THE REQUIREMENT FOR SECURITY IN E-COMMERCE

Shahin Samimi*

Fariba Rastegar*

Abstract: *Organizations and companies with given the important and value of their information needs are designing a robust Information Security Management System needs are designing a robust Information Security Management System that Along with environmental changes may need to update your system. Because of advances in technology, enabling organizations to easily access the information and data provided. Firstly, we will introduce the concepts of electronic security and safety protocols and usage of these protocols.*

Keywords: *Electronic commerce, information security, encryption, safety protocols.*

*Department of Computer Engineering, Behbahan Branch, Islamic Azad University, Behbahan, Iran

1. INTRODUCTION

Lack of firsthand information on real cases has made planning and overcoming security threats much more difficult. Now there are some correspondents got specialty in the field of cyber security, and have many solutions to protect electronic business technologies against potential criminals within cyberspace. Many companies have found that to succeed in electronic business, in addition to security approaches designed to protect sources of information technology, some investments and planning are required to create a comprehensive security program

2. DIFFERENT ASPECTS OF INFORMATION SECURITY

Today, information security is not considered a new subject. But according to technology development and evolution of data transferring system, methods of protection have got basic and fundamental changes. Generally, security within electronic business may be regarded as a simple relation between data and information protection against internal and external misuses during any stage of electronic business (including register, send, receive, etc.).

Considering these issues within electronic business in general and within electronic funds transfer in particular, has a special situation in designing and developing systems. Such systems should be responsive to security issues which will be explained below.

2.1. Accessibility

A safe and secure system should provide access and availability of data in an appropriate time and place coupled with a protection against any unauthorized access to data. But any system can face the following risks:

The risks include network error, power failure, operational mistakes, application mistakes, hardware error, software system error, and viruses.

The approaches to overcome the risks consist in selecting a preferred communication path, preventing power failure, quality test for software and hardware, limiting access, and providing data support system [1].

2.2. Confidentiality

Confidentiality consists in protecting messages against misuse, tracking, and eavesdropping. Confidentiality can encounter some risks such as unauthorized access by intraorganizational people, and hirelings or by tracking during transmission. Cryptography of messages is usually used to overcome these risks.

2.3. Message Integrity

What it meant by integrity is to prevent any manipulation or unwanted deletion of message. In addition, it includes sequence integrity in order to preventing repetition, and loss of message. Message integrity confronts the risk for incidence of accidental mistakes or those resulting from manipulation within data recording phase, and also output degradation. In order to overcome such risks, the approach to confirm message end to end and message sequence may be used.

2.4. Validity and reliability of message

Another aspect of data systems security is validity and reliability of the message. It consists in providing security for sender and receiver identity, and possibility of affirming transmission and receipt of the message. Validity of message faces the risk of impersonation. Confirming message authentication by a combination of what user knows, what user has, and physical features of user may be used to overcome impersonation [2].

2.5. Inspection and handling capability

It consists in registration of data to be inspected, based on pre-determined conditions for confidentiality, and integrity. Risks and strategies to overcome the risks are the same as mentioned for confidentiality and integrity.

3. ECONOMICALITY FOR DATA SYSTEMS TECHNOLOGIES

As the approaches to overcome the risks threatening security are numerous and various, one of the most important and basic factors having a significant role in providing security for systems, is cost consideration. In other words, a balance should be made between potential risks and cost for overcoming those risks. So, we should not always look for those systems that provide maximum security because such systems occasionally cost a lot and using them is not economically reasonable [3].

4. ENCRYPTION

Encryption includes much of business electronics security. One of the most effective methods to protect network security is encryption of all data that is flowing within the network, and replacing basic words (a simple algorithm form) is the basis for cryptographic algorithm also may be used in digital information. Another common usual method and technique is by using an algorithm equipped with a code key that is actually a series of numbers and consists of encryption rules. Encryption is usually divided to two categories by key management [4].

4.1. Symmetric encryption/Series/Private key

In this method, encryption security depends on a determined and divided code and it is used to encrypt and decrypt at the beginning and the end of the message. The characteristic# feature in this method is that both parties of business exchanges must use the same key for encryption and decryption of electronic data interchange. If the message for electronic data interchange encrypted by the same encryption key, it could not be decrypted by any different key.

4.2. Asymmetric encryption/ Public key (PKI)

This method has been invented to remove symmetric key deficits. A pair of key is used in this method. Each of two keys could encrypt information decryption of which is only possible by another key. A pair of key only assigned to one business partner.

5. PROTOCOLS AND SOFTWARE FOR ENCRYPTION

Various methods of encryption have illustrated above. According to the above mentioned methods, there are numerous software to provide security for electronic exchanges especially within electronic business.

5.1. Data encryption Standard (DES)

This encryption has been suggested by US Department of National Standards. It is an encryption plan by using a symmetric key. DES uses an alpha number sequence as key to encrypt and decrypt a message. DES is used as hardware in most of computer-based data-processing system. It has a 56 bit key, the processor needs a high speed, and a low speed processor could be applicable.

5.2. Encryption technique by a general and private key (RSA)

In order to solve some of the problems of DES, asymmetric technique RSA introduced. In this method, a private key and a corresponding public key are used instead of a private key for encryption and decryption of messages. Although data protection implemented in the best way by this method, but it is not helpful in identity confirmation.

5.3. Pretty Good Privacy (PGP)

This method is a combination of IDEA and RSA. PGP is either considered a standard for encryption and decryption, or it is the name of a software product for electronic mail. PGP may be used for creating digital signatures by encrypting characters added to the end of the message.

5.4. Digital certificate

The way digital certificate functions is that a person or an organization is going to send an encrypted message applies a digital certificate from an organization involved in issuing digital certificate. Then the relevant organization issues an encrypted digital certificate consisting of a public key for applicant, and other information related to him/her. Of course, the reference issuing digital certificate would provide its own public key publicly.

After sending message, receiver will decrypt it by using a public key enclosed to message, and he will consider whether it has been issued by the reference issuing certificate, then he will get the sender's public key and identity information included within the certificate.

5.5. Security Sachets Layer (SSL)

One the most famous methods to provide security for electronic exchanges within the internet is SSL. SSL is a protocol for encryption produced by Netscape, and it is accepted by most of great producers of internet products. SSL is established too sent confidential documents within the internet; it uses a private key to encrypt sent messages.

SSL encrypts all data exchanged between host and customer. According to process of SSL, rate of function will be reduced considerably.

5.6. Sate Electronic Transactions (SET)

SET is a special protocol designed for bank operations, and transactions by credit cards. SET is an open standard for processing credit cards transactions within the internet which has been invented in cooperation of the great companies producing software such as Microsoft, Netscape, and the great companies for credit cards such as visa, and master card. SET observes confidentiality of transactions in a way that seller has access to demanded commodity information, the price, and whether payment is confirmed, but he has not access to customer payment method.

6. CONCLUSION

Unwillingness to providing information about security deficits rises from a common fear that the public awareness of such deficits can cause customers distrust of the company ability in protecting its own assets, therefore, the company will lose its customers and as a result, it will lose its profitability. As customers do not trust to record financial information online, the companies may not get anything by confirming, voluntarily the fact that each become victims for security-related crimes. Because of media excitements regarding Internet and its capabilities, keeping a positive view in public opinion towards electronic business security is a main concern for most of the companies and it is quite necessary to remain in competition.

REFERENCES

[1] Ravi Kalakota, Andrew B. Whinston. “Electronic Commerce: A Manager’s Guide”, Addison-Wesley, ISBN: 0-201-88067-9

[2] Davies, Simon G. 1997. “Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity”. In Technology and Privacy: The New Landscape Edited by P. Agre and M. Rotenberg. 143-165. Cambridge, MA: MIT Press.

[3] Chaum, David. 1985. “Security Without Identification: Transaction Systems To Make Big Brother Obsolete”. Communications of the ACM, 28 : 1030-1044

[4] Steve H. Weingart. “Physical security for the ABYSS system”. In Proceedings of the IEEE Computer Society Conference on Security and Privacy, pages 52–58, 1987.