A Comparative Study of Secure Electronic Transaction Mechanisms for E-Commerce

RongJou Yang 1, Hann-Jang Ho 2, and I-Ming Shieh 1
1 Department of Information Management
2 Department of Computer Science and Information Engineering
WuFeng Institute of Technology
117, Chian-Kuo Rd., Sec. 2, Ming-Hsiung, Chia-yi 621
Taiwan

Abstract: - It is mandatory how to proceed with the transaction of on-line ordering and, in the meantime, to obtain proper protection of data security. Currently, there are three ways for secure electronic payment mechanism of credit card: Secure Socket Layer (SSL), Secure Electronic Transaction (SET), and 3D Secure. Although the secure connection mechanisms can be modified to be applied to the mobile device, this paper focuses on the comparison and analysis of the secure connection mechanisms for electronic commerce. We discuss the advantages and shortcoming of these secure transaction mechanisms.

Key-Words: - Digital Certificate, PKI, Digital Signature, TLS, SSL, SET, 3Dsecure

1 Introduction
Since the invention of World Wide Web (WWW) by Tim Berners-Lee in 1990, Internet has gradually been employed to conduct the marketing activities and change the buying behavior of consumers following the development of EC-related technology. E-Commerce has numerously been employed as another virtual channel which is different from traditional brick-and-mortar channel in order to create business opportunity. Internet population increases rapidly following the rising and flourishing development of Internet. According to the investigation by ACI-FIND, Institute of Information Industry, Taiwan, the Internet population arrives 8 million and 920 thousands (39%) by June, 2004, which is 80 thousands more than in 2003 and has a 1% growth rate. Commercial Internet accounts arrived 1 million including most of the mobile accounts [1] which means much more enterprise have entered the EC market.

Security is still a big issue concerning Internet shopping. According to eBrain Market Research, Consumer Electronics Association (CEA) conducted an investigation on the consumers’ intention of Internet shopping so as to understand the favorites of consumers and found that the lower price of the product is still one of the key factors and the convenience, privacy, and security are the next. Also, according to the investigation on the mandatory factors of Internet shopping from Princeton Survey Research Associates for Consumer Web Watch, the convenience, security, and trust are three most mandatory factors for consumers [1]. Therefore, the security of Internet shopping is a matter of importance.

According to the investigation on Internet users in Taiwan from Visa with the assistance of ACNielsen consult, Taiwan, most of consumers pay by credit card and Cash on Delivery (COD) the next for the on-line transaction in second half-year, 2002 [2]. Therefore, the security concern of Internet shopping has drawn extra attention in addition to the privacy and the spreading out of fabricated credit card. The security mechanism especially in Internet cash flow based on the credit card payment thus plays a critical role. The security mechanism SSL has first been employed as most popular network data encryption standard. SET, developed by VISA International, MasterCard, and other technical partners, has encountered difficulty since 1996 due to the complicate usage. 3D Secure, developed by VISA International in 2002 to improve the shortcoming of complicate usage, is the future trend although it has less security than SET. SSL data encryption is the most popular solution to enhance the confidence of consumers and assure the security of data.

A digital certificate, issued by a certification authority (CA), is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It contains applicant’s name, a serial number, expiration dates, a copy of the certificate holder's public key which is used for encrypting messages and digital signatures, and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. The digital certificates usually conform to X.509 standard and can be kept in registries so that
a digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message (encrypted or not) or the signer of a document in order to ensure that the original content of the message or document that has been sent is unchanged.

A PKI, known as asymmetric cryptography, uses the public key cryptography, which is the most common method on Internet for authenticating a message sender or encrypting a message consists of a digital certificate, issued by CA which is verified by registration authority (RA), which includes the public key or information about the public key, one or more directories where the certificates (with their public keys) are held, and a certificate management system.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA, an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman) by CA. Then, we can send an encrypted message using the receiver's public key and decrypt an encrypted message using the receiver's private key, or send an encrypted signature using the sender's private key and decrypt an encrypted signature to authenticate the sender using the sender's public key.

A PKI (public key infrastructure) enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and revoke the certificates which can be checked by Web Sentry from Xcert based on the Online Certificate Status Protocol (OCSP).

2 On-line Secure Transaction
Mechanisms
Due to the development of Internet, EC has been vigorously developed in recent years. According to the research report on Internet user behavior in Taiwan, it is indicated that only 22.2% out of 57.7% EC Web site visits of Internet users conducts their on-line transaction mainly because of the lack of a sense of security and privacy except the dislike of the products [1]. Therefore, secure electronic transaction mechanism must be employed to enhance the sense of security and privacy. Some most popular security mechanisms employed in on-line transaction are discussed as follows:

2.1 Secure Sockets Layer (SSL)
SSL [3], developed by Netscape Communicator in 1994, is a mainstream of commonly-used protocol for ensuring the security of a message transmission between client-side and server-side on the Internet by using the technology of cryptography. Private Communications Technology (PCT), developed by Microsoft in 1955, is a modification of SSL v2 to improve the shortcoming and is backward compatible. SSL v3 provides additional features such as NEW encryption algorithm and closure handshake in addition to the additional functionalities in PCT.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. Included as part of both the Microsoft and Netscape browsers and most Web server products and developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use. TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

According to Stalling [4], SSLv3.0 has support for Fortezza (KEA & Skipjack), while TLSv1.0 doesn’t. TLSv1.0 has 9 more alert protocol messages than SSLv3.0 and the cryptographic computations of TLS v1.0 are slight in the Certificate Verify, Finished, MAC generation, and key generation. SSLv3.0’s padding length is the minimum bytes that results in a total length that is a multiple of the cipher’s block length. TLSv1.0’s padding length is any amount up to 255 bytes that results in a total length that is a multiple of the cipher’s block length.
acceleration of EC over the Internet has increased the demand for PKI solutions.

2.1.1 Operating Mode of SSL

SSL protocol provides two-party security protection of Internet transaction in order to prevent the interception, alteration, and destruction of transactional data during the transmission. It is placed between TCP/IP and application and employed to encrypt the data transmitted between client side and server side as indicated in Figure 1 [5].

Fig. 1 Credit Card Processing in SSL Encryption [5]

SSL provides a secure channel between client side and server side and can identify the right originated data source client side. SSL connection is created on top of TCP so that the security protection of data transmission can be achieved with little modification of application. The confidentiality and reliability between two communicated applications are accomplished by using the asymmetry encryption algorithm to exchange the key pair (public and private key) and using the symmetry encryption algorithm to encrypt and decrypt the data.

2.2 Secure Electronic Transaction (SET)

SET is a system for ensuring the security of financial transactions on the Internet. With SET, a user is given a digital certificate (electronic wallet – can be kept in registries so that authenticating users can look up other users' public keys) which is issued by a certification authority (CA) and contains applicant's name, a serial number, expiration dates, a copy of the certificate holder's public key used for encrypting messages and digital signatures, and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the three-party – purchaser, a merchant, and the bank – in a way that ensures privacy and confidentiality.

SET makes use of Secure Sockets Layer (SSL) from Netscape, Secure Transaction Technology (STT) from Microsoft and Visa and Secure Electronic Payment Protocol (SEPP) [6] from Mastercard, and Secure Hypertext Transfer Protocol (S-HTTP) from Terisa System. Based on Internet Keyed Payments Protocol (iKP) [7] from MasterCard, IBM, Netscape, GTE, and Cybercash, an architecture for secure payments involving three or more parties, SET also uses some aspects of a public key infrastructure (PKI) which enables users of a basically insecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

SET protocol provides a strict and complete security mechanism which involves three-party (consumer, merchant, and card issuers) authentication. However, the consumers must install the e-wallet provided by card issuer. It is quite inconvenient to use. Therefore, comes another security mechanism 3D Secure which is discussed in 2.3.

2.2.1 Operating Mode of SET

Assume that a customer has a SET-enabled browser and that the transaction provider has a SET-enabled server. SET protocol works as follows and is indicated as in Figure 2:

1. The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank. The customer receives a digital certificate.

2. This electronic file functions as a credit card for online purchases or other transactions. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.

3. Third-party merchants also receive certificates from the bank. These certificates include the merchant's public key and the bank's public key.

4. The customer places an order over a Web page, by phone, or some other means.

5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.

6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.

7. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by referring the certificate to the bank or to a third-party verifier.
(8) The merchant sends the order message along to
the bank. This includes the bank's public key, the
customer's payment information (which the
merchant can't decode), and the merchant's
certificate.

(9) The bank verifies the merchant and the message.
The bank uses the digital signature on the
certificate with the message and verifies the
payment part of the message.

The bank digitally signs and sends authorization to the
merchant, who can then fill the order.

2.3 3D Secure
3-D Secure, developed by Visa International, is based
on the Three Domain Model of payment systems
which are Issuer Domain, Acquirer Domain, and
Interoperability Domain. In 3D Secure, cardholder
identity is confirmed by using issuer-defined
validation process, prior to authentication processing.
SSL/TLS is employed to enable secure and reliable
communication channels between cardholder and
issuer using a server certificate and the strongest
cryptography the cardholder browser supports and to
provide confidentiality of payment and order
information by using underlying transport-level
strong cryptographic facilities. For each purchase,
successful authentication dialog between cardholder
and issuer is to ensure that the person presenting a
payment card is entitled to use that card.
Authenticated, secure communication channels
among all non-cardholder entities are established by
using cryptographically strong facilities.

SSL/TLS sessions are established only with
known parties who are authenticated using
certificates or who log on using Visa-managed ID
and password. Visa-enabled strong issuer digital
signature on authentication response is employed to
ensure integrity of authentication response and
confirmation that the response originated from the
card issuer. The features of 3-D Secure Protocol are
as follows:

(1) Provides global framework for the authentication
of remote payments.

(2) Reduces operational expense by minimizing
chargebacks for unauthorized use.

(3) Can be implemented without requiring
specialized cardholder software or hardware?

(4) Can be enhanced by the issuer as needed to meet
customer management and security requirements
without impact on the acquirer or merchant?

(5) Is extensible into emerging channels such as
mobile telephones, PDAs, and digital TV?

(6) Is based on globally accepted technical standards
provided by international standards bodies such
as the Internet Engineering Task Force (IETF)?

(7) Provides a centralized archive of payment
authorizations for use in dispute resolution.

2.3.1 Operating Mode of 3D Secure
3-D Secure within the Three Domain Model is
indicated in Figure 3. The basic functions of 3-D
Secure are as follows:

(1) Messages to request and receive the results of
authentication flow between the Acquirer and the
Issuer Domains within the Interoperability
Domain via the Internet.

(2) Messages to perform cardholder authentication
flow between the cardholder and the issuer
within the Issuer Domain.

(3) Messages to request authorization and payment
processing flow between the merchant and the
acquirer within the Acquirer Domain.

(4) Messages to perform authorization and payment
processing flow between the acquirer and the
issuer within the Interoperability Domain via
VisaNet.

Transport security is always required in that some
3-D Secure messages have built-in provisions for
security that are independent of the transport
technology and others depend upon security
techniques provided by the transporting facilities.
Messages in 3-D Secure flow among entities both
within and between the three domains. Various
fundamental technologies that are used to protect the
confidentiality of those messages and to ensure the
authenticity of the parties sending and receiving the
messages are as follows:

(1) ID and password

(2) Public key cryptography including digital
certificates
(3) Hardware security modules

(4) Practices and procedures prescribed by published Visa policies and guidelines

(5) Digital signatures (used to ensure that the authentication response from the issuer Access Control Server is valid)

(6) Transport level security

The 3D Secure Purchase Transaction Flow is indicated in Figure 4 as follows:

(1) Shopper browses at a merchant site, selects items, and then finalizes the purchase. The merchant has all the necessary data, including card number and user device information.

(2) The Merchant Server Plug-in (MPI) sends the PAN (and user device information, if applicable) to the Visa Directory Server.

(3) Visa Directory Server queries the appropriate Access Control Server (ACS) to determine whether authentication (or proof of attempted authentication) is available for the PAN and device type. If an appropriate ACS is not available, the Visa Directory Server creates a response for the MPI and processing continues with Step 5.

(4) The ACS responds to the Visa Directory Server, indicating whether authentication (or proof of attempted authentication) is available for the card number.

(5) The Visa Directory Server forwards the ACS response (or its own) to the MPI. If neither authentication nor proof of attempted authentication is available, the merchant, acquirer, or payment processor submits a traditional authorization request.

(6) The MPI sends a Payer Authentication Request (PAReq) to the ACS via the shopper’s device.

(7) The ACS receives the PAReq.

(8) The ACS either authenticates the shopper by using processes applicable to the card number (password, chip, PIN, etc.) or if attempts ACS functionality is available, creates the proof of authentication attempt.

(9) The ACS then formats the PARes message with the appropriate values and signs it.

(10) The ACS returns the PARes to the MPI via the shopper’s device.

(11) The ACS sends selected data to the Authentication History Server (AHS).

(12) The MPI receives the PARes. The MPI validates the PARes signature (either by performing the validation itself or by passing the message to a separate Validation Server). If appropriate, the merchant proceeds with the authorization exchange with its acquirer.

3 Comparison of Secure Transaction Mechanism

The comparison of three on-line secure transaction mechanisms: SSL, SET, and 3D Secure is indicated in Table 2.
Tab. 2 Comparison of SSL, SET, and 3D Secure

<table>
<thead>
<tr>
<th>Functionality</th>
<th>SSL</th>
<th>SET</th>
<th>3D Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate and Standard Specification</td>
<td>Client-side certificate only and not strict identification</td>
<td>Mandatory and strict identification</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Privacy</td>
<td>Protected through client-server point to point encryption (RC4, RC5, DES, IDEA, Triple DES)</td>
<td>Transaction information protected through DES key hashing code while card information through RSA digital envelope hashing code or triple DES key</td>
<td>Transaction information protected through encryption</td>
</tr>
<tr>
<td>Integration</td>
<td>Symmetric cryptography; Message checked by keyed MAC computations (MD5, SHA-1)</td>
<td>Message protected with SHA-1 digest and digital signature</td>
<td>Assured with message certificate</td>
</tr>
<tr>
<td>Authentication</td>
<td>Asymmetric or public key cryptography</td>
<td>Through content and sender’s digital signature of each transaction</td>
<td>Through password verification of cardholder</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Deficiency</td>
<td>Through content and receiver’s digital signature of each transaction</td>
<td>Through complete log information</td>
</tr>
</tbody>
</table>

4 Conclusion

Secure payment mechanisms can set consumers’ mind at ease to conduct the on-line transactions. It also provides the convenience for consumers by applying it to mobile device. This paper investigates the on-line security mechanisms and its application in mobile EC. A secure payment mechanism is an efficient instrument to promote EC. This paper investigates the mainstream of secure payment mechanism: SSL, SET, and 3D Secure. SSL is inadequate. SET is inconvenient while better than SSL in security concern. 3D Secure, based on SSL, improves the shortcoming of SET and is more convenient in use while not so strict as SET concerning the security.

Acknowledgement

This work was supported by NSC, Taiwan under grant no. NSC-94-2622-E-274-002-CC3.

References:


