Card Secure Code for Preventing Fraudulent Use of Credit Cards Online

Kuen-Liang Sue and Chien-Lin Juan
Department of Information Management, National Central University
Jhongli City, Taoyuan County, Taiwan
{klsue@mgt.ncu.edu.tw, 93423006@cc.ncu.edu.tw}

Abstract-*The online credit card payment generally prevails over the Internet, but actually it has some serious faults. For this reason, we provide two new mechanisms for safe use of credit card online. This research applies the personal identification number and cryptography to eliminate malicious stores and people. Because the solution in this paper is based on the frame of existing e-commerce payment systems, we need not change hardware and software substantially and the implementation is inexpensive when enhancing safety of the electronic transaction.*

Keywords: Credit card, e-commerce, electronic transaction.

1. Introduction

The issues of secure online transaction in e-commerce are widely emphasized; however, people pay much attention to protect data transmission but neglect the procedural drawbacks in the electronic transaction systems.

There are two secure problems in using credit card online: First, the malicious or false stores may overrun readily the Internet since the fake ATM which is high technical entry threshold appears in the real world. Second, gathering card information is not difficult, so people who steal the credit card information can get a great deal of service and goods by shopping violently over the Internet. Neither merchants nor consumers are fully authenticated [1].

When a consumer pays with credit card in a physical store, the card information through merchants' Point of Sale (POS) is carried to the bank that verifies cards. Nevertheless, what you need to do in online payment is input credit card number and expiration date with keyboard or even voice on telephone. Once someone lets out our credit card receipts, a party having a mind to do something illegal will use our credit card accounts and the card holders know nothing about that until they receive bill at the end of a month.

According to the above-mentioned, the existing electronic transaction security is in need of improvement. It can be observed that the common process of online credit card payment shown in Figure 1.

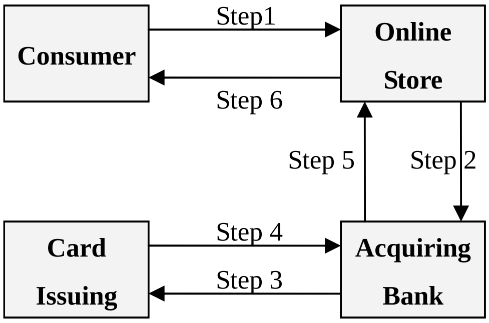

Figure 1. Common procedures of existing online credit card payment

The online transaction steps shown in Figure 1 are explained as follows:

Step 1. A consumer decides to buy and pay with credit card. The transaction data and credit card information are conveyed to the online store.
Step 2. The store transmits the credit card data immediately to its acquiring bank.
Step 3. The acquiring bank passes on the data that store have transmitted to the card issuing bank.
Step 4. The card issuing bank verifies the data, and then gives an authorization response to the acquiring bank.
Step 5. The authorization response forwarded by the acquiring bank is transmitted to the online store.
Step 6. The consumer gets the authorization response and ends the transaction.

Unfortunately, it can be observed in the existing process that anyone who obtains the card number and expiration date is able to shop on the Internet with others' credit card. Hence this is an obvious vulnerability in the current e-commerce payment.

The rest of this paper is organized as follows. Section 2 gives a brief description of some related works in electronic payments. In Section 3, we describe our solution, two schemes of Card Secure Code. The discussion and evaluation of our proposal is presented in Section 4, followed by the conclusion in Section 5.

2. Related Works

Generally speaking, e-commerce mechanism protects the transmission of credit card data and Secure Socket Layer (SSL) is one of the most common methods. Meanwhile, the launch of Secure Electronic Transactions (SET) payment also tries to enhance the transaction security [1]. However, they have their respective restrictions in operation.

The SSL connection only promises the connection security between users and remote transaction servers. Fraudulent use still happens because credit card number and expiration date may be collected by malicious parties yet.

Although SET is designed to avoid electronic transaction data to be let out, it progress complicated procedures as applying the digital signature technologies and authorization of Certification Authority (CA). Meanwhile, all transaction parties must have SET standard software. Hence it is not universal for its complex way.

Encryption methods cannot be neglected when we refer to transaction security. Among them, RSA technology is the most essential in the paper. Three American scholars Rivest, Shamir and Adleman from MIT, brought up a public-key cryptography system in 1978, hence the acronym RSA is from the first letters of their last names. RSA algorithm is an asymmetric cryptography, which uses two prime numbers to do duty as encryption and decryption keys. RSA has been proved that it is a very secure cryptography. The pair keys are called public key and private key with the length of 40 to 1024 bits.

Having the protection against online payment flaws in mind, scholars M. Bellare and so on in year 2000 proposed three schemes in the *i*KP secure electronic payment system [2]. The research makes use of cryptography, digital signature and secure personal storage device. For the space restriction we do not describe in detail. All three schemes tend to be complicated and every party must have the same standard infrastructure with the result that it may have similar promoting obstruction like SET.

Besides, America Express and Visa, each issues a kind of limited-use credit card to eliminate some disadvantages in electronic payments. However, a consumer must surf the card issuing bank website to get a code every time when they would like to shop online. The above way is too inconvenient, so Rubin and Wright [3] in AT&T labs proposed an off-line model to generate limited-use and variable credit card numbers for one time use or limited use. The generation of limited-use 16-digit card numbers is based on the account number and some transaction restrictions such amount, merchandize categories and expected sopping date by adopting a symmetry key.

By contrast with American Express' and Visa's on-line way, Rubin and Wright improve the way, but the off-line software of token generation is still probably cracked. Online consumers must decide transaction restrictions in advance so that it is quite inconvenient. Moreover, conditional restrictions used for encryption may be the same or exposed. Our research refers to Rubin and Wright's paper and then we bring up a solution expecting to have a better performance and higher security.

3. The Card Secure Code

The physical credit card payment can confirm that shopping is done by a card holder himself. On the contrary, the online credit card may be used by anyone who knows the card number and expiration date.

To solve problems of credit card security, this paper proposes Card Secure Code, CSC, the mechanism of two alternative schemes. For succinctness of the following discussion, we will use symbols in Table 1 to describe the content.

Table 1. Illustration of symbols used in the paper

Symbol	Illustration
Cnsmr	Consumer
Str	Online Store
ABnk	Acquiring Bank
CIBnk	Card Issuing Bank
CCN	Credit Card Number
EDt	Expiration Date
PIN	Personal Identification Number
TSN	Transaction Serial Number
PInfo	Purchase Information
Data	Transaction Data
RNbr	Random Number
AR	Authorization Response
K_{pb}	Public Key
K_{prv}	Private Key
SK	Symmetric Key

The symbol "Data" in Table 1 indicates merchant terminal number, merchant invoice number, transaction code, transaction request date/time, amount, etc. that the credit card payment systems should deliver.

3.1. Proposal for CSC Scheme 1

In Scheme 1, card issuing banks should make every credit card own an exclusive online transaction personal identification number. Encrypting a consumer's PIN as well as the random number [4, 5] that the online store gives can produce a card secure code, which confronts malicious Web users. Figure 2 shows the process of this scheme.

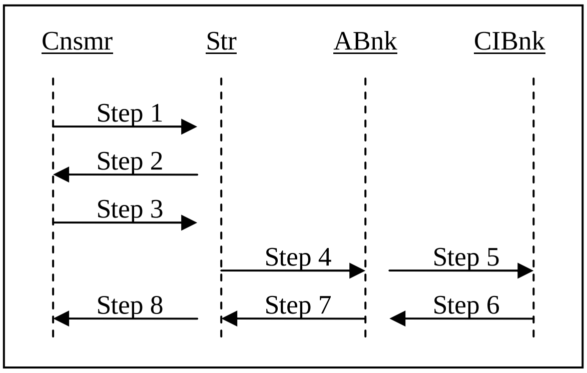

Figure 2. Transaction procedures of CSC Scheme 1

The steps corresponding with Figure 2 are expatiated as follows:

Step 1. A consumer decides to buy and pay with credit card. His or her transaction data and credit card information are conveyed to the online store.

Step 2. The online store transmits the random number and transaction serial number which are encrypted by a symmetric key to its consumer.

Step 3. The consumer uses the card issuing bank's public key to encrypt the PIN and random number so that derives a card secure code. Then the secure code with transaction serial number passes to the store.

Step 4. The online store gets together transaction data immediately. It makes transaction serial number and random number in symmetric encryption. Afterward the encrypted transaction serial number and random number along with credit card number, expiration date, transaction data and consumer's encrypted secure code transmit to the bank for asking an authorization response.

Step 5. The acquiring bank passes on the data that store have transmitted to the card issuing bank.

Step 6. The card issuing bank verifies the data, and then gives an authorization response to the acquiring bank.

Step 7. The authorization response forwarded by the acquiring bank is transmitted to the online store.

Step 8. The consumer gets the authorization response online and ends this transaction.

The transaction procedures of Scheme 1 shown in Figure 2 is similar to that of Figure 1, but between step 2 and step 4, we apply card secure code which comes from a PIN and random number to verify the credit card. At step 2, the store encrypts transaction and random number and passes them to the consumer. The random number is used for producing card secure code when it encrypts with user's PIN. We express the above steps in the following notation:

Step 1. CCN, EDt, PInfo
Step 2. SK[TSN, RNbr]
Step 3. TSN, K_{pb}[PIN, RNbr]
Step 4. CCN, EDt, SK[TSN, RNbr], Data, K_{pb}[PIN, RNbr]
Step 5. CCN, EDt, SK[TSN, RNbr], Data, K_{pb}[PIN, RNbr]
Step 6 to step 8. TSN, AR

It is worthy to notice that the online store passes RNbr to the card issuing bank in step 4 and step 5. So the card issuing bank is capable of verifying the secure code which contains PIN and RNbr between step 5 and step 6. Our so-called K_{pb} and K_{prv} indicate that the RSA asymmetric keys. The public key is used as an encryption key while the private key is used as an decryption key.

CSC Scheme 1 can avoid illegal individuals to trade over the Internet by collecting others' card numbers and expiration dates. It only has two more steps than the way of conventional online credit card. However, the random numbers are controlled by the stores, so the consumers' PINs may be known by stores if they use spoofing [6] or convey null or arranged RNbr values. Therefore, we have the alternative of Scheme 2.

3.2. Proposal for CSC Scheme 2

In Scheme 2 described in this paragraph, the random number should be sent out by the acquiring bank. The secure code is encrypted by the public key, and card issuing bank uses its private key to know whether the PIN and random number are valid. Scheme 2 can prevent from stores' replays.

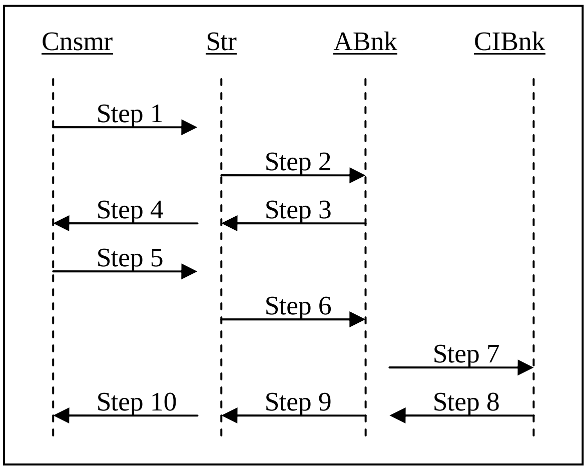

Figure 3. Transaction procedures of CSC Scheme 2

The steps corresponding with Figure 3 are expatiated as follows:

Step 1. A consumer decides to buy and pay with credit card. The transaction and credit card data are conveyed to the online store.

Step 2. The online store immediately transmits the credit card number, expiration date and transaction serial number to its acquiring bank.

Step 3. The acquiring bank passes on the encrypted random number with the same transaction serial number to the store.

Step 4. The store forwards the encrypted random number with the same transaction serial number to the consumer.

Step 5. The consumer uses the card issuing bank's public key to encrypt the PIN and random number so that gets a card secure code. Then the secure code with transaction serial number passes to the store.

Step 6. The store forwards the consumer's card secure code and transaction data along with the transaction serial number and random number to the acquiring bank.

Step 7. The acquiring bank arranges card number and expiration date in step 2 as well as secure code, transition data, transaction serial number and random number in step 6. All of them send to card issuing bank for asking an authorization response.

The other step 8 to step 10 are the same as step 6 to step 8 in Scheme 1. Among the foregoing, those steps can be described as the following notation:

Step 1. CCN, EDt, PInfo
Step 2. CCN, EDt, TSN
Step 3. SK[TSN, RNbr]
Step 4. SK[TSN, RNbr]
Step 5. TSN, K_{pb}[PIN, RNbr]
Step 6. SK[TSN, RNbr], Data, K_{pb}[PIN, RNbr]
Step 7. CCN, EDt, SK[TSN, RNbr], Data, K_{pb}[PIN, RNbr]

There is no credit card number in it between step 3 and step 4, so we adopt the symmetric encryption in order to consume less time. Every time when transacting payment, the acquiring bank issues the random number. After the consumer receives the random number, he or she uses the public key to encrypt the random number and fixed PIN, i.e. K_{pb}[PIN, RNbr]. After step 7, the bank encrypts the card secure code, i.e. K_{pb}[PIN, RNbr], with its private key and then gets a number N:

$$\begin{aligned} N &= K_{prv}[\ K_{pb}[\text{PIN, RNbr}]] \\ &= \text{PIN, RNbr} \end{aligned}$$

It can be audited if N is equal to consumer's personal identification number plus random number. If they are the same, the bank recognizes the transaction, but otherwise, it refuses this payment and informs the store. Owing to the random numbers that are produced by banks, the unworthy merchants and criminal gangs have no way out shopping online illegally.

4. Discussion

Our Card Secure Code in this paper solves a good deal of problems that exist in the Internet transaction security. We find that they are able to answer to expectations of secure electronic payment [7, 8]. We arrange the discussion about our proposal in this section.

4.1. Evaluation of CSC Scheme 1

4.1.1. Identity confirmation. Between step 2 and step 3 in Scheme 1. We exploit the random number as well as the PIN to confirm a user's identity. That is similar to the physical signature which indicates a card holder's free will and avoids an impostor as much as possible.

4.1.2. Uniqueness of data and security of transmission. The advantage of applying the respective PIN and unique random number in Scheme 1 is that it improves the traditional data item. Because using only credit card number and expiration date is dangerous since they are easy to be collected. Also, PINs do not appear in the plain text between customers and stores, so customers' data as well as PINs are under protection.

4.1.3. Low switching cost and easy to use. This paper's proposal keeps the original framework of credit card payment so it fits consumers' experiences. As the expected system constructs according to the present framework, switching cost is low and system is easy to implement. It can even apply for other electronic payments and telephone calling.

4.1.4. Protecting stores against deliberate denials. In fact, protecting merchants from been deceived by criminal gangs is indispensable. Consumers are not apt to deny transaction content owing to the use of card holders' PIN and given random number. The conventional ways almost do not protect online stores if consumers deny recognizing the trade.

4.2. Evaluation of CSC Scheme 2

The system procedures in Scheme 2 are similar to those of Scheme 1. Yet, it is more complicated and has a little higher cost than the Scheme 1. In the level of security, it has all characteristics of Scheme 1 and still owns other advantages. We evaluate Card Secure Code Scheme 2 in the following paragraph.

4.2.1. Difficult to crack. Besides applying RSA cryptography, the random numbers in Scheme 2 are produced by the acquiring bank. Therefore we avoid someone who collects card information to use fraudulently. That one would like to crack the ciphertext of security code is very difficult and the claim can be supported in the example of RSA-129.

4.2.2. Acceptable complexity. Because RSA public key count at the client side, users' computing devices will have lower load. Moreover, only card issuing bank is able to unlock the ciphertext avoiding data let out. Encryption needs just less computing capability. The encryption with public key is not a severe and complicated security mechanism for personal devices. In generally, conventional digital signature applies private key as encryption and public key as decryption. It is different from this paper. Most importantly, besides using hash function, bank should have all clients' public key under digital signature. It consumes more time than that of our research.

4.2.3. Protecting banks with raising transaction trust. After the card issuing bank decrypts the ciphertext, it can check if N equals the random number given by the acquiring bank and user's fixed PIN. Since the random numbers in Scheme 2 are not produced by online stores, we may prevent malicious stores' tricks and protect banks by enhancing online transaction trust.

5. Conclusion

This paper proposes a simply equipped framework and achieves the security principal point which we have just discussed and estimated. Most essentially, it is fit for past trade habits of online users. Scheme 1 makes it invalid to gather credit card information, so a lawless party knowing our card information cannot shop unceasingly over the Internet. But Scheme 1 may not prevent malicious stores from interpenetrating to know consumers' PIN absolutely; therefore, we have the alternative of Scheme 2.

In the past, to avoid fraudulent use, some online stores would ask consumers to facsimile their credit card copies and signatures to the store websites. Owing to the inconvenient the way is not in common use. Now we propose that exploiting PIN which acts as physical signature comes to identity confirmation in both secure and fast way.

CSC Scheme 2 contributes to prevent fake consumption records coming from fake and malicious stores because acquiring banks control the random numbers. In the same way, collecting others' credit card information cannot pretend to shop online. It costs two steps more to contrast with Scheme 1 and consuming time a little longer. However, since our proposal only uses PIN as well as public and private keys which exchange their role, it is still simple than the digital signature.

This research focuses on network security generally, and connecting time may a bit longer than today's infrastructure as a result of applying Card Secure Code. However, our schemes, most importantly, need not renovate hardware and software substantially. If you stress transaction speed, CSC Scheme 1 is a good alternative; if you highlight the security, CSC Scheme 2 is the top priority. Applying the two schemes, their switching costs are inexpensive and both of them do enhance the security in the online transaction.

References

[1] K.C. Laudon and C. G. Traver, *E-Commerce: Business, Technology, Society, Second Edition*, Addison Wesley, 2003.

[2] M. Bellare et al., "Design, implementation, and deployment of the *i*KP secure electronic payment system," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, April, 2000.

[3] A. D. Rubin and R. N. Wright, "Off-line generation of limited-use credit card numbers," *Pre-Proceedings of the Fifth International Conference on Financial Cryptography*, pp. 165-175, 2001.

[4] K. Y. Lam, S. L. Chung, M. Gu, and J. G. Sun, "Lightweight security for mobile commerce transactions," *Computer Communications*, vol. 26, pp. 2052-2060, December, 2003.

[5] A. Singh and A. Santos, "Grammar based off line generation of disposable credit card numbers," *17 ACM Symposium on Applied Computing*, 2002.

[6] E. W. Felten et al., "Web spoofing: an Internet con game," *Proceedings 20th National Information Systems Security Conference*, 1997.

[7] L. C. Ferreira and R. Dahab, "A scheme for analyzing electronic payment systems," *Proceedings of the 14th Annual Computer Security Applications Conference*, December, 1998.

[8] S. P. Shieh and C. T. Lin, "An efficient and secure credit-card based billing schemes for telephone services," *International Conference on Mobile Computing*, March, 1999.