The Application of Security Technology on Computer Software Development

Xiaolei Zhao

Weinan Normal University, Weinan, Shaanxi, 714099, China

ABSTRACT. *Today's society is the Internet age, the rapid development of computer technology, computer software technology has also been applied in depth, and penetrated into various areas of society, directly affecting people's lives and work. The development of computer software has also become an important symbol of national social progress, and it is highly reflected in the comprehensive strength of the country. This paper starts with computer development and software development, analyzes the security problems and security risks in computer software development, and proposes corresponding security measures to avoid these problems and improve the security of software development technology.*

Keywords: Security Technology; Computer; Software Development; Application Analysis

1. Introduction

Computer network is an important part of social development. In the 21st century, it is the Internet age. With the in-depth application of computer technology, social production has entered a new stage of development, directly affecting people's life and work, and changing people's way of life. However, with the in-depth application of the network in life and work, people's life and work are more dependent on computer networks. With the increase of the number of users, the continuous development of software technology, the field of computer software is more comprehensive, user information. Security has become an important factor affecting the development of computers. The security risks of computers have restricted the further development of computer networks. Therefore, it is necessary to pay attention to the security technology in software development to ensure the security of user information.

2. Overview of computer software development

Software development is the process of constructing a software system according to user requirements. The development process includes the capture analysis of requirements, the design and implementation of system functions, and the final test. Generally speaking, software is implemented in a certain programming language,

and it needs to be implemented by means of software development tools in the development process. With the development of computer technology, network terminal equipment is no longer a single computer device, and has developed into a terminal device that is small and portable, such as a smart phone or a tablet computer. In addition to changes in smart terminal devices, computer systems and application software are constantly being updated with the development of the times to meet people's needs for computer use.

With the in-depth application of computer software, the field of software is also becoming more and more extensive, and the software is more convenient and sensitive, and more and more humanized. Especially in recent years, the software industry is developing rapidly, and the types of software developed by software companies are gradually increasing, and the functions are becoming more and more powerful, such as handheld bus, online booking, online ordering, etc., which only need to be realized by using a network terminal. It should be noted here that the convenience of the computer network makes the user save personal information during the use process, and the security of the computer software has become the focus of everyone's attention. Computer viruses, hacker attacks and other factors affect the security of computer software. Once computer software is compromised, user information will leak and cause serious damage to users. This requires computer software to pay attention to security issues during the development process and strengthen the application of security technologies.

3. Security risks in computer software development

Computer software development has been continuously developed with the upgrading of computers. The user experience has risen, the operation efficiency is high, and the software is more humanized. However, the security problems encountered in software development are becoming more and more serious. There are many factors that affect the security of computer software. Let's analyze them one by one:

Software development is inseparable from physical equipment such as computer infrastructure and network communication equipment. If these physical equipments have problems, they will directly threaten the security of the computer, thus affecting computer software development. There are many reasons for physical equipment damage. For example, natural disasters, aging of the circuit, human damage and other factors cause poor contact of the equipment, so that the computer can not operate normally, or even completely damage the network equipment, causing the computer system to collapse, thus bringing more to the user. More trouble. The causes of external factors are complex and cannot be expected to be threatened by security. It is difficult to use technology to improve the safety factor. Once a problem occurs, the software development work will fall short. This requires daily maintenance of computer equipment, regular cleaning and maintenance, timely inspection of wiring problems, improvement of inspection system, and improvement of computer network security.

In the process of software development, there are problems in itself. Because software development is developed by people, in the process of development, the level of technical personnel is uneven. In addition, China's software industry is at the initial stage of development, and professional and technical personnel are few. The practical experience is not rich, and there are many loopholes in the developed software. If the security barrier is not set, the software code will be leaked, and the computer software itself has a copy function. Once the source code leaks, the competitor will plagiarize and put it into use. , resulting in the production of piracy. The piracy incidents are endless, leading to serious threats to personal intellectual property. This requires software developers to have a strong sense of security and confidentiality, to encrypt and store the storage tools and development equipment with code to avoid code leakage.

The processing of information is a key part of the use of computers, but in the process, it is vulnerable to viruses or hackers. Hackers use computer network knowledge to attack target computers, intercept or falsify transmission information on the network, destroy the normal operation of the system, cause network system paralysis, affect computer software development work process, and more, in the process of network information transmission. The original legal information is deleted and modified to deceive the user to achieve the purpose of the attack; or the transmission of the intercepted data, thereby stealing the user information and affecting the privacy of the user. The transmission process of information is a relatively fragile link. Once infected by a virus, it will spread at an extremely fast speed, slow down the computer running speed, seriously affect computer software development, and even cause system paralysis, damage data files, and cause irreversible loss. .

4. Application of security technology in computer software development

A computer's firewall is a security barrier that helps computers isolate unsafe network information. It only allows audited application protocols to enter, largely ensuring that computer networks are protected from harmful information. The computer's firewall can scientifically divide the network functions according to actual needs, such as scientific isolation protection of the network segments that are more important inside the computer network, and reduce the impact of the overall network operation on the operation of the computer. Vulnerability scanning technology, as its name implies, is a self-examination technique that is performed before the computer system is attacked. This technology can clearly show the security vulnerabilities in the computer network system and repair them in time to prevent network attacks. In addition, vulnerability scanning technology can evaluate the security factor of computer systems and firewalls, reducing the incidence of security problems. Information encryption technology essentially re-encodes target information and hides real information. Even if the information is illegally stolen, it will not lead to the leakage of real information. It can effectively improve the security of information systems. At present, information encryption technology is widely used in the field of e-commerce, and it also plays an important role in the security of information.

Intrusion detection technology is a new type of attack prevention technology. It mainly analyzes the system structure of the computer and the characteristics of the network system. Then it collects statistics on the abnormal behaviors in the computer network, and detects the attack activities and provides early warning. Intrusion detection technology shoots multiple fields. It is a combination of statistical technology, communication technology, artificial intelligence, and reasoning technology. It accurately monitors the attack behavior of computer network systems, reduces computer network attacks as much as possible, and reduces user losses. Monitoring behavior can be divided into host, network, and hybrid intrusion detection technologies according to different monitoring objects. The intrusion detection technology for the host is mainly to comprehensively check the data of the computer operating system to protect the security of the host; the network-based intrusion detection technology mainly aims to protect the security of the entire network by monitoring and analyzing the network data circulation; hybrid intrusion technology The scope of protection is more comprehensive and comprehensive, combining the advantages of host and network intrusion detection technology, making the protection effect more significant.

Computer anti-virus technology is mainly to do a good job of virus prevention, virus inspection, and virus elimination to protect computer system security. Preventing viruses is to install virus protection software on the computer, which fundamentally reduces the possibility of virus intrusion, such as system monitoring. There are two main types of virus inspection procedures, one is based on the characteristics of virus transmission, and the other is analysis. The computer's operational data, and the results are saved, the accumulated data is compared with the existing data to determine the virus infection results. Destroy the virus by using anti-virus software to operate, but the virus will be updated, using anti-virus software can not completely kill the virus. This requires timely upgrade of anti-virus software to improve the anti-virus capabilities of the software. In addition, computer software is tracked by criminals using tracking technology, stealing internal computer information, destroying confidential files, and causing serious damage to users. This requires anti-tracking technology to carry out the tracking and interception. The anti-tracking technology uses the assembly tool to monitor the computer software in real time to prevent the software operation from being tracked and improve the security of the system.

5. Conclusion

The development prospects of the information age are very broad. Therefore, it is necessary to comply with the development of the times, increase the development of computer software, and solve people's needs. However, the security of computer software development seriously restricts the development of computer software technology. This requires strengthening computer security technology and improving the security, reliability and practicability of software development.

6. Acknowledgement

References

[1] Yang Shuguang(2015). Application Research of Computer Software Development Technology. Communication World, no.06, pp.12-19.

[2] Xiang Sihao(2015). Application and Research of Computer Software Development Technology. China New Communication , no.09, pp.68-72.

[3] Guo Qing, Huang Yong(2015). Development and application of computer software based on information security environment analysis. Communication World, no.19, pp.123-130.