ISSN : 0974 - 7435 Volume 10 Issue 9

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(9), 2014 [3377 - 3381]

Analysis of computer system vulnerability

Xin Gao[1]*, Xiaoyu Zhao[2]

[1]Yellow River Conservancy Technical Institute, (CHINA)

[2]Zhengzhou Vocational College of Economics and Trade, (CHINA)

E-mail : gao_xin11@163.com; doumor@qq.com

ABSTRACT

With the gradual development of science and technology, computer systems become more and more complicated. Meanwhile, computer system security is not well guaranteed. A number of lawbreakers take advantage of computer system vulnerability, which is a threat to computer system security. Computer system security cannot be strengthened unless assessments and researches on computer system vulnerability are carried out. This paper aims to cover the definition of computer system vulnerability and explain the causes of the problem. At last, this paper will conclude several methods of doing computer system vulnerability assessment.

KEYWORDS

Computer system; Vulnerability; Assessment.

INTRODUCTION

With the rapid development of science and technology, China's degree of information improves correspondingly and computer systems become more complicated. However, the speed of updating computer systems is so fast that designers don't realize the flaws in their designs. Some lawbreakers take advantage of these flaws, avoid security strategies and destroy computer systems. The degree of defect is called computer system vulnerability. Computer system vulnerability is the intrinsic property of each computer system. In other words, there is no computer system without vulnerability. With the wide spread of computer science and technology, hacker technology develops as well. Many hackers make use of the flaws of computer systems, attack on these flaws and paralyze the whole network.

The emergence and development of computer network makes originally independent host computers related to each other, which boosts the efficiency of computer systems. When people enjoy the benefits of convenient Internet services, they also need to face various threats from Internet. More and more hackers design computer virus and attack computer systems. Security events emerged in the period of host computer terminal. At that time, hacker used computer virus to attack an independent host computer. After the emergence of Internet, computer virus can be transmitted through several ways. Based on Internet, hackers invented many ways of attacking computer systems. More attacking targets and more attacking methods make people pay more attention to computer system security. Figure 1 is about China's Internet computers and security events.

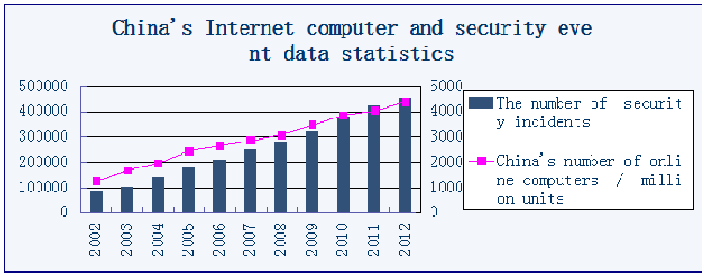

Figure 1 : China's internet computer and security events data statistics

According to the data given by China's Internet Network Information Center (CNNIC), the number of computers is increasing rapidly in China, and the number of security events is increasing as well, whose increasing rate is higher than that of computers. The statistics show that computer system security is being threatened by various computer viruses in the Internet era. There are mainly two reasons for more and more Internet security events. One reason is that Internet is applied to more fields, and the other reason is that hackers improve their attacking methods. Fundamentally, the main cause of increasing Internet security events is computer system vulnerability. 95% China's security events lie in computer system vulnerability. Hackers make use of the flaws computer systems, enter the inner system, destroy the system and paralyze the whole network. So it is of great important to carry out an assessment of computer system vulnerability.

Computer system vulnerability originated in Internet security events. The field emerges relatively early, but it is still a hot research field. However, the computer system vulnerability assessment is still in the initial stage, and it is mainly used to sum up the experience of the actual use of computer systems and use the collected experience to assess other computer systems. This process depends on the process of extracting information and matching information. The research focus is about how to induce more accurate information sources. This kind of computer system vulnerability assessment is the most popular one. The relatively mature network security scanning method is the typical application of the assessments. Based on this kind of computer system vulnerability assessment, some experts start to employ fault tree, Petri nets, finite-state machine and other theories to carry out computer system vulnerability assessment, trying working out a more comprehensive assessment method.

INTRODUCTION OF COMPUTER SYSTEM VULNERABILITY

The definition and classification of computer system vulnerability

Computer system vulnerability can be regarded as the security loophole of computer network, and it is in the aspect of unexpected use. The complexity makes it difficult for designers to take all aspects of the computer systems into consideration. Therefore, hackers take advantage of the flaws, enter the inner system and do damage to the system. Computer system vulnerability mainly lies in the process of designing and achieving hardware, software and agreements. As the inherent property, these flaws can be used by hackers to destroy the system in an authorized way.

Computer system vulnerability can be classified into three types: entity vulnerability, software vulnerability and Internet communication vulnerability. Entity vulnerability is mainly caused by the lack of integrity and entirety in the design of computer hardware. Entity vulnerability can do harm to CPU and paralyze the system. The head failure of hardware can result in read-write failure and the paralysis of the whole computer system. External factors like electromagnetic pulse, high temperature and strong magnetic field, can also damage the computer hardware heavily. Software vulnerability is the most common one, because software vulnerability is tightly related to computer system. Hackers usually enter software by inserting virus into certain program, calling functions and programs and getting powers. The functions of computer software are made up of different links. The design and programming, even application is quite different from each other in terms of ideology level. A mistake of certain algorithm or programming can make illegal module invade legal program, which shows that one reason of software vulnerability is the integrity of executable files. Internet communication vulnerability is highly connected with software vulnerability. Computer network can achieve hardware sharing, software sharing, data sharing and sharing of controlling information, but there are some problems and loopholes in recognizing users' identities. Advanced Internet communication circuits are telephone line, microwave circuit, special line, etc. These circuits can be easily influenced by electronic interference, and the transmitting information can be gotten easily as well. The interface between networks also has flaws. All these flaws become the breakthrough point of illegal intrusion and offer hackers ways of entering systems.

Causes and harms of computer system vulnerability

The reason for the existence of computer system vulnerability is that programmers do not fully understand the inner programs. In the process of designing and programming, programmers don't take every aspects of computer systems into consideration, which causes computer system vulnerability. Some programmers program in an incorrect and unsafe way, which worsen computer system vulnerability. Influenced by occupation habits, programmers usually assume that their programs can be operated in any situation. Thus, programmers may easily ignore the operating situation, applicable objects and external factors when they are constructing computer system. It can be concluded that in order to maintaining the normal operation, programmers need to consider the stability of the system and all the factors above. In addition, users' incorrect use will also bring about potential danger to computer system and result in computer system vulnerability.

The harm of computer system vulnerability can be shown in several aspects, for instance, disclosure of confidential information, wide spread of Internet virus and hacker intrusion, which can do great harm to individual users and enterprises by cause numerous economic loss. With the gradual improvement of the degree of information, more severe computer system vulnerability can be a threat to national security in the aspects of politics, economy and military. Essentially, computer system vulnerability can harm five kinds of system securities, which are reliability, confidentiality, entirety, usability and undeniableness. Reliability refers to reducing incorrect false alarm in the operation of computer system and improves the efficiency of computer system. Confidentiality means protecting users' information from disclosure and getting by unauthorized third party. Entirety requires that programs or information should not be tampered, forged, inserted and deleted purposely in the process of storing, communication and operation. In other words, programs or information cannot be destroyed

or lost. Usability means guaranteeing that users can enjoy the services offered by computer and information network. Even some program is damaged; the system can also provide users with effective functions. Undeniableness is about the users of computer system, and it refers to guaranteeing information actors to be responsible for their behavior.

ANALYSIS OF COMPUTER SYSTEM VULNERABILITY ASSESSMENT

Significance of computer system vulnerability assessment

Programmers carry out computer system vulnerability assessment by obtaining relative information, checking up the information and analyzing whether a single network or network service is normal or not. Computer system vulnerability assessment assumes the computer system being attacked, quantifies the attacks and checks whether the system have strong risk response to the attacks. If computer system vulnerability outweighs the risks, the normal operation will be disturbed and threatened. With the rapid development of computer science and technology, many computer attacks and network security events occurred. These attacks and security events take place mainly because of the security vulnerability of computer system itself, and the vulnerability become the breakthrough point of hackers' or computer virus' intrusion. Strengthening computer system vulnerability assessment can improve the stability and security of computer systems, decrease computer system vulnerability and reduce the occurrence of computer attacks and network security events.

Corporative computer system vulnerability assessment

Corporative computer system vulnerability assessment method firstly assumes that the third party's visit to the computer system is legal, and allows it to looking through information and using resources. The information gotten by the third party is legal resources and is gotten through standardized system check. It should guarantee that every check is done by different assessment programs. The managers of computer systems can pass the check, undertake assessment, divide the task into different parts and put them on different platform. Then programmers use corporative computer system vulnerability assessment method to conduct high density examination. In this way can programmers find the flaws and loopholes of the computer system, check out abnormal data, files and the trail left by hackers. In a word, corporative computer system vulnerability assessment method is very reliable.

Non-corporative computer system vulnerability assessment

Non-corporative computer system vulnerability assessment method is used when computer systems find the intruder. Then computer systems keep full record of intruder's actions and detect its Internet behavior, assessing the vulnerability of Internet service systems. In order to execute non-corporative computer system vulnerability assessment, the intruding program should pass the state test and check out whether the computer system has system vulnerability by employing technologies like version information, agreement coordination, port state, etc. Non-corporative computer system vulnerability assessment usually be done on a separate platform. Programmers use a single analyzer to support the entrances of several operating platforms. TABLE 1 is the comparison between corporative computer system vulnerability assessment and non-corporative computer system vulnerability assessment.

TABLE 1 : Comparison of vulnerability analysis of computer

Method of characteristics	The executive body	Access to information source	Access to information condition	There may be platform	Reliability
The cooperative analysis	Administrator	The detection information	Assume legal detection	Multiple	Very reliable
Analysis of non cooperative	Hacker	Attack and return information	If the illegal invasion	one	The relatively reliable

According to TABLE 1, it can be concluded that non-corporative computer system vulnerability assessment is more convenient, while the more complex corporative computer system vulnerability assessment is more reliable.

Computer system vulnerability assessment method based on rules and models

The assessment of computer vulnerability mainly check out whether computer systems are infiltrated and discover new permeability changes and change sequences. The former one should be done by using general matching rule, and the later one should be done by making model analysis. The relatively mature network security scanning method is the typical application of the computer system vulnerability assessment. It is also an assessment method based on rules and models. It mainly uses rules and divides rules into three aspects, finding flaws, getting information, detecting flaws. Comparison of detection method of operating system is shown in TABLE 2.

TABLE 2 : Comparison of detection method of operating system

Using the TCP/IP protocol information	Active feature detection	Method	Advantage	Shortcomings
		Response analysis of ICMP	High accuracy	Firewall blocking UDP or ICMP protocol is not reliable
		Response analysis of TCP segment	Three port, high accuracy	In the case of firewall can only open a port, can not guarantee the accuracy
		Analysis of TCP segment delay	Only one port	Slow speed
Passive detection			Not easy to be found	Analysis of the data is more complex
Using the system and service of Banner			Simple, fast, efficient	Sometimes easily information deception, even unable to obtain information

Since network security scanning method is based on rules, it can only make vulnerability assessment of a single host computer. So the vulnerability assessment of the whole computer network should be carried out by using technology based on models.

CONCLUSIONS

Computer systems play a very important role in social life. It is also the necessary infrastructure that promotes economic development. However, because of some internal and external factors, computer systems have inherent vulnerability. Therefore, more effective computer system vulnerability methods should be applied. In this way can computer system security be improved?

REFERENCES

[1] Xing Xujia, Lin Chuang, Jiang Yixin; A Survey of Computer Vulnerability Assessment [J]. Chinese Journal of Computers, **01**, 01-11 **(2004)**.
[2] Liu Li; A Survey of Computer Vulnerability Assessment [J]. Digital Technology and Application, **10**,51 **(2013)**.
[3] Huang Bo; On the vulnerability of computer systems and Hacking protection[J]. Network Security Technology & Application, 09, 14-15 **(2011)**.
[4] Long Teng; On the vulnerability of computer systems and Hacking protection [J]. Computer CD Software and Applications, **07**, 130-131 **(2013)**.
[5] Zhou Haifeng; Assessment of computer system security vulnerability [J]. Science & Technology Information, **11**, 27 **(2012)**.
[6] Xu Xin, Yang Lanqin; Analysis of Computer System Stability and Vulnerability Assessment [J]. Coal Technology, **04**, 148-149 **(2013)**.
[7] Liu Bin; Assessment of computer system vulnerability [J]. Silicon Valley, **23**, 118-120 **(2013)**.
[8] Yang Errui, Zhu Hongwei; Analysis of Computer System Stability and Vulnerability Assessment [J]. Silicon Valley, **07**, 151-152 **(2013)**.