Application Analysis of Security Technology in Computer Software Development

Sirui Lyu *, Haiyang Guo, Kairui Zhang

Faculty of Engineering and Applied Science, Queen's University, Kingston, Ontario

* Corresponding Author Email: 17sl76@queensu.ca

Abstract. At present, citizens benefit from the facilities provided by information network technology in all aspects of daily life. However, the particularity of the computer network environment also causes many unfavorable factors in the application of network technology. If these negative factors are not restricted, they will have a direct impact on the development of information technology industry. Therefore, creating a good business environment for this network has become a key issue in the field of computer software development. Facts have proved that computer security not only affects the economic development of enterprises, but also affects the security of information provided to users. In order to cope with these shortcomings, designers have developed many computer security tools to solve the problems of computer network operation caused by security risks.

Keywords: Computer; Software development; Security technology; app; application.

1. Introduction

Computer software can help improve the efficiency of users' work and study, mainly including two kinds of system software and application software. System software includes Windows, DOS, Unix, Linux, etc. Its main function is to coordinate the operation of the computer and control the hardware equipment of the computer. The purpose of developing application software is to improve the work or study efficiency of users such as QQ and Office[1]. Whether it is system software or application software, developers must follow the following steps in the development process. First, developers must analyze the feasibility of the software to determine whether the software has been developed; Secondly, developers must analyze the functional requirements of the software in order to gradually optimize the structure and function of the software; Software developers must design the overall function and architecture of the software in detail again, and design and develop the front and back of the software; Finally, once the developers have completed the development of the software system, researchers must also conduct a comprehensive and functional test of the software to avoid errors that may affect users' work and study. In the process of developing large-scale software, it is difficult to develop because of its rich functions. Although the efficiency and quality of software development in China have been improved with the development of information technology, there are still problems in the lack of cooperation between developers and users and the lack of basic technology. The above problems not only hinder the realization of some functions of the software, but also affect the compatibility and stability of the software. Last but not least, the lack of basic technology may also lead to some risky security software, which will also have an impact on the security of user information.

2. Computer software development in the security risks

2.1. Their own vulnerabilities

The security risks caused by software defects are the most common in software development. Software defects are caused by various reasons, such as the negligence of developers or the limitation of programming language. For example, software written in C language often has some defects. In order to improve the security of users' private information, software developers must upload corresponding files regularly so that users can fix existing vulnerabilities. The appearance of software

vulnerabilities will not only be exploited by criminals, but also steal all kinds of private information of users, causing financial and property losses to users to a certain extent, and will also lead to the collapse of software during operation.[2]

2.2. Information management

As you know, in the process of software development, software development engineers and software development engineers not only have to create many programming files, but also write related instruction files. The disclosure of these documents will not only affect the security and stability of the software system during its operation, but also bring great financial losses to software development companies because of the loss of software copyright. In order to avoid this problem, many software companies have developed information management systems and solutions to manage data and explanatory documents reasonably. Generally, information management methods can be roughly divided into two categories: offline management and online management. Offline management means that software development companies store personal information on offline devices during software development to prevent illegal elements in the network from obtaining important information. Online management means that software development companies store important information in their software development on network devices. Although this information management method can make it easier for software developers and designers to access data, it also poses a threat to the security of related information. For example, many software development companies have created their own private data storage network (NAS), in which important data can be stored. Although part of the NAS private cloud, criminals can invade the private sector and use various networks to transmit data.

2.3. Hacker or virus attack

In the process of computer software development, there are also security risks of hackers or virus attacks. First of all, viruses are parasitic, and virus programs can be parasitic in a program. If the program is not running, the virus program will be hidden and cannot be detected. When the program is running, the virus program will cause some damage to the user's system; Secondly, virus programs are contagious and can be copied or mutated constantly in the user's system, thus infecting a large number of files and programs; Finally, virus software is also destructive, no matter what the type of virus software is, it will cause damage to the user's system or files. For various interests, hackers often use virus software and system vulnerabilities to attack various types of software to obtain important data.

3. Analysis of the application of security technology in software development

3.1. Firewall and information encryption technology

Firewall technology is a relatively traditional computer security technology, but it is an important security technology that can effectively isolate malicious attacks. Its essence is a traffic protection barrier installed between the internal network and the external network. This technology can completely isolate or hide unsafe network information during use, and build a safe and stable environment for the whole computer operating network. In all aspects of computer software application, all access and transmission information in the internal network must be continuously detected by the firewall, and access is allowed only after the detection meets the standards[3]. To some extent, the firewall has the ability to effectively avoid and block Trojan virus, illegal elements, malicious programs and other internal network access behaviors, and can effectively provide a high-quality and safe environment for computer software development projects.

3.2. Intrusion detection technology

At present, the traditional computer security technology can no longer guarantee the security of all kinds of information and data in the process of software program development. It is necessary to apply more advanced intrusion detection technology to effectively expand the scope of protection and improve the protection effect in an all-round way. As a new computer security technology, intrusion detection technology combines statistics technology, communication technology and virus reasoning technology. In the process of spreading network information data, relevant technicians can analyze the structural characteristics of computer systems including network systems. By analyzing abnormal unauthorized access and attacks, we can send out further alarms, clear the access attack route, and effectively protect the overall security of the computer system. Applying intrusion detection technology in the development process can not only effectively prevent unauthorized attacks from invading, but also reduce the loss of the target computer. Different from the firewall technology analyzed above, intrusion detection technology has stronger detectability, and can defend and clear criminals before they try to attack, so as to prevent potential problems before they happen.

3.3. Vulnerability scanning and repair technology

Vulnerability scanning technology is a comprehensive detection technology for itself, and the process of detection and scanning is before the computer system is violently attacked. Compared with firewall technology and information encryption technology, vulnerability scanning technology has more prominent autonomy and early warning, so it has a wider range of applications.[4] The use of vulnerability scanning technology can achieve the purpose of preventing potential problems in the process of computer development, and at the same time effectively reduce the probability of security risks and problems, thus ensuring the legitimate rights and interests of users and companies. The security of computer network technology has improved the overall level of social benefits.

3.4. Security authentication and identification technology

In the process of computer development, security authentication and identification technology is a relatively advanced and cutting-edge network security technology. Security authentication technology enables software engineering developers to further upgrade and convert computer software programs by using modular planning and design mode, effectively ensuring that computer network systems are always in a relatively safe and stable operating state.[5] The related programs of this mode are usually composed of hardware drivers, software operating systems and network security monitoring systems. Among them, the hardware driver usually monitors the working state of the computer's external devices in the whole process, so as to transmit relevant data information to the internal software application. Software operating systems are usually composed of hardware devices and system terminal interfaces, which not only use other types of security technologies, but also support most mainstream interfaces, storage devices and other external devices.

4. Conclusions

In short, with the continuous development of network information technology and computer technology, security, confidentiality and privacy are issues that users generally attach importance to. Therefore, in the process of developing computer software programs, relevant technology developers must apply important security technologies. On the one hand, from the perspective of software development and user use, comprehensively grasp the general security risks and system failures, and take preventive measures; On the other hand, it is necessary to master security technologies such as firewall and information encryption technology, intrusion detection technology, anti-virus technology, vulnerability scanning and repair technology, security authentication and identification technology, and effectively solve computer security-related problems.

References

[1] Analysis of user experience in computer software development [J]. Wang Yuxian. Software Engineer, 2013(10)

[2] Analysis of computer software development and application and its future development trend [J]. Yao Dan. Information System Engineering, 2018(05)

[3] The application practice of active defense technology in computer software development [J]. Zeng Junyi. Intelligent Computers and Applications, 2020(05)

[4] The application of layered technology in computer software development [J]. Zhu Jiangyi. Electronic Technology and Software Engineering, 2016(23)

[5] The application and development trend of computer software development technology in the new period [J]. Zhao Huina; Wang Huifang. Science and Technology Communication, 2017(20)