ROLE OF MULTIPLE ENCRYPTION IN SECURE ELECTRONIC TRANSACTION

Himanshu Gupta
Senior Faculty Member,
Amity Institute of Information Technology, Amity University Campus,
Sector – 125, Noida (Uttar Pradesh), India.
E-mail: himanshu_gupta4@yahoo.co.in

Vinod Kumar Sharma
Professor & Dean, Faculty of Technology,
Gurukula Kangri Vishwavidyalaya,
Haridwar, India
E-mail: vks_sun@ymail.com

ABSTRACT

Security of electronic transaction over insecure communication channel is a challenging task that includes many critical areas as secure communication channel, strong data encryption technique and trusted third party to maintain the electronic database. The conventional methods of encryption in Secure Electronic Transaction can only maintain the data security. The confidential information of customer could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption methods to enhance data security as well as authentication of data communication. The multiple encryption technique provides sufficient security for electronic transactions over wireless network. In this research paper, the needs of multiple encryption technique in Secure Electronic Transaction are proposed to enhance the security of confidential data. This technique increases the data security in such a manner that unauthorized user can not access any part of information over wireless network as internet.

KEYWORDS

Secure Electronic Transaction ; Data Security; Multiple Encryption.

1. INTRODUCTION

Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet. SET is a set of rules and regulations that enable users to perform financial transactions through existing payment system over insecure wireless network (internet) in much secure and reliable manner [1]. SET is an application to provide various security services as confidentiality, data integrity and authenticity for all electronic transactions over the internet. Secure Electronic Transaction (SET) is essential for the successful electronic transaction over the wireless network; confidentiality is required to hide the sensitive data from unauthorized user, data integrity is required to ensure that whole information is transferred without any modification through intruder, and authentication is

required to ensure the sender and receiver that the performed transaction is valid and authentic [2].

In electronic transaction over insecure wireless network as internet, various risk factors are analyzed: There is no option to see the product physically which we want to purchase, There is no guaranteed security of online transaction over wireless network, and A long time is required to deliver the ordered item to the customer. In fig 1, various risk factors by internet non-shoppers and shoppers can be seen through a survey.

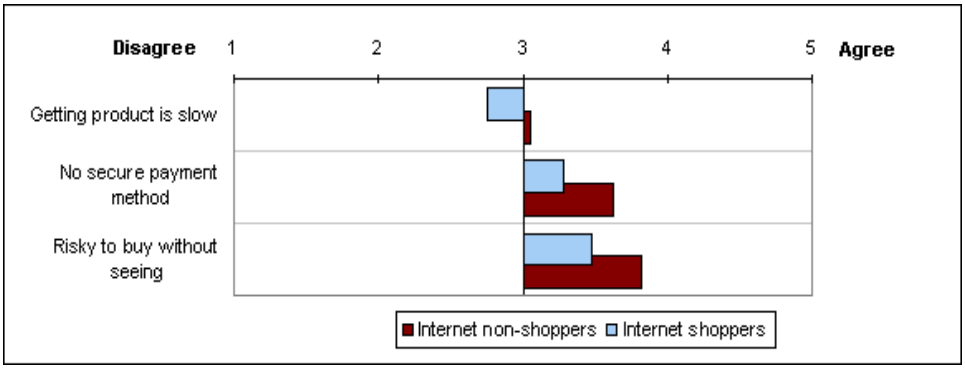

Fig 1: Risk factors perceived by shoppers and non-shoppers

SET uses a security algorithm that generates a digital certificate as a substitute for the customer's credit card number. This allows merchant to credit transaction amount from customer's credit cards account without asking credit card number. SET use effective cryptographic techniques like as digital signature standard (DSS) to generate digital certificates and public key cryptographic algorithm to allow communicating parties to authenticate each other and exchange required information in secure manner [3].

In Secure Electronic Transaction (SET), merchant's website, secured web server and financial bank's server for the verification of customer's database makes an important role for successful transaction. Secure Electronic Transaction (SET) follows the following steps for successful electronic transaction:

1. The customer opens Master Card or Visa Card online payment system and fills all required information using his/her credit card.

2. The customer gets a copy of digital certificate generated by trusted certificate distribution authority. This certificate includes a public key and expiry time, which are required for secure online transaction.

3. Trusted third-party also receives certificates from the credit/debit card issuer bank. These digital certificates include the public keys of bank and merchant.

4. The customer confirms the order through web page of merchant's website.

5. The web browser of customer validates the authenticity of merchant and confirms that the merchant is authentic and valid.

6. The web browser of customer transmits the order information to the merchant in encrypted format. This order information includes the public keys of merchant and bank and payment details.

7. The merchant authenticate the customer through verifying the digital signature on customer's certificate. This process may be occurred through bank as well as trusted third party.

8. The merchant transmits the order information to the concern bank. This information includes the bank's public key and customer's online payment information along with merchant's certificate.

9. The bank performs the several verification processes for the merchant and message authentication. Using digital signature on certificates, bank verifies the details of online payment.

10. The bank generates the final approval for requested transaction to the merchant.

In such a way SET undergoes for various processes to perform electronic transaction in secure manner over wireless network.

Multiple encryption is a technique to enhance the data security by performing the encryption process multiple times using same or different types of encryption key (algorithm). Multiple encryption increases the complexity of data encryption in such a manner that intruder or unauthorized user can't decrypt the data, if some encryption keys (algorithms) are known [4].

In cryptography, multiple encryption as found in 3DES and AES provides cryptographic assurance of a message's integrity. The simplest approach to increasing the key size is to encrypt twice, with two independent keys K1 and K2. Letting P be a 64-bit plaintext, C a 64-bit ciphertext, and K a 56-bit key, the basic DES encryption operation can be represented as:

$C = S_K (P)$,

and simple double encryption is obtained as:

$C = S_{K2} [S_{K1} (P)]$

While exhaustive search over all mentioned keys (K1-K2 pairs) requires more operations and is clearly infeasible, this cipher can be broken under a known plaintext attack (where corresponding plaintext and ciphertext are both known) with 2^{56} operations. The time required is therefore no greater than is needed to cryptanalyze a single 56-bit key exhaustively. If P and C represent a known plaintext--ciphertext pair, then the algorithm for accomplishing this double encryption encrypts P under all 2^{56} possible values of K1, decrypts C under all 2^{56} values of K2, and looks for a match. For obvious reasons, this is called a "meet in the middle" attack [5].

Triple DES (Data Encryption Standard) is a common example of multiple encryption, which uses three DES keys as K_1, K_2 and K_3 with the size of 56 bits.

The encryption algorithm can be stated as:

$$\text{Ciphertext} = E_{K3}(D_{K2}(E_{K1}(\text{Plaintext})))$$

I.e., DES encrypts with key K_1, DES *decrypts* with key K_2, and then DES encrypts with keyK_3.

Decryption is the reverse process as:

$$\text{Plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{Ciphertext})))$$

I.e., decrypt with key K_3, *encrypt* with key K_2, and then decrypt with key K_1.

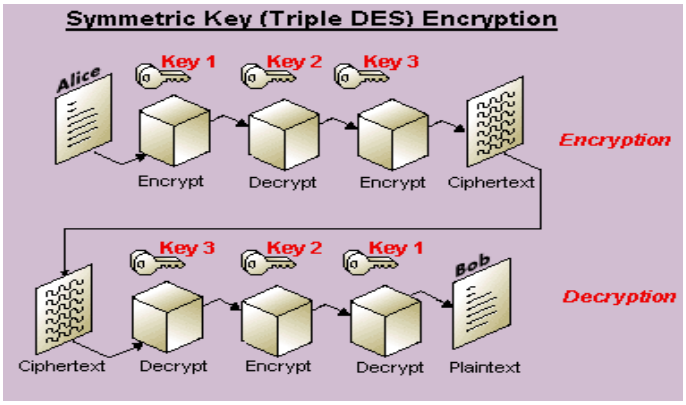

Fig. 2: Description of Multiple Encryption (Triple DES)

In Fig 2, the complete process of Triple DES is described. Each triple encryption process is taken place on the plaintext having size of 64 bits of data. In this technique, the middle operation is the reverse of the first and last operations. This improves the strength of the algorithm when using a set of different keys instead of symmetric keys or same keys.

2. BACKGROUND AND DEVELOPMENT

Secure Electronic Transaction (SET) was developed by VISA and MasterCard with the help of other companies like as Microsoft, GTE, IBM, Netscape, VeriSign and RSA in 1996. Secure Electronic Transaction (SET) was based on X.509 certificates, which is a digital certificate used for authentication purpose. The first version of Secure Electronic Transaction was launched in May, 1997.

In Secure Electronic Transaction (SET), various encryption algorithms are used such as DES (Data Encryption Standard) and RSA algorithm. Data Encryption Standard (DES) is a 56-bit key algorithm, which is used to encrypt online transactions. This encryption technique was not much secure and can be easily cracked using modern software embedded hardware. In 1993, using a concept of brute force attack, a DES cracking machine was designed by a scientist Michael Wiener. In 1996, a great scientist Schneier proposed that a parallel machine can be designed that cracks DES system within a second. So, for the secure transaction the DES was replaced by powerful and reliable system as Secure Electronic Transaction (SET).

Secure Electronic Transaction (SET) permitted communicating parties to identify and authenticate each other in hidden manner and exchange sensitive information securely. The

main advantage of SET is that all communication will be taken place in hidden manner. In SET, the merchant cannot access the customer sensitive credit card information. Such strong protection is provided for the benefits of customers as well as credit/debit card companies to avoid any type of financial frauds.

3. ROLE OF ENCRYPTION IN SECURE ELECTRONIC TRANSACTION

The popularity of online shopping is increasing day by day, in which customer provides the credit card information to make payment for requested product. Secure Socket Layer (SSL) and Transport Layer Security (TLS) keeps record of credit card details safe from intruder and unauthorized users. SET handles such type of situations by requiring merchants and credit/debit card holders to register themselves before any online transaction. A trusted certificate authority makes an important role to register cardholders and merchants and after final approval certificate authority issues the security details and a unique signature key for online transactions. These details and digital signature will be used for the authentication purpose. All order information and confirmations carry digital signatures, which provide non-repudiation and authentication services to avoid any fraud and can be used to resolve any dispute [6].

A Secure Electronic Transaction (SET) involves three parties: the credit/debit cardholder, the merchant, and a bank as a payment gateway. The credit/debit cardholder shares the order information with the merchant though merchant website but not with the bank (a payment gateway). But credit/debit cardholder shares the payment information with the payment gateway (bank) but not with the merchant. A set of dual digital signature establishes this partial sharing of information and allowing all communicating parties to confirm that they are performing the same transaction. In this process, each communicating party receives the hash format of the required information. The cardholder signs the hashes of payment and order information. Each communicating party can verify and confirm that the hash in their possession matches with the hash signed by the cardholder. The cardholder and merchant compute equivalent hashes for the bank to compare. All communications between communicating parties are highly protected. Merchants cannot access the credit card information of customer. In SET, intruder or criminal is not able to make any transaction because it requires cardholder signature and a secret number received by trusted third party after registration. A merchant can be authorized to receive credit card numbers and has the option of accepting payments given a credit card number alone.

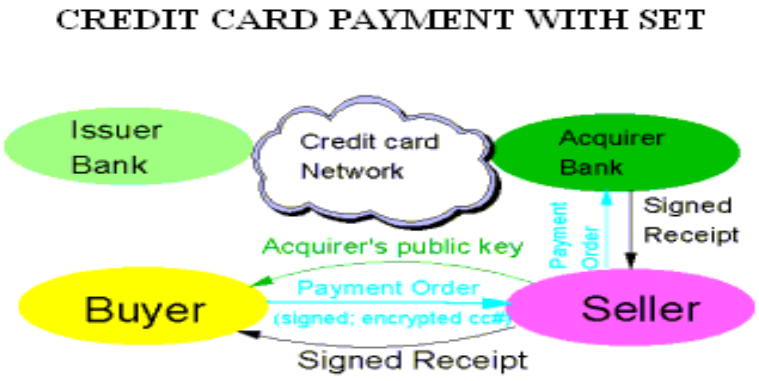

Fig 3: Secure Electronic Transaction using Credit Cart

In Fig 3, whole process of Secure Electronic Transaction (SET) is shown. In this, SET involves three communicating parties as buyer, seller and the bank as a payment gateway. The online transaction is taking place over wireless network as Internet in secure manner.

Authentication is an important issue for online users who perform online transactions over unreliable and insecure wireless network. All communicating parties must have faith in the authenticity of each other through trusted third party. In absence of authentication, any intruder or unauthorized user could pose as a merchant and tarnish the merchant's reputation by failing to deliver products and billing up the credit card bills in illegal manner. So, authentication is a critical factor to achieving trust in electronic commerce [7].

According to the Data Security for electronic transaction [8], the general steps for the SET are:

- **Customer to Merchant**
  1) Customer sends both the order and payment details to the merchant, together with his certificate.
  2) The payment details will be encrypted; merchant will not be able to read the payment details.
  3) The merchant uses the customer certificate to verify the customer.
- **Merchant to Customer's Bank**
  1. Merchant will send this payment details to his bank who will then forward it to the customer's bank to request authorization that the customer has sufficient available credit for the purchase.
- **Confirmation of Order**
  1. Once the authorization is received, the merchant will send an order confirmation to the customer.
- **Shipping of Goods**
  1. Upon confirmation by the customer, the merchant will deliver the goods to the customer
- **Request for Payment By Merchant**
  1. Lastly, the bank makes a request to the customer's credit card bank for payment.

4. OVERVIEW OF THE PROPOSED ENCRYPTION TECHNIQUE

This idea differs with existing data encryption technique used in Secure Electronic Transaction standards to provide better information security over the wireless network as internet. It may enhance the data security enormously due to use of data encryption multiple times with different advance encryption keys. It increases the complexity in encryption as well as decryption process in such a manner that a long time is required to analyze the correct keys to decrypt the encrypted data.

In cryptography, as much as we encrypt the data multiple times we will get the strong and secure encryption algorithm. So, using three encryptions in triple DES, we can achieve greater level of security in comparison of single or double encryption. The use of double encryption

does not provide the adequate security and cannot be recommended as a secure encryption technique. In triple DES, triple encryption can provide substantial improvements in data security.

A. Conventional Encryption Technique in SET

1. Take original confidential information as plaintext.
2. Employ Simple Hash Algorithm, result comes out as Message Digest.
3. Encrypt Message Digest with private key to generate Digital Signature.
4. Transmit the data with Digital Signature to the receiver side.

B. Multiple Encryption Technique in SET

1. Take original confidential information as plaintext.
2. Employ Simple Hash Algorithm, result comes out as Message Digest.
3. Encrypt Message Digest multiple times with different encryption keys to generate more advance and complex Digital Signature.
4. Transmit the data with newly generated Digital Signature to the receiver side.

So, using multiple encryption we can get more secured and advanced digital signature, which is very complicated to crack by any intruder or unauthorized party.

5. CONCLUSION

Multiple encryption is an ambivalent encryption technique for Secure Electronic Transaction and it will play an important and revolutionary role in secure electronic transaction over wireless network. Multiple encryption in Secure Electronic Transaction describes the enhanced security as well as integrity of confidential data due to multiple encryption operations. The main advantage of multiple encryption is that it provides better security because even if some secret or encryption keys are cracked or some part of cipher texts are broken, the confidentiality and privacy of original data can still be maintained by multiple encryption. Secure electronic transactions with multiple encryption will be an important part of electronic commerce in the future. Such level of security is required to earn the interest and trust of customers, merchants and financial organizations for online transaction over wireless network. The ideal of the secure electronic transactions protocol (SET) with multiple encryption is important for the success of electronic commerce.

REFERENCES

1. Wikipedia: The free Encyclopedia, Technical Weblink: http://en.wikipedia.org/wiki/Secure_Electronic_ Transaction#History_and_development
2. IBM Corporation. An overview of the IBM Secure Electronic Transaction and the IBM Commerce Point Product, June 1998, Weblink: http://www.software.ibm.com/commerce/set/overview.html

3. MBA Knowledge Base, Management Article Weblink:http://www.mbaknol.com/business-finance/secure-electronic-transaction-set/
4. Wikipedia: The free Encyclopedia, Technical Weblink: http://en.wikipedia.org/wiki/Multiple_encryption
5. Ralph C. Merkle, Martin E. Hellman, On the Security of Multiple Encryption, A technical note on Programming Technique & Data Structure in Stanford University, Department of Electrical Engineering, Stanford, CA published in ACM, 1981, Volume 24, Number 7.
6. Schneier, Bruce. Applied Cryptography, John Wiley & Sons, Canada 1996
7. IBM Corporation. Cryptography and SET, June 1998, Weblink: http://www.software.ibm.com/commerce /payment/part2.html
8. Data Security for e-Transaction. Retrieved on April 12th 2008, from Weblink: http://www.comp.nus.edu.sg/~jervis /cs3235/set.html

AUTHOR 1:

Himanshu Gupta is a Senior Faculty Member in Amity Institute of Information Technology, Amity University, Noida, India.

Himanshu Gupta is having specialization in Network Security & Cryptography. He is having prestigious membership in various famous and reputed Technical and Research organizations such as CSTA (USA), Computer Society of India (India), TIFR (India), IACSIT (Singapore), UNESCO (Paris) and IEEE Computer Society (USA). He has successfully filed a patent "A Technique & Device for Multiphase Encryption" under the domain area of Network Security & Cryptography in the field of Information Technology. He has attended many National and International Seminars, Workshops & Conferences and has been presented many research papers in the field of Information Technology. He has visited many countries as Malaysia, Singapore and Bangkok for the academic and research purpose. He has been delivered many technical sessions in the field of "Network Security & Cryptography" in various reputed universities and research organizations as an invited speaker.

AUTHOR 2:

Dr. Vinod Kumar is associated with teaching and research activities since last 30 years. He is presently working as Professor, Department of Computer Science and Dean, Faculty of Technology, Gurukul Kangri University, Haridwar since last 13 years .

Dr. Vinod Kumar has been Founder Head of the Computer Science Department, Founder Dean, Faculty of Technology and Founder Directorl, College of Engineering and Technology, at GKU Haridwar. Fifteen researchers have already got the degree of Ph.D awarded under his guidance and Eight are pursuing research for their Ph.D. He has published about 75 research papers in various national/ international journal/conferences of repute. He is a member of IEEE, USA and Association of Computing Machinery (ACM), USA. Also, He is a Senior Life Member of Computer Society of India, Life Member System Society of India, Life Member, International Goodwill Society and Life Member of Ramanujan Mathematical Society. He has been Chairman of Haridwar Chapter of Computer Society of India.