Security Analysis of a Computer Network

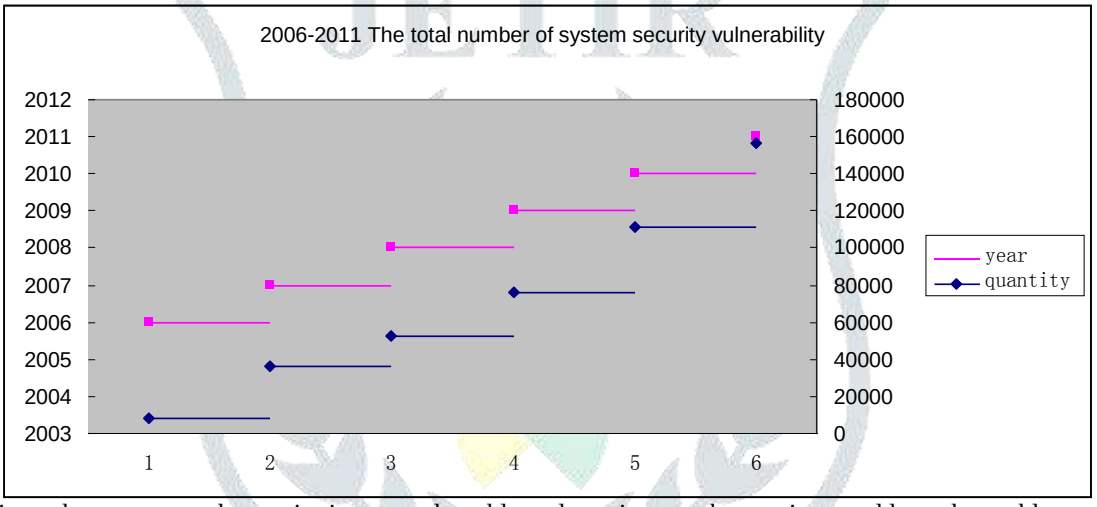
Niwesh Kumar
M.Tech in Computer Science and Engineering Sarvepalli Radhakrishnan University,Bhopal
(Madhya Pradesh)India

ABSTRACT: In this tmethods for security analysis at the IP layer are presented and evaluated. The evaluation is mainly focused on deployment in real high speed networks. Next, a solution comprising selected method is proposed. The goal of this solution is to simplify work of a network administrator and speed up the security incident response. Finally, the proposed solution is tested in the campus network of the SRK University.

Keywords: computer network security; threats; basic technique; measures

INTRODUCTION

With the progress of time, computer technology has been greatly developed and today's network communication system has spread to every corner of the world, involving political, economic, military and all walks of social life. It plays an extremely important role. However, besides fun and convenience, computer also brings to us a lot of security risks due to its openness and connectivity. Users are now faced with a large number of security threats. Is computer network safe? Criminal cases are frequently visitors of domestic and international coverage. Reports on systematic security vulnerabilities are never rare. Table 1 shows the report on security vulnerabilities of information system by the U.S. security organization CERT / CC.



These iron facts indicate that our network security is very vulnerable and requires much attention to address the problem.

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 toanalyze.

2. BASIC TECHNOLOGIES OF COMPUTER NETWORK SECURITY

3.1 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.

3.2 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.

3.3 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.

3.4 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:

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.

4. MEASURES TO IMPROVE NETWORK SECURITY

5.1 Online anti-virus measures.

According to the characteristics of computer network virus, effective prevention on the virus is difficult and complex. It is a daunting task for network managers to monitor the prevention work. Previous work is only limited to every client computer, in which every user needs to install anti-virus software and on your machine, such as KV300 system, or Rising anti-virus software, etc. However, due to limited computer skill of users, this approach is hard to ensure the safety of the whole network system. As an effective solution to prevent the, the basic requirement is to meet the following demands:

1. Install anti-virus software on computers
2 Update the virus database in users' machines
3 Released the latest virus database upgrade file from the WAN connection 4 Coordination and management of remote users' virus scanning
5 Address user-reported problems timely
6 Download and preview scan report provided by users 7 Remote control user options
8 Improve the execution speed and zooming ability in large-scale networks

People are more capable of preventing online viruses. More anti-virus measures have emerged in order to effectively guarantee the network security. Network management personnel can install a complete set of virus software on any client server through one source server. As there are many types of software, network managers should take into account their own situation to achieve the "best use." When choosing solutions, managers should address current situation and leave room for further developments.

5.2 Measure to prevent hackers.

The invasion and attack can be divided into subjective and objective security issues. Subjectivity security issue mainly refers to errors made by network management personnel. Objectivity security issue mainly refers to loopholes in computers and the network where hackers exploit these vulnerabilities to conduct various forms of attack.

5.2.1 Use safety tool

The above-mentioned basic techniques of computer network security can collect safety issues of host computers. Network management personnel identify these problems in a timely manner and install the patch. Network managers take the advantage of scanning tools (such as NAL's Cyber Cop Scanner) to scan host computers, learn about the weakness links take appropriate preventive and repair measures.

5.2.2 Firewall technology

This paper has described the firewall technology. In short, firewall technology is to prevent others from accessing your network device like a shield. There are three types of firewall technology, namely, packet filtering technology, agent technology, and status monitoring technology. Packet filtering technology is to verify the IP address by setting it. Those IP addresses that do not match those settings will be filtered by the firewall. But this is the first layer of protection. Agent technology is to verify the legitimacy of requests sent by accept client of proxy server to. This technology also involves with user authentication, login, simplified filtering criteria and shielding the internal IP addresses. Status monitoring technology is the third generation of network security technologies, which is effective for all levels of network monitoring. It makes it possible to make timely security decisions. Firewall technology can successfully prevent hacker from intrusion in the local

network and protect the network.

5.2.3 Measures about switch

When designing a large-scale regional computer network, we need to ensure that the switch is connected to a network or in a separate network, so that the switch can form a separate management network. This will effectively reduce the number of network switches and narrow the scope of failure. By using search and location, it is also convenient for network managers to quickly handle remote network accidents.

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.

REFERENCES

[1] Translated by Cheng Peiqing, et al. *Computer network security. Publishing House of Electronics Industry*, **1994**.9

[2] Li Wenlong. Face to face with a hacker. *internet world*.**1999**(2):2~8

[3]Xiao Ze. Research on computer network security analysis model [J]. *Journal On Communications*, **2012**(3):269. [4]Zhang Cheng. Research on computer network security analysis model [J]. *Practical Electronics*, **20l3**(v)=148- 149.

[5] Hong Yaling. Research on computer network security analysis model [J]. *Computer CD Software and Applications*, **2013**(z):1-152.

[6] Wang Yuan. Quantitative Evaluation Method of Network Security Situation [D]. Ph.D. Dissertation, university of science and technology, **2003**.

[7] Cui Jing, Liu Guangzhong, the basics of computer network [J]. *Tsinghua University Press*, **2010**.07.01.

[8] Wang Wenbing, security of computer network [J], *Tsinghua University Press*, **2010**.06.01