"ANALYSIS AND RESEARCH OF COMPUTER NETWORK SECURITY AND CRYPTOGRAPHY"

[1]PROF. RAHUL BAMBODKAR
DMIETR, Sawanghi (Meghe), Wardha ,India
rahulbambodkar1@gmail.com

[2]PROF. AKHIL ANJIKAR
RGCER, Hingna Road, Wanadongri, Nagpur, India
akhil.anjikar09@gmail.com

ABSTRACT: *Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.*

***Keywords**:* Network Security, Cryptography, Data Security,

1. INTRODUCTION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network.

Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non repudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Non repudiation deals with signatures. Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either malicously or by accident, in transmission. Extensions to the check summing techniques that we encountered in reliable transport and data link protocols. Cryptography is an emerging technology, which is important for network security. The widespread use of computerized data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission. Due to continuing advancements in communications and eavesdropping technologies, business organizations and private individuals are beginning to protect their information in computer systems and networks using cryptographic techniques, which , until very recently, were exclusively used by the military and diplomatic communities. Cryptography is a vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorized access[1].

1.1 OVERVIEW OF COMPUTER NETWORK SECURITY

Computer network security is fundamentally network information security. It refers to the network system that we use to preserve and flow information and data which may otherwise be exposed to accidental or deliberate damage, leaks or changes. Generally speaking, network security is inextricably related to the confidentiality integrity, authenticity and reliability of network. Its control technologies and concepts are necessary to analyze.

2. BASIC TECHNOLOGIES OF COMPUTER NETWORK SECURITY

2.1 Firewall Technology

Firewall technology is an array of safety applications to exert mandatory access on external network by using predetermined safety facilities between network systems. Data transfer between two or more networks should follow certain safety measures to monitor the performance, determine whether the communication between the networks is allowed, and monitor the running of the network.

2.2 Data Encryption Technology

Data encryption technology categories can be divided in data storage, data transfer, data integrity, authentication and key management techniques. Data encryption is stored in the memory in order to prevent data loss and destruction. The transmission process in the information encrypted is commonly in the form of circuit encryption and port encryption. Data integrity identification technology is to protect information transfer, storage, access, identification and confidential treatment of people and data. In this process, the system is characterized by the parameter value judgment on whether the input is in line with the set value. Data are subject to validation, and encryption enhanced the protection. Key management is a common encryption in many cases. Key management techniques include key generation, distribution, storage, and destruction, etc.

2.3 Intrusion Detection Technology

Intrusion detection technology is to ensure the safety of the design and the rational allocation. Intrusion detection technology can quickly find anomalies in the system and the authorized condition in the report. It can address and resolve system vulnerabilities in a timely manner. Technologies that are not in line with security policies are frequently used.

2.4 Anti-virus Technology

Anti-virus technology not simply refers to anti-virus software technology. From the effects of its use, it can be classified into network anti-virus software and stand-alone anti-virus software. Online anti-virus software focuses on network connection against viruses. Once the virus has invaded the network or diffused to other network data, it will be promptly detected by online virus software, be killed and deleted.

3. THREATS OF COMPUTER NETWORK

3.1 Online virus and its features

Computer network makes it possible to transfer and exchange information, but also makes computer virus spread and endangers people's safety and privacy. Every day, dozens of virus are found and spread fast, peeking into other’s privacy. Survey result of 1500 companies is shown in Table II: Each year, nearly 99 percent of companies have suffered from varying degrees of virus damages.

A computer virus is a program capable of autonomous replication with different degree of destruction. Users cannot perceive the replication of these viruses because they hide in the data or frequently used files. Once users use these data or files, the virus will begin replication and spread. This type is called a first-generation computer virus. Now there is a new form of the virus, which is different from the first generation. It doesn’t need to hide in the data at all. It hides itself in the network and causes inconvenience to users of malicious code. It takes the advantage of the web media, spreads fast and causes wide range of harm. Table III shows the number of new viruses discovered the domestic anti-virus software company in recent years:

3.2 Threats of hackers

Besides viruses, there is also a safety hazard, namely, hacker and hacker program. Hacker mainly refers to the illegal invaders to the computer system, who have powerful skills and talents and are obsessed with computers. Hackers may secretly get access to some restricted areas without consent and sneak into other people's computers systems. Currently, hackers are piled in groups, the development trend of which is staggering. Hacker causes great harms, including theft and embezzlement in financial and economic fields. They also spread false advertisings to scam money, steal military, commercial and political secrets, attack other people's copyrights, and manufacture new virus software to spread yellow information. According to the research of FBI, the losses of network security register $ 7.6 billion in USA. The computer network intrusion happens for every 20 minutes. Huge losses are unavoidable.

4. THREATS OF COMPUTER NETWORK

4.1 Online virus and its features

Computer network makes it possible to transfer and exchange information, but also makes computer virus spread and endangers people's safety and privacy. Every day, dozens of virus are found and spread fast, peeking into other’s privacy.

4.2 Threats of hackers

Besides viruses, there is also a safety hazard, namely, hacker and hacker program. Hacker mainly refers to the illegal invaders to the computer system, who have powerful skills and talents and are obsessed with computers. Hackers may secretly get access to some restricted areas without consent and sneak into other people's computers systems. Currently, hackers are piled in groups, the development trend of which is staggering. Hacker causes great harms, including theft and embezzlement in financial and economic fields. They also spread false advertisings to scam money, steal military, commercial and political secrets, attack other people's copyrights, and manufacture new virus software to spread yellow information. According to the research of FBI, the losses of network security register $ 7.6 billion in USA. The computer network intrusion happens for every 20 minutes. Huge losses are unavoidable.

5. CRYTOGRAPHIC PRINCIPLES

A. Redundancy

Cryptographic principle 1: The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

B. Freshness

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

6. CRYPTOSYSTEM TYPES

6.1 Asymmetric cryptosystems

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by Diffie and Hellman in 1976 [10]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other, used for deciphering, is kept secret. The two keys are generated such that it is computationally infeasible to find the secret key from the public key. If user A wants to communicate with user B, A can use B's public key (from a public directory) to encipher the data. Only B can decipher the ciphertext since he alone possesses the secret deciphering key. The scheme described above is called a public-key cryptosystem or an asymmetric cryptosystem[11]. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures[12].

6.2 Symmetric cryptosystems

In symmetric cryptosystems (also called conventional, secret-key or one-key cryptosystems), the enciphering and deciphering keys are either identical or simply related, i.e. 684 IEE PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984 one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure channel, for example a private courier, and the number of keys can be very large, if every pair of users requires a different key, even for a moderate number of users, i.e. n(n — l)/2 for n users. This creates a key-distribution problem which is partially solved in the asymmetric systems. Examples of symmetric systems are the data encryption standard (DES) [4] and rotor ciphers.

7. CONCLUSION

Computer network security is a complicated issue, involving many aspects of computer technology, network management, network usage and maintenance. In order to increase computer network security, we should mix various types of applications for protection measures. It is necessary to develop more effective security solving measures, thereby to improve the computer network security prevention and. It is a long way to go to ensure the normal operation of large-scale network system and communication and maintain sustainable and efficient transport network. To build a harmonious secure computer network security system, we need to take advantage of a variety of integrated network security and green data networking products to form an intelligent network protection system, and thus make computer network security meet various needs.

8. REFERENCES

[1] DENNING, D., and DENNING, P.J.: 'Data security', ACM Computer. Surveys, 1979, 11, pp. 227-250

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] 'Data encyption standard', FIPS PUB 46, National Bureau of Standards,Washington, DC Jan. 1977

[5] Murat Fiskiran , Ruby B. Lee, ―Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments‖, IEEE International Workshop on Workload Characterization, 2002. WWC-5, 2002.

[6] Coron, J. S. , " What is cryptography?", IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.

[7] Pfleeger, C. P., & Pfleeger, S. L.," Security in Computing", Upper Saddle River, NJ: Prentice Hall.2003.

[8] Salomon, D., "Coding for Data and Computer Communications", New York, NY: Spring Science and Business Media.2005.

[9] Shannon, E. C.,"Communication theory of secrecy system", Bell System Technical Journal, Vol.28, No.4, 1949, pp.656-715.

[10]DIFFIE, W., and HELLMAN, M.: 'New directions in cryptography', IEEE Trans., 1976, IT-22, pp. 644-654

[11] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Computer. Surveys, 1979, 11, pp. 305-330

[12] RIVEST, R.L., SHAMIR, A., and ADLEMAN, L: 'A method for obtaining digital signatures and public-key cryptosystems', CACM, 1978, 21, pp. 120-126