Proceedings of the Sixth Annual Paper Meet
and International Conference
The Institution of Engineers, Bangladesh
Mechanical Engineering Division
27 -29 January, 2000
Paper No. 33 pages 253 -257

BUILDING TRUSTS ON E-COMMERCE : SECURITY OF DATA TRANSMISSION ISSUES

Md. Saiful Islam
Dept. of Electrical & Electronic Engineering
Bangladesh Institute of Technology, Chittagong
E-mail: eeebite@globalctg.net

ABSTRACT

Internet consists of millions of computer network interconnected that provides the e-commerce environment around the globe. When data moves around the Internet it is subjected to threat like interruption, interception, modification and fabrication. Obviously data transmission security is the most important concern for companies transmitting secret, sensitive information. The most basic protection used by citizen to protect their home and property is a lock. The e-commerce environment encryption is the Internet lock. This paper deals with the security measures of data transmission in the network by encryption technology. I investigated private key the encryption method in details along with its advantages and disadvantages especially in the e-business.

INTRODUCTION

In e-commerce environment there is no or limited face to face contact between the buyer and the seller unlike the traditional physical transaction. The transaction s are impersonal, anonymous and automated. Such dehumanised business environment accompanied by all kinds of technical innovations necessarily brings up opportunities for fraud by individual and corporation alike. The e-commerce world is distributed geographically with myriad of access points, with hundreds and thousands of intranet and Internet network connection is confronted with heavy task to secure the system against theft, fraud and electronic terrorism. For such system to reach its full potential, businesses and consumers must be confident about the privacy and security of proprietary information and transaction from unauthorised access and disclosure. The problem is exemplified in fig.1, which depicts trends in the industry toward more people who have sufficient knowledge to do damage to a computer installation in an organisation.

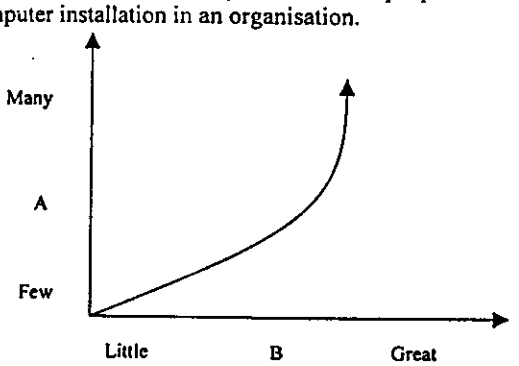

Fig. 1
A: Number of people who can do damage, B: Amount of damage that can be done.

Due to the open and complex nature, the problem of network security is hard. First and foremost, a network is designed to accept request from outside. In a network system there is a flow of information from a source, such as file, to a destination, such as another file or a user. During this process, the data contained in the file may be interrupted, intercepted, modified or fabricated. So, network security measures are needed to protect data during transmission. The most powerful and most common approach to countering the threats is encryption. Encryption is a potent solution to many network security issues. The most obvious use of encryption is to protect network traffic from eavesdroppers. It can be used to protect passwords, sensitive files being transferred over networks etc.

MAJOR TYPES OF SECURITY VIOLATIONS

Security is usually considered as encompassing three primary attributes, confidentiality, integrity and availability, with respect to various information entities such as data, programs, access control parameters, cryptographic keys and computational resources (including processing and memory). Confidentiality implies that information can not be read or otherwise acquired except by those to whom such access is authorised. Integrity implies that information can not be altered except under properly authorised circumstances. Availability implies that resources are available when desired. All three of these attributes must typically be maintained in the presence of malicious users and accidental misuse and ideally also under certain types of system failures.

The types of security violations of the above three attributes are best be characterised by viewing the function of the computer system to be proving information. In general, In general there is a flow of information from source to destination. The normal flow in depicted in fig.2 (a). The remainder of the figure show four general categories of security violations:

Interception: An asset of the system is destroyed or become unavailable . This is a threat to availability. Examples include destruction of a communication line, or the disabling of the file management system

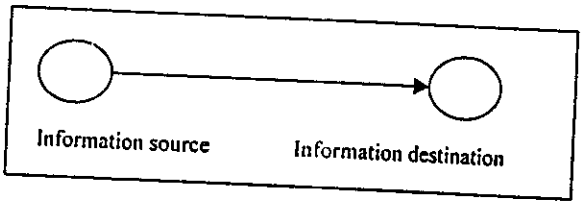

Fig. 2(a)

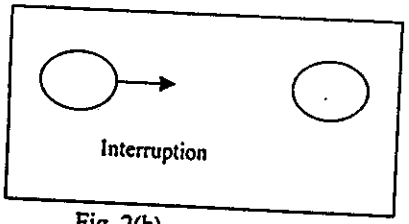

Fig. 2(b)

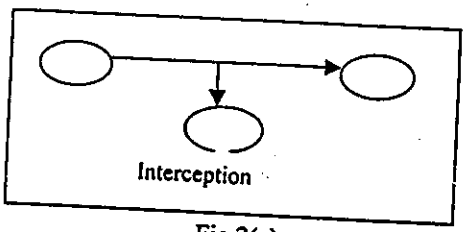

Fig.2(c)

Interception: An unauthorised party gains access to an asset. This is a threat to secrecy. The unauthorised party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network and the illicit copying of files or programs.

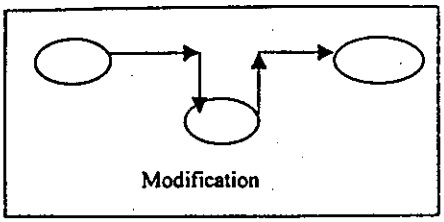

Fig. 2(d)

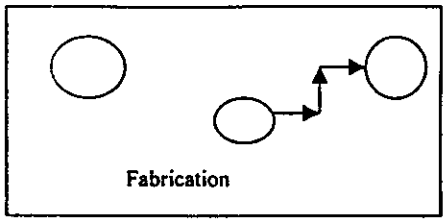

Fig.2(c)

Modification: An unauthorised part not only gains access but tempers with an asset. This is a threat to integrity. Examples include charging values in a data files, altering a programs that it perform differently, and modifying the content of messages being transmitted in aa network.
Fabrication: An unauthorised party inserts counterfeit objects into the system. This is also a threat to integrity. Examples include the insertion of spurious messages in a network or the addition of records to a file.

FUNDAMENTALS OF ENCRYPTION

The most powerful and most common approach countering the threats highlighted in the above discussion is encryption. It is a processes that conceals meaning by changing intelligible message into unintelligible messages and can be achieved by means of either a coder or cipher. A code system uses a predefined table or dictionary to substitute a meaningless word or phrase for each message or part of message . A cipher uses a computable algorithm that can translate any stream of message bits into an unintelligible cryptogram. The reverse of encryption is decryption, in which the cipher-text is reversed to the original intelligible message. The encryption/decryption process is depicted in fig.3. If encryption is to be used to counter these threats, then we need to decide what to encrypt and where the encryption gear should be located.

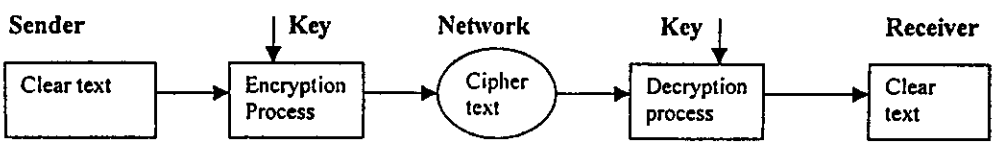

Fig. 3 : Encryption and decryption process

PRIVATE KEY ENCRYPTION

The encryption process consists of an algorithm and a key. Key is a relatively short bit string that controls the algorithm. Once, the cipher-text is produced, it transmitted. Upon reception, the cipher-text can be transformed back to the original plain-text by using a decryption algorithm that was used for encryption. Here, two simple encryption process is discussed.

Substitution ciphers: Substitution is the simpler form of encryption . Substitution ciphers entail the replacement of letter or a group of letter for original letter or letters .In the following example each key is substituted with another letter of full alphabet.

Plain text	:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution letter	:	FGQRASEPTHUIBVJWKLXYZCONMD

Transposition ciphers: It is more sophisticated approach to cryptography , in which keys of the letter are reordered, but not necessarily disguised. The following illustration shows an example of transposition ciphers approach. Suppose SECURITY is the key. This key is used to number columns. Column 1 is used is placed under the key whose letter is closest to the start of the alphabet *i. e.* A, B, C etc. The plain text is then written as series of rows underneath the key. The cipher-text is then read out by columns, starting with the column whose key letter is the lowest in the alphabet. The Phrase **" by low sell high and do it today"** is listed as follows:

S	E	C	U	R	I	T	Y
5	2	1	7	4	3	6	8
B	U	Y	L	O	W	S	E
L	L	H	I	G	H	A	N
D	D	U	I	T	T	O	D
A	Y	A	B	C	D	E	F

The Cipher-text is : YHOAULDYWHTDOGHTCBLDASAOELIIBENDF

The security of private key encryption depends on the encryption algorithm and security of the key. It is assumed that it is impractical to decrypt a message on the basis of the cipher-text plus the encryption/decryption algorithm. So, we don't need to keep the algorithm secret, we need only to keep the key secret.

A principal disadvantage on any type of private key structure is that all sites of the network must have knowledge of the common key. Some administrative and logistic problems arise in the distribution (and confidentiality) of the keys. Until recently, the idea of the private key has been the dominant approach for providing network cryptography. Network sites will change the key periodically; for example, every 24 hours or, if necessary , every few minutes.

THE DATA ENCRYPTION STANDARD (DES)

The most widely used encryption scheme is based on data encryption standard, adopted in 1977 by the national Bureau of Standards (NBS) ,USA. For DES, data are encrypted in 64-bit using a 56-bit key. Using this key, the 64-bit input is transformed in a series of steps into a 64-bit output. The DES has flourished and widely used, especially in financial application as well as in other areas also.

CONCLUSION

As commerce in the web become more common, business also must deal with consumer fears and for this cryptography is a essential tool. There is a legitimate need and uses of cryptography for individual consumers. The widespread use of encryption technology in the e-commerce may bring issues and concern for the governments in respect of protection of privacy of citizen,

maintaining public safety, encouragement of economic well being, enabling enforcement of law and protection of national security, because this could also be used for illegal activities detrimental to public safety. So, government should consider whether any restriction should be imposed to use cryptography and what agency should be responsible to have access to public keys.

REFERENCES

1. Firewalls and Internet Security : Repelling the wily Hacker, Addison-Wesley, Reading, MA-Cheswick, W.R and Bellooin, S. M. 1994
2. Kanfman, C., Perlman, R. and Speciner, Network Security, Princtice-Hall , Engle Wood Cliff, NJ, !994
3. Network intrusion detection, IEEE Network (May/June): 26-41
4. Parker, D.B., Demonstrating the Elements of Information Security with Threats, pp-421-430, In proc. 17th Nat. Comp. Security Conference NIST, Gaitherburg
5. Stubblebine, S.G. and Gligor, V. D. 1992, On Message Integrity in Cryptographic Protocols, pp-85-104, In proc. IEEE Computer Sc. Symp. Res. Security Privacy, Oakland, CA, May
6. Uyless Black, Computer Network Protocols , Standards, and Interfaces,Prentice-Hall, 1995
7. Yu. C. F. and Fligor O.G. 1990, A Specification and Verification method for preventing Denial Service, IEEE trans. Soft. Engg. 16(6): 581-592