A Purchase Protocol with Live Cardholder Authentication for Online Credit Card Payment

Hannan Xiao, Bruce Christianson
School of Computer Science
University of Hertfordshire
College Lane, Hatfield, AL10 9AB, UK
h.xiao, b.christianson@herts.ac.uk

Ying Zhang
Department of Engineering
University of Cambridge
Cambridge, CB3 0FA, UK
yz282@cam.ac.uk

Abstract

While online shopping are becoming more accepted by people in modern life, cardholders are more concerned about card fraud and the lack of cardholder authentication in the current online credit card payment. This paper proposes a purchase protocol with live cardholder authentication for online transaction which combines telephone banking and online banking together. The order information and payment information are sent though the Internet and encrypted by asymmetric key encryption. The cardholder is authenticated by the card issuing bank ringing back to the customer's phone number and the cardholder inputting the secure PIN and the amount to pay. The live cardholder authentication makes the cardholder feel securer and card fraud difficult. Furthermore, the protocol does not require the cardholder to obtain a public key certificate or install additional software for the online transaction.

Keywords— *online credit card payment, card fraud, authentication*

1. Introduction

When a cardholder presents his credit card at a retailer shop, the card is read by a card reader and the cardholder is required to input a PIN. After the PIN is verified, the transaction is approved to go ahead. The possession of the four-digit PIN is used to authenticate the cardholder. Before the use of Chip and PIN, cardholder signature was used in the past but is replaced by Chip and PIN because it is easier to forge a signature than guessing a PIN.

The process is different when a credit card is used online. Most online shopping sites only require the input of card details including the three digits at the back of the card. Another person other than the cardholder may get hold of the information and use it shopping online. The lack of cardholder authentication in the current online payment has resulted in online shopping fraud being one of the major card fraud. Cardholders are becoming more concerned about releasing their card information. Secure protocols are needed to enhance the security of online shopping.

Ideally, a secure protocol for online transaction should provide mutual authentication of a customer and a merchant; that is to authenticate that a cardholder is a legitimate user of a payment card account, and that a merchant can accept a payment card transactions. In addition, the payment information should be always confidential and data integrity should be ensured. Apart from the requirements in the aspects of security, an online credit card payment system should also be easy to deploy in real world without burdening the card issuer, the merchant and the cardholder too much. The system must be easy to use for the cardholder who chooses online shopping initially for the benefits of its convenience. The protocol should also let the cardholder feel secure.

Many solutions have been proposed for thwarting credit card fraud [1, 2, 3, 4, 5, 6, 7]. Among them [2, 3, 5], the common way of authenticating a cardholder is to use digital signature based on the public key infrastructure (PKI). This requires the cardholder to have a public key certificate before commencing an online purchase, which makes the task at cardholder side impractical and inconvenient. As a result, the cardholder authentication is omitted in some of the schemes [3, 4].

This paper is motivated by providing a purchase protocol with live cardholder authentication in online purchase procedure similar to the Chip and PIN used at the onsite shopping. It combines telephone banking and online banking together. The order information and payment information are sent though the Internet and encrypted using asymmetric key encryption. The cardholder authentication is done through the public switched telephone network (PSTN) by the card issuing bank ringing back to the customer's contact

978-0-7695-3324-7/08 $25.00 © 2008 IEEE
DOI 10.1109/IAS.2008.44

IEEE computer society

phone number and requesting the input of the secure PIN and the amount to pay.

The rest of this paper is organized as follows. Section discusses the related work in online payment schemes. Section 3 presents the protocol including its assumptions, notations and major phases. Section 4 evaluates the protocol and finally section 4 summarizes the paper.

2. Related Work

The Secure Electronic Transaction (SET) protocol [5] was devised by Visa and Mastercard; it achieves high security by five sub-protocols together: cardholder registration, merchant registration, purchase request, payment authorization, and payment capture. SET requires all participation entities including the cardholder to have a public key certificate before a purchase. Because of the complicity and high overhead of the protocol and its dependency on the PKI, SET has not been implemented in the industry after its design in 1997.

Different from the SET, credit card payment using Secure Socket Layer (SSL) [3] is widely accepted in e-business. SSL provides data confidentiality by using symmetric key encryption which is faster than the public key encryption, and merchant authentication by digital signature. The authentication of the cardholder is seldom deployed since a cardholder usually does not have a public key certificate. Nevertheless, using symmetric key encryption enables the merchant to access the payment details of the cardholder and in many cases store such information in its database. Once the database is tampered, the lost data may cause more cases of card fraud.

Recently, PayPal [6] has been popular among cardholders because it does not require the input of card details online. Instead, a valid email address is considered as a PayPal account identifier and used for online payment. However, PayPal has poor authentication during its registration phase phase through which the payment information such as card details or account number and sort code are associated with a valid email address. Once the association is created, using the valid email address and the correct password will make the bank account or credit card to pay for a purchase. An attacker Eve may easily register by Bob's bank account details and her email address, and get Bob to pay for her shoppings later on.

Another effort to avoid repetitively use of card details is to use one-time credit card transaction number (CCT) [4]. A CTT is used only once, thereby whether the CCT is stored by the merchant or stolen by an attacker does not matter after its use. The concern is that CCTs do not provide authentication of the cardholder. The current CCT in use is stored on the credit card, and once the card is inserted into a card reader, a new CCT will be calculated based on a secret stored on the card and known to the issuing bank. The issuing bank can verify which card is being used but not who is using the card.

3. The Purchase Protocol with Live Cardholder Authentication

3.1. Assumptions

It is assumed that a cardholder trusts the branded bank that issues him a credit card. He has to if he is willing to deposit his money in the bank. When obtaining a credit card the cardholder has given his personal information to the bank such as identity, date of birth, addresses, contact email address, and contact telephone number(s). The financial and personal information is kept safely by the bank. The bank gives the customer a Personal Information Number (PIN) to use. Of course, initially, the bank has authenticated the cardholder by his identification document such as driving licence, passport and billing address.

It is also assumed that a PKI exists to facilitate the protocol. All the business entities including merchants, payment gateways, card issuing banks, and merchant acquiring banks have registered with some Certificate Authority (CA) and been issued public key certificates. The CA or a cluster of CAs are trusted by all the business entities. The honesty of a merchant should have been checked during the registration procedure (which is actually a bit risky). A cautious customer always checks a merchant's recent credit before deciding to buy a good from the merchant online. These entities should have at least two private and public key pairs; one used for encryption and the other for signature. The business entities know the public keys of one another.

It is not assumed that a cardholder has obtained a public key certificate before purchasing online because it is impractical to ask all the cardholders to do so. However, a cardholder trusts the CAs that issue the public key certificates for the business entities. The cardholder does not have to know the public keys of the business entities.

3.2. The Purchase Protocol

Figure 1 plots the sequence of the purchase protocol which includes five phases:

1. Purchase request: the cardholder initializes a purchase request and sends it to the merchant. This is done in step S.1.

2. Authorization and authentication request: the merchant processes the purchase request and sends an authorization and authentication request to the payment gateway. This is done in step S.2.

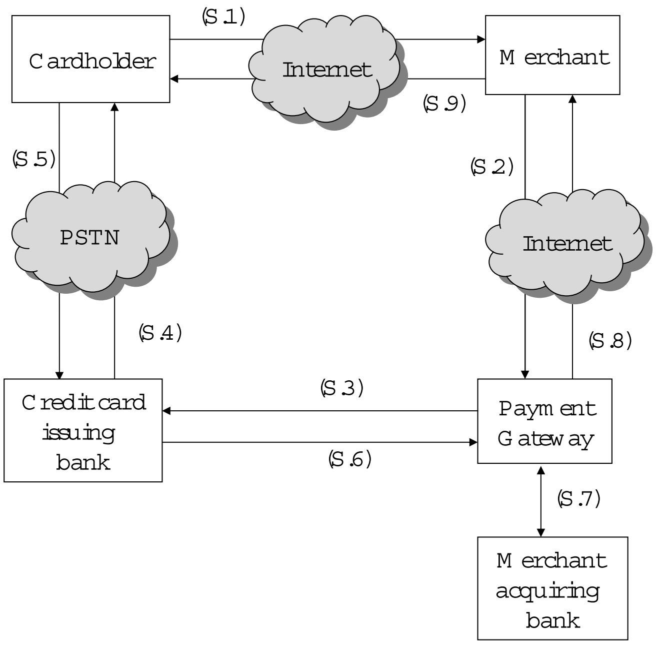

Figure 1. The purchase protocol with live authentication

3. Authorization and authentication: the payment gateway processes the authorization and authentication request, passes it to the card issuing bank who then authenticates the cardholder through the PSTN. This phase includes steps S.3, S.4, and S.5.

4. Authorization and authentication response: The card issuing bank sends an authorization and authentication response back to the payment gateway who then instructs the merchant acquiring bank and the merchant. This phase includes steps S.6, S.7 and S.8.

5. Purchase response: The merchant sends an purchase response back to the cardholder. This is done in step S.9.

The above phases are explained in details below. The notations in use are listed in Table 1.

Table 1. Notations

C	Cardholder
M	Merchant
P	Payment gateway
$CardB$	Card issuing bank
$pubEK$	Encryption key of a private public key pair
$priSK$	Signing key of a private public key pair
XID	Global unique transaction ID
$OrderInfo$	Order information
$PayInfo$	Payment information
$PurAmt$	Purchase amount
$OIEncrypt$	Encrypted order details
$PIEncrypt$	Encrypted payment details
$CardSign$	Cardholder signatures
$auCode$	Authorization and authentication code

Phase 1: Purchase Request.

(S.1) The cardholder browsers the merchant's shopping site and finds the goods that he wants to buy. When the payment information pops out, he fills in his credit card information. When the cardholder clicks the "submit" button, a Java applet is downloaded from the merchant's shopping site – we call it a payment applet. When the payment applet is downloaded to the cardholder site, it obtains from the merchant site the public keys of the payment gateway and the merchant, and a nounce that serves as a globally unique transaction identifier. The payment applet also generates an asymmetric key pair for the cardholder since it is assumed that the cardholder may not have an issued certificate as the merchant and the payment gateway. The asymmetric key pair is used for providing the integrity of the order and payment information but not for authenticating the cardholder.

The payment applet sends the order and the payment information to the merchant's shopping site using dual encryption to ensure that the merchant can only read the order details but not the payment details.

$$C- > M : \text{OIEncrypt, PIEncrypt, CardSign} \tag{1}$$

where the payment applet has computed the following.

$$\begin{aligned}
&\text{OIEncrypt} = \\
&\qquad \text{Crypt}_{\text{pubEK}_M}(\text{XID, OrderInfo, pubSK}_C, \\
&\qquad\quad \text{Hash(XID, PayInfo, PurAmt))} && (2) \\
&\text{PIEncrypt} = \\
&\qquad \text{Crypt}_{\text{pubEK}_P}(\text{XID, PayInfo, PurAmt, pubSK}_C, \\
&\qquad\quad \text{Hash(XID, OrderInfo))} && (3) \\
&\text{CardSign} = \\
&\qquad \text{Sign}_{\text{priSK}_C}(\text{Hash(XID, OrderInfo),} \\
&\qquad\quad \text{Hash(XID, PayInfo, PurAmt))} && (4)
\end{aligned}$$

The encrypted order details are shown in (2). The payment applet first combines the globally unique transaction identifier, the payment information which includes the credit card number, expire date, cardholder name, etc, and the purchase amount that the cardholder needs to pay. It then calculates the hash of the combination, and concatenates the hash value with the transaction identifier, the order information that may include goods description, price, etc, and the verification key of the cardholder. The payment applet then encrypts the concatenation by the public key of the merchant's encryption key pair.

As shown in (3), the encrypted payment details are in a similar format as the encrypted order details. The payment applet combines the transaction identifier and the order information, and calculates the hash of the combination. The payment applet then concatenates the hash value with the transaction identifier, the payment information, the purchase amount that the cardholder needs to pay, and the verification key of the cardholder. Similarly, the payment applet encrypts everything by the public key of the payment gateway's encryption key pair.

(4) expresses the cardholder signature on the hash values of the order details and the payment details. The hash values are duplicated in the signature, the encrypted order details, and the encrypted payment details, so that various parties can verify the integrity of the information. By this way, although the payment details are kept secret to the merchant, and the payment gateway merchant does not know what the pay is for, either of them is able to verify the integrity of the piece of information that is only known to the other.

Phase 2: Authorization and Authentication Request.

(S.2) After receiving the purchase request, the merchant decrypts the encrypted order details, and verifies the integrity of the order details by calculating the hash value of the order details and then comparing the value with the one contained in the cardholder's signature. The merchant also verifies the hash value of the payment details by comparing the two values of the payment details in the encrypted order details and the cardholder's signature.

If the verifications are successful, the merchant combines the transaction identity, the encrypted payment details which it cannot read, the cardholder's signature, the hash value of the order details, and the verification key of the cardholder. The merchant signs everything, encrypts its signature using the payment gateway's public key, and sends the encrypted message to the payment gateway (5).

$$\begin{aligned}
&M- > P : \\
&\qquad \text{Crypt}_{\text{pubEK}_P}(\text{Sign}_{\text{priSK}_M}(\text{XID, PIEncrypt,} \\
&\qquad\quad \text{CardSign, Hash(XID, OrderInfo), pubSK}_C))
\end{aligned} \tag{5}$$

Phase 3: Authorization and Authentication

(S.3) The payment gateway decrypts the encrypted payment details by using its own private key and the public key of the merchant. It calculates the hash value of the payment details and compares it with the one supplied in the cardholder's signature. The payment gateway also verifies the integrity of the order details by comparing the hash value from the decrypted message and the one contained in the cardholder's signature. Successful verifications show that the cardholder and the merchant agree on the transaction.

The payment gateway then combines the global transaction identifier, the payment information and the purchase amount. It calculates the hash of the combinations, and signs the hash value. The payment gateway concatenates the combination and the signature, and encrypts the concatenation by the credit card issuing bank's public key. The encrypted message is forwarded to the issuing bank (6).

$$\begin{aligned}
&P- > CardB : \\
&\qquad \text{Crypt}_{\text{pubEK}_{CardB}}(\text{XID, PayInfo, PurAmt,} \\
&\qquad\quad \text{Sign}_{\text{priSK}_P}(\text{Hash(XID, PayInfo, PurAmt)))}
\end{aligned} \tag{6}$$

(S.4) After receiving the authorization and authentication request, the card issuing bank checks the payment details of the cardholder in its database and finds the contact number of the cardholder. The bank rings back to the cardholder's prime phone number which is a land line or a mobile phone, and asks the cardholder to confrim the transaction by inputting the PIN of the credit card and the purchase amount of the transaction.

(S.5) The cardholder inputs the PIN through the number pad on his phone as he does on a card reader in a retail shopping site, press #, and then inputs the purchase amount omitting the numbers after the decimal point, and press # again to end the confirmation. Data is sent through PSTN provided by the telephone service provider.

The protocol authenticates the cardholder by four conditions: the correct credit card details, use of the right telephone, correct PIN, and correct purchase amount. Missing any of these conditions will make the transaction unsuccessful. The input of the correct purchase amount allows the cardholder to tell for which purchase this confirmation is in case that the cardholder has used the same card twice in a short time.

Phase 4: Authorization and Authentication Response.

(S.6) The issuing bank sends an authorization and authentication code back to the payment gateway if it receives the right PIN and right purchase amount back though the PSTN. If the PIN is wrong, a response code is sent back and used to denote any error that might have had occurred during the verification or transaction process (7).

$$\begin{aligned} &CardB->P: \\ &\quad \text{Crypt}_{\text{pubEK}_P}(\text{XID, PurAmt, auCode,} \\ &\qquad \text{Sign}_{\text{priSK}_{CardB}}(\text{hash(XID, PurAmt, auCode)))} \end{aligned} \tag{7}$$

(S.7) The payment gateway schedules debiting the cardholder's account and crediting the merchant's acquiring account.

(S.8) The payment gateways sends the authorization and authentication code to the merchant shopping site to inform the merchant to be ready to issue the goods (8).

$$\begin{aligned} &P->M: \\ &\quad \text{Crypt}_{\text{pubEK}_M}(\text{XID, PurAmt, auCode,} \\ &\qquad \text{Sign}_{\text{priSK}_P}(\text{hash(XID, PurAmt, auCode)))} \end{aligned} \tag{8}$$

Phase 5:Purchase Response.

(S.9) The merchants shopping site generates feedback based on the authorization / response code received by the payment gateway. Some of the codes may be interpreted as: "You card has been billed.","Insufficient funds." or "Incorrect PIN.".

4. Evaluation of the Protocol

4.1. Security

Confidentiality of the message is provided by asymmetric key encryption. The messages are always encrypted by the receiver's public key in its encryption key pair. This is based on the assumption that the business entities either know each other's public key at the moment of the transaction or can obtain the public key through other channels when necessary. The order details are just known to the cardholder and the merchant. More importantly, the payment details are known to the cardholder, the payment gateway and the card issuing bank only, making the merchant impossible to store the card information in its database. This avoids card frauds in case of an attack is mounted on the database.

Integrity of the order details and the payment details is assured by the payment applet at the cardholder side signing the hash values of the order details and the payment details. The merchant and the payment gateway verify both the hash values of the order details and payment details separately although either of them can only read the order details or the payment details alone. The verification key of the cardholder is encrypted and sent to the merchant and payment gateway. Integrity of the data exchanged between the payment gateway and the card issuing bank is provided by the signature on the hash value of the data.

Authentication of the cardholder is done through PSTN. The cardholder needs to pick up the phone call from the bank at the prime contact number that he has given to the bank initially or updated afterwards. He then keys in the correct PIN and the correct purchase amount omitting the numbers after the decimal point. If the phone number is a fixed line, it makes a card fraud difficult unless someone breaks into the house. Choosing a mobile phone number makes the online shopping mobile and more convenient, but it has the risk that the cardholder may lose his credit card and mobile phone together. In this case the authentication only lies in the confidentiality of the PIN. Authentication of the merchant is through its signature on the hash value of the message to be sent. This is the same for the payment gateway and the card issuing bank.

4.2. Usability

The protocol keeps the functions at the customer side as simple as possible. It does not require a cardholder to obtain a public key certificate or install any software for the purpose of online shopping. The cardholder should accept the PIN authentication process easily because it is similar to the process of onsite shopping. The live verification process also gives the cardholder a sense of security.

The deployment of the protocol requires a PKI for the business entities. It also requires the card issuing bank to call back at the cardholder's primary phone number stored in its database and verifies the PIN and purchase amount inputted by the cardholder. These functions are deployable at the bank side with reasonable cost.

4.3. Attack

To mount a card fraud attack in the protocol, an attacker must know the card details, the PIN, and the prime contact telephone number that the cardholder leaves at the bank. The attacker should also have control of the phone during a purchase. The attacker might get the payment details thorough packet intercepting or database stealing, he may even get the PIN through shoulder surfing when the cardholder inputs his PIN in a supermarket. The attacker then has to steal the cardholder's hand phone or break into the cardholder's house in order to validate the authentication and authorization, which a high technology attacker normally doesn't like to do. Alternatively the attacker may attempt the PSTN, but it is not easy attempting the PSTN thanks to its closed architecture. It is assumed that the calling back is done through the traditional PSTN but not voice over IP (VoP).

5. Summary

Current online credit card payment is not secure due to its lack of cardholder authentication. This paper proposes a purchase protocol with live authentication of cardholder for online credit card payment which combines telephone banking and online banking together. The protocol has five phases: (1) purchase request, (2) authorization and authentication request, (3) authorization and authentication, (4) authorization and authentication response, and (5) purchase response. The order information and payment information are sent though the Internet and encrypted by asymmetric key encryption. The protocol authenticates the cardholder by the card issuing bank ringing back to the customer's contact phone number and the cardholder inputting the secure PIN and the price to pay. The live authentication of cardholder makes a cardholder feel securer and card fraud difficult. Furthermore, the cardholder does not need to obtain a public key certificate or install additional software for the transaction.

References

[1] G. Bella, F. Massacci, and L. Paulson. Verifying the SET purchase protocols, 2001. Technical Report 524, Computer Laboratory, University of Cambridge, available from http://citeseer.ist.psu.edu/bella01verifying.html.

[2] G. Bella, F. Massacci, and L. Paulson. Verifying the SET registration protocols. *IEEE Journal of Selected Areas in Communications*, 21(1):77–87, 2003.

[3] A. O. Freier, P. L. Karlton, and P. C. Kocher. The SSL protocol version 3.0. Available from: http://wp.netscape.com/eng/ssl3/ssl-toc.html.

[4] Y. Li and X. Zhang. Securing credit card transactions with one-time payment scheme. *Electronic Commerce Research and Applications*, 4(4):413–426, 2005.

[5] MasterCard and VISA. SET secure electronic transaction specification. Available from: http://www.cl.cam.ac.uk/research/security/resources/SET/.

[6] PayPal. PayPal's privacy to fight identity fraud. Available from: https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/securitycenter/buy/Privacy-outside.

[7] H. C. Yu, K. H. Hsi, and P. J. Kuo. Electronic payment systems: an analysis and comparison of types. *Technology in Society*, 24(3):331–347, 2002.