Type and Security Analysis of Computer Network Operating System Based on Improved Data Structure

Zhang Lijun

School of Software and Applied Science and Technology, Zhengzhou University, 450000

Keywords: Improving data structure; Computer; Network; Operating system; Security.

Abstract: With the large-scale application of computer network, the current computer network and information security has become a major issue facing the state and enterprises and institutions. Under such a huge network system, it is imperative to standardize and organize the application of computer network operating system, as well as further adjustments in technology. To improve the quality of contemporary netizen and the great progress and development of computers in an all-round way. In a general computer operating system, basically, some tool software is provided according to the specific needs of the user to facilitate their operation, monitor, limit or change the data flow across the firewall, and improve the data structure as much as possible to the outside. The network shields the information and structure of the protected network to achieve security protection for the network. Network security is the basic guarantee for making full use of network resources. Therefore, analysing various security risks in the network is very important to ensure network smoothness and information security.

1. Introduction

With the rapid development of computer technology, information network has become an important guarantee for social development. The computer network is also being constructed and improved day by day. This development brings great convenience to the society and realizes the sharing of resources. To a certain extent, it greatly improves the efficiency of people's work, and thus, to a certain extent, it also improves the modernization level of major enterprises. The openness, sharing and internationality of the Internet pose great challenges to the security of computer network applications. Therefore, in the process of network applications, attention should be paid to network threats from various aspects, including physical transmission line attacks, communication protocol attacks and real-time attacks of hardware and software vulnerabilities. Network security means that the hardware, software and data in the network system are protected, and hidden programs are hidden in every link of the computer usage process. They may be invaded by Trojan horse programs or malicious viruses when downloading, running and sending e-mails. To the users of the system, information and data are stolen, information system collapse or paralysis and other losses. It is destroyed, altered, and leaked without accident or malicious reasons. The system runs continuously and reliably, and the network service is not interrupted. Nowadays, the more and more popular Internet knowledge has created huge obstacles to information protection. How to protect the information security while the computer network is developing continuously becomes a major problem in the development of computer networks.

Physical security refers to the physical protection of various computer devices and related devices in the network system, avoiding damage and loss, etc. Logical security includes information integrity, confidentiality and availability. Computer network is a double-edged sword, which needs to be utilized and grasped reasonably. With the continuous development of information technology, hacker technology is ubiquitous, they can easily use the computer network for information acquisition and disclosure at will, and it is difficult to find specific personnel responsible for this. For the specific operation of computer network operating system, staff and technicians must distinguish its different types clearly in order to facilitate the sustainable development of computer network. To ensure the normal operation of the computer network, the computer network operating system can be called the heart of the computer. The computer network operating system can realize

the normal operation of the computer, and can manage the network resources scientifically and share information. The specifications of the specifications, but also to ensure that its physical environment is appropriate. A secure network environment needs to increase the detection of information on the network access port to detect and process bad information in a timely manner. The so-called access control list refers to the setting of the access source, which can effectively prevent bad visitors, so that the internal data of the enterprise can be protected to a certain extent. The technical basis for improving the data structure is information fusion technology based on knowledge and redundant reasoning methods, and most of the work is to classify the data through pattern matching, data mining, feature selection and machine learning.

2. Materials and Methods

Improving data structure is a logical structure, which provides a security mode for a set of software or system. Specifically, improving the data structure provides a series of rules. The computer operating system can help users to deal with tedious work content, manage files scientifically, facilitate operators to use and select files, and help system users understand the actual situation of the computer. Regular computer testing and management system memory, so as to ensure the efficient and normal work of the computer. At the same time, if the computer network operating system is not properly managed and maintained, the computer network information security problem will be aggravated. Therefore, this is also a strict requirement for the specific managers of computer network information system. Once they find that there are loopholes in the computer network system, they need to analyze and understand the specific problems pertinently. Use the network backup server to implement backup of different host data in the LAN to ensure that backup resources can be called up in time when there is a problem in the local network. A secure access list device is implemented at the core of the computer. In this way, the security protection capability of the computer network can be improved to a certain extent.

Intrusion detection can protect the network system inside the computer to a certain extent. It can detect the hidden dangers in the first time and stop them in time. Efficient anti-virus system has the functions of virus scanning and cleaning, monitoring and identification, and automatic upgrade. Some can also retrieve data and detect local or remote computer vulnerabilities through periodic vulnerability scanning of the system. Ensure that the system entity has a safe physical environment. Safe environment refers to the computer room and its facilities. It mainly includes the environment conditions of computer system, including temperature, humidity, air cleanliness, corrosiveness, pests, vibration and impact, Electrical disturbance and so on. There must be specific requirements and strict standards. Email and web server anti-virus, as well as network client anti-virus and more. The operation of these anti-virus measures can further purify the computer network operating system and improve the overall safety factor of the computer network operating system. Improve the integrity check and two-way authentication before calling between the data structure modules to ensure that the module has not been modified. And after the module is loaded into the memory, the module needs to check the side to ensure that it has not been modified during the loading process. The improved data structure parameters are shown in Table 1 and Figure 1.

Table 1 Improving data structure parameters.

	Modular	Dynamic
Self-integrity testing	11.32	9.14
Two-way authentication analysis	9.05	8.22

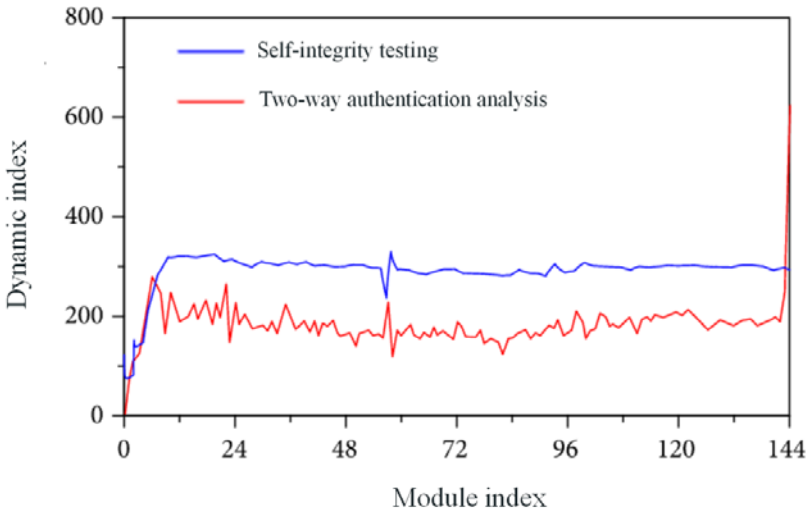

Figure 1 Improving data structure parameters.

In the computer network operating system, the operation concept of real-time system is that real-time system is needed when users issue special instructions, such as operation within control time. All of them conform to the relevant procedure standards and can support the normal operation of all procedures. Operating system design concept, the kernel is very stable, faster, can be fully compatible, and use. The system is a system that can accomplish many tasks and support multiple users to use at the same time. It is the object itself that carries out integrity detection. The object's digital certificate is generated by the system as soon as it is added to the system. And it is also signed by the system. The system saves the list of the objects. When it involves major information, financial data, and statistical information of government agencies, it must be encrypted and stored. It can be used as the system's NTFS file system, and encryption technology is used to encrypt and store important data. For the security operation of the computer system, it is necessary to carry out layer-by-layer protection, which needs to be protected from the bottom of the computer security architecture, so as to improve the information security protection of the computer system. When the network is connected with the host, its detection can play its biggest role. Only in this way can it truly play the role of network protection.

3. Result Analysis and Discussion

Traditional system administrators are concerned with many issues, such as installation and configuration, backup and recovery, resource sharing, system security and performance optimization, which are important aspects of network management today. Moreover, the complexity of the network makes the managed objects in the system not centralized, but decentralized. Provide secure remote access means; use virtual private network technology; secure mail and secure Web server are also important security products. However, for a specific network system, after the security risk assessment determines the appropriate security requirements, it is technically possible to construct a security device platform that meets the basic requirements. Specifically, the relevant responsible personnel should regularly check the computer's specific content and system from the computer network, mainly check the system and important files that the computer network often operates, and make sure everything is normal. The maintenance work should be carried out on the entire operating system, and the operating software of the computer system should be updated. It is also necessary to protect the computer system by using computer anti-virus software, so as to timely and effectively handle the system vulnerabilities.

Secure resources make it easier to remember login information. Using key-based authentication and copying the key only to a predefined, authorized system will obtain and use a more robust and difficult-to-crack authentication certificate. Two-way authentication establishes a trustworthy relationship between the two modules through integrity detection. The purpose of the first step is to

determine the requirements of the system, clarify the requirements of the system, and establish a targeted security strategy for the system. Security policy is an important achievement at this stage, because it serves as the pillar of the system and provides a solid foundation for building a trusted system. Scope control is the factor that affects the project change. It ensures that all changes are managed according to the overall change control process. Finally, effective control is carried out when changes occur to ensure that changes are within the acceptable scope of the project.The operation completes the task quantity, so that it is more efficient to carry out reasonable operations, multiple paths to work, and to ensure completion within the specified time. The control module is a central hub, which is mainly used to maintain the coordinated operation of each module in the system, and to process each event in an orderly manner according to certain strategies.

Information security policy describes the security objectives of an organization at a high level. It describes what should be done rather than how to do it. Determining the organization's security strategy is the precondition for an organization to achieve safety management and technical measures, otherwise all security measures will not be targeted. Module manager is the core part of the firewall, which is used to manage the improved data structure. The cryptographic service provider is used to provide encryption, decryption and key peer-to-peer operation for upper services. At present, the common software firewalls mainly include Skynet firewall, Kaspersky firewall and Rising firewall. The hardware firewall is installed at the junction of the internal network and the external network of the unit. It is applied to enterprises and institutions with strong function and high cost. The installation of a firewall can prevent unauthorized users from accessing internal network resources, thereby effectively protecting internal devices and various information resources. A packet filtering router is a router embedded with firewall firmware, and software such as a proxy server is a software-type firewall. Use a firewall to monitor all your packets to keep your site safe. It monitors each passed data message and request. On the one hand, the passage of trusted messages and application requests is allowed, and on the other hand, harmful or suspicious messages are prohibited from being blocked by the simultaneous exclusion of people and data that you "disagree", to the maximum extent possible in the network. Hackers come to access your network.

4. Conclusion

In this paper, the types and security analysis of computer network operating system based on improved data structure are studied. Network security technology and tools are the foundation, a high level of network security technology team is the guarantee, and strict management is the key. Understand the potential safety hazards of websites, and always pay attention to new management technology and security defense technology. The security problems that have arisen should be solved by the fastest and most effective way, and the security problems that have not arisen at present should be predictable, so as to ensure the reliability of the website operation. Under the improved data structure, each module of the system should be initialized before running, that is, each module should be digitally signed for later integrity detection.Then, the integrity check and mutual authentication are performed before the modules are called. Comprehensive audit analysis and reporting, security management components for security trend analysis. Collect security incidents from a variety of security devices and analyze the correlation between these events to derive real security incidents from these numerous security incidents. The source address of the firewall packet is modified to become the IP address of the firewall itself, so that the external network cannot understand the structure of the internal network. The address translation technology is used, and all network connections can be initiated only internally, thus improving network security.

References

[1] Holk E, Newton R, Siek J (2014) Region-based memory management for GPU programming languages:enabling rich data structures on a spartan host[J]. ACM SIGPLAN Notices, 49(10):141-155.

[2] Brown J M, Bossomaier T, Barnett L . (2017) Review of data structures for computationally efficient nearest-neighbour entropy estimators for large systems with periodic boundary conditions[J]. Journal of Computational Science, 23:109-117.

[3] Papadopoulos L, Walulya I, Tsigas P, et al. (2015) A Systematic Methodology for Optimization of Applications Utilizing Concurrent Data Structures[J]. IEEE Transactions on Computers, 65(7):1-1.

[4] Grossi R, Iacono J, Navarro G, et al. (2017) Asymptotically Optimal Encodings of Range Data Structures for Selection and Top- k Queries[J]. ACM Transactions on Algorithms, 13(2):1-31.