Mobile Payment System with Privacy Protection

Kuenliang Sue, Wanpu Hsieh

Department of Information Management, National Central University, Chung-Li, 320, Taiwan, China
{klsue, im880703}@mgt.ncu.edu.tw

ABSTRACT

Trade security is the main point of the payment system. The system should fit the security issues such as confidentiality, authentication, and non-repudiation. However, the privacy problem seems to be ignored. This article proposes a new structure to improve the privacy of mobile payment system when consumers buy something via mobile device. The new system needs to fit three points: familiarity, privacy, and non-repudiation.

Keywords: mobile payment, non-repudiation, privacy, mobile commerce

1. INTRODUCTION

The trade behaviors are changing gradually because of the rise of mobile commerce. In the past trade activity, people needed to bring a lot of cash by themselves. Gradually, the applications of the plastic currency grow, people reduce the times using cash. Then, the appearance of e-commerce, the trade is no longer confined to face-to-face. The trade no longer needs to stay in one regular place. However, some problems still exist. Although plastic currency is convenient, people need to take a lot of cards with themselves. Even the trade of e-commerce can be remote, the security and convenience are still insufficient. Fortunately, mobile payment can change the predicament. People do not need to bring many cards because the tool of the trade is the mobile communication device that we can find easily on our person. Convenience of the trade increases greatly. The trade activity can be processed in any time, at any where, and with any people. Nevertheless, due to the congenital defect of the mobile device, it is unable to carry on the complicated security mechanism. The security problem is the key point in mobile payment system. Figure 1 shows the traditional payment model of credit card. This is the payment model of e-commerce, too. With this model, we can understand the trade activity in the past.

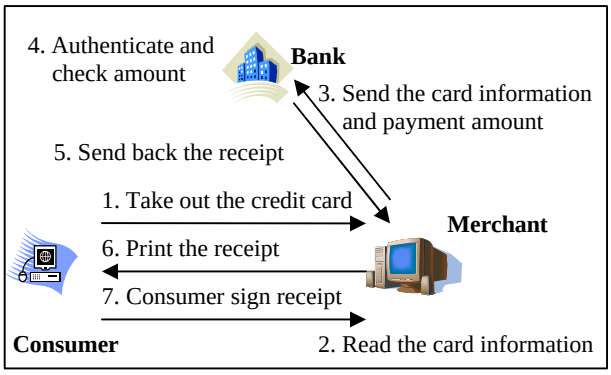

Figure 1. Traditional credit card payment model

Step 1, consumers take out the credit card to begin the trade. Step 2, the merchant uses a card reader to read the credit card information of consumer. Step 3, merchant sends the credit card information to the bank. Step 4, the bank authenticates the consumer and checks amount to finish the payment. Step 5, the bank sends the receipt back to confirm the trade. Step 6, after the merchant receives the receipt, merchant will print out the trade receipt to do a confirmed by consumers. Step 7, consumers need to sign and confirm on the receipt. After finishing those steps, trade behavior by using credit card completes.

Although using plastic currency is very general for people nowadays, it seems that the whole procedures do not pay enough attention to the security issues. Potentially, one can pretend himself is someone else and forge a trade by using other people's credit card number. The similar situations also happen on the network. Except for worrying about the criminal gang to record the number of the card, consumers also need to believe the merchant very much and think that the merchant will not steal the personal information of the consumer. Because we must transfer the personal credit card to the merchant to help us read the information and finish the trade procedure. Although we can use receipts to confirm whether the amount of money of consumption and goods have mistakes or not, the important private information like trade account may be recoded and collected during the step of reading the card. Hence, the evil-minded merchant can use the information, forge into consumers and consumers are unable to be aware of it.

In order to remedy these known defects, this article proposes an improved architecture and meets the following demands. First, follow the past trade habits of the consumer, but change the paying device into the mobile community device or other hand-hold community device. Secondly, strengthen privacy protection and disable the merchant to learn account information and accumulate shopping habits of the consumers. Also, the telecommunication operator (operator) is unable to know what the user bought. Last, offer the non-repudiation trade security.

2. RELATED WORKS

This section will review the related works of mobile payment system. In wireless mobile payment system the greatest challenge is the security threat. The study of Welch and Lathropped [1] divided these attacks into seven kinds as shown in Table 1. Except for unauthorized Access and Replay, others are set up on the basis of collecting and analyzing the package. Moreover, the Session High-Jacking attack could take the session instead of the user.

Table 1. The attack of wireless security

Traffic Analysis	Analyze the transmitting flow in the network
Passive Eavesdropping	Collect and analyze the network package to understand its content
Active Eavesdropping	Attract the destination to sending the specific package voluntarily to collect and succeed in analyzing packages
Unauthorized Access	The abnormal authorizes
Man-in-the-middle	Steal a glance or modifies the package that destination send
Session High-Jacking	Get involved and replace the session of the destination
Replay	Repeat sending the used package

Hence, wireless network also need to consider several important issues in the network security, such as confidentiality, authentication, authorization, integrity, non-repudiation. The best solution relies on encryption and the authentication mechanisms. Encryption mechanisms can offer the confidentiality and integrity. Authentication mechanisms can offer authentication, authorization, non-repudiation. In addition, the personal privacy of the consumer, e.g. shopping habits, is important security issues, too.

In order to apply mobile payment to the commercial trade, several trade systems considering about security issues are proposed. The research of Soliman and Omari [2] propose a dynamic encryption mechanism, the encryption key does not need regular storing in user's device, but produce the encryption key dynamically to avoid the encryption key lost or stolen. This system adopts symmetrical encryption to maintain confidentiality of consumer's trade and the encryption key exchange mechanism is also proposed to overcome the problem about losing encryption key. Later, Kungpisdan, Srinivasan, and Le propose an encryption key management mechanism [3] to improve the symmetrical encryption problem that may be lost of key if the encryption key does not change. Maybe this kind of systems can protect confidentiality, but the importance of non-repudiation is not mentioned.

In the model of the trade, non-repudiation is a very important security mechanism. All of the symmetrical encryption systems are unable to offer non-repudiation. Thus, Fourati, Ayed, Kamoun, and Benzekri propose a research that hope to take SET [4] mechanism to provide non-repudiation and personal privacy [5]. After consider the operation ability of mobile device, take the authentication mechanism of the part of SET, and combine WTLS/TLS [6] [7] to build a non-repudiation system which mixes the advantage of the two. Except for adopting the method like this, there are also systems introducing the mechanism of digital signature to improve performance. Such as the research of Herzberg, it adopts the digital signature mechanism of DSA [8] to satisfy non-repudiation.

In addition, the privacy of consumer also needs protection in the trade. The research of Sue adopts user identity (UID) to replace the cell-phone number [9] when the trade message transmitted to the merchant. Because consumers' user identity is regular, merchants probably collect customer's private information, such as habit about consumption. If the UID is not always the same, consumer's privacy can be protected. Based on the similar concept, Rubin and Wright [10] propose the variation code method in the payment system of the wired network. It utilizes random codes to prevent consumers' credit card number from spreading in the network. Combine the UID [9] and variation code methods [10] for wireless applications, the merchant probably can not accumulate consumers' shopping habit.

However, this method needs to assistance of the operator. Hence the operator has an opportunity to accumulate consumers' shopping habit. The main reason of the problem lies in the structural design. The mobile payment model is often modified by e-commerce payment model. Only the trade equipment of the front-ends is changed. No matter which payment model is adopted, the account numbers of the trade should pass to the merchant. Consumers will lose the privacy, such as shopping habits.

3. A NOVEL MOBILE PAYMENT SYSTEM

This article proposes a novel model to reduce the security risk of the credit card payment and provide privacy protection in mobile payment. The proposed system will employ mobile equipment as the front-end traded device and the trade information will not be transmitted via any merchants. Hence, the system is able to protect the security of the trade account. The structure of the system is shown as Figure 2.

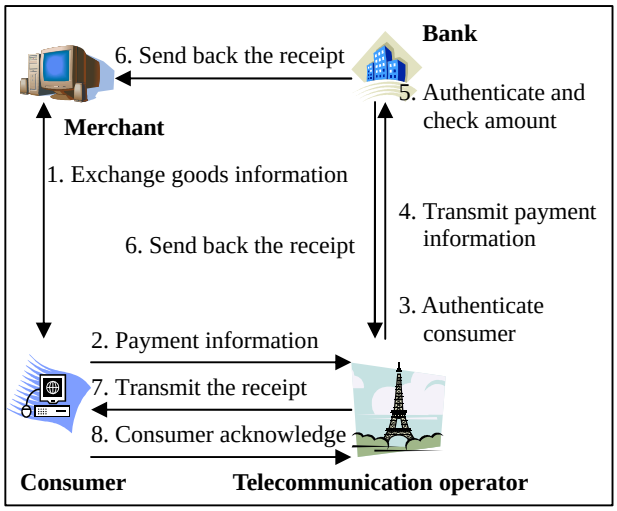

Figure 2. Structure of Payment System

3.1 Structure of Payment System

In order to exchange the trade message with consumer's mobile equipment directly, the trade structure demands some techniques to support, such as the Bluetooth interface. The interface is better an independent set to disable merchant from acquiring consumers' information, such as cell-phone number or account number. The banks in such system need to connect with the operators to deliver trade information to the users of the mobile payment system. In addition, consumers' mobile equipment needs the memory devices to store private key because this article applies consumers' private key to do digital signature to maintain non-repudiation. However, the signature algorithm is part of asymmetrical algorithms, several researches point out that the asymmetrical algorithms is more complicated than the symmetrical algorithms. Hence, we can select an asymmetrical algorithm to minimize the burden of mobile device when implementing the proposed payment system. According to the comparison [11] shown in table 2, the RSA algorithm is adopted to do digital signature.

Table 2. Digital signature perform comparison sheet[11]

Signature	Verifiable Encryption	
	#exponentiations	Size (bytes)
RSA	**7.5**	**400**
Gennaro et al	7.5	400
GramerShoup	8.7	544
GQ	10.5	544
Schnorr	8.3	388
ElGamal	8.5	388
DSA	11.6	484

In addition, we can adopt shorter private key on the mobile device to reduce the computation load and request the telecommunication operator to employ other complicated digital signature algorithm for security after confirming users because the telecommunication operator has no restriction on computation. If consumers lose the mobile device, they just need to notify the operator stopping the service of the cell-phone. The forgers will be unable to pass the second layer authentication mechanism, and obtain the digital signature of the telecommunication operator. It can protect both the banks and consumers.

3.2 Procedure of Payment System

In this section, the trading procedures of the proposed system will be introduced. Table 3 defines the code to help readers understand.

Table 3. Code contrast

Name	**Code**
Merchant	Merchant
Consumer	Consumer
Telecommunication operator	Operator
Bank	Bank
Hash function	Hash
Item identity	Item_id
Item price	Item_price
Merchant identity	Merchant_id
Trade identity	Trade_id
Message Authentication Code	MAC
Cell-phone number	PhoneNum
Digital signature of Consumer	Sign_U
Digital signature of operator	Sign_O
Digital signature of the bank	Sign_B
Digital signature text of Consumer	Text_Usign
Digital signature text of Operator	Text_Osign
Digital signature text of the bank	Text_Bsign

The payment system has 8 steps. The motion of each step and content of each message will be introduced below

Step 1, (Item_id, Item_price, Merchant_id, Trade_id) + MAC

Consumers communicate with the trade system of the merchant and get the trade message from it via the bluetooth interference. In order to prevent the trade information from being modified, the merchant will use hash function to product message digest, such as MD5 [12] or SHA-1 [13]. The detailed composition of message is shown in Figure 3.

Hash

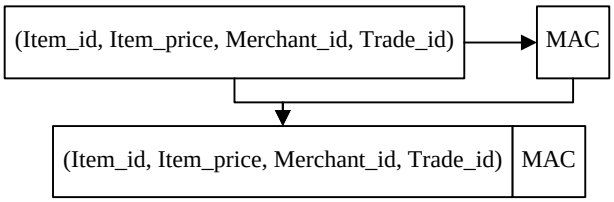

Figure 3. Trade procedure - Step 1

Step 2, Sign_U(Trade_id, MAC) + PhoneNum

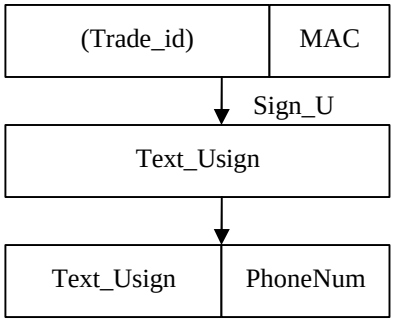

Figure 4. Trade procedure - Step 2

Consumers' mobile device will receive the trade message from the trade system of the merchant. Then consumer takes out the trade identity and MAC, and signs to respond the trade. Transmit the message to the telecommunication operator by GPRS or other wireless technology. The content of message is shown Figure 4. To prevent the operator and the bank from knowing the detailed content of the items that consumers bought, only the trade identity is transmitted.

Step 3, Authenticate consumer

When the operator receives the message that consumers transmitted, the operator will do the GSM authentication method to confirm the user identity of the mobile device.

Step 4, Sign_O(Sign _U(Trade_id, MAC), PhoneNum)

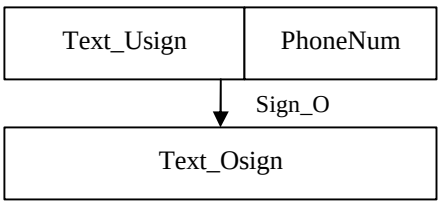

Figure 5. Trade procedure - Step 4

If consumers pass authentication, the operator will do digital signature to show the responsibility. In order to strengthen the non-repudiation, the operator can adopt more complicated digital signature algorithm. The content of the whole digital signature are shown in Figure 5. Later, transmit the message to the bank.

Step 5, Authentication and payment inside the bank

When the bank receives messages from the operator, the bank will verify operator and consumers by the digital signature of them respectively. Then, the bank confirms consumer's available amount and pays the money.

Step 6, Sign_B(Trade_id, MAC)

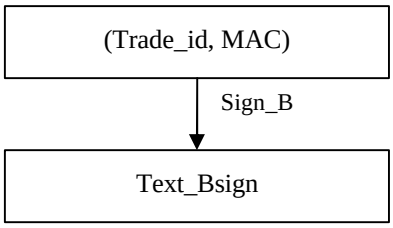

Figure 6. Trade procedure - Step 6

After finishing the payment, the bank produces the receipt of the trade and adds the digital signature to show the responsibility. The content of receipt is shown in Figure 6.

Step 7, (Text _ Bsign)

This procedure only passes the receipt that is come from the bank. The operator does not need to add any digital signatures on the receipt because mobile device will need more complex computation if there are more digital signatures. In addition, the content of receipt is just trade identity, has no safety consider.

Step 8, consumers acknowledge the operator.

Step 8 is to ensure that consumers have already the receipt, but it is not the essential procedure. Such procedure can be omitted to simplify the procedure of the system and payment check can be done by the bank monthly.

Here showing some expected goals which this article tries to satisfy. First is familiarity. Although consumers have more one action, it can protect the individual privacy of consumer. Actually, the action is equivalent to the consumer signature in the past. Furthermore, such action can be simplified by software design, the consumer just need to press the next button when mobile device receives the trade message. Second is that the privacy of consumers is protected. The merchant only participates in Step 1 and Step 6 (Figure 2). These two procedures transmit the receipt and the trade message which include item identity, item price, and trade identity. The merchant are unable to know the account that consumers use for trade, and even can not accumulate shopping habit of consumers because consumers do not transmit the user identity or the cell-phone number to the merchant. As in the aspect of the operator and the bank, because consumers just transmit the trade identity in Step 2 (Figure 2), the operator and bank are unable to know what consumers buy and accumulate consumers' shopping habit. Hence, consumer's privacy of shopping habit and trade account

can be protected. Third is the non-repudiation. Three digital signatures of the consumer, the bank, and the operator are used in this system and represent non-repudiation of three participants. Consumers' digital signature makes consumers unable to deny the trade. Digital signature of the operator makes the operator can not deny ever passing the trade messages from authenticated consumers to the bank. Digital signature of the bank makes the bank can not deny approving the payment.

4. EVALUATION OF SYSTEM SECURITY

This section analyzes the system structure and system procedure to evaluate the system if fit the request of security. Evaluation will follow three aspects: bank, merchant, and consumer.

4.1 Confidentiality

Confidentiality is usually done by encryption, but this system does not apply the encryption algorithm. Here is another opinion of the confidentiality in trade. Because the message which is transmitted by consumers in the network has important information inside, such as bank account of consumers, trade items information. The confidentiality protects the message not to be watched. If the information does not be transmitted in the network or the message transmitted in the network does not include such important information. Then, encryption may not be necessary, and indirectly satisfy the confidentiality.

4.2 Integrity

Integrity is designed to protect the merchant. Because the merchant only participates in the beginning step 1and the step 6 of the trade procedure shown in figure 2. The merchant may be afraid that the price of the items or the items identity will be changed. Let the merchant add MAC which is made by hash function on the transmission message. In after procedure among transmission, the MAC needs to be transmitted without changed until the message transmitted back to the place of merchant.

4.3 Authentication

The Authentication has difference opinion because of the participant. From the view of the consumers, consumers add digital signature on the transmitted message to the bank, in order to confirm that no other people can start the trade request without consumer's permission. According to the digital signature added by the bank consumers can also authentication the bank. From the view of the bank, confirm the trade is authorized by consumers using the digital signing of consumers. From the view of the merchant, because the received receipt has digital signature of bank, the merchant can confirm the bank had already paid the amount.

4.4 Non-Repudiation

The non-repudiation also finishes through the mechanism of digital signature. By digital signature, consumers can't deny the trade, the operator can't deny authentication consumers and pass trade request made by consumers. The bank can't deny finishing consumers' payment. The trade is invalid unless there is assurance of digital signature.

4.5 Privacy

The protection of privacy is the key of this article. About trade account which includes the credit card number and bank account, the merchant has no way to receive trade account because trade message is transmitted by consumers. In addition, the consumer is authenticated by using digital signature, and trade account of consumers is never transmitted in the network. About shopping habit, the transmitted message in the network only has the trade identity and MAC, the bank and operator only know the identity without meaning. Therefore, the system can protect privacy of consumers.

5. CONCLUSION

The proposed system in this article puts emphasis on three parts, familiarity, privacy, and non-repudiation. First, the trade behavior does not change very much. Instead of using credit card, consumers use the mobile device with them to do trade activity. Hence, consumer will just perceive the change of trade device. The mobile device, e.g. handset, is familiar to consumers. Secondly, consumer's privacy can also be protected. The merchant, operator, and bank can't accumulate shopping habit of consumers. Third, the proposed system using digital signature to protected the trade non-repudiation. Table 4 shows the comparison of relevant payment system research in the past.

Table 4. Systematic comparison of payment

	Encryption system	Digital signature system	Account protected system	The proposed system
Confidentiality	◎	◎	◎	◎
Non-repudiation	×	◎	×	◎
Account protect	×	×	◎	◎
Trade privacy	×	×	×	◎

(◎: Offer, ×: Does not offer)

The proposed mobile payment system satisfies not only the payment security and non-repudiation requirement in the traditional electronic trade but also the protection of consumer's privacy which is paid attention gradually now. In this system, the merchant, operator, and bank

can't accumulate shopping habit of consumers.

Perhaps someone will query that this model needs consumers to transmit trade message to the operator and this step will increase the transmission burden of the network. In fact, under the primitive transmission structure, consumers must transmit the trade message to the merchant. In our design, the message is just transmitted to operator instead. Hence, the change will not increase the transmission burden of the network.

REFERENCES

[1] Welch, D., Lathrop, S., "Wireless Security Threat Taxonomy", *2003 IEEE Workshop on Information Assurance United States Military Academy*, pp76–83, West Point, NY, Jun. 18-20, 2003.

[2] Soliman, H. S., Omari, M., "An Efficient Application of A Dynamic Crypto System in Mobile Wireless Security", *Wireless Communications and Networking Conference 2004/IEEE Communications Society*, Vol. 2, Mar. 21-25, 2004.

[3] Kungpisdan, S., Srinivasan, B., Le, P. D., "A Secure Account-Based Mobile Payment Protocol", *International Conference on Information Technology: Coding and Computing (ITCC 2004)*, Vol. 1, pp35 – 39, Apr. 5-7, 2004.

[4] "SET Specifications", http://www.setco.org, 1997.

[5] Fourati, A., Ben Ayed, H.K., Kamoun, F., Benzekri, A., "A SET Based Approach to Secure the Payment in Mobile Commerce", *Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN.02)*, pp136 – 137, Nov. 6-8, 2002.

[6] Howell, R., "WAP Security", *Concise Group Ltd.*, http://www.vbxml.com/wap/articles/wapsecurity/default.asp

[7] WAP Forum, "Wireless Transport Layer Security Specifications", Version Apr. 2001, http://www.wapforum.org, April, 2001.

[8] Herzberg, A., "Payments and Banking with Mobile Personal Devices", *Communications of the ACM*, Vol.46, No.5, 2003.

[9] Sue, W.H., "Adaptive payment system for mobile environment", *Dissertation submitted to Department of Electrical Engineering National Taiwan University*, 2003.

[10] [Rubin, A. D., Wright, R. N., "Off-line generation of limited-use credit card numbers", *AT&T Labs – Research*, 2002.

[11] Ateniese, G., " Efficient verifiable encryption (and fair exchange) of digital signatures", *6th ACM conference on Computer and communications security*, 1999.

[12] Rivest, R., "The MD5 Message Digest Algorithm", *Request for Comments (RFC) 1321*, Internet Activities Board, Apr., 1992.

[13] National Institute of Standards and Technology, "Secure Hash Standard", *Federal Information Processing Standard Publication 180-1*, U.S. Department of Commerce, Apr., 1995.