Digital Envelope Removal Using Enhanced Diffie Hellman Key Exchange In Set Protocol

V.Sumathy[1], R.Evangelin Hema Mariya[2]

[1,2].Assistant professor, Kingston Engineering college, Vellore-59

Abstract: An incredible Communication needs quality and security for better performance .Nowadays Security plays a vital role in Internet. Nowadays the E- marketing has grown exponentially 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 uses cryptographic techniques such as encryption/decryption, digital signatures, digital certificates, digital envelopes and 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 proposed work attempts the removal of digital envelope using well known Diffie Hellmann key exchange algorithm. The hardness in security is enhanced by improving the Diffie-Hellman encryption algorithm by adding some more security codes in current 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.

Keywords- Modified Diffie Hellmann algorithm , Digital Envelope, Hash function, SET Protocol, Private Key, Public Key, Secret key.

1. INTRODUCTION

The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. Internet is widely used for many purposes such as entertainment, information, communication, electronic commerce etc. In the emerging global economy, ecommerce 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. SET protocol is designed for this purpose. Credit cards, smart card etc..transactions come under the category of Secure Electronic Transaction(SET).Diffie-Hellman will be used in many applications like SSL, SSH, SET. This paper is framed fully on how digital envelopes removed in SET using proposed Diffie Hellmann key exchange algorithm.

Diffie-Hellman in SSL

Secure Sockets Layer (SSL) is a cryptographic protocol which was developed by Netscape. SSL (now up to version 3.0) is a tunnelling protocol that allows a proxy server to act as a tunnel between the client and the server. SSL runs at the application layer and provides secure transaction of data such as credit card details, between a client and an E-commerce server. SSL uses certificates, private/public key exchange pairs and Diffie-Hellman key agreements to provide privacy (key exchange), authentication and integrity with Message Authentication Code (MAC). This information is known as a Cypher Suite and exists within a Public Key Infrastructure (PKI). This is most commonly done for business/financial traffic, e.g. credit card transactions. Specifically, "securing information" in this context, means to ensure confidentiality (prevent eavesdropping), authenticity (the sender is really who he says he is), and integrity (the message has not been changed en route). Users may not know they are using SSL, but they probably will notice the padlock.

Diffie-Hellman in SSH

Secure Shell (SSH) is a both a protocol and a program used to encrypt traffic between two computers. It is a very common protocol for secure remote login on the Internet. SSH performs the initial key exchange using the "diffie-hellman-group1-sha1"method.The Diffie-Hellman key exchange provides a shared secret that cannot be determined by either party alone. Furthermore, the shared secret is known only to the participant parties. In SSH, the key exchange is signed with the host key to provide host authentication. The security of the Diffie-Hellman key exchange is based on the difficulty of solving the Discrete Logarithm Problem (DLP).

Diffie-Hellman in SET

Secure Electronic Transaction (SET) was a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET was not itself

a payment system, but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion.When a customer purchase a product or services over Internet then 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. This is to be called the 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.

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. EXISTING 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. 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.

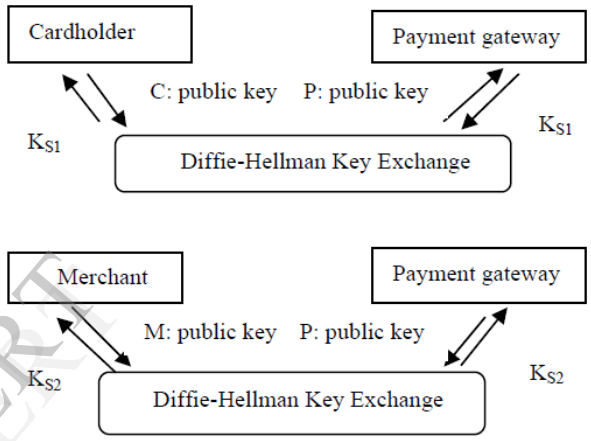

Fig. 1. Diffie-Hellman Key Exchange Algorithm in SET protocol

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 secret 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.

IV. PROPOSED SCHEME

Digital Envelope Removal Using Enhanced Diffie-Hellman Key Exchange Algorithm:

1. Global Public Elements: Prime number q; $\alpha < q$ and α is a primitive root of q.
2. User A Key Generation and User B Key Generation:
3. Select private X^A ,$X^A < q$
   Select private X^B, $X^B < q$
4. Calculate public Y^A; $Y^A = \alpha X^A \bmod q$
   Calculate public Y^B ; $Y^B = \alpha X^B \bmod q$
5. Calculation of Secret Key by User A:

$K = (Y^B) X^A \bmod q$

Calculation of Secret Key by User B: $K = (Y^A) X^B \bmod q$ .The result is that the two sides have exchanged a secret value. Furthermore, because X^A and X^B are private, an adversary only has the following ingredients to work with: q, α, Y^A, and Y^B. Thus, the adversary is forced to take a discrete logarithm to determine the key. For example, to determine the private key of user B, an adversary must compute $X^B = dlog_{\alpha, q}(Y^B)$. The adversary can then calculate the key K in the same manner as user B calculates it. The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo q prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible. The Enhanced Diffie-Hellman Key Exchange Algorithm

Sender Side

1. $X^a < q$ (user can select any random number less than q)
2. $Y^a = a X^a \bmod q$ (Y^a is a public key of sender)
3. $K = Y^b X^a \bmod q$ (where Y^b is a public key of receiver and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Encrypt every letter of plain text using pow.

Receiver Side

1. $X^b < q$ (user can select any random number less than q)
2. $Yb = a X^b \bmod q$ (Y^b is a public key of receiver)
3. $K = Y^a X^b \bmod q$ (where Y^a is a public key of sender and K is a private key)
4. $pow = 2^K$
5. pow = pow + q

Decrypt every letter of Cipher text using pow.

Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User A can generate a one-time private key X^A, calculate Y^A, and send that to user B. User B responds by generating a private value X^B calculating Y^B, and sending Y^B to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Alternatively, user A could pick values for q and α and include those in the first message.

V. Result Discussion

S.NO	Name of the operation	No. of Times Digital Envelope Used in SET	Digital envelope removal using modified Diffie hellman key exchange
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

TABLE I LIST OF OPERATIONS REQUIRED

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. The below graph shows the comparison between the existing and the proposed scheme. Thus the proposed key exchange will increase the

complexity of the crypt analysis.

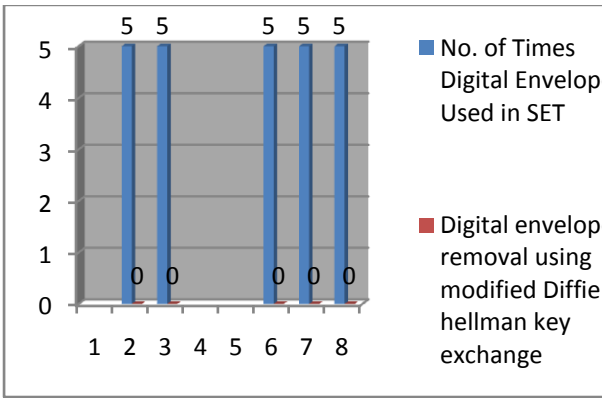

Fig 3: comparison of Existing and proposed scheme.

VI. 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 existing 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 it 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 he overhead for certificates that means the need of CA. The hardness in security is enhanced by modified Diffie-Hellman encryption algorithm by adding some more security codes in current 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 proposed key exchange in SET protocol is more resistant for crypt analysis like man-in-the-middle attack, brute force attack etc.,

VII.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.
[8] Eun-Jun Yoon and Kee-Young Yoo, "An Efficient Diffie-Hellman-MAC Key Exchange Scheme", 2009 Fourth International Conference on Innovative Computing, Information and Control.
[9] Michel Abdalla, Mihir Bellare, and Phillip Rogaway, " DHIES: An encryption scheme based on the Diffie-Hellman Problem", In Proc.of ACM CCS '01, ACM Press September18,2001.
[9] SSH Communications Security Home Page, http://www.ssh.com/.
[10] OpenSSH Home Page, http://www.openssh.com/.