Measuring SSL and SET against e-commerce consumer requirements

Pita Jarupunphol[1] and Chris J. Mitchell

Information Security Group, Royal Holloway, University of London, UK.
P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk

Abstract

The threat of credit card fraud is arguably one of the most serious issues in e-commerce, since it makes consumers reluctant to engage in this alternative method of shopping. Most previous authors have focussed on technical and business issues, whilst virtually ignoring consumer confidence. If consumers are to lose their fears of e-commerce fraud, then it is important that the security solutions deployed address their concerns and not just the concerns of those building and operating the e-commerce infrastructure. According to Hassler (2000), Secure Socket Layer (SSL) and Secure Electronic Transaction (SET) are the two main industry standard means for securing Internet e-commerce communications. Currently, SSL is almost always used in preference to SET for Internet e-commerce security. SET was specifically designed to secure entire e-commerce transactions, but has been largely ignored. This paper assesses how well these existing security schemes meet consumer concerns, and hence how effectively they can increase consumer confidence. In addition, this paper also briefly considers how elements of these two protocols might be combined to offer both security and ease of use.

Keywords

Electronic Commerce (E-Commerce), Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), digital certificate, digital signature.

1 Introduction

According to Jarupunphol and Mitchell (2001), there is a mismatch between real and perceived levels of risk for e-commerce consumers. There is thus a need for security measures to address both actual security threats and also customer perceptions of security threats. Most of the previous security analyses have focussed on the actual threats, whilst paying much less attention to the perceived threats. However, unless these perceived threats are successfully addressed, e-commerce will fail to meet its true potential because of continuing customer fears. According to Friedman et al. (2000), lack of financial confidence and security confidence are reducing consumer acceptance of this innovative online shopping technology.

Currently, the two main industry standard means for securing Internet e-commerce transactions are SSL, including the IETF variant TLS (Rescorla 2001), and SET (Merkow et al. 1998). However, for various reasons, including ease of installation, lower investment costs and the much greater complexity of SET, SSL is almost always used in preference to SET for Internet e-commerce security. This paper seeks to address the perceived threats, and assesses how well the two most commonly discussed approaches to securing e-commerce, namely SSL and SET, match up to the perceived threats. This paper also considers the feasibility of combining elements of these two protocols.

[1] Pita Jarupunphol was supported by the Rajabhat Institute of Phuket (Thailand).

2 Analysis of perceived consumer security requirements

A number of payment methods have been used in Internet e-commerce, including plastic (debit/credit) card, electronic cash (e-cash), and electronic cheque (e-cheque), (Oppliger 2000). In the business-to-consumer (B2C) context, the credit card is the most commonly used method of payment for e-commerce consumers, (Treese and Stewart 1998). According to an Internet shopping habits survey conducted by Survey.Net (http://www.survey.net), 36.0% 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 compromise of credit card numbers is clearly a serious threat to the consumer. Credit card numbers can be compromised in two main ways.

- Data transmission – financial information may be stolen by an interceptor.

- Data storage – financial information may be compromised by an intruder hacking into an e-commerce merchant website.

There is currently a mixture of consumer attitudes to e-commerce. Some people are happy to use this new method of shopping, whereas others perceive e-commerce as being too risky. According to a survey of consumer attitudes to Internet shopping conducted by Harris Interactive (http://www.harrisinteractive.com), security is arguably the main consumer concern. 57% of participants worry that their credit card numbers will be abused. Whilst fraud at the merchant, either initiated by the merchant or resulting from attacks on merchant servers, is not the foremost concern of users, it is nevertheless of importance. This is particularly the case since it could lead to large numbers of credit card details falling into criminal hands, and theft of credit card numbers is the most significant user concern (Tomlinson 2000). Hence, in our discussion below we consider the effectiveness of SSL and SET in protecting the privacy of credit card numbers both whilst communicated and while stored, e.g. in merchant servers.

3 Overview of SSL and SET

SSL, developed by Netscape, is a protocol that provides security for an Internet communications link. When used to protect an e-commerce transaction, all data sent from the customer PC to the merchant website will be encrypted in order to ensure data confidentiality, (Sherif 2000), (SET 1997), (also see Figure 1).

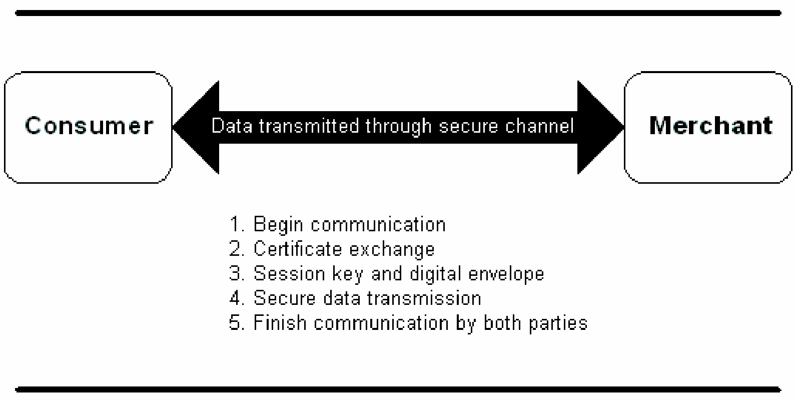
Consumer
Data transmitted through secure channel
Merchant
1. Begin communication
2. Certificate exchange
3. Session key and digital envelope
4. Secure data transmission
5. Finish communication by both parties

Figure 1: SSL security for e-commerce transactions

The SET scheme is, however, different from the SSL scheme; differences include the number of participants and the additional applications required to complete SET transactions. SET, invented by Visa and MasterCard (http://www.visa.com, http://www.mastercard.com), is designed to address security threats arising to both transmitted and stored data. Specifically, unlike SSL, SET provides protection for payment and order information both when transmitted and when stored at the merchant. In particular, the user account information is encrypted in such a way that it is only accessible to the Acquirer, thus preventing its compromise whilst stored at the merchant server. The main information flows in SET are shown in Figure 2, (Sherif 2000), (SET 1997).

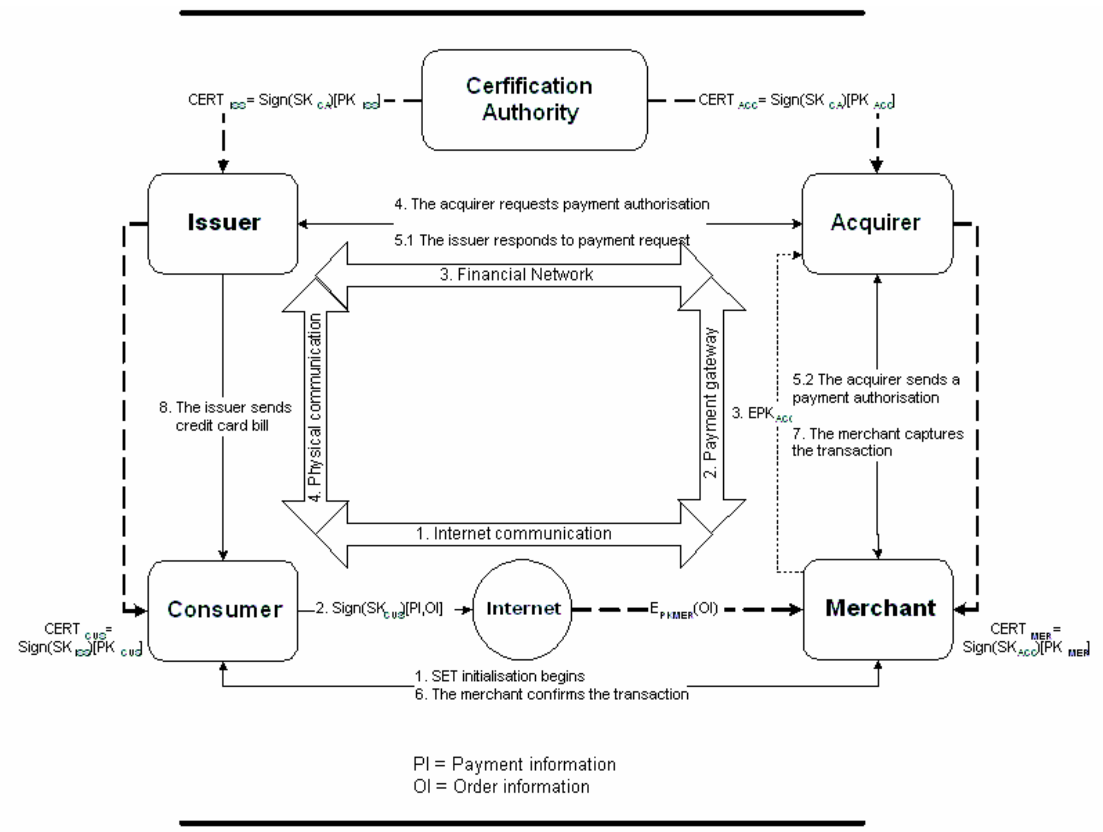
Cerfification Authority
CERT ISS= Sign(SK CA)[PK ISS]
CERT ACC= Sign(SK CA)[PK ACC]
Issuer
Acquirer
4. The acquirer requests payment authorisation
5.1 The issuer responds to payment request
3. Financial Network
4. Physical communication
2. Payment gateway
3. EPK ACC
5.2 The acquirer sends a payment authorisation
7. The merchant captures the transaction
8. The issuer sends credit card bill
1. Internet communication
Consumer
2. Sign(SK CUS)[PI,OI]
Internet
E PKMER(OI)
Merchant
CERT CUS= Sign(SK ISS)[PK CUS]
CERT MER= Sign(SK ACC)[PK MER]
1. SET initialisation begins
6. The merchant confirms the transaction
PI = Payment information
OI = Order information

Figure 2: SET process in e-commerce transactions

4 Comparison: SSL versus SET

Table 1 compares SSL and SET in the context of e-commerce consumer requirements, based on a survey of consumer perceptions to Internet shopping conducted by the National Consumer Council (NCC 2000). Although a variety of possible risks are considered in the survey, we focus on those security issues of greatest concern to e-consumers. As a result, personal issues including the inability to touch goods, the absence of personal contact, delivery problems, and the dislike of shopping with a credit card, are excluded from the table.

Security issues of concern to e-commerce consumers	**Within the scope**	
	SSL	**SET**
Confidentiality of sensitive information		
• Afraid of credit card being stolen online	Y	Y
• Afraid of personal data being abused	Y/N	Y
Merchant Integrity		
• Afraid of fraudulent suppliers	Y/N	Y
Payment Integrity		
• Hidden charges	N	Y

Table 1: SSL and SET versus security issues of concern to e-consumers

As can be seen from Table 1, significant differences exist between SSL and SET with respect to the issues of concern to e-commerce consumers. Two of the differences highlighted in the table are with respect to the abuse of personal data, since SET protects personal information stored on merchant servers whilst SSL does not, and with respect to trustworthiness of sellers. Since abuse of personal data is apparently one of the two most important issues of concern to consumers (NCC 2000), these differences are potentially significant. Payment integrity is also a significant difference. We now consider these three main differences between SSL and SET in a little more detail.

4.1 Confidentiality of sensitive information

In order to conduct e-commerce, consumers need to submit their credit card numbers to merchant websites through the Internet. Many consumers are concerned that their credit card numbers might be stolen during data transmission. There exist well-established cryptographic techniques that can be used to address this threat; see, for example, (Ghosh 1998, Hassler 2000). Both SSL and SET employ well-established secure techniques for data encryption in order to provide confidentiality for transferred e-commerce data.

Although both SSL and SET seem to provide sufficient security to protect the data transmission process, there is a difference in the level of assurance for consumer payment information after it has been sent to a merchant web server. We have seen that a significant number of consumers are concerned about the trustworthiness of their merchant. Hence countermeasures that deny merchants access to sensitive customer information will potentially be of value in allaying customer fears.

As far as data storage is concerned, there is a significant difference between SSL and SET. When SSL is used, order and payment information are stored at a merchant web server and then the merchant will pass payment information, which contains the consumer credit card details, to the acquiring bank. Therefore, the merchant has access to consumer payment information, which may be a serious cause of concern to e-commerce consumers.

By contrast, in SET, different types of transaction information will be separately transmitted to specific recipients. The order information is encrypted in such a way that it can be decrypted by the merchant, while payment information is encrypted using an acquiring bank's public key and hence is not available to the merchant. This means that merchants will only be able to access order information, whilst payment information will be forwarded directly to the acquiring bank in encrypted form.

We can conclude that SET seems to be much more effective in preventing merchant fraud than SSL, since SSL, by its nature as a communication security protocol, cannot offer any protection for order and payment information stored at the merchant web server.

4.2 Merchant integrity

As opposed to the situation for most conventional debit/credit card transactions, there is no face-to-face contact in Internet shopping. Consumers are often concerned that the merchant that they communicate with may not be valid. As a replacement for photos and signatures used for conventional face-to-face authentication, digital certificates or digital IDs based on X.509 public key certificates (ITU-T 2000), have been widely used in both SSL and SET to authenticate principals in cyberspace.

In both SSL and SET, as part of the transaction process consumers and merchants authenticate each other using public key certificates. However, there are some significant differences between SSL and SET in terms of the institutions issuing certificates.

In SSL, consumers and merchants can obtain the necessary certificates from any trusted third party acting as a Certification Authority (CA). The CA public key needed by the consumer to authenticate the merchant' s certificate will typically be embedded in the consumer' s web browser, and will be distributed with the browser software. Handling of certificate revocation will depend on the facilities offered by the web browser (currently, this is typically a process not widely supported).

Note that, since the merchant's certificate is issued by a third party, all that is being achieved in SSL is entity authentication, and the user gains no guarantees about the reputability of the merchant. Finally, note also that, in SSL, only the merchant actually needs a certificate, as authentication of the consumer to the merchant is optional.

In SET, consumers (cardholders) can apply for digital certificates from their issuing bank, while the acquiring bank will be responsible for issuing digital certificates for merchant e-commerce (SET 1997). In this case and as opposed to the case for SSL, consumers can be assured that there is a financial institution certifying the merchant before making a transaction.

4.3 Payment Integrity

Payment information sent from cardholders to merchants must remain accurate and not be modifiable. Consumers need to be sure that the payment made will not be altered. Payment integrity services mean that if there is a change in payment information such as the details of the order, the recipient will be aware that the information was altered in transit. Digital signatures can be used in the electronic environment to replace conventional signatures for proving that a message originated with the signer and guaranteeing its integrity.

SSL and SET both use well-established cryptographic techniques to assure the integrity of e-commerce messages. SSL and SET thus both provide payment integrity services for transmitted data. However, there is a difference in the integrity protection provided for stored data between SSL and SET. With the use of SSL, the integrity protection only applies to the communications path between users and merchants. However, in SET the security critical parts of the transaction are protected using digital signatures that can be verified by the acquirer. As a consequence, the use of SSL does not provide any integrity protection for stored data, whereas SET does.

5 Current status of SSL and SET

As previously stated, SET potentially offers a higher level of security protection for e-consumer transaction information than does SSL. Despite this, SSL is widely used to protect e-commerce transactions whereas SET has not really taken off. Some of the reasons for this are as follows.

- Unlike SSL, SET initialisation is complicated. In particular, key pairs need to be established for each entity (and public keys certified), (SET 1997). According to Lieb (1999, p.2), ‘the effort to obtain digital certificates has held up deployment of SET technology’.

- Interoperation of SET requires special software to be installed by every participating entity, whereas there is no need for additional software when using SSL.

- SET is somewhat inflexible in that, since digital wallets need to be present in the consumer PC, performing e-commerce transactions from third party PCs (e.g. in airport lounges, Internet cafes, etc.) is difficult, (Rescorla 2001).

- Implementing SET is costly since special applications are required to implement it (unlike SSL, which is built into commonly used web software).

- SET has not been adopted to any great extent, and is widely perceived as being ‘dead’.

- The low speed and high complexity of transactions is another commonly made criticism of SET that reduces its attractiveness to both merchants and consumers, (Sherif 2000).

6 Combining SSL/TLS with SET

As stated earlier, SSL provides security purely for a communications link, and hence its use fails to address many of the security issues for an e-commerce transaction. By contrast, SET can provide integrity, confidentiality, and authentication services for entire e-commerce transactions. Although SSL is much simpler to implement and use, SET still appears to be the most appropriate scheme for Internet e-commerce security, given that many consumers remain very concerned about the threat of credit card fraud. We now concentrate on the possibility of combining elements of the two protocols; one being popular, lightweight and in widespread use and the other being comprehensive in its security coverage.

One way in which SSL and SET might be combined would be by focussing on the e-commerce transaction relationships. This might enable us to replace SET with SSL in the areas causing most implementation difficulties.

Electronic payment or e-payment systems generally comprise four main relationships: consumer and merchant, merchant and acquirer, acquirer and issuer, and issuer and consumer. When a consumer purchases products or services from a merchant, consumer financial information will pass in several stages via the merchant, an acquirer, and an issuer until the consumer receives a confirmation of the transaction from the merchant, and ultimately a bill is physically sent from the issuer to the consumer. In what follows, we focus on the relationship between consumer and merchant, since this is both the link of potentially highest security criticality and is also the source of many of the implementation issues with SET. One existing step in this direction is the 3D SET scheme, which we now describe. Note that this is by no means the only possible way in which elements of SET and SSL can be combined, although we do not explore this issue further here.

6.1 3D SET

One reason that SSL/TLS has been so widely adopted is that it offers a measure of security without requiring the consumer to perform any initialisation process (apart from installing a web browser). However, one problem with SSL/TLS is that merchants do not authenticate the cardholder. Remedying this defect inevitably appears to require the user to have security credentials of some kind, which implies an initialisation process of the type required by SET. One possible way to make SET much simpler for e-commerce consumers would be to remove the requirement for consumers to store certificates on their PC, and instead give this responsibility to the issuer, who communicates with the merchant's bank (acquirer) directly. This is precisely the approach adopted by 3D SET (Bounie and Vaninetti 2001), proposed by Visa as an alternative version of the SET scheme. 3D SET operates between the three domains in an e-commerce transaction, namely the acquirer, issuer, and interoperability domains. When consumers order products or services under 3D SET, all payment facilities, including consumer certificates, are securely stored at the issuer secure server. SSL could be used to secure consumer payment information when sent between consumer and merchant.

7 Conclusions

The use of both SSL and SET has clear benefits to e-consumer and merchant. Although SSL is very convenient to use to protect Internet e-commerce transactions, SET obviously addresses the lack of consumer confidence in e-commerce rather better than does SSL. However, the complexity of SET scheme has restricted its adoption by e-commerce end-users. The 3D SET technology appears to be a possible means to reduce the complexity of SET implementation at end-users. Furthermore, the possibility of combining SSL and SET is also likely to encourage consumers to participate in e-commerce, offering both convenience and confidence. In a further paper we will consider the future of SET in e-commerce.

8 References

Bounie, D. and Vaninetti, L. (2001), "E-Payments: Which Systems in Europe for the Coming Years?", *ENST*, August.

NCC Report (2000), "E-Commerce and Consummer Protection: Consumer – real needs in a virtual world", *National Consumer Council*, August.

ITU-T (2000), *Recommendation X.509 (03/00) – Information technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks*, March.

Friedman, M., Kahn, P. H. and Howe, D. C. (2000), "Trust online", *Communications of the ACM*, Vol. 43, No. 12, pp34-40, December.

Ghosh, A. K. (1998), *E-Commerce Security, Weak Links, Best Defences*, John Wiley and Sons, New York.

Hassler, V. (2000), *Security Fundamentals for E-Commerce*, Artech House, Massachusetts.

Jarupunphol, P. and Mitchell, C. (2001), "Actual and perceived levels of risk in consumer e-commerce", In *Proceedings of 2nd International We-B Conference*, November, pp.207-216.

Lieb, J. (1999), "Getting secure online – an overview", *CommerceNet – The Strategies Report*, Vol. 1, No. 3, pp1-4, July.

Merkow, M. S., Breithaupt, J., and Wheeler, K. L (1998), *Building SET Applications for Secure Transactions*, John Wiley and Sons, New York.

Rescorla, E. (2001), *SSL and TLS – Designing and Building Secure Systems*, Addison-Wesley, Boston.

SET (1997), *Secure Electronic Transaction Specification – Book 1: Business Description,* SetCo.Org, May.

Sherif, M. H. (2000), *Protocols for Secure Electronic Commerce*, CRC Press, Florida.

Tomlinson, M. (2000), "Tackling e-commerce security issues head on", *Computer Fraud and Security*, Vol. 2000, No. 11, pp10-13, November.

Treese, G. W. and Stewart, L. C. (1998), *Designing Systems for Internet Commerce*, Addison-Wesley, Boston.