Security Issues and Technical Support in Computer Software Development

Wei Gong

Chongqing Technology and Business Institute, Chongqing, 400052, China

Keywords: computer; software development; security issues; technical support

Abstract: Nowadays, the application of computers has become more popular, and computer technology has been integrated with many jobs. However, at the same time, we also find that information technology faces more and more serious security risks, so this requires us to discuss how to develop software in a safe information environment. This problem has gradually attracted people's attention.

1. Introduction

With the development of computer networks, computer information security is facing a great threat, and computer security issues become more and more prominent. Many dangers, hiding risks and possible attacks in modern computers have certain concealment and potentiality. They exist in computer technology in a hiding form, which affects the development and application of computer technology. Security technology is an effective technology for computer software development and defense. It can protect against the eavesdropping and intrusion of illegal users, and can effectively prevent the intrusion of malicious software, making computer information more confidential, complete and authentic. Even in a safe information environment, research and exploration on information security management and protection should be strengthened to make the information environment more secure and conducive to the development and utilization of computer software.

2. Security Issues in Computer Software Development

According to the authoritative definition, computer software mainly refers to programs and their documents in computer systems, which are mainly divided into two categories: system software and application software. At present, in addition to scientific research and medical treatment, most people use computers mainly based on application software. Various, full-featured and personalized application software greatly satisfy people's life and learning. However, compared with the physical form of the hardware which can be touched and seen, the software is invisible. The operation of the software on the machine can tell us whether the function is normal. The security of computer software is crucial to the performance of computers. It is an important aspect of data security in computer information systems. Especially in today's e-commerce boom, strengthening the security management of enterprise computers, ensuring the normal and orderly conduct of e-commerce services, and ensuring the security of information and funds is a real problem, which brings a lot of difficulties in design and management of computer software.

Computer software security issues include the security of the software system, and normal and continuous operation of software system. It involves two security principals. From the perspective of the software user, the user needs reliable and secure software with high quality and low price which is easy to operate. From the perspective of software developers, in addition to meeting the security needs of end users, developers must protect the intellectual property rights of software developers to prevent software systems from being copied or tracked by criminals for profit. It can be seen that the security of computer software not only involves the security of the use of software systems, but also the software itself and the rights of software developers. As a product, computer software is a special brain labor achievement and a special resource in computer systems. The security of computer software is related to the security of the entire Internet information system and is an important part of computer security.

Copyright © (2018) Francis Academic Press, UK DOI: 10.25236/dpaic.2018.016

3. The Main Factors to Improve the Security of Computer Software Development

3.1 Information security.

Information is processed data that is stored in a computer. As a tool for information storage and transmission, computers play a big role in the behavior and decision-making of information receivers. The development of modern information technology, especially computer networks, is the manifestation of the gradual commercialization of information. The construction of various information products and information engineering has also gradually revealed information security issues. Information security is a relatively complex and comprehensive system, which refers to the security of computers, related equipment and facilities, information and computer operating environment. This system covers not only computer technology equipment but also the personnel. In order to protect the security of information, it is necessary to consider various factors.

3.2 Information security environment.

The information security environment is a relatively secure environment, which cannot completely eliminate information security incidents. The development of today's social network information technology has made information security involved in the world economy, politics, culture, military and diplomacy. To build a secure information environment, we can only avoid the occurrence of information security incidents, reduce the leakage of information and the occurrence of risks, and minimize the threat of information security. The construction of information security environment is a complex system engineering, which needs to change from concept to design, and conduct design and management to make it a sustainable development process. To build a secure information environment, security management must be strengthened and a scientific security management mechanism must be developed. Security management includes risk management, security education and security strategy. To reduce security risks, security management must be strengthened from these three aspects. In the safety management, we must pay attention to people. People are the key factor of information security and the weakest link. We must strengthen the management of people at all times. To establish a safety management mechanism, it is necessary to strengthen the management of people, follow the principles of multiple-person responsibility system, limited term of office, separation of duties, strengthen the management of information, and ensure the security of the information environment.

4. Security Technical Measures in Computer Software Development

4.1 Management measures.

First of all, we must improve the laws and regulations related to computer security. It mainly includes the "Intellectual Property Protection Law", the "State Secret Law", the "Information Network Security Law", the "Data Protection Law", the "Computer Information System Security Protection Regulations", the "Interim Provisions on the International Network Management of Computer Information Networks", and the "Computer Software Protection Regulations". Secondly, we must do a good job in the popularization and education of computer knowledge, let the public understand the development history, working principles and usage methods of computers, and cultivate the public's legal concept of software copyright and intellectual property rights. Finally, the computer industry should develop appropriate entry barriers and industry technical specifications and standards.

In addition, in order to ensure the security of computer software, there must be institutions and units in charge of the matter at the national level. The developers of computer software must have a strict organization and management process to strictly monitor and manage the links from the development of software and end users. For the unit in charge of the computer, a special software security inspection department and a special group should be set up to combat illegal copy and dynamic tracking of software to engage in corresponding inspection and supervision. For developers, we need to set up a corresponding security assurance group to supervise all aspects of software development and organize safety performance testing and evaluation. For the end user, there is also a corresponding user management system, which limits the copy and porting of the software.

4.2 Encryption measures.

Information encryption technology refers to the use of certain information encryption calculation methods in computer information storage and transmission engineering to turn information plaintext into unreadable ciphertext. To read the information, you must know the method of information decryption, which will prevent illegal intruders from reading confidential information. The process of converting computer plaintext information into unreadable ciphertext is the encryption of information. The process for information readers to convert ciphertext into plaintext is information decryption. The decryption of information requires a corresponding key. It is very difficult to read encrypted information, so information encryption technology is a very effective way to ensure information security.

Information encryption technology is divided into storage encryption technology and transmission encryption technology according to the different purposes of encryption. Storage encryption technology is to prevent the leakage of information in information storage, mainly in the form of ciphertext storage and access control. The ciphertext storage is mainly realized by the conversion of the encryption algorithm, the additional password, and the setting of the encryption module. Access control mainly judges the legality by discriminating users, and mainly tends to review and limit qualifications and permissions. Transmission encryption is the encryption of the information transmission process to prevent leakage and invasion by illegal users during the transmission of information. This encryption mainly includes two forms: line encryption and end-to-end encryption. The former is to set different encryption keys on different lines. This encryption method can effectively prevent information leakage on the information transmission line, but it is easy to ignore the safety of the information source and sink. End-to-end encryption means automatic encryption at the sending end of the information. When the encrypted information is transmitted to the receiving end, it will be automatically reorganized and decrypted, so that the encrypted information becomes readable again.

(1) Secret key. The secret key is an important means of information encryption and the main object of confidentiality and privacy. The secret key is private and non-public. However, because of the large number of keys used in computer information exchange, there are many identical keys. Therefore, once the individual's key is known by a third party, its information with other users is likely to be stolen by the third party, which threatens personal information security. The more times the same key is used, the more likely the information secreted by such a key is leaked. In order to improve the confidentiality of information and prevent illegal theft of information, it is necessary to constantly change the key and reduce the exposure of the key. To ensure the security of key usage, a distribution center can be established on the Internet to provide a secure and reliable key. Each user only knows one key that can talk to the distribution center. This can not only meet the user' needs for information confidentiality, but also reduce the key repetition rate to ensure the security and reliability of the key.

(2) Quantum encryption. Quantum encryption technology is a technical means to judge whether computer information is attacked. This technology can realize the all-optical network of the traditional cryptosystem, and can improve the key exchange and information encryption to the fiber level. Once an illegal intruder wants to detect and accept the information sent by the user, it will affect the quantum state of the user. The user can judge whether the information is attacked according to the change of the quantum state, and take measures in time to avoid more losses.

5. Summary

With the rapid development of information technology, the development of electronic payment, online office and other technology has made information security the most concerned part of people's production and life. The development and utilization of computer software is more important in the future. It will provide impetus for development in the coming period and will also ensure the improvement of computer technology. But we should also know the importance of computer security. Only by ensuring the security of computer equipment and software systems can people's lives and work be facilitated.

References

[1] Wang Huabing. *Design and Development of Computer Network System Based on Network Data* [J]. *Electronic Design Engineering*, 2017, 25(17): 185-190.

[2] Zhang Xiao, Li Zhi and Zhao Ziyan. *Research and Implementation of Problem-oriented Software Development Collaborative Modeling Tools* [J]. *Computer Science*, 2018, 45 (9): 119-122, 134.

[3] Li Zhaobin, Li Weilong and Wei Zhanqi. *Research and Implementation of Key Modules of SDN Data Security Processing Mechanism* [J]. *Computer Applications*, 2018, 38 (7): 1929-1935.

[4] Wang Jimei, Jin Lianfu. *Research and Solution of Web Service Security Problem* [J]. *Computer Applications and Software*, 2004, 21(2): 91-93.

[5] Liu Qiang, Fei Lili and Wang Jian. *Disadvantages of Computer Network System and Suggestions of Security Software Development* [J]. *Information Technology and Informatization*, 2014, (5): 146-147.