Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 5, No. 1, 2023

Functions Analysis of Network Terminal Information Security Management and Control

Zhengnan Ji, Ying Wu, Liguo Ma and Yulun Zhang *

Shenyang Joint Logistic Support Center, Shenyang 110015, China
*** Corresponding author:** Yulun Zhang

Abstract: With the rapid development and wide application of information technology, the problem of information leakage caused by security threats such as network hackers, viruses, misoperation and hardware failure also appears. The research on network terminal information security management and control system is to solve the above problems. This paper elaborates the system functions from the perspective of three roles: terminal user, policy administrator and system administrator. Through network information security management and control of terminal, all user operations are documented on the computer, real-time monitoring of sensitive information, timely prevention of illegal operations, and effectively solve the problems of security data acquisition, management, monitoring and audit. It improves the real-time response and perception ability of network security protection.

Keywords: Information Security; Terminal Control; Data Leakage Prevention; Security Policy.

1. Introduction

With the rapid development of information, networking and digitization in our country, the application of information equipment such as computer and network facilities are more and more extensive, which greatly improves the efficiency of information transmission [1-3]. However, the accompanying threats, such as network hackers, viruses, misoperations, computer hardware failures and so on, may lead to the loss or even leakage of important information stored in the computer at any time [4,5]. As an important content of information management, information security has attracted great attention and become an important issue that needs to be considered in the information management of all units.

The purpose of network terminal information security control is to solve some security risks existing in the network and realize the comprehensive management of each network terminal. The system is divided into three roles: terminal user, policy administrator, and system administrator. The functions of the management and control system are analyzed as follows from the perspective of roles.

2. Terminal User

Terminal users are passive users of the management and control system. The network administrator installs the management and control system on the user's computer terminal, and the terminal users automatically register with the server when they install it for the first time. The system cannot have a significant impact on the normal operation of the user, and the system will record the user's various operation information. If all the user's operations are normal computer use, the user will not feel that the control system is installed in the computer, only when the user has illegal operations (such as illegal use of unregistered USB flash drive, illegal handling of classified information, etc.). Only then will the management and control system give a terminal warning to the user, indicating that an illegal operation has occurred, and report the detailed information about the illegal operation to the server as an event. The end-user use case analysis is shown in Fig 1.

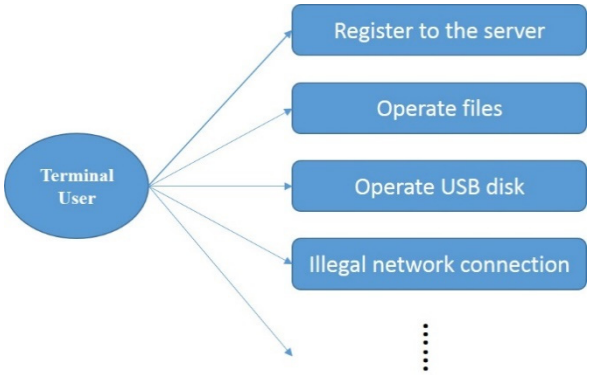

Fig 1. Terminal User Use Case

3. Policy Administrator

The policy administrator is responsible for the management of terminal policies in the private network information security management and control system, including the formulation, modification, delivery, query, and deletion of policies. The policy administrator use case analysis is shown in Fig 2.

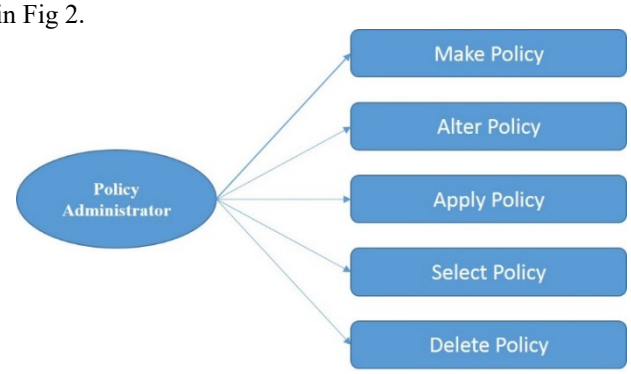

Fig 2. Policy Administrator Use Case

3.1. Make Policy Use Case

Policy formulation is a process by which the policy administrator formulates security management and control

policies for each terminal or type of terminal based on the specific situation of an organization and an individual. Table 1 describes the functions, performers, preconditions, postconditions, basic event flow, and exception event flow of the policy formulation use case.

Table 1. Make Policy Use Case

Use Case Name	Make Policy
Brief Description	Formulate security control policies.
Executor	Policy Administrator
Precondition	The user chooses to enter the association information.
Postcondition	Completion of submission.
Basic Event Stream	Enter the policy generation module, click the Input menu, and enter the associated information of the security management and control policy.
Abnormal Event Stream	When the user clicks the exit button, the system exits the entry function. If an error occurs, the save operation fails.

Policy formulation use case description: As an executor, the policy administrator enters the policy formulation process, clicks enter, enters the associated information elements of the security management and control policy, and saves the submission. If the policy is successful, the policy is in the state to be assigned. If the user clicks exit during operation or the system fails to save, and the system is in the initial state. Use case descriptions are shown in Table 1.

3.2. Alter Policy Use Case

Policy modification is the process of modifying the existing security management and control policies. Table 2 describes the functions, performers, preconditions, postconditions, basic event flow, and exception event flow of the policy modification use case.

Policy modification Use case description: As an executor, the policy administrator enters the policy modification process, clicks Modify, modifies the information related to the security management and control policy, and saves and submits the policy. If the policy succeeds, the policy is in the state before the modification (to be assigned or allocated). If the user clicks exit during operation or the system fails to save, and the system is in the initial state. Use case descriptions are shown in Table 2.

Table 2. Alter Policy Use Case

Use Case Name	Alter Policy
Brief Description	Modify the existing security management and control policies.
Executor	Policy Administrator
Precondition	Click the Modify button to enter the modify page.
Postcondition	The policy is saved and submitted successfully. The policy is in the state before the modification.
Basic Event Stream	The user enters the maintenance and modification module and modifies related security management and control policies.
Abnormal Event Stream	When the user clicks the exit button, the system exits the modification function. If an error occurs, the save operation fails.

3.3. Apply Policy Use Case

A policy delivery case is a process by which a policy administrator sends edited security management and control policies to corresponding terminals based on actual conditions. Table 3 describes the functions, primary performers, preconditions, postconditions, basic event flow, and exception event flow of the policy assignment use case.

Table 3. Apply Policy Use Case

Use Case Name	Apply Policy
Brief Description	Send the developed security management and control policies to end users or end user groups.
Executor	Policy Administrator
Precondition	On the policy list page, select the policy to be delivered and the policy execution terminal.
Postcondition	Click the Back button to return to the policy list interface.
Basic Event Stream	The user enters the policy list and sends the selected policy to the specified terminal.
Abnormal Event Stream	When a user clicks the exit button during delivery, or an error occurs, policy delivery fails.

Policy delivery case description: As the primary executor, the policy administrator enters the policy assignment process. On the policy list page, select the policy to be delivered, select the object to be delivered, and send the policy to the selected end users or end user groups. If the user clicks Exit or the system makes an error, the delivery fails.

3.4. Select Policy Use Case

The policy query use case is a process for the policy administrator to view the policy execution status of the current private network information security management and control system client. Table 4 describes the function of the policy query use case, main executor, preconditions, postconditions, basic event flow, and exception event flow.

Table 4. Select Policy Use Case

Use Case Name	Select Policy
Brief Description	View the execution of security management and control policies.
Executor	Policy Administrator
Precondition	On the policy list page, click the corresponding policy or the terminal user to be queried in the installed client list to view policy delivery.
Postcondition	Click the Back button to return to the policy list interface or client list interface.
Basic Event Stream	The user enters the policy list or client list to view the policy execution status.
Abnormal Event Stream	The query operation fails if the user clicks the exit button during the query or an error occurs.

Policy query Use case description: As the primary executor, a policy administrator enters the policy query process. On the policy list page, click a policy to view the terminals that have been sent to the policy. On the list of installed clients, click a terminal to view the policies that have been loaded on the terminal. If the user clicks exit during operation or the system makes an error, the query fails.

3.5. Delete Policy Use Case

Table 5 describes the function of the policy removal use

case, primary executor, preconditions, postconditions, basic event flow, and exception event flow.

Policy deletion Use case description: As the primary executor, the policy administrator enters the policy deletion process. On the policy list page, click a policy to view the terminals that have been sent to the policy. Click Disable All to stop using the policy, and then click Delete to delete the policy. If the user clicks exit during operation or the system makes an error, the query fails.

Table 5. Delete Policy Use Case

Use Case Name	Delete Policy
Brief Description	Delete an existing security management and control policy.
Executor	Policy Administrator
Precondition	Click the policy in the policy list to view the policy delivery status and disable the policy.
Postcondition	Click the Back button to return to the policy list interface.
Basic Event Stream	The user enters the policy list, selects the policy to be deleted, deactivates the policy, and deletes the policy.
Abnormal Event Stream	The deletion operation fails when the user clicks the exit button during the deletion process or an error occurs.

4. System Administrator

The system administrator is responsible for the comprehensive management of the private network information security control system, including client audit, user management, event management, data management, report generation, etc. The system administrator use case diagram is shown in Fig 3.

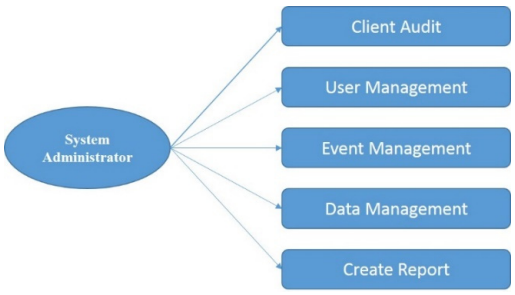

Fig 3. System Administrator Use Case

4.1. Verify Client Use Case

This function is used to audit the computer terminal of the installed system client, improve the terminal information, and make it a legitimate user of the system. Use case descriptions are shown in Table 6.

4.2. User Management Use Case

Table 6. Verify Client Use Case

Use Case Name	Verify Client
Brief Description	Audit computer terminals with installed system clients.
Executor	System Administrator
Precondition	Terminal waiting for review by the system administrator.
Postcondition	The terminal to be audited becomes a legitimate user.
Basic Event Stream	System administrator improves the information of terminals waiting for review, so that they have the legal identity of the system.
Abnormal Event Stream	The audit cannot be completed if the information provided by the terminal to be audited is incomplete.

This function is used to manage and maintain system users. Use case descriptions are shown in Table 7.

Table 7. User Management Use Case

Use Case Name	User Management
Brief Description	Manage and maintain system users
Executor	System Administrator
Precondition	Add users, modify users or delete users.
Postcondition	User information has changed.
Basic Event Stream	The system administrator logs in to the user management module, maintains the user information, and then saves it.
Abnormal Event Stream	If duplicate users exist, send a message to the system administrator indicating that the user cannot be repeated.

Table 8. Event Management Use Case

Use Case Name	Event Management
Brief Description	Maintain the network information security events of the whole system.
Executor	System Administrator
Precondition	The system successfully receives network information security events reported by terminals.
Postcondition	Event information is stored in the database.
Basic Event Stream	The system administrator manages system events and forms a security profile.
Abnormal Event Stream	If the format of the event reported by the terminal is different from that of the system, the operation fails.

4.3. Event Management Use Cases

This function is used by system administrators to manage network information security events reported by terminals and generate a situation diagram to visually display the security status of each unit or terminal. Use case descriptions are shown in Table 8.

4.4. Data Management Use Case

Table 9. Data Management Use Case

Use Case Name	Data Management
Brief Description	Manage and maintain the system data information.
Executor	System administrator.
Precondition	Data exists in the system.
Postcondition	The data information of the system is stored in the database and backed up.
Basic Event Stream	The system administrator logs in to user operation records and maintains user behavior logs.
Abnormal Event Stream	The operation fails if a system error occurs.

Table 10. Create Report Use Case

Use Case Name	Create Report
Brief Description	Organize and analyze the security events received by the system and generate reports.
Executor	System administrator.
Precondition	Event information exists in the system.
Postcondition	Generate a security health report.
Basic Event Stream	The system administrator organizes the event information in a certain period of time into a report and provides it to the management department. This helps the management personnel learn about the overall security status of the organization.
Abnormal Event Stream	The system did not receive the data or the operation failed because of an error.

This function is used to manage and maintain all system data, including user information, policy information, and event information. Use case descriptions are shown in Table 9.

4.5. Create Report Use Case

This function is used to sort out and analyze network information security events received by the system, and generate security status reports for management departments. Use case descriptions are shown in Table 10.

5. Conclusion

Network is a double-edged sword. Its wide application not only brings convenience to people's work and life, but also brings corresponding security threats, such as: viruses, hackers, trojans and so on. In view of the existing problems in the information security control of network access terminals, this paper analyzes the functional key points of network terminal security control from the perspective of using roles, introduces the role functions in the form of use case diagram, and expounds the brief description of each function, executor, pre-condition, post-condition, basic event flow and abnormal event flow in the form of use case table. A detailed functional analysis description was formed. In the process of implementation, also need to pay attention to the following issues:

(1) In order to maintain the system's control over access terminals, system processes should be kept online during the whole process of terminal operation, and corresponding measures should be taken to avoid system control function failure due to system processes being killed or offline [6].

(2) Because the management and control system require all access terminals to report various violation information to the server in real time, the system is required to operate stably and reliably, and crashes and system crashes cannot occur without reason [7].

(3) In order to maintain the smooth feeling of network use by users, all operations of the installed client are required to be carried out in the background, and users are not required to perform any other operations [8].

References

[1] Liu Shuanglin,Guo Yefang, Shi Yiming, etc. Security Control of Power Grid Bidding Information based on distributed blockchain [J]. Information Technology, 2021(10): 70-74.

[2] Wei Ran;Yao Sheng. Enterprise Financial Risk Identification and Information Security Management and Control in Big Data Environment[J]. MOBILE INFORMATION SYSTEMS. Volume 2021, Issue . 2021.

[3] An Ningyu, Su Li, Tian Ye. Research on 5G Information security risk [J]. Security Science and Technology, 2020(09):8-14.

[4] Xia Junling. Research and Design of multilevel document security Model based on Electronic tags [D]. Xi 'an: Xidian University, 2011.

[5] Liu Lijie. Research on Improving information security level based on desktop Management and Control technology [J]. Science and Technology Innovation and Application, 202,12(09): 162-165.

[6] Xie Bolin, Yu Shunzheng. Application layer real-time active defense system based on application layer protocol analysis. Journal of Computer Science, March 2011.

[7] Du Xiaojie, LIANG Chengdong, Peng Shiqiang,etc. Hierarchical protection evaluation data leak prevention System based on blockchain [J]. Electronic Quality. 2022(10):72-76.

[8] Sheela Gowr. P; Kumar. N. Data Leakage Prevention System: A Systematic Report[J]. International Journal of Recent Technology and Engineering (IJRTE). Volume 8, Issue 4 . 2019. PP 367-377.