ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

Security Enhancement in Secure Electronic Transaction Protocol (SETP)

Satyanshu Srivastava, Rakesh Bharti
Department of Computer Science & Engineering
United Institute Of Technology, Allahabad 211006 India

Abstract: ***Secure Electronic Transaction protocol is a very comprehensive protocol used for the secure electronic transaction in ecommerce to provide authentication and confidentiality to the transaction. It contains some shortcomings such as the use of 56 - bit keys Data Encryption Standard (DES), and is slow in process. The best attack against it is key exhaustion so due to the advancements in the computer technology it is possible. It was not much secure and not fast. In this paper we propose a new concept to improve the security and the speed of the protocol. We use AES-128[1] which replaces DES-56 bit keys. In AES-128 the key exhaustion is not easy this enhances the security and the speed of the Secure Electronic Transaction Protocol. We also provide the comparison study of the previous and the proposed technique.***

I. INTRODUCTION

Internet is widely used for many purposes such as entertainment, communication; e-business etc. e-commerce is an important part of e-business commonly known as electronic commerce or e-com. It refers to a wide range of online business activities for products and services. Any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact consists of the buying and selling of products or services over electronic systems such as Internet and other computer networks comes under the category of e-commerce. [14][15]Online transactions are an important part of e-commerce. When we sell or buy a product we have to pay for it. Online payments are performed with the help of online transactions. For the successful and secure online transaction there is a protocol Secure Electronic Transaction protocol. That protocol is concerned with the security as well as other aspects of the online transactions. Secure Electronic Transaction (SET)[16] is a very comprehensive security protocol which uses cryptography to provide security services to the transaction.[10][11] The customer place order to the merchant through the website. For this he/she will send the list of items to be purchased, to the merchant. Then the merchant returns an order from to the customer. This order form contains the Order No., list of items, individual price of items, quantity of the items, total price etc. a copy of merchant's certificate is also send by the merchant that the customer can verify that the particular merchant is legal person for the transaction or not. If the order form is according to the customer requirement then customer sends the purchase request message. [13] That message includes the payment related information, information of the items to be purchased and certificates of the customer to the merchant. The merchant can verify the customer through the customer's certificate. The payment information contains the information such as credit card details (Card No., expiration date etc). This information is confidential and should not be viewed by the merchant for this purpose it is encrypted in such manner that merchant is unable to decrypt it.

II. EXISTING SECURE ELECTRONIC TRANSACTION PROTOCOL

In this the order information (OI) and Payment Information(PI) is hashed using SHA-1 and their combined message digest which is payment information message digest(PIMD) and order information message digest(OIMD) is again hashed with SHA-1.[17] The new payment order message digest (POMD) is encrypted with the private key of the customer. The result is Dual Signature. [Fig:1] That dual signature, order information customer's certificate which contains the public key of the customer and PIMD is again encrypted with DES-56 keys (Symmetric Key Encryption). The 56 bit key (DES) is sent to the other side with the

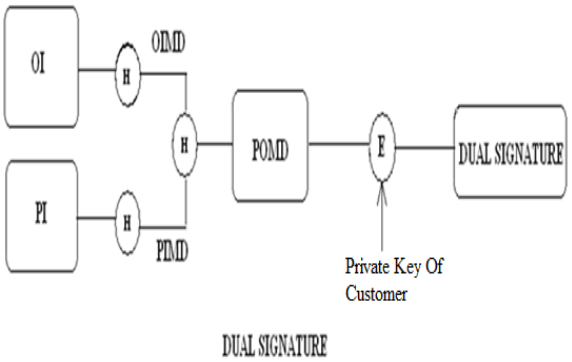

Fig: 1 Dual Signature

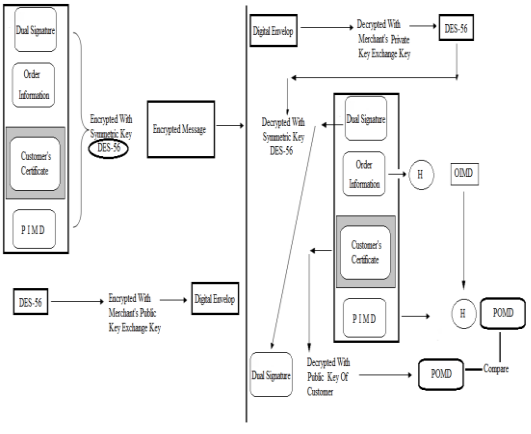

Fig: 2 SET Encryption and Decryption

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

Help of merchant's public key exchange key. At the receiving side the reverse processes are applied for the result. It provides confidentiality and the authentication.

III. SECURITY ENHANCEMENT IN SET PROTOCOL

In the existing SET protocol there is a use of symmetric key[7] cryptography (DES-56) to encrypt dual signature, Order information, payment information message[8][9] digest and customer's Public key certificate[Fig:2]. Since DES-56 is not secure due to 56 bit key size. So we enhance the security of SET protocol by replacing the 56-bit key with AES-128 which contains 128 bit key size[2] Due to this enhancement the SET protocol will became more secure and the speed of encryption and decryption is also increased in comparison to existing protocol.

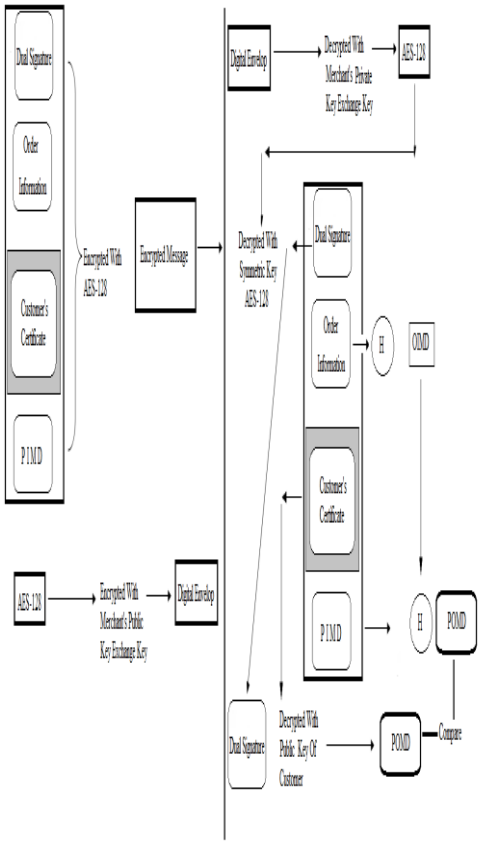

Fig: 3 Enhanced SET Encryption and Decryption

IV. COMPARATIVE ANALYSIS OF EXISTING AND ENHANCED SET

A strong symmetric key encryption algorithm such as the [5] AES has one basic security goal that is best defense against the cryptanalytic attack it should be key exhaustion. [Fig:3] The key exhaustion is the best attack, and then key size determines the symmetric key algorithm's strength. To find an n-bit key, it is, [3]on average, necessary to try 2^n–1 keys, but if we make *n* sufficiently large, this becomes wildly impractical. We know breaking 56-bit DES by key exhaustion is practical. Since [4][6] AES uses 128, 192, or 256-bit keys so key exhaustion is impractical.

Security Analysis

S. No	Key Size (Bits)	No. Of Alternative Keys	Time required at 1decryption/µs	Time Required at 10^6 decryption/µs
1	32	2^{32}=4.3x10^9	2^{31}µs= 35.8 min	2.15 millisecond
2	56	2^{56}= 7.2x10^{16}	2^{55}µs= 1142 year	10.01 hours
3	128	2128=3.4x10^{38}	2^{127}µs=5.4x10^{24} Years	5.4x10^{18} years
4	**168**	**2^{168}=3.7x10^{50}**	**2^{167}µs= 5.9x10^{36} Years**	**5.9x10^{30} years**

Security Analysis
Speed Analysis

Size of File	DES-56	AES-128
5 KB	1343.75 ms	828.125 ms
10 KB	2625.0 ms	1890.625 ms
15 KB	3781.0 ms	3125.0 ms
20 KB	4171.875 ms	3671.875 ms

Encryption Time in MS

Size Of File	DES-56	AES-128
5 KB	140.625 ms	123.625 ms
10 KB	343.75 ms	375.0 ms
15 KB	828.125 ms	453.125 ms
20 KB	1109.375 ms	1078.125 ms

Decryption Time in MS

Time is in milliseconds.[5] Based on above observations we can say that after the enhancement in SET protocol it will become more secure and fast.

V. CONCLUSION

Secure electronic transaction protocol is used for the electronic transaction. We propose a technique which replaces the DES-56 bit with AES-128 bit key. Based on the above observations we can say that it enhances the security of the protocol. After using this technique the confidentiality and authentication rises to the greater extent.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 6, December 2012

REFERENCES

[1] FIPS, "Specification for AES" Nov-2001.

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

[3] "Speed comparison of Popular Crypto Algorithm" Crypto++ Benchmark5.6.0 2005.

[4] Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael" June 1998.

[5] "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP. 84- 89.

[6] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."Dr. Dobb's Journal, March 2001, PP. 137-139.

[7] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP.

[8] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, Feb. 1978, pp. 120-126.

[9] Federal Information Processing Standard 180-2, Secure Hash Standard, Nat'l Inst. Standards and Technology, 2001.

[10] RFC 3174 Secure Hash Algorithm-1.

[11] SET Secure Electronic Transaction Specification: Business Description. MasterCard and VISA. [Online]. Available: http://www.setco.org/set_specifications.htm.

[12] SET Secure Electronic Transaction Specification: Programmer's Guide. MasterCard & VISA. [Online]. Available: Http://www.setco.org/set_specifications.htm

[13] MasterCard & VISA. SET Secure Electronic Transaction Specification: Formal Protocol Definition, May 1997. Available Electronically at http://www.setco.org/set\ specifications.html.

[14] R. Hunt. "PKI and Digital Certification Infrastructure", Ninth IEEE International Conference on Networks (ICON'01), October, 2001.

[15] Lawrence C. Paulson Computer Laboratory, University of Cambridge "Verifying the SET Protocol: Overview".

[16] Douglas H. Steves , Chris Edmondson -Yurkanan ', Mohamed Gouda "Properties of secure transaction protocols", The University of Texas at Austin. Austin. TX 78712. USA.

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

Author Profile

Satyanshu Srivastava is M.Tech in Computer Applications from Indian School of Mines Dhanbad. His research interest is in Vehicular Ad-hoc Networks (VANET), Cryptography and Network Security, Routing Algorithms. He is an active member of Computer Science Society of India. He is currently working as an Assistant Professor in the Department of Computer Science and Engineering in United Group of Institutions, Allahabad, India

Rakesh Bharti is M.Tech (Gold Medalist) in Computer Science from Uttarakhand Technical University. He has eight years of teaching experience in various reputed engineering colleges. He has published many papers in various national and international journals and conferences. His research interest is in Distributed Computing, Digital Image Processing. He is currently working as an Assistant Professor in the Department of Computer Science and Engineering in United Group of Institutions, Allahabad, India