ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

SET & SSL: IS THERE A COMPARISON FOR A GOOD NIGHT SLEEP

Anssi Mattila

Laurea University of Applied Sciences, Leppävaara Unit

Abstract. There are several security protocols that try to secure data traveling over the Internet. Protocols offer security on different layers and to different needs. One of the most important duties for security protocols is to ensure the secrecy of financial information traversing the Internet. Deploying security protocols has many effects depending on the viewpoint. In this paper two most utilized security protocols, Secure Electronic Transaction (SET) and Secure Sockets Layer (SSL) are reviewed.

Keywords: privacy, protocol, security, SET, SSL

1 Introduction

The number of illegal happenings on the Internet is growing logarithmically, while financial institutions are deploying electronic payment systems over the Internet. The need for secure payment systems/protocols to be used in payment transactions is obvious. There already exists secure mechanisms, but why are they not widely in use? Finland has been among the very first to adopt the newest secure payment systems, e.g. Secure Electronic Transaction (SET). SET offers security for customers, merchants and financial institutions. If you are worried about your privacy when using your credit card, e.g. VISA, number during payment transaction on the Net, why wouldn't you do it in safe way when/if it is possible?

While it hasn't been published any serious frauds people seem to think that there is no evident danger, so why to use any odd systems that anyone hasn't even heard being used. Some commercial companies even seem to encourage people to use the unsafe method when paying their *virtual* buyings.

TABLE 1: Barriers of Electronic Commerce [6]

Reason	N	%

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

Lack of trust in overseas transaction	3305	57,4
Lack of security	3199	55,5
Lack of domestic business doing electronic commerce	2587	44,9
Lack of credit card	2451	42,5
The unability to touch the products	2363	41,0
Catalogs of poor quality	1757	30,5
Slow network connections	1381	24,0
Lack of grocery stores on the Internet	981	17,0

According to a survey conducted by Petteri Järvinen [6], the biggest barries that prevent electronic commerce for growing are related to security issues. SET seems to cope with the biggest problems, and there are other security protocols that try to minimize the risk of compromising customer's privacy too.

SET introduces important innovation called dual signature, which makes it possible to link a payment to a order and the other major point is that information sent during a transaction can be read only by the participant to which the information is essential. Other protocols don't ensure this, e.g. Secure Socket Layer (SSL). SET is a special purpose protocol, developed to guarantee security in payment transactions over the Internet.

The security on the Internet has been implemented on different levels of the TCP/IP "stack" (FIGURE 1).The Internet community has developed application-specific security mechnanisms in a number of application areas, including electronic mail (S/MIME,PGP), client/server (Kerberos), SSL for web access and others too (IPSec …).

For the moment the two most utilized security protocols are SET and SSL. First we take a look at SET's basic features and then SSL's. Then a brief comparison is made between these two.

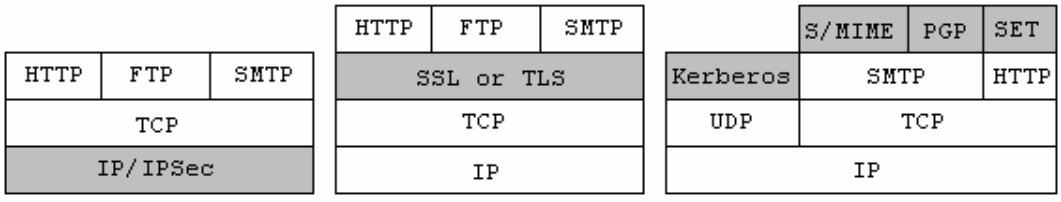

FIGURE 1: Security on the Internet on different layers

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
IJECBS
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

2 Secure Electronic Transaction (SET)

SET is an open encryption and security specification designed to pretect credit card transactions on the Internet. Wide range of companies were involved in developing the initial specification (IBM, Microsoft, Netscape, RSA, Terisa and Verisign.

SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network (e.g. Internet) in a secure fashion. In essence, SET provides three services:

- A secure communication channel among all parties involved in a transaction
- Trust by the use of X.509v3 digital certificates
- Privacy, because the information is only available to parties when and where necessary

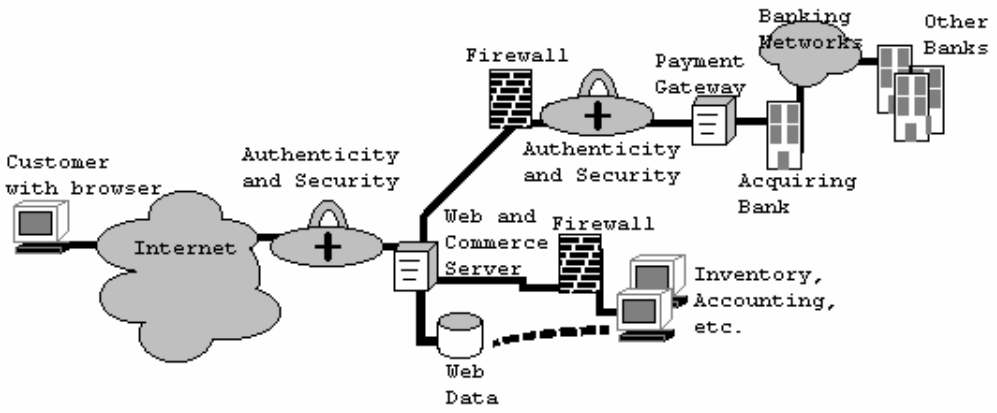

FIGURE 2: E-commerce payment process

There are several participants in SET payment process (FIGURE 2):

- Cardholder: An authorized holder of a payment card (e.g., MasterCard, Visa), that has been issued by an issuer.
- Merchant: A merchant is a person or organization that has goods or services to sell to the cardholder. Of course these goods or services are offered via a Web site or by e-mail.
- Issuer: Issuer is a financial institution (e.g. bank) that provides the cardholder with the payment card.
- Acquirer: The acquirer provides authorization to the merchant that a given card account is active and the proposed purchase doesn't exceed the credit limit, and also provides electronic transfer of payments to the merchant's account.
- Payment Gateway: The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

merchant excanges SET messages with the payment gateway ocer the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

- Certification Authority: An entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants and payment gateways. The existence of CA infrastructure will affect greatly the success of SET.

2.1 Dual signature

SET introduces an important innovation called dual signature (FIGURE 3). The idea of dual signature is to link two different messages that are intended for two different recipients. In this case, the customer wants to send order information to the merchant and the payment information to the bank. There is no need for the merchant to need customer's credit card number, and the bank shouldn't no the details of the order sent to the merchant, but the linkage is needed to prevent certain unwanted situations. There is no way for the merchant to claim that a specific payment is intended for another order than the original. Customer is afforded extra protection (privacy) by keeping these two things separated with this dual signature.

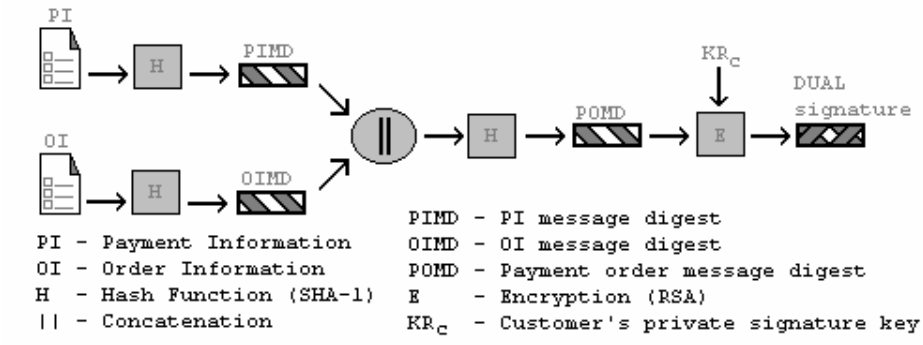

FIGURE 3: Construction of dual signature

The creation of dual signature by the customer could be presented in the following way:

$$DS=E_{KR_C}[H(H(PI)||H(OI))]. \qquad \{1\}$$

Let's suppose that the merchant is in possession of the dual signature (DS), the order information (OI) and the message digest for the payment information (PIMD). The

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

merchant can compute the following two quantities with the customer's public signature key:

$$H(PIMD)||H(OI)) \text{ and } D_{KU_C}[DS]. \quad \{2\}$$

When these two match the merchant has verified the signature. According to the same procedure, the bank is in possession of the customer's PI, the public signature key, the message digest for the order information (OIMD) and DS. Then the bank can verify the signature by testing that the following two quantities match:

$$H(H(PI)||OIMD) \text{ and } D_{KU_C}[DS]. \quad \{3\}$$

It follows from {1},{2} and {3}:

a) The merchant has received OI and verified the signature.
b) The bank has received PI and verified the signature.
c) The customer has linked the OI and PI and can prove the link between them.

How is it *impossible* for the merchant to link a certain payment to another order? The merchant should find order information that helps to create the same order information message digest as the original, which is signed with the customers private signature key. In the case that the message digest is a 128-bit number, the probability to find that message digest is about $1 : 3{,}4 \times 10^{38}$ - how about a longer message digest.

2.2 Payment processing in SET

There are three major transactions that together form the payment process:

- Purchase request: Before purchase request exhange begins, the cardholder has finished browsing, selecting and ordering, and the merchant has sent a completed order form to the customer. All this happens without SET. In order to send SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. When the merchant receives the Purchase Request message from the cardholder, he will perform the following actions:
    1. Verifies the cardholder certificates by means of its CA signatures.
    2. Verifies the dual signature using the customer's public signature key.
    3. Processes the order and forwards the payment information to the payment gateway for authorization.
    4. Sends a purchase response to the cardholder.
- Payment authorization: The payment authorization ensures that the transaction is approved by the issuer, and that the merchant will receive payment.
- Payment capture: This process causes funds to be transferred to the merchant's account. But before this the payment gateway verifies that the merchant is allowed to reveive the payment.

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

3 Secure Sockets Layer (SSL) and Layer Security (TLS)

SSL was originated by Netscape. Version 3 of the protocol was designed with public review and input from industry and was published as an Internet draft document. After submitting the protocol for Internet standardization, the TLS working group was formed within IETF to develop a common standard. The first version of TLS is very close to and backward compatible with SSLv3. [5]

SSL was designed to make use of TCP to provide a reliable end-to-end secure service. SSL is a channel-based security protocol, in other words protocol secures the channel being used. Actually SSL is a protocol ”family” belonging to two different layers (FIGURE 2).

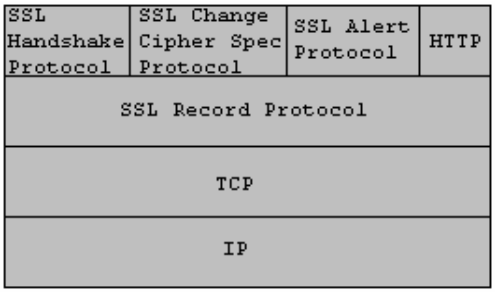

FIGURE 4: SSL protocol ”family”

The SSL Record Protocol provides basic security services (message confidentiality and integrity) to various higher layer protocols. In particular, the hypertext transfer protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL. Three higher layer protocols are defined as part of SSL. The simples SSL-specific protocol is Change Cipher Spec Protocol, which causes the update of cipher suite to be used on a connection. SSL Alert Protocol is used to convey SSL-related alert messages to the peer entity. The most complex SSL protocol is the Handshake Protocol, which allows the client and server to authenticate each other and to negotiate an encryption and message authentication code (MAC) algorithm and cryptographic keys to be used to protect data sent in an SSL record. The Handshake Protocol is used before any application data is transmitted.

SSL is in common use today in many e-commerce servers, and offers ”session-level” security, meaning that once a secure session is established all communication over the Internet is encrypted.

A SSL session is the equivalent of using a scrambler on the telephone line to the catalog merchant. When the data arrives at the merchant’s web site, all the information is decrypted and whether or not it is stored in a secure format is the responsibility of the merchant. The user has no control over the security of their information, he only has to trust the merchant. So,

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

- the cardholder has to trust that the merchant will guard their credit card information securely and the cardholder is assuming a risk in doing so.
- And cardholder has no assurance that the merchant is authorized to accept credit card payment.

There is also a security risk from the merchant's point of view. The mecrhant has no proof that the customer is the true owner of the credit card.

Additionally, since SSL encrypts everything, the display of complex pages can be slow, therefore sites protected by SSL use quite minimal graphics to minimize the impact on performance.

4 SET versus SSL

SET is compared to SSL because it is the only security protocol for the moment, that could challenge SET. As mentioned earlier SET is developed only for conducting safe electronic commerce. SSL is a lower level protocol, so it is developed for other purposes than electronic commerce too. SET's dual signature is something that SSL can't cope with. There are no means that SSL could offer to guarantee that the credit card user is authorized to use it, and the merchant is authorized to accept purchases of goods or services with credit card. And when using SSL the card holder doesn't know how the merchant saves his sensitive information (credit card number, address, order, etc.).

One thing that is important nowadays is the virus threat. SET is an application that could be threatenet by a virus, e.g. Trojan Horse.

It has been argued that SET is slow, in other words SET affects system's performance too much. GartnerGroup conducted a survey [2] which said that near-term improvements in cryptographic algorithm performance, cryptographic hardware performance and server hardware performance out-accelerate anticipated transaction loading or every class of server. Moore's law says that CPU performance doubles every eighteen months. This brings extra power to servers to handle SET transactions. In every establishment of secure connection with the purchaser server running SET has to deal with six messages instead of SSL's three.

The fact that SSL encrypts everything, instead of encrypting only the sensitive information, makes it difficult to design web pages that please customers eye. SET makes it possible to include graphics because the encryption concerns only sensitive information, not the whole web page.

Providing security services on the application layer offers the most flexible way to handle individual security needs. And the higher level that performs the encryption the less encryption overhead runs over the Internet, but more modifications to the protocols above and beneath transport layer are required.

5 Conclusions

ISSN (Online): 2230 - 8849
International Journal of Enterprise Computing and Business Systems (Online)
IJECBS India
Frequency: Bi-Annual
Specialized, Refereed and Indexed Journal in International Scientific and Corporate Databases

http://www.ijecbs.com

Volume 2 Issue 2 July 2012

Deploying security protocols has many effects depending on the viewpoint and of course the viewer. These protocols bring extra load on the Internet, they might affect the graphics of customer's application, and they might affect the simplicity of the payment transaction.

An exhaustive simulation of usage of SET and SSL by GartnerGroup proved that there is no significant effect on performance of the server, the payment gateway and customer's PC. Today's CPUs of PC's can easily handle the security applications, server CPUs will be even more powerful in the near future. Using these protocols don't bring any intolerable expencies to any of the participants of the payment transaction. I think that the gained security is worth of a little extra money, work and toleration to get a good night sleep.

References

[1] Bishop, M., Cheung, S.,Wee,C. (1997). "The Threat from the Net", IEEE Spectrum August 1997.

[2] Le Tocq, C., Young, S. (1998). SET Comparative Performance analysis, A White Paper from GartnerGroup

[3] SET Secure Electronic Transaction Specification - BOOK 1: Business Description (Version 1.0: May 1997)

[4] Oppliger, R. (1997). "Internet Security: Firewalls and Beyond". Communications of the ACM, Volume 40. No. 5.

[5] Stallings, W. (1998). Cryptography and network security:principles and practice. (second edition) Prentice Hall,New Jersey.

[6] Internet-käyttäjäkysely 1998, Petteri Järvinen Oy, 1998

[7] Aldridge, A., White, M., Forcht, K. (1997). "Security considerations of doing business via the Internet: cautions to be considered", INTERNET Research (volume 7, number 1), 1997