Abstract:
Electronic payment is the very important step of the electronic business system, and its security must be ensured. SSL/TLS and SET are two widely discussed means of securing online credit card payments. Because of implementation issues, SET has not really been adopted by e-commerce participants, whereas, despite the fact that it does not address all security issues, SSL/TLS is commonly used for Internet e-commerce security. The three-domain (3D) security schemes, including 3-D Secure and 3D SET have recently been proposed as ways of improving ecommerce transaction security. Based on our research about SSL, SET, 3D security schemes and the requirements of electronic payment, we designed a secure and efficient E-Payment protocol. The new protocol offers an extra layer of protection for cardholders and merchants. Customers are asked to enter an additional password after checkout completion to verify they are truly the cardholder, the authentication is done directly between the cardholder and card issuer using the issuer security certificate and without involving the third party (Visa, MasterCard).

Keywords:
E-commerce, Secure Socket Layer (SSL), Secure Electronic Transaction (SET), 3D-Secure

1. Introduction

Electronic commerce or e-commerce provides participants, including consumers and merchants, with a number of benefits, such as convenience and time savings. E-commerce transactions can be categorized into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government [1]; we focus on B2C transactions in this paper. In B2C transactions, the credit card is the most widely used method of payment for Internet ecommerce transactions. According to an Internet shopping habits survey conducted by Survey.Net (http://www.survey.net), 36% of Internet users purchase goods by transmitting their credit card number via a secure form; the percentages for other payment methods are significantly lower. Given that the debit/credit card is the primary means for consumers to purchase products or services online, the possible compromise of credit card numbers is a serious threat to the consumer. The E-payment system brings users with higher efficiency, credibility and speeding-up transactions settlement, which reduce the pay risks caused by time lags in handling the bills. However, it also comes with new risks, i.e. security problem of transactions.

The research reported here builds on the electronic payment security; we study the security of e-commerce protocols and we propose a new efficient protocol to ensure a high security for electronic payment transactions.

The objective of our protocol is to provide issuers with the ability to authenticate cardholders during an online purchase without involving the third party VISA or MasterCard. We define a new transaction flow involving cardholder, merchant, payment gateway and card issuer, and allowed parties to identify themselves to each other and exchange information securely using digital certificate. For some implementation reasons, the cardholder is not requested to have his digital certificate, he use the password code to be authenticated by the card issuer.

2. Security Requirements of E-Payment

It goes as follows [2]:

2.1 Information confidentiality

All information during the transactions has the request of being kept confidential. For instance, account number and user name may be embezzled by others who
have access to them; business opportunity may be lost if
order and payment information of your customer’s are
obtained by competitors. Thus, encryption is required in
the E-C information transmission.

2.2 Data integrity

E-C should provide medium to identify data
integration, ensuring the Web data do not be altered in
transmission.

2.3 Authentication of participants

The parts involved may have never met each
other. So to make the transaction successful, the first step
is to identify the two parts, which is the essential
prerequisite of transactions.

2.4 Non-repudiation

The transaction must have such services that
enable one party to prevent another party denying having
taken a particular action, e.g. sending order/payment
information, confirmation of order/payment. Both
consumer and merchant also require this service.

2.5 End-user implementation Requirements

We focus here on the major barriers causing
implementation failures in SET and other protocols
including usability, flexibility, affordability, speed of
transaction, and interoperability.

- **Usability**  – The system must be easy to implement,
  including installation. The consumer requires the card
  issuer and merchant to provide a secure system that is
  not complex, while the merchant requires the acquirer
  and security software developers to provide a simple
  application that meets the security requirements.

- **Flexibility** – The system must allow e-commerce
  consumers to order products or services from any
  location, and not just from one PC. Here, the
  consumer is the entity requiring the flexibility service,
  while the merchant is the entity providing the service.

- **Affordability** – The costs of implementing and using
  the system must be affordable for consumers and
  merchants, since these end-users are unlikely to be
  prepared to pay significantly extra to participate in
  Internet e-commerce transactions. For example,
  consumers are not willing to pay for a digital
certificate in order to conduct e-commerce
transactions although it is required in some e-
payment scheme such a SET . Merchants will also not
wish to invest significantly in engineering e-payment
infrastructure.

- **Reliability** – The system must be reliable since it is
  used for the transmission and manipulation of
  sensitive information.

- **Availability** – The system must be available when
  needed.

- **Speed of transaction** – The transaction speed must
  be acceptable for e-commerce end-users.

- **Interoperability** – The system must be interoperable
  between different computing platforms, web browsers
  and server software packages in order to enable its
  use by the widest possible spectrum of e-commerce
  consumers and merchants.

E-C secure protocols are the widely recognizes
logical operating standards for secure completion of
information exchange, as well as the critical technique to
ensure the confidentiality, integrity, authentication and
non-repudiation of online transactions. Their completion
serves as a key to provide online security. Internet E-C
security protocol is the central research areas in E-C as the
endeavors to promote the development of E-C, and
guarantee its security. The prevalent protocols are
Security Socket Layer (SSL), Secure Electronic
Transactions (SET) and 3D-Secure.

These protocols allow using cryptography to
send confidential information on the Internet without
being readable to malicious individuals. However, it
turned out that these protocols are not as secure as we
thought they would be. Indeed, several errors were
discovered in cryptographic protocols after some years of
use. The consequences that can generate vulnerability in
a cryptographic protocol can be costly
and irreversible for companies and individuals.

In this paper, we consider how E-commerce
security requirements are fulfilled by our new protocol
based on payment gateway and digital signature.

3. Related Work

There have been many studies of E-commerce
security. Security in E-commerce was described in the
paper written by Dhilon [3] who introduce the stages to be
provided for online purchase, the approach is based on
encryption and compression for making information
unreadable. However, E-commerce security has become a
consistent and growing problem as new internet
technologies and application are developed; it needs new
architecture to adapt to many changes. Al-SLamy [4]
described the role of Pretty Good Privacy (PGP) to
provide confidentiality, authentication, compression and
segmentation services for E-commerce security. Byung
Secure Sockets Layer (SSL) is a commonly used protocol used to encrypt messages between web browsers and web servers [7]. It encrypts the datagrams of the Transport Layer protocols. SSL is also widely used by merchants to protect the consumer’s information during transmission, such as credit card numbers and other sensitive information. SSL is used to provide security and data integrity over the Internet and thus plays an important role. SSL has now become part of Transport Layer Security (TLS), which is an overall security protocol. One of the major problems of SSL is that the merchant can store the sensitive information of the cardholder, and the protocol does not prevent the non-repudiation because the client authentication is optional.

SET (Secure Electronic Transaction) come to resolve the weakness of SSL in authentication and protection of sensitive information, SET ensures payment integrity, confidentiality and authentication of merchants and cardholders [8]. But SET is characterized by the complexity and the cost supported by the merchant (compared to the alternative proposed by SSL) because of the logistics of certificates distributing and client software installation, also it’s difficult to manage non-repudiation. To deal with it, VISA introduce 3D-secure [9], this protocol is based on the introduction of additional control when buying online in addition to the classic sensitive cardholder data. The customer validates the payment in new window by entering a secret data agreed with its own bank (password, date of birth, code received by SMS or generated by a personal drive).

4. Secure Electronic Payment Protocol Design

Our main idea is to design a secure and efficient protocol to protect online payment transactions against the fraud without involving the third party, our protocol respond to the requirements of e-payment security: confidentiality, integrity, authentication and non-repudiation.

Our Secure Electronic Payment (SEP) protocol avoids the complexities relating to the implementation unlike SET and 3D-secure, integration and utilization are also easier than before.

For the convenience of written expression, we use the following notational conventions in this paper.

- **C**: Cardholder
- **M**: Merchant
- **PG**: Payment Gateway
- **IB**: Issuer Bank or Cardholder Bank
- **CA**: Certificate authority
- **Vshop**: Virtual Shopping Site
- **PAN**: Card Number
- **CVV2**: Card Verification Value or Crypto (three digits)
- **ExD**: Expiry date of the card
- **OI**: Order Information
- **PI**: Payment Instructions
- **OIMD**: OI Message Digest
- **PIMD**: PI Message Digest
- **POMD**: Payment Order Message Digest
- **K**: Symmetric key generated randomly
- **Kum**: Public key of merchant
- **Kupg**: Public key of payment gateway
- **Kuis**: Public key of issuer bank
- **Krm**: Private key of merchant
- **Krpg**: Private key of payment gateway
- **Kris**: Private key of issuer bank
- **S**: Sign
- **E**: Encrypt
- **D**: Decrypt
- **V**: Verify signature
- **H**: Hash
- **||**: Concatenation
- **#**: Disconnect
- **Eq**: Equal

Our SEP protocol includes the following entities (see figure 1):
Figure 2. Description of SEP protocol

A. Registration process

Merchant, payment gateway and issuer bank should register and obtain certificates from certificate authority (CA) before they involve in the SEP transaction. Cardholder should register and obtain a password from his issuer bank (IB) before he involve in the SEP transaction.

B. Purchase Request

Cardholder browses for items, select items to be purchased from the Vshop and get an order which contain the list of items to be purchased. Before stating purchase the cardholder and the merchant agree upon the order description amount. The cardholder then sends to the merchant his local ID and a fresh random challenge. The purpose of this is to give the cardholder with the merchant's signature certificate and the payment encryption certificate.

1- Cardholder generates OI, encrypted PI and dual signature. The dual signature is encrypted under a symmetric key generated randomly for the encryption; the cardholder is not requested to have own certificate (see figure 3).

2- Cardholder prepares the purchase request and sends it to the merchant (see figure 4).

3- The merchant extract the symmetric key, process the OI and transmit the encrypted PI to the payment gateway. (see figure 5)

C. Authorization Request

1- Merchant signs and sends authorization request to payment gateway, he sends the symmetric key K1 used for dual signature, the encrypted PI. The authorization request is encrypted under a symmetric key generated randomly. The payment gateway verifies the dual signature and gets PI. (see figure 5)

2- The payment gateway transmits the authorization with PI to the issuer bank through a secure and private interbank financial network. (see figure 6)

D. Authorization Response

1- The issuer bank verifies PI, verifies authorization request and run some issuer controls to check if the cardholder is allowed to make this transaction.

2- The issuer sends an authorization response and issuer bank certificate to the payment gateway through the secure interbank financial network (see figure 7). The authorization response contains the response code and the action code. The response code indicates if the authorization request is approved or no, the action code indicates if the cardholder is asked to be authenticated using his password. The purpose of this step is to give the cardholder with issuer bank encryption certificate.

3- The payment gateway signs and sends the authorization response and issuer certificate to the merchant. (see figure 8). The merchant check the action code, if the action code equals to ‘Y’ which mean that the cardholder should be authenticated then, the merchant sends an authentication request to the cardholder containing the issuer certificate and some authorization data(see figure 9).

E. Cardholder Authentication Request
1- The cardholder verifies the issuer certificates and sends his personal password encrypted under the symmetric key.(see figure 10)

2- The merchant verifies the authorization data and transmit the encrypted password to the payment gateway.(see figure 11)

3- The payment gateway verifies authorization data, the hash of the encrypted password and transmits the encrypted password to the issuer for verification. The issuer decrypts the encrypted password and checks if is it the correct one for this cardholder.(see figure 12)

F. Cardholder Authentication Response and final payment

1- The issuer bank decrypts and verifies the password code, ensures the consistency between the authorization request and cardholder authentication request, debits the cardholder account and sends a payment response to the payment gateway. (see figure 13)

2- Finally the payment gateway transmits the payment response to the merchant (see figure 14). Merchant verifies the response and ships the good to the cardholder.

Figure 4. Purchase request from cardholder to merchant
Figure 5. Authorization request from merchant to payment gateway

Figure 6. Authorization request from payment gateway to issuer bank

Figure 7. Authorization response from issuer bank to payment gateway

Figure 8. Authorization response from payment gateway to merchant
Figure 9. Authorization response from merchant to cardholder

Figure 10. Cardholder authentication request from cardholder to merchant

Figure 11. Cardholder authentication request from merchant to payment gateway

Figure 12. Cardholder authentication request from payment gateway to issuer
4.1 SEP and Information Confidentiality

For each step of transmission a symmetric key is generated randomly to encrypt electronic payment data. The encryption prevents the illegal information access and information stealed in transmission.

4.2 SEP and Authentication

- Cardholder authenticates merchant and issuer bank
- Merchant authenticates payment gateway and issuer bank
- Payment gateway authenticates merchant and issuer bank
- Issuer bank authenticates cardholder using the password code.

4.3 SEP and Information Integrity

Data integrity is ensured by using MACs (Message Authentication Code) based on hash functions MD5 (16 bytes) or SHA-1 (20 bytes). The MAC is sent for every message transmitted between ecommerce actors.

4.4 SEP and Non-Repudiation

The non-repudiation property is guarantee by using the password code during the cardholder authentication request. The issuer bank authenticates the card and the cardholder, so the cardholder can not deny the fact that he had sent information afterwards.

4.5 SEP and End-user Implementation Requirements

- Usability: cardholder, merchant needs to install a special plug. The initialization process is so simple, since the cardholder does not need to have his certificate.
- Flexibility: SEP protocol have the desirable property that it can be used from any PC, as is currently the case for e-commerce transactions relying simply on SSL/TLS for cardholder-merchant communication security.
- Affordability: if we compare SEP with 3D-Secure, 3D-Secure needs more investment in term of connectivity with VISA and ACS setup cost, also the merchant should be able to manage the cardholder authentication redirection to VISA. SEP needs just the attribution of security certificates to merchant, payment gateway and issuer bank, and plug-in setup.
- Reliability: Of course, whilst the presence of incorrect functionality in security critical elements of SEP protocol is unlikely, there is still a significant possibility that accidental
vulnerabilities will be present in implementation. Past experience indicates that it is very difficult to produce software which does not possess vulnerabilities exploitable by malicious software.

- **Availability:** Unlike 3D-Secure, for SEP protocol card issuers and acquirers are not required to implement any system with VISA. Once the issuer has the software, they can support SEP transactions. Equally, consumer will be happy to perform a simple registration process to get the password coder and install the plug-in, no security certificate is needed.

- **Speed of transaction:** SEP protocol employs DES for symmetric encryption and RSA for certificate verification. The issuer verification of cardholder identity is an important factor for transaction performance. The SEP protocol avoid the complexity of 3D-Secure related to Visa directory. It’s difficult to decide about transaction speed because it’s related also to networking speed and server’s performance.

- **Interoperability:** SEP plug-ins can be installed on the consumer PC easily, so interoperability issues are less likely to arise.

5. **Conclusion**

SEP protocol is a good transaction protocol for credit card payment. In this paper we improved how well SEP protocol meets the e-payment security requirements and identified end-user implementation requirement. A future research topic is to analysis the security and the performance of our protocol.

**REFERENCES**


