Research on Measures for Computer Application System Security Technology Strengthening

Guihua Xi

School of Computer Engineering Jingchu University of Technology, Jingmen Hubei, 448000, China

Keywords: Computer, System security technology, Strengthening measures.

Abstract. With the continuous development of science and technology, in particular of information technology, network information technology is applied in daily production and life more and more widely, and people attach more and more importance to the security of computer application. The operating mode and constructing environment of computer application system are complex, which is demanding for security assurance of computer application system. As network information technology develops rapidly, system security technology should be further applied and developed, to lay a foundation for computer application system security technology.

Introduction

The rapid development of science and technology, in particular of network information technology, promoted the progress of computer security technology. Presently, the information industry is an important pillar in economy. As the informatization level continuously rises, people bother about information security problems while enjoying the convenience brought by informatization. Information security problems will interfere and even hinder information exchange, and damage sustainable development information. Thus, how to safeguard computer network information security and information system security with system security technology is a key problem in future development process.

Overview of Computer System Security Technology

Presently, all walks of life are concerned about computer information security, because computer information security is closely linked to enterprises' economic benefits and information security. Computer has become indispensable for people's daily life. Thus, the security of computer system becomes of great importance. Only the security of computer system is guaranteed, a safe network environment and information data can be ensured. The security of computer system will be affected by various factors, and then encountered with hidden dangers , which will hinder the progress and development of computer networking technology. With the continuous development of networked technology and information technology, people attach more and more importance to computer privacy and security. Computer system can store a large amount of information and data. If a safe network environment cannot be guaranteed, the computer system security may be threatened and damaged. From the angle of computer system security, computer system application security technology is of great importance, with which the security of computer system at all levels can be guaranteed, and the overall efficiency of computer system can be raised. If no security technology is provided, the security of operation of computer system cannot be guaranteed.

Importance of Computer Application System Security Technology

Any security incident occurring in the operational process of computer system may affect the whole computer network. In actual application of computer system, security incidents usually are caused by the following factors. First, external network may affect and threaten computer system, such as illegal monitoring, information alteration, interception, or removal, or hacker attack, etc. Second, security incidents may be caused by misuse or deliberately sabotage of computer system. The

main purpose of applying security technology to computer system is to guarantee safe and stable operation of computer system. Generally, computer systems are developed based on a uniform standard. Then, rational measures should be taken to guarantee the integrity, non-repudiation, authentication, denial of service, confidentiality, etc., and stable and effective computer operation, without risk or security vulnerability. The security threats of computer system mainly come from: confidential information interception (user identity information, bank card information, and telephone number, etc.) via phishing website (such as fake ticketing website), computer system attack or system information alteration or falsification by means of virus epidemic, computer system collapse due to hacker attack, and internal information interception and even computer system damage via computer information security system. Therefore, rational and scientific security technology should be selected based on particular situations to prevent security incidents[1].

Measures for Strengthening Computer Application System Security Technology

Access Control Technology.

Access control technology refers to verifying legitimate access by checking the username and password and timely inspecting the default limits of user account to guarantee safe access to network. The key for a user to access to network, actually, rests in user password. If no password or a simple password is set, the user password appears vulnerable. Thus, it is recommended to set a password consisting of letter, digit and character, etc., and encrypt the password by means of public key or one-way function, etc., so that repeated failure to input a right password will be automatically considered by the system as illegal invasion, and the system will automatically lock the account for the time being after warning error. Besides, in the case that a computer network system contains different information contents, different access right setting according to particular needs of users is feasible. Specifically, users, by access right, can be divided into: audit user, general user, administrator, etc.. Administrator mainly acts to monitor the overall network, and other users can access to specific contents within their scope of access.

Encryption.

Encryption is an important technology for preventing confidential information stored in computer system from leaking or alteration. Once system data is encrypted, a key ciphertext known by user only will be formed. The rationale of decryption and encryption of computer system is that user sets plaintext password, and the computer converts the encrypted information into ciphertext, decrypts the ciphertext in a certain way at the time of ciphertext transmission, forms a plaintext password instruction. In this way, the password inputer can know the cryptographical message by himself. If encryption is applied to computer system, hidden dangers of illegally cracking password should be analyzed, such as virus, hacker, etc. There are two main measures for preventing such hidden dangers, i.e. asymmetric secret key encryption and symmetric secret key encryption. Symmetric secret key encryption, actually, is to send cryptographical message in a plaintext way, form ciphertext information, decrypt the message by inputting the plaintext password, and transmit decryption key and encryption key via a public secure channel. Symmetric secret key encryption includes a 64-bit key, and 64-bit data block occurs in actual operation. That is, 16 rounds of conversion and replacement processing 64-bit data block in advance are required for data encryption each time. In that case, 64-bit ciphertext data will be formed to process 8-bit data for odd-even check, and other data indicate the length of password. Asymmetric secret key encryption, actually, is to that after encrypted module is set in a plaintext way and ciphertext is transmitted via channel, the recipient can obtain the ciphertext decryption module. That is, user can obtain information. Asymmetric secret key encryption is performed by three steps, i.e. secret key formation, encryption, decryption[2].

Firewall Technology.

Firewall technology is mainly applied to enhance the overall network security, with which internal network information interception prevention, network access control strengthening and network equipment damage prevention can be realized. In actual analysis procedure, it is firewall that controls

internal and external network access, mainly including host, router and other networks, etc. Computer firewall technology is of certain influence and subject to limitations. Thus, it is recommended to combine encryption, accessing technology and firewall technology together. In actual operation, firewall system mainly has four structures. First, packet filter firewall. The key linking internal network to external network is filtering router. Router is capable of examining external data network packet, helping to guarantee a safe environment for computer operation to a certain extent. This kind of firewall structure can be rationally installed in computer system that is without given software or not operates given application program, suitable for small simple network like home network. Second, dual-homed host firewall. This type mainly links internal network to external network via a network controlled by dual-homed host and with safe network interface and proxy server. In this way, the protected network will be completely isolated from external network environment, and the IP address of internal network become unavailable in external network. Third, screened host gateway firewall. This type rationally links internal network to external network via filtering router, and rationally sets the bastion host in external network, which will be subject to simple filtering rules. In this case, the security of the bastion host is required to be strengthened continuously. Fourth, screened subnet firewall. This type is mainly used to screen subarea from appearing between internal network and external network. Besides, it requires two filters for linking internal network to external network and that the information server and the bastion host be rationally set in system, so that safe internal and external subnet can be formed to effectively reduce the degree of any damage to internal network[3].

Database Security Technology.

Database is mainly used to store data information. Database security technology refers to that only legitimate user can operate the database, such as managing, sharing, using or saving information, which can prevent data information error, dropout or confidentinosity, etc. To guarantee the security of database, it is required to control the database system. That is, the operating system can run only after accessing to DBNS, mainly including preventing illegally system use, user authorization, and maintaining normal statistical database information, etc. The basic function of database is sharing data resources. In the process of sharing data resources, it is required to rationally apply encryption. If the database administrator wants to access or control the network, access monitoring and follow-up examination shall be subject to, and the sensitive database password should be changed timely.

Intrusion Detection Technology.

With intrusion detection technology, the problems and defects of firewall technology can be overcome. Thus, intrusion detection technology is usually applied as supplement to firewall, to enhance the security of computer operation. Essentially, intrusion detection technology is to monitor the process of data transmission of computer system in real time, which is a security protection technology. Intrusion detection technology mainly consists of response unit, event generator, event database, and event analyzer. Event generator acts to monitor the overall computer system and timely report suspicious events. If any file similar to virus that is required to be reported and analyzed occurs during data information transmission, the event analyzer can timely analyze the suspicious events, to determine the actual nature of the data information. If it is still unable to determine the suspicious events, the response unit accepts the reported data, timely give feedback, and stops data information transmission before virus and data analysis, so as to completely isolate the suspicious file(s) from others. In actual operation, there are many methods of reporting suspicious events. Event database is essentially a position for storing data information. Relative to firewall technology, intrusion detection technology is superior, because it can determine whether the firewall technology is capable of accurately analyzing and judging dangers or not. Intrusion detection technology is an active technology of identifying security threats, while firewall technology is a passive technology of receiving security threats and dangers. With intrusion detection technology, hidden dangers that may affect the computer system or actions that violate the computer system can be timely identified, and rational solutions can be put forward. Thus, intrusion detection technology is a supplement to firewall technology. For security of computer, it is recommended to combine intrusion detection technology and firewall technology[4].

Strengthen the Management over Computer Operator.

To guarantee the overall security of computer application system, not only advanced security technologies should be used, but the professional competence and technical merit of the management also should be continuously improved. Most computer network security problems are caused by misaction of computer operator. Thus, to eliminate computer network information security problems, regular training should be provided to computer operators, to ensure the operators to know better about network security technology, and become more proficient in handling hidden dangers, to minimize unnecessary losses. Besides, the personnel management system also should be further perfected, specifying the responsibilities and obligations of operators, and showing the role and importance of computer system application security technology. At last, a defense system is also required, in which security technologies are rationally planned, the advantages and disadvantages are detailed, and the security level of technologies is identified. In this way, effective solutions can be put forward[5].

Conclusion

To sum up, with the continuous development of science and technology, in particular of information technology and network technology, computer becomes indispensable to people's life, and people attach more and more importance to network information security and computer system security. For this reason, it is needed to further develop computer system security technology to guarantee a sustainable development trend of computer system security technology. In this paper, some application system security technologies were covered, including encryption, access control technology, firewall technology, intrusion detection technology, and database security technology. It was also suggested that the changefulness and complexity of environment should be considered, pointing a new direction for further researching computer information system security technology.

References

[1] Cui Xining, Shen Yulong, Li Yahui, et al. Research Progress of Integrated Avionics System Security Technology,*2012 Proceedings of China National Computer Congress*.2012:1-1.

[2] Wu Jinzhou. Application Research of Computer Information System Security Technology, *Super Science*,2015(21):246-247.

[3] Cai Liyan. Discussions on Electric Power Automation System Security Technology, *Super Science*,2013(33):195-195,196.

[4] Chai Jigui. Research and Application of Computer Information System Security Technology, *Value Engineering*,2012,31(3):160.

[5] Gao Jianpei. Analysis of Application of Computer Information System Security Technology from the Perspective of Network Security, *Network Security Technology & Application*,2015(6):71,73.