MOBILE PHONE ELECTRONIC PAYMENT BASED ON CALL BACK TECHNIQE AND ONE TIME PASSWORD

MOHAMMAD AMIN PIRBONYEH
Computer Engineering Department
Islamic Azad University,Kazeroon Branch
Fars -Iran

REZA JAVIDAN
Computer Engineering Department
Islamic Azad University, Beyza Branch
Fars - Iran

ABSTRACT

Financial payment via mobile phones, mobile payment, as a subset of electronic payments has encountered many challenges regarding security because of public dispersion of mobile phone which increase the possibility of eavesdropping and abusing. Although this problem can be removed by using encryption protocols, however, restrictions in hardware resources of mobile phone such as low transition rate and low bandwidth of communication channel, limited calculation capacities of processor, battery and memory, prevent from direct usage of available encryption protocols in this environment. In this paper a new security algorithm for mobile phones based on call back technique and one time password is developed. This algorithm provides the required security for mobile payment regarding above resource restrictions. The simulation results on prototype data indicate the efficiency of the proposed algorithm.

Keywords: Mobile phone; security; call back; one time password*; cryptography.*

1. Introduction

The mobile electronic commerce is defined as any interaction with financial cost or value which is accomplished by communications network and mobile phone. (Mannan et al. 2007) In recent years, the mobile electronic commerce has been considered as a commercial opportunity and many organizations have considered it more than before. (Rajanish et al. 2011) Such mobile commerce is usually performed by mobile phones, because of their availability. However, in these systems, user accounts and their financial information should be protected against abusing. As a result, operators and companies have tried to increase the security of these systems. (Al-Dala'in 2008)

Many encryption algorithms are developed in recent years. However, they can't be used directly in mobile phones. There are three main reasons for this problem. First, most of mobile phones have not equipped with powerful CPU and have limited amount of internal memory. Therefore they have not enough capability for performing high level encryption. Meanwhile, most of mobile phones have not been equipped with special processors for performing special type of calculations which need more time to be processed. As the second reason, in comparison with wired networks, wireless networks have lower bandwidth and less reliability. Therefore, establishing security in wireless networks is more difficult than 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. (Raju et al. 2008)

In this paper a new security algorithm for mobile phones based on call back technique and one time password is developed. This algorithm provides the required security for mobile payment regarding above resource restrictions. As a result of this algorithm, there is no need to use heavy process on mobile phone for high level encryption. Meanwhile, it protects from interception and user identification is confirmed completely and integrity, authentication, and non – repudiation all are provided. This paper is organized as follows. In Section 2, the principle of cryptography is explained. In Section 3 the new algorithm is proposed. Discussion on the proposed method is the subject of Section 4. Finally in Section 5, conclusions and remarks are outlined.

2. Fundamental of Cryptography

Cryptography is the application and study of hiding information It prevents message from abusing by unauthorized persons.

It is used for protecting data in public networks. Usually advanced mathematical algorithms are used for encoding the messages. (Douligeris and Serpanos 2007) Data transmission on a network should pass the following specifications: (Salama *et al*. 2009)
Security: the sent data cannot read by unauthorized users.
Identity: the persons who take part must be one who pretends.
Integrity: received data and sent data must be equal.
Cryptographic algorithms usually implement the above specifications to prevent unauthorized users to access the imperative data. Cryptographic algorithms are divided in two main groups:

1. *Cryptography of general key (public key);* where source key is not equal the destination key. In this type of coding, two keys are used. One is public and the other is private. (Douligeris et al. 2007)
2. *Cryptography of private key*; where a single key is used both in source (for encoding) and destination (for decoding). We will explain them in two following subsections. (Douligeris et al. 2007)

2.1. Asymmetric key Cryptography

This cryptographic approach also called public key, involves the use of asymmetric key algorithms, that is, two different keys are used for cryptography; one public key is used for encryption and the other private key is used for decryption. Every user has one public and one private key. An unauthorized person can't decrypt data by using public key because encrypted data can only decrypted by private key. Figure 1 shows this method. The public key cryptography allows recipients and senders to use the secret key without previous agreement. (Douligeris et al. 2007) The key in this method composed of eight data fields. The two fields are used for encryption data (by using public key) and the other six fields are used for decryption data (by using the private key). Data encoding is performed by the following formula:

$$X = Y \wedge K \bmod R \qquad (1)$$

Where X is the encrypted data, Y is the main data, k is the private key and r is the product of multiplying two primitive numbers which have been selected carefully. These kinds of calculations are very slow on bit processors. Cryptography with this model is also 500 times slower than encryption of private key which is described in the next subsection. (Salama *et al*. 2009)

2.2. Symmetric-key Cryptography

Symmetric-key algorithms also called private keys, are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption This kind of cryptography which is also called symmetric is more common than public key. It uses one key for both encryption and decryption. All users who are the members of one group must have the same key. In this method, both the sender and the recipient know about the cryptography of data. The basic concept is the subscription of one code and the two groups of participations reach an agreement on a common key. Therefore, the possibility of encryption and decryption of messages is provided with regarding to this fact that they are aware about the secure key. (Douligeris et al. 2007) Figure 2 shows the basic of this method. The most common application of this type of cryptography is in the intelligent cards and data encryption algorithm which is applied on slow processors. However, exchanging the secure key on a public network needs a safe channel. As a result, using his method is more appropriate when the keys are stored using a safe method or when the key is exchanged between two systems, that their identities is specified before. Since the encrypted data can be intercepted and decrypted by a normal computer, this type of cryptography is not appropriate for sensitive data. (Salama *et al*. 2009) In this method, it is impossible to determine who has issued the encrypted message because the key has been shared between two users. With regard to this fact, transferring private key is performed faster than public key (Song 2007).

2.3. Mobile Phone Payment Cryptography

Cryptography is a proven solution, which can be used to secure mobile communications. The usage of public key cryptography can provide the confidentiality, authentication, integrity and non-repudiation security services needed to secure mobile communications. Due to the limitation of the mobile devices resources, implementing a cryptography solution to secure communication has become a challenge.(Al-Bakri *et al.* 2011) 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.(Toldinas *et al.* 2011) In a comparative study for this problem is printed out. 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. Despite of PCs and the systems which are connected to the wired networks, the mobile systems use batteries with limited energies.

2.4. Experiments

To realize the experiments we have developed the program that implements the algorithm in C# language for .the NET Compact Framework. The experiments were performed on the PDA of the model ASUS P750 (Pocket PC platform, Intel PXA270 520 MHz CPU, 256 MB RAM, Windows Mobile © 6 Professional CE OS 5.2). (Toldinas *et al.* 2011) We can note that for all optimal solutions the block size and the key size are equal. Based on these results, we can construct three security profiles for mobile device users as follows:

1) *Low energy / low security:* so far considered secure, but theoretically crackable.
2) *Medium energy / medium security:* suitable for top secret information; consumes ~ 10% more energy than low energy/security profile.
3) *High energy / high security:* suitable for top secret information; consumes ~ 8% more energy than medium energy/security profile (Toldinas *et al.* 2011).
These profiles are summarized in Figure 3.

These problems all direct us to develop a new security algorithm based on mobile phone resources.
In our proposed method, the call back technique is used. When user connects to a server and after confirming the username and password, 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 dial up users. Phone number of every user is registered in him/her specification. (Charlie et al. 2009) 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 which its number has been registered in the server. In 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, a password can only be used one time and it is impossible to use it again. (Charlie et al. 2009)

3. The Proposed Method

In this part our new proposed method for mobile phone payment is explained. In our proposed method, A SIM card (stands for Subscriber Identity Module, is a portable memory chip used in cellular telephones) number, phone serial number and 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, his/her SIM card number, phone serial number and the username account is checked by the payment server. Every generate 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. Figure 3 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. 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 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. The new password has been encrypted; it has been decrypted in server and will be compared with available passwords. When it becomes conformed, the new password will be removed from the passwords of server 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 the previous transaction password. If the server password is similar to the received password of mobile phone, these same passwords will be removed and transaction will be performed.

4. Discussion

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

1) *Username and Password:* These two elements are used for every transaction.
2) *Subscriber Identity Module (SIM) number:* The SIM card number is unique. Every user has his/her number
3) *The serial number of mobile phone (Device ID)*: Device ID is unique. It establishes more security together with the SIM card number.
4) *The one time passwords*: They are produced by the password generator program which is also is safe against interception.
5) *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 conformity. As a result of confirmation, the previous transaction password will be sent and the transaction will be completed. If unauthorized person 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 be also 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 password creator must be activated by username and password account. In the wireless communications, signals are distributed in the environment and the passwords can be intercepted by unauthorized persons. In the proposed method, the problem of people who can listen and intercept the information has also been removed; because one time password are used and these passwords cannot be used again. Other benefits of the proposed method are: Omitting the need of using complicated algorithms such as public key. There is no need to use phones with fast and powerful processors and high memory capacity because complicated cryptographic operations are not used on 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 produces one key, and then the cryptography is performed by using this key. The complexity of new 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. In almost all existed 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. 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. Table 1 shows a comparison between time consuming between our proposed method and other state-of-art algorithms.

5. Conclusion

Mobile phone payment is an alternative payment method that instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services. Recently, mobile payment using mobile phone, as a new subset of electronic payment in ICT world, is extensively considered by researchers. In this type of financial payment, security is an important problem. For establishing such security, many cryptographic algorithms are developed. Meanwhile, the symmetric and asymmetric algorithms as two common methods are very complicated and they need strong hardware sources for processing cryptographic algorithms. However, mobile phones usually have limited hardware resources. As a result most of the current cryptographic algorithms cannot be run on most of mobile phones. In this paper, a new cryptographic algorithm for mobile phone based on call back technique and one time password is developed. The proposed algorithms can be implemented on most of mobile phones even with limited hardware resources while providing enough security. In this algorithm, all data are protected against interception. As a result of applying the call back techniques and two passwords in every transaction, the integrity, authentication and authorization are provided.

6. References

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci., 10(15): 1656-1661.

Al-Bakri S H, Mat Kiah M L, Zaidan A A, Zaidan B B, Mahabubul Alam G (2011). Securing Peer-to-Peer Mobile Communications Using Public Key Cryptography: New security strategy. International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011. ISSN 1992 - 1950 ©2011 Academic Journals

Al-Dala T (2008). A Review Of Current Online Payment Systems Related To Security And Trust Solutions. Suhuai Luo, Peter Summons School of DCIT, Newcastle University Newcastle, Callaghan NSW 2308, Australia.

Barkan E, Biham E, Keller N (2008). Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. J. Cryptol., 21(3):392-429.

Challa N, Pradhan J (2007). Performance Analysis of Public key Cryptographic Systems RSA and NTRU. IJCSNS Int. J. Comput. Sci.Netw. Security, 7: 87-96.

Charlie R , Craig Z (2009) Microsoft widows server 2008

Douligeris C, Serpanos DN (2007). Network Security Current Status and Future Directions. Institute of Electrical and Electronics Engineers, Inc. Published by John Wiley and Sons, Inc., Published simultaneously in Canada.

Liang LR, Nambiar S, Lu C (2004). Analysis of Payment Transaction Security in Mobile Commerce. Department of Computer Science, University of the District of Columbia. Virginia Polytechnic Institute and State University Washington.

Mannan M, Van Oorschot PC (2007). Using a Personal Device to Password Authentication from An Untrusted Computer. School of Computer Science, Carleton university Ottawa, Canada.

Raju P, Gajwani A, Gonsalves TA, Srinivas ChR (2008). Analysis of Mobile Infrastructure for Secure Mobile Payments.

Rust C, Salsano S, Schnake L (2009). The SIM card as an Enabler for Security, Privacy, and Trust in Mobile Services.

Salama D, Minaam1 A, Abdual-Kader2 HM, Mohamed Hadhoud2 M (2009). Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types. Higher Technological Institute 10th of Ramadan City, Faculty of Computers and Information, Minu¯ya University2 Elbetrol st., Elsalam Area, Kafr Sakr, Sharkia, Egypt. International Journal of Network Security, Vol.11, No.2, PP.78{87, Sep. 2010

Rajanish D, Sujoy P (2011). Adoption of Mobile Financial Services among Rural Under-Banked, Indian Institute of Management Ahmedabad-380 015 -India

Song X (2007) Mobile Payment and Security. Helsinki University of Technology Telecommunications Software and Multimedia Laboratory.

Toldinas J, Stuikys V, Damasevicius R, Ziberkas G, Banionis M (2011). Energy Efficiency Comparison with Cipher Strength of AES and Rijndael Cryptographic Algorithms in Mobile Devices . Electronics and Electrical Engineering ISSN 1392 – 1215 2011. No. 2(108)

Toorani M, Shiras AAB (2008). SSMS - A Secure SMS Messaging Protocol for the M-Payment Systems.

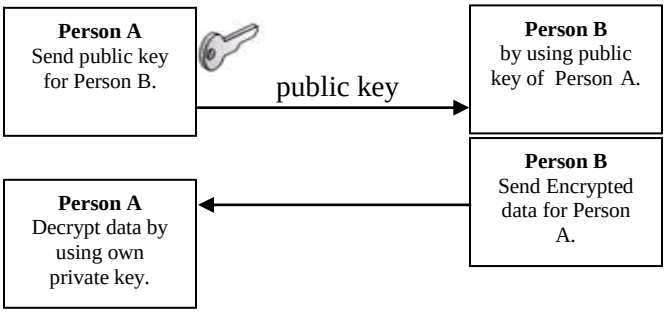

Figure 1. The cryptographic process according to the public key between two users.

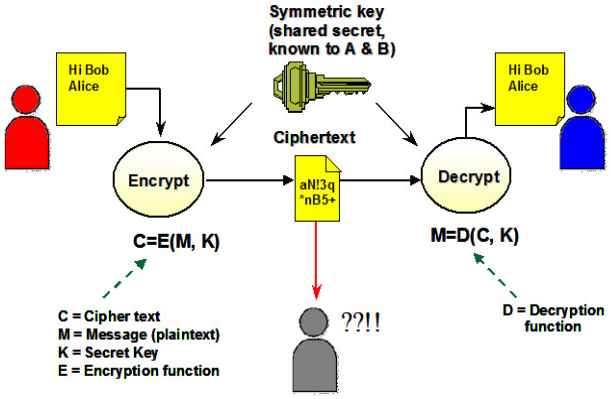

Figure 2. Cryptography based on private key.

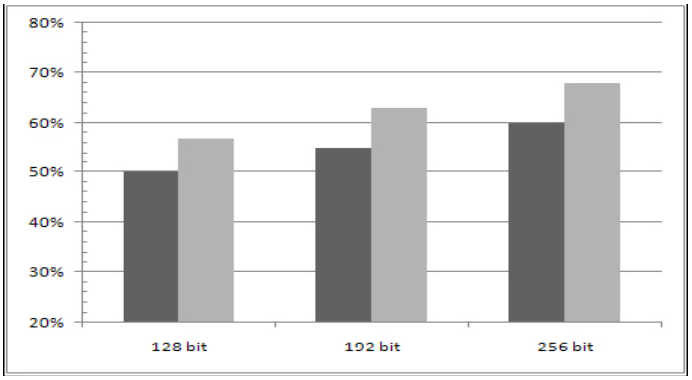

Figure 3. Comparison of security profiles for encryption (left) and decryption (right): energy consumption vs block/key size.

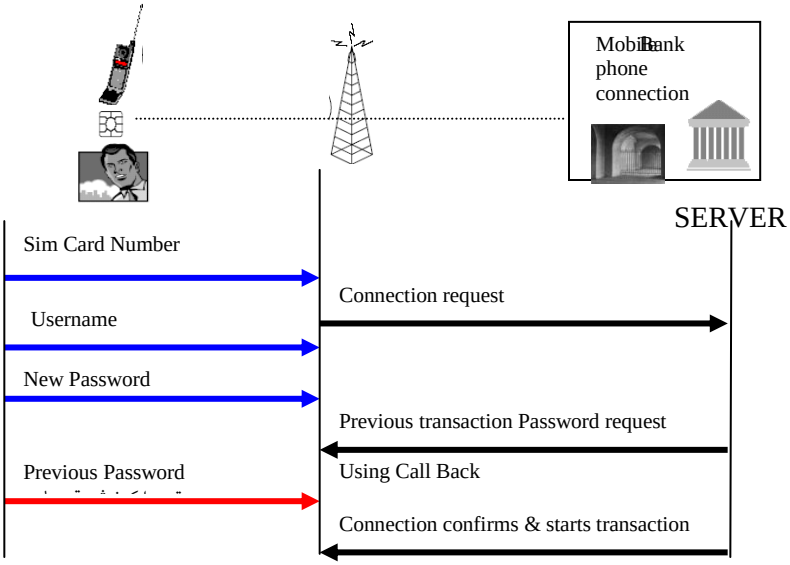

Figure 4. The security process of the proposed method

Table 1. A comparison between usual cryptographic keys and the proposed method

Key length	Time to key generation	Encryption	Decryption
64stib 128stib 192stib 256stib	1.8sm 2.1sm 2.6sm 2.9sm	2.2sm 3.2sm 3.6sm 5.4sm	2.8 sm 3.4 sm 4 sm 7 sm
32 bit password for our proposed algorithm	1sm	-	-