International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-2 Issue-6, May 2013

Network Security Design Based on Internet Information System

S. U. Kadam, P. D. Khawale

Abstract— The network information security use is closely related to the field of e-commerce applications. The Network security Evaluation, is a hot issue, in development of computer and network. Without trust, most business operators and clients may decide to decline use of the Internet and revert back to traditional methods of doing business. The encryption technology of e-commerce platform for network security, implementing information encryption and transmission on the network by using DES algorithm. Cryptography is allows secure storage of sensitive data on any computer.

Keywords- network security; encryption; security; e-commerce

I. INTRODUCTION

An important feature of digital business is the area of electronic commerce. The main tool use in businesses to protect their internal network is the firewall. A firewall is a hardware and software system that allows only external users with specific characteristics to access a protected network. While firewalls are indispensable protection for the network at keeping people out, today's focus on e-business applications is more about letting the right people inside your network. Network security can be defined as protection of networks and their services from unauthorized modification, destruction, or discovery, and provision of guarantee that the network performs in critical situations and have no harmful effects for neither user nor for employee. The International Telecommunication Union ITU, the International Information Processing IFIP, World background Organization WCO is all running to develop standards related to electronic commerce. DES was the result of a research project set up by International Business Machines (IBM) corporation in the late 1960's which resulted in a cipher known as LUCIFER. In the early 1970's it was determined to commercialise LUCIFER and a number of important changes were introduced. The encryption technology of e-commerce platform for network security, implementing information encryption and transmission on the network by using DES algorithm. E-commerce security strategies deal with two issues: protecting the integrity of the business network and its internal systems. The field of information Technology(IT) Security as information technologies is represent merely component of information systems. A setting of a security can be defined as an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system property as well as the system as a whole against any intentional or unplanned threat.

Manuscript published on 30 May 2013.
***Correspondence Author(s)
S. U. Kadam , Computer Science and Engineering. , PVPIT College, Pune, India.
P. D. Khawale, PVPIT College, Pune, India.

II. NETWORK SECURITY

Security plays very important role on E-commerce. Most security initiatives are defensive strategies — aimed at protecting of the network E-commerce is a collection of multi-technology, including the exchange of data (such as electronic data interchange, e-mail), access to data (shared databases, electronic bulletin boards), and automatic data capture (bar codes), etc.. In e-commerce the situation is there are five interrelated and interacting components (people, software, hardware, procedures and data), one comes to the conclusion that e-commerce systems are (and should be looked upon as) information systems, comprising a technological communications and an organisational framework, rather than pure technological infrastructure. Security harms of TCP/IP TCP/IP, which is the main protocol used by Internet, has good behavior of interconnection, the independent technology of net, it support to many other protocols of application, and so on.

Result based on the risk analysis, security policy is created. It consists of two parts:

1) General security policy: The description of its processes and Organization, security policy Objectives, security infrastructure, identification of Assets, confidential data and general threats, Description of present status and description of Security measures, contingency plans.

2) System security policy: It defines implementation of security policy in a specific system of a company. With security mechanisms based on security policy being in place, it is important to monitor their actual functionality.

Internet security method

1) Physical Internet security

2) Encryption techniques :

The information on the net, which is transporting or storing, could be encrypted in order to prevent the steeling behaviors from the third party. Encryption is the most common method of ensuring confidentiality.

3) Virtual private network (VPN) technology:

VPN technology using variable public network as a transmission medium of information, through the additional security tunnels, user authentication and access control technology similar to a private network security.

4) Data encryption technology

The so-called data encryption is to re-encode the information in order to hide the information content, so that unauthorized users cannot obtain the information content, it is an important security way in e-commerce.

5) Firewall techniques :

Firewall technology is a secure access control technology. The basic types mainly are application gate, circuit-level gate firewall based on the packet filtering, and firewall based on the all-state checking. Firewall technology used in an insecure public network security environment to accomplish local network security. Firewalls should a small part of the business security infrastructure

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

5) strengthen the preventing and treatment of viruses: Viruses are the most showing threat to client systems. Setting the client-level protecting, web access, e-mail serve level protection, and file application serve level protection. Setting all the system files and executive file read-only is useful to protect important files. Restraining using floppy disk with uncertain resource, as well as the piratical software, is significant for cutting the spread path of the viruses. The e-mails should be kept unread, the same to the accessories. The multiple privilege access schemes present in Unix, VMS and other multi-user operating systems prevents a "virus" from damaging the entire system. It will only damage a specific user's files. A part of concern should also be put into the insecurity the system itself, which needs updating from the realty-explorer regularly. If the system had be found to be contagious unluckily during the checking, corresponding methods should be carried out to clear the viruses away from the net.

III. ENCRYPTION CRYPTOGRAPHY

Encryption is the most common method of ensuring confidentiality. Cryptography from the Greek for "secret writing" is the mathematical "scrambling" of data so that only someone with the necessary key can "unscramble" it. Cryptography alter the structure of the secret message. Cryptography is allows secure transmission of private information over unconfident channels. Cryptography is allows secure storage of sensitive data on any computer.

Encryption

The process of data encryption is to process the original plaintext files or data according to an algorithm, formation it unreadable piece of code, referred to as "ciphertext". The process is the decryption process is the process of translating encoding information into its original planetext. Encryption techniques such as secret-key, public-key and digital signatures are the most common method of ensuring transaction privacy, confidentiality and integrity.

Terminology of Cryptography:

- Cryptographic/Cipher System: A method of disguising a message so only authorized users may read it.
- Cryptology: The study of cryptography.
- Encryption: The process of converting plaintext into ciphertext.
- Decryption: The process of converting ciphertext back to its original plaintext.
- Cryptographic Algorithm: computational procedure used to encrypt and decrypt messages
- Cryptanalysis: The process of finding a weakness in, or actual breaking of, a cryptographic system.

Types of Cryptographic Techniques :

- Symmetric Cryptography:

In Symmetric Cryptography both encryption and decryption are performed using the same secret key. symmetric key cryptography is computationally efficient with shorter keys and shorter lifespan.

- Asymmetric Cryptography:

In Asymmetric Cryptography both encryption and decryption are performed using the public key private key, which two must match to use, or cannot open the encrypted files.

IV. DESIGN OF NETWORK SECURITY

The main platform uses DES encryption Algorithms. DES performs an initial permutation on the entire 64 bit block of data. DES was the outcome of a research project set up by International Business Machines (IBM) corporation in the late 1960's which resulted in a cipher known as LUCIFER. In the early 1970's it was decided to commercialise LUCIFER and a number of significant changes were introduced. The changed version of LUCIFER was put forward as a proposal for the new national encryption standard requested by the National Bureau of Standards (NBS)3. DES was agreed as a federal standard in November 1976, finally adopted in 1977 as the Data Encryption Standard - DES (FIPS PUB 46). DES used the block size is 64 bits.

DES is based on a cipher known as the Feistel block cipher. The block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Most symmetric encryption schemes are based on this structure (known as a feistel network). DES gives two inputs - the plaintext to be encrypted and the secret key. The method in which the plaintext is accepted, and the key arrangement used for encryption and decryption. DES is a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and only operates on 64 bit blocks of data at a time5 (be they plaintext or ciphertext). The key size used is 56 bits, however a 64 bit (or eight-byte) key is actually input. Plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input.

Structure

DES performs an initial permutation on the entire 64 bit block of data. It is then divide into 2, 32 bit sub-blocks, Li and Ri which are then passed into alternately; this criss-crossing is known as the Feistel scheme, is also known as a round ,of which there are 16 (the subscript i in Li and Ri indicates the current round). Each of the rounds are identical and the effects of increasing their number is double - the algorithms security is increased and its temporal efficiency decreased. These are two conflicting outcomes. For DES the number chosen was 16, probably to guarantee the elimination of any correlation between the ciphertext and either the plaintext or key6. At the end of 16th round, the 32 bit Li and Ri output quantities are swapped to create what is known as the pre-output.

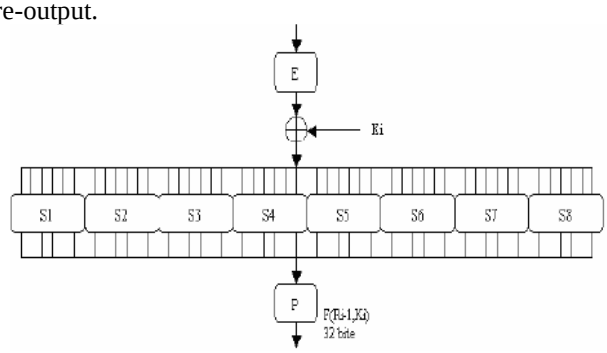

Fig-1: Process map

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This [R16, L16] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit ciphertext. So in total the processing of the plaintext proceeds in three phases as can be seen from the left hand side of fig-1:

1. Initial permutation (IP - defined in table) rearranging the bits to form the "permuted input".
2. Followed by 16 iterations of the same function (substitution and permutation). The output of the last iteration consists of 64 bits which is a function of the plaintext and key. The left and right halves are swapped to produce the pre-output.
3. Finally, the pre-output is passed through a permutation (IP−1 - defined in table) which is simply the inverse of the initial permutation (IP). The output of IP−1 is the 64-bit ciphertext.

Table 1: Initial permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table 2: Inverse initial permutation (IP−1)

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Table 3: Expansion permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Table 4: Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

The inputs to each round consist of the Li, Ri pair and a 48 bit subkey which is a shifted and contracted version of the original 56 bit key. DES also uses a key to customize the transformation. The use of the key can be seen fig-1:

- Initially the key is passed through a permutation function.
- For each of the 16 iterations, a subkey (Ki) is produced by a combination of a left circular shift and a permutation which is the same for each iteration.

Decryption process is similar to the encryption process, decryption process and the encryption process are on the contrary, the only the middle sub key is reverse order. Security problems of TCP/IP TCP/IP, which is main protocol used by Internet, has good qualities of interconnection, support to many other protocols of application, and so on. In order to achieve the stability and reliability of communication, the design uses TCP protocol of transport layer.

Implementation:

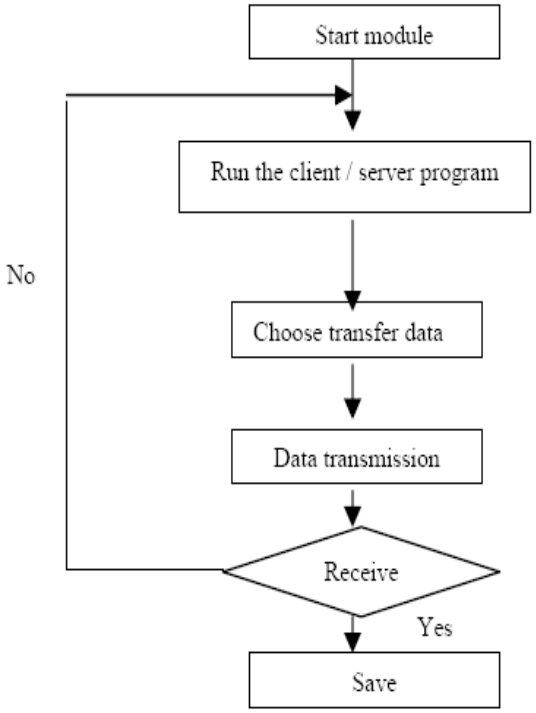

Fig- 2: Encryption Process

Enter each other's IP address computer system and port number, enter key both sides priory agree, the key can be a number or a character, such as '12345678 ' or 'abcgtf ', save the file. Open the ciphertext to the right of browsing, select declassified file, choose to save the original path, click on the decrypt button, if the decryption success will prompt the user to decrypt successfully. Need to attention to several questions:

(1) The decryption key and encryption keys must be the same as, or cannot be restored out of the original.

(2) Network transmission errors may occur from time to time, after which you can re-send.

To complete encryption, most secret key algorithms use two main techniques known as substitution and permutation. DES of course isn't the only symmetric cipher. There are many others. Such ciphers include: IDEA, RC4, RC5, RC6 and the new Advanced Encryption Standard (AES). AES is an important algorithm and was originally meant to replace DES (and its more secure variant triple DES) as the standard algorithm for non-classified material.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

However as of 2003, AES with key sizes of 192 and 256 bits has been found to be secure enough to protect information up to top secret.

V. CONCLUSION

E-businesses should better support for third-party transaction services, trust infrastructure, privacy platforms and security solutions. At present, Internet-based e-business applications are in the time of the rapid development, leading to its security technology and safety management failed to keep pace, especially in the security context, the gap between China and developed countries is still relatively large. With the constant improvement of standards for ecommerce, security technology continues to improve, we believe that e-commerce will have a more worldwide-the future. Encryption technology of e-commerce platform for network security, implementing information encryption and transmission on the network. Even though there are useful laws focusing on several aspects of e-commerce trust, privacy and security, common agreements between the different countries are still missing.

REFERENCES

1. Hu Xiangdong,Wei Qinfang. "*Application of Cryptography Tutorial*" Beijing: Electronic Industry Press, 2005:172-220
2. Nayunipatruni Suman , "*Network Security Evaluation Based on Information Security*" ,International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011
3. Xi Jianrong, "*Network Security Platform Design Based on WWW Information System*" , International Conference on Machine Vision and Human-machine Interface 2010
4. Xie Xiren*." Computer Networks (4th edition)*" Beijing: Electronic Industry Press, 2006:280-330
5. Wang YanPing, Zhang Yue. "*Windows network and communications programming*" Beijing: People's Posts & Telecom Press, 2006:51 – 80
6. Wang Zhengjun "*Visual C++ 6.0 programming from entry to the essence*" Beijing: People's Posts & Telecom Press, 2006:200 - 220
7. Zhang Hongqi. "*Information network security*" Tsinghua University Press, 2002:81 - 94
8. Katsikas.SK, Lopez.j., Pernul.G, "*Trust, privacy and security in digital business*" Computer System Science and Engineering Volume 20, Issue 6, November 2005, Pages 391-399
9. Yu Shaojun. "*E-Commerce Security Analysis and data encryption technology*" China's management of information technology (Integrated version), 2007
10. ShiHua "*Network transmission of data technology research*" Scientific and technical information, 2006

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)