Bulletin de la Société Royale des Sciences de Liège, Vol. 85, 2016, *p.* 1136 - 1147

Guaranteeing of trust and security in e-commerce by means of improved SET protocol

Nasrin ALISHIRVANI[1], Batool MORTAZAVI [2]
[1] Payame Noor Faculty Member, n_alishirvani@pnu.ac.ir
[2]Payame Noor Faculty Member, b_mortazavi@pnu.ac.ir

Abstract

Secure and reliable strategies are required in order to extensively operationalize e-commerce. Trust, service quality, security, privacy and dispute resolution strategies are among the most important issues needed to be considered in e-commerce transactions. In this paper, the most important e-commerce transaction protocol and its characteristics will be discussed. After discussing the limitations of this protocol, several solutions will be presented to overcome those limitations.

Keywords: Set Protocol, TSET Protocol, Security Assurance, Trust Factor

1. Introduction

With the rapid development of information technology (IT) and increasing popularity of e-commerce, two main questions have been posed:

1) how to ensure the security of data submitted on open networks (internet)?

2) how to identify and complete an online secure payment?

In this regard, the Secure Electronic Transaction (SET) protocol has been developed as a single standard for secure electronic payment and transfer of information over insecure open networks. The SET protocol has three advantages making it more secure than other protocols; these advantages include:

1. *Data Confidentiality* done by message encryption that makes it unreadable for the outsiders.
2. *Data integrity* done by confirming merchant signature and ensuring that messages are exchanged with no change.
3. *Authentication* done by digital signature certification and ensuring that claims made by people involved in a transaction are verifiable and indisputable.

Regardless of the type of payment system, payment relies on certain principles such as trust at a basic level. The buyer must trust the seller for goods delivery and the seller must trust the buyer for receiving the money on time. For credit cards, the main mechanism for the creation of trust

was comparing the buyer's signature and the signature on the back of his/her card. However, with the increase of credit card fraud, an online license check has been commonly used, even for low-value payments. Credit cards payments in SET protocol use both techniques of digital signature and online license check.

2. Regulations and responsibilities of SET protocol

In SET protocol, different rules are set; some are very simple and some are very complicated [1].

Cardholder: a person who is the holder of the payment card used to order goods and services.

Merchant: a person or an organization that sells goods or provides services to the cardholder.

Issuer: an organization that provides credit cards for the cardholders; or, the side responsible for paying the debts of the cardholders; the issuer balances the cardholders' negligence of paying their debts; issuers are actually a financial institution or a bank. Other than the credit cards, there must be no other relationship between the credit cardholders and the issuers; however, most cardholders have at least one card taken from their issuer.

Trademark: brand recognition and consciousness are two key issues considered in the marketing of credit cards. Some trademarks are owned by financial organizations issuing credit cards; other trademarks are owned by card-issuing banks (consortia of financial institutions) that advertise and promote the trademark, offer practical rules and provide a network for payments and electronic funds transfers. The SET protocol provides a controlled access to these networks via internet.

Acquirer: an organization that provides card authorization and payment services for the sellers. Most sellers are willing to accept more than one type of credit card; but, they do not want to be associated with a number of card-issuing organizations. These sellers can achieve this objective by using services offered by an acquirer. These services include support for check by phone or oral permit and e-transfer of payments to the sellers' accounts. Currently, these services can include the SET protocol services as well. The costs of these services are paid by the sellers through a small percentage of each transaction.

Payment gateway: it is provided by a receiver. The current between-SET payment gateways and networks of card-issuing organizations provide a commonality for the licenses and costs of financial operations. In other words, payment gateways are working as a proxy in card-issuing organizations' networks.

Certificate Authority (CA): provides a public key certificate. Various certificates are provided in the SET protocol for different rules set for a public key users (cardholders, sellers and payment gateways). However, all of them are related to each other in a hierarchical order; so that, each SET party can use public key certifications to build trust on the other side of each transaction.

3. SET advantages

- SET provides methods of business protection and cost breakdown along with adequate security for electronic payments; it also bans credit card fraud.
- SET retains online merchant credibility.
- SET keeps confidential information and improves the quality of online shopping; a cardholder's card number can never be stolen in SET protocol.
- SET provides banks and card-issuing organizations with a broader space on the internet; it also reduces the risk of online credit card fraud.
- SET is more competitive than other payment methods.
- SET provides a common ground for every stages of online transaction; so that, a system can be built on products of different merchants.

4. SET constraints and complexities

Despite its advantages, the SET protocol has the following limitations:

1. SET cannot guarantee that the merchant transfers goods to the buyer after receiving proper payment through the payment gateway [2[.
2. SET offers no way to ensure the quality of purchased products; if the products are not as expected by the customers, they must be able to replace them or withdraw their money;
3. SET cannot guarantee an end-to-end security (customer to merchant). During the transaction process, a network may be hacked by any organization at any point in time; if a network is hacked, more money can be taken away from customers' accounts without their knowledge [3 & 4].
4. SET does not resolve despite and denial issues; thus, when a dispute arises, the SET protocol cannot offer solutions to settle it down.
5. SET endangers customer privacy [5].
6. There is no trust mechanism in the SET protocol.

7. Important information about transactions, particularly e-commerce, does not stored via the SET protocol and there is no possibility of banning denial.
8. SET is practically large and complicated. In a typical SET transaction process, a digital certificate requires 9 confirmations and 7 data transfers; a digital signature requires 6 confirmations, 5 signatures, 4 symmetric encryptions and 4 asymmetric encryptions. The SET protocol involves many entities such as customers, merchants and banks and all of them need to change their systems for interoperability. In the SET protocol, the banking software must be installed on customers' computers and certificates are required in all stages of the transaction process; thus, the implementation of SET is relatively high [7].

In addition to the above-mentioned limitations, there are criticisms regarding poor usability and public key vulnerability in the SET protocol. In the process of payment, the accumulation of additional overhead, related to public key infrastructure, is not appropriate. SET operations require the installation of specific software on both merchants' and buyers' computers creating overhead expenses. In this protocol, the private key must be saved in an electronic wallet installed on the customer's computer; thus, password is not safe enough. Low speed and high complexity are among the most common criticisms of the SET protocol. These features make both customers and merchants discouraged. SET is not flexible because electronic wallets must be installed on the users' computers in order to address potential issues related to their credit cards' numbers. Development and standardization of the software -used to facilitate the process for the customers- require update and reinstallation that are considered as limitations of the SET protocol. Moreover, customers should install their electronic wallets and save their digital certificates and specifications of their credit cards in them. Interoperability in SET protocol is another significant problem.

5. Improving SET protocol

5.1 Hierarchical security control in SET protocol

Although the SET protocol is extensively used in e-commerce, the transactional side of SET is only a model that has been limited in the B2C model. In the SET protocol, low efficiency, insufficient security, incompatibility and high costs have been combined; therefore, in this section, the SET's hierarchy of security control mechanism and electronic transaction authentication system -that increases security- will be discussed.

The main issue in a hierarchical security control is that the security control system is divided into different levels, each requires different security considerations. Accordingly, lower levels require less security, encryption and decryption and the transaction process will be completed faster. A customer may select different levels of security based on his/her business condition or security needs. In cases of low-value transactions or when customers trust their merchants, they usually select lower levels of security to speed up the process. Otherwise, they typically select higher levels of security to ensure the transaction's security.

The security control mechanism is divided into 5 levels (A to E) [7]:

Security level A: safety requirements are not high at security level A; therefore, this level of security is mostly used in low-value transactions; no transfer, certificate authentication or digital signature is required at level A; there are less encryption and decryption processes at this level and the transaction process is completed simply and fast.

Security level B: similar to the SSL security protocol, security level B is mainly used in slightly large transactions (such as brand clothes); the only advantage of security level B is that it performs identification and authentication processes on both cardholder's and merchant's computers. When business parties' digital signatures are not required, the identification and authentication processes are not necessary, neither between cardholders and banks nor between merchants and banks.

Security level C: this level of security is higher than security level B; at this level, the SSL protocol is processed between cardholders and merchants (in SET protocol, this process has been done between merchants and banks); this level of security is mainly used in relatively large transitions (such as household electrical appliances) and high-security situations. The use of SSL protocol is easier than the use of SET protocol; therefore, all processes are completed more easily in the SSL protocol.

Security level D: this level of security is one of the main SET protocols used primarily in high-value transactions (such as expensive items); the nature of security level D is similar to the SET protocol.

Security level E: this level of security processes the improved SET protocol and is the highest level of security; security level E has all the advantages of SET protocol and resolves some of its limitations. As the encryption algorithm of SET protocol has been improved and extended, the encryption and decryption processes are completely flexible and not limited to the original SET

algorithm. Moreover, disputes between cardholders and merchants can be easily resolved at this level of security; issues such as who should maintain transaction information are resolved at this level; this level is basically appropriate for large transactions; at this level, operations are more complicated and slower than at other levels of security.

5.2 Strengthen of security in the SET protocol using digital signature center

One way to overcome the SET protocol's limitations is using electronic transaction authentication system that may be replaced with the traditional CA. Figure (1) shows the necessary structure for this. In this model of payment, the following procedures are done [7]:

1. Transaction logs are stored at the transaction authentication center. In case of any problem, the authentication center reveals the transaction logs for decision-making. It is obvious that the transaction data must not be stored by merchants or customers because they may change the information.
2. The transaction authentication center plays the role of an observer or a protector of the data. If the payment is authentically done, the customer must receive his/her goods or services. Accordingly, the authentication center records all information to ensure that the merchant will provide the promised goods or services.

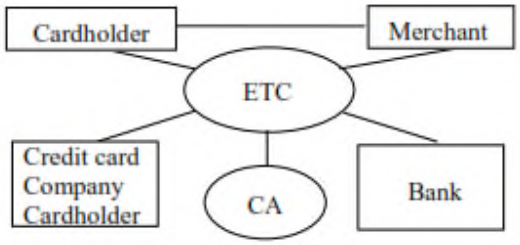

Figure 1. The improve SET payment model[8]

With the improvement of SET protocol, the number of agents participating in this protocol has reached to 4. Since this system is developed based on a PKI financial authentication center, it is highly reliable technologically and politically. Bank card information exchange centers now cover most financial networks; thus, neither the merchant, nor the cardholder needs to open a bank account in the same bank; moreover, the merchant is not required to sign a contract with the bank prior to the date of payment. After joining the system and before initiating their online

transactions, the merchants establish relationships with one or several payment systems; thus, the authentication process, used to check the trusted list, is greatly simplified.

5.3 Model of credit evaluation

Among the limitations of SET protocol is the customer's lack of knowledge about the merchant's reputation. Rep (>0), in this model, shows a merchant's reputation after his/her involvement in e-commerce. For a merchant who is just connected, the value of 0.20 is considered as the REP value; larger numbers indicate higher reputation. Satisfaction (Sat) is the user's subjective feeling that can be divided into five degrees: very good (1), relatively good (0.8), average (0.6), bad (0.4) and very bad (0.2). In high-value transactions, the merchant's reputation becomes more important for the customer. The time interval between two consecutive transactions is also an important factor in merchant's reputation.

In addition to the above mentioned factors, there is an effective factor that can be calculated as follows [7]:

When a customer asks for a merchant's reputation, an effective factor is calculated and delivered to the customer by the payment center.

'Now' refers to the time of users' requests; time of last transaction is the time span a merchant has spent to complete his/her last transaction; it can be calculated in terms of hour, day, month, etc. When a user announces his/her assessment of a particular merchant, payment center updates the effective factor and adds Sat value to the previous Rep value. In this equation, the importance of transaction (Trm) and the average transaction value (Arg Trm) are also considered (their effects are reflected as a weight coefficient (Trm/Arg Trm)). During a given time, if a customer does not announce his/her assessment, the minimum Sat value (0.2) will be automatically considered by the payment center.

5.4 Token based secure electronic transaction (TSET)

As mentioned, security and trust are two important factors in e-commerce. In the Token-based SET (TSET) protocol, issues related to trust between merchants and customers, customer satisfaction and end-to-end security are considered. In the TSET protocol, there is a trusted third party that uses the SLL protocol [8]. In this model, the TTP directs different components involved in a transaction. A trusted third party keeps all transaction logs and uses them in case of

any dispute. The saved transaction logs provide authentic records of all transactions and solve issues such as late or non-payment of debts. Furthermore, data related to merchants' reliabality are saved in the TTP and customers can access them before initiating any transaction. Finally, the TTP can act as a mediator in the event of any dispute. In figure (2), the transaction process in the TSET protocol is shown.

Two factors of trust and token will be discussed in the following paragraphs:

Trust factor: the proposed method to calculate the trust factor is as follows [9]:

The merchant's trust factor remains in the TTP. A customer can view his/her intended merchant's trust factor via the TTP website; if the merchant's trust factor is satisfactory, the customer can continue the transaction. Trust factor is calculated as follows:

In this equation, TF_M is merchant's trust factor and TV_M is merchant's reliability. A merchant's reliability is determined by the total number of transactions and the total number of customers' complaints. Reliability can be calculated as follows:

When a merchant receives a customer's demand regarding returning his/her money or replacing a product more than once, the reliability will be calculated as follows:

Based on this equation, the customer does not have to experience the same cycle twice. The trust factor is divided into 10 degrees ranging from 0 to 100; trust factor is announced to the customers; so that, they can about their transactions.

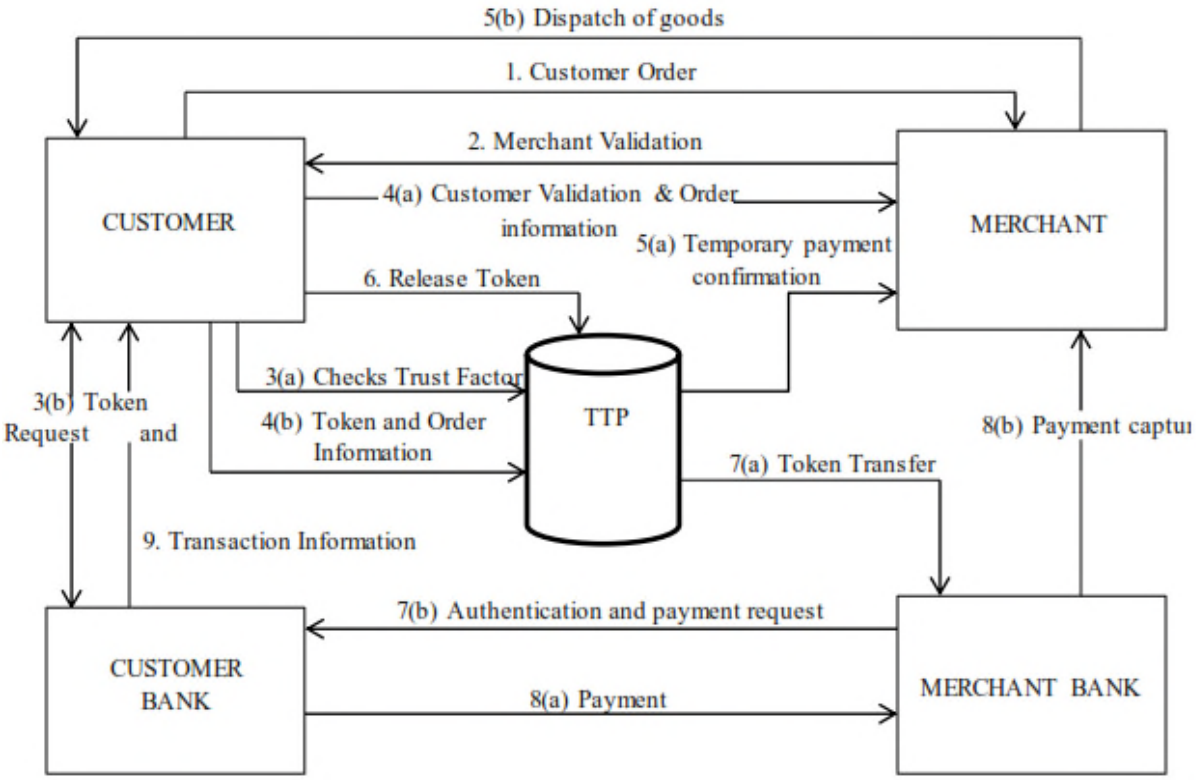

Figure 2.The transaction process in the TEST protocol

Token format: for each transaction, the customer's bank creates a token (figure 3) containing information about the payment, customer's digital certificate, merchant's digital certificate, token ID and time tag; the bank only releases an amount of money indicated in the token. The customer's and merchants digital certificates show that a token is created for a specific customer and a specific transaction. Token ID is exclusive for each transaction; it is a 256-bit code used by the customer's bank only for one transaction. When a transaction is done via a specific token ID, the token ID will never be recreated. Token ID is encrypted via the AES symmetric key and Rijndeal Algorithms [10]. Time tag is used as a valid proof of the time and date of transaction in case of any dispute.

AM	$DCert_C$	$DCert_M$	TKN_{ID}	TS

Figure 3.stucture of the Token

The customer's bank keeps a copy of password. Therefore, before releasing the transaction money, customer's bank can compare the password with its copy. In case of any fraud or

interference, the transaction will be immediately stopped by the customer's bank. Then the customer bank reports that the password has been tampered. Then, TTP sends a message to the customer and the whole process will be done once again. Thus, the password ensures an end-to-end security in the TSET protocol, because any change in password is immediately identifiable and stops the transaction process.

The TSET protocol characteristics can be summarized as follows:

Trust mechanism: according to the TSET, customers can check a merchant's reliability prior to the initiation of a transaction. Everything depends on the customer in the TSET protocol.

Service quality: in the new protocol, customers can return their product if its quality is not as expected. TTP acts as the ruling party and ensures that a merchant returns a customer's money or exchanges his/her product on time. Failure to settle this dispute leads to a decreased trust factor. Thus, this protocol guarantees that the merchants will provide the best products or services in their transactions.

End-to-end security: the new SET protocol ensures an end-to-end security. At any point in a transaction, the customer's bank detects any change in password and immediately stops the transaction process. Therefore, the end-to-end security ensures that a merchant receives a preset amount of money and no more.

Disputes: all transactions are done through the TTP that ensures the fairness of transactions. If any dispute arises, the TTP can offer the saved transaction logs. Neither the customer, nor the merchant can deny the transaction logs.

Privacy: in this protocol, neither the merchant, nor his/her bank has access to the customer's accounts information. In addition, the transaction data are only known by the customer and the merchant.

6. Conclusion

Security, service quality and privacy are important factors in e-commerce. It has been indicated that the SET protocol cannot adequately ensure the mentioned factors. However, this protocol can be improved by the use of a hierarchical security control system, digital signature authentication center and calculation of merchants' reliability. By using trust factors and tokens, the TSET ensures an end-to-end security and encourages the merchants to provide their customers with goods or services with high quality. Moreover, the availability of a trusted third

party is a helpful reference for solving possible disputes between the merchants and the customers. Accordingly, the TSET protocol has guaranteed issues necessary in e-commerce.

References

1. Sung Woo Tak, Eun Kyo Park,A Software Framework for Non-Repudiation Service Based on Adaptive Secure Methodology in Electronic Commerce, Kluwer Academic Publishers, 2004
2. Xun-yi Ren, Li-li Wei, Jun-feng Zhang, Xiaodong Ma, The Improvement of SET Protocol based on Security Mobile Payment, Journal of Convergence Information Technology, Volume6, Number 7, July 2011.
3. Sugata Sanyal, Ayu Tiwari and Sudip Sanyal (2010), A Multifactor Secure Authentication System for Wireless Payment , Emergent Web Intelligence: Advanced Information Retrieval Book Series: Advanced Information and Knowledge Processing, First Edition, 2010, Chapter 13, pp. 341-369, XVI, Springer Verlag London Limited, 2010.
4. Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal (2005),'CompChall: Addressing Password Guessing Attacks', Information Assurance and Security Track (IAS'05), IEEE International Conference on Information Technology: Coding and Computing (ITCC'05), USA. April 2005, pp 739-744, IEEE Computer Society.
5. Tan Soo Fun, Leau Yu Beng, Rozaini Roslan, and Habeeb Saleh Habeeb (2008) ,'Privacy in New Mobile Payment Protocol', In Proceedings of World Academy of Science, Engineering and Technology, Vol.30, pp. 443-447.
6. M Franklin, M Yang, "Towards Provably Secure Efficient Electronic Cash," ReportCUCS-018-92. Columbia University Department of Computer Science, 2005.
7. Zhang Boping, Shang Shiyu, "An Improved SET Protocol", Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), Huangshan, P. R. China, August 21-23, 2009, pp. 267-272
8. Xu Yong and Liu Jindi (2010), 'Electronic Payment System De-sign Based on SET and TTP,' 2010 International Conference on EBusinessand and E-Government, Guang-zhou, 7-9 May 2010, pp. 275-278.
9. Rajdeep Borgohain, Chandrakant Sakharwade, Sugata Sanyal, TSET:"Token based Secure Electronic Transaction", 2013.

10. Joan Daemen, Vincent Rijmen(2002), ‘The Design of Rijndael: AES - The Advanced Encryption Standard.’ Springer, 2002. ISBN 3-540-42580-2.