GREATER PRIVACY PROTECTION FOR ON-LINE CREDIT CARD PAYMENT

Tzu-Chang Yeh[1], Jung-Bin Li[2], Jing-Jang Hwang[3]
Institute of Information Management,
National Chiao Tung University
1001 Tah Hsueh Rd., Hsinchu, Taiwan
Tel/Fax: +886-35712121x57419/+886-35723792
[1]e-mail: cheer@mis.mhit.edu.tw
[2]e-mail: jbli@ms19.hinet.net
[3] e-mail: jjhwang @spring.iim.nctu.edu.tw

ABSTRACT

Privacy is always one of the primary concerns in electronic commerce. Consumers must have the right to keep their buying habits and personal information confidential, especially when it comes to on-line credit card payment. Not just only because this payment method has been becoming the trend of modern consuming practice, but also it involves the sensitivity of privacy information. Based on the need-to-know principle, transaction information should be distributed properly among participants to be against aggregation and analysis. In this paper, the privacy required for on-line credit card payment is described, and the privacy protection on three common payment protocols such as SSL, SET and 3D SET are also analyzed in detail. Two solutions are then proposed to enhance privacy protection for cardholders.

Keywords: electronic commerce, privacy, credit card, payment

INTRODUCTION

Privacy 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, collected, gathered, and analyzed easier than ever. Privacy protection is therefore becoming an important issue in the cyber era. In a fraud research led by CyberSource [1], consumers' fraud concerns negatively impact their on-line shopping demand. The loss of customer goodwill is ranked as the major negative impact for on-line merchant sales. According to the American National Consumers League survey conducted by Opinion Research Corporation International [2], most consumers prefer to pay on-line orders with credit cards (67%), while the greatest concern was that their credit card numbers would be stolen if they provided the information on-line (41%). Twenty-four percent of the survey respondents ranked the abuse of their personal information as their greatest concern on on-line commerce. In another fraud research by CyberSource for UK [3], total credit card security and the guarantee of keeping one's personal information private in any on-line transaction process, as well as protection against unauthorized access to customer information in particular, are shown to be the major concerns of consumers. Therefore, building up customers' confidence in on-line credit card payment weighs great importance to 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 major payment method in the physical world. This method has been commonly applied on-line, but still lack of cardholders' confidence. In order to help build up consumers' confidence in on-line credit card payment for the booming electronic commerce, privacy protection for customers is in great need to be enhanced. Taking advantage of its convenience, SSL has become the most commonly used protocol for on-line credit card payment nowadays, but only the confidentiality and the integrity of information data between cardholders and merchants are secured. Unscrupulous merchants can steal cardholders' credit card information that contains the key elements needed to counterfeit credit cards and/or to initiate fraudulent transactions. SET [4][5][6], the secure electronic transaction protocol proposed by VISA International and MasterCard International, is deemed to be a de facto standard, but gains little acceptance due to its complication and high cost. Additionally, banks can aggregate cardholders' transaction data for further analysis [7]. Recently the successor of SET, 3D SET [8], 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 SET, but all transaction detail and history of the cardholder are stored at the bank that infringes the right of cardholders on the matter of privacy protection. Banks have long been trusted by cardholders; however, negative impacts such as branch closure programs, poor customer services and security problems with Internet banking are all undermining customers' trust in banks.

In this paper, we first examine the privacy needed by the on-line credit card payment, and then analyze the privacy protection on the major protocols. Based on the need-to-know principle, two methods are proposed to improve the privacy protection.

THE TRANSACTION MODEL OF CREDIT CARD PAYMENT

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 authentication 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 order to the merchant.
2. The merchant sends an authorization request to the issuer via the acquirer.
3. After verifying the status of the credit card, the issuer sends an authorization response back to the merchant to assure the merchant of the payment.
4. 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.

To pay on-line by credit card, the business process resembles that of mail order or telephone order. Based on the need-to-know principle, the following requirements should be considered to enhance privacy protection for cardholders.

- Only the cardholder and the issuer know the credit card number.
- Only the cardholder and the merchant know the order information.
- The issuer should not know which merchant the cardholder deals with.

PRIVACY PROTECTION ON SECURITY PROTOCOLS

SSL

Originally developed by Netscape, SSL has been universally accepted on the World Wide Web for authenticated and encrypted communication between clients and servers. The SSL Protocol is designed to provide a private and reliable channel between two communicating entities. This protocol has the lowest level *SSL Record Protocol* for encapsulation of higher level protocols. One such encapsulated protocol, the *SSL Handshake Protocol*, allows the server and the client to perform mutual authentication and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives information. One advantage of SSL is that it is independent of application protocols. The application designers and users have no need to consider the implementation details of SSL.

Although SSL has been a widely accepted security protocol, it is still not the best choice for consumers in the sense of privacy protection. SSL does establish a perfectly secure channel between the consumer and the merchant; it cannot, however, protect the consumer from the merchant's malicious aggregation of transaction information and, even the worse, credit card counterfeits and fraudulent transactions. Hence, making transactions on-line with straightforward SSL encryption/decryption does not fully satisfy the concern upon consumer privacy protection.

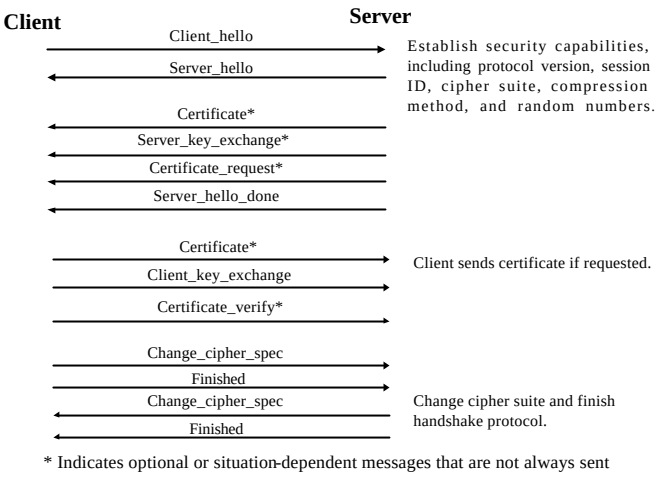

Figure 1. Handshake protocol of SSL

SET

SET, jointly developed by VISA, MasterCard, IBM, GTE, Microsoft, Netscape, etc., is a security paradigm for on-line credit card payment. A payment gateway, a device operated by an acquirer or a third party that processes merchant payment messages, is defined in SET specification. We do not distinguish between the payment gateway and the acquirer here. SET uses public key encryption/decryption to provide the confidentiality of payment information and to ensure payment integrity. It uses digital signatures 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. 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 generates a purchase request including the Order Information (OI) and the Payment Instruction (PI), which are signed by the cardholder's private key as a dual signature. OI is for the merchant; while PI, protected by a digital envelope encrypted with the acquirer's public key, is for the acquirer.
2. After receiving the purchase request from the cardholder, the merchant generates an authorization request (AUTH REQ), which includes the amount to be authorized, and then transmits the request along with PI to the acquirer.
3. The acquirer examines the validity of the merchant's authorization request and the cardholder's PI by verifying the signatures and ensures the consistency of the two messages. The acquirer then sends an authorization request, including credit card information

and transaction amount, through a financial network to the issuer.

4. After ensuring that the credit card is not stolen, revoked or over its credit limit, the issuer authorizes the transaction and sends the authorization response to the merchant via the acquirer.
5. The merchant transmits a purchase response to the cardholder according to the received authorization response.

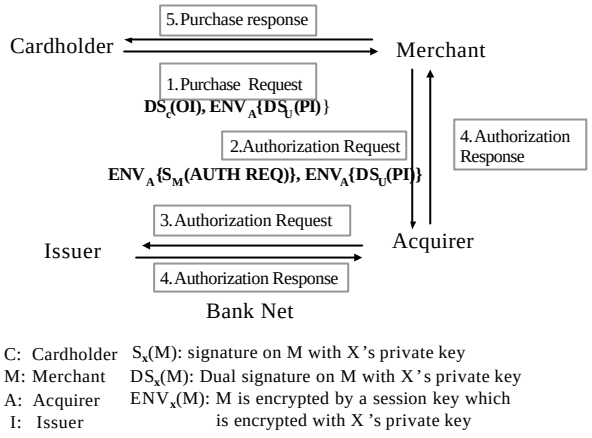

Figure 2. The payment authorization using SET

However, the acquirer receives unnecessary access to the consumer's payment information while it only needs to get the authorization response from the issuer. This situation violates the basic privacy requirement mentioned in the previous section. The same problem occurs when the issuer knows which merchant the consumer makes his/her transaction with; it just needs to verify the consumer's digital signature on payment information.

Hwang and Hsueh proposed a revised SET protocol [7] using the credit card certificate – an anonymous surrogate for the credit card – to conceal the cardholder's credit card number in the electronic marketplace. This revision also uses transaction IDs to allow the cardholder generates his/her monthly statement by linking payment details provided by the issuer and the information stored in E-wallet to avoid possible data aggregation by the issuer.

3D SET

VISA introduced a three-domain model (3D SET) in August 1999. Visa EU has mandated its member banks to adopt 3D SET by October 2001. Minimum standards are set, and the issuer and the acquirer are free to determine security and authentication schemes for their own cardholders and merchants respectively. The 3D SET [8] looks at the activity between the following parties:

- The merchant and their bank – Acquirer Domain
- The cardholder and their bank – Issuer Domain
- The cardholder's bank and the merchant's bank – Interoperability Domain

SET was too complicated and too costly to be successfully carried out. A Cardholder needs to install E-wallet and to apply for a certificate on his/her PC. To increase the convenience for the cardholder, the function of E-wallet 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 to pay on-line by credit card. 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, the merchant can be authenticated and then access his/her server side merchant server. Merchants using 3D SET to authenticate consumers – by accepting payments from bank-issued server side wallets – will not be liable for fraudulent transactions.

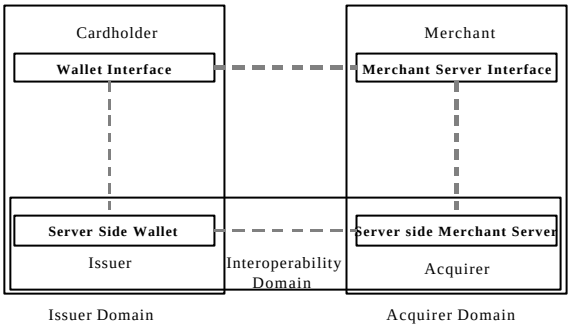

Figure 3. The 3D SET model

Basically, 3D SET is working on a basis that all banks are trustworthy. The transaction information is primarily recorded and maintained by the issuer and the acquirer. Hence in comparison to the original SET, 3D SET enhances the responsibility of banks. If the transaction information can be protected from any malicious intention of aggregation by an individual party, the cardholder's privacy can be secured even under the assumption that banks are not always reliable.

OUR PROPOSED SOLUTIONS

As none of the three protocols stated above can fully secure consumer privacy, this paper proposes two revisions on the original SET protocol.

Solution 1

The major concept in this solution is that PI here is not verified by the acquirer, but the issuer instead. The PI in a purchase request is protected by the digital envelope, which is made by the issuer's public key. The verifications of the credit card certificate and the digital signature are now the duties on the issuer. Once the issuer authenticates the customer's signature in PI, equivalently it means the customer's agreement to pay for the corresponding transaction. With this, the issuer will no longer need to know which merchant the customer is dealing with. Hence

the merchant ID can be accordingly removed from PI. The acquirer may link the authorization response and the authorization request together by transaction IDs to ask for redemption

Herein the detailed transaction flow, shown in Fig.4, is described as below:

1. The purchase request transmitted from the cardholder to the merchant includes PI and OI, which are signed by the cardholder's private key as a dual signature. PI is also protected by a digital envelope made by the issuer to prevent the merchant or the acquirer from knowing the cardholder's sensitive card information.
2. The merchant first authenticates the cardholder's digital signature in OI. If valid, it then generates and signs the authorization request (AUTH REQ). This signed information is then sent out to the acquirer altogether with the PI from the cardholder.
3. The acquirer verifies the validity of the merchant certificate, and examines the signature signed on AUTH REQ. The acquirer may request for authorization from the issuer with the authorization request and PI via the bank net or the Internet.
4. After receiving, the issuer obtains PI with its private key and authenticates the cardholder's signature on PI. By confirming the consistency of the authorization request and PI, the issuer notifies the merchant the authorization decision via the acquirer.
5. The merchant generates a purchase response based on the received authorization response. The cardholder may proceed with the transaction with a positive purchase response.

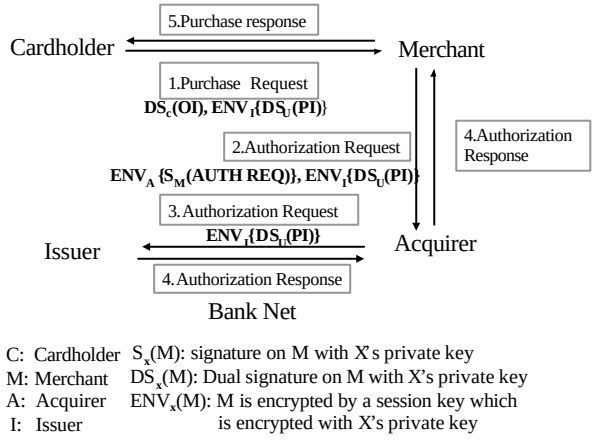

Figure 4. The proposed revision on SET payment authorization

Solution 2

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

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 protect cardholders from such losses.

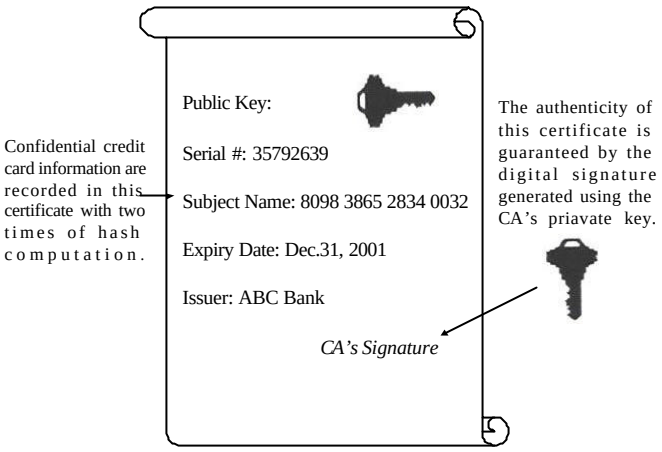

Figure 5. An illustration of a SET certificate

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 verifying the consistency between the certificate and PI, the acquirer still can verifies the card information without knowing the cardholder's detail in this case. Hence the cardholder's detail information is only known to the issuer and the cardholder. This meets the basic privacy requirement in the previous section.

PRIVACY ANALYSIS

SSL

SSL encrypts the link between the cardholder and the merchant to provide confidentiality and integrity of transmitted card information. It is inadequate because it protects transaction details only when it is in the transmission channel; once the information has arrived at the web site, it will be decrypted to plain text which leaves no ways to prevent any kind of frauds. Some malicious merchants may use the cardholder's credit card information that provides the key element needed to counterfeit cards and/or to proceed fraudulent transactions.

SET

SET has the following shortcomings.

1. The issuer has to trust the acquirer's verification about the cardholder's signature on PI. After sending the authorization response to the merchant via the acquirer, the issuer guarantees the merchant for the payment.

Bearing the risk of false payment, the issuer should validate that whether PI is indeed signed by the cardholder to commit the payment. However, the cardholder's signature is verified by the acquirer instead. Hence in the original SET, the issuer has to rely on the trust relationship with the acquirer completely.

2. The cardholder's credit card number is revealed to the acquirer. It is the issuer that decides whether the payment is approved or not. The acquirer simply forwards the authorization response received from the issuer to the merchant. The acquirer does not need to know the cardholder's card information to perform its function.
3. The issuer knows all merchants whom the consumer has made his/her transactions with.

3D SET

Credit card number can be sealed from the acquirer using pseudo card number assigned by the issuer. However, server side wallet resided at the issuer routes purchase requests from the cardholder, and communicates with other SET components (merchant, acquirer and CA). It stores the cardholder's private key, certificate, account information, purchase transaction detail and history. The cardholder's buying habit can thus be aggregated and analyzed. Moreover, the acquirer manages server side merchant server for merchants. Both PI and OI are open to the acquirer.

Namely, 3D SET reduces the loading of the cardholder and the merchant, trying to fit in the newly emerged environment of mobile transactions. The merchant no longer needs to set up a merchant server to participate in this architecture. To the contrary, 3D SET increases the loading of banks, and removes the right of the cardholder and the merchant to control their individual information. Such scenario is a negative impact on the issue of privacy protection.

The proposed methods

Our two revisions on SET are discussed respectively as the followings:

Method 1.

1. The cardholder's credit card number is concealed from the acquirer. It is the issuer to decide whether this transaction is approved. The acquirer only forward encrypted PI received from the cardholder via 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 the acquirer cannot decrypt the encrypted PI, the cardholder's credit card number is protected from the acquirer.
2. The issuer keeps non-repudiation evidence by itself for future dispute solving. Cardholder's signature on PI represents cardholder's authorization on this payment, it is the only evidence that the issuer needs to hold against cardholder's repudiation.
3. The issuer does not know which merchant the cardholder deal with.
4. The increased efficiency by simplifying the certificate verification process. On-line payment involves money transfer. Strict certificate verification, including certificate chain setting and CRL check, is needed to authenticate participants. Many complicated certificate verifications are needed in a transaction using SET, the cardholder need to verify the acquirer's certificate by traversing the trust chain to the root key to get the acquirer's public key for encrypting the digital envelop of PI. The acquirer also has to validate the cardholder's certificate by traversing the trust chain to the root key and check revocation status to get the cardholder's valid public key for verifying the cardholder's signature on PI. Because no existing trust is built up between the cardholder and the acquirer, the complex mutual certificate verification must be done carefully to avoid dispute. In the proposed method, using the existing trust relationship built between the cardholder and the issuer, PI is verified by the issuer, not the acquirer, to simplify the certificate verification and reduce potential risk.

Method 2.

We suggest that the cardholder's sensitive information should be stored in the certificate after two times of hash computation. In that case, only hashed credit card information, H(credit card information), has to be recorded in PI, and the acquirer may verify the validity of the credit card without knowing the detail information of the cardholder. The cardholder's privacy is thus secured.

Recording twice-hashed credit card information in the cardholder's certificate may raise some security concerns. Due to the characteristics of hash function, the possibility of collision may increases, which means that different cardholders may have exactly the same hashed information recorded on their certificate. This case reduces the authenticity of cardholders. The serial number of a cardholder certificate can be concatenated as part of the input of the second hash computation. This unique number may effectively reduce the occurrence of collision.

CONCLUSION

Credit card is a popular mean for customers to pay on-line. However, the privacy protection issue poses a major concern to most customers. To encourage the development of electronic commerce, privacy protection mechanisms should be improved to build up consumers' confidence. In this paper, we summarize the requirements for protecting cardholders' privacy, analyze the privacy protection on three common payment protocols, such as SSL, SET and 3D SET, and propose two methods to enhance privacy protection in the context of on-line credit card payment.

REFERENCES

[1] CyberSource Corp. (2000), "CyberSource Fraud Survey", http://www.cybersource.org/fraud_survey

[2] The National Consumers League, http://www.fraud.org/news/1999/oct99/102099.htm
[3] CyberSource Corp. (2000), "CyberSource Fraud 2000 Survey for UK", http://www.cybersource.com/solutions/risk_management/uk_fraud_survey.xml
[4] MasterCard and VISA (1997), *Secure Electronic Transaction (SET) Specification, Book 1: Business Description (version 1.0).*
[5] MasterCard and VISA (1997), *Secure Electronic Transaction (SET) Specification, Book 2: Programmer's guide (version 1.0).*
[6] MasterCard and VISA (1997), *Secure Electronic Transaction (SET) Specification, Book 3: Formal Protocol Definition (version 1.0).*
[7] J.J. Hwang and S.C. Hsueh (1998), "Greater Protection for Credit Card holders: a revised SET protocol", *computer standards & interfaces*, (19), pp.1-8.
[8] VISA EU, "3D SET", http://www.visa.be/pd/eu_shop/merchants/3d_set/main.html