

A Secure Credit Card-based Billing Scheme for Telephone Services

Shiuh-Pyng Shieh, Chern-Tang Lin, Maujy Peng*, Wen-Chi Yang*, Jim-Ning Yang*

Department of Computer Science and Information Engineering,
National Chiao Tung University, Hsinchu, Taiwan

*Computer and Communications Lab., Industrial Technology Research Institute, Hsinchu, Taiwan

Abstract

MasterCard and VisaCard use credit cards to support a number of services, such as Masterphone or Visaphone, which allow cardholders to make phone calls from any telephone. However, these services take little or no security precautions. Although SET protocol has defined a secure payment method for card transactions over open networks, it cannot fit in telephone systems. In this paper, we propose two credit card-based payment schemes for telecommunication systems: one for public switched telephone networks and another for the Internet telephony. The proposed schemes can securely authenticate callers without exposing their secret information on the communication networks.

1 Introduction

Masterphone and Visaphone services allow cardholders to make phone calls from any telephone [3]. These services provide a convenient means for making international long distance calls via cards for tourists. To use overseas access or to make a chargeable local call, it is common to call a toll free service number and give the operator the caller's card number, personal identification number, and the callee's phone number. The call will be connected after the verification of account details. Then the cost of calls will be automatically debited the card owner's account. There are credit card phones with wipe readers which allow people to make calls using commercial credit cards as well as coins [5]. To make a call, customers must swipe their credit card through the reader of the phone, wait for authorization and then dial the number they want. Charges for these calls appear on cardholders'

monthly statements from their card company.

In today's credit card-based telecommunication services, the credit card numbers and personal identification numbers are often transmitted from cardholders to the telephone company over the telephone line without security precautions. However, this information provides the key elements needed to create counterfeit cards or fraudulent telephone calls. Thus, they should not be exposed to the telephone network system in plaintext form. The goal of this paper is to propose a method for the authentication of users without leaking the credit card numbers.

A simple credit card phone environment is shown in Figure 1. The authentication process takes place between the caller and the credit card authentication center

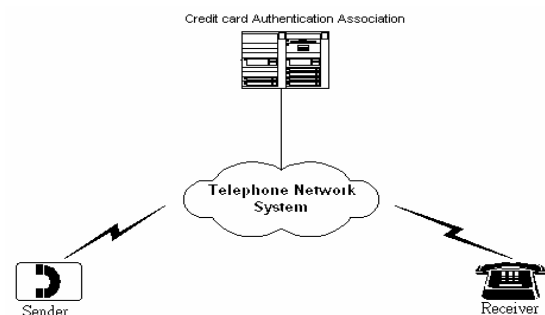


Figure 1: Credit card Phone System

(CCAC). CCAC is a gateway to check the authority of the caller. During the authentication process, the telephone company authenticates a caller only via CCAC and should not get both the credit card numbers and personal identification numbers. After the authentication process, the telephone company must get some evidences from the

CCAC. The evidence is a kind of digital signature to prove the user has made phone calls. The telephone company can charge the credit card company the cost of calls by the evidences from the CCAC. Then the credit card company will send the bill to its customers.

In this paper, we propose a secure credit card-based billing scheme for the public switched telephone network. This scheme can authenticate callers via CCAC and guarantee the confidentiality of callers' secret information. This scheme can be also applied to mobile telecommunication systems [1, 2, 7, 8, 14], such as GSM [10]. In our scheme, we assume that the credit card can authenticate the user directly, such as using a personal identification number (PIN) shared between the card and its owner. And the private key cryptosystem is sufficient for the authentication between the caller and the CCAC. Since signing documents with the private key cryptosystem is difficult, the public key cryptosystem is adopted to generate the digital signature as the evidences of calls. The public key cryptosystem also helps create a secure communication conveniently via the telephone network system.

With both the private and public cryptosystems, we propose a secure credit card-based billing scheme over the public switched telecommunication network. This scheme is also suitable for mobile telecommunication networks.

Recently, Visa and MasterCard have jointly developed the Secure Electronic Transaction (SET) protocol as a secure payment method for card transactions in the Internet [15]. In SET specifications, a cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling and taxes. The cardholder sends the merchant a completed order, which is digitally signed by cardholders who possess certificates. This method cannot be adapted easily to the credit card telephone service because a telephone charge cannot be determined until the conversation is

over. After the telephone conversation, the caller may evade or refuse to sign the bill. So, the signed messages must be acquired in the telephone conversation. To resolve the problem, we design another billing scheme based on our secure credit card-based billing scheme for the Internet telephone environment.

In the paper, we will outline the credit card-based telecommunication system environment and propose a communication protocol in Section 2 and 3. The payment flowchart for the Internet telephone network will be presented in Section 4. Finally, we will give our conclusions in Section 5.

2 Secure Credit Card Phone Environment and Notations

As the credit card phone environment shown in Figure 1, we assume that the caller is Alice and the callee is Bob. The entire process can be divided into four states shown in figure 2. When Alice makes a call to Bob via the telephone network system with a credit card, the telephone network system will request the CCAC whether or not she can make this call. The challenge of the user authentication is how to guarantee the confidentiality of user's secret information, such as the credit card number. If the CCAC authorizes her to make the call to Bob, the telephone network system will provide communication channel between Alice and Bob. Since a telephone charge cannot be determined until the conversation is over, we use a periodic payment scheme. That is, before the communication, CCAC must give the telephone company a communication evidence which allows the communication for a predefined interval. If the interval is arrival, the telephone company should reconfirm whether the caller would continue this conversation. If yes, the telephone company will get another evidence from CCAC and continue supporting this communication. Otherwise, the communication line will be broken. By these communica-

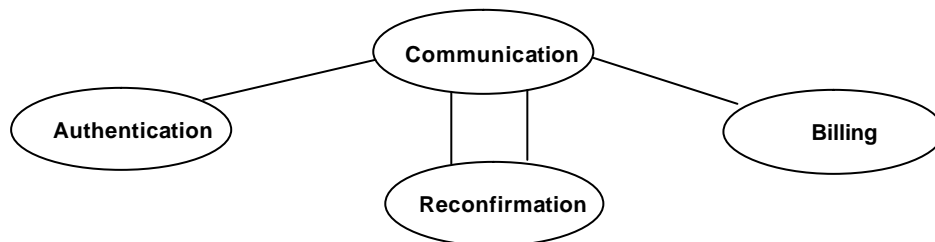


Figure 2: The state transition of the proposed protocol

tion evidences, the communication company can get the telephone charge from Alice's credit card account later. But the challenge of the periodic payment scheme is how to reduce the overhead of reconfirmation in order to keep the smooth of communications.

For user authentication, we use the challenge-response protocol [12]. That is, the system (CCAC) gives the user an authentication token (a challenge) and the user must return a response based on this token and some secret shared between the system and user. Then the system can authenticate the user by checking if the response is correct or not. To compute the response, we assume that each user has a hand held authentication card that verifies the card-holder with a unique password (PIN, personal identification number) whenever the user power-on this card. The card has an eight character alphanumeric display and a thin membrane keypad for operation as shown in Figure 3 [9]. Since users' credit card numbers are sensitive data, they should not be revealed as well as sent in plaintext form to the telephone company. For this reason, we assume that callers' telephones have encryption and decryption functions that support secure communication with CCAC and propose a secure credit card-based billing scheme for telephony over public communication networks. In this way, the telephone company can still acquire evidences to charge users such

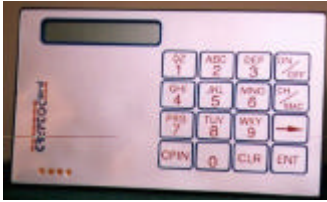


Figure 3: An hand held authentication card

that the user cannot deny the calls he/she made.

The following notations are used in the description of our proposed protocol:

- M : Alice's hand held authentication card which must support a private key cryptosystem.
- T_1 : The caller's (Alice's) telephone which must support a public key cryptosystem.
- T_2 : The callee's (Bob's) telephone which does not support any cryptosystem.
- C : Credit card authentication center who has two pairs

of key (E_C, D_C) and (P_C, S_C) , where (E_C, D_C) is for message encryption and decryption; (P_C, S_C) is for message signature and verification.

- N : The telephone network system which has a pair of keys (E_N, D_N) , where (E_N, D_N) is for message encryption and decryption.
- ID_a : Alice's credit card number.
- K_a : The secret key shared by C and Alice (recorded in her authentication card M).
- n_i : Nonces.
- t_i : Timestamps issued by N .
- z : The authentication token which is a random number.
- \oplus : Exclusive OR operation.
- $\{message\}_K$: An encrypted message which uses K as the key.

3 The Secure Credit Card-based Billing Scheme

The credit card-based billing scheme is shown as Figure 4.

Step 1: Alice calls her credit card authentication center C via the telephone T_1 with her card number ID_a and Bob's telephone number T_2 . The telephone T_1 generates random numbers n_1 with the public keys E_N and E_C to compute $X_{11} = \{T_1, T_2, N, C, ID_a \oplus n_1\}_{E_N}$ and $X_{12} = \{T_1, T_2, N, C, ID_a, n_1\}_{E_C}$. Then T_1 sends the message (X_{11}, X_{12}) to the telephone network system via telephone line.

Step 2: The telephone network system N uses the private key D_N to decrypt the message X_{11} . Consequently, N acquires the caller identity T_1 , the callee identity T_2 , CCAC identity C , $ID_a \oplus n_1$, and message X_{12} . The authentication message X_{12} is then forwarded to C .

Step 3: The credit card authentication center C uses the private key D_C to decrypt the message X_{12} . Then C knows the caller identity T_1 , callee identity T_2 , the telephone company N , the credit card number ID_a , nonce n_1 . C generates a random number z as an authentication token and sends it to the telephone network system.

Step 4: N passes the message z to T_1 .

is a legitimate user or not. If Alice is a legitimate user, C uses card number ID_a , nonce n_1 , timestamp t_1 and the private key S_C to generate a signature $X_{71} = \{T_1, T_2, N, C, ID_a \oplus n_1, t_1\}_{S_C}$. C keeps the record $(ID_a, T_1, T_2, N, C, n_1, t_1)$ and sends this signature X_{71} to the telephone network system N as an evidence for billing. Since the telephone network system N knows

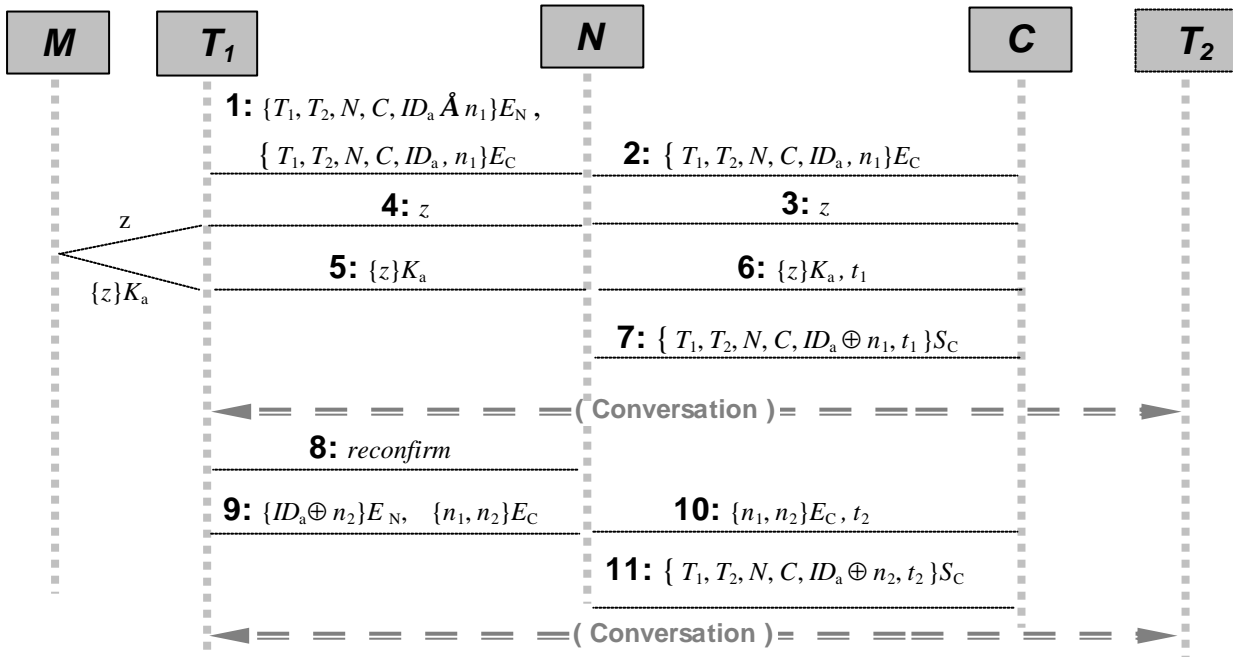


Figure 4: The secure credit card-based billing scheme

Step 5: For authentication, Alice inputs her PIN number into her authentication card M . If the verification succeeds, Alice types in the token z , which was seen on the telephone. The card responds with the message $X_{51} = \{z\}_{K_a}$, which will be input into the telephone T_1 . The telephone sends the response message X_{51} back to N .

Step 6: The telephone network system C sends the message (X_{51}, t_1) to C , where t_1 is the startup time for billing.

Step 7: The credit card authentication center C uses ID_a 's secret key K_a to check whether Alice

$T_1, T_2, C, ID_a \oplus n_1$, and t_1 , it can verify the signature X_{71} with the public key P_C . If the signature X_{71} is correct, N should establish a communication channel between T_1 and T_2 .

Steps 8-11: In advance, the telephone network system N needs to negotiate a reconfirmation interval with the credit card authentication center C by a contract. If the conversation between T_1 and T_2 is longer than the interval time, N should issue a reconfirmation signal to T_1 periodically. When T_1 receives a reconfirmation message, the telephone will generate a random number n_2 and send the message

$(\{ID_a \oplus n_2\}_{E_N}, \{n_1, n_2\}_{E_C})$ to the telephone network system. Then N has to get the evidence $\{T_1, T_2, N, C, ID_a \oplus n_2, t_2\}_{S_C}$ from C with timestamp t_2 as shown in Figure 3, where C saves the record $(ID_a, T_1, T_2, N, C, n_2, t_2)$.

Suppose $\{T_1, T_2, N, C, ID_a \oplus n_j, t_j\}_{S_C}$ is the last evidence. The telephone company sends the message $(T_1, T_2, N, C, ID_a \oplus n_1, t_1, ID_a \oplus n_j, t_j)$ and the signature $(\{T_1, T_2, N, C, ID_a \oplus n_1, t_1\}_{S_C}, \{T_1, T_2, N, C, ID_a \oplus n_j, t_j\}_{S_C})$ as a bill for the charge of this call. When the C gets this bill, C verifies the signature. If it is correct, C has to pay this call. For recognition of the caller, C has to search the records of calls. The charge of this call will appear on the caller ID_a 's monthly credit card statements.

Since in telephone systems, we cannot guarantee the caller is in a secure environment. It is undesirable for a cardholder to sign a payment directly on the telephone with his/her private signing key. However, he/she can trust the CCAC to be his/her agent of signing. Note that for anonymity the telephone will not send the credit card number ID_a and nonce n_1 to the telephone network system. We use challenge-response authentication card to prevent the replay attack and ensure the freshness of the calling request. A two-way challenge-response authentication protocol needs at least three steps. In our system, steps (1, 4, 5) is for the mutual authentication of the caller and the telephone network system; and steps (2, 3, 6) is for the mutual authentication of the telephone network system and the credit card authentication center. In the authentication process, the CCAC is trusted to issue the evidences of charges periodically in Steps (7, 8, 9, 10, 11).

There are four kinds of assailant in the system: outsiders, the caller, the CCAC and the telephone company. Anyone, who wants to make a toll-free call, he/she should generate a victim Alice's credit number ID_a and the response message $\{z\}_{K_a}$ to impersonate Alice. Since the computation of the authentication response message $\{z\}_{K_a}$ takes place internally within Alice's personal authentication card, Alice's secret authentication key K_a is never revealed by the authentication card. Therefore impersonating a victim to make a phone call is difficult even if he/she conspires with the telephone company.

In the payment system, the CCAC must be trustful and impartial. If a caller conspires with the credit card authentication center C , the caller can impersonate a victim and cheat the telephone network system N . In this way, the telephone company will believe a forged evidence and bill the victim. Consequently, the CCAC can collect the payment from a victim's account. The fraud hurts customers' interest. Therefore, the CCAC must be impartial and trustful. Furthermore, since the telephone company does not have the credit card authentication center C 's secret key S_C , it cannot produce a forged evidence.

In addition to the public switched telephone networks, this billing scheme can be also applied to mobile telecommunication systems, such as GSM. It is essential to the convenience of calling. No matter where a caller is, he can borrow a handset nearby to make a phone call. Owner of the handset will not be responsible for the charge of this call. The expense of calls will be charged to the caller's credit card account.

4 Internet Telephone Payment Diagram

In the Internet, the Internet telephone also face the same problem. Internet telephony uses the Internet infrastructure as a telephone network to stream packet real-time A/V between endpoints [11]. If a user wants to call regular phones, he needs to connect to a phone gateway. The telephone Internet service provider may offer services to either improve the quality of the A/V connections, and/or provide gateways to the switched telephone network (to basically integrate Internet telephony into today's fabric). It is anticipated that these services might be "for a fee". IDT has announced a similar service that will allow Internet phone users to make calls into major US cities for ten cents per minute. Like SET, the "Merchant" is an Internet Telephone Service Providers. The "Cardholder" would like to pay for services with credit cards. The fundamental model in SET is that if the cardholder and merchant agree on an order and prices, SET provides for the payment of the order, and then the merchant delivers the order [6]. SET cannot be used to collect the fee directly, since the cost of calls will not be known until cardholders complete their calls. A simply Internet Phone payment diagram is shown in Figure 5.

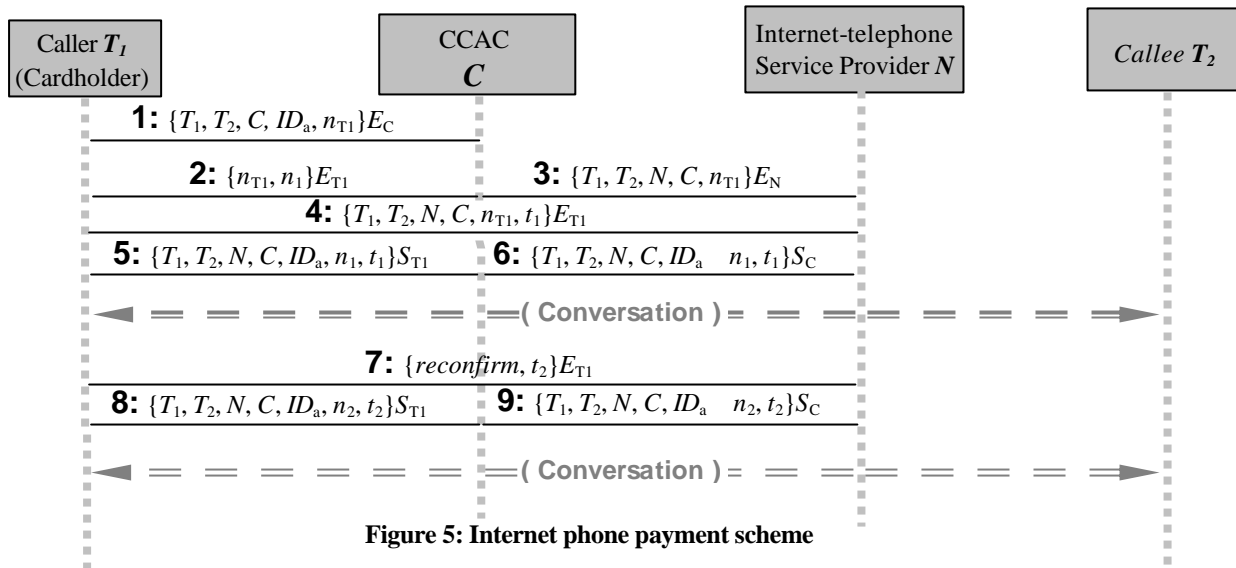


Figure 5: Internet phone payment scheme

In the Internet, cardholders can communicate with their CCAC directly. In our Internet phone payment scheme, not only the Internet telephone service provider has the evidences of calls from the CCAC (see the 6th or 9th message in Figure 5), but also the CCAC have the evidences of calls from cardholders (see the 5th or 8th message in Figure 5). Therefore, the need of trustiness of the CCAC decreases. In addition to this advantage, the caller need not remember the address of the Internet telephone service provider, since the card authentication center will choose the best service provider. Note that, in the scheme, n_{T1} is a random number generated by T_1 and is used to verify whether the message 4 comes from the legal Internet telephone service provider chosen by CCAC. By this way, no service provider can cheat T_1 into believing that the provider is authorized by CCAC unless CCAC give him the secret n_{T1} .

5 Conclusions

There are different kinds of service providers. For example, Internet telephone service providers allow people to use a computer to make phone calls. The personal communication service provider let people use his/her handset to get any information from anywhere and communicate with anyone at anytime. Since the credit card does not have physical mechanisms limitation, everyone can register more than one credit card number. The use of credit card to pay the charge of services is very convenient. In this paper, we propose a secure payment scheme for public switched telephone networks with which the expense of calls will be charged from the cardholder's account. This protocol is also suitable for mobile telecommunication networks, such as GSM. Furthermore, we design an Internet phone payment scheme to integrate

Internet telephony with today's telephone systems, where people can use his/her computer to call someone who has an ordinary telephone.

Reference

- [1] Beller, "Privacy and Authentication on a Portable Communications System", IEEE Journal on Selected Areas in Communications, vol. 11, no. 6, August 1993.
- [2] V. Bharghavan, "Secure Wireless LANs", ACM, pp.10-17, 1994.
- [3] CitiBank, "Masterphone Service", (<http://www.citibank.com/argentina/e/gc/arcpdbaa.htm>), 1996.
- [4] Chenturvasan Duraiappan and Yuliang Zheng, "Enhancing Security in GSM", Proceedings of International Computer Symposium, pp.297-302, 1994.
- [5] Hongkong Telecom, "International Calls", (<http://hkt.net/international.htm>), 1996.
- [6] Internet Bank of DISCS, "Electronic Commerce", (<http://137.132.88.57/ibank/chap2.htm>), 1996.
- [7] Refik Molva, Didier Sarmfat and Gene Tsudik, "Authentication of Mobile Users", IEEE Network, pp.26-34, March/April 1994.
- [8] Yi Mu and Vijay Varadharajan, "On the Design of Security Protocols for Mobile Communications", 1996.

- [9] NetPartners, "CRYPTO Card", (<http://www.netpart.com/crypto/tokens.html>), 1996.
- [10] Moe Rahnema, "Overview of the GSM System and Protocol Architecture", IEEE Communications Magazine, pp.92-100, April 1993.
- [11] Kenvin M. Savetz and Andrew Sears, "FAQ: How can I use the Internet as a telephone ?", ver. 0.5, July 25 1996.
- [12] Bruce Schneier, "Applied Cryptography: protocols, algorithms, and source code in C", 2nd, pp.47-74, 1996.
- [13] M. Tatebayashi, N. Matsuzaki and D.B. Newman, "Key Distribution Protocol for Digital Mobil Communication System", Advances in Cryptology - Crypto' 89 Proceedings, pp.324-334, 1990.
- [14] Vijay Varadharajan and Yi Mu, "Design of Secure End-to-End Protocols for Mobile Systems", Wireless' 96.
- [15] Visa and MasterCard, "Secure Electronic Transaction (SET) Specification, Book 1: Business Description", June 17 1996.