete payment system is operated by payment system provider who maintains a relationship with banks (Issuer, Acquirer). The graphical view of typical online payment system is represented below [8].

B. Public Key and Cryptography in Mobile Networks

Mobile networks have limitations [3, 5, 6] such as Low power storage capacity, Computational capability, Resources, Battery Constraints, makes the public key cryptography infeasible for them. In 2009, a new standard was proposed for public key cryptography by name NTRU cryptosystem [9]. The results shows that NTRU algorithm is much faster than RSA, the key size is one quarter than RSA with similar security level as RSA and key generation time is 200 times faster than RSA as presented in shen et al. NTRU is 1133 times faster than 2048-bit RSA when compared the data throughput (Hermans et al).The NTRU algorithm was approved by the IEEE in February 2009 as public key algorithm with standard 1363.1.The usage of NTRU provides the same level of security provided by RSA and it is having the ability to work in limited computing environments. These properties made NTRU are an efficient public key cryptography algorithm for mobile networks.

C. Scope of Public Key Cryptography in the Proposed Protocol The issuer is the main source of financial transactions from where the actual fund is transferred to Acquirer by the payment Gateway. In the proposed protocol, the issuer and the Buyer possess the individual public key pairs and thus can generate digital signatures. In public key cryptography; the public key must be certified. We assume a Certification Authority, CA, authenticate the public key of Issuer and Buyer.CA certifies the public key of Issuer using its private key CAPvtKey. The public key of CA is conveyed in an authenticated manner to all the entities involved. This can be done through any efficient algorithm.

D. Related Work

In this section several existing standard payment protocols are analyzed briefly. Secure Electronic Transaction (SET)

Protocol: SET is set of security protocols enables users to employ the existing private credit card payment infrastructure on an open network, such as Internet in a secure fashion. Cardholder, Seller, Issuer, Acquirer, Payment Gateway, and Certification Authority forms the major participants in the protocol. SET is public key cryptography based protocol. The SET protocol supports three types of transaction steps which are Purchase request, Payment authorization, Payment capture [7,8]. iKP Protocol: The iKP(i-Key Protocols) where i=1,2,3 is a set of payment protocols. Three parties are involved in IKP: Buyer, Seller, and Acquirer gateway. iKP is based on public key cryptography .i value indicates the number of parties possess the public key pairs and can generate digital signatures. As i increases from 1 to 3, the security requirements met by iKP increases [2]. The major drawback of SET and iKP protocols is that they can be successfully implemented for wired networks but not for mobile networks in terms of computation and security. SET and iKP are based on public key cryptography which involves high computational operations such as public key encryptions and decryptions. A Certification Authority (CA) is needed to authenticate the public keys possessed by the engaging parties. The public key of the Certification Authority must be transmitted in a secure manner to all the parties which increases the number of messages exchanged. The SET and iKP uses RSA algorithm for encryption which makes the system slower. In our algorithm we use NTRU algorithm which faster than RSA.

2. My Contributions

We present a protocol based on public key cryptography based on the work done in NTRU for mobile networks which provides all the security requirements [1] in mobile payment transactions. Till now public key cryptography is used only for wired networks (Desktop). Similarly Symmetric key is used for wireless networks. The advantage of Asymmetric key over Symmetric key is non repudiation. The non repudiation property ensures that a party cannot deny the transaction she originated. In financial transactions non repudiation is a most important factor. Symmetric key may suffer from MAC attacks. To the best of Authors knowledge it is the first protocol to be used for Mobile networks based on public key cryptography. The non-repudiation cannot be proved from symmetric key cryptography as the key is shared between two parties.

3. Security Requirements in M-Commerce

In this section we analyze the security requirements [1] for a Mobile Payment in view of the above mention system entities. Buyer (B), Seller (S), Issuer (I), Acquirer (A), and Payment Gateway (PG). Party authentication: The receiver must know the sender of the message is the intent and valid sender.

Transaction privacy: All the transactions must be secure. Proof of transaction authorization by user: When an Issuer debits certain amount from certain credit card; the issuer must possess unforgettable proof that the owner of the credit card has authorized the payment. The Issuer also need to take care of replay attacks, the amount, currency, order description Impossibility of unauthorized payments : It must be impossible to for adversaries to get the Credit Card Number and PIN from the payment transaction and use it later.

4. Multifactor Authentication

Single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. To provide secure web transactions using cell phones multi factor authentication techniques have to be used. In our system we are using multi factor authentication using two different modes. The implementation is performed using Biometric Properties and SMS. While SMS has been used in previous approaches to the problem, we are introducing the new concept of Biometric Properties as a novel method of authenticating a transaction and the user.

A. Biometric Authentication

Biometric Authentication is the technique which is used to identify both the user and the ongoing transaction. It 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.

Biometric Identification is:

* Image of finger-print is created by user itself.
* Image is generated with the help of inbuilt finger-print scanners on the devices which are used by users.
* This image is encrypted using public key cryptography before send through the wireless media.

The Bank or Financial institution will keep a record of users finger-print and match the same during the online web transaction.

B. SMS Authentication

Another method to validate user transaction is an SMS confirmation. The Bank or financial institution stores user cell phone number to provide multifactor authentication. We believe that users will carry their cell phone and can receive and send the short message. As a result, only valid users who have account will receive confirmation SMS from the authentication server.

After getting an SMS the user can acknowledge the choices. When authentication server receives “YES” it knows that the user is valid and the user has approved their initiated transaction. On the other hand, if the user sends a “NO” or the user does not send any response within a specified time period then the transaction will be rolled back and terminated.

C. Secure Web Authentication Protocol

This shows the Protocol for secure web authentication using Mobile devices. This protocol starts with the action of money transfer decided by user. Here we assume that the user information is available at server which includes

user's cell phone number. A separate authentication server is recommended to maintain strong security to authenticate users and their transactions with regular web and database servers of user information.

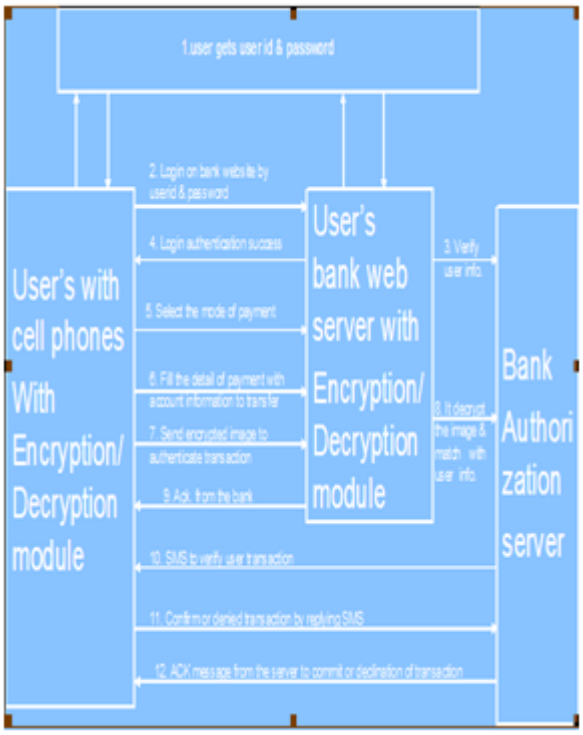

Figure 1: Multifactor secure Web authentication protocol using mobile

Below we describe each step of the above protocol.

1. User gets username & password from the Bank. Each user has only one username/password to their account.
2. A Web-based username/password basic authentication is used to identify the user to the Web server.
3. The username and password will be verified by the Bank Authentication Server. After user recognition the user will get option screen to proceed further.
4. The user will get a notification of a successful logging with welcome message. This step also generates a session key.
5. The user will select mode of payment. We have considered two modes of payment: Credit Card based system & Account based Electronic transfer. It is straightforward to add other modes to our system.
6. User will insert the details of payment by filling in a simple form with details such as merchant's bank and branch code information, invoice number and account number to which an amount has to be transferred.
7. The user generates an image of finger-print using finger-print scanners which is inbuilt in the mobile device. All details of the transaction, with attached image, will be further encrypted by NTRU encryption technique and submitted to the bank web server. The bank web server would pass it on to the authentication server where it would be decrypted and matched with the finger-print image which is stored in the user's information on server side.
8. The bank authorization server decrypts the received message. It then verifies the image received from the user by comparing it with the stored image in the user account information at server database. If both images match then it goes to the next step. If no image matched with those in database then the authentication server will deny the user transaction and display appropriate error message to the user.
9. Bank server generates an acknowledgement to the user, which makes user free to logout from the web portal and wait for a confirmation SMS or to initiate another financial web transaction.
10. After completing the database updation with respect to the ongoing transaction, the authentication server will send an SMS to the user's cell phone to verify the initiated web transaction. The cell phone number of the user is available on authentication server.
11. The user would confirm their initiated transaction by choosing "YES" or deny it by choosing "NO" by replying confirmation SMS.
12. The server will notify the user by a Message to acknowledge the successful completion of transaction or declination of the transaction.

5. Security Requirements Met by the Proposed Protocol

Party authentication: All the messages in the proposed protocol are encrypted with the shared keys between entities. As the key is shared between two entities only, the receiver can assure that the message comes from the Authenticated party only.

Transaction privacy: All the transactions are encrypted with the sharing keys and the message contains CCN and PIN double encrypted, hence the privacy is guaranteed.

Transaction integrity: All the transactions are concatenated with the hash of the entities involved, which ensures integrity of the message to the receiver.

Proof of transaction authorization by user: The message sent to Issuer contains public key of Buyer (BPubKey). The message is encrypted with Public key of Issuer which can be decrypted only with Issuer private key. Hence the message is unaltered by any means. On decryption, the Issuer retrieves the public key of Buyer which confirms the Issuer that the transaction is authorized. Impossibility of unauthorized payments: To send a legitimate payment message to Issuer, the adversary must know the CCN, PIN, EXPIRATION, without knowing this he cannot create a fake request. The CCN, PIN, EXPIRATION are sent in a secure format using the Public key of Issuer, to decrypt the fraudulent must need the private key, which is not possible.

6. Performance Analysis of the Proposed Protocol

In this section we compare our protocol with SET [7] and iKP [2] protocols which are standardized protocols for e-commerce transactions in wired networks. The below table demonstrates the number of cryptographic operations involved at each party.

Cryptographic Operations		SET	iKP	ours
Public key Encryptions	B	1	1	1
	S	1	-	-
	PG	1	-	-
Public key Decryptions	B	-	-	1
	S	1	-	-
	PG	2	1	-
Signature Generation	B	1	1	-
	S	3	3	-
	PG	1	1	-
Signature verification	B	2	3	-
	S	2	2	-
	PG	1	2	-
Symmetric key Ency/Decr	B	2	-	3
	S	-	-	6
	PG	-	-	2
Key Generation	B	-	-	1
	S	-	-	2
	PG	-	-	1

Figure 2: Comparison of Cryptographic Operations of SET,iKP and ours protocol

We can see that in our protocol only one public key Encryption and one decryption are done by Buyer. The key generation process is required to update the keys regularly. However, this would not cause the time consumption as this can be done offline.

7. Conclusion

We have proposed first of its kind of account based protocol based on public key cryptography which is applicable to wireless networks. We have shown that the proposed protocol has advantages over SET [7] and iKP [2] protocols, in that it has lower computation at each party since only two public key operations are required. In our protocol, Buyers can ensure that their account information will not be compromised by any parties involved. As a result with our proposed protocol the mobile users can have efficient and secure payments and it may gain more acceptability than existing protocols.

References

[1] V. Ahuja, Secure Commerce on the Internet, Academic Press,1996

[2] 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 iKP Secure Electronic Payment System , IEEE Journal of Selected Areas in Communications, 2000.

[3] S. Cimato, Design of an Authentication Protocol for GSM Javacards, LNCS Vol. 2288, 2002, pp. 355-368.

[4] E. V. Herreweghen, Non-Repudiation in SET: Open Issues, LNCS Vol. 1962, 2001, pp. 140-156.

[5] S. Kungpisdan, B. Srinivasan, and P. D. Le, A Practical Framework for Mobile SET Payment, Proceedings of International E-Society Conference 2003, pp. 321-328.

[6] L.M. Marvel, Authentication for Low Power Systems, Proceedings of IEEE MILCOM 2001.

[7] MasterCard and Visa, SET Protocol Specifications, 1997.http://www.setco.org/set_specifications.html

[8] William Stallings “Cryptography and Network Security Principles and Practices” Fourth edition PHI.

[9] J.Hoffstein, J.Pipher and J.Silverman. NTRU: A ring based public key cryptosystem,Algorithmic Number Theory (ANTS III),Portland, OR, June 1998,Lecture Notes inComputer Science 1423.

Author Profile

Pawandeep Singh Aujla is currently studying in SGGS World University, Fatehgarh, in department of computer science and engineering. He received his Bachelor’s in Technology degree in Computer Science from Punjab Technical University, India. His areas of interest include Multifactor Security Protocol for Wireless Networks and software engineering. Currently he is doing research in field of “A Multifactor Security Protocol for Wireless Payment-Secure Web Authentication using Biometric Characteristics”.

Harneet Arora is an Assistant Professor in Department of computer science and engineering at Sri Guru Granth Sahib World University, Fatehgarh Sahib. She holds a Master of engineering degree in from Punjab University, Chandigarh. She has published several papers in the field of wireless sensor networks. Her research interests include Wireless Networks, Grid computing, Artificial Intelligence and Information Retrieval.