A purchase protocol with multichannel authentication

A Purchase Protocol with Multichannel Authentication

Hannan Xiao[1], Bruce Christianson[1], and Ying Zhang[2]

[1]School of Computer Science, University of Hertfordshire
College Lane, Hatfield, AL10 9AB, UK
h.xiao, b.christianson@herts.ac.uk
[2]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 at the customer's phone number and the cardholder inputting the secure PIN and the amount to pay. The multichannel authentication makes the cardholder feel secure and card fraud difficult. Furthermore, the protocol does not require the cardholder to obtain public key certificates or install additional software for the online transaction.

Keywords: online credit card payment, card fraud, multichannel 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. 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 frauds. 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]. 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 at the customer's contact 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 2 discusses the related work in online payment schemes. Section 3 presents the protocol including its assumptions, notations and major phases. Section 4 analyzes the protocol from the view of security and usability, respectively. Finally section 5 summarizes the paper.

2. Related Work

2.1 Authentication in Credit Card Payment Schemes

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 public key certificates 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 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 could easily register by Bob's bank account details and her email address, and get Bob to pay for her shopping 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.

The proposed protocol in this paper is light-weighted, much less complex than SET, and has less computation overhead. This is because the protocol uses asymmetric key encryption only without the complexity of digital envelope which contains both asymmetric and symmetric key encryptions. Unlike SSL using fast symmetric encryption only, this protocol uses dual signature to ensure that the merchant does not get access to the user's account details.

2.2 Multichannel Authentication

As Wong and Stajano discussed in [7, 8] the idea of using multiple channels in security protocols has been existed long before we realized them. Protocol messages being transmitted through multiple communication channels of different security properties offers significant advantages for the protocol's security and usability. An early example of multiple channel protocol is in an ad hoc networking environment where a device (duckling) gets imprinted via physical contact before communicating with others via wireless channels [9].

Multichannels are also proposed to authenticating Internet users in web-based services especially electronic commerce services. Many patents are filed around the idea of using PSTN to authenticate users. In [10], an authentication server is connected to two networks and receives custom order information from one network and forwards the confirmation request to the other. In [11] a mobile phone or other communications terminal associated with a user is used. A vending node communicates with an authentication platform which either returns a telephone number to be displayed for the user to call or which calls the alleged user's phone or terminal for confirmation. Similar ideas are found in [12, 13, 14, 15, 16]. However, these patents do not specify an explicit protocol to use.

Cellular phone networks are chosen by commercial authentication service providers for Internet services such as Signify [17], Identrica [18], SaintLogin [19] and SecureCall [20] as an authentication channel besides the Internet because of cellular networks' popularity worldwide. These authentication services use a centralized authentication server to link with the Internet service provider. The authentication server sends one-time password over SMS to authenticate users in [17]. Users are requested to call a static [18] or a one-time phone number [19] at the authentication server. Alternatively, the authentication server in [20] calls back the user's cellular phone and requests the input of user PIN. These authentication models can be further applied when a session-id is created between the web service provider and a PC using a barcode reader on a mobile phone [21].

The proposed protocol is similar to SecureCall [20] in calling back the user and requests the input of user PIN. However, the protocol does not use a separate authentication server as in SecureCall but integrates the calling back function with the card issuing bank, and uses a landline rather than a cellular phone. This makes the protocol securer at the loss of mobility.

3. The Purchase Protocol

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 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 card-

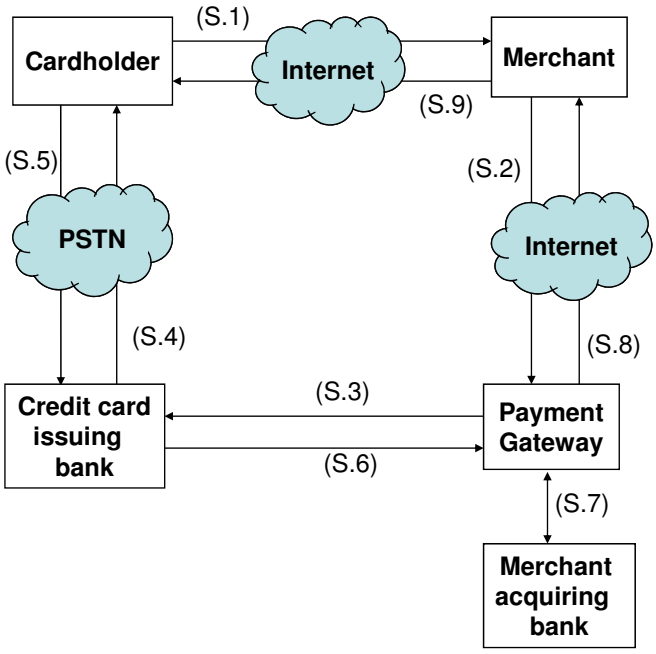

Figure 1. The purchase protocol with live authentication

holder 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.
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

Notation	Meaning
C	Cardholder
M	Merchant
P	Payment gateway
$CardB$	Card issuing bank
$pubEK$	Encryption key of a public key pair
$priDK$	Decryption key of a public key pair
$pubVK$	Verification key of a public key pair
$priSK$	Signing key of a 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. After the payment applet is downloaded to the cardholder's machine, it locally generates an asymmetric key pair for the cardholder because 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.

$$C->M: \text{OIEncrypt, PIEncrypt, CardSign} \quad (1)$$

where the payment applet has computed the following.

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

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).

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

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).

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

(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).

$$CardB->P:$$
$$\text{Crypt}_{\text{pubEK}_P}(\text{XID, PurAmt, auCode,}$$
$$\text{Sign}_{\text{priSK}_{CardB}}(\text{Hash(XID, PurAmt, auCode)))} \quad (7)$$

(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).

$$P->M:$$
$$\text{Crypt}_{\text{pubEK}_M}(\text{XID, PurAmt, auCode,}$$
$$\text{Sign}_{\text{priSK}_P}(\text{Hash(XID, PurAmt, auCode)))} \quad (8)$$

Phase 5: Purchase Response.

(S.9) The merchants shopping site generates and sends feedback to the cardholder 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.".

$$M->C:$$
$$\text{Crypt}_{\text{pubEK}_C}(\text{XID, PurAmt, auCode,}$$
$$\text{Sign}_{\text{priSK}_M}(\text{Hash(XID, PurAmt, auCode)))} \quad (9)$$

4. Protocol Analysis

Yu etc. compared electronic payment systems in [22] from the aspects of technology, economy, social, institution and law. We analyze the proposed rotocol from security, economic and social aspects in this section.

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.

Non-repudiation of the transaction is provided in the protocol through phase 4 of authorization and authentication response and phase 5 of purchase response. Once the cardholder confirms his purchase via telephone, he cannot deny the order given he is the true owner of the card. On the merchant side, if he confirms the transaction went through in purchase response, he should ship the goods to the cardholder; otherwise he should not charge the cardholder. The cardholder can use his credit card bill and the merchant's purchase response message as proof in case of a dispute.

4.2 Formal Model

The above general analysis can be proved by inductive method of protocol verification Isabelle/HOL [23] in which a protocol is modelled by the set of all possible traces of events that it can generate. We have not verified the protocol yet but specified the key phases in Isabelle. Phase 3 of authorization and authentication is shown in Fig. 2 while phases 1, 2, 4 and 5 are attached in the appendix.

The Isabelle events' expressions and meanings are explained in Table 2. There are three existing forms of events in Isabelle, i.e., $Says$, $Gets$, and $Notes$. It is not assumed, however, that a $Says\ A\ B\ X$ implies a $Gets\ A\ X$ event because the message X is sent over an insecure network Internet. We define two new events $Calls$ and $Answers$ that happen through PSTN. They are used in $SET\_Phase3.2$ and $SET\_Phase3.3$ of Fig. 2 when the card issuing back authenticates the cardholder through PSTN. The protocol specification is rather self explanatory when referring to the protocol explanation in Section 3. We should notice that the event $Says\ C\ CardB\ \{\!|(Number\ (PIN\ C),\ Number\ PurAmt|\!\}$ in $SET\_Phase3.3$ is transmitted through PSTN too.

Table 2. Isalelle events

Event	Meaning
$Says\ A\ B\ X$	A sends message X to B
$Gets\ A\ X$	A receives message X
$Notes\ A\ X$	A stores X in its internal state
$Calls\ A\ X$	A calls phone number X
$Answers\ A\ X$	A answers phone number X

$$
\begin{array}{l}
SET\_Phase3.1: \\
\quad [\![evsPhase3.1 \in set\_pur; \\
\quad\ Gets\ P\ Crypt\ (pubEK\ P) \\
\qquad\qquad Sign\ (priSK\ M) \\
\qquad\qquad \{\!|Number\ XID,\ PIEncrypt,\ CardSign, \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ OrderInfo|\!\},\ Key\ (pubVK\ C)|\!\} \\
\qquad \in set\ evsPhase3.1]\!] \\
\Longrightarrow Says\ P\ CardB\ Crypt\ (pubEK\ CardB) \\
\qquad\qquad \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt, \\
\qquad\qquad\ Sign\ (priSK\ P) \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt|\!\}|\!\} \\
\quad\ \#\ evsPhase3.1\ \in\ set\_pur \\
\\
SET\_Phase3.2: \\
\quad [\![evsPhase3.2 \in set\_pur; \\
\quad\ Notes\ CardB\ (Number\ (PhoneNumber\ C)); \\
\quad\ Gets\ CardB\ Crypt\ (pubEK\ CardB) \\
\qquad\qquad \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt, \\
\qquad\qquad\ Sign\ (priSK\ P) \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt|\!\}|\!\} \\
\qquad \in set\ evsPhase3.2]\!] \\
\Longrightarrow Calls\ CardB\ (Number,\ (PhoneNumber\ C)) \\
\quad\ \#\ evsPhase3.2\ \in\ set\_pur \\
\\
SET\_Phase3.3: \\
\quad [\![evsPhase3.3 \in set\_pur; \\
\quad\ Notes\ C\ (Number\ (PIN\ C)); \\
\quad\ Answers\ C\ (Number,\ (PhoneNumber\ C)) \\
\qquad \in set\ evsPhase3.3]\!] \\
\Longrightarrow Says\ C\ CardB\ \{\!|(Number\ (PIN\ C),\ Number\ PurAmt|\!\} \\
\quad\ \#\ evsPhase3.3\ \in\ set\_pur
\end{array}
$$

Figure 2. Isabelle expressions of the purchase protocol. Phase 3: authorization and authentication.

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).

In the protocol the cardholder has direct contact with the merchant and the card issuing bank, but not the payment gateway; the payment gateway in this way is transparent to the cardholder. A malicious payment gateway Alice can re-encrypt a received authorization and authentication request to generate a valid request for another payment gateway Bob using Bob's public key. Bob would then waste resources when processing the ingenuine request, resulting in Denial-of-Service for other genuine requests. A bad merchant could also collude with a payment gateway so as they both get cardholder's account details and shopping patterns.

4.4 Usability

The economic aspect lies in the following:

1. The cost of transaction. 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.

2. Atomic exchange. During the transaction, the cardholder will be charged if he confirms the purchase because he sends the payment details to the merchant already. However, we cannot say the protocol provides atomic exchange since the cardholder consumes first but pay later.

3. User range. The protocol is limited to users who have a credit card and a landline telephone.

4. Finiancial risk. The financial risk at the cardholder side is low since the credit card company has taken most of the risk.

The social aspect lies in the following.

1. Anonymity. The protocol has good anonymity. Merchants are unable to attain information about the cardholder's account; and the payment gateways are unable to analyse the spending habits of the cardholder.

2. Convenience. 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.

3. Mobility. The protocol is poor in terms of mobility. A cardholder is only able to authenticate himself through PSTN at the place with the landline telephone whose number he leaves with the bank.

5. Summary

Current online credit card payment is not secure due to its lack of cardholder authentication. This paper proposes a purchase protocol with mutichannel 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 at 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 secure and card fraud difficult. Furthermore, the cardholder does not need to obtain public key certificates or install additional software for the transaction.

Acknowledgement

The authors would like to thank the reviewers of this draft and our previous conference paper published in IAS 2008 [24] for their valuable comments.

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/.

[7] F. L. Wong and F. Stajano. Multi-channel protocols. In *Proceedings of 13th Security Protocols Workshop, Lecture Notes in Computer Science 4631*, Berlin, 2005. Springer-Verlag.

[8] F. L. Wong and F. Stajano. Multichannel security protocols. *IEEE Pervasive Computing*, 6(4):31–39, 2007.

[9] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues in ad-hoc wireless networks. In *Proceedings of 7th Security Protocols Workshop, Lecture Notes in Computer Science 1796*, pages 172–182, Berlin, 2000. Springer-Verlag.

[10] S. Goldthwaite, G. Crellin, and W. Graylin. System and method for payment transaction authentication, US patern 2004/0019564. Jan. 29, 2004.

[11] M. J. Yates, S. M. Thompson, N. H. Edwards, M. M. Gillford, and D. J. McCartney. Transaction authentication, US patern 2004/0064406. Apr. 1, 2004.

[12] R. L. Willard and O. E. Khandaker. Online payment system and method, US patern 2005/0182720. Aug. 18, 2005.

[13] M. R. Sendo and R. S. Sherman. Methods and apparatus for conducting secure online monetary transactions, US patern 6,970,852. Nov. 29, 2005.

[14] J. Wankmueller. System and method for secure telephone and computer transactions, US patern 2005/0289052. Dec. 29, 2005.

[15] G. Peng, J. Kang, G. Wei, J. Yao, N. Wang, L. Zhang, and J. Liang. Secure online payment system and online payment authentication method, US patern 2007/0288392. Dec. 13, 2007.

[16] K. Chatterjee. System and method for authenticating users of online services, US patern 2008/0072294. Mar. 20, 2008.

[17] Signify the password ondemand, Accessed May 2009. http://www.signify.net/services/services_pod.asp.

[18] Identrica two factor authentication, Accessed May 2009. http://www.identrica.com/.

[19] Saintlogin, Accessed May 2009. http://www.saintlogin.com/html/cosa.html.

[20] Securecall, Accessed May 2009. hhttp://www.thirdnetworks.co.jp/sc/03ser02.html.

[21] S. Mizuno, K. Yamada, and K. Takahashi. Authentication using multiple communication channels. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 54–62, New York, NY, USA, 2005. ACM.

[22] 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.

[23] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *J. Comput. Secur.*, 6(1-2):85–128, 1998.

[24] H. Xiao, B. Christianson, and Y. Zhang. A purchase protocol with live cardholder authentication for online credit card payment. In *The 4th International Conference on Information Assurance and Security (IAS)*, pages 15–20. IEEE Computer Society, 2008.

Appendix

$$
\begin{array}{l}
SET\_Phase1: \\
\quad [\![evsPhase1 \in set\_pur;\ M = Merchant;\ P = Payment\ gateway;\ C = Cardholder; \\
\quad\ Key\ (priSK\ C) \notin used\ evsPhase1;\ (priSK\ C) \neq 0; \\
\quad\ Key\ (pubVK\ C) \notin used\ evsPhase1; \\
\quad\ Key\ (priDK\ C) \notin used\ evsPhase1;\ (priDK\ C) \neq 0; \\
\quad\ Key\ (pubEK\ C) \notin used\ evsPhase1; \\
\quad\ OIEncrypt = Crypt\ (pubEK\ M) \\
\qquad\qquad \{\!|Number\ XID,\ Number\ OrderInfo,\ Key\ (pubVK\ C),\ Key\ (pubEK\ C) \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt|\!\}|\!\}; \\
\quad\ PIEncrypt = Crypt\ (pubEK\ P) \\
\qquad\qquad \{\!|Number\ XID,\ Number\ PayInfo,\ Key\ (pubVK\ C) \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ OrderInfo|\!\}|\!\}; \\
\quad\ CardSign = Sign\ (priSK\ C) \\
\qquad\qquad \{\!|Hash\ \{\!|Number\ XID,\ Number\ OrderInfo|\!\}, \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ PayInfo,\ Number\ PurAmt|\!\}|\!\}; \\
\quad\ Gets\ C\ \{\!|Key\ (pubEK\ M),\ Key\ (pubEK\ P),\ Number\ XID|\!\} \\
\qquad \in set\ evsPhase1]\!] \\
\Longrightarrow Says\ C\ M\ \{\!|OIEncrypt,\ PIEncrypt,\ CardSign|\!\} \\
\quad\ \#\ Notes\ C\ (Number\ XID) \\
\quad\ \#\ evsPhase1 \in set\_pur
\end{array}
$$

Figure 3. Isabelle expressions of the purchase protocol. Phase 1: purchase request.

$$
\begin{array}{l}
SET\_Phase2: \\
\quad [\![evsPhase2 \in set\_pur; \\
\quad\ Gets\ M\ \{\!|OIEncrypt,\ PIEncrypt,\ CardSign|\!\}; \\
\qquad \in set\ evsPhase2]\!] \\
\Longrightarrow Says\ M\ P\ Crypt\ (pubEK\ P) \\
\qquad\qquad\ Sign\ (priSK\ M) \\
\qquad\qquad\ \{\!|Number\ XID,\ PIEncrypt,\ CardSign, \\
\qquad\qquad\ Hash\ \{\!|Number\ XID,\ Number\ OrderInfo|\!\},\ Key\ (pubVK\ C)|\!\} \\
\quad\ \#\ evsPhase2 \in set\_pur
\end{array}
$$

Figure 4. Isabelle expressions of the purchase protocol. Phase 2: authorization and authentication request.

```
SET_Phase4.1 :
    ⟦evsPhase4.1 ∈ set_pur;
     Notes CardB {|(Number (PIN C))|};
     Gets CardB Crypt (pubEK CardB)
                  {|Number XID, Number PayInfo, Number PurAmt,
                    Sign (priSK P)
                      Hash {|Number XID, Number PayInfo, Number PurAmt|}|};
     Gets CardB {|Number (PIN C), Number PurAmt|}
       ∈ set evsPhase4.1⟧
⟹ Says CardB P Crypt (pubEK P)
                    {|Number XID, Number PurAmt, Number auCode,
                      Sign (priSK CardB)
                        Hash {|Number XID, Number PurAmt, Number auCode|}|}
     # evsPhase4.1 ∈ set_pur

SET_Phase4.2 :
    ⟦evsPhase4.2 ∈ set_pur;
     Gets P Crypt (pubEK P)
               {|Number XID, Number PurAmt, Number auCode,
                 Sign (priSK CardB)
                   Hash{|Number XID, Number PurAmt, Number auCode|}|}
       ∈ set evsPhase4.2⟧
⟹ Says P M Crypt (pubEK M)
                 {|Number XID, Number PurAmt, Number auCode,
                   Sign (priSK P)
                     Hash {|Number XID, Number PurAmt, Number auCode|}|}
     # evsPhase4.2 ∈ set_pur
```

Figure 5. Isabelle expressions of the purchase protocol. Phase 4: authorization and authentication response.

```
⟦evsPhase5 ∈ set_pur;
     Gets M Crypt (pubEK M)
                 {|Number XID, Number PurAmt, Number auCode,
                   Sign (priSK P)
                     Hash {|Number XID, Number PurAmt, Number auCode|}|}
       ∈ set evsPhase5⟧
⟹ Says M C Crypt (pubEK C)
                 {|Number XID, Number PurAmt, Number auCode,
                   Sign (priSK M)
                     Hash {|Number XID, Number PurAmt, Number auCode|}|}
     # evsPhase5 ∈ set_pur
```

Figure 6. Isabelle expressions of the purchase protocol. Phase 5: Purchase response.