

## Mobile Payment System Using Dynamic Transaction Numbers

Kuen-Liang Sue and Chung-Hsien Tsai

*Department of Information Management, National Central University*

*Jhongli City, Taoyuan County, Taiwan*

*{klsue@mgt.ncu.edu.tw, 93423002@cc.ncu.edu.tw}*

**Abstract**-With the developing of information technology, people nowadays can buy everything through the Internet conveniently. Also, handset devices are becoming more and more popular which makes it possible to purchase goods and services in the Internet anywhere and anytime. However, traditional payment schemes do not suffice for our needs as more novel commercial services were provided. Therefore, it's urgent to construct a safer and more convenient payment scheme.

This paper designs a mobile payment system in which the consumers purchase goods in the store or in the Internet by using cell phones and dynamic transaction numbers. Besides explaining our payment architecture and processes in detail, we evaluate the security of our scheme from aspects of users and attackers. As a result, our mobile payment system can not only satisfy security criteria of confidence, integrity, authentication, and non-repudiation but also provide full transaction privacy to consumers.

**Keywords:** mobile payment, payment system.

### 1. Introduction

Recently, Internet plays an important role in our daily life. In many occasions, such as business communication, shopping, and entertainment, Internet makes getting information easier. As for shopping, people can buy anything through Internet without going out to real stores. Also, the emergence of e-commerce changes the way of purchasing- from buying thing in real stores to shopping in the web store. What we need to do is sitting in front of the computer and connecting to the Internet, and we start enjoying the fun and conveniences of purchasing on the web.

With the developing of handset devices and telecommunication technologies, cell phones become more and more popular. Everyone in Taiwan has at least one mobile phone [1]. Besides, the formulation of such protocols as Wireless Application Protocol (WAP) and Wireless Markup Language (WML) makes the dream of surfing the internet through cell phone come true [2,3]. To catch this new trend, many commercial applications are developed and integrated into cell phones. Consumers are greatly attracted by these advantages: the convenience that

cell phone brings makes it possible to transact without any restriction of time and place, which explores the door of mobile commerce.

In addition to the changes of traditional commerce, people are aware that the use of conventional currencies is insufficient. The demand on a more convenient and secure currencies is increasing. While the new plastic and electronic currencies, such as credit card, smart card, and e-cash, were designed to fulfill those demands, there are still critical barriers that we have to overcome. Hackers or attackers can easily pretend to be the legal users and consume at will if they get the credit card numbers and the expiration date. That will not only cause great losses to both merchants and consumers, but also restrain the development of novel payment tools and e-commerce.

In order to promote the m-commerce and improve existing payment schemes, the securer and more convenient payment architecture is needed urgently. We attempt to construct a payment model which provides consumers security and convenience. Under the condition of high popularization of cell phones and the highly developed telecommunication technology [4], we propose a new idea – using cell phone as a payment tool.

In this paper, we propose a mobile payment model which uses cell phone as the main payment media when consumers make transactions. To reduce the risk of security and provide the user with higher privacy, we will introduce the idea of “dynamic transaction number” at first. The second part of this paper summarizes the existing mobile payment mechanisms. The third part will go into detail about our payment mechanism and architecture. The fourth part will discuss and evaluate the security of our model from both the attacker and the defender's points of view. The final part gives conclusions and possible future research.

### 2. Related Works

Before introducing our model, we first review some existing mobile payment mechanisms and discuss their advantages and disadvantages.

Because of the considerations of the transaction cost and the convenience, some mobile payment mechanisms using credit card numbers were proposed.

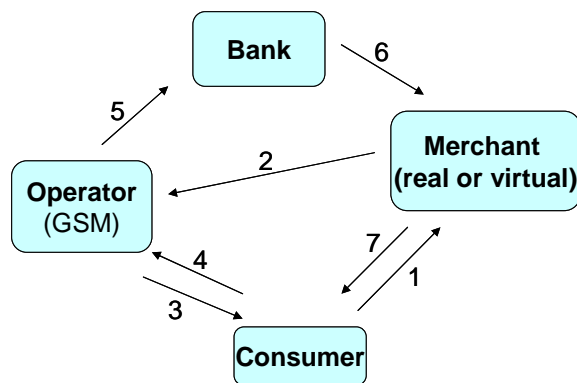


Figure 1. Process of mobile credit payment

In [5], Li used consumer's personal cell phone number as the transaction code instead of credit card number. The author claimed that cell phones should take the place of credit cards when making transaction because of the properties of convenience and security that the cell phone own.

His payment process can be depicted as Figure1, and the process is illustrated as follows:

**Step1:** The consumer can buy products in the real store or the web store, and give the seller his cell phone number.

**Step2:** The merchant summarizes the transaction-related information, such as the product's ID, the transaction date and the customer's cell phone number. Then, through wired Internet, he submits these data to the USSD (Unstructured Supplementary Service Data) sever of telecommunication service provider.

**Step3:** The operator then makes an USSD connection with the consumer through the phone number, and confirms the transaction information with the consumer.

**Step4:** After the consumer confirms the transaction information, he will use his personal private key which is stored in the SIM card of the mobile phone to sign the transaction data, and transfer the data back to the operator.

**Step5:** The operator delivers the signed transaction data to the cooperative bank.

**Step6:** The bank uses the consumer's public key to verify the consumer's identity and then checks his credit line. The bank also verifies the certificate of the merchant at the same time. After the verification, the bank deals with the transaction and transfers the receipt to merchant.

**Step7:** The consumers get the result of the transaction from the merchant.

The advantage of the payment mechanism mentioned above is that we can reduce the consumers' risk even if the phone number is eavesdropped. Usually, it is very risky that consumers provide the credit card number and due date when paying with credit card. Besides, the usage of the digital signature in the SIM card can prevent the consumer identity from being forged.

Nowadays, transaction privacy that consumer desired is more and more emphasized. We cannot guarantee the privacy when making transactions by a consumer's phone number. Merchants may gather the consumer's consuming habits or promote their new products by sending messages if they know the phone numbers of the customers. This will bother the consumers to certain extent. Hence, how the payment mechanism provides the transaction privacy cannot be ignored.

Su designed and implemented a mobile payment system with high flexibility [6]. His proposal for mobile payment is similar to the mechanism mentioned before. When the customer transacts, he transferred a fixed "User Identification" to merchant instead of phone number. The merchant summarizes the transaction data and submits it to the operator. Then the operator confirms the transaction to the consumer through the phone number of the corresponding user identification.

Although consumers own their purchasing privacy to some degree by using the "User Identification", the operator still control the private transaction information. Moreover, because the "User Identification" is fixed, the merchants still can collect the consuming habits of certain customer. Therefore, we propose a mobile payment mechanism which not only satisfies the conditions of security, such as confidence, integrity, and non-repudiation, but also provide full transaction privacy by making use of dynamic transaction number. Rubin and Wright proposed a scheme in which a dynamic and limited-lifetime credit card number through symmetric encryption is used [7]. Since the credit card number can just be used a few times, it reduces the security risk. Considering the characteristics of our payment scenario, we adopt the asymmetric encryption protocol to produce a dynamic transaction number, and we believe that it can provide the consumer with the complete privacy during the whole transaction process.

### 3. Our Payment Mechanism

The mobile payment mechanism we proposed uses the "dynamic transaction number" to ensure the confidence and privacy. The participators in the transaction process include the merchants, operators, and banks. They will not disclosure the identity of consumer and the contents of sensitive transaction information simultaneously. In the following, we will illustrate the payment mechanism in detail: the architecture of the payment system is described in section one; the details of the transaction process are illustrated with Figure 2 in section two.

#### 3.1 The architecture of payment mechanism

The participators in our payment system include: consumers, merchants, operator, and banks.

**Table 1. Symbols of the payment procedure**

Symbol	Description
<i>PhoneNo</i>	The consumer's phone number
<i>UserK<sub>private</sub></i>	The consumer's private key
<i>UserK<sub>public</sub></i>	The consumer's public key
<i>OpK<sub>private</sub></i>	The operator's private key
<i>OpK<sub>public</sub></i>	The operator's public key
<i>Password<sub>T</sub></i>	The transaction password which is only known by the consumer and the operator.
<i>RandomNO</i>	A random number.
<i>TransNo</i>	The transaction number.
<i>ID<sub>Merchant</sub></i>	The identity of the merchant.
<i>Certificate<sub>M</sub></i>	The certificate of the merchant.
<i>Amount</i>	The total price of the goods.
<i>SerialNo<sub>T</sub></i>	A serial number.
<i>Date-Time</i>	The date and time of the transaction.
<i>TransData</i>	The transaction data.
<i>TransRe</i>	The transaction receipt.
<i>OperatorID</i>	The identity of the operator.
<i>PIN</i>	Personal identification number.
<i>PaymentRe</i>	The payment receipt.

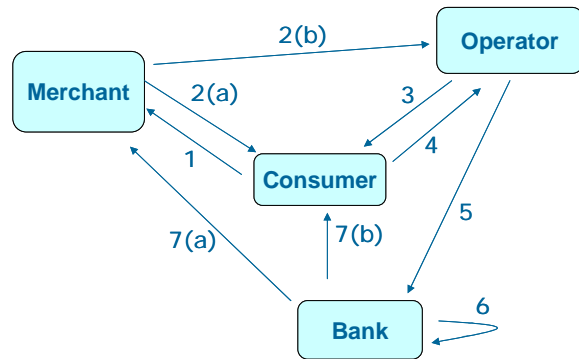
- **Consumer:** The consumers can purchase the merchandise with cell phone at a store or website. The operator's public key and the consumer's private key are stored in the SIM card and are used to verify the consumer's identity and to encrypt the transaction data.
- **Merchant:** The merchants provide service or goods to consumers. They might be real store or the web store. In the process of transaction, the merchants are responsible for summarizing and transferring the transaction data to the operator.
- **Operator:** The telecommunication operator plays an important role in the payment system. After receiving the transaction data from the merchants, the operator has to confirm this transaction with the consumer using USSD messages. The operator also has an asymmetric key for data encryption.
- **Bank:** The bank is responsible for settlement of accounts and the verification of consumers and merchants. After the settlement, the bank will transfer the receipts to consumer and merchant.

After the introduction of the participants, we now describe the process of the payment mechanism in brief: When the consumer goes shopping at a real store or a web store, he has to transfer the "transaction number" to the merchant at first. Then, the merchant summarizes the transaction data and transfers the data along with the transaction number to the operator through the fixed network. Meanwhile, the merchant prints the transaction receipt to the consumer. The operator then confirms the transaction with the consumer through USSD messages after receiving the transaction data. If the transaction is confirmed, the transaction data will be signed by

consumer's private key and submitted to the bank. The bank verifies the consumer's signature and the certificate of merchant, and then settles account and submits the payment receipts to both merchant and consumer.

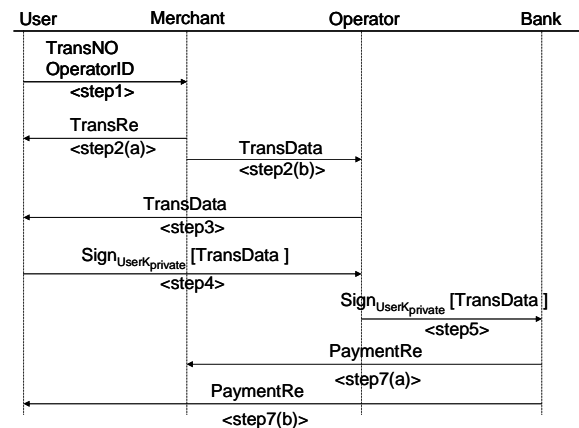
### 3.2 The procedure of mobile payment

After introducing the architecture of our payment scheme, we illustrate the procedure step by step. At the beginning, we define the related symbols used in the procedure in Table 1.



**Figure 2. The procedure of payment mechanism**

The transaction procedure of payment mechanism is shown in Figure 2. And we illustrate the processing of the transaction data and the direction of data flow.



**Figure 3. Data flow of transaction procedure**

**Table 2. Symbols of the cryptography**

$E_K[X]$	encryption of X using key K
$D_K[Y]$	decryption of Y using key K
$  $	concatenation
$Verify_{(K)}[Z]$	verification of Z using key K(if it is necessary)
$Sign_K[Z]$	signature of Z using key K
$\rightarrow$	the direction of data transferred

The information transferred between participants is shown in Figure 3, and the symbols of cryptography are summarized in Table 2. The

payment procedure can be presented more clearly by reading Figure 2 and Figure 3 simultaneously. In the following, we will illustrate the content of every step in words and symbols.

**Step1:**

(a) The consumer goes shopping at real store or website and chose to pay with his or her mobile phone. He generates a transaction number (*TransNo*) by using his personal private key to encrypt the following data: his phone number (*PhoneNo*), his transaction password (*Password<sub>T</sub>*), and a random number (*RandomNO*).

$$TransNo = E_{OpKpublic} [ PhoneNo // Password_T // RandomNO ]$$

(b) After the generation of transaction number, the consumer transfers it to the merchant through wireless transmission or just tells the number to merchant orally. While shopping in the website, the consumer has to enter the transaction number into the accurate field of the web page. In addition to the transaction number, the consumer also transfers the identity of the operator to the merchant because the merchant needs to know what telecommunication operator the consumer belongs to.

$$User \rightarrow Merchant : TransNo // OperatorID$$

**Step2:**

(a) The merchant summarizes the transaction data (*TransData*) which include the transaction number, the identity of merchant, the certificate of merchant, the price, the serial number of transaction, and the transaction time. Then the merchant transfers the transaction data with its signature to the operator through fixed network.

$$TransData = TransNo // ID_{Merchant} // Certificate_M // Amount // SerialNo // Date-Time$$

$$Merchant \rightarrow Operator : TransData$$

(b) At the same time, the merchant prints out the receipt of transaction (*TransRe*) to consumer (consumer has to print out the receipt by himself when shopping in the web store). The receipt not only includes all contents of transaction data but also the name and price of the good he had purchased.

$$Merchant \rightarrow User : TransRe$$

**Step3:**

(a) After receiving the transaction data, the operator decrypts the transaction number (*TransNo*) immediately, and then verifies the transaction password of the consumer in case that the transaction number is forged by someone else.

$$D_{OpKprivate} [ TransNo ] = PhoneNo // Password_T // RandomNO$$

$$Operator : Verify [ Password_T ]$$

(b) The transaction number would be invalid if the transaction password wasn't correct. In such situation the operator will reply the result to consumer through short message. Otherwise, the operator transfers the transaction data to the consumer through USSD messages, and waits for consumer's response.

$$Operator \rightarrow User : TransData$$

**Step4:**

The consumer confirms the transaction data from the operator. If the transaction data is correct, the cell phone verifies the consumer with the personal identification number (*PIN*). After the input of correct PIN, the cell phone signs the transaction data by using the private key of the consumer and transfers the signed transaction data back to the operator.

$$User \rightarrow Operator : Sign_{UserKprivate} [ TransData ]$$

**Step5:**

The operator transfers the transaction data which is signed by the consumer to the cooperative bank through internet.

$$Operator \rightarrow Bank : Sign_{UserKprivate} [ TransData ]$$

**Step6:**

The bank verifies the signature of the consumer by using the public key of consumer, and verifies the certificate of merchant. The bank checks the consumer's credit line after all the verification is passed, and then settles account.

$$Bank : Verify_{UserKpublic} [ Sign_{UserKprivate} [ TransData ] ]$$

$$Verify [ Certificate_M ]$$

**Step7:**

Finally, the bank transfers the transaction payment receipt (*PaymentRe*) to both merchant and consumer. The merchant shows the results of the transaction and delivers the merchandise or service to the consumer.

$$Bank \rightarrow User : Merchant : PaymentRe$$

Above, the procedure of payment mechanism has been demonstrated in detail. According to the security criteria, we evaluate our payment mechanism from different points of view in section four.

## 4. Analysis of Security and Discussion

When we talk about security and related subject, some security requirements should be achieved, as mentioned in [8]. In this section, we evaluate our payment mechanism from two angles: the angle that stands on the defense side and the other from the attacker's angle.

### 4.1 Evaluate from the defense side

**4.1.1 Confidentiality.** We first consider the aspect of data storage; the sensitive data of transaction and the encryption keys are stored in the SIM card which is a tamper-resist device. And if the cell phone was lost or stolen by others, the verification of the PIN prevents the cell phone from misusing by someone else.

As for data transmission, the data between the merchant and the operator or between the operator and the bank can be transferred through the wired network such as ADSL, which use SSL transaction protocol to ensure the security of data. And the signal

protection mechanisms of GSM/UMTS ensure the secure connection of USSD between the operator and the consumer [9].

**4.1.2 Privacy.** The transaction privacy of the consumer depends on the transaction number — the merchant cannot get personal information of the consumer, and has no corresponding key to decrypt the transaction number. Therefore, the merchant is unable to collect the purchasing habits of a consumer.

In the aspect of the operator and bank, only the price of merchandise is in the transaction data. So, even though the operator knew well about the identity of the consumers, they cannot know what merchandise the consumer has purchased (as shown in Figure 3). In our payment mechanism, the consumers have the overall privacy.

**4.1.3 Authentication.** The consumer is authenticated three times in our payment mechanism:

- First, the operator verifies the transaction password (Password) after decrypting the transaction number (as description in step 3).
- Second, the cell phone verifies the PIN after the consumer confirms the transaction data from the operator (as description in step 4).
- Third, the bank verifies the signature of the consumer with the corresponding key.

With those three authentications, the risk of counterfeit is reduced to the minimum.

As for the merchant, the bank authenticates the merchant by verifying its certificate.

**4.1.4 Non-repudiation.** After the consumer confirms the transaction, he has to sign a digital signature on the transaction data. Then, the bank authenticates the consumer by verifying the signature. The transaction is confirmed if the signature was correctly verified, and the consumer cannot deny the transaction. The bank transmits the payment receipt to merchant after account settlement, so the merchant can avoid the risk of consumer's bad debit.

**4.1.5 Integrity.** After the merchant summarizes the transaction data, it prints out a transaction receipt to the consumer; then the bank transfers a payment receipt to the consumer after the account settlement (as shown in step 7 (b) of Figure 3). These two receipts can be combined through the serial number of the transaction. The consumer can ensure the integrity of the transaction by comparing these two receipts.

**4.1.6 Other Discussion.** Besides the security criteria mentioned above, our payment mechanism is also feasible. The main reason is that it will not take great cost to the participator to adopt the payment mechanism into his business model.

## 4.2 Evaluation from the Aspect of Attackers

William proposed that there are many network security essentials need to be considered [10]. He classified the threats of security into four categories: interruption, interception, modification, and fabrication. In the following, we discuss our mechanism from those four categories.

**4.2.1 Interruption—the attack on availability.** In our payment mechanism, the attackers may take denial-of-service as their purposes. For consumer, the virus attack which may exhaust the power of mobile phone can be overcome by removing the program. But, if the consumer doesn't download any unknown program, the hacker will have no chance to attack.

In the aspects of the merchant, hackers may attack the POS or the transmission network by cutting the connection of Internet generally. This kind of attacks has been prevalent in wired network, and the defense measures are too numerous to enumerate. Generally speaking, the merchant can prevent those attacks by firewall and other technologies.

As for the operator and the bank, the back-end servers which store a lot of data may be the target of the attacks. However, both operator and bank make the best effort to protect the servers so that it cannot be easily destroyed. As to the network, they also adopt multiple mechanisms to secure the connection of network.

The hackers do not prefer the attack of interruption for its limited benefit, even if the attack might be successful.

**4.2.2 Interception—the attack on confidentiality.** It may bring the great benefits to attackers if they get the content of the transaction data during the payment process. So the attacks on confidentiality are frequently.

In our payment mechanism, the consumer has to transfer the transaction number to the merchant. Once transaction number is eavesdropped, it is very hard for the hackers to unravel the cipher text. The reason is that the transaction number is encrypted by using the public key of the operator, and only the operator has the corresponding private key to decrypt.

Besides, transferring through fixed network (which uses SSL transaction protocol) can protect the data between merchant and operator and between operator and the bank. Even if the attacker successfully intercept and unravel the encrypted data, he will never pass the multiple authentications and purchases the goods by using the illegal transaction number. If the transaction data transferred from the operator seems to be tampered, the consumer will deny the transaction to the operator and may change his transaction password later.

**4.2.3 Modification—the attack on integrity.** The attacks on integrity are useless because there are two protections of transaction integrity in our payment system: the receipt and the signature.

In step 2 of our transaction process, the merchant prints out the transaction receipt to consumer. The transaction receipt contains all the transaction information. If attackers modify the transaction data, the consumer can deny the transaction basing on the corresponding transaction receipt.

Besides, the bank transfers the payment receipt to both consumer and the merchant after settles the account. If the attacker was the consumer himself who tampered with the amount of the price, the merchant can reject the transaction by checking the payment receipt.

The digital signatures of the consumer and the merchant are very effective against the attacks on integrity. The attacker will fail to tamper the transaction data when the bank verifies the signature.

**4.2.4 Fabrication—the attack on authenticity.** The attack of fabrication is the most serious threat when paying with credit card. Similarly the attackers may want to forge the cell phone and the SIM card or pretend to be the legal consumers to make the illicit transaction in our payment mechanism. Nevertheless, there are three components including transaction password, PIN number of the cell phone, and the verification of signature to the consumers in the proposed mechanism to overcome the problem.

The illegally-generated transaction number will fail in the verification stage of the operator. Even if the attackers are capable of fabricating a SIM card, they still fail to make transactions without the valid private key.

In summary, we know that our payment mechanism ensures relatively high security for all participants.

## 5. Conclusion

The development of the Internet, handset devices, and telecommunication technologies are changing the way of our life extremely, especially in commerce. Lots of novel business models emerge rapidly. However, the most important and insecure stage in the transaction is payment. Without an appropriate payment mechanism, any business model will be hardly put into practice. Therefore, we have an urgent need for designing a securer and more convenient payment mechanism.

The payment mechanism we proposed adopts the cell phone to be the payment tool. The mobile phone generates a dynamic transaction number for the payment, so the consumers can go shopping without worrying that the transaction number is eavesdropped. Furthermore, the risk can be minimized even if the consumer lost the cell phone or the cell phone was forged. Because of the protection of asymmetric

encryption and the transmission of information without sensitive data, the consumers enjoy complete privacy in the entire process of the transaction. In addition, the participators can reduce the cost if they use our payment mechanism in their business model.

Our payment mechanism is very suitable for the payment with large amounts of money because it provide the overall protection of security and privacy. Our future work is to make the payment mechanism more flexible and integrate it with other payment systems, such as micro-payment system, e-cash and so on, to formulate a more omnibus and robust payment system for the new era.

## 6. References

- [1] Wei-Han Hsu, "Analysis of Mobile Payment Systems", *Master Theses, Department of Information Management, National Taiwan University*, September 2003.
- [2] David McKitterick, and Jim Dowling, "State of the Art Review of Mobile Payment Technology", *TCD Computer Science Technical Reports*, 2003.
- [3] Cheng-Huang Yen, *Mobile and wireless communications*, Key Hold Information INC, 2003.
- [4] Teppo Halonen, "A System for Secure Mobile Payment Transactions", *Master Theses, Department of Computer Science, Helsinki University of Technology*, January 2002.
- [5] Chia-En Lee, "A Secure and Convenient Mobile Credit Payment Scheme Using Public Personal Information", *Master Theses, Department of Information Engineering and Computer Science*, Feng Chia University, July 2003.
- [6] Wen Hung Su, "Adaptive Payment System for Mobile Environment", *Master Theses, Department of Electrical Engineering, National Taiwan University*, 2002.
- [7] Aviel D. Rubin, and Rebecca N. Wright, "Off-line generation of limited-use credit card numbers", *Financial Cryptography Conference*, February 2001.
- [8] Mobile Payment Forum, "Mobile payment forum white paper", December 2002.
- [9] S. Schwiderski Grosche and H. Knospe, "Secure mobile commerce", *Electronics & Communication Engineering Journal*, 2002.
- [10] William Stallings, *Network Security Essentials*, Prentice Hall, 2000.