International Core Journal of Engineering Volume 8 Issue 9, 2022
ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

Computer Network Information Security and its Defense Strategy based on the Growth of Attack Capability

Xiaokang Chen

Sichuan Normal University Chengdu, Sichuan 610066, China

Abstract

With the growth of the times, computer meshwork technology has developed rapidly and has become an inseparable part of today's society. Computer meshwork services have penetrated into the economic production activities of enterprises and people's daily life, and subtly affect the way of economic production activities and people's living habits. However, while the computer meshwork technology brings convenience, its growth also faces a series of problems. These problems have become a difficult problem for people today. Various criminals take advantage of people's dependence on computers to take some illegal means to illegally reselling the business of enterprises. Confidentiality and personal information of residents have seriously endangered the social order and brought a lot of worries to people in the process of using computers. The problem of computer meshwork information security has also aroused extensive attention from all walks of life, the government, enterprises, society and Individuals have adopted various virtual meshwork-specific technologies to ensure their own information security. The issue of computer meshwork information security has attracted people's attention, and they are looking forward to the implementation of relevant measures. Therefore, this paper proposes a detailed strategy for computer meshwork information security and its protection based on the increasing attack capability. First of all, a brief overview of the problems faced by computer meshwork information security in computer meshwork technology is given, and a mathematical model is used to simulate and analyze. Secondly, some targeted strategies are provided for the protection of computer meshwork information security.

Keywords

Attack Capability Growth; Computer Meshwork Information Security; Meshwork Information Protection.

1. Introduction

With the rapid growth of sci & tech, the power of computer meshwork technology functions is obvious to all, and the research on meshwork information security construction has become more in-depth, and customers' requirements for meshwork security have gradually increased[1]. In the context of the era of big data, when enterprises use computer technology for information management, they need to strengthen the protection of information security and information risks. In the era of big data, the use of information technology has increased, and by establishing a more complete meshwork system, it has provided a good meshwork environment for some personalized industries[2]. In order to ensure the effective use of information, it is necessary to combine virtual technology[3], meshwork security protection technology, and firewall technology to deal with viruses and improve meshwork security information. The construction of meshwork information security can strengthen the protection and intelligent monitoring of the meshwork environment, and build a safe meshwork information environment through the combination of environmental monitoring and information

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

interaction software systems. Moreover, there are many factors that affect the information security of computer meshworks, including human factors, natural environment factors, and system vulnerabilities[4]. Similarly, both developed and developing countries are facing the problem of computer meshwork information security. This problem is currently in urgent need of solving. In this regard, this paper proposes to improve the security of computer meshwork information based on the growth of attack capability and make effective protection strategies. In the process, it is necessary to combine the occurrence of various meshwork security problems and take reasonable protection measures to ensure the security of the entire computer meshwork. reliable. And this paper studies the impact of hackers' attacks, hoping to improve the ability to respond in time and make computer meshwork communication secure.

2. Overview of Computer Meshwork Information Security and its Analysis Model

2.1 Computer Meshwork Information Security

Computer meshwork information security not only includes the security of related machines and equipment, but more importantly, the security of user information data stored in the computer. The security of user information stored in the computer includes not only the physical data security, but also the logical security of the data. Computer meshwork information security is not an abstract concept. When it is detailed to information data, it becomes a real method and measure. In practice, in order to maintain the security of computer meshwork information, people often carry out some artificial technology implantation and management restrictions, so that the security of computer meshwork information can be guaranteed. However, with the continuous growth of computer meshwork technology, some criminals will use the loopholes of the system to carry out malicious damage, which is a major threat to computer meshwork information security[5].

2.2 Influencing Factors of Computer Meshwork Information Security

In this era, people surf the Internet very daily, and many important communication activities are realized through computer meshworks. The user's demand for computer functions and the frequency of use make them put forward higher requirements for computer meshwork information security. Indeed, when the data information stored in the computer by the user is destroyed, it will not only cause property damage, but also seriously threaten life safety[6]. Therefore, the maintenance of computer meshwork information security is very necessary. In order to better maintain the security of computer meshwork information, we must identify the factors that lead to the insecurity of computer meshwork information, so as to prescribe the right medicine. Next, mainly from the four main threats to computer meshwork information security factors, namely:

(1) Vulnerabilities in the computer meshwork system itself:

I believe everyone has heard the saying "A thousand miles of dikes are destroyed by ants' nests"! This sentence is also applicable to the maintenance of computer meshwork information security. Even if there is a small system loophole in the computer meshwork system, the consequences are unpredictable. On the one hand, the loopholes in the computer meshwork may be caused deliberately, on the other hand, it may be caused by the lack of technology or the negligence of the work process. In short, in any case, it is absolutely not allowed to cause loopholes in the computer meshwork system. When there are loopholes in the computer meshwork system, criminals can use these loopholes to carry out illegal activities such as information destruction and information theft.

(2) Man-made sabotage:

The man-made sabotage here is mainly from the hacker attack, which is an important threat factor affecting the information security of the computer meshwork at present. Hackers are a group of technical and wise groups, and their attacks have a strong purpose, and often bring huge damage to the target of the attack. Hackers' attacks include the destruction and theft of existing information and data in the computer system, and even the paralysis of the entire computer meshwork system. At the

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

same time, some hackers have excellent technology and can easily steal without the user's knowledge. The man-made damage of this kind of hacker attack brings a great threat to the computer meshwork information security[7].

(3) Virus threat:

Computer viruses are not biological viruses that people mistakenly think, but are essentially a type of computer code or data. Computer viruses have the following characteristics:

①It is self-replicating, and this type of instruction or computer data can be self-replicating.

②It is hidden. Generally speaking, this type of virus has an incubation period and can hide in the computer files of the computer.

③It is extremely destructive and contagious. Once a computer virus is stimulated, it can quickly generate a series of chain reactions, resulting in the loss or damage of the file data originally stored in the computer, which will seriously lead to the paralysis of the entire computer.

This extremely destructive and infectious nature undoubtedly brings great damage to users[8].

④Natural factors:

Natural factors mainly include temperature and humidity. Because computers are electronic devices after all, like other electronic devices, they are extremely susceptible to changes in the external environment. At present, many computers on the market do not achieve waterproof and high temperature operation. Once the indicators of these natural factors exceed their tolerance, the application of the computer will be damaged, and some may even fail to work normally.

2.3 Computer Network Security Analysis Model

Definition 1: Vulnerability refers to defects caused by errors in system hardware, software or security policy, and is a software or hardware feature that violates security policy[9]; trust vulnerability refers to defects caused by trust between hosts Security flaws.

Here both vulnerability and trust vulnerability are denoted as V. The exploit of the vulnerability by the attacker is represented as Vx (Host-sour, Host-dest), where the subscript x represents different vulnerabilities; Host-sour represents the source host of the vulnerability, that is, the source host of the attack; Host-dest represents Vulnerable target host, that is, the target host of the attack.

Every time the attacker launches an atomic attack, it will bring dual changes in the environment and attack capability. Therefore, we have the following definitions:

Definition 2: The environmental change ΔE is the environmental change when the attacker uses vulnerability or other means to attack the meshwork[10]. When an attacker uses the vulnerability Vx to attack the meshwork, the change brought by the attack to the meshwork environment is expressed as the environmental change ΔEx, which can be expressed as the following formula:

$$V^{'}(Host-sour, Host-dest) = \Delta E_x \tag{1}$$

Definition 3: Attack capability increment ΔA refers to the increase in the attacker's capability when the attacker uses vulnerability or other means to attack the meshwork[11]. When the attacker exploits the vulnerability Vx to attack the meshwork, the increase of the attacker's capability is expressed as the increment of attack capability ΔAx. It can be expressed as formula (2). The impact of an attacker's attack or vulnerability exploitation is expressed as Equation (3).

$$V^{''}_{x}(Host-sour, Host-dest) = \Delta A_x \tag{2}$$

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

$$V_x(Host-sour, Host-dest) = \Delta A_x + \Delta E_x \quad (3)$$

Definition 4: The attack model M is a finite state automaton, expressed as $M(S, \tau, \Delta A_0 + \Delta A_t)$. Where S={ΔA} represents the attacker's ability change increment set; the initial increment is $\Delta A_0 = \varnothing$, and $\Delta A_0 \in \{\Delta A\}$; the termination increment $\Delta A_t \in \{\Delta A\}$ is the attacker's target increment; $\tau = \{V_x\}$ it represents the exploited vulnerability and attack set.

As shown in Figure 1, the external firewall and the internal firewall divide the meshwork into three parts: one part is the external meshwork, which is what we call the Internet; the other part is the internal meshwork, which is also the target meshwork of the attacker. There are two running Linux, respectively. The host of Windows; the third part is the critical area of the internal meshwork and the external meshwork, where a Web server running IDS is placed. The intrusion detection system exists between the internal meshwork and the internal firewall.

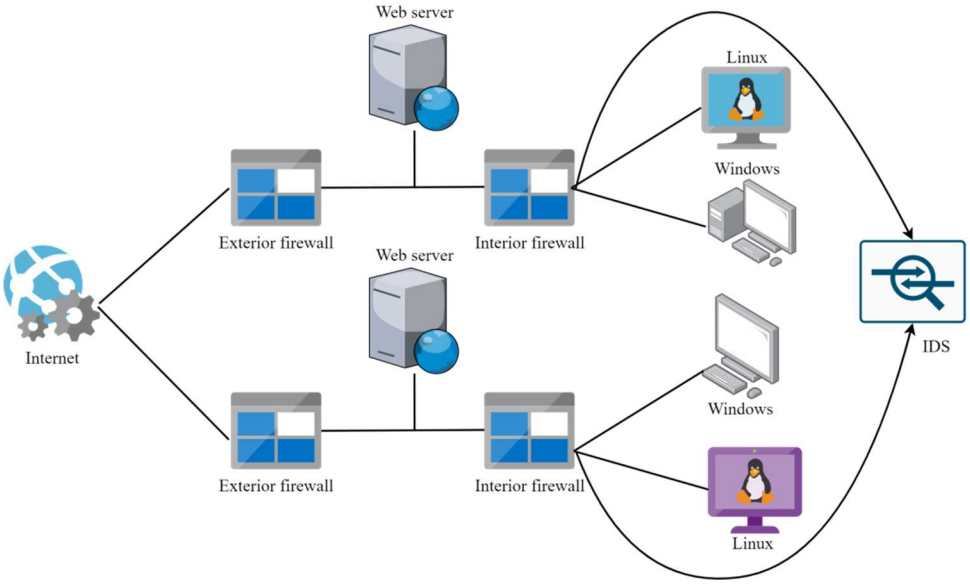

Figure 1. Network topology

The host with Windows installed on the internal meshwork is mainly used for work and Internet access. The Linux machine is installed with the mysql database. For the convenience of growth and use, the mysql database on Linux can be directly accessed through the Windows host. All users in the external meshwork can access the IDS Web server, as well as Windows hosts on the internal meshwork.

There is a buffer overflow vulnerability in the IDS Web server, an attacker can use this vulnerability to gain root privileges and shut down the ID S service; there is a JDBC remote vulnerability on the Windows host, which allows an attacker to remotely execute arbitrary dll as a user; There is an SMB privilege escalation vulnerability in the Windows system, and an attacker who successfully exploits this vulnerability can complete the privilege escalation of the local user; the Linux system has a trust vulnerability, that is, trusting the Windows host, allowing the host to access the mysql database as a specific user; the Linux system has A single-byte buffer overflow vulnerability that can be exploited by a remote attacker to execute arbitrary commands on the system with root user privileges. According to the above description, the connectivity between the hosts of the instance meshwork is shown in Table 1:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

Table 1. Host connectivity of the instance meshwork

Hosts	Attacker	web server	Windows	Linux
Attacker	z	80	m	m
web server	z	z	z	z
Windows	m	80	z	trust
Linux	m	m	z	z

Note: m means that the two subjects are not physically connected; z means that they are physically connected; 80 means that A can access B through port 80; trust means that A can log in to B as a user because it trusts B.

3. Protection Strategies for Computer Meshwork Information Security

We get from the experiments: From the attacker's perspective , if the attack occurs during the day , the intrusion alarm may significantly affect the intrusion; conversely , if it is at night , the intrusion alarm may affect the intrusion less . Hence the result of the environmental analysis is denoted as ids + E Change , where ids ∈ {s , d , b} . The analysis of the minimum environmental change can be carried out according to the above two combined with the actual situation . Through minimal environment change analysis , we can analyze the attack paths that attackers may take under certain conditions , thereby effectively preventing attacks . Of course, in the face of computer meshwork information security, we must take the following countermeasures:

①Learn to install an antivirus software suitable for your computer type in your computer

At present, one of the main reasons why computer meshwork information security is threatened is the invasion of computer viruses. Many hackers will take certain measures to spread viruses to computers when they are in action. To this end, users should choose a suitable anti-virus software for their computers to prevent viruses from invading computers. Take a simple example: the antivirus software installed on a single computer targets remote resources in the local workstation, scans and analyzes them to detect viruses, and then removes them. However, we do not install anti-virus software once and for all. With the upgrade of computer viruses, anti-virus software must be regularly updated and upgraded. Only in this way can we be able to deal with more advanced viruses. In addition, because some computer users only use the computer without protecting the computer, some people have used the computer for a year, and have not disinfected the computer once, which is not desirable. The azimuth antivirus, timely clean up the potential virus that may exist inside the computer. Finally, when the computer is accidentally infected with a virus, the user should use the latest version of anti-virus software to control it in time to prevent the spread of the virus.

②To increase the firewall's control over the computer

Firewall settings are also an important factor that affects computer meshwork security. The firewall can be said to be a protective shell of the computer. By setting the firewall, it can effectively prevent other users outside the meshwork from using the meshwork. At the same time, it also uses permissions to restrict the meshwork use behavior of internal personnel, which can effectively reduce information. The probability of being stolen, when the most important, the firewall also has the function of monitoring the user's meshwork usage behavior. The firewall records the user's meshwork usage behavior in the form of logs, and makes judgments at any time. Once suspicious behavior occurs, it will be taken immediately. measure. However, it is undeniable that the current design level of my country's computer firewall is still relatively low, and it cannot effectively maintain meshwork information security. To this end, my country's information security departments should increase the research on firewalls, improve their security performance, better maintain meshwork information security, create a safe and harmonious meshwork environment for people, and reduce worries.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

③Learn to use the special technology of virtual meshwork to maintain

The special technology of virtual meshwork mainly includes key technology, identity authentication technology, tunnel technology, encryption technology, etc. The Internet itself is an open meshwork. Cause information leakage, but we can use effective means to maintain our personal information security. For example, when using information encryption technology, data encryption policies are applicable to open meshworks. Data encryption can protect dynamic data such as data, files, and passwords in the meshwork and reduce data loss after being attacked. When setting a password, people should try to avoid using information such as initials, birthday, phone number and other easily leaked information as passwords. It should be noted that users should not select "save password" during meshwork operation, and do not use the "remember password" function. If the user remembers the password, the password set by the user will remain permanently on the meshwork and be used by criminals; At the same time, Yinghu also regularly changes the password, so that even if the original password is leaked, losses can be reduced. These are all things that individual users can take note of when using public meshworks. As long as the user's personal meshwork security awareness is improved, the possibility of information being leaked will be greatly reduced.

④ Improve the meshwork management system to prevent meshwork security threats

An effective security management system can maintain strong computer meshwork security. To this end, relevant departments should continuously strengthen the security of computer information meshworks and strengthen their management. In addition, professional security technology and management personnel must be continuously delivered, and relevant enterprises should also continuously strengthen the safety awareness of employees, conduct regular training for information personnel, strengthen the confidentiality awareness of management personnel, and keep important passwords and instructions strictly confidential. Government departments can also use administrative means to regularly publicize computer security management, urge computer users to use the Internet safely and legally, and improve users' laws, regulations and moral concepts.

4. Conclusion

The continuous growth of computer technology provides a guarantee for the growth of the meshwork and the utilization of information. In the context of the growth of attack capabilities and the growth of big data, the security of meshwork information is reduced. In order to ensure the effective use and preservation of information, it is necessary to continuously update meshwork information security technology, pay attention to the effective preservation of information, and reasonably apply computer technology to ensure that cyber security. In a word, the maintenance of computer meshwork information security is not a matter for one individual, nor for a certain company, but for the whole society and this country. Therefore, we must join hands to create a civilized and legal meshwork environment, so that the computer meshwork can better serve our production and life.

References

[1] A-Manjiang A. Analysis of the Computer Network Information Security and the Protective Measures Towards It[J]. Journal of Xinjiang Vocational University, 2012,23(6):189-191.

[2] Pokorny J. NoSQL databases: a step to database scalability in web environment[J]. International Journal of Web Information Systems, 2013, 9(1):278-283.

[3] Han-qing, Chen, Jian-ping. Application Research of Maintenance Technology Based on Computer Virtual Technology[C].2018,10(1):1-49.

[4] Lin L. Study of computer meshwork information security technology[J]. Electronic Design Engineering, 2010,12(6);333-336.

[5] Lin Z , Wei Z. Research on computer meshwork information security and protection strategy[J]. Network Security Technology & Application, 2014,14(3):46-47.

[6] Yue L. The research on computer meshwork information security and protection strategy[J]. Network Security Technology & Application, 2014,15(3):57-59.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202209_8(9).0005

[7] Xian-Zong L I , School S S. Research on Computer Network Security Defense Technology[J]. Computer Knowledge and Technology, 2015,9(2):298-299.

[8] Liu H F. Brief Analysis of Influencing Factors of Computer Network Information Security and Prevention[J]. Information Security and Technology, 2013,21(16):256-258.

[9] Pfleeger S L. Analyzing Computer Security: A Threat/ Vulnerability/ Countermeasure Approach, Rough Cuts[J]. 2011,16(8):368-371.

[10] Abnett A C. Computer Security Environment, US20190026503[P]. 2019,5(1):1-13.

[11] Brouwer M , MD Adler. SYSTEM AND METHOD FOR CONTENT PROTECTION BASED ON A COMBINATION OF A USER PIN AND A DEVICE SPECIFIC IDENTIFIER: US, US20110252243 A1[P]. 2011,3(1):1-27.