Research on the Construction of Host Security Protection System Based on Network Traffic

Yanhong Shang[1], Jing Zhang[2,*]
[1]Computer Science Department, TangShan Normal University, Tangshan, Hebei, China, 063000
[2]TangShan Normal University, Tangshan, Hebei, China, 063000

Article Info
Volume 83
Page Number: 5620 - 5626
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

The technology in the construction of a host security protection system based on network traffic effectively solves the protection of enterprise information by applying the downlink. With the rapid development of the Internet, the original security system has been unable to meet the economic and information security of individual enterprises. The successful development of research on the construction of host security protection system based on network traffic will escort the economic construction of enterprises.

Keywords: *Host Security, Intrusion Detection, Access Control, Network Traffic;*

1. Introduction

With the rapid development of network information, people's lives have also entered a huge information age. The Internet has brought great changes to people's lives, bringing great convenience to food, clothing, housing, and transportation. The Internet has become ubiquitous in life[1-3]. Following this is the sharing of various information and multi-path propagation, personal data information is easily leaked and other hazards, and enterprises will also cause economic losses due to information security[4-6]. Therefore, network information security companies have emerged and become increasingly powerful. The inherent security firewall of computer systems can no longer achieve a series of security problems. Based on network traffic, this article proposes security policy software, which can play a good role both inside and outside the computer. The protection function completely provides a good environment for the network.

2. Host network security

2.1. The concept of host network security

Host network security is a security system built around the protected host. The elements it considers include network characteristics such as IP address, port number, protocol, and even MAC address, and operating system characteristics such as users, resource permissions, and access time. Comprehensive consideration of these characteristics to achieve fine-grained control of user network access. In addition, considering the security during network transmission, the host network security system also includes secure transmission with users and neighboring servers, as well as authentication services to prevent identity fraud.

Host network security technology is a kind of active defense security technology. It combines the network characteristics of network access and operating system characteristics to set security policies. It can decide whether to allow or not according to the visitor of the network access and the time, place and behavior of the visit. Interviews continue to implement different permissions for the same user in different places, so as to ensure that the permissions of legitimate users are not illegally invaded.

2.2. Application of big data in information security protection

With the development of the Internet, the amount of electricity data is increasing day by day, and the security threats it produces are also increasing, and it is difficult to detect in time. The variety of data and the large amount of data have caused the traditional security technology to detect problems. The speed of data can no longer be adapted. The era of information explosion. If the massive information is not processed in a timely manner, it is easy to reduce the speed of the system, cause the system to crash, and then affect the production and operation of the enterprise; if its security is not checked, it will be vulnerable to malicious attacks or data tampering of the problem data, causing bad influences. The application of big data technology can effectively solve this problem. Big data technology can quickly identify a large amount of data and isolate the data with security threats, which saves data processing time and processor computing resources. In the application of big data technology in power companies, it is necessary to improve the intelligence of basic equipment, increase sensor equipment and upgrade application software, and integrate data in the entire local area network for easy processing.

2.3. Application of smart cloud platform in information security protection

The application of big data technology requires a high-performance computing platform, and the cost of a high-performance computing platform is relatively high, and it is easy for enterprises to build it themselves to cause a waste of resources. Therefore, the application of cloud platform technology reasonably solves this problem. The cloud platform can meet the requirements of big data technology to process a large amount of data in a short time and obtain correct results. It can store a large amount of data, and because it has a large amount of cloud resources, it can perform rapid statistical analysis on the data, while saving The transmission bandwidth resources of big data can compress the data that needs to be transmitted.

2.4. Application of VPN

VPN is to build a secure and encrypted circuit for data transmission on the basis of the actual network. In the VPN network, data packets are highly encrypted, and the access user has a strict identification protocol to ensure the safe transmission of data, thereby ensuring internal network security.

While applying new technologies, it is also necessary to upgrade and maintain traditional information security protection measures, update virus databases in time, use different antivirus software for different pertinence, and perform cross-antivirus; timely repair system vulnerabilities through genuine channels Download patches; monitor the operating status of the protective wall at any time, and process files in the isolation area in time.

The following evaluations are made for the safety effect of the host playing:

There is a multi-index evaluation system composed of n encrypted objects $u_1, u_2, \cdots, u_n$. m indicators $x_1, x_2, \cdots, x_m$ to be evaluated, $x_{ij} = x_j\left(x_i\right)\left(i = 1, 2, \cdots, n; j = 1, 2, \cdots, m\right)$ is the observation value evaluation data matrix (decision matrix) of the evaluated object u_i on the index x_j , which can be expressed as shown in formula (1) :

$$A = \left[x_{ij}\right]_{n \times m} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{bmatrix} \quad (1)$$

2.5. Introduction to the host network security protection technology adopted by USAMS

Intrusion detection system is an important aspect of network security research. From the technical report made by James Anderson in the U.S. Air Force in 1980 [2], the concept of human intrusion detection has been developed for the first time for more than 20 years. In this report It points out that audit trails can be used to detect unauthorized access to files, and provides definitions of some basic terms, including threats, attacks, infiltrations, and vulnerabilities.

Intrusion detection is the discipline of detecting and responding to computer misuse [3]. It is to identify those who are not authorized to use computer systems (such as password-decipherers) and those who have legitimate identities but abuse their privileges (such as internal attacks). By). Current human intrusion detection systems not only detect intrusions (successful attacks), but also unsuccessful attacks. Attacks are all attempts to destroy the security of the system: that is, confidentiality, integrity, availability, and authentication; human invasion is a successful attack, which includes internal attacks, external attacks, and misoperations.

AC is the core content of the information security assurance mechanism, the main means to achieve data confidentiality and integrity, and the basic purpose of host security protection. AC is to restrict access to the subject (or called the initiator, which is an active entity; such as users, processes, services, etc.), to access objects (resources that need to be protected; such as files, memory, network packets, and I/0 devices, etc.)), so that the computer system can be used within the legal scope; the access control mechanism determines what users and programs that represent the interests of certain users can do and to what extent. Two important processes of AC: (1) verify the legal identity of the subject through "authentication"; (2) restrict the user's access level to resources through "authorization".

There are two main types of visit control: network visit control and system visit control. Network access control restricts external access to host network services and system internal user access to external access, which is usually implemented by a firewall. System access control gives different users access to different host resources. The operating system provides certain functions to implement system access control, such as the UNIX file system. Under normal circumstances, these two types of access control are independent of each other, so it is impossible to combine their respective characteristics for control. For example, user attributes cannot be added when using firewalls to implement network access control, and network attributes cannot be added when using UNIX file system functions for file access control.

The security strategy of a computer system is formulated to describe the security requirements of the system. It is a set of rigorous rules that restrict user behavior. This rule stipulates all authorized access in the system and is the basis for implementing access control. The secure computer system follows a certain security strategy design. Its security firstly depends on the security strategy, and secondly depends on the mechanism to implement this strategy.

3. USAMS system model and overall design

3.1. USAMS system model

The system model of USAMS is shown as in Figure. 1.

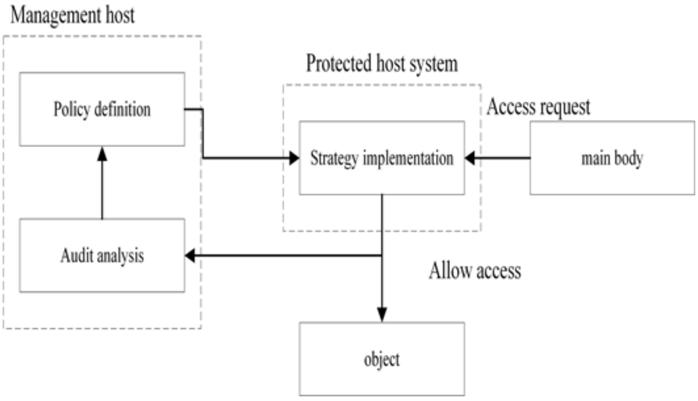

Figure 1. Reference schematic diagram of USAMS system model.

3.2. Host network security protection technology in USAMS

(1) Host-based intrusion detection technology HIDS

USAMS uses HIDS to protect the host. HIDS can monitor suspicious connections in real time, check system logs, monitor illegal visits and typical applications. It can also judge application layer intrusion events based on the characteristics of different operating systems, and monitor system attributes, file attributes, sensitive data, and attack process results. It can accurately determine the intrusion event, and quickly respond to the intrusion event, combined with the packet filtering function module on the host to cut off the network connection from the suspicious address. In order to minimize the chance of intrusions, the host implements strict access control, and its security rules combine network characteristics and operating system sustainability, so that different users have different access rights to resources at different times and places.

HIDS runs on the protected host and monitors its security log, file system, process status and other information. Once an abnormal or suspicious operation is found, a new log record is formed and matched with the predetermined attack characteristics or intrusion logic. If it matches, HIDS will issue an intrusion alert to the administrator or take other corresponding actions to respond to it.

HIDS has a variety of implementation detection methods, which are based on IDA (Intrusion Datection Agent): run multiple IDAs on the protected host, and each IDA is an independent and autonomous detection program that undertakes specific detection tasks. In order to enhance the adaptability of the system, different IDAs can also adopt different detection methods and technologies.

(2) Access control PBMAC based on multi-level security strategy

USAMS combines the characteristics of network access control and system access control to achieve strict and fine-grained access control. Network access control attributes include: source IP address, source port, destination IP address, destination port, etc. System access control (take the file system as an example) attributes include: users, groups, resources (files), permissions, etc. Coupled with restrictions on the user's use time period (start and end time), formulate corresponding security rules to achieve strict access control.

USAMS has only two roles of system administrator and user for the current popular host operating system, adding the role of security administrator. The security administrator takes the security policy as the core when managing, manages the host group joining the system through USAMS, and is responsible for the security management of each distributed host. The system administrator is the administrator who has the system management authority of each host and is responsible for the maintenance and management of the host system. The user refers to the ordinary user of the host. USAMS implements PBMAC based on the new network security model P2DR. The management interface of the security administrator is the policy management interface, through which the security administrator can configure and modify the security policy of the protected host.

In USAMS, the subject represents the user or the process of operation by the user. It is an entity that allows information to flow between objects; the object represents file storage, etc. An object is an information entity or an entity that receives information from other subjects or objects. The subject can also be treated as an object. In a multi-level secure computer system, each subject and object has a security level. The security level of the object represents the sensitivity of the information contained in the object, and the security level of the subject represents the degree to which the subject is trusted. There are many types of subjects and objects in USAMS. It implements a multi-level security strategy by adjusting the authority of each subject and object. As the current host system only provides security measures such as identity authentication, autonomous access control and auditing, USAMS introduces a mandatory access control mechanism. Generate policy configuration information through policy templates. According to the function and focus of each host, the strategy template focuses on network security configuration for file servers, WWW servers, etc.; for engineering computers, it focuses on user management, process control, and file management. At the same time, the policy template provides policy configuration information of different security levels for hosts with the same function.

After generating the policy configuration information, the security administrator can modify the policy configuration according to specific needs to make the security policy more suitable for different needs.

The current host system controls users through the user's file permissions. USAMS introduces the authority list to strengthen the management control and audit of users, as shown in Figure 2.

The user's access to the host can be accessed through the network and the machine. When the user wants to access the network, the network service authentication module judges the user's IP address and access time, and prohibits illegal IP address or legal IP address illegal time access.

When the user passes through the network service authentication module or visits through the machine, it needs to pass the enhanced user authentication module. The host operating system performs user authentication by entering a user name and password and verifying its correctness. Different host systems have different functions in this part. The user authentication module strengthens and unifies the authentication process, increases the control of the time period of its use of the machine, restricts the time period of its use of the machine to legal users, and prohibits them from using the host during the period of non-use of the machine.

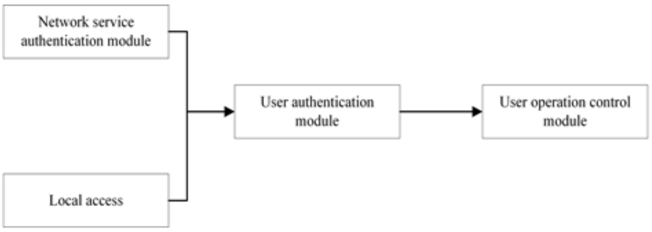
Network service authentication module
Local access
User authentication module
User operation control module

Figure 2. USAMS user machine security control process.

After the user enters the system, the user operation control module judges whether the operation performed by the user is legal or not according to the operation performed by the user and the user's authority list, and prohibits the user from performing unauthorized operations.

USAMS introduces the security control of the user's machine to prevent internal legal users and illegal users from operating the host system illegally and legal users and illegal users from operating the host system at legal times. Combining the control of user names and passwords, it realizes Mandatory control of user permissions. The problem of how to restrict the authority of users (including system administrators) within a controllable range is solved, illegal access activities are prevented, and the security protection of the host system is realized.

3.3. The overall design of USAMS

According to the feature that the host system in the secure network is physically completely isolated from the outside, the possibility of being attacked by the outside (Internet) is very small. Most of the illegal, illegal, and abusers are internal legitimate users with different access rights. The security of the host system is mainly aimed at the unauthorized behavior and human intrusion of the internal users of the information system, and mainly solves the problems of the security of the operating system, the security of the file system, the security of the application system and the security of the storage medium. The security of the operating system is the core of the security of the host system. It mainly involves account and password, data encryption, permission classification, operation history, service program agent restriction, server isolation, output device isolation, computer process and file system scanning, time control, Audit and tracking, system-level intrusion detection and abnormal event statistics, etc. The mainstream operating system of the servers in the local area is the UNIX operating system. Therefore, it is very necessary to study the security of the UNIX operating system and to develop and apply the corresponding security detection management software.

According to the adaptable host security model proposed above, the following will elaborate on the design philosophy of USAMS. It is planned to automatically audit and analyze the behavior of online users, to automatically analyze the system audit records and system gushing distribution status, and to adopt active systems. Detection and system time monitoring, and the use of policy templates to identify abnormal behavior patterns, effectively solve the security problems of hosts in the confidential network, and basically change the security and confidentiality of its internal key information systems. Only administrative orders, and especially effective technical means are used to ensure The unfavorable situation.

The design principles are shown in Table 1:

Table 1. Design principles.

Serial number	Principle	Explanation
1	The security of the system itself	The safety system cannot bring new safety holes. For this, there should be a special self-checking module.
2	Impact on the operating system	It must not have a significant impact on the normal operation of the host, and the system must not be paralyzed due to errors in the safety system (good fault tolerance)
3	Impact on network performance	No obvious impact on normal network communication, performance tuning should be performed on network communication
4	Scalability of functional modules	As the functional modules running under different conditions are not the same, the scalability of the modules should be fully considered when designing the main body.

The goal of the subject is to be able to target the violations, violations, and abuse of the system by internal legitimate users with different access rights in the confidential network; through automatic system configuration detection, automatic audit and analysis of online user behavior; automatic analysis of system audit Record and system vulnerability distribution status; through active system detection and system event monitoring and detection, monitor computer violations, violations, and abuse events; and monitor and restrict system administrators' system management behaviors through restricted shell to ensure the safe operation of the system ; Restrict the user's access scope and use commands through the restricted shell. This will lay a solid foundation for the gradual establishment and improvement of the USAMS security system to ensure the security, consistency, availability and controllability of various confidential information.

4. System implementation of USAMS

USAMS has implemented several functions that an audit management software should have, namely; system security policy configuration, online auditing of user behavior, real-time monitoring of system operating status, fine-grained user access control, post-audit, and system flooding Detection. In particular, user identity authentication and access control strategies have realized user login based on IP and time period and the use of system resources, reached various performance indicators required by system design, and basically solved the host system in the secret-related LAN Existing problems. USAMS has implemented security protection for multiple SGI workstations on the IRIX system, and is in the trial operation stage, and is currently operating well. It has the characteristics of management convenience, timely update, flexible customization, distinctive use time control, convenient and effective authority management, robust system structure, and perfect management framework.

As a security audit system, it needs to consider its own security. USAMS implements it through the following aspects: the security audit system on the host has a self-checking function; the communication between each host and the monitoring machine is achieved through SSL; the monitoring machine guarantees physical Security; monitor and console communicate via https, etc.

However, the functions of the system need to be further improved. For example, the real-time performance and automation of dynamic policy response are not high. The application layer expansion method is used to enforce the security policy, which will easily lead to the generation of system security hidden channels. Times development.

5. Conclusions

The rapid development of the network has led to the transparency of a lot of information, security issues have become the top priority, and network information security technology has emerged. Network information security is mainly to ensure the economic security of the Internet public's property. Enterprises also pay more attention to network security issues, build a protection system according to the enterprise's situation, and create good network conditions for enterprises in the network age.

Acknowledgments

1. Hebei Natural Science Foundation; Research on credibility evaluation system of dynamic cloud services based on multi-source information fusion (No. F2019105134);

2. Scientific research project of Tangshan Normal University; Research on solid liquid ratio spraying system(No..2020C06).

References

[1] Zhang Y, Mao Y, Zhong S. Joint differentially private gale-shapley mechanisms for location privacy protection in mobile traffic offloading systems.[J]. IEEE Journal on Selected Areas in Communications, 2016, 5(9): 1-10.

[2] B. Cheng, Y. Lv, Y. Zhan. Constructing China's Roads as works of art: a case study of “esthetic greenway” construction in the Shennongjia Region of China [J]. Land Degradation & Development, 2015, 55(7): 1060-1066.

[3] Karegar H K, Soleimanisardoo A. Alleviating the impact of distributed generations and network operation modes on protection system [J]. IET Generation Transmission & Distribution, 2019, 14(1): 101-110.

[4] Strohmeier M, Moser D, Schaefer M, et al. On the applicability of satellite-based air traffic control communication for security [J]. IEEE Communications Magazine, 2019, 57(9): 79-85.

[5] Gan S, Liang S, Li K, et al. Long-term ship speed prediction for intelligent traffic signaling [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 4(1): 1-10.

[6] El-Malek A H A, Salhab A M, Zummo S A, et al. Effect of RF interference on the security-reliability tradeoff analysis of multiuser mixed RF/FSO relay networks with power allocation [J]. Journal of Lightwave Technology, 2017, 35(9): 1490-1505.