Account Based Mobile Payment by Diffie-Hellman Key Exchange Protocol

Kuen-Liang Sue, Wen-Jr Wu
Department of Information Management, National Central University
Jhongli City, Taoyuan County, Taiwan
Tel.+886-3-4267270
EMAIL:{klsue@mgt.ncu.edu.tw, 93423037@cc.ncu.edu.tw}

Abstract: With the development on techniques of mobile communication, the daily activities benefit from these techniques more than ever. In order to make living more convenient, the mobile payment has been brought up in recent years. The consideration for carrying out the mobile payment is very difference from that in the wired electronics payment scheme because of the characteristics of mobile device. In this article we develop a mobile payment scheme that is based on reducing the operation of the device, and furthermore achieves the demands of security. It can create the session key for each transaction by means of using the "Diffie-Hellman key exchange" protocol. The use of the Message Authentication Code (MAC) can achieve the integrity of electronic commerce. Both of them do not need a large number of operations and complex algorithm so it can achieve the purposes of this investigation: a secure, convenient and light-computation scheme for mobile payment.

Keywords: E-finance, Mobile payment, Authentication c ode, Key exchange

I. Introduction

Along with mature and widespread development of the internet technique, more and more people enjoy the convenience of the Internet. It also expands the consumer market rapidly expand, and many business services also have been brought on the Internet. These businesses activity working on the internet can be general named as E-Commerce.

Like many commercial services, the most important action is the payment after consuming on the internet. As a result, the electronic payment plays a very important role in the electronic commerce. Many electronic payment schemes have been implemented, and these electronic payments are not only adopted in the virtual store on the internet but also applied on the real store, such as CyberCash[1], Paybox[2], Mobipay[3], Sonera Shopper[4] and Paypal[5].

In the recent years, because of the rapid development of the mobile communication network, the mobile communication network is no longer limited by transmitting the traditional voice data, and the data transmission on the mobile communication network also has been carried out. In the technique aspect, the data transmission rate on the mobile communication networks also increases continuously. Nowadays the data transmission rate in the 3G system also comes to 144 kps. Those techniques development make business activities execute on the mobile communication network. The business activities on the mobile comm-unication network can be named for mobile commerce. People will be able to use the mobile device to purchase the product or service. However, in a business activity, payment is an essential process. It is no doubt that payment is also an essential process in the mobile commerce.

However, unlike wired environment, there are many restrictions in the wireless environment. First, in wireless environment, the bandwidth is lower than wired environment, and the transmission error rate is higher. It also makes long latency. Secondly, the power of mobile device is limited. The memory and operation abilities are much weaker than the desktop computer. If we transplant current e-payment scheme which has implemented on the wired environment directly to the wireless environment, undoubtedly there will be many problems.

In this paper, we propose an account-based mobile payment scheme applied in wireless environment. The purpose of this scheme depends on reducing the computing quantity of mobile device. Thus, it can match the characteristics of the mobile device which are addressed on the above section. In the security of transmission, we don't use the SET[6] or iKP[7] because of reducing the computation load and the communication overhead. Another reason is to overcome the restrictions of mobile device and reduce the influence of the high transmission error in the wireless network.

The organization of this paper is introduced as following. In section 2, we introduce the related technique using in our proposed scheme. In section 3, we will introduce proposing mobile payment scheme. In section 4 we will discuss and evaluate the security of our scheme from different points of view. In section 5 we gives conclusions.

II. Background

II. 1 Public key and secret key cryptography

The cryptography in the communication can be classified into two categories. One is public key cryptography; another is secret key cryptography. The next sections will describe the features of them respectively.

The public key cryptography is also known as asymmetric cryptography. It uses difference keys to encrypt and decrypt the communication data. The private key is only known by the sender, and he uses this key to encrypt the data

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 625 - 630.

which he wants to send. The receiver uses the public key which was published from the sender for everyone to decrypt the date encrypted by sender. Each user in the network needs to have two keys: a public key which is available for anyone; a private key which the sender will keep by her/himself. It also needs a trusted third party to manage the key and verify whether the key is valid or not. The drawbacks of this cryptography are time-consuming, and the computational overhead of device is heavy. There are many known public key cryptography, such as RSA[12], DSA[14] and ECC[13].

The secret key cryptography has also been known as symmetric cryptography. It uses the same key to encrypt and decrypt the communication data. All participants joining this system have to trust completely and each participant preserves a key copy of other participants. Sender and receiver have to share the same key before communication. In the process of generating the secret key, the relevant information of generating keys has to guarantee against eavesdropping. It can achieve through assigning the secure gateway. Once the secret key is obtained by the third party, the data of communication does not be protected and becomes very dangerous. The advantages of secret key encryption are that the encryption time of symmetric cryptography is shorter than public key cryptography and this cryptography suits for encrypting a large amount of data. There are many known secret key cryptography, such as DES[15], AES[16] and RC5[17].

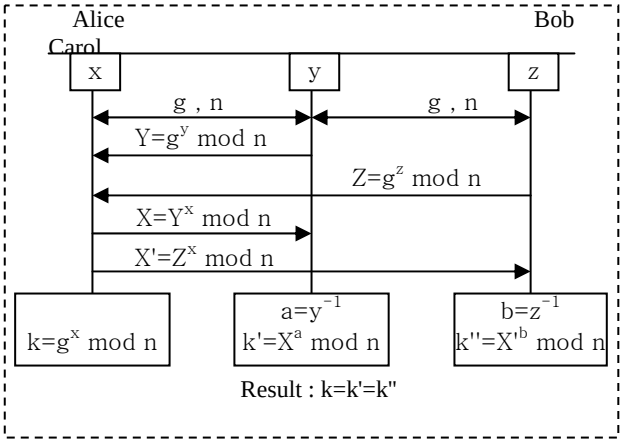

FIGURE 1. Process of three way exchange key

II. 2 Diffie-Hellman key change scheme

"*The Diffie-Hellman key exchange scheme*" is the first and well-known key distribution system invented in 1976, in which a common key could be established between two parties.[8] By using this key exchange scheme, communication parties can generate session key that needs to be used in the communication session. Generating a session key is very easy through this key exchange scheme, and can be completed without using complex algorithm. So it is suitable for using this algorithm in the small equipment which only has low computation capability, like mobile device.

II. 3 Extension of Diffie-Hellman key exchange scheme

Based on *Diffie-Hellman key exchange* scheme ,we can extent the two parties exchange key to three parties [9]. The Figure 1 shows the process of exchange key among three parties. The detail is described below.

First of all, Alice, Bob and Carol generate a number by themselves respectively.

Secondly, all of them coordinate two values, g and n.

Thirdly, Bob sends Y to Alice. The Y is counted by g, y and n. The equation is shown in (1).

$$Y=g^y \bmod n \quad (1)$$

In this function, if the attacker eavesdropped the Y, g and n in the second step, he/she still can not compute the y.

The next three steps like third step. In step 4), Carol sends Z to Alice. The equation Z is shown in Figure 1. In step 5), Alice sends X to Bob. In step 6), Alice sends X' to Carol.

Finally, Alice calculates the value k. Bob calculates the value k'. Carol calculates the value k''. The equation of k, k' and k'' shown in Figure 1. The result of this mechanism is that all of the values k, k', k'' are identical. Therefore, Alice, Bob and Carol share the same session key.

II. 4 Message Authentication Code (*MAC*)

Documents which transmit in the public communication and computing environments are very dangerous, especially in the wireless environment. Documents may be hacked easily by anyone. It is very important to check the consistency of the document when a receiver receives this document. The Message Authentication Code is a scheme that can verify the consistency of document. [11] The process of *MAC* is as follows:

Step 1) Initial: Sender and receiver have the same authentication key

Step 2) Sender: s*MAC* = *MAC* (original document, authentication Key)

Step 3) Sender → receiver: s*MAC* + document copy

Step 4) Receiver: r*MAC* = *MAC* (document copy, authentication key)

If s*MAC* = r*MAC* then

Document is correct

Else

Document may be modify and isn't valid document.

End if

In Step 1), both of parties need to obtain and know the same authentication key before communicating with each other.

In step 2), a sender uses an *MAC* algorithm which takes the original document and the authentication key into count to generate a message digest. The *MAC* algorithm often uses a hash algorithm to accomplish.

In step 3), the sender transfers the document copy and the message digest to the receiver.

In step 4), a receiver generates a message digest which is created by *MAC* algorithm by using the received document and his authentication key. Then receiver compares message digest received from sender with the one generated by receiver. If both of then are equal, the document is correct. Otherwise, the document may be modified by hacker. By using *MAC*, we can verify whether document is consistent or not.

III. Proposed Scheme

III. 1 Abbreviation

The abbreviations of the relevant data used in following description are shown in Table 1.

TABLE 1. Abbreviations of the data used in the proposed mobile payment scheme

Abbreviation	Description
PG	Payment Gateway – a trusted third part. It is responsible for verifying the accuracy of transaction and transferring accounts
TID	Transaction Identification number
M	Merchant
Ma	Merchant account in the payment gateway
C	Customer
Ca	Customer account in the payment gateway
OI	Order Information
P	Total price of orders
eKi{message}	Encrypt the message via the key Ki
dKi{message}	Decrypt the message via the key Ki
MAC{message, Ki}	Run the *MAC* algorithm. The inputs are message and authentication key Ki
Kcp	Session Key between customer and payment gateway
Kmp	Session Key between merchant and payment gateway
Kcmp	Session Key among customer merchant and payment gateway
PIN	Personal Identification Number

III. 2 Basic assumption

- The customer's device can access the Internet, e.g. GPRS.
- Customers and merchants have an account at least in the payment gateway. And payment gateway maintains the accounts.
- The transmission is reliable in wireless environment. It means that it will retransmit data if errors occur.
- All of the keys – *Kcp*, *Kmp* and *Kcmp* – are generated by the use of *Diffie-Hellman key exchange* scheme.
- Payment gateway is a public's trusted third party.
- When customers and merchants login the payment gateway, both of them need to input account and password to authenticate.

III. 3 Payment process

Our payment scheme idea is that customer and merchant send transaction information separately to the payment gateway. Both of customer and merchant can not get another part's information, because the information is hidden by the use of *MAC* which is a one-way hash function. When the payment gateway successful receives the transaction information from both customer and merchant, it will compare the information whether they are equal or not. If both of them is equivalent, we can say that the data is correct. Then the payment gateway will transfer an account. After accomplishing transfer, the payment gateway will send receipt to them. The process is shown in Figure 2 and the detail is described below:

Step 1) $M \rightarrow C$: *TID* , *OI* , *P*
Step 2) *C* : confirm the orders
Step 3) *C* : input *PIN* number on the mobile device
$M \leftrightarrow PG$:
generate *Kmp* (must login payment gateway)
$C \leftrightarrow PG$:
generate *Kcp* (must login payment gateway)
$C \leftrightarrow M \leftrightarrow PG$: generate *Kcmp*
Step 4) $M \rightarrow C$: *eKcmp*{*MAC*(*Ma, Kmp*)}
Step 5) $M \rightarrow PG$:
eKcmp{*eKmp*{*Ma*},*TID*,*OI*,*P*,*MAC*(*Ma*,*Kmp*)}
Step 6) *C* : *uMAC* =
MAC((*TID*||*OI*||*P*||*Ua*||*MAC*(*Ma*,*Kmp*)),*Kcp*)
$C \rightarrow PG$: *eKcmp*{*eKcp*{*Ua*},*uMAC*}
Step 7) *PG* : *rMAC* =
MAC((*TID*||*OI*||*P*||*Ua*||*MAC*(*Ma*,*Kmp*)),*Kcp*)
Compare if *rMAC* = *uMAC*

In step 1), after a customer shops at a real store or a web store, the merchant will transmit *TID*,*OI*,*P* to customer's mobile device. In a real store, it can be accomplished by point-of-sale system. In a web store, it can be done through wireless communication system as *GPRS*.

In step 2), the customer checks the *OI* and *P* shown on the mobile device's screen. If the information is correct, he/she starts payment process and goes to step 3). If not, he/she can cancel the transaction and restart again.

In step 3), the customer inputs a *PIN* number for first authentication. If the *PIN* number is correct, customer, merchant and payment gateway generate the keys – *Kcp*, *Kmp* and *Kcmp* – which are necessary in the payment process. Those keys are generated by the method of the extension of *Diffie-Hellman key exchange* scheme which is discussed in the sections 2.2 and 2.3.

In step 4), the merchant uses the *Kcmp* to encrypt

MAC(*Ma*, *Kmp*) and transfers it to the customer. Only merchant, customer and payment gateway know the key, *Kcmp*, and all communication data among merchants, customers and the payment gateway will be encrypted by *Kcmp*. Consequently, the data are protected and under security.

In step 5), the merchant transmits order information, the merchant account which is encrypted by *Kmp* and *MAC*(*Ma*, *Kmp*) to the payment gateway. The reason to send *eKmp*{*Ma*} and *MAC*(*Ma*, *Kmp*) is that the payment gateway can verify whether the merchant account is correct or not. Of course, the communications between them are encrypted by the key, *Kcmp*.

In step 6), when the customer receives the data transmitted from the merchant, it generates *uMAC*. The equation of *uMAC* is shown in (2).

$$uMAC = MAC((TID||OI||P||Ua||MAC(Ma,Kmp)),Kcp) \quad (2)$$

Because of using *MAC*, the size of the information will shorter than the one without using *MAC*. For this reason, it suits to transmit it in the wireless environment. Then the customer transmits *uMAC* and *Ua* which is encrypted by *Kcp* to the payment gateway.

In step 7), when the payment gateway receives all information from the customer and the merchant, it first computes the *rMAC*. The equation of *rMAC* is shown in (3).

$$rMAC = MAC((TID||OI||P||Ua||MAC(Ma,Kmp)), Kcp) \quad (3)$$

After the payment gateway calculates the *rMAC*, it compares with *uMAC* which receives from customer before. If *rMAC* is equal to *uMAC*, the payment gateway starts transferring an account.

IV. Analysis of Security

IV. 1. Evaluation from the aspect of security criteria

When we talk about the security of e-commerce, we usually have to achieve the following security criteria of authentication, non-repudiation, integrity, and confidentiality. Because m-commerce is some kind of e-commerce, m-commerce has to achieve these four security elements to evaluate the system.

IV. 1. 1 Authentication

Customers need to key in *PIN* number on the cell phone, before using the cell phone to pay. Hence it can procure the authentication. In case the cell phone is stolen, it can not work without *PIN* code. In the payment gateway, customers and merchants have to login the system when they want to conduct a transaction. It needs account information and password when they login the payment gateway. Therefore, there are also ID identify in the payment gateway to ensure the security for the system.

IV. 1. 2 Confidentiality

In the proposed scheme, merchants transfer *TID*, *OI*, and other related information to customers without encrypting in the first step. While in other transferring steps, all participators use *Kcmp* to perform symmetric cryptography. Because there is no account information in the message of the first step, if some information is changed by illegal ways, customers can make sure whether the information is right or not and refuse the requirement. So there is not any influence in the confidentiality of the scheme.

IV. 1. 3 Integrity

When transferring information in the system, all information use *MAC* to ensure the integrity except for the first step. In first step, the customers check the transaction data shown on the screen of mobile device manually. In others steps, the computer will use *MAC* to check the integrity automatically. It is easy to use *MAC* to achieve the integrity. The output of *MAC* will be different if the input is different. In our scheme, the input data are composed of *TID*, *OI* and other related information. Most of them are difference in each transaction. It is hard to find that all input data is equal to old one. Therefore, we can ensure that the *MAC* can achieve the integrity in the proposed scheme.

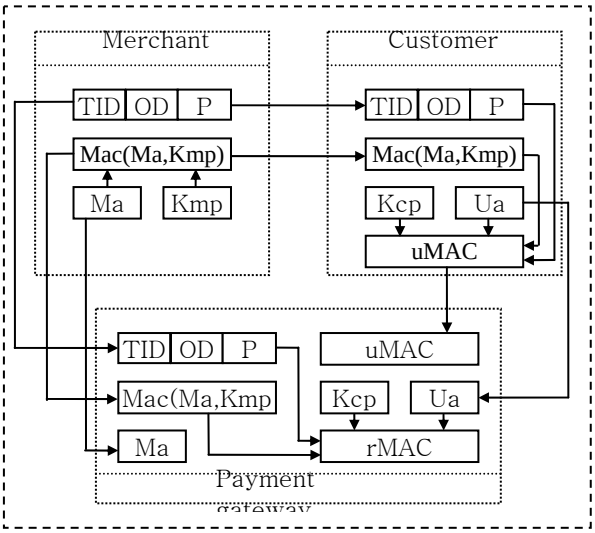

FIGURE 3. Data flow in our payment scheme

IV. 1. 4 Non-repudiation

Before dealing, customers and merchants have to login the payment gateway first and then they can proceed to go through the payment process. Customers and merchants use the Diffie-Hellman key exchange protocol to obtain keys, so that an account has a session key. The payment gateway will record the relationship between accounts and session keys. The system uses the method to achieve non-repudiation.

When customers and merchants transfer their account, all of them use their individual session key to encrypt. Before producing the session key, customers and merchants have to login the payment gateway, and payment gateway is a public reliable third party. So based on the reason, the system can reach non-repudiation.

IV. 2 Evaluation from the aspect of attacker's role

In our proposed scheme, we do not evaluate malicious payment gateway, because it is a public trusted third party. In this section, we only evaluate the aspects of malicious merchant, customer and other attackers.

1) Malicious merchant

First, a malicious merchant may fabricate a transaction. This action will make customer lost his money unknowingly. In our scheme, merchant needs customer's account to conduct a transaction. In Figure 3, when conducting a transaction, customer's account information is never transmitted to the merchant. When transmitting the *Ua*, it is also encrypted by session key "*Kcp*" and "*Kcmp*". For this reason, it has a very low probability to happen that the *Ua* is obtained by other one.

Secondly, the merchant will modify the price higher than original one when it transfers price to payment gateway. But the *rMAC* will not be equal to the *sMAC* which both of them need price information to generate.

Thirdly, malicious merchant may deny the transaction. In our scheme, transaction records will be recorded by payment gateway when conducting a transaction. As merchant logins the payment gateway, he needs *Ma* and password. But both of them are not easy to obtain. All transmissions of the *Ma* are encrypted by session key "*Kmp*" and "*Kcmp*". It is very difficult to steal the *Ma*'s information.

2) Malicious consumer

In the first place, malicious consumer may modify the price lower than original one when it transfers price to payment gateway. Like above section, the *rMAC* will not be equal to the *sMAC* when payment gateway compares *rMAC* with *sMAC*. Then the transaction will be canceled.

In the next place, malicious consumers may deny the transaction. In our scheme, customer will input *PIN* code in the mobile device first when performing the mobile payment. Transaction records also will be recorded by payment gateway. The information of *U*a is encrypted by session key "*Kcp*" and "*Kcmp*". So it is very difficult to eavesdrop the *Ua*'s information.

3) Other attacker

All of transmission in our proposed scheme use *Kcmp* to encrypt data. Because we use symmetric cryptography, the time of encryption is short. And each session key only uses one time. If anyone wants to modify transaction data, he must compute the *Kcmp*. But computing the *Kcmp* is not easy. Even though he computes the *Kcmp*, the transaction has already been completed early.

V. Conclusions

With the development of communication network, there are more and more people enjoy the convenience of using mobile device. It does not like the traditional wired environment which is limited to a fixed place. It can be worked at any time and any where. With smaller size and lighter weight, mobile devices can be a basic platform for many business activities in the future. But mobile device's electricity, memory and computation ability are not as strong as traditional PC, so these factors need to be considered in developing service in mobile devices.

When using asymmetric cryptography, it will consume much time and electricity of the device. In our proposed scheme, we use symmetric cryptography to save electricity and decrease computing time. In the way, we can extend the lift time of the device and decrease the waiting time when customers perform the payment process.

In the cryptography, the most importance thing is how to obtain the encryption key. In our payment scheme, we use Diffie-Hellman key exchange scheme to generate all the session keys we need. The process of key generation is simple and does not need complex operation. Hence, the method is appropriate to mobile devices which usually have low computing ability.

In the respect of security, the keys of conduct a transaction are different in each transaction. Therefore, there is useless to steal the keys, because all session keys only use one time. Another reason is that the transaction is accomplished when attackers obtain all session keys, because the time of conduct a transaction is short. If the keys is not easy to obtain, and most of the communication in our scheme is encryption, our scheme is secure.

In the respect of key management, we do not use public key infrastructure (*PKI*). In our scheme, we use "*Diffie-Hellman key exchange*" to generate session keys. The key management is done by payment gateway. Because there is no usage of *PKI* , the communication times will reduced. The less the communication times is, the more security the payment scheme is.

As above mention, our payment system offers a secure payment system and fits the characteristics of mobile device.

References

[1] CyberCash : http://www.cybercash.com/
[2] Paybox : http://www.paybox.com/
[3] mobipay : http://www.mobipay.com/
[4] Sonera Mobile Operations, Paivi Helanto, Sonera Corporation, March 2002.
[5] "The PayPal Phenomenon", EC research report, CommerceNet Taiwan, Jan 2002.
[6] Mastercard and Visa, SET Protocol Specifications, 1997. http://www.setco.org/set_specifications.html
[7] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H.Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, & M. Waidner, "Design, Implementation, and Deployment of the iKP Secure Electronic Payment System", IEEE Journal of Selected Areas in Communications, 2000.
[8] Diffie, W. & Hellman, M, "New Directions in Cryptography," IEEE Transactions on Information Theory, 1976, 22(6), 644-654.
[9] [9] B. Schneier, "Applied Cryptography Second Edition", John Wiley & Sons, Inc. New York, U.S.A, 1996, 514.
[10] N.Sadeh, "M-commerce: technologies, services and business modes", Wiley computer publish,Boston, U.S.A., 2002, 134-140.
[11] John R. Black, Jr, "Message Authentication Codes", Computer Science, 2000.

[12] R.L. Rivest, A. Shamir, and L.M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, 1978, 21(2), 120-126.
[13] Masaaki Shirase and Yasushi Hibino, “An architecture for elliptic curve cryptograph computation”, ACM SIGARCH Computer Architecture News, 2005, 33(1), 124-133.
[14] CORPORATE NIST, “The digital signature standard”, Communications of the ACM**,** 1992, 35(7), 36-40.
[15] “Data encryption standard (DES),” National Bureau of Standards(U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield,VA, 1977.
[16] J. Daemon and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.
[17] R.L. Rivest. “The RC5 encryption algorithm.” In Proceedings of the 2nd Workshop on Fast Software Encryption, 1995, 86-96.