MEASURING 3-D SECURE AND 3D SET AGAINST E-COMMERCE END-USER REQUIREMENTS

Pita Jarupunphol and Chris J. Mitchell
Information Security Group
Royal Holloway, University of London
{P.Jarupunphol, C.Mitchell}@rhul.ac.uk

ABSTRACT

The threat of credit card fraud is arguably the most serious issue of concern to e-commerce participants, including consumers and merchants. 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 e-commerce transaction security. These schemes can provide the participants in an e-commerce transaction with a greater range of security services than provided by naive use of SSL/TLS, without introducing significant implementation complexity for merchant or consumer. However, in e-commerce, not only security requirements but also implementation requirements must be considered. This article contrasts the effectiveness of 3-D Secure and 3D SET in meeting e-commerce end-user requirements, including both security and implementation issues.

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 categorised into business to business (B2B), business to consumer (B2C), consumer to consumer (C2C), and public/private sectors to government (Hassler, 2001); we focus on B2C transactions in this paper.

In B2C transactions, the credit card is the most widely used method of payment for Internet e-commerce transactions (Treese and Stewart, 1998). 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 (Jarupunphol and Mitchell, 2001).

As has already been discussed in elsewhere (see, for example, Bellman et al., 1999; Jarupunphol, 2001; Jarupunphol, 2002a), many consumers perceive e-commerce as being riskier than other shopping methods. These consumers are particularly concerned that their financial information, such as their credit card numbers, may be compromised.

Moreover, not only do numerous consumers perceive that shopping via e-commerce is particularly risky, but also a number of e-commerce business organisations believing that the likelihood of fraud in e-commerce is higher than for non e-commerce transactions. According to the Information Security Breaches Survey (DTI, 2002), some business opinions regarding e-commerce security are as follows.

- 61% of UK businesses believe that e-commerce systems are more of a target for fraud than non e-commerce systems,
- 32% believe that e-commerce and non e-commerce systems are equally a target for fraud, and
- only 7% think that e-commerce systems are less of a target for fraud than non e-commerce systems.

Consequently, various methods have been proposed to address the security risks arising in e-commerce.

Secure Socket Layer (SSL) or the SSL-based protocol Transport Layer Security (TLS) (Rescorla, 2001) are almost always used in preference to Secure Electronic Transaction (SET) (Merkow et al., 1998; SET, 1997a; SET, 1997b) for Internet e-commerce transaction security. This is primarily because, despite comprehensively meeting all security requirements, SET fails to meet end-user implementation requirements. SSL/TLS, on the other hand, whilst being simple to implement, does not meet all the end-user security requirements. Recently, the three-domain (3D) architecture (Wrona et al., 2001) has been introduced to try and meet both security and implementation requirements. Two main examples of 3D schemes have been proposed, namely 3-Domain Secure (Gpayments, 2002; Visa 3-D Secure, 2001a; Visa 3-D Secure, 2001b), which builds on the SSL/TLS protocol, and 3D SET (Bonnie and Vaninetti, 2001; Wrona et al., 2001), which is a 3D version of SET.

In this paper, we consider how well e-commerce end-user requirements are fulfilled by these two 3D schemes.

2. ADVANTAGES AND DISADVANTAGES OF SSL/TLS AND SET

Before considering the 3D protocols which are the main subject of this paper, we start by considering the main advantages and disadvantages of the SET and SSL/TLS protocols when used for e-commerce security. This serves as a background for the discussion of the two 3D protocols, given that they are

based on these schemes. For more detailed discussion of these issues see, for example, Jarupunphol and Mitchell (2002c).

2.1. Brief analysis of SSL/TLS

The main advantages of SSL/TLS, when used to protect e-commerce transactions, are as follows.

- Ease of use for e-commerce end-users. The cardholder can use SSL/TLS completely transparently because it is already built into commonly used web browsers, and merchants can also implement SSL/TLS without changing their payment model in any way.
- The system is not complex, resulting in minimal impact on transaction speed.

The main disadvantages of SSL/TLS for e-commerce are as follows.

- The merchant cannot reliably identify the cardholder. In cases where consumers use a stolen credit card to initiate e-commerce transactions, merchants are responsible for 'card not present' transaction charge backs (Caunter, 2001; Treese and Stewart, 1998).
- Since SSL/TLS only protects the communications link between consumer and merchant, it does nothing to protect sensitive cardholder information whilst it is stored at the merchant server. Merchants therefore need to implement additional security measures to protect the secrecy of this information.
- SSL-based e-commerce permits the merchant to see consumer payment information, potentially causing security concerns to cardholders.

2.2. Brief analysis of SET

The main advantages of SET are as follows.

- SET ensures the confidentiality of payment information at all stages of transaction processing, including data transmission and data storage.
- SET prevents the merchant from seeing consumer payment information, since the payment information is forwarded to the acquirer in encrypted form (encrypted using the acquirer's public key).
- To ensure merchant privacy, SET prevents the acquirer from seeing consumer order information stored at the merchant web server.

The main disadvantages of SET are as follows.

- Implementing SET is more costly than SSL/TLS for both consumers and merchants.
- Using SET is much more complicated than using SSL.
- SET does not permit the cardholder to place an order from PCs other than the cardholder's SET-initialised PC because the cardholder's private key required to conduct a SET transaction is stored in this PC.
- SET employs complex cryptographic mechanisms that may result in an unacceptable transaction speed.

3. THE 3-DOMAIN E-PAYMENT ARCHITECTURE

Before considering the 3-D Secure and 3D SET payment systems in detail, we introduce the 3-Domain (3D) payment model which underlies them both.

3.1. Participants

In electronic payment systems (Hassler, 2001), there are four main types of participant, namely consumers, merchants, issuers, and acquirers. These roles are also required in 3D-based payment systems. In addition, a payment gateway, which is an entity responsible for providing access to payment authorization functions and for capturing payment information in an online financial exchange, is required.

The roles of these participants can be summarised as follows.

Consumer (C) – The entity that purchases products or services from the merchant via the Internet.

Merchant (M) – The entity that sells products or services to the consumer via the Internet.

Issuer (I) – The entity that issues the consumer a credit card and also responds to an online payment request from the acquirer via the payment gateway.

Acquirer (A) – The entity that forwards the payment request from the merchant to the issuer via the payment gateway.

3.2. The three domains

3-D Secure and 3D SET are built upon the relationships between three 'domains', namely the acquirer, issuer, and interoperability domains (Bounie and Vaninetti, 2001; Visa 3-D Secure, 2002a; Visa 3-D Secure, 2002b; Wrona et al., 2001).

Acquirer Domain – The acquirer domain covers the relationship between the merchant and acquirer.

Issuer Domain – The issuer domain covers the relationship between the cardholder and the issuer.

Interoperability Domain – The relationship between the acquirer and issuer domains is supported by the interoperability domain.

4. 3-D SECURE AND 3D SET

We now give an overview of the 3-D Secure and 3D SET payment systems.

4.1. 3-D Secure

The 3-D Secure payment system can be regarded as the integration of SSL with the 3D model. As mentioned above, when used simply to protect the cardholder-merchant link, SSL/TLS does not provide verification of the cardholder, which can result in credit card fraud at the consumer side. Integration of the 3D architecture with SSL can help address this issue. 3-D Secure, originally known as 3D SSL, was developed by Visa.

In 3-D Secure, the payment gateway, which provides an interface between the merchant/acquirer' s payment system and the Visa proprietary payment network VisaNet, must be implemented in the acquirer domain (Visa 3-D Secure, 2002b). Merchants are responsible for installing an SSL/TLS Merchant Plug-In (MPI) at their servers, as would normally be the case if they wish to implement SSL/TLS for consumer-merchant communication protection. For 3-D Secure, this MPI is required to have additional functions to handle communication with a centralized Visa directory (GPayments (2001; Gpayments, 2002).

Within the Issuer domain, each card issuer is required to maintain a special server known as the Access Control Server (ACS). The ACS is used to support cardholder authentication.

The Visa directory is a server in the Interoperability domain, used to enable communications between merchant servers and card issuers.

To protect the security of communications between the various entities, 3-D Secure requires the following links to be protected using SSL/TLS: cardholder-merchant, cardholder-ACS, merchant-Visa Directory, and Visa Directory-ACS, Visa 3-D Secure (2002b).

Figure 1 shows how 3-D Secure operates (Visa 3-D Secure, 2002a; Visa 3-D Secure, 2002b; Wrona et al., 2001) (see also the explanation below the figure). The numbered steps shown in figure 1 are explained below. In this explanation, C, M, I, A and VDir denote the Cardholder, Merchant, Issuer, Acquirer and Visa directory respectively.

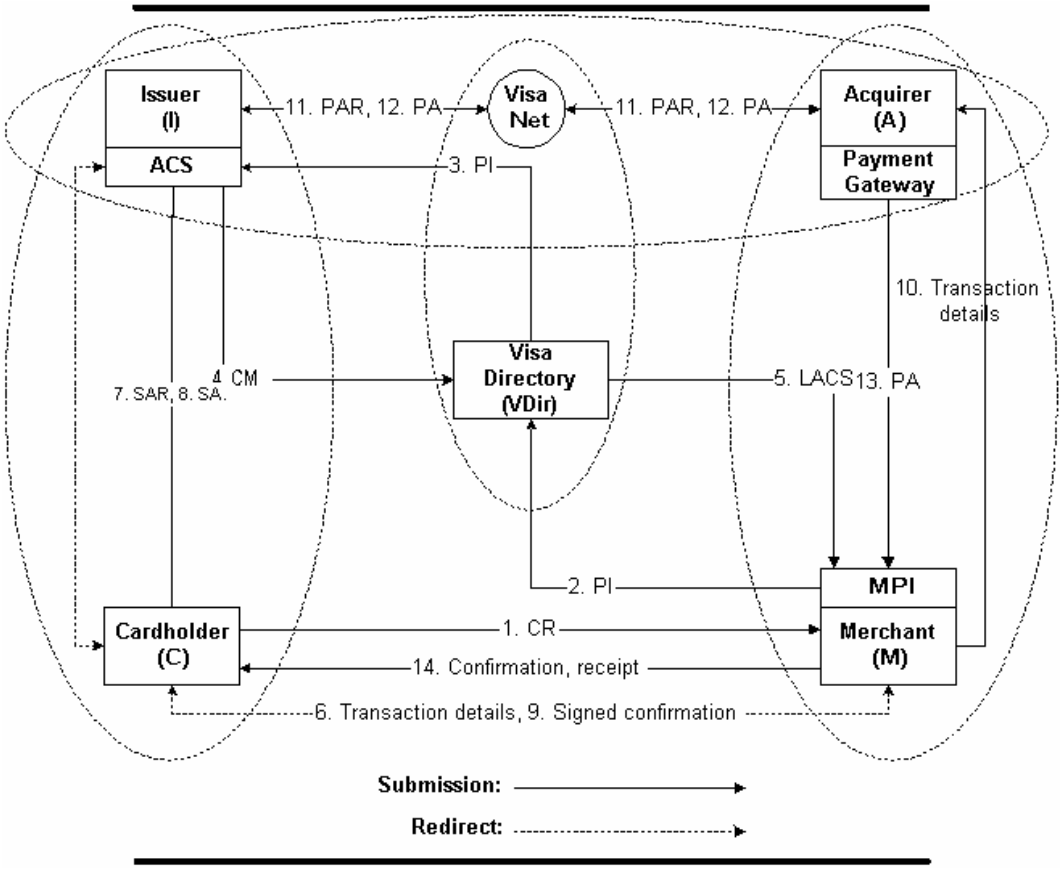

Figure 1: The 3-D Secure transaction procedure

C→M: The cardholder submits a checkout request (CR) to the merchant when the details of a transaction have been decided. In this process, all purchasing information transmitted to the merchant server will be protected by SSL/TLS.

M→VDir: After the purchase information has been transmitted to the merchant server, the MPI at the merchant server sends a request to the Visa directory for the URL of the ACS of the issuer of the card.

VDir→I: The Visa directory checks the validity of the card and queries its participation in the 3-D Secure scheme with the ACS at the issuer server.

I→VDir: The issuer sends a confirmation message (CM) to the Visa directory confirming the validity of the card details.

VDir→M: The URL of the issuer's ACS (LACS) is sent to the MPI.

M→C→I: The MPI redirects the cardholder browser to the issuer's ACS.

I→C: The issuer's ACS requests secret authentication (SA) information, such as username and password, from the cardholder.

C→I: The cardholder enters his/her SA into the browser on his/her PC, from where it is sent to the issuer's ACS.

I→C→M: If the cardholder validation process is successful, the issuer's ACS redirects the cardholder browser back to the MPI and sends a payment verification signed by the issuer.

M→A: The merchant transmits transaction details to the acquirer to request payment authorisation (PA) as in a 'normal' Internet transaction.

A→I: The acquirer sends a payment authorisation request (PAR) to the issuer via Visanet.

I→A: The issuer responds by sending a PA to the acquirer.

A→M: The acquirer sends the PA details back to the merchant.

M→I: The merchant confirms the transaction and issues a receipt to the cardholder.

4.2. 3D SET

3D SET (Server-based SET) is another 3D payment scheme that predates 3-D Secure. 3D SET was developed by a number of SET software vendors (Gpayments, 2001), and maps the SET payment system into the 3D model. As a replacement for the traditional SET digital wallet that must be stored at a consumer PC, 3D SET uses a SET Wallet Server in the issuer domain. The cardholder' s certificate is also securely stored at the issuer' s secure server.

Within the acquirer domain, there is no need for the merchant to have a certificate installed at the merchant server. As in the issuer domain, the acquirer stores the merchant' s certificate and implements the payment gateway at the acquirer secure server.

Figure 2 shows how 3D SET operates. The 3D SET transaction procedure involves the following main steps, as indicated in Figure 2. In this explanation, and as previously, C, M, I and A denote the Cardholder, Merchant, Issuer and Acquirer respectively.

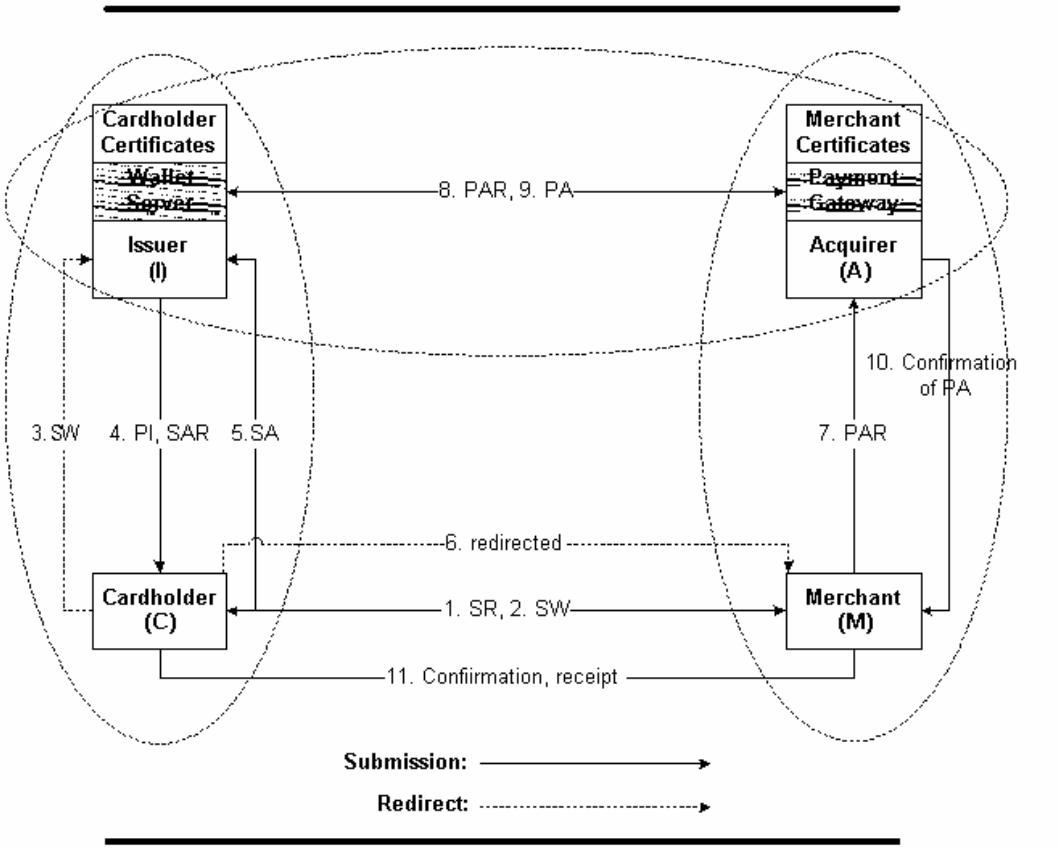

Figure 2: The 3D SET transaction procedure

C→M: The cardholder passes a SET request (SR) message to the merchant.

M→C: The merchant sends a SET Wake-up (SW) message to the cardholder.

C→I: The cardholder's browser redirects the (SW) message to the SET Wallet Server at the issuer.

I→C: The issuer displays a window to the cardholder containing the payment information (PI), and requests entry of secret authentication information (SAR).

C→I: The cardholder enters the secret authentication (SA) information. If the verification is successful, the issuer will perform the SET transaction.

C→M: The cardholder browser is redirected back to the merchant after the cardholder authentication process is completed.

M→A: The merchant sends the payment authorization request (PAR) to the acquirer.

A→I: The acquirer forwards the PAR to the issuer.

I→A: The issuer responds with a payment authorisation (PA) to the acquirer.

A→M: The acquirer confirms authorisation of the transaction to the merchant.

M→C: The merchant confirms the transaction and issues a receipt to the cardholder.

5. OVERVIEW OF E-COMMERCE END-USER REQUIREMENTS FOR E-PAYMENT SCHEMES

This paper measures the effectiveness of the proposed 3D protocols against e-commerce end-user requirements. The end-user requirements must therefore first be defined. Note that e-commerce end-users here include both consumers who use the Internet to purchase products or services, and

merchants who provide such services to consumers. Understanding end-user requirements, however, is very complicated, since end-user perceptions of innovative technologies can be influenced by various factors, including via the members of a social system (Roger, 1983).

In order to get a clear picture of e-commerce end-user requirements, we divide requirements into different categories. In particular we focus here on security requirements and implementation requirements. There are reasons to believe that these are two particularly important categories of requirements. First note that security requirements have driven the design of such systems as SET, and it is perceptions about the security, or more precisely the lack of security, that prevent many potential users of e-commerce from engaging in it.

Second, observe that, as pointed out in Jarupunphol and Mitchell (2002b, 2002d), SET has failed to meet e-commerce end-user requirements because of implementation issues, in spite of providing a full set of security services. Thus, despite the fact that the end-users are very concerned about the security of their sensitive information, system developers cannot ignore implementation factors.

5.1. Security requirements for e-payment schemes

Hassler (2001) states that security requirements for electronic payment systems include confidentiality, integrity, authentication, and non-repudiation. Following this approach, the following security requirements can be identified for the e-commerce end-users.

- Payment confidentiality – Consumer financial information must be kept confidential, including during transmission and storage. Here, the consumer is the entity requiring the confidentiality service, while the merchant is the entity providing the service.
- Payment integrity – The integrity of the transaction must be protected, including during transmission and storage. Both consumer and merchant require this service.
- Entity authentication – Both consumers and merchants require entity authentication services in order to verify the identity of the entities with whom they are dealing.
- 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.

5.2. Implementation requirements for e-payment schemes

We focus here on the major barriers causing implementation failures in SET schemes (Jarupunphol and Mitchell, 2002b, 2002d) including usability, flexibility, affordability, speed of transaction, and interoperability. Apart from these requirements, it is important to consider another major factor, namely whether e-commerce end-users can actually use the payment scheme. That is, is the system ready for the consumer and merchant to implement? Thus we also consider availability as one of the implementation requirements.

In addition to availability, reliability is also an important factor to be considered, as it ensures that the software or system will perform appropriately. In (IEEE STD610.12, 1990; Musa and Everett, 1990; Whittaker and Voas, 2000), software reliability is defined as the probability that software will not cause the failure of a system for a specified time under specified conditions. Furthermore, data input and output must be correctly displayed by the given functions. In e-commerce, this means that the data inputs of consumers (e.g. order, payment, and billing information) and merchant transaction information must be correctly displayed to consumers by their Web browser.

Hence the following end-user implementation requirements can be identified.

- 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 (Jarupunphol and Mitchell, 2002d). Merchants will also not wish to invest significantly in engineering e-payment infrastructure (Treese and Stewart, 1998).
- 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.

6. ASSESSING 3-D SECURE AND 3D SET AGAINST THE END-USER REQUIREMENTS

We now measure 3-D Secure and 3D SET against the e-commerce end-user requirements identified in the previous section.

6.1. Security requirements

We first consider the security requirements identified in Section 5.2.

Confidentiality Both 3-D Secure and 3D SET provide for the encryption of payment information using state of the art cryptographic techniques. Note, however, that in 3-D Secure the merchant has access to all the consumer's payment information, just as would be the case in today's typical environment, where SSL/TLS is used to protect the customer-merchant Internet link.

Integrity Although traditional SSL alone cannot provide payment integrity for stored data, 3-D Secure can address this problem, since the payment information (PI) must be authorised and signed by the issuer prior to passing to the merchant. In 3D SET, the integrity provisions supported by SET still apply, although the process is performed via the interoperability domain where the issuer holds the cardholder's certificate and the acquirer holds the merchant' s certificate.

End entity verification Both 3-D Secure and 3D SET provide a measure of mutual authentication between merchant and consumer. In 3-D Secure, authentication of merchant to cardholder is supported by the use of SSL, whereas authentication of cardholder to merchant is performed indirectly through the use of the ACS (that is, the ACS vouches to the merchant that it has authenticated the cardholder). In 3D SET, the issuer authenticates the cardholder, and the acquirer is responsible for ensuring that it is communicating with the correct merchant, and hence mutual authentication is therefore performed via the interoperability domain.

Non-repudiation Because of the end entity verification mechanisms provided by both 3-D Secure and 3D SET, consumers and merchants cannot deny having participated in a completed transaction. The consumer cannot deny ordering products or services from the merchant, and the merchant also cannot deny having received the consumer order. Hence both 3-D Secure and 3D SET effectively meet consumer and merchant security requirements.

6.2. Implementation requirements

3-D Secure and 3D SET are next further assessed against the implementation requirements identified in Section 5.3.

Usability 3-D Secure has the major advantage for the merchant that it preserves the payment model used for existing SSL/TLS-protected e-commerce transactions. Initialisation is also simple for both merchant and cardholder; the merchant simply needs to install a special plug-in on his/her server, and the cardholder needs no special software and must simply follow an on-line enrolment process with the card issuer, using a 'standard' web browser.

3D SET is also simple to initialise, since the cardholder does not need to generate his/her own key pair and obtain a certificate – all this is taken care of by the card issuer. Similarly, the merchant initialisation is also simple, since the acquirer takes care of the key management and certification for the merchant. However, unlike 3-D Secure, the payment model for 3D SET is now different to the current mode of operation, and more significant changes will be necessary to the payment application running on the merchant server.

Flexibility Both 3-D Secure and 3D SET have the desirable property that they can be used from any PC, as is currently the case for e-commerce transactions relying simply on SSL/TLS for cardholder-merchant communications security. This is achieved since neither of these 3D schemes require special software or keying material to be installed on the e-commerce PC.

Affordability In 3D SET, merchants are still required to have a point-of-sale (POS) application to send a SET Wake-up message in reply to a SET request message from the cardholder. In addition, the POS application is also used in order to communicate with the payment gateway installed at the acquirer' s server. Although it is not clear whether consumers need to pay for their 3D SET certificate, we assume here that there is more investment in using 3D SET than using 3-D Secure because of the requirement for the POS application at the merchant web server.

Reliability The 3-D Secure Merchant Plug-In and the merchant software for 3D SET must also perform their functions correctly. Although implementation failures of these 3D protocols have not yet been reported, this is not surprising because of their recent emergence. Nevertheless, it can reasonably be assumed that the likelihood of system failures is low, since these two 3D protocols are supported by large reputable organisations.

Of course, whilst the presence of incorrect functionality in security critical elements of implementations of the 3D schemes is unlikely, there is still a significant possibility that accidental vulnerabilities will be present in implementations of the schemes. Past experience indicates that it is very difficult to produce software which does not possess vulnerabilities (e.g. arising through buffer overflows) exploitable by malicious software.

Availability One of the major issues with SET is the problem of availability. Consumers can perform all the work of installing SET on their PC, but they cannot use it unless merchants also install SET at their servers. Consumers will certainly not wish to go to the trouble of performing the installation unless they are convinced that SET will be of immediate practical benefit to them. In exactly the same way, merchants will not wish to invest in a costly SET implementation unless they are convinced that a significant number of consumers will have the necessary SET installation to use their SET transaction service.

This issue is to a large extent avoided by 3-D Secure. Of course, as with any such system, 3-D Secure requires card issuers and acquirers to implement the system before anyone else – however, there are a relatively small number of such entities. Once the acquirer and issuer support is in place, merchants can install 3-D Secure in the knowledge that consumers will be immediately capable of using the system, since consumers do not need to install any new software on their PC (they simply need to carry out a simple registration process which can be totally web based). Equally, consumers will be relatively happy to perform a simple web registration process, since the time required will be minimal, and there will be no software to install or letters to write. Thus availability should not be an issue for 3-D Secure.

Similar arguments apply to 3D SET. Customers can be enrolled using a simple process, and it will be much simpler to convince merchants that the (smaller) investment necessary to use 3D SET will have a speedy return. However, it is also true that, as discussed under 'Usability' above, since Merchants will have to adopt a somewhat different payment model to use 3D SET, there are greater availability issues with this scheme than with 3-D Secure.

Speed of transaction 3-D Secure primarily employs SSL/TLS (Visa 3-D Secure, 2002b) to meet security requirements. Apart from this, in 3-D Secure there are other features that may affect the transaction performance, including using the Visa Directory and the Issuer ACS to verify the cardholder's identity.

By contrast, 3D SET uses complex cryptographic mechanisms to secure entire e-commerce transactions, e.g. certification among participants, protection mechanisms for consumer and merchant sensitive information, etc.

It is difficult to decide which 3D scheme is more effective with regard to transaction speed, for the following reasons.

- It is possible for Issuer and Acquirer servers to perform SET operations very quickly, as long as appropriate hardware and software are used.
- In both schemes the central servers may prove to be a bottleneck.
- Apart from software/hardware requirements, high-speed networking is required to enable the various necessary interactions to be performed quickly.

Interoperability How well 3-D Secure and 3D SET meet the interoperability requirement remains unproven, since the two systems have not yet been widely deployed. However, since neither system relies on special software being installed on the consumer PC, and instead makes use of 'standard' browser features, interoperability issues are less likely to arise.

In 3-D Secure, the only remaining problems would appear to be merchant – Visa Directory interactions. This link is protected using 'standard' means (i.e. SSL/TLS), and also there is only one Visa Directory – thus again interoperability should not be a major problem.

In 3D SET, interoperability between merchant server and acquirer server should not be an issue, since we assume that the merchant software is supplied by the acquirer. This only leaves interactions between issuer and acquirer servers. Whilst interoperability problems could arise here if cryptographic and other SET functionality is provided by different vendors, the numbers of parties involved should be sufficiently small that such problems can be overcome quickly.

In summary, both the 3D schemes would appear to have fewer potential interoperability problems than SET. However, 3-D Secure would appear to offer a slight advantage over 3D SET, given that the complex cryptographic functionality in SET is likely to be one possible cause of interoperability issues.

6.3. 3-D Secure or 3D SET?

We now summarise and compare how well the two 3D schemes meet the identified end-user requirements. Table 1 gives a comparison between the two 3D protocols with respect to e-commerce end-user requirements.

Requirements	E-commerce end-users				Effectiveness against end-users	Comments
	Consumer		Merchant			
Security	**3D SET**	**3-D Secure**	**3D SET**	**3-D Secure**		
Confidentiality	Yes	Yes*	Yes	Yes	3D SET (marginally)	The merchant has access to all the consumer's payment information
Integrity	Yes	Yes	Yes	Yes	Equally effective	Both 3D SET and 3-D Secure meet the requirements
Verification	Yes	Yes	Yes	Yes	Equally effective	Both 3D SET and 3-D Secure meet the requirements
Non-repudiation	Yes	Yes	Yes	Yes	Equally effective	Both 3D SET and 3-D Secure meet the requirements
Implementation	**3D SET**	**3-D Secure**	**3D SET**	**3-D Secure**		
Usability	Yes	Yes	Yes*	Yes	3-D Secure	The payment model for 3D SET is different to the current mode of operation
Flexibility	Yes	Yes	Yes	Yes	Equally effective	Both 3D SET and 3-D Secure meet the requirements
Affordability	Yes	Yes	Yes*	Yes	3-D Secure	More investment in using 3D SET than using 3-D Secure
Reliability	Yes	Yes	Yes	Yes	Equally effective	Both 3D SET and 3-D Secure meet the requirements
Availability	Yes	Yes	Yes*	Yes	3-D Secure	Usability issues
Speed of transaction	N/A*	N/A*	N/A*	N/A*	Unclear	Appropriate hardware and software, bottleneck, high speed networking
Interoperability	Yes	Yes	Yes	Yes	3-D Secure (marginally)	Cryptographic and other SET functionality provided by different vendors

Table 1: 3-D Secure and 3D SET versus e-commerce consumer requirements

As can be seen from the table, 3-D Secure and 3D SET can both fulfil end-user security requirements because of the strong cryptographic algorithms deployed by the protocols and the issuer server/cardholder interaction that provides entity verification at the client side (consumer). Thus we suggest that 3-D Secure and 3D SET are equally effective in securing Internet e-commerce transactions, if security is the only concern. Note, however, that 3D SET has a slight advantage with respect to confidentiality since the merchant server does not have access to the cardholder payment details.

However, the differences between 3D SET and 3-D Secure are more significant when we consider the effectiveness of the two schemes in meeting implementation requirements. Although the speed of transaction issue still seems to be a potential barrier to both these 3D schemes, the 3-D Secure scheme appears to be a better fit to the implementation requirements. Nevertheless, apart from certain issues at the merchant side, 3D SET is also capable of meeting end-user requirements.

These results indicate that, although 3D SET offers slight advantages over 3-D Secure in fulfilling e-commerce end-user security concerns, overall 3D SET performs less well than 3-D Secure in meeting the identified requirements.

7. CONCLUDING REMARKS

As has already been discussed, issues of concern to e-commerce end-users can be addressed by either 3-D Secure or 3D SET. In addition, although both schemes appear to fit well to the identified implementation requirements, 3-D Secure has significant advantages over 3D SET. As a consequence, the 3-D Secure scheme would appear to be more likely to be widely used for future e-payment security.

References

Bellman, P., Lohse, L., and Johnson, E. J. (1999). Predictors of online buying: Findings from the Wharton virtual test market. *Communications of the ACM*, 42(12):32–38, December.

Bounie, D. andVaninetti, L. (2001). E-Payments: Which Systems in Europe for the Coming Years? ENST. (http://www.enst.fr/egsh/news/fichiers%20pdf/IR13.pdf).

Caunter, N. (2001). The real cost of fraud to e-tailers. Computer Fraud and Security, 2001(8):17.

DTI (2002). *Information Security Breaches Survey 2002*, Department of Trade and Industry (DTI) and PricewaterhouseCoopers.

GPayments (2001). Authentication — The missing element in online payment security. (http://www.gpayments.com/pdfs/GPaymentsAuthenticationWhitepaper.pdf).

GPayments (2002). Visa 3-D Secure vs. MasterCard SPA — A comparison of online authentication standards.

Hassler, V. (2001). Security Fundamentals for E-Commerce. Artech House, Massachusetts.

IEEE STD 610.12 (1990). IEEE STD 610.12-1990 — IEEE Standard Glossary of Software Engineering Terminology.

Jarupunphol, P. and Mitchell, C. J. (2001). Actual and perceived levels of risk in consumer e-commerce. In Proceedings of 2nd International We-B Conference, pages 207–216. Edith Cowan University Press.

Jarupunphol, P. and Mitchell, C. J. (2002a). Consumer risk perceptions in e-commerce. In *Proceedings of UKAIS2002*, pages 308-315. Leeds Metropolitan University, Leeds, April.

Jarupunphol, P. and Mitchell, C. J. (2002b). Failures of SET implementation: What is amiss?. In *Proceedings of 7th Asia-Pacific Decision Sciences Institute Conference 2002*. ISSN: 1539-1191. National Institute of Development Administration, Bangkok, July.

Jarupunphol, P. and Mitchell, C. J. (2002c). Measuring SSL and SET against e-commerce consumer requirements. In Proceedings of the International Network Conference (INC 2002), pages 323–330. Plymouth University Press, Plymouth, July.

Jarupunphol, P. and Mitchell, C. J. (2002d). The future of SET. In *Proceedings of UKAIS2002*, pages 9-17. Leeds Metropolitan University, Leeds, April.

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

Musa, J. D. and Everett, W. W. (1990). Software-reliability engineering: Technology for the 1990s. IEEE Software, 7(6):36–43.

Rescorla, E. (2001). SSL and TLS — Designing and Building Secure Systems. Addison-Wesley, Massachusetts.

Roger, E. (1983). *Diffusion of Innovation 3rd edition*. The Free Press, New York.

SET (1997a). SET Secure Electronic Transaction Specification — Book 1: Business Description. SETCo.Org.

SET (1997b). SET Secure Electronic Transaction Specification—Book 2: Programer's Guide. SETCo.Org.

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

Visa 3-D Secure (2002a). 3-D Secure: Introduction – Version 1.0.2, September. Visa International.

Visa 3-D Secure (2002b). 3-D Secure: System Overview – Version 1.0.2, September. Visa International.

Whittaker, J. A. and Voas, J. (2000). Toward a more reliable theory of software reliability. IEEE Computer, 33(12):36–42.

Wrona, K., Schuba, M., and Zavagli, G. (2001). Mobile payment — state of the art and open problems. In Fiege, L., Mühl, G., and Wilhelm, U. G., editors, Proceedings of 2nd International Workshop WELCOM, volume 2232 of Lecture Notes in Computer Science, pages 88–100. Springer–Verlag.