Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

ELSEVIER

Computer Standards & Interfaces 25 (2003) 119–129

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Securing on-line credit card payments without disclosing privacy information

Jing-Jang Hwang[a,*], Tzu-Chang Yeh[b,c], Jung-Bin Li[b]

[a] *Department of Information Management, Chang Gung University, 259 Wen Hwa 1st Road, Kweishan, Taoyuan 333, Taiwan*
[b] *Institute of Information Management, National Chiao Tung University, 1001 Tah Hsueh Road, Hsinchu 300, Taiwan*
[c] *Department of Information Management, Ming Hsin University of Science and Technology, Hsin Feng, Hsinchu 304, Taiwan*

Received 4 March 2002; received in revised form 5 September 2002; accepted 12 September 2002

Abstract

Two revisions of the original Secure Electronic Transaction (SET) protocol are proposed to conceal cardholders' identities in the electronic marketplace in which cardholders' trust for banks can be reduced to a minimum. Constrained by being extensions of the existing card payment networks to the Internet, most on-line credit card payment schemes in use or proposed in recent papers assume the sensitive card information could be disclosed to all the participating banks. The assumption used to work well in traditional credit card payments before. However, negative impacts such as banking scandals, closure programs due to poor management, and security problems with Internet banking are all undermining cardholders' trust in banks. The issuer is the trusted bank selected by the cardholder, but the acquirer is not. To reveal the cardholder's sensitive card information to every possible acquirer implies potential risk. Based on the need-to-know principle, the two revisions are proposed to relax the assumption mentioned above.

In our solutions, the sensitive card information is well protected along the way and can be extracted only by the issuer. A cardholder needs only to select a trustworthy issuer, instead of worrying about the possible breakdowns of every involved acquirer. The cost to achieve our more secure schemes demands only minor information modifications on the legacy system.

Keywords: Electronic commerce; Privacy; Credit card; On-line payment

1. Introduction

Information privacy is defined as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used" [1]. It has been a critical concern long there before the advent of computers. As computer technologies advance and the popularity of Internet grows, personal information could be recorded, gathered, analyzed, and misused easier than ever. Privacy protection is therefore becoming an important issue in the cyber era. Especially when it comes to on-line credit card payments. Not just only because this payment method has been becoming the trend of modern consuming practice, but also it involves the sensitivity of personal information. One of GartnerG2's reports [2] shows that

* Corresponding author. Tel.: +886-3-3283016x5815; fax: +886-3-3271304.
E-mail address: jjhwang@mail.cgu.edu.tw (J.-J. Hwang).

0920-5489/02/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
doi:10.1016/S0920-5489(02)00102-2

approximately 60% of on-line adults in the US do not do business on the web due to security and privacy concerns. Another Gartner's report [3] indicates that credit cards are used for 93% of all transactions in the on-line world. The Information Technology Association of America found that 74% of Americans are worried that their personal information on the Internet could be stolen or used for malicious purpose [4]. Therefore, the issue of privacy protection for on-line credit card payments is in great need to be addressed for the development of electronic commerce.

With a growing scale of wide acceptance and a mature business operation infrastructure, payment by credit card has been a common payment method in the physical world. This method has also been commonly applied on-line, but cardholders' confidence needs to be improved. Taking advantage of its convenience, Secure Sockets Layer (SSL) has become the most widely used protocol for on-line credit card payments nowadays. However, it is designed only to provide a private and reliable channel between two communicating entities. Unscrupulous merchants can steal cardholders' credit card information that contains the key elements needed to counterfeit credit cards and/or to initiate fraudulent transactions. Secure Electronic Transaction (SET) [5–8], the secure electronic transaction protocol proposed by VISA International and MasterCard International, is deemed to be a de facto standard. But, there is agreement in the market that SET has not taken off. The complexity and cost of implementing SET have been obstructing barriers. Moreover, some researchers [8] pointed out that SET does not address the concern of data aggregation. Constrained by being an extension of the existing card payment networks to the Internet, the acquirer can obtain the cardholder's card number and the issuer has a complete record of the cardholder's credit card transactions which could be aggregated for further analysis. Recently the successor of SET, 3D SET (3 Dimension SET) [9], is proposed to improve the portability and the flexibility for cardholders to pay on-line. The core protocol of 3D SET is the same as that of SET. Based on the inherent assumption that banks are trustworthy, all the transaction details and history of the cardholder are stored at the bank. Having long been trusted by cardholders, banks can always access to sensitive data over their cardholders, which they should not know. However, negative impacts such as banking scandals, closure programs due to poor management, and security problems with Internet banking are all undermining cardholders' trust in banks. The Behrens's report from GartnerG2 [2] shows that 86% of on-line American adults are very concerned about the security of bank and brokerage account numbers when doing on-line transactions. According to Riem's survey [10], a serious case happened in December 2000 draws much attention. Halifax, a British bank, was forced to shut down one of its credit card sites after leaving cardholder details exposed. Three of the largest British banks have also been identified as having security holes in their systems. Academically, some protocols are also proposed in recent papers to improve the privacy protection for cardholders [8,11,12].

In this paper, we first examine the necessary privacy protection for on-line credit card payments, and then analyze the protection on the major protocols that are either in use or proposed in recent papers. Based on the need-to-know principle proposed in Refs. [8,13,14], transaction information should be available only to parties that need it to avoid data aggregation and misuse. Two revisions of the original SET protocol are proposed to conceal cardholders' identities in the electronic marketplace. Cardholders' trust for banks can thus be reduced to a minimum. A cardholder needs only to select a trustworthy issuer, instead of worrying about the possible breakdowns of every involved acquirer.

2. Privacy requirements

In this brick-and-mortar world, there are four roles involved in the transaction model of credit card payment. The *issuer* is a financial institution that issues a credit card to the *cardholder*. The *acquirer* is a financial institution that processes payment authorizations and payments for the *merchant*. When a cardholder intends to buy something at a merchant's place and wishes to pay by credit card, the flow of a transaction is described as follows:

1. The cardholder presents his/her credit card and signs a purchase request to the merchant.
2. The merchant sends an authorization request to the acquirer.

3. The acquirer forwards the authorization request to the issuer through the existing financial networks.
4. After validating the status of the credit card, the issuer sends an authorization response back to the merchant via the acquirer to guarantee the corresponding payment.
5. If the transaction is authorized, the merchant then fulfills the order (e.g., by giving goods) and gives the cardholder a copy of the purchase order; or the order is rejected.

In this scenario, the credit card information is known to all the merchants that the cardholder has dealt with and to all the corresponding acquirers which the cardholder may not trust. Moreover, the issuer keeps all the cardholder's transaction history that could be analyzed to find out the cardholder's spending habits.

For on-line credit card payments, the sensitive personal information could be collected easily from the public network. Having all that information in one place would make it very tempting for the company to sell data about cardholders' preferences to marketers. The privacy concern must be addressed to win cardholders' confidence. Based on the need-to-know principle that was proposed in Refs. [8,13,14], every participant should know only the information needed to perform its job. The following requirements should be considered to enhance the privacy protection for the cardholder to pay on-line.

R1 The credit card information should be shared only between the cardholder and the issuer. That is also defined as a privacy requirement in RFC2905 [15]. The merchant and the acquirer do not need the credit card information to perform their job.

R2 The order information should be shared only between the cardholder and the merchant. The issuer and the acquirer do not need to know the content of the order information.

R3 The real identity of the merchant should not be exposed to the issuer. It is unnecessary for the issuer to perform its function. The issuer needs only to verify the cardholder's authorization on the corresponding payment. In the existing card payment infrastructure, the merchant's name is sent from the acquirer to the issuer. The issuer keeps all the cardholder's transaction history that could be analyzed to find out the cardholder's spending habits. The selling of the cardholder's financial information makes the cardholder the target of telemarketing. Without the merchant information, the issuer's ability to trace the cardholder's buying habits is limited.

3. Related works and analysis

Firstly, three relevant schemes that have been implemented in marketplace are analyzed. Then two protocols in literatures will be discussed.

3.1. SSL

Originally developed by Netscape, SSL is designed to provide confidentiality and integrity of data exchanged between two communicating entities. It is simple, cheap and quick to implement, and, is the most widely used payment scheme on the Internet. SSL does not intend to provide complete protection for on-line credit card payments. Because it only encrypts the link between the cardholder and the merchant, additional mechanisms are needed to transmit credit card information and authorization information from the merchant to the banks. Moreover, once the credit card information is received by the merchant, it will be decrypted to plain text. That violates the privacy requirement R1 mentioned in the previous section. In this case, the card information is vulnerable to disclosure and misuse. As merchants usually do not have the expertise to design and build the security infrastructure for their web sites, their databases containing numerous cardholders' card information are always the open targets of hackers. Furthermore, some malicious merchants may use the cardholder's credit card information that provides the key elements needed to counterfeit cards and/or to initiate fraudulent transactions. Because only the merchant receives the order information, the requirement R2 can be achieved. As the authorization process resembles that of the card-present transaction, the merchant's name is included in the authorization request made by the acquirer. So, the requirement R3 is not addressed.

Doing transactions on-line with straightforward SSL encryption/decryption does not fully satisfy the

concerns upon cardholders' privacy protection. Although SSL has been a widely accepted security protocol, it is still not the best choice for cardholders for the need of privacy protection.

3.2. SET

SET, jointly developed by VISA, MasterCard, IBM, GTE, Microsoft, Netscape, etc., is a security paradigm for on-line credit card payments. A payment gateway, a device usually operated by an acquirer that processes payment messages for the merchant, is defined in SET specification. We do not distinguish the payment gateway and the acquirer here. SET uses public key encryption/decryption to provide the confidentiality and the integrity of the payment information. It uses the digital signature to authenticate all parties involved in the payment process, including the cardholder, the merchant, and the acquirer to ensure entity legitimacy prior to the transaction. To protect the cardholder's privacy, the payment information including the credit card number is protected from the merchant and the order information is protected from the banks. Fig. 1 illustrates the message flow in the SET protocol.

Before introducing SET protocol, the following notations should be stated:

C: Cardholder
M: Merchant
A: Acquirer
I: Issuer
Sx(M): Message M is signed by X's private key.
DSx(M): The dual signature on message M. Such dual signature is encrypted by X's private key.
ENVx(M): Message M is protected by the digital envelope. Such envelope is encrypted by X's public key.

If a cardholder intends to initiate an on-line payment after picking items to be purchased from the merchant's web site or electronic catalogs, the following main steps are taken:

1. The cardholder's electronic wallet (E-Wallet) generates Order Information (OI) and Payment Instruction (PI). These two documents must be signed by the cardholder with his private key. The signature is called as a dual signature. OI is sent to the merchant; while PI, protected by a digital envelope encrypted with the acquirer's public key, is sent to the acquirer through the merchant.
2. After receiving the purchase request from the cardholder, the merchant generates an authorization request (AUTH REQ), which includes the amount to be authorized. The request is signed with the merchant's private key, protected by the digital envelope encrypted with the acquirer's public key, and then transmitted along with the encrypted PI to the acquirer.

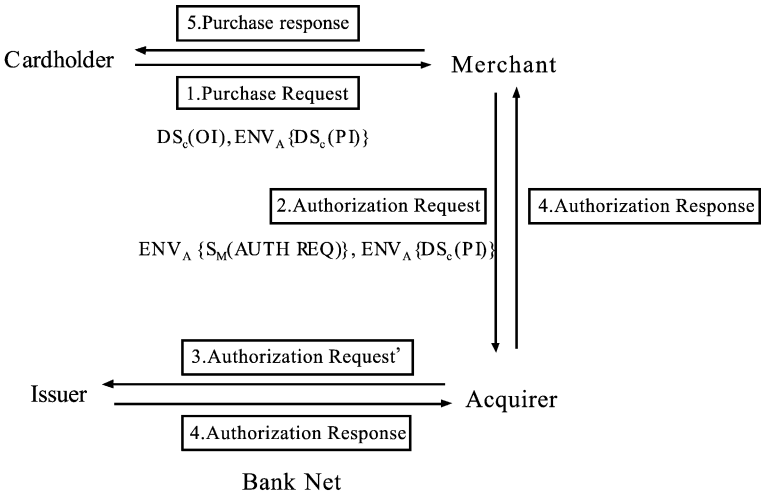

Fig. 1. The SET protocol.

3. After verifying the signatures and ensuring the consistency between AUTH REQ and PI, the acquirer creates its own Authorization Request', including the merchant's name, the credit card information, and the transaction amount, etc., and then sends it through the private financial networks to the issuer.
4. The issuer verifies whether the credit card is stolen, revoked, or over its credit limit, and then sends the authorization response to the merchant via the acquirer.
5. According to the received Authorization Response, the merchant transmits Purchase Response to the cardholder.

SET is designed to ensure the security of electronic transactions over the Internet. It does provide well protection. The requirement R2 is achieved since the order information is protected from the banks. However, constrained by being an extension of the legacy system to the Internet, SET does not address the following concerns.

1. The acquirer receives unnecessary access to the cardholder's payment information. It is the issuer who can approve the payment. The acquirer simply forwards the authorization request and response to the issuer and the merchant, respectively. The acquirer does not need to know the cardholder's card information to perform its function. The privacy requirement R1 is not addressed.
2. The issuer has to trust the acquirer's verification about the cardholder's signature on PI and the consistency between the AUTH REQ and PI. After sending the authorization response to the merchant via the acquirer, the issuer assures the merchant of the payment. Bearing the risk of false payment, the issuer should validate whether PI is indeed signed by the cardholder and the amount to be authorized is agreed by the cardholder to commit the payment. However, these are verified by the acquirer instead. Hence, in the original SET, the issuer has to rely on the trust relationship with the acquirer.
3. The issuer knows which merchant the cardholder transacts with while it just needs to verify the cardholder's authorization on the corresponding payment. The privacy requirement R3 is also not considered.

Hwang and Hsueh [8] proposed a revised SET protocol using the credit card certificate—an anonymous surrogate for the credit card—to conceal the cardholder's credit card number in the electronic marketplace.

3.3. 3D SET

To improve the portability and the flexibility for cardholders, VISA introduced 3D SET in August 1999. VISA EU mandated its member banks to adopt 3D SET by October 2001. As shown in Fig. 2, 3D SET [9] looks at the activities among the following parties:

- The merchant and the acquirer—Acquirer Domain
- The cardholder and the issuer—Issuer Domain
- The issuer and the acquirer—Interoperability Domain.

Using the existing relationship, the issuer and the acquirer are free to determine security and authentication schemes for their own cardholders and merchants, respectively, such as PIN or password. The original SET protocol fits into the Interoperability Domain.

To increase the convenience for the cardholder, the function of E-Wallet in SET is divided into a centralized server side wallet engine residing at the issuer and a light-weight, easy-to-download wallet interface on the cardholder's device. Through the wallet interface, an authenticated cardholder can access his/her server side wallet. The server side wallet can perform the same operations as E-Wallet. Without complicated installation, the cardholder is also free from the burden of maintenance, upgrades and implementation of new releases. Due to the low computation demand of the client side, either a PC, a WAP mobile phone, or a digital TV can be used as the cardholder's Internet access device. Similarly, through the merchant server interface, an authenticated merchant can access his/her server side merchant server. Merchants using 3D SET to authenticate cardholders will not be liable for fraudulent transactions.

Basically, 3D SET is working on the inherent basis that all banks are trustworthy. The transaction information is primarily recorded and maintained by the issuer and the acquirer. Banks take up more responsibilities in 3D SET than that in SET.

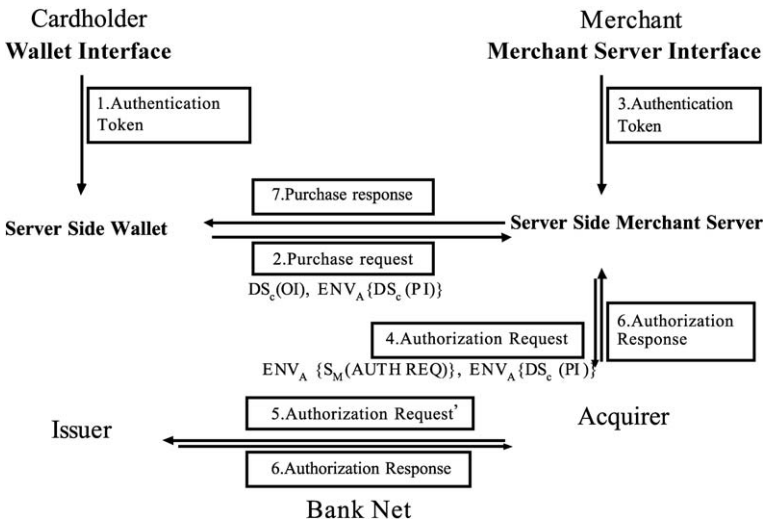

Fig. 2. The 3D SET model.

While the credit card number can be sealed from the acquirer using pseudo card number assigned by the issuer, the server side wallet residing at the issuer routes purchase requests from the cardholder, and communicates with other SET components (the merchant, the acquirer and CA). The issuer stores the cardholder's private key, certificate, card information, and purchase transaction details and history. The issuer keeps everything needed to proceed with identity theft. That also weakens the cardholder authentication. Moreover, the acquirer manages the server side merchant server for the merchant. Both PI and OI are open to the issuer and the acquirer. None of the requirements R1, R2, and R3 is considered.

Namely, 3D SET reduces the loading of the cardholder and the merchant in order to fit in the newly emerged environment of mobile transactions. On the contrary, 3D SET increases the loading of banks, and removes the rights of cardholders and merchants to keep their individual information confidential. Such scenario is a negative impact on the issue of privacy protection. If the transaction information can be protected from any malicious intention of aggregation by any single party, the cardholders' privacy can be secured even under the assumption that banks are not always trustworthy.

Recently, two protocols are proposed in papers to enhance cardholders' privacy protection by concealing the cardholders' identities from the merchant.

3.4. Mu and Varadharajan's protocol

Mu and Varadharajan [11] proposed a novel anonymous scheme in which the involvement of the on-line financial institution can be reduced to a minimum. Using an anonymous public key certificate issued from the bank, the cardholder conceals his/her identity from the merchant. Using the technique of equality proof of knowledge, the merchant can verify the authenticity of the credit card by itself without knowing the cardholder's card information. However, because the acquirer and the issuer are not distinguished here, the requirement R1 is not discussed. It is the issuer who can check the status of the credit card. Without the issuer's confirmation before delivering goods or providing services, the merchant has to bear the risk of being cheated. Because the public key technology is heavily applied in this scheme, the transaction efficiency is limited. Besides, as only the messages transmitted between the cardholder and the merchant are defined, the merchant and the financial institutions (addressed as the acquirer and the issuer in our paper) need additional mechanisms to transmit the authorization information. The payment slip used in the scheme, containing the merchant information and the order information, must be forwarded to the financial institutions for verification. The requirements R2 and R3 are not addressed.

3.5. Schneider and Felten's protocol

Schneider and Felten [12] proposed an efficient anonymous scheme using one-time pads. The static identifier of the traditional credit card, the credit card number, has been replaced with a one-time identifier, and each identifier is used only once for a transaction. This mechanism prevents the linkage of multiple transactions to a single party. That satisfies the requirement R1. However, the use of one-time pads consumes a significant amount of storage capacity. Frequently the cardholder has to apply for another new smart card containing unused fresh one-time pads, and so does the merchant. In addition, the focus of the scheme is the anonymous authentication. The transaction parameters, containing the order information, are transmitted in plain text during the whole process. The requirement R2 and R3, is not considered in the scheme.

4. Our proposed solutions

Two solutions revising SET are proposed to provide better privacy protection.

4.1. Solution 1

We use the same notations mentioned earlier in the introduction of SET.

The major concept in this solution is that PI here is not verified by the acquirer, but the issuer instead. The PI in Purchase Request is protected by the digital envelope made by the issuer's public key. The verifications of the cardholder's certificate and digital signature are now the duties of the issuer. Once the issuer authenticates the cardholder's signature on PI, equivalently it means the cardholder's authorization on the corresponding payment. With this, the issuer will no longer need to know which merchant the cardholder is dealing with. Hence, the merchant's name can be accordingly removed from Authorization Request' in Fig. 3. Since the merchant's ID included in PI is defined by the acquirer, it is not universally unique. Only the acquirer can derive the merchant's name from the merchant's ID. Therefore, the issuer cannot know which merchant the cardholder is dealing with. The acquirer may link the authorization response and the authorization request together by transaction IDs to ask for redemption.

The detailed transaction flow, shown in Fig. 3, is described as follows.

1. Purchase Request, transmitted from the cardholder to the merchant, includes PI and OI. Both PI and OI are signed by the cardholder's private key as a dual signature. PI is also protected by the digital envelope made by the issuer's public key to prevent the merchant or the acquirer from knowing the cardholder's sensitive card information.

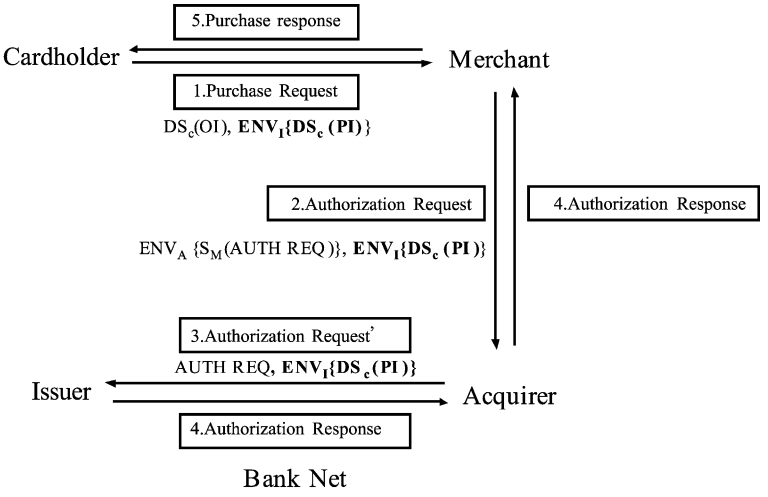

Fig. 3. The proposed extension to the SET protocol.

2. After authenticating the cardholder's signature on OI, the merchant generates and signs the authorization request (AUTH REQ). This signed information is protected by the digital envelope made by the acquirer's public key and then is sent out to the acquirer along with the encrypted PI.
3. After verifying the merchant's signature signed on AUTH REQ, the acquirer generates Authorization Request' including AUTH REQ and the encrypted PI.
4. After receiving Authorization Request', the issuer obtains PI with its private key, verifies the validity of the card, authenticates the cardholder's signature, and then confirms the consistency between AUTH REQ and PI. The issuer replies the acquirer with the authorization response. The acquirer then forwards the authorization response to the merchant.
5. The merchant generates a purchase response based on the received authorization response and sends it to the cardholder. The cardholder may proceed with the transaction with a positive purchase response.

4.2. Solution 2

In the original SET, sensitive credit card information including the card number, the expiry date, etc., is recorded as a hashed value rather than plain text in the cardholder's certificate. When the acquirer needs to verify the cardholder's signature on PI, it first extracts the credit card information from PI, computes the hash value of credit card information, and then compares the result with the subject name recorded in the cardholder's certificate. The link between the certificate and PI can thus be verified.

In this scenario, the cardholder's sensitive information is exposed at the acquirer's place, and it may possibly cause unexpected loss from the cardholder's point of view. Hence, we propose a revision of SET to address the cardholder's concern.

As shown in Fig. 4, we herein suggest that the cardholder's credit card information is recorded in the certificate after two times of hash computation instead of one. If it is H^2 (credit card information) stored in the certificate, only H (credit card information) has to be shown in PI. By validating the consistency between the certificate and PI, the acquirer still can verify the validity of the card without knowing the card number. Then the acquirer sends H (credit card information) received from PI to the issuer for authorization. Moreover, the merchant's name can be removed from Authorization Request' just as that in Solution 1 because it is not needed for the issuer to perform its function.

5. Analysis

SET, as well as the derivatives, is designed as an extension of the existing card payment networks to the Internet. Ignoring this assumption, we have indeed proposed solutions for a different environment.

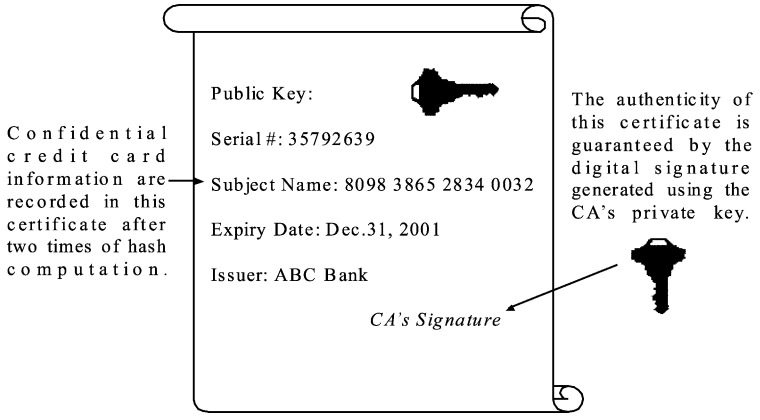

Fig. 4. An extension to a SET certificate.

Because our solutions modify the information contents passing through the existing proprietary card payment networks, they should not be considered as extensions to the legacy system. Modifications on the legacy system are necessary if our solutions are to be implemented. And such modifications demand extra cost. However, due to the high cost of the proprietary networks for banks, Internet is now considered a good substitute. The extra cost to achieve our solutions will be more justified. SET is an open standard that facilitates and encourages interoperability between SET-compliant products and services. As our solutions are only revisions of SET, interoperability and compatibility will remain untouched.

Our two solutions will be discussed respectively as follows.

5.1. Solution 1

5.1.1. Privacy

1. The cardholder's credit card number is concealed from the acquirer. It is the issuer who can approve this transaction. The acquirer only forwards the encrypted PI received from the cardholder via the merchant to the issuer for verification and credit card status checking. After receiving the authorization response from the issuer, the acquirer returns it back to the merchant. Because only the issuer can decrypt the encrypted PI, the cardholder's credit card number is protected from the acquirer and the merchant. The privacy requirement R1 is thus satisfied.
2. Because the order information is sent only to the merchant just as that in SET, the privacy requirement R2 is met.
3. Because the merchant's name is removed from Authorization Request', the issuer does not know which merchant the cardholder is dealing with. Without the order information and the merchant's name, the issuer's ability to analyze the cardholder's buying habits is limited. That meets the privacy requirement R3.

5.1.2. Other benefits

1. The issuer keeps non-repudiation evidence by itself for future dispute solving. The cardholder's signature on PI represents the cardholder's authorization on this payment. It is the only evidence that the issuer needs to hold against cardholder repudiation.
2. The efficiency is increased by simplifying the certificate verification process. On-line payments involve money transfer. Strict certificate verification, including certificate chain traversing and certificate revocation list (CRL) checking, is needed to authenticate participants. In SET, the cardholder needs to be assured that he/she do not send his/her sensitive information PI to an unauthorized acquirer. Without existing trust is built up between the cardholder and the acquirer, the complex mutual certificate verification must be done carefully in every transaction to avoid disputes. The cardholder needs to verify the acquirer's certificate by traversing the trust chain to the root key for encrypting the digital envelope of PI. The acquirer also has to validate the cardholder's certificate by traversing the trust chain to the root key to get the cardholder's valid public key for verifying the cardholder's signature on PI. However, the cardholder's certificate is revoked by revoking the card which it is tied to. The issuer maintains the revocation status of the cardholder's card. Through Authorization Request, the acquirer verifies the status with the issuer. Namely, the acquirer cannot verify the validity of the cardholder's certificate directly. In the proposed solution, PI is not verified by the acquirer, but the issuer instead. Using the existing trust relationship built between the cardholder and the issuer, the process of certificate verification can thus be simplified and the potential risk reduced. The issuer approving certificate request for the cardholder and maintaining the list of canceled payment cards can authenticate the cardholder directly using the public key of Cardholder Certificate Authority (CCA). The cardholder only needs to keep a key, the issuer's public key, to protect PI for all transactions.

The main difference from SET is that the key used to encrypt the digital envelope for protecting PI has been changed from the acquirer's public key to the issuer's public key. The decryption of PI has been moved to the issuer. To achieve this solution, extra

software is needed for the issuer to process the encrypted PI and the message fields of the existing financial networks need to be changed.

5.2. Solution 2

We suggest that the cardholder's sensitive information should be stored in the certificate after two times of hash computation, i.e. H^2 (credit card information). In that case, only hashed credit card information, H (credit card information), has to be recorded in PI. Without knowing the card number, the acquirer still can verify the consistency between the cardholder's certificate and PI. Due to the property of one-way hash function, it is easy to compute the hashed value, but computationally infeasible to invert. The repeated hashing technique has been widely used in many applications, such as one-time password authentication [16,17], micropayment [18–20], and conditional anonymity [21].

Given only hashed credit card information, H (credit card information), the acquirer cannot obtain the credit card information. And, attackers cannot derive H (credit card information) from H^2 (credit card information) recorded in the cardholder's certificate to forge PI. The credit card information is known only to the cardholder and the issuer. Therefore, privacy requirement R1 is achieved. Because the order information is sent only to the merchant just as that in SET, the privacy requirement R2 is met. The privacy requirement R3 can also be achieved since the merchant's name is removed from Authorization Request'.

As compared to Solution 1, Solution 2 can be a quick and easy choice in implementation. A hashed value will replace plain text in the existing field keeping credit card information, and the merchant name field will be left as blank. Without changing the message fields of the existing financial networks, SET can be enhanced to protect the secret credit card information from unnecessary exposure to all acquirers. The cost to achieve Solution 2 is one additional hash computation for PI generation in every transaction. Furthermore, one additional hash computation is needed for certificate generation. As for the verification of PI, the issuer can keep the hashed credit card information, H (credit card information), as the cardholder's record in its database.

6. Conclusion

Credit card is a popular mean for cardholders to pay on-line. However, the privacy protection issue poses a major concern to most cardholders. To encourage the development of electronic commerce, privacy protection should be improved to build up cardholders' confidence. In this paper, we summarize the requirements for cardholders' privacy protection, analyze three relevant and in use schemes: SSL, SET, and 3D SET, and protocols proposed in recent papers. Based on the need-to-know principle, two revisions of SET are proposed to secure cardholders' privacy even under the assumption that banks are not always trustworthy. The credit card number is transmitted not in plain text but in an encrypted form or as a hashed value from the cardholder to the issuer. As a result, the sensitive card information is concealed in the electronic marketplace. Without leakage of the sensitive information, the possible frauds could be reduced. Although there are many ways to safeguard cardholders' privacy, minimizing the need for collecting personal information is always one of fundamental principles.

Acknowledgements

Part of this research was funded by the National Science Council of Taiwan under the Contract of NSC 89-2416-H-009-038, while the first author of this article was working at National Chiao Tung University (NCTU).

References

[1] IITF principles, supra note 19, at 5.
[2] L. Behrens, Privacy and security: The hidden growth strategy, May 31, 2001, http://www.gartnerg2.com/site/searchresults.asp.
[3] K. Caldwell, The public policy report, CommerceNet Newsletter 3 (5) 2001, http://www.nii.org.tw/cnt/info/Report/20010504.html.
[4] ITAA, ITAA poll finds almost three of four Americans concerned about cyber security, Dec. 11, 2001, http://www.itaa.org/isec/pubs/e200112-05.pdf.
[5] MasterCard and VISA, Secure Electronic Transaction (SET) Specification, Book 1: Business Description, version 1.0 (1997).
[6] MasterCard and VISA, Secure Electronic Transaction (SET)

Specification, Book 2: Programmer's guide, version 1.0 (1997).
[7] MasterCard and VISA, Secure Electronic Transaction (SET) Specification, Book 3: Formal Protocol Definition, version 1.0 (1997).
[8] J.J. Hwang, S.C. Hsueh, Greater protection for credit card holders: a revised SET protocol, Computer Standards and Interfaces 19 (1998) 1–8.
[9] VISA EU, 3D SET, http://www.visaeu.com/virtual_visa/merchants/3dset.html.
[10] A. Riem, Cybercrimes of the 21st century: crimes against the individual—part 1, Computer Fraud and Security 6 (2001 June) 13–17.
[11] Y. Mu, V. Varadharajan, A New Scheme of Credit Based Payment for Electronic Commerce, Proc. LCN'98, 1998, pp. 278–284.
[12] M.A. Schneider, E.W. Felten, Efficient Commerce Protocols Based on One-Time Pads, Proc. ACSAC'00, 2000, pp. 317–326.
[13] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen, M. Waidner, Design, implementation, and deployment of the iKP secure electronic payment system, IEEE Journal on Selected Areas in Communications 18 (4) (2000 April) 611–627.
[14] Australian Transaction Report and Analysis Centre, RGEC report—research and technical advice volume 3, Dec. (1999), http://www.austrac.gov.au/text/publications/rgec/3/pdf/ch1.pdf.
[15] Network Working Group, AAA Authorization Application Examples, RFC 2905, http://www.faqs.org/rfcs/rfc2905.html.
[16] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981 November) 770–772.
[17] N.M. Haller, The S/KEY one-time password system, RFC 1760 (1995 February), http://www.faqs.org/rfcs/rfc1760.html.
[18] R. Rivest, A. Shamir, PayWord and MicroMint: Two simple micropayment schemes, MIT Laboratory for Computer Science, May (1997).
[19] Hallam-Baker, M. Phillip, Micro Payment Transfer Protocol (MPTP) version 0.1, W3C Working Draft, 22, Nov. (1995), http://www.w3.org/pub/WWW/TR/WD-mptp951122.
[20] R. Hauser, M. Steiner, M. Waidner, Micro-payments based on iKP, IBM Research, 12 February 1996, Research Report 2791.
[21] R. Hauser, G. Tsudik, On shopping incognito, Proc. 2nd USENIX Workshop on Electronic Commerce, Nov. 1996.

Jing-Jang Hwang began his academic career in 1976 as an instructor at National Chiao Tung University (NCTU) in Taiwan. He worked at NCTU for more than 25 years until the summer of 2002, and is now a professor of Chang Gung University. Given leave of absence from NCTU, he studied Business Administration at the University of Cincinnati, and then studied Computer Science at the University of Florida. He received his PhD degree from the University of Florida in 1987. In addition to teaching, he has designed several computerized information systems, which include the administrative and the library systems of NCTU itself, the business system of a securities brokerage firm, and the office automation system of the judicial courts in Taiwan. Since 1990, he has also been involved in research on subjects of cryptography, information security, and electronic commerce, and has contributed research articles, in the English language as well as in the Chinese language, to various magazines and journals.

Tzu-Chang Yeh received her BE degree in Computer Science and Information Engineering and MS degree in Management Science from National Chiao Tung University, Taiwan, in 1988 and 1990, respectively. Now, she is currently an instructor of the Department of Information Management, Mingshin University of Science and Technology and a PhD candidate in the Institute of Information Management, National Chiao Tung University.

Jung-Bin Li received his BBA degree in Computer and Information Science from the Soochow University, Taiwan, in 1993, and MS degree in Information Management from the London School of Economics, UK, in 1996. Currently, he is a PhD candidate in the Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan. His research interests include information security and electronic payment systems.