Secure Electronic Transactions (SET): A Case of Secure System Project Failures

Pita Jarupunphol and Wipawan Buathong

Abstract—**Secure Electronic Transactions (SET) is a security protocol for an electronic payment system that utilises PKI to address e-commerce security and privacy concerns. Although PKI technologies used by the SET protocol were proven to be effective in addressing security issues in e-commerce, several implementation issues were found from SET applications de-signed to support security mechanisms ofPKI. SET failed to be implemented by e-commerce end-users. This paper studies how SET was predicted, designed, and rejected by e-commerce end-users. PKI issues associated with SET implementation in B2C e-commerce are also reviewed. Although e-commerce end-users are concerned about security issues, usability is a more dominant factor than security for a secure system project to be adopted by the users.**

Index Terms—**Certification authorities (CAs), public key infrastructure (PKI), secure socket layer (SSL), secure electronic transactions (SET)**

I. Background

When e-commerce was introduced as an alternative shop-ping method a decade ago, a number of research scholars believed that the growth of e-commerce relied on a number of security-related factors [1], [2], [3], [4] although e-commerce provided many benefits to consumers (e.g., convenience, greater choice, lower prices and more information). In order to address e-commerce security requirements, well-established cryptography was believed to be a 'magic pill'. An apparently secure e-commerce website would, in theory, convince potential e-commerce customers to become regular e-commerce customers. According to Giff [5], "[a]n example of increasing security to increase trust comes from people being more willing to engage in e-commerce if they are assured that their credit card numbers and personal data are cryptographically protected". In this light, PKI (Public Key Infrastructure) [6] was pointed out as a solution to e-commerce security and privacy concerns.

According to Farrell and Zolotarev [7], PKI is vital for e-commerce security, since many applications that use PKI are not Web services and PKI is the only choice available for connecting business relationships to keys and identities when more than one domain is involved. In addition, Piper [8, p.24] stated that "Security is obviously a major concern for all potential users of E-commerce and the use of (public key) cryptography is an important issue". PKI is the subject of standardization by a number of bodies, including the IETF, ITU-T and ISO/IEC. PKI is the infrastructure necessary for wide-scale use of public key cryptography (PKC) [9], [10]. It supports a variety of practically valuable cryptographic operations, including encryption, digital signature and entity authentication. In e-commerce, the PKI solution based on application-specific PKIs had never been integrated with e-payment systems until the emergence of SET in 1996 although general purpose PKIs were initially used in SSL/TLS (Secure Socket Layer/Transport Layer Security) [11]. SET was believed among security experts as the most secure electronic payment system that could protect the entire e-commerce transactions. This paper investigates how SET was predicted, designed, and rejected by e-commerce end-users.

Manuscript received January 10, 2013; revised March 12, 2013.

The authors are with the Department of Informatics, Faculty of Science and Technology Phuket Rajabhat University, Phuket,83000 Thailand(e-mail: p.jarupunphol@pkru.ac.th, w.buathong@pkru.ac.th).

II. Secure Electronic Transactions

SET is a security protocol for an electronic payment sys-tem. It was invented by Visa and MasterCard in 1996 [12], [13]. A number of reputable IT organizations participated in SET developments (e.g., GTE, IBM, Microsoft, Netscape and Verisign). SET employs both symmetric and asymmetric cryptography to protect purchasing information sent between SET participants, including customer, merchant, the acquirer, and the issuer. Key management for SET is based on the use of a PKI to reliably distribute public keys between SET participants. SET supports long key lengths for both symmetric and asymmetric encryption, such as triple DES and 1,024 bit RSA [14]. SET was designed to address the limitations in the security provisions for e-commerce that were not being fulfilled by SSL/TLS. A number of security experts predicted that SET would become a standard for e-commerce payment system [15], [16], [17]. SET had "the potential to become a dominant force in assuring secure electronic transactions. SET provides an open standard not only for protecting the privacy but also for ensuring the authenticity, of electronic transactions" [16, p.22].

When SET was first introduced in 1996, it was expected to be widely used within two years [18, p.120]. SET'use was predicted to flourish in the future, since it would be supported by software, hardware, or even coexist with SSL/TLS. "Within the next two to three years, SET will become the predominant method for credit card purchases on the Internet. It will be implemented initially in software only, but will later be supported by smart cards. For some time, the currently preferred method of using SSL to encrypt payment details on their way from payer to payee will coexist with SET" [19, p.35]. Security mechanisms of SET were predicted to be a key enabler of global use of e-commerce. According to Merkow et al. [13, p.1], "Secure Electronic Transactions (SET) will help make the new 'industrial revolution' a reality

in the 21st century, this time without smokestacks or assembly lines...[t]he fact is, SET now provides the mechanism to unleash explosive and unlimited global commerce the likes of which the world has never before seen".

The use of PKI solutions was also expected to be widely used as a standard mean for e-commerce security as a result of implementation of SET. According to Birch [20, p.454], "One of the first 'mass' market uses of public key certificate infrastructure is being driven by the implementation of the Secure Electronic Transaction (SET) standard. In the near future, payment card holders who want to use their cards online will be issued with SET certificates. This means that banks are developing capabilities and infrastructure with interesting implications, but they're not the only people with an interest in the emergence of such an infrastructure and it won't be long before an entirely new business sector emerges around the use of public keys and digital signatures".

III. Security Architecture of SET

SET architecture utilises PKI to address limitations found in SSL/TLS. The following are SET technologies designed to support PKI.

A. Mandatory Digital Certificates

SET enforces the use of digital signatures to authenticate identity of customer and merchant in order to mitigate the risk of information being manipulated by a malicious third party. In the SET scheme, Certificate Authority (CA) issues digital certificates to the issuing bank or 'the issuer' *($CERT_{ISS}$ = $Sign_{(SKCA)}[PK_{ISS}]$)* and the acquiring bank or 'the acquirer' *($CERT_{ACC}$ = $Sign(SK_{CA})[PK_{ACC}]$)*. The issuer and the acquirer also play important roles in issuing digital certificates that are mandatory in the SET scheme. Customers must apply for digital certificates from their issuing bank *($CERT_{CUS}$ = $Sign(SK_{ISS})[PK_{CUS}]$)*, whilst the acquiring bank will be responsible for issuing digital certificates for merchants *($CERT_{MER}$ = $Sign(SK_{ACC})[PK_{MER}]$)* [14], [21]. In order for customers to obtain digital certificates, SET requires the customer to have been through an initialization process. For example, an asymmetric key pair for the customer must be generated. Then, the e-consumer's public key must be sent to the customer's bank ('the issuer'), which generates a public key certificate for the customer using the issuer's private signature key. The system 'root' public key will be distributed to the customer, along with the customer's public key certificate. The customer's private key will be stored in a 'digital wallet' on the customer's PC, which typically will be password protected.

B. Dual Signatures

SET ensures the confidentiality and privacy of purchasing information at all stages of transaction processing, including data transmission and data storage. In the SET scheme customer purchasing information is classified into order and payment information (OI and PI) [12], [13]. Both OI and PI are encrypted with separate public keys. Merchant public keys are used to encrypt OI *($E(PK_{MER})[OI]$)*, and acquiring bank public keys are used to encrypt PI *($E(PK_{ACC})[PI]$)*. This is to make sure that the encrypted OI can only be decrypted by the merchant and the encrypted PI can only be decrypted by the acquiring bank. Merchants will only be able to access OI, whilst PI will be forward directly to the acquiring bank in encrypted form. In addition to confidentiality protection, the integrity of OI and PI is also covered by well-cryptographic mechanisms of SET. If there was unauthorized access to a merchant's web server, the confidentiality of consumer PI would not be affected.

C. Digital Wallet

SET was designed to ensure the merchant obtain cardholder authentication as part of an e-commerce transaction. SET enforces customer self-authentication. They perform this on their local PC by entering a password that activates their digital wallet prior to initiating a transaction. The customer's PC then transmits OI and PI, encrypted with separate public keys, to the merchant *$Sign(SK_{CUS})\{E(PK_{MER})[OI]|E(PK_{ACC})[PI]\}$* [12], [13], [14]. In addition, SET was designed to protect against repudiation of a transaction by having the issuing bank and the acquiring bank both play a crucial role in verifying the transaction. The issuing bank will provide a payment authorization (PA) to the acquiring bank once the cardholder has been authenticated and agreed the payment. Similarly, the acquiring bank will inform the merchant once the PA has been provided by the issuing bank. Due to having both issuer and the acquirer involved in verifying each transaction, SET transactions are approved by major financial institutions such as Visa and MasterCard as 'card present' transactions. An overview of the interaction among the participants in SET transaction can be briefly described below.

1) $C \rightarrow M : SET_{request}$ (The cardholder requests SET initialisation from the merchant).
2) $C \rightarrow M : SET_{response}$ (The merchant responds SET initialisation to the customer).
3) $C \rightarrow M$: *Sign* $(SK_{CUS})\{E(PK_{MER})[OI]|E(PK_{ACC})[PI]\}$ (The cardholder submits and signs OI and PI encrypted by the merchant's public key and the acquirer's public key respectively).
4) $M \rightarrow A$: $E(PK_{ACC})[PI]$ (The merchant forwards PI encrypted by the acquirer's public key to the acquirer).
5) $A \rightarrow SET_{gateway} \rightarrow I : PA_{request}$ (The acquirer requests payment authorization from the issuer via SET payment gateway).
6) $I \rightarrow SET_{gateway} \rightarrow A : PA_{response}$(The issuer responds payment authorization to the issuer via SET payment gateway).
7) $A \rightarrow M : PA$ (The acquirer sends a payment authorization to the merchant).
8) $M \rightarrow C : PA_{confirmation}$ (The merchants confirm and capture the transaction).

IV. Complexity of SET

Although the security properties of SET were superior to SSL/TLS in preventing potential e-commerce fraud [22], SET was not implemented due to its complexity. The elegant security architecture of SET caused a number of significant problems. PKI solutions that were expected to be a 'magic pill' for e-commerce security issues instead became 'toxic'.

A number of criticisms were leveled at SET. These varied from poor usability to the vulnerability of PKI. According to Bellis [23, p.79], "the amount of overhead involved in the massive Public Key Infrastructure (PKI) and registration process required by SET, [means] it will never be widely adopted". That author further points out that adding the extra overhead of a PKI infrastructure was not appropriate for the payment process at that time. This view was also supported by Treese and Stewart [24], who argued that use of PKI in SET was not compatible with the existing e-payment infrastructure (of the 1990s), since SET prevented merchants from seeing consumer credit card numbers.

The use of PKI also made SET initialization complicated. In particular, key pairs needed to be established for each entity (and public keys certified) [25]. This criticism is reinformed by Lieb [26, p.2], who claimed that "the effort to obtain digital certificates has held up deployment of SET technology". In addition, operation of SET required special software to be installed by both customers and merchants, there were more tasks for customers and merchants to implement SET than those of SSL/TLS. This made SET initialisation more complicated, on top of the already complex requirements for obtaining digital certificates. Since a private key had to be stored in a digital wallet installed on a customer PC, using password protection was not considered secure enough [27], [28], [29].

The complexity of SET also made e-commerce transactions slow [30], [31]. According to Whinnett [32, p.449], "Insufficient speed also discourages on-line shopping and creates the danger that users will interrupt transactions if they are not implemented quickly enough". The low speed and high complexity of transactions was a common criticism of SET, and these properties reduced its attractiveness to both merchants and consumers. SET was also inflexible, since digital wallets needed to be present in the consumer's PC in order to address potential misuse of credit card numbers [11]. Although many software vendors were developing and standardizing digital wallets in order to make it easier for consumers to use them (e.g., the MasterCard wallet based on IBM wallet v2.1 [33] supported both the SET and SSL protocols), consumers were still required to obtain digital wallets and set up their digital certificates and credit card details into the wallets.

While there were a number of PKI interoperability issues, interoperability among SET products was also a significant problem of SET. This included certificate translations among trusted third parties (TTPs) that had different certificate policies. These sets of rules and understandings are almost inevitably different, which means that interpreting a certificate issued as part of different TTPs becomes very problematic.

V. Attempted Solutions to SET Problems

After SET experienced significant resistance from e-commerce participants, several SET extensions were introduced in order to address complexity and facilitate greater adoption of SET [34], [35], including the PIN [29], chip [28], and server-based wallet extensions [33].

A. SET/EMV

PIN and Chip extensions were proposed to address SET problems related to the secrecy of private keys. By integrating SET with PIN extensions, the vulnerability of a private key entirely protected by a password was addressed. PIN extensions provided authentication process. By integrating SET with Chip extensions, the storage location of a private key would be protected by security features of IC. PIN and Chip extensions contributed to SET/EMV, a new project of SET integrating with EMV. The EMV Specifications defined how compliant IC cards and payment terminals should interact. These specifications were established to enable IC cards to be used to replace existing credit and debit magnetic strip cards, without requiring a separate merchant terminal for each card brand. Like SET, EMV employed a PKI mechanism to support the provision of confidentiality and integrity for transactions.

SET/EMV was proposed to reduce the complexity of SET end-user initialization, but retain SET's security features [35]. There is no need for consumers to generate a key pair specifically for SET, since the key pair and certificates already contained in the EMV smart card can be used instead. SET/EMV addresses flexibility problems by allowing consumers to purchase products or services from any PC that has a smart card reader and the appropriate software installed. SET/EMV also addresses problems of the security of private keys, since the private key is no longer stored on the consumer's PC. However, SET/EMV was still rather complicated for consumers since it required an additional device (an IC card reader) to be connected to the consumer's PC. Major SET-required components and complex cryptographic mechanisms were still required for SET/EMV. Merchants were still required to invest in a point-of-sale (POS) application to allow communications from the cardholder via the SET scheme. The POS application was also needed in order to communicate with the payment gateway installed at the acquiring bank's server.

B. 3D SET

3D SET is a product of server-based wallet extensions [33] that is based on three-domain (3D) architecture [36]. With the server-based wallet, all consumer functionality (including the digital wallet software and the digital certificate) is securely implemented on the card issuer's server. Implementing the wallet and the cardholder certificate at the level of card issuer addresses implementation issues with SET, since it eliminates both the need to download wallet software to every cardholder and the requirement for a cardholder to obtain a digital certificate. The server-based wallet concept was also extended to the merchant, enabling the payment gateway and merchant certificates to be kept at an acquirer server. In this case, 3D SET was built upon the relationships between three 'domains': 1) acquirer (the relationship between the merchant and the acquiring's bank); 2) issuer (the relationship between the cardholder/consumer and the issuer); and 3) interoperability (the acquirer and issuer domains are supported by the inter-operability domain) [36]. Among the three domains, a URL redirection technique was used to enable communications.

3D SET replaced the traditional SET digital wallet that must be stored on a consumer's PC with a SET Wallet Server

in the issuer domain [37]. Instead of having the customer's certificate stored on the customer's PC, the certificate is stored on the issuer's secure server. The customer does not need to generate his/her own key pair and obtain a certificate, since all this is taken care of by the card issuer. In the meantime, the acquirer stores the merchant's certificate and implements the payment gateway at the acquirer secure server. This makes merchant initialisation simple, since the acquirer takes care of key management and certification for the merchant. As with similar to SET/EMV, major SET-required components and complex cryptographic mechanisms were also required for 3D SET. However, consumers did not require an additional device to participate in 3D SET.

VI. Summary

SET was designed to address security problems in e-payment systems perceived to be the most significant barriers restricting the growth of e-commerce. SET security architecture was based on PKI. SET was perceived as a potential magic pill for e-commerce security problems. If the main purpose of security engineering is to build a dependable system that addresses security requirements [38], then SET appeared to be the most appropriate e-payment system for securing e-commerce transactions.

However, the use of PKI in SET contributed to many problems which restricted users to adopt SET. E-commerce end-users were not willingly to adopt SET because of several usability issues. Particularly, they refused to adopt SET when they were enforced to comply with SET security requirements. A number of efforts to address SET problems sought to reduce SET complexity while maintaining its security architecture. PKI was attached by SET developers as the only solution for addressing all e-commerce security requirements. Although several significant problems of SET could potentially be addressed by evolutionary SET products such as SET/EMV and 3D SET, security was overcome by other concerns. Unfortunately, removing SET security architecture appeared to be the only solution for removing all SET problems. In other words, SET was no longer a magic pill, but something undesirable for e-commerce end-users. The story might have been different if SET has been designed in the same way as 3D SET where all SET security requirements could be handled by the 3D architecture. E-commerce end-users may just need to assured that they will be safe when they participate in e-commerce.

References

[1] A. Bhatnager, S. Misra, and H. R. Rao, "On risk, convenience, and internet shopping behaviour," *Communications of the ACM*, vol. 43, pp. 98-106, November 2000.

[2] K. Caldwell, "Global electronic commerce-moving forward," *Commerce Net: The Public Policy Report*, vol. 2, pp. 2-17, December 2000.

[3] V. Farrell, Y. Leung, and G. Farrell, "A study on consumer fears and trust in internet based electronic commerce," in *Proceedings of 13th International Bled Electronic Commerce Conference*, pp. 647-658, June 2000.

[4] M. Friedman, P. H. Kahn, and D. C. Howe, "Trust online," *Communications of the ACM*, vol. 43, pp. 34-40, December 2000.

[5] S. Giff, "The influence of metaphor, smart cards, and interface dialogue on trust in ecommerce," MSc project, University College London, 2000.

[6] C. Adams and S. Lloyd, *Understanding Public-Key Infrastructure: concepts, standards, and deployment considerations*, New Riders, Indianapolis: Macmillan, 1999.

[7] S. Farrell and M. Zolotarev, "XML and PKI-what's the story?" *Network Security*, vol. 2001, pp. 7-10, September 2001.

[8] F. Piper, "Some trends in research in cryptography and security mechanisms," *Computers and Security*, vol. 22, pp. 22-25, January 2003.

[9] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.

[10] C. J. Mitchell, "PKI standards," Information Security Technical Report, vol. 5, pp. 17-32, November 2000.

[11] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, 2001.

[12] L. Loeb, *Secure Electronic Transactions: Introduction and Technical Reference*, Boston: Artech House, 1998.

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

[14] Secure Electronic Transaction LLC (SETCo), *SET Secure Electronic Transaction Specification*, version 1.0 ed., May 1997.

[15] K. Chen, H. Lee, and B. Mayer, "The impact of security control on business-to-consumer electronic commerce," *Human Systems Management*, vol. 20, no. 2, pp. 139,147, 2001.

[16] Q. Chen, C. Zhang, and S. Zhang, "Overview of security protocol anal-ysis," in *Secure Transaction Protocol Analysis Models and Applications*, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, vol. 5111, pp. 17-72, 2008.

[17] V. C. Storey, D. W. Straub, K. A. Stewart, and R. J. Welke, "A conceptual investigation of the e-commerce industry," *Communications of the ACM*, vol. 43, pp. 117-123, July 2000.

[18] R. Oppliger, *Security Technologies for the World Wide Web*. Artech House, Massachusetts, 2000.

[19] N. Asokan and A. Phillipe, "The state of the art in electronic payment systems," *IEEE Computer*, vol. 30, pp. 28-35, 1997.

[20] D. Birch, "Secure electronic commerce – i: The certificate business public key infrastructure will be big business," *Computer Law & Security Review*, vol. 13, no. 6, pp. 454-456, 1997.

[21] Secure Electronic Transaction LLC (SETCo), *SET Secure Electronic Transaction Specification*, version 1.0 ed., May 1997.

[22] J. D. Tygar, "Atomicity in electronic commerce," *Net Worker*, vol. 2, pp. 32-43, May 1998.

[23] E. Bellis, *Beautiful Security, ch. Beautiful Trade: Rethinking E-Commerce Security*, Sebastopol: O'Reilly, 2009.

[24] G. W. Treese and L. C. Stewart, *Designing Systems for Internet Commerce*, Massachusetts: Addison-Wesley, 1998.

[25] L. D. Stein, *Web Security*, Addison-Wesley, Massachusetts, 1998.

[26] J. Lieb, "Getting secure online-an overview," Commerce Net-The Strategies Report, vol. 1, pp. 1-4, July 1999.

[27] Ford and M. S. Baum, *Secure Electronic Commerce*, Prentice Hall, 2001.

[28] Secure Electronic Transaction LLC (SETCo), *Common Chip Extension -Application for SETCo Approval*, version 1.0 ed., September 1999.

[29] Secure Electronic Transaction LLC (SETCo), *Online PIN Extensions to SET Secure Electronic Transaction*, version 1.0 ed., May 1999.

[30] P. Jarupunphol and C. J. Mitchell, "Measuring SSL and SET against e-commerce consumer requirements," in *Proceedings of the International Network Conference (INC 2002)*, Plymouth University Press, pp. 323-330, July 2002.

[31] P. Jarupunphol and C. J. Mitchell, "The future of SET," in *Proceedings of UKAIS 2002*, Leeds Metropolitan University, pp. 9-17, April 2002.

[32] D. Whinnett, "End user acceptance of security technology for electronic commerce," in *Proceedings of 4th International Conference on IS&N*(A. P. Mullery, M. Besson, M. Campolargo, R. Gobbi, and R. Reed, eds.), *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, vol. 1238, pp. 447-457, 1997.

[33] IBM e-business, *Internet Wallet Choices and Answers for Business and Technical Managers*, 1999.

[34] P. Jarupunphol, "A critical analysis of 3-D Secure," in *Proceedings of the 3rd Electronic Commerce Research and Development (E-COM-03)*, Gdansk, Poland, pp. 87-94, October 2003.

[35] P. Jarupunphol and C. J. Mitchell, "Implementation aspects of SET/EMV," in *Towards the Knowledge Society: eCommerce, eBusiness and eGovernment*, The 2nd IFIP Conference on e-commerce, e-business and e-government, IFIP I3E 2002 (J. L. Monteiro, P. M. Swatman, and L. V. Tavares, eds.), pp. 305-315, Kluwer Academic Publishers (IFIP Conference Proceedings 233), Boston (2002), October 2002.

[36] K. Wrona, M. Schuba, and G. Zavagli, "Mobile payment- state of the art and open problems," in *Proceedings of 2nd International Workshop*

WELCOM (L. Fiege, G. Mühl, and U. G. Wilhelm, eds.), *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, vol. 2232, pp. 88-100, 2001.

[37] P. Jarupunphol and C. J. Mitchell, "Measuring 3-D Secure and 3D SET against e-commerce end-user requirements," in *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*, National University of Ireland, Galway, pp. 51-64, June 2003.

[38] R. Anderson, *Security Engineering-A Guide to Building Dependable Distributed Systems*. John Wiley and Sons, 2001.

Pita Jarupunphol is a lecturer in informatics at Phuket Rajabhat University. He completed his B.B.A. (business computing) from Dhurakitpundit University (Thailand) in 1996. He received his Master's Degree in information systems from the University of Wollongong (Australia) in 1999. His research interests include different aspects of e-commerce security. In addition to e-commerce security, he is also interested in mind-machine and cognitive informatics.

Wipawan Buathong is an assistant professor and a Head of Informatics Department at Phuket Rajabhat University. She received Bachelor's Degree in computer education from Surin Teachers College (Thailand) in 1994. She completed her Master's Degree in Information Technology from King Mongkut's University of Technology Thonburi (Thailand) in 2001. Her research interests include data mining and e-commerce security.