International Journal of Information Technology and Knowledge Management
January-June 2012, Volume 5, No. 1, pp. 227-229

AN NESTED ENCRYPTION SCHEME FOR SECURE ELECTRONIC TRANSACTION

DINESH KUMAR[1] and KAVITA DUA [2]

ABSTRACT:- Research e-commerce security protocols, describes the development of e-business status, analysis of e-commerce security threats and security requirements, given the status of e-commerce security protocol to study the security of e-commerce in the Secure Sockets Layer protocol used mainly SSL protocols and secure electronic transaction protocol.

Key-Words- Ciphertext; Encryption; Security Protocols; Transaction

1. INTRODUCTION

SET Secure Electronic Transaction protocol is currently the focus of attention into, people tried to study all aspects of SET protocol, in order to change its safety, adaptability, speed, complexity, and so there's enough. China's network information security research started late, less investment, research scattered strength, and the gap between technologically advanced countries, especially in terms of system safety and security protocols work with foreign gap even greater. However, the network information security of our country, after all, has a certain basis and conditions, especially in cryptography research, the accumulation of more and better foundation. Has mastered the part of network security and e-commerce security technology, some domestic research and development departments have also been a security gateway, electronic trading systems to commercial security, CA certification bodies and part of the core cryptographic algorithm and a number of security products and so on. In this paper, e-commerce security protocol for the study, mainly the security of e-commerce transactions on the SET protocol analysis and research, spending the existing deficiencies and shortcomings, and the concrete solutions are the nested encryption scheme and the SET classification model for security control. Nested encryption scheme to some extent, the SET protocol encryption algorithm to solve the control of others (United States), not enough security, encryption and decryption are not flexible, adaptive poor enough. SET extension model of security control can solve the SET protocol, regardless of the situation brought out slowly across the board, the operating complex and difficult to promote the shortcomings.

2. E-COMMERCE SECURITY RESEARCH

With the rapid development of Internet, e-commerce as a new business model worldwide is moving forward at an alarming rate The Internet's own network and open, a lot of important information on the Internet needs to be passed, the process of transmission of information necessary requirement for adequate security, the need to enhance consumer confidence in the reliability of transactions, and enhance the network of illegal alien invasion protective measures. Therefore, security is seen as the key to the healthy development of e-commerce, and the urgent need to overcome the problem by the attention. E-commerce security as a whole can be divided into two parts: computer network security and business transactions. Computer network security, including: computer network equipment security, computer network security, database security. Characterized by its own computer network for possible security problems, the implementation of network security enhancements to ensure the security of computer networks as the goal itself. Security is tight around the business transactions on the Internet on traditional business applications for a variety of security problems in computer network security based on the protection of e-business process goes smoothly.

2.1 The Problem of E-Commerce Security

(1) Basic technology is relatively weak. Foreign e-commerce security technology, its structure or encryption algorithms so good, but due to restrictions on their password policy, open the algorithm for them can hardly be kept secret, the potential security risks greatly.

(2) Architecture is incomplete. Most e-commerce security person in charge before, “fire brigade” role, stop-foot lame the disease. This "temporary solution" approach, the problem is always endless. In recent years, people have begun to solve the problem from the architecture, it should be said that significant progress had been made in theory, but in practical application there is need to work harder.

(3) E-commerce information storage security risks. Information security is stored in the static storage of information in e-commerce security. Its information security risks include: information and unauthorized alteration of information is called content. Corporate Intranet and Internet connection, the e-commerce information storage security is facing both internal and external problems: internal problems, mainly business users

[1] Research Scholar Ph.D (Computer Science) NIMS University, Jaipur, Rajasthan, INDIA

[2]Associate Professor, Kurukshetra University, Kurukshetra Haryana,

unauthorized intentional or unintentional or unauthorized e-commerce information call free to add, delete , modify the e-commerce information; external risks, mainly outsiders without permission into enterprise Internet, e-commerce information on the intentional or unintentional unauthorized calls or to add, delete, modify.

2.2 E-Commerce Security Issues and Reason

The current security problems facing e-commerce include the following:

(1) Steal information: Even if the data is encrypted, but if the encryption strength is not enough, an attacker can also get information on the contents of code-breaking, resulting in information disclosure.

(2) Tampering with the information: Attacker to control the format and rules of information after all means of interception of information tampering, destruction of the authenticity and integrity of business information.

(3) Counterfeit identity: Attacker to use illegal means to the legitimate user identity information by using fake identity and other transactions, to obtain illegal benefits, thus undermining the reliability of transactions.

(4) Denial: Some users of the information sent or received malicious denial, in order to evade responsibilities.

(5) Virus: Network, in particular the development of Internet has greatly accelerated the spread of the virus, while more and more destructive virus, a serious threat to e-business.

(6) Malicious damage: Since an attacker can access the network, may distort the information network, control confidential information online, or even sneak into the internal network, the consequences are very serious.

3. Set E-Commerce Security Protocol

SET protocol (Secure Electronic Transaction) is called Secure Electronic Transaction protocol, Master Card and Visa by the United Netscape, Microsoft and other companies, in June 1, 1997 launch of a new electronic payment models. SET protocol is applied to credit card on the Internet-based electronic payment system agreement. It uses public key cryptography and X.509 digital certificate standard, mainly used in B2C mode of security protection of payment information. SET protocol itself is more complex, more stringent design, high security, it can ensure the confidentiality of information transmission, authenticity, integrity and non-repudiation. SET protocol is a digital signature to ensure the message integrity and message origin authentication, digital signature and message encryption using the same encryption principles. The digital signature generated by RSA encryption algorithm with message digest, message digest is the message get through the HASH function only after the message corresponds to the value, the message for each data bit will cause a change in the information summary about half of the data bits change. The two different messages with the same message digest of the possibility of its small, it makes one-way HASH function derived from the message digest calculation of a summary of the information is not feasible.

3.1 SET Protocol Analysis and Research

SET protocol designed to compare the tight, high security, is unmatched by other security agreement, but so far has not been widely used. The reasons are: require the installation of the package too costly to support SET system. SET requirements in the banking network, business servers, the customer PC, install the appropriate software; also, SET also requires certificates to be issued to the parties, which makes the payment system using SET protocol security protocol than with other systems much more expensive. SET protocol is too complex, processing speed, complete the transaction process. SET protocol restrictions on encryption technology, making it less flexibility and adaptability. And so on. Therefore, the study SET protocol, refine and improve the SET protocol, for solving the e-commerce security issues and promote further development of important academic and practical significance.

3.2 SET Protocol Flaw

In the international security guarantees as a card payment protocol SET, is both a common and mature security protocol, but there are still deficiencies in the application:

Realizing the complexity, the cost is too high, poor interoperability.

Cardholders pay later, some businesses will not guarantee delivery of goods in the hands of the cardholder, the transaction status in the inequality.

Cardholder did not receive an order confirmation receipt business; either party may be denied the goods are correct.

The true identity of the cardholder, shopping, all exposed to the privacy of businesses, not to bring the consumer cardholder anonymity.

Facing the possible loss of interest. When the item was damaged during the transfer of goods is not the cardholder or the choice of goods, as well as businesses face the possibility of fraud, the cardholder can not make a valid save.

3.3 Improved Nested Encryption Scheme

SET protocol can only use the DES algorithm and the RSA algorithm for encryption and decryption of information, resulting in SET protocol, including encryption and decryption not working, poor adaptability; but also for each algorithm key length for export control, the other computer speed and computing power continues to improve, both algorithms have the example has been cracked, so, sexy people to worry about the safety of SET; all countries wishing to

use their own intellectual property rights developed encryption algorithms, do not want security on the controlled person. This is the SET protocol can not be one of the main widely used. Nested encryption scheme is proposed and the application of e-commerce security to meet the current needs of cryptography. It is consistent with SET protocol standard system, using a variety of rigorous theoretical proof, the practice shows that the maturity is safe and effective algorithm (which can be self-developed), but not limited to a specific algorithm, according to a kinds of combinations for encryption and decryption processing of encryption and decryption programs. Nested encryption scheme can solve the above problem exists SET protocol, can improve the SET's encryption strength, flexibility and adaptability.

The principle of nested encryption scheme is based on need, first select a kind of proprietary encryption algorithm to encrypt information, then information exchange encrypted SET default encryption algorithm used to encrypt again, and then send the final result to the receiver; receiver after receiving the first SET the default encryption algorithm used to decrypt, and then use a proprietary encryption algorithm to decrypt and obtain the original information.

Nested encryption algorithm workflow is as follows:

The sender of the first encryption method used to send the message to encrypt plaintext to get cipher text.

The sender for the recipient's digital certificate for authentication.

The sender will I be Hash cipher text operations, generate a message digest.

Private Key of the sender encrypts the message digest to get a digital signature.

The sender with a randomly generated symmetric key encryption of ciphertext I get cipher text II.

The sender with a digital certificate from the receiver to get the receiver's public key to the symmetric key encryption, digital envelope generation.

Sending the ciphertext II, digital signatures, digital envelopes and with the sender's digital certificate to send to the receiver.

The receiver receives the message, the sender first digital certificate for authentication.

The receiving party with their own private key to decrypt the digital envelope, get the symmetric key.

With a symmetric key of the receiver II to decrypt the ciphertext, the ciphertext.

Receiver on the Hash operation I ciphertext to generate a new message digest.

Receiver with a digital certificate from the sender to get the sender's public key to decrypt the digital signature to get the message digests.

Receiver compares the two messages digests to determine the integrity of the message.

4. CONCLUSION

According to the development of e-business status, analysis of e-commerce security threats and security needs of e-commerce security protocols are given the status of domestic and foreign research on several of the more common security protocols were introduced, and mainly for the SET protocol analysis and research, that its deficiencies and to improve and perfect the proposed encryption scheme and the nested model of security control of two extension programs, new programs and original programs will be compared and evaluated.

REFERENCES

[1] Li C, Wang Y, Yang D. A Trust Evaluation Model For Future Peer-To-Peer E-Commerce Environments [A]. Proceedings Of The Workshops On Globecom [C]. Honolulu, Hi, 2009.1-6.

[2] Dong P, Wang H, Zhang H. Probability-Based Trust Management Model For Distributed Commerce [A]. Proceedings Of The Ieee International Conference On Network Infrastructure And Digital Content [C].Beijing, China, 2009. 419-423.

[3] Hu B, Wang R C, Wang H Y. A Modified Security Solution based on SPA for servants' reputations in P2P systems [J]. Acta Electronica Sinica, 2007, 35(2): 244-247.

[4] SIMON M. K. Evaluation of average bit error probability for space-time coding based on a simpler exact evaluation of pair wise error probability [J]. Int Journal Communication and Networks, 2001,(3):257 -64.

[5] Wenling, Wu. Dengguo, Feng. : Collision attack on reduced-round Camellia. Sci China Ser F-Inf Sci, 48(1): 78—90.(2005)

[6] Biham, E.□Dunkclman, O.Keller, N.: Related-Key Boomerang And Rectangle Attacks✓In□Advances In Cryptology✓Proc of the EUROCRY□ LNCS, 3494, 507—525 (2005)

[7] Fergueon, N., Keisey, J. Lucks, S.:Schneiez B improved cryptaaalysh of Rijndael-In Proctol.