Transaction Security of Mobile Payments Using IMEI number and Call Back Technique

Sonali Bhutad , Prof. Sachin Bojewar , kajal Jewani
Department of Computer Engineering, Vidyalankar Institute of Technology , Wadala, Mumbai ,India
sonalibhutad@gmail.com,sachin.bojewar@vit.edu.in
jewani_kajal@yahoo.co.in

***Abstract*—Growing of wireless networks and popularity of handheld devices such as mobile phones represents an incredible opportunity to give power to mobile devices as a payment device. Unfortunately, some problems like limitation of power, less powerful processor of mobile phones needs new suitable algorithm for mobile phone payment. Recently, many public key cryptography algorithms are presented for mobile payment . However, limited capabilities of mobile devices and wireless networks make these algorithms unsuitable for mobile network. In this paper a new security algorithm for mobile phones based on call back technique and one time password using IMEI number is developed .This algorithm provides the required security for mobile payment regarding resource restrictions. The simulation results on prototype data indicate the efficiency of the proposed algorithm.**

***Keywords— call back, IMEI, one time* password, security**

I. INTRODUCTION

Mobile payment is the payment (transfer of funds in return for a good or a service) where the mobile phone is involved in the initiation and confirmation of the payment.

Although, there are many developed encryption algorithms, they can't be used directly in mobile phones. There are three main reasons for this problem. First, most of the mobile phones have not been equipped with powerful CPU and have limited amount of internal memory. Therefore they do not have enough capability to perform high level encryption. Meanwhile, most of the mobile phones have not been equipped with special processors for performing special type of calculations which need more time for processing. Secondly, wireless networks have lower bandwidth and less reliability as compare to wired networks. Therefore establishing security in wireless networks is more difficult than that in traditional wire networks. Finally, cryptography is necessary for establishing security in mobile payments. However, the complexities of cryptographic algorithms are not usually specified for users. When these complexities become revealed, the acceptance of these algorithms will be difficult. [2]- [3]

In the algorithm proposed in this paper ,the mobile number (which is registered at the relevant Financial Organization beforehand)is used in conjunction with the encryption methods used in transactions. In spite of the Personal Computers and the systems being connected to the wired networks, the mobile systems uses batteries with limited energies. These problems all direct us to develop a new security algorithm based on mobile phone resources.

This algorithm uses the following terms:

A. IMEI number

The International Mobile Equipment Identity or IMEI is a number, usually unique to identify GSM or CDMA mobile phones. It is usually found printed inside the battery compartment of the phone. The IMEI number is used by the GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing the network in that country. For the proposed algorithm, password generator program is stored in the handset, therefore IMEI plays important role in handset authentication.

B. Call Back Technique

When a user connects to a server and confirms the username and password, the server disconnects the user connection and tries to connect to the user directly. This technique is applied in the Windows Server operating system for confirming the identity of the dial up users. Phone number of every user is registered in him/her specification. If any user account has been stolen or another person tries to connect to the server, he is only able to communicate by its line through which its number has been registered in the server.

C. One Time Password

Password for every transaction will be generated using IMEI number which is unique. Same password is stored on the server, which uses same software generator program where it can be crosschecked for authentication.

III. LITERATURE SURVEY

Consider a scenario, where we have three accounts in different banks and hence three credit/debit cards. We need to remember three passwords and keep them secret. If we lose these cards, we need to inform three organizations to

lock the accounts temporarily and reissue new password for these accounts. Even the latest authentication technology, such as 3-D Secure [4] developed by Visa, uses a PIN/Password based authentication for its card holders and it inherits similar authentication drawbacks as the traditional systems [2].

Another issue is about use of cryptography algorithms on limited resources of mobile phones. Basically, the cryptography is an operation which needs many processes to be executed. As the complexities of the algorithm increase, the number of processes will also be increased . Therefore, generally for cryptography, strong processors should be used. Meanwhile, as a result of using more processes, and more strong processors, more power will be consumed. Although the security of encryption algorithms is very important, however, for mobile payment, they are limited to the mobile phone resources such as processor capabilities and memory capacity. The rate of consuming energy is another important factor in selecting algorithm for such systems.

In the next section, we will explain the proposed method for mobile phone payment using above technique together with one time password generation. In one time password generation using IMEI, a password can only be used one time and it is impossible to use it again.

A. Mobile Payment Solutions

Mobile payment solutions may be classified according to the type of payment affected, and based on the technology adopted to implement the solution. There are a variety of combinations of these frameworks , technology adopted and mode of payment, a survey of which would constitute a study in itself. There are three different models available for m-payment solutions on the basis of payment:

1. Bank account based
2. Credit card based
3. Telecommunication company billing based

1). *Bank Account based M-Payment*

Banks have several million customers and telecommunication operators also have several million customers. If they both collaborate to provide an m-payment solution it is a win-win situation for both industries. In this model, the bank account is linked to the mobile phone number of the customer. When the customer makes an m-payment transaction with a merchant, the bank account of the customer is debited and the value is credited to the merchant account.

2). *Credit Card based M-Payment*

In the credit card based m-payment model, the credit card number is linked to the mobile phone number of the customer. When the customer makes an m-payment transaction with a merchant, the credit card is charged and the value is credited to the merchant account. Credit card based solutions have the limitation that it is heavily dependent on the level of penetration of credit cards in the country. In India, the number of credit card holders is 15 million. Only this small segment of the population will benefit in the credit card based model.

3). *Telecommunication Company Billing of M-Payments*

Customers may make payment to merchants using his or her mobile phone and this may be charged to the mobile phone bills of the customer. The customer then settles the bill with the telecommunication company This may be further classified into prepaid airtime (debit) and postpaid subscription (credit) Proposed algorithm uses Bank Account based mobile payment solution .

.

IV. PROPOSED METHOD

In our proposed method, the phone number, the phone serial number and the username account are registered inside the payment server. A password generator program is run on the server as well as on the mobile phone. The customer receives one password by executing the password generator program from his / her mobile phone. When user connects to the payment server, phone serial number and the user name account is checked by the payment server. Payment server will check authorized handset using IMEI number. Every generated password will be kept in phone memory for establishing security for the next payment. Afterward, the payment server will reconnect to the customers' mobile phone using call back technique. The payment server receives the password of the previous transaction from mobile phone. When the password of previous transaction becomes confirmed, the transaction will be performed and completed. Fig.1 shows the process of the proposed method. The password generator software is installed on the mobile phone. It produces the encrypted passwords which are also available in the payment server. Accessing this software can be done using user account.

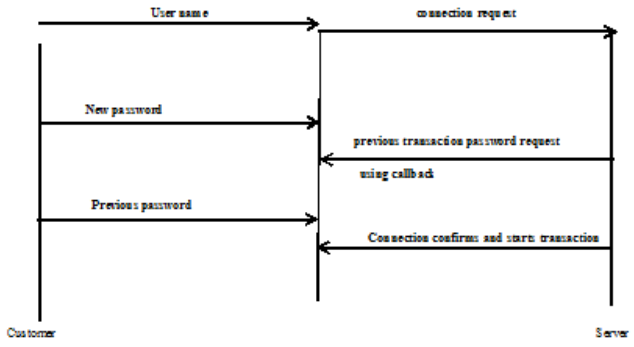

Fig 1: The Security process of the proposed method

The encrypted passwords are kept on the password generator program of the mobile phone. The decryption operation is only performed in order to check the password on the server. There is no need for any cryptographic algorithm on the mobile phone.

This will overcome the restriction of processor and memories of mobile phone systems. Even if it is necessary to have the previous password for starting a new transaction, it will increase the security of the payment. Actually, in this method two passwords are used. One of them is new and the other is the previous password. Firstly the new password is encrypted, then it is decrypted in server and finally it will be compared with the available passwords. When it is verified, the new password will be removed from the passwords of server and it is kept for the next transaction. After connecting the mobile phone to the payment server, the authentication of user account with the username and the new password will be done. Then, the primitive connection will be interrupted and the server reconnects to the mobile phone. It requests for the previous transaction password. If server password is similar to the received password of mobile phone, these same passwords will be removed and transaction will be performed.

V. ADVANTAGEOUS

The proposed method uses four different elements for establishing the security:

1) *Username and Password:* These two elements are used for every transaction.

2) *The phone serial number:* Known as Device ID, is unique. It provides more security together with the phone number.

3) The one time passwords: They are produced by the password generator program which is also safe against interception.

4) *Call back technique:* make people sure about the required security of mobile phone payment.

Based on call back technique, after user is connected to the payment server, the primitive connection will be interrupted and the server itself restarts the communication with the mobile phone and the previous transaction password will be requested for confirmation. As a result of confirmation, the previous transaction password will be sent and the transaction will be completed.

If any unauthorized person gets access to the password creator program, he/she is only able to have a communication with server and cannot perform the transaction. Because based on call back, the server will reconnect to the actual mobile phone. Even if the abuser has the phone device itself, the previous transaction password should also be known. As a result of using one time password, even when the mobile phone is stolen, the communication with payment server cannot be established because the software of the password creator must be activated by username and password account. In the wireless communications, signals are distributed in the surroundings and the passwords can be intercepted by unauthorized persons. In the proposed method, the problem of unauthorized persons listening and intercepting the secret information has also been solved; because one time password is used.

Other benefits of the proposed method are:

- Complicated algorithms such as public key are not required.
- There is no need to use phones with fast and powerful processors and high memory capacity because complicated cryptographic operations are not used in the mobile phone.
- The level of security in this system is very high because one time passwords and call back technique are used together. In this new method, authentication, integrity and authorization all are provided. This system establishes all security factors regardless of encryption or decryption in the mobile phone.

At first the cryptographic system compares the time required for our proposed method with that of other state-of art algorithms.[1] The proposed algorithm is equal to the production of the smallest key in the cryptography process. The mobile phone only produces max 32 bit passwords. The new algorithm is appropriate for mobile phones which have limited resources produces one key, and then the cryptography is performed by using this key.

The complexity of almost all the existing mobile payment methods, cryptographic algorithms are used for security establishment. Such cryptographic systems use a key for encryption and decryption and the crypto time depend on cryptographic key length. Table I. shows a comparison between time consuming between our proposed method and other state-of art algorithms.

TABLE I. A COMPARISON BETWEEN USUAL CRYPTOGRAPHIC KEYS AND THE PROPOSED METHOD

Key length	Time to key Generation	Encryption	Decryption
64 bits	1.8ms	2.2ms	2.8ms
128 bits	2.1ms	3.2ms	3.4ms
192 bits	2.6ms	3.6ms	4ms
256 bits	2.9ms	5.4ms	7ms
32 bit Password for Our proposed	1ms	--	--

algorithm			

However, in the proposed algorithm process time for generation of one time password is very short because these passwords have a 32 bit length which is shorter than the cryptographic keys.

VI. CONCLUSION

In this paper, we have proposed a simple and efficient IMEI-based authentication mechanism along with callback technique for electronic transaction systems. The password generated by the user's mobile phone is verified by the payment server using direct communication with the user. Thus it provides far greater security than the credit card based authentication mechanisms. With the widespread use of GSM technology worldwide, the proposed algorithms can be implemented to provide enough security on most of the mobile phones which have only limited hardware resources.

REFERENCES

[1] Reza Javidan, M. A. Pirbonyeh" ANew Security Algorithm for Electronic Payment via Mobile Phones"

[2] P. Raju – atom technologies limited. A.Gajwani – B. TeleservicesLimitedProf. T.A. Gonsalves – IIT Madras. Ch.RajaSrinivas – TataTele Services Limited Mobile

[3] L.R.Liang, S.Nambiar, C. Lu."Analysis of Payment Transaction Security in Mobile Commerce", Dept.of Computer Science.Department of Computer science university of of the District of Columbia . Virginia Polytechnic Institute and state university washington,2004

[4] Christos Douligeris, DimitriosN. Serpanos,"Netw Security"Current Status and Future Directions.Copyright © 2007 by the Institute of Electrical and Electronic Engineers, Inc. All rights reserved .Published by John Wiley and Sons, Inc., Published simultaneously in Canada

[5] D.Salama,A.Minaam1,H.M.AbdualKader2,andM`Mohamed Hadhoud2,"Evaluating the Effects of Symmetric Cryptographic Algorithms on Power Consumption for Di®erent Data Types", Higher Technological Institute 10th of Ramadan City1 Faculty of Computers and Information