Snags and Remedial Solutions of Secure Electronic Transaction

R. Vijayalakshmi

***Abstract*— Secure Electronic Transactions is a very wide-ranging protocol used for secure transaction which is to provide authentication and confidentiality. It contains some inadequacies such a low in processing speed when 56 bit key DES is used and it also faces complexity problem. For the above hitch I designate curative elucidation formulated by different authors in this paper.**

***Index Terms*— E-commerce; Secure Electronic Transaction(SET); Data Encryption Standard(DES); Advance Encryption Standard(AES); Order Information(OI); Payment Information(PI); Payment Order Message Digest(POMD); Order Information Message Digest(OIMD); Payment Information Message Digest(PIMD); Public key Infrastructure(PKI);**

I. Introduction

E-commerce refers to a wider-angle of online products and services. Organizations interact with each other electronically in a prescribed format rather than by manual exchanges data it is the business transaction.

Online payments are performed with the help of online transaction which uses SET Protocol. SET is a communication protocol to protect the credit card details during online transactions which put on a specific standard.

SET bring into play array of cryptographic algorithms to truss the surreptitious data's throughout the communication. There are four major security requirements for safe e-commerce. They are Authentication, Encryption, Integrity and Non-repudiation. To provide security during electronic transaction encryption method is implemented. Encryption can be implemented in two ways, Asymmetric (public-key) and symmetric (secret-key) cryptography. The secret-key cryptography used in SET is DES, which is used to protect PIN numbers during financial transactions. SET uses asymmetric cryptography method (RSA) to encrypt the DES keys and for authentication [1].

II.PAYMENT PROCESSING:

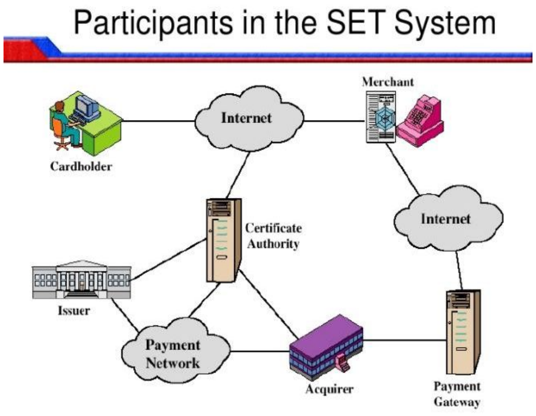
Merchant Certificate is an indication of that the merchant is an endorsed merchant authenticated by acquirer bank. Order outline restrain order number, Items, quantity, price per quantity, total price, etc.,

Then the customer checks the order form for his requirement and fills it. He sends payment transaction details, order information and customer certificate to the merchant.

Payment transaction details contains Credit card no, date of expiry, etc., and customer certificate indicates that the he is an authenticated customer. In view of the fact that the payment information is not to be mentioned so it is hurl in an encryption form which cannot be decrypted by merchant.

The OI, PI are hashed using an algorithm and the message digest OIMD, PIMD are created respectively [12]. Via private key of the customer, this POMD shaped from PIMD & OIMD is encrypted. This is labeled as Dual signature. Along with DES -56 key Order Information, dual signature, Public key of the customer and PIMD is encrypted and sent to the merchant using merchant's public key. At the merchant side, the reverse process is applied to view the order details.

During this payment processing the SET achieves confidentiality and authentication. Without the STP protocol facilitate the issuers to substantiate the card holder for the duration of transaction making use of the third party (VISA or Master card). So the transaction involves card holder, merchant, Gateway, card issuer and allows the card holder to securely transform information using digital certificate.



III.FUNCTIONS OF SET:

Provide for confidential payment information that is transmitted with payment information

Ensure integrity for all transmitted data

Provide authentication that a buyer is a legitimate user of a branded bank card account

Manuscript received May 18, 2017

R. Vijayalakshmi, Department of computer science and Applications, Nazareth College of Arts & Science, University of Madras, Chennai, Tamil Nadu, India

Provide authentication that a merchant can accept bank card payment

Ensure the use of the best security practices & design techniques to protect all legitimate parties

Ensure the creation of a protocol that is neither dependent on transport security mechanism nor prevents their use

Facilitate and encourage interoperability across software and network provider.

IV.DISADVANTAGE:

Time is required to build consequence among a critical mass of users

It may take several years for technical specification and implement to be installed tested and debugged

It may take several years to address how web commerce should be integrated for handling payments

Two or three years are needed to build confidence among participants that secure e-commerce transaction.

V.SPEEDY PROCESS:

When DES-56 bit key is used for encryption, due to small size of key we cannot attain the security and the progression becomes very slow, it is overcome by AES 128 bit key [2]. It also enhances the security of the payment processing. Later than accomplishment of AES 128 bit key there is an augment in payment dispensation [3].

VI.COMPLEXITY OF SET:

When comparing with SSL, SET procures more security properties in preventing fraud [4]. SET faces the complexity problem. According to Bellis [5, p.79],"the amount of overhead involved in the massive public key infrastructure and registration process required by SET, it will never be widely adopted". The use of PKI in SET turns out to be thorny, since key pairs are considered necessary for each encryption. The intricacy ended ecommerce transaction slows [8] [9].

SET did not support online shopping due to this low speed. The low speed and high complexity was common censure of SET and this makes merchant and consumer to word SET processing.

SET was also firm; In order to address potential mishandling of credit card number since digital wallets needed to be present in the consumers PC [10].

To address complexity SET includes the PIN [7], CHIP[6]. These extensions were used to handle the secrecy of private keys. The vulnerability of private key exclusively cosseted through a password, via the PIN extension [1]. The storage area of private key would be confined by security features of IC, using the CHIP extension [11]. These two extensions are contributed to EMV (Europay - MasterCard-Visa) which employs a PKI mechanism for providing confidentiality and integrity of transaction. Thus the complexity of SET is solved.

CONCLUSION:

E-commerce is the gift to do business through the Internet. It is not just present of computers and absence of papers. More security issues are there which keeps away many organizations from doing business through web. Secured Socket Layer (SSL) and Secured Electronic Transactions (SET) are the foremost well-liked Ecommerce security protocols. Each one of them has its realm of use, its products and its own encryption procedure. Doing analysis is not an easy thing. Through internet exchange of critical data such as credit card number, passwords, or any sensitive private information is not an easy processing, but some remedy measures are applicable. Thus we studied two drawbacks and solutions.

REFERENCE:

[1]Iyanda Olukunle, Otusile Oluwabukola, Awodele Oludele,"Overview of Secure Electronic Transaction International Journal off Artificial Intelligence and Mechatronics, Volume 2, Issue 3, ISSN 2320-5121.

[2] NIST,"Selecting the Advance Encryption Standards"2003.

[3]Satyanshu Srivastava,Rakesh Bharti, "Security Enhancement in Secure Electronic Transaction Protocol" IJEIT volume 2,Issue 6, December 2012.

[4]J.D.Tygar,"Atomicity in electronic commerce." Net worker,vol.2, pp. 32-43,may 1998.

[5]E.Bellis, Beautiful security,ch. Beautiful Trade: Rethinking E-commerce Security,Sebastopol: O'Reilly, 2009.

[6]Secure Electronic Transaction LLC (SETCo), Common Chip Extension-Application for SETCo Approval, version 1.0 ed., September1999.

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

[8]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.

[9]P.Jarupunphol and C.J.Mitchell,"The future of SET,"in Proceedings ofUKAIS 2002,LeedsMetropolitanUniversity,pp.9-17,April 2002.

[10]E.Resorla, SSL AND TLS: Designing and Building Secure Systems, Addison-Wesley, 2001.

[11]Pita Jarupunphol and Wipawan Buathong, "Secure Electronic Transaction: A Case of Secure System Project failures" IACSIT International Journal of Engineering and Technology,Vol. 5,No.2,April 2013.

[12 Shao-ping Chen School of Banking, Jiangxi University of Finance and Economics, China, 330013 "Study on A Safe and Efficient Payment Modell in E-commerce".

Authors

R. Vijayalakshmi, Assistant Professor in Department of Computer Science and Applications at Nazareth College of Arts and Science, Avadi, Chennai, India. Her research interests are Software Engineering concepts and E-commerce.