Research on computer software security problems and countermeasures in the new era

Chen Nuo
Grade 19, School of Computer and Software, Nanjing University of Information Engineering, Nanjing 210044, Jiangsu

Absrtact: With the development of computer and network technology, the security of computer system is threatened, which also puts forward higher requirements for the security of computer software. In order to improve the overall security of the computer system, technicians should focus on computer software security, conduct in-depth research on software security upgrades, electronic encryption and other technologies, and provide effective protection for computer system security. Based on this, the article analyzes and studies the security problems and countermeasures of computer software in the new era, expounds the background of computer software security research, explores the security vulnerabilities of computer software, analyzes the security problems of computer software, and puts forward practical measures for computer software security for reference.

Keywords: computer; Software security; Security upgrade

Introduction

To ensure the normal operation of the computer, the technical staff should put the security of the computer software first, which is also the requirement of the software users. However, how to ensure the normal operation of software and effectively use computer software has become the most important content of social development. Although the economy continues to develop and science and technology are also progressing, there are still some problems in computer software security in China. Only by solving the problems in a targeted way can we play a better role.

1. Research background of computer software security

Computer software refers to the general name of relevant programs and documents during system operation. In a computer, a program should be set with a certain code before it can be started. In addition, software documentation is a convenient software for users, which helps them understand relevant programs. Computer software is generally divided into system software and application software. System software mainly includes Windows, UNIX, etc. Application software is small software developed to complete tasks. Computing application software includes social software, game software, office software and management software. With the cross era development of computers, computers will be applied in all fields. However, due to the imperfect system construction, the security of computers has not been guaranteed, and the vast majority of people do not pay attention to the security of software, which leads to frequent software security accidents. At present, computer security problems mainly include quality problems, illegal copy and attack problems. There are still some security vulnerabilities in software design, which are vulnerable to hackers' attacks, thus causing failures. The development of computer software requires a lot of energy. In order to obtain economic benefits more quickly, some criminals can copy the code and program of stolen software, which brings more hidden dangers to computers. Computer software is prone to multiple vulnerabilities during system design. The virtual software characteristics of the system make it impossible for network supervision to obtain effective information at the first time, so hackers can not be found in time, which affects the effective use of computer software.

Compared with hardware, software is more vulnerable to security threats. In this regard, the technical staff has brought convenience to more enterprise employees through the development and application of various office software. At the same time, the software of game entertainment developed by technicians has enriched people's lives and brought more fun to people's lives. But at the same time, the software information will be easily stolen and tampered, and the computer system will also be vulnerable to virus attacks and lead to paralysis, which is not conducive to the security of property production. Computer software should meet the needs of users to ensure its security and stability.

2. Research on computer software security vulnerabilities

2.1 Common types of software security vulnerabilities

All computer systems have security weaknesses. Under the background of the new computer age, software security problems are more serious. The weak points of computer network security provide convenience for hackers. Due to the huge amount of information at this stage, the widespread use of low-level languages will aggravate the existence of weaknesses, leading to the introduction of malicious code.

The vulnerabilities of software security itself mainly include the following points: First, overflow in the buffer area will cause more security problems, which is due to the use of insecure programming languages, resulting in the phenomenon of access overruns. At present, the buffer generally has a fixed value. The programmer should consider whether the data conforms to the capacity when analyzing the computer storage. Secondly, stack destruction is the final result of buffer overflow attacks. Some attackers will carefully construct data, change the process of program control, and execute data. Thirdly, among the computer software security problems, the competitive condition is a common software bug, which is generally difficult to solve. It is relatively rare and has great uncertainty. The problem of file competition conditions is difficult to solve. Before using a file, the overall attributes of the file are generally checked and its defects are analyzed. Finally, the format string vulnerability is a kind of program code defect. Now many software products have these vulnerabilities, in which the specified data can be written in memory, and the data can be analyzed to change the program execution process. Software security vulnerability is one of the important aspects. The attacker uses the same browser as the victim and sets the ID to intercept the target data, so that random seeds can be obtained in a short time to crack the password.

2.2 Prevention of software security vulnerabilities

In order to prevent buffer overflow from threatening computer programs, technicians should conduct an overall analysis of the risk factors and use the security version to prevent software security vulnerabilities. Wangwang will have a system bug in the computer software, and no buffer overflow is found in the program source code inspection. This requires technicians to do a good job in program operation, and use the non executable stack in the LINUX operating system, so that the patch has never played a good role in protecting the buffer overflow.

To prevent the competitive condition vulnerability, you can operate the code, lock the code, prevent TOCTOU and avoid directly applying the file name, so as to protect the security of the file and ensure that the file will not be changed. In computer operation, the functions of the lowest file system of the operating system should be effectively processed to avoid the use of access and other functions. To prevent format string vulnerabilities, format constants should be used directly to prevent multiple vulnerabilities. The function that generates the format string vulnerability will not check the type and number of parameters. During the use of the function, ensure that the number of parameters matches the type to prevent the vulnerability. Using windows to output data under Windows can also help avoid vulnerabilities. Random data vulnerabilities should use a good random number generator to provide a safe random number stream, so that attackers can understand the details of the algorithm and guess the relevant information of the data stream.

3. Computer software security issues

3.1 Software is attacked

Computer virus. The environment of computer operation is complex, and many factors will affect the security of software. Among them, the most common security problem is the direct invasion of computer viruses, which can quickly spread computer viruses in a short period of time, and can tamper with software programs in the system through autonomous replication and dissemination of viruses, and call data and personal information. It is easy to disclose personal privacy information, which is destructive. However, when encountering attack problems, the vast majority of users are difficult to find viruses, even if there are problems, it is also difficult to remove them.

Hacker intrusion. Due to technical limitations, there will be weaknesses in the development of computer systems. Hackers will often regard such vulnerabilities as the target of attack, so as to attack with weak points, obtain business secrets as quickly as possible, and obtain business information about individuals and enterprises. At this stage, the computer security monitoring system in China is not perfect, there are many hacker attacks, and the network has a strong virtual nature, which can not be scientifically and effectively prevented, which also increases the security risks of computer software.

Software cracking. The development of computer software has certain difficulties, which requires high capital investment. Among them, some criminals will specially crack the source code files in the software, track and monitor the software, analyze the user's operating habits, crack the files in the computer software, crack the computer software problems, and seek personal gains from them. This destructive behavior infringes the interests of software developers and does not respect intellectual property rights, resulting in a great degree of security problems.

Information theft. Some criminals steal personal information from individual users and bring information security problems to users. In recent years, global information security problems have occurred frequently, and individual rights and interests cannot be guaranteed. The harm brought by information eavesdropping is also great.

3.2 The user’s awareness is not strong

Computer users often lack security awareness in computer applications. In this regard, users should constantly enhance their security awareness. If the operating computer lacks security awareness, it is easy to have computer failures. Especially in application software, many users lack security awareness. In order to meet their own needs, they install a large number of unknown source software, which has many viruses and trojans. If users have operational problems, they will bring more opportunities to hackers, thus causing more security risks to the software.

3.3 Network security problems occur

Under the background of computer network, the network factors in the computer software security problems are more obvious, and the software network security problems will be affected by viruses and trojans. The vulnerability of software network security mainly includes the following aspects: First, it destroys the computer system. Some computer viruses are easy to cause destructive effects on computer systems during operation, which mainly include computer hardware systems and computer software systems. Secondly, the loss of data and materials. The loss of computer customer information and data is also a basic problem of software security. The reasons for the loss of customer information are closely related to security issues such as computer trojans.

4. Research on practical measures of computer software security

With the continuous upgrading of computer security technology, technicians should improve software security management and improve the construction of management mechanism. To ensure the normal operation of the computer, the technical staff should put the security of the computer software in the first place, which is also the basic requirement of the software users. However, how to ensure the normal operation of software and effectively use computer software has become the most important content of social development. Although the economy continues to develop and science and technology are also progressing, there are still some problems in computer software security in China. Only by solving the problems in a targeted way can we play a better role.

4.1 Use security software with higher security level

In the use of security software, the security level determines the computer's ability to resist viruses. Because of this, in order to improve the performance of computer security, the software with the highest security level should be effectively applied. In computer systems, security software mainly includes anti-virus software, system tools and anti rogue software. In this regard, technicians need to adjust the security level of the software, which generally needs to be determined by a professional software testing organization. At the same time, users also need to pay attention to the following aspects during the use of security software. First of all, avoid repeatedly installing different brands of security software in the computer, which is likely to cause the problem of software killing by mistake, thus causing the computer system to be sluggish. Secondly, regularly upgrade the virus database of security software to determine its virus detection capability. Finally, security software deals with viruses found at this stage. Computer customers should improve their security awareness and not log in to software of unknown origin, so as to ensure that computers are in a safe state.

4.2 Add security test in software trial

In the link of computer software design and development, adding software security performance test will help improve software security, thereby reducing security problems in software. Software security testing mainly includes the following aspects: First, compatibility testing, that is, compatibility testing of software and system hardware to test the problems. The second is to find loopholes, find the loopholes in the software by using the exclusion method, and repair the loopholes at the first time. Third, we should do a good job in security research. In the software trial phase, we should investigate the experience of the trial users, so as to find loopholes and properly handle them. Fourth, develop security testing. Recruit professional testers in the society to better solve security problems.

The level of computer software development is closely related to its security. In this regard, when designing software, software developers should take corresponding technical measures to solve problems in combination with the development needs of users and their usage habits. During the code writing, the actual characteristics of the industry code should be combined to complete the writing, make comments on the code, and analyze the test software to find out the security vulnerabilities. In the source code, software developers need to do a good job in encryption, improve the rain proof performance of the software itself, and carry out analysis and research in combination with the actual situation.

4.3 Upgrade for software security issues

In the process of using the software, new security problems occur frequently, and the changes and upgrades of Trojan viruses will affect the security of the software. In this regard, technicians should do a good job in software development and upgrading, and carry out professional upgrading services for security problems, so as to better solve problems. This type of upgrade service mainly includes the following centralized types: first, software version upgrade. During software development, version upgrade is the most critical content. During the version upgrade, new security technologies should be used to deal with problems, so as to better improve the security of the software. The second is targeted upgrading. This is when security problems have occurred in the software, and the software package is used to repair the newly discovered vulnerabilities and new trojans.

4.4 Strengthen the management of computer software protection measures

In the computer application link, the optimization of software encryption technology will help to better improve the security of software. In the network operation, encryption technology helps to better improve the security of software information. In the actual software security processing work, encryption technology generally includes electronic authentication technology and secret key technology. The application of secret key technology can complete the decryption faster, but it has certain difficulties. Electronic authentication technology is to use information electronic means to verify identity by sending documents. It includes relatively many technical means, including passwords, electronic signatures and other types.

5. Conclusion

To sum up, computer software security is the premise to ensure the normal use of computers. Computer software security management is a complex project, and software will inevitably have certain security vulnerabilities. Only by reducing security risks and effectively preventing the use of software, can the safe use of computers be improved as much as possible. Software security is an important component of the overall security of the computer system. Computer enterprises should pay attention to software development, pay attention to the key significance of software development, and use certain practical technical measures to solve problems, so as to better improve the security of the computer system.

References:

[1] Cao Shuhuai, Huang Chongzheng. Discussion on Computer Software Engineering Security Problems and Countermeasures [J]. Science and Technology Innovation Guide, 2019, 16 (30): 105-106

[2] Dong Bing. A Brief Talk on Computer Software Security Problems and Protection Countermeasures [J]. Computer Products and Circulation, 2018 (12): 15

[3] Meng Lanru, Shi Junru. Problems in Computer Software Security Detection and Countermeasures [J]. Information Recording Materials, 2021,22 (07): 72-74

[4] Li Zhengdi, Peng Wenxue, Ruan Xuan, Sun Xinjie. Analysis of the Defense Measures for Computer Software Security Problems [J]. Computer Knowledge and Technology, 2021,17 (08): 77-78

[5] Lu Na. Research on Computer Software Security Detection under Multi platform and Detection Implementation Method [J]. Computer Products and Circulation, 2020 (07): 23