On-Line Payment with Cellular Phone[1]

Lih-Chyau Wuu[*], Yi-Wei Lu, Yu-Jung Shen, and Yen-Hung Chen

Department of Electronic Engineering, National Yunlin University of Science and Technology
Yunlin 640, Taiwan, R.O.C.
E-mail: wuulc@yuntech.edu.tw

Received 1 March 2006; Revised 4 May 2006 ; Accepted 8 May 2006

Abstract. Recent rapid development in mobile communication enables people being with cellular phone wherever they go. It is practical to enhance the functionality of cellular phone, and one is to boost consumer-friendly mobile transactions by replacing traditional credit card payment system. However, previous researches focus on the improvement of smartcard technology [1]. That means the handset must be upgraded and that will hinder the take-up of mobile commerce [2-5]. In this paper, we propose an on-line payment scheme that people can securely complete their transactions by their current cellular phones with no need to upgrade their handsets. Our scheme uses SIM card, User ID and Password to solve the insecure flaws of credit card such as signature forgery, stealing behavior of untrustworthy merchants. Furthermore, the secure information of people such as credit card number, cellular phone number never travels across the network.

Keywords: security in digital systems, m-commerce, on-line payment, virtual credit card, cellular phone

1 Introduction

The proliferation of credit cards [6-8] started in the USA in the early 1950s. They allow people to shop without cash. Such a convenience causes the credit cards to spread rapidly and widely around the world. However, credit cards are convenient but do not provide anonymity, and continuous improvements of organized crime make people nervous whenever they use the cards. For example, while people go shopping and pay by card, the untrustworthy merchant may have an opportunity to steal the secure data of the card by a special POS (Point of sales) terminal. Furthermore, traditional card transaction system uses signature for authentication, which is easy to be imitated when a card is lost.

In this paper, we propose an on-line payment scheme to improve the insecure flaws of credit cards system mentioned above. It is expected that, in the near future, people will be with cellular phone wherever they go. In our scheme, people pay their transactions by their cellular phones, instead of credit cards. This makes the cellular phone have one more function: virtual credit card [9-10].

The virtual credit card is a representation of a traditional credit card that stores custom information, including name, address, card number and relevant information on the PC or cellular phone. Companies such as Motorola, Trinitech, Ericsson, Visa and Mondex have been working on putting virtual credit card on handset's smartcard. That means people must upgrade their handsets for virtual credit card. In our scheme, the virtual credit card is stored in the bank, not on the phone. People must give their cellular phone number to and get their user identification (UID) and password from the bank. People do not need to upgrade their handsets in our scheme. A payer presents his/her UID, instead of credit card, to a merchant during a transaction. After that, the payer will receive a call to authorize the transaction on line.

Our scheme uses (1) UID to provide anonymity and prevent the merchant from learning credit card number, cellular phone number of the payer; (2) the GSM authentication protocol [11] and payer's password to verify payer's authentication, (3) on-line conversation recording to enforce non-repudiation. To accomplish a transaction in the scheme, UID, cellular phone number and password of payer must be coincident. That prevents unauthorized people from counterfeit even when the cellular phone is lost.

2 System Architecture

The participants of our scheme include client, merchant, authentication gateway and bank as shown in Fig. 1. A

[1] Taiwan Patent No.-163818

[*] Correspondence author

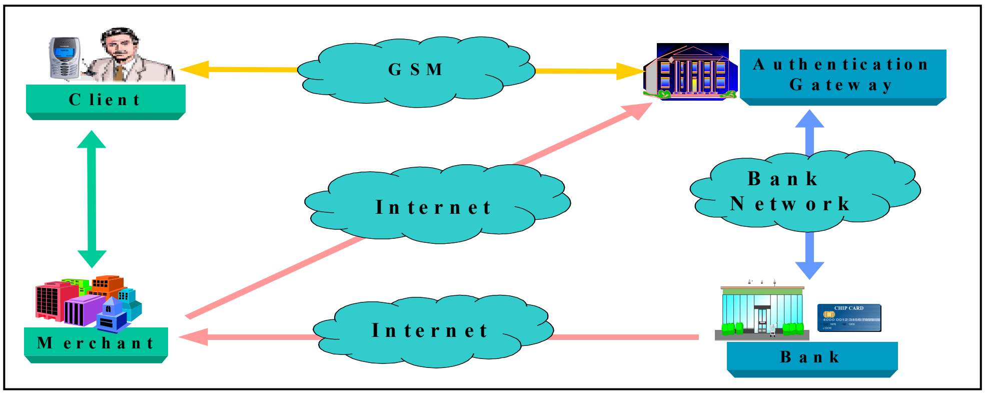

Fig.1. System Architecture

client is an authorized holder of a virtual credit card and a GSM cellular phone. A merchant is a person or organization that has goods or services to sell to clients. A bank is a financial institution that issues virtual credit cards to clients and establishes accounts with both merchants and clients. In our scheme, clients and merchants have to open an account at the bank to get their user identification (UID) and *merchant identification* (MID) respectively before engaging any transaction. The merchants are also required to install the merchant software into their computers to automatically process all the messages exchanged in a transaction via internet. An authentication gateway is a function operated by a bank or a designated third trusted party to implement authentication of a client and non-repudiation during a transaction. In conventional credit card system, each local area has a credit card center to manage all transactions with other banks. Our authentication gateway is to replace the credit card center; thus, it is assumed to have one authentication gateway in each local area and it will not increase the surcharge of a transaction.

Our system has two phases: the registration phase and transaction phase.

2.1 Registration phase

As mentioned above, clients and merchants must open an account before they engage any transaction. For safety, our scheme asks that clients and merchants must go to a bank to open their accounts in person. The clerk of the bank checks the identity of the client/merchant first, then stores private information of the client/merchant such as personal/store name, cellular phone number, account number, address, E-mail into the bank database. At the same time, the bank will produce a UID/MID, password for the corresponding client/merchant. The client/merchant can ask to change the UID/MID and password if he/her feels that it's difficult to remember the default UID/MID and password. After that, the bank will send UID, cellular phone number, password and credit quota if the applicant is a client, or MID, password if the applicant is a merchant, to the authentication gateway. Figure 2 illustrates the registration flow.

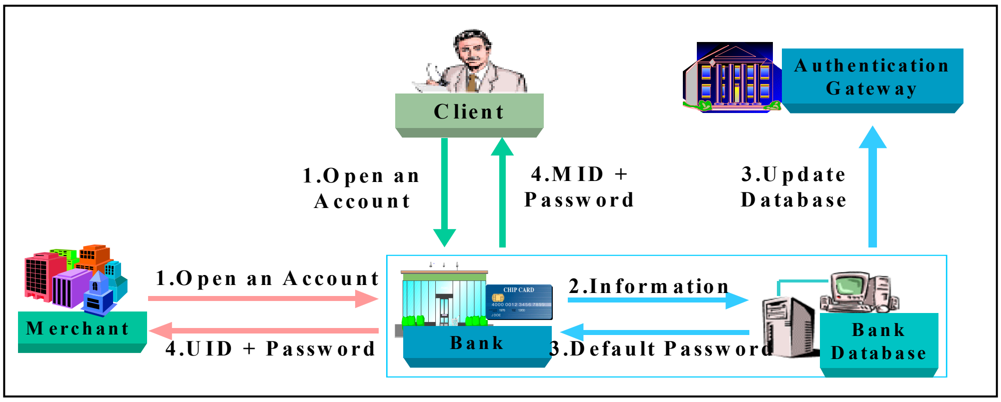

Fig.2. Registration phase

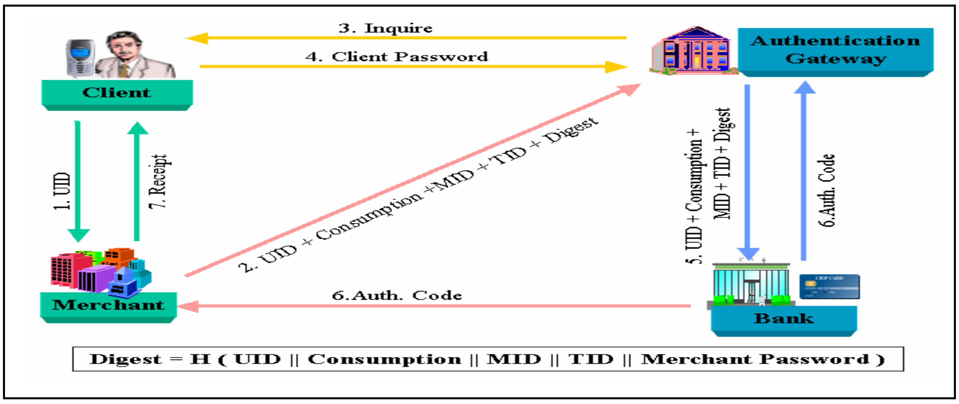
3. Inquire
4. Client Password
Authentication Gateway
Client
1. UID
7. Receipt
2. UID + Consumption +MID + TID + Digest
5. UID + Consumption + MID + TID + Digest
6.Auth. Code
Merchant
6.Auth. Code
Bank
Digest = H (UID || Consumption || MID || TID || Merchant Password)

Fig.3. Transaction phase

2.2 Transaction phase

A transaction shown in Figure 3 consists of the following seven steps:

Step 1: When a client gets to pay in store, he just tells the merchant his own UID, instead of credit card. Then, the client waits for a call from the authentication gateway to on-line check his transaction behavior (consumption).

Step 2: After getting the UID from the client, the merchant must send the transaction information including UID, consumption, MID, TID, and the digest of the transaction, to the authentication gateway by merchant's POS (Point of Sales) terminal via Internet. The digest of the transaction is computed as follows: Digest = H (UID||consumption||MID||TID|| Merchant password), where H is a hash function such as MD5 or SHA-1 [12]. TID is the transaction ID used to prevent the authentication gateway from replay attack. The Digest is used to provide message integrity as well as source authentication.

Step 3 and 4: As the authentication gateway receives the transaction information from the merchant, it first applies the same function H to compute a digest, and then compares it with the digest of the received message. If they are the same, the message integrity and source authentication is assured. The authentication gateway also checks whether the consumption is over the credit quota. If everything is O.K., after the checking process, the authentication gateway will make a call to the client. The call to the client is via voice dialogic system to inquire client's password and consumption. The authentication to the client is dependent on the security of GSM system [11] and the input of the client correct password. Since our system records the whole process, it enforces the non-repudiation as long as the client himself confirms the transaction behavior.

Step 5: As the confirming process is succeeded, the authentication gateway sends the transaction information, including UID, consumption, MID, TID, and the digest of the transaction, to the bank via a secure channel.

Step 6: Bank stores the transaction information into its database, then makes a signature on the digest of the transaction. The signature is called as an authentication code. That is, Auth. Code = ESKbank(the digest of the transaction), where ESKbank(M) means to use the private key of the bank to encrypt the message M. The bank may update the credit quota if necessary. After that, the bank sends the Auth. Code to the authentication gateway and the merchant.

Step 7: After receiving the authentication code, the authentication gateway and the merchant decrypt the Auth. Code by the public key of the bank to compare with its original digest of the transaction. If they are the same, the message integrity and source authentication is assured. The authentication gateway stores the transaction information accompanied with its Auth. Code into its web site to make that the client can check his/her bill again via Internet when necessary. As for the merchant, its POS terminal will print a receipt of this transaction to the client. To get the payment, the merchant presents the Auth. Codes to the bank.

2.3 Our Implementation

In order to simulate the proposed scheme, we use Microsoft Visual C++ Programming tool, Microsoft Access 2000, ODBC and Microsoft IIS 5.0 to implement Merchant module, Authentication gateway module and Bank module. Authentication gateway module uses the Voice Card of Dialogic Corporation [13] to handle the calling process and interactive voice response. There are 4 telephone lines in the voice card and 300 clients in our system. In average, the transaction phase illustrated in Fig. 3 needs 60 seconds to finish the interactive confirming process, which is the bottleneck of the system.

3 Comparisons and Discussion

In this section, the properties of our cellular phone payment scheme is described first, and then the differences among the current credit card transaction system, web-enabled ATMs [16], Teledit [17] and ours are pointed out.

3.1 The Properties of Our Scheme

- **Provide Anonymous Transaction**
  In our scheme, the merchant only gets the UID of the client. The true status and the cellular phone number of the client are not revealed to the merchant. It means that the merchant does not know who does the transaction. Though the authentication gateway and the bank can know who does the transaction, they can not know the content of transaction since the merchant only sends the consumption, not the detail of the transaction, to them.
- **Provide Authentication of Legal Client and Merchant**
  The cellular phone and the password of the client are used by the authentication gateway to verify a legal client. The password of the merchant being implicated in the digest of the transaction is used to verify a legal merchant.
- **Enforce Non-repudiation**
  In our scheme we use Automatic Voice System to talk with the client and record the whole conversation that the client cannot repudiate his transaction behavior. At step 6 of the transaction phase, the merchant receives the Auth. Code from the bank that the bank can not repudiate the payment required by the merchant.
- **Afford Triple Protection**
  To protect the genuine client, our scheme needs cellular phone, user ID and password of a client to do a transaction. That protects client from money loss even if the cellular phone was stolen.
- **Facilitate Convenience**
  No real card is needed. It does not require the upgrade of cellular phone. Every brand or model running GSM can afford to our scheme. Furthermore, our scheme does not depend on transport security mechanisms. That means our scheme can securely operate over a raw TCP/IP stack.
- **Create Applicability**
  The proposed scheme can not only apply to credit card system but also be available in Internet e-commerce.

3.2 Contrasts with Credit Card System

Table 1 highlights the comparison with the current credit card system, web-enabled ATMs [16], Teledit [17] and our cellular phone on-line payment scheme.

Table 1. A comparison of current credit card, web-enabled ATMs, Teledit and our scheme

	Current Credit Card	Web-enabled ATMs	Teledit	Cellular Phone Payment
Legal Client Verification	Photo and Signature	Smart Card and Password	Phone Number, ID number and Password	UID, Cell phone and Password
Verification Responsibility	The Merchant	The Bank	Telecommunication Company	Authentication gateway
Counterfeit Card	Magnetic Strip Card: Easy	Smart Card: Difficult	SIM card: Difficult	Virtual credit card: Difficult
Notice of Card/Phone Lost	Difficult, slower	Easier, faster	Easier, faster	Easier, faster
Communicating Way	Private line	Internet	Internet	Internet

Legal Client Verification
The photo and signature of people is used to identify the holder of a card on traditional credit card system. However, the methods are easy to be forged. Web-enabled ATMs uses Smart Card and password to authenticate the clients. Teledit and Our scheme apply three-level protection (for example, UID, Cellular phone, and Password) to enhance the security of authenticating process.

- ♦ **Verification Responsibility**
  For credit card system, the merchants take the responsibility of identification, but most merchants do not have the ability or equipment to identify. Ours asks the authentication gateway to take the responsibility of identifying legal clients and merchants, and the other two schemes let the bank and the telecommunication company to take the responsibility of identification.
- ♦ **Counterfeit Card**
  The secure data on traditional magnetic strip credit card is easy to being copied by the untrustworthy merchant. However, the data on the SIM (Subscriber Identification Module) card of the cellular phone is difficult to being copied.
- ♦ **Notice Card/Phone Lost**
  Cellular phone is considered as a bigger device than credit card that people is easy to notice when his/her phone is lost or stolen. In case card/phone lost/stolen, our scheme is more secure than credit card system since the person who picks up/steals the phone cannot use the virtual credit card unless he/she knows the UID and Password.
- ♦ **Communicating Way**
  For credit card system, the merchant communicates with credit card center by a special POS terminal via private line. The other three schemes let the merchant communicates with the authentication gateway via Internet. Furthermore, our scheme ensures source authentication and integrity of messages.

4 Conclusion

In this paper, we have proposed an on-line payment scheme with cellular phone. Our scheme protects the holder of virtual credit card from framing and forging. In particular, it provides anonymity and non-repudiation of payer. In our implementation, we do establish four participants to simulate the whole process of a transaction. The drawback in our system is that a transaction takes too much time, especially the authentication process between a client and an authentication gateway. This is because we use voice system in the authentication gateway to identify the client on-line by GSM. We will focus on integrating the latest wireless tech-product to improve the drawback. For example, if the authentication gateway of our system communicated with the client by WAP (Wireless Application Protocol) [14] or GPRS (General Packet Radio System) [15] to transmit authentication message, that would be faster than the one using voice system to do authentication.

References

[1] L. Kail, P.L. Yang, Z. Jun, A flash IC card with programmable security code, *Proc. of 4th International Conference on ASIC*, 2001, pp.584-587

[2] A. Zdravkovic, Wireless point of sale terminal for credit and debit payment systems, *Proc. of IEEE Canadian Conference on Electrical and Computer Engineering,* Vol.2, 1998, pp.890 -893.

[3] D. V. Thanh, Security issues in mobile e-commerce, *Proc. of 11th International Workshop on Database and Expert Systems Applications,* 2000, pp.412-425.

[4] J. Claessens, B. Preneel, J. Vandewalle, Combining World Wide Web And Wireless Security, *Network Security*, 2001, pp.153-172.

[5] A. Tsalgatidou and J. Veijalainen. “Mobile Electronic Commerce: Emerging Issues”. *Proc. of EC-Web 2000*, London-Greenwich, U.K., 2000a.

[6] Visa International Service Association, “Visa credit cards”, *http://corporate.visa.com/pd/ consumer_credit.jsp*

[7] MasterCard International Incorporated, “MasterCard credit cards”, *http://www. mastercard.com/us/personal/en/aboutourcards/credit/index.html*

[8] D. Eastlake, B. Boesch, S. Crocker, and M. Yesil, CyberCash Credit Card Protocol Version 0.8. *Internet RFC 1898*, February 1996.

[9] ECT News Network, Inc. “E-Commerce News Wireless Credit Cards How Soon and How Pervasive”, *http://www.ecommercetimes.com/story/2455.html* .

[10] X. Xianhua, S.S. Yuan, G. Ling, T.C. Lim, Virtual card payment protocol and risk analysis using performance scoring, *Proc. of 15th International Parallel and Distributed Processing Symposium*, 2001, pp.1-7.

[11] C.C. Lo and Y.J. Chen, "Secure Communication Mechanisms for GSM Networks", *IEEE Transactions on Consumer Electronics,* Vol. 45, No. 4, November 1999, pp.1074-1080.

[12] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall International Inc., 1999.

[13] Dialogic Corporation, *GlobalCall^{TM} Analog Technology User’s Guide For UNIX and Windows NT*, Dialogic Corporation, 1999.

[14] Open Mobile Alliance Ltd, “What is WAP?” , *http://www.wapforum.org/what/index.htm*.

[15] GSM Association, “GSM World - GPRS Platform”, *http://www.gsmworld.com/technology/gprs/index.shtml.*

[16] Financial Information Service Co., LTD, “Web-enabled ATM”, *http://www.fisc.com.tw/FISCWeb/Business/Content.aspx?No=144&FC=F03EC*.

[17] Danal Co, Ltd. “Teledit Service”, *http://www.teledit .com/eng/service/up_teledit_intro.asp*.