A Survey of E-Commerce Security

QIN Zhiguang, LUO Xucheng, GAO Rong
(School of Management, University of Electronic Science and Technology of China Chengdu 610054 China)

Abstract E-commerce is a very active field of Internet research. A very important aspect of e-commerce is its security. Because of the variety of e-commerce applications, many security policies, protocols and techniques are involved in the deployment of the security. The related standards and protocols of e-commerce are studied in this paper. The general model of e-commerce security is set forth. In this model, two most important e-commerce protocols including secure sockets layer (SSL) and secure electronic transaction (SET) are analyzed. The open problems and new trends of e-commerce security are presented.

Key words e-commerce security; SSL; SET; new trends

E-commerce is business that is conducted on the Internet using any of the applications that rely on the Internet, such as e-mail, instant messaging, shopping carts, web services, universal description, discovery and integration (UDDI), file transport protocol (FTP), and electronic data interchange (EDI), among others. Electronic commerce can be between two businesses transmitting funds, goods, services and/or data or between a business and a customer\cite{1}. In SEMPER\cite{2}, the term electronic commerce is generally understood to span the whole range of business situations that are at least partially supported by a communication network such as Internet. In spite of all kinds of definitions, the essential point of e-commerce is that the business is operated by means of computer network, especially Internet. E-commerce activities include establishing and maintaining online relationships between an organization and its suppliers, dealers, customers, strategic partners, regulators, and other agents related to (or in support of) traditional delivery channels\cite{3}. Other activities include: 1) Merchandise searches and comparisons by consumers; 2) Merchandise information presentation and promotion by manufacturers and retailers; 3) Post-purchase customer support; 4) Communication between/among participants of business; 5) Other activities that are not directly related to the transaction itself.

E-commerce is more efficient than traditional commerce, so it will finally supplant the latter. In recent years, the research of E-commerce is very active. Many protocols are proposed and a lot of e-commerce support platforms such as WebSphere are developed. According to the definitions of e-commerce, the business processes are operated by means of computer network. Thus, we can say that the security of e-commerce is composed of two layers. The foundation is network security and the upper layer is application-specific security. Since the commercial property of e-commerce, Security is crucial to e-commerce. However, e-commerce has its own properties. The requirements of e-commerce security must be confirmed and the problems related must be solved. In this paper, the general model of e-commerce security is set forth, two e-commerce protocols including secure sockets layer (SSL)\cite{4} and secure electronic transaction (SET)\cite{5} are analyzed, and the open problems and new trends are presented.

1 The General Model of E-Commerce Security

E-commerce is a very important Internet application. The foundation of e-commerce security is network security. According to the properties of e-commerce, we educe the requirements of
e-commerce security.

1) Confidentiality. This requirement prevents unauthorized disclosure of information. It can be done by means of symmetric encryption algorithms such as DES, AES.

2) Integrity. This requirement ensures that information is protected from unauthorized alterations, unintentional modifications, or change. Message Authentication Code is used to do this.

3) Availability. This requirement ensures that information and critical services are available when needed to meet business requirements. It requires many security techniques and involves several aspects of information security. For example, the intrusion detection and prevention, disaster recovery, and so on.

4) Non-repudiation. This requirement assures that a specific action occurred. It comprises of non-repudiation of origin, non-repudiation of submission, non-repudiation of receipt, and non-repudiation of delivery. Digital signature is an approach to guarantee this.

5) Fairness. This requirement ensures that situations like payment without delivery, or delivery without payment, do not happen. Fairness is tightly related to non-repudiation. Many protocols such as Ref.[6] present have been developed to address this problem.

E-commerce operates on Internet or intranet. The main transaction models are B2B and B2C. In order to identify or authenticate the identity of the other party on the Internet, public key infrastructure (PKI) offers the best support for this requirement. Based on PKI, several security services can be implemented. These security services include digital signature and key management. The most important e-commerce protocols are SSL and SET which are built upon PKI and other cryptographic primitives. SSL is above TCP layer and below application layer. It is used to support secure web transaction. SSL provides a solution to the identity authentication, confidentiality and integrity of transaction. SET is an open protocol which is designed to protect the credit card transaction on the Internet. In SSL and SET there are other cryptographic primitives such as symmetric key encryptions used. There are other protocols which solve the specific problems of e-commerce. In Ref.[7~11], the non-repudiation and fairness are discussed and several protocols or variations are proposed. With the development of e-commerce, new e-commerce protocol will emerge. We think the new protocols will build upon the PKI and other cryptographic primitives as existing protocols. Upon these e-commerce protocols, the specific e-commerce applications can be developed. According to different applications, the different security policy and protocols should be adapted, and many technologies will be dealt with. In a general way, we introduce a general model of e-commerce security from the perspective of security (not from the viewpoint of network protocol stack). The general model can meet the requirements of e-commerce security. This model is depicted in Fig.1. Following this model, we will describe the SSL and SET.

![Fig.1 General model of e-commerce security](image)

2 Two Most Important E-Commerce Protocols

The two most important e-commerce protocols are SSL and SET. In the general model, the two protocols are above the information security infrastructure such as PKI and below the specific e-commerce applications. Nowadays, almost all e-commerce applications are built upon SSL or SET. We discuss the two protocols in the following.

2.1 SSL

SSL is designed to supply an end-to-end security service over TCP. This protocol was presented by Netscape communication and evolved into an Internet standard which is called transport layer security (TLS)[12]. Although there are some differences between SSL and TLS, in this paper, we deem the SSL and TLS...
the same. Fig. 2 is the protocol stack of SSL.

<table>
<thead>
<tr>
<th>Handshake Protocol</th>
<th>Change Cipher Spec Protocol</th>
<th>Alert Protocol</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Record Protocol</td>
<td>TCP</td>
<td>IP</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 2 SSL protocol stack

The SSL protocol includes four sub-protocols: 1) SSL record protocol; 2) SSL handshake protocol; 3) Change Cipher Spec Protocol; 4) Alert Protocol.

Among them, the SSL record protocol and handshake protocol are two major sub-protocols. The SSL record protocol defines the format used to transmit data and provides two services for SSL connections: 1) Confidentiality: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. 2) Message Integrity: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

The SSL handshake protocol involves using the SSL record protocol to exchange a series of messages between an SSL-enabled server and an SSL-enabled client when they first establish an SSL connection. This exchange of messages is designed to facilitate the following actions: 1) Authenticate the server to the client. 2) Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support. 3) Optionally authenticate the client to the server. 4) Use public-key encryption techniques to generate shared secrets. 5) Establish an encrypted SSL connection.

The architecture of SSL is well defined, but there are some problems of the application of SSL. The main attack to SSL is man-in-the-middle attack. SSL allows many key exchange algorithms, but some algorithms such as Diffie-Hellman key exchange have no certificate concept[13]. The participants of a session can’t authenticate each other. The man-in-the-middle attack can be done easily. To avoid this attack, key agreement algorithms with certificates should be adapted. Another problem is that the strength of the encryption in current web browser is not strong enough.

2.2 SET

The SET protocol was created out of a joint effort of MasterCard, Visa and other industries in 1996. The objective of SET is to solve the security of payment on the Internet. SET protocol provides four security services.

1) The confidentiality of the message.

The message of account and payment is secure when it is transported by network. The number of credit cards is known to bank but not to merchants. SET protocol uses DES to support the confidentiality of message.

2) The integrity of data.

The message sent to merchants including subscribing, personal data and payment instructions. Using RSA digital signature and SHA-1 hash function, SET guarantees the messages transported can’t be tampered illegally.

3) Authentication of the cardholder’s account.

Merchants can authenticate the cardholder is the owner of the legal credit card. SET approaches this objective by using the X.509 digital certificate and the RSA digital signature algorithm.

4) Authentication of the merchant.

The cardholder can authenticate the merchant and confirm the business relationship between the merchant and the financial organization. Then, the feasibility of credit card payment can be identified.

The interaction among the business entities in SET is illustrated as Fig. 3. A typical purchase process is depicted in following:

1) The customer registers an account from the bank.

2) The customer receives an electronic certificate which is used for online transaction.

3) The merchant receives the certificates. The merchant must acquire two certificates of his two public key. One public key is used for the signature of the message; the other is used for key exchange. The merchant also needs a copy of certificate of the payment gate.

4) The customer orders the merchandises.
5) The customer authenticates the merchant by
web browser.

6) The web browser sends the order and payment
information. The order information is encrypted by
using public key of the merchant and the payment
information is encrypted by using the public key of the
bank.

7) The merchant requests the payment sanction.
This action guarantees the customer has enough money
to perform this payment.

8) The merchant validates this order and send this
information to customer.

9) The merchant offers the merchandises or
services.

10) The merchant requests payment form payment
gateway.

SET is a comprehensive e-commerce transaction
protocol. It supplies all secure mechanisms in
transaction process. However, the SET protocol is so
complex that the security and correctness need to be
proved.

3 Open Problems and New Trends

Although it has been studied for several years,
e-commerce has not been pervasive. The range of
e-commerce is limited to shopping on the Internet,
Internet auction, B2B business, and so on. However, to
some extent, some current models are not real
e-commerce because the payment is sometimes not
electronic. There are many causes for this state, for
example, the consuming concept of the customer, the
suspicion of the strength of cryptographic algorithms,
and so on. However, the essential cause is that the
e-commerce has not gained the same functions of
traditional business in some aspects. To solve these
problems, we should depend on the e-commerce
security techniques and develop new e-commerce
protocols. We can identify some open problems related
to security:

1) The information security infrastructure is not
well constructed.

In china, the PKI is not constructed nation wide.
Until March 2003, the draft of electronic signature is
approved by State Department.

2) The privacy protection.
Consumers need the privacy protection as in
traditional commerce. Although some works have been
done in this field, the perfect paradigm has not
emerged.

3) The intellectual property protection.
The most suitable commodities for e-commerce
are digital products such as music, movie, e-book, and
so on. However, these products can be easily copied.
The technique of intellectual property protection needs
to be developed.

Although new computing techniques such as web
services and peer-to-peer computing are emerging,
these techniques may attract the e-commerce
advocators to promote the development of e-commerce,
but the essential approach is to win the trust of
e-commerce participants. The new trend of
e-commerce security is trustworthy computing. The
trustworthy computing technique should be developed
and used in e-commerce. But we think there is a long
way to go.

References
Webopedia Computer Dictionary[EB/OL].
http://www.webopedia.com/TERM/e/electronic_commerce
.html, 2004-03-08
Electronic Marketplace for Europe[M]. Lecture Notes in
Computer Science. Berlin: Springer-Verlag, 2004. 1 854
Decision Line, 2001, 32(1): 7-10

(Continued on page 199)