Removal of Digital Envelopes in SET Protocol Using Diffie Hellmann Key Exchange Algorithm

Sachin Tripathi, Sumitra Kisan

***Abstract*- The E- marketing has grown exponentially over the last decade and has really helped the merchants to sell their products and services to large number of customers. The prime requirements for any E-commerce transactions are privacy, authentication, integrity maintenance and non-repudiation. The SET protocol has been developed by the major credit card companies in association with some of the top software corporations to ensure secure credit card transactions ,where the prime requirements are achieved using cryptographic techniques such as encryption/decryption, digital signatures, digital certificates and digital envelopes.. The SET protocol uses various numbers of digital envelopes for secure exchange of secret keys between cardholder, merchant and payment gateway. The digital envelopes are formed by encrypting the randomly generated session key using public key cryptography that requires key certificates provided by trusted third party called Certification Authority (CA). The present paper attempts the removal of same using well known Diffie Hellmann key exchange algorithm. The proposal results in less number of keys for secure exchange of information, reduces the time required to encrypt/decrypt the digital envelopes , less overhead require for authentication of keys used to form digital envelope .The comparison with existing SET implementation is also addressed in the paper that shows the effectiveness of proposal.**

***Keywords*- Diffie Hellmann, Digital Envelope, Hash function, RSA, SET Protocol.**

I. INTRODUCTION

INTERNET is widely used for many purposes such as entertainment, information, communication, electronic commerce etc. In the emerging global economy, e-commerce and e-business have increasingly become a necessary component of business strategy and a strong catalyst for economic development. Electronic commerce refers to a wide range of online business activities for products and services. It also pertains to any form of business transaction in which the parties interact electronically rather than by physical exchange or direct physical contact consists of the buying and selling of products or services over Internet and other computer networks. Online transactions are an important part of the e-commerce. When a customer purchase a product or services over Internet then for payment online transactions are used. For the successful online transaction there should be a protocol and that protocol should contain some properties related to the security and other aspects. On February 1,1996, Visa International and MasterCard announced together with others(including Microsoft, IBM, Netscape, SAIC,GTE, RSA, Terisa Systems, and VeriSign), the development of a single technical standard for safeguarding payment card purchases made over open networks. This standard was to be called the Secure Electronic Transaction (SET) [1][2][3]. Prior to this effort, Visa and MasterCard were pursuing separate specifications, and the new SET specification represented a convergence of those individual efforts. In mid-December 1997, a new corporate entity called SET Secure Electronic Transaction LLC (SETCo) was formed by Visa and MasterCard to provide a structure that would govern and direct the future development of the SET (Secure Electronic Transaction) protocol as well as other key functions that are required to support the implementation of this standard. In conjunction to this, agreements with American Express and JCB Co., Ltd. to become full partners in SETCo have been negotiated. SET protocol is designed for this purpose. Credit cards, smart card etc. transactions come under the category of Secure Electronic Transaction (SET).

The study of SET protocol conclude that it uses various numbers of digital envelopes that requires number of cryptographic operations such as encryption, decryption, authentication of public key provided by Certification authority CA, and number of key exchange operation among the participants. So, in this proposal, our aim is to remove the digital envelopes used in the SET protocol so that the above problem can be solved. It can be done with the help of Diffie-Hellman (DH) key exchange algorithm [4, 5]. The basic principle used is that generate the secret key at each participant using DH protocol instead of exchange of same using digital envelopes.

Manuscript received 01.27.2012, revised 04.13.2012.

Sachin Tripathi is with the Department of Computer Science & Engineering, Indian School of Mines, Dhanbad, Jharkhand-826004.
E-mail: var_1285@yahoo.com.

Sumitra Kisan is with the Department of Computer Science & Engineering, Indian School of Mines, Dhanbad, Jharkhand-826004.
E-mail: sumitrakisan@gmail.com.

II. ROLE OF DIGITAL ENEVELOPES

After the study of present SET protocol implementation, it is found that a number of digital envelops are used during SET message exchange. The digital envelope is nothing, but the randomly generated session key which is encrypted with the public key exchange key of the recipient participants. So to send the session key, the public key exchange key of the various SET participants are required prior to the communication.

From the study, it is found that digital envelops are used during following message exchange between the various SET participants:

1) The cardholder sends the digital envelopes to the payment gateway through the merchant, so that the payment gateway can get the symmetric key to decrypt the payment information.

2) The merchant sends the digital envelopes to the payment gateway to decrypt authorization related information.

3) The payment gateway sends digital envelopes to the merchant to decrypt the authorization response block. It also sends digital envelops to merchant to decrypt the captured token information.

4) The merchant again sends the digital envelop to the gateway to decrypt the captured token.

5) Finally the gateway sends the digital envelop to merchant to decrypt captured response block.

Hence it is clear that so many public key exchange keys are used for the above digital envelopes. It also increases the communication among the participants. And the other problem is that it increases the cost and overhead to generate and authenticate the key exchange key which is done by Certificate Authority [2].

III. PROPOSED SCHEME FOR DIGITAL ENEVELOPE REMOVAL

According to the Diffie-Hellman Key Exchange Algorithm, the sender and the receiver can generate the same secret key. So it does not need to send the encrypted symmetric key to the receiver to decrypt the message. In SET protocol the Diffie-Hellman Key Exchange Algorithm can be applied in the case where the two participants use the same secret key.

In the SET protocol the following pairs use same secret randomly generated session key:

- Cardholder → Payment gateway
- Merchant → Payment gateway

As discussed in previous section, five different digital envelopes are used. So Diffie-Hellman Key Exchange algorithm can be used five different times during complete SET message exchange in between the cardholder, merchant and the payment gateway. For sake of clarity block diagram is shown below figure 4.1. The key generation will be made as per the well known Diffie Hellmann protocol between cardholder and payment gateway, merchant and payment gateway. The common session keys will be generated as a result.

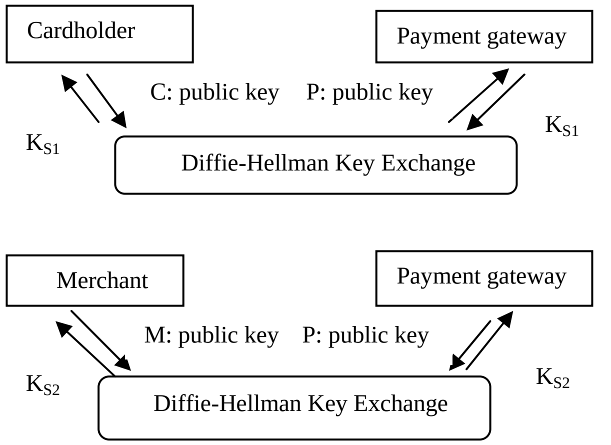

Fig. 1. Diffie-Hellman Key Exchange Algorithm in SET protocol

IV. COPMPARISION WITH EXISTING SET PROTOCOL IMPLEMENTATION

In the existing SET protocol 5 digital envelopes are used among the cardholder, the merchant and the payment gateway in different way as mentioned in the previous section. Because of the digital envelopes, the overhead is more in the existing SET protocol.

As the justification: - The digital envelope is generated by encrypting the secret key (randomly generated session key) with the public Key Exchange Key of the recipient. So, prior to the communication the sender requests for the public Key Exchange Key to the recipient. Then the recipient publishes its public Key Exchange Key with the authentication certificate which adds more overhead to the SET protocol. Because, issuing of the certificate is a big task and it cost a lot. It involves the chain of Certificate Authority.

Hence for generating one digital envelope the following operations are needed

1) Sending request message to the recipient for public key exchange key
2) Recipient issues the key authentication certificate from the CA
3) Recipient sends the public key exchange key with the key certificate

4) Sender encrypts the message containing secrete key with the public key exchange key of the recipient.
5) Recipient decrypts the message to get the secrete key with its private key exchange key.

As mentioned above, in the existing SET protocol 5 different digital envelopes are used.
Hence by using the Digital Envelope in the SET protocol the overall operations required are:-

TABLE I
LIST OF OPERATIONS REQUIERDE

Sl.No	Name of the operation	No. of Times Usec (Existing SET)	No. of Times Used(Proposed SET)
1	Sending request message to the recipient for public key exchange key	5	0
2	Recipient issues the key authentication certificate from the CA	5	0
3	Recipient sends the public key exchange key with the key certificate	5	0
4	Message encryption	5	0
5	Message decryption	5	0

From the table it is clear that apart from request/response message exchange, in proposed SET implementation, five encryption/decryption security operations are not required. From the previous research work [6], the encryption and decryption time performance are already observed. According to that research work the encryption and decryption time performance are as follows:-

TABLE II
ENCRYPTION TIME PERFORMANCE (in msec)

	DES-64	AES-128	AES-192	AES-256
5MB	1468.75	828.125	671.875	640.625
10MB	2625.0	1890.625	1796.875	1359.375
15MB	3781.0	3125.0	3165.625	3109.375
20MB	4171.875	3671.875	3312.500	3203.125

TABLE III
DECRYPTION TIME PERFORMANCE (in msec)

	DES-64	AES-128	AES-192	AES-256
5MB	156.25	140.625	140.625	140.625
10MB	343.75	375.0	359.375	390.625
15MB	828.125	453.125	437.5	437.5
20MB	1109.375	1078.125	1003.125	993.375

Hence the performance of proposed SET protocol is improved over present SET implementation. Hence all other operations (cryptographic operations), involved with the digital envelope are eliminated. It reduces all the overheads, listed above which are generated by the digital envelope. Though, many calculations are needed for the Diffie-Hellman Key Exchange algorithm, the cost involved is less than the cost involved with the digital envelope. It is clear that the number of encryptions and decryptions used in digital envelope are not needed in our proposal. Hence according to the encryption and decryption time performance, five times of each encryption and decryption time can be reduced by using any encryption/decryption technique mentioned above. It also reduces 5 keys which are used as Key Exchange Key and overhead required for authentication of same provided by CA's. Thus it increases the performance of the SET protocol.

V. CONCLUSION

SET is a complex which includes advanced cryptography for safe data transfer, and hashing technologies for data integrity. It uses digital certificates for authentication of the parties involved in the transaction. After study of SET protocol it is found that it uses number of digital envelopes to send the secrete key (randomly generated session key). The digital envelope involves many overheads (Encryption, Decryption, Key exchange key, Certificates). All these can be removed if we eliminate the use of digital envelope. Hence in the proposed scheme the essence of digital envelope is removed with the help of well known Diffie-Hellman Key Exchange algorithm. The performance comparison results in that proposed scheme reduces 5 cryptographic operations (encryption/decryption), 5 key exchange keys and 10 message transmissions (requesting and receiving of public key exchange key). It also eliminates the overhead for certificates that means the need of CA.

REFERENCES

[1] SET Secure Electronic Transaction Specification: Formal Protocol Definition, May 1997.

[2] SET Secure Electronic Transaction Specification: Formal Protocol Definition, May 1997.

[3] W. Stallings, "Cryptography and Network Security 4th Ed," Prentic, 2005.

[4] Lawrence C. Paulson Computer Laboratory, University of Cambridge "Verifying the SET Protocol: Overview" Formal Aspects of Security, Lecture Notes in Computer Science, 2003, Volume 2629/2003, 233-237.

[5] White Diffie and Martin Hellman. New Directions In Cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976.

[6] E.Rescorla, "Diffie-Hellman Key Agreement Method", RFC-2631, June 1999.

[7] Satyanshu Srivastava, "Performance comparison of DES and AES encryption techniques in SET protocol", thesis in M.Tech. in computer applications from ISM Dhanbad, May 2010.