ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

A Study of the Security Management System for University Privileged Accounts Linked with Fortification Machines: Practical Research

Yunjie Li[1], Dan Zhang[1,*], Xianjun Meng[1], Yanbo Chen[1]

[1]Educational Technology and Information Center, Shenzhen Polytechnic, Shenzhen, 518055, China
**Corresponding author: dreamingbench@163.com*

Abstract: *In practice, the management mode and methods of privileged account in information systems often have significant security risks. This paper studies and elaborates on the security management system of privileged accounts and the technical characteristics and advantages of bastion host. Through the seamless linkage of the two, an efficient, long-term, and secure privileged account security management system is proposed, which can achieve full coverage and lifecycle management of different types of privileged accounts, timely identify account risks and dispose of them, and meet industry regulatory requirements. The system satisfies the requirements of industry regulations and laws.*

Keywords: *Privileged account management, Bastion host, Information security, Operation and maintenance management*

1. Introduction

With the widespread application of technologies such as cloud computing, big data, DevOps, process automation, and IoT in information technology, the number of information system platforms and applications in universities continues to increase, and the number of privileged accounts is also growing rapidly. However, the management of these accounts is becoming increasingly difficult, and security incidents caused by improper management of privileged accounts are occurring frequently, resulting in significant economic and social losses for various organizations [1].

Currently, most universities use various types of privileged credentials (such as passwords, keys, SSH keys, tokens, certificates, and tokens) to authenticate users and applications that use privileged accounts. However, there are many problems with managing privileged accounts, such as the difficulty for the operations and security management department to grasp the situation of data center privileged accounts, the management of account passwords by individuals leading to plaintext storage and account sharing, the severe problem of weak passwords that are easily guessed or cracked, and the existence of a large amount of "hard-coded" data in middleware, application code, and configuration files that are difficult to manage manually [2]. Attackers often use unprotected privileged accounts and credentials for lateral penetration to steal data and damage the information assets of universities. Therefore, protecting and monitoring privileged accounts is a key aspect of university information security construction.

To address the above issues, a university information security construction should design an effective privileged account management (PAM) system [3], which is positioned to center around the full lifecycle management of privileged accounts, with the basic principle of minimizing permission management, and with privileged session management and monitoring as important means. The goal is to systematically implement the unified management, standardized use, and global monitoring of privileged accounts in various business scenarios, while reducing the probability of data security incidents caused by privileged account leaks or misuse.

Fortification machines provide a more efficient way to change the way IT infrastructure interacts with operations personnel, effectively addressing operational risks and supporting a variety of operational terminal applications. This allows administrators to free themselves from complex operational management and focus on enhancing the core value of the data center [4, 5]. With the development of university network architecture and the deepening of information construction, network operations tasks are becoming increasingly complex and diverse [6, 7].

ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

In this context, a comprehensive PAM system is essential to provide a unified, standardized, and global management approach for privileged accounts. By linking PAM with fortification machines, a more secure and efficient privileged account management approach can be achieved, which can effectively control and monitor privileged account activities, prevent security risks caused by unauthorized access, and meet the requirements of university network security construction.

2. Study on the Privileged Account Management System

2.1 Characteristics of the System

The privileged account management (PAM) system has the characteristics of automatic account discovery, automatic detection of weak passwords, regular password changes and verification, secure storage of accounts, and account management policies, which can effectively meet the needs of different business scenarios in the privileged account management process [8].

(1) Automatic account discovery: The system can continuously discover changes in the IT environment. By manually or automatically triggering account discovery policies, the system can use pre-defined privileged accounts to connect to target devices in batches, scan the target devices, compare them with historical scan results, and promptly discover unmanaged accounts, backdoor accounts, zombie accounts, and accounts with changed permissions. This allows security personnel to quickly understand the distribution, use, and changes of privileged accounts within the organization.

(2) Automatic detection of weak passwords: The system provides comprehensive detection of weak passwords for target devices, supporting platforms including Linux/Unix, Windows Server, Oracle, MySQL, MS SQL Server, etc. The system can customize weak password sets and rules, and comprehensively detect the distribution of weak passwords for resources.

(3) Regular password changes and verification: Regular password changes and verification are the most important tasks in account management. The PAM system supports the change of system account passwords for host, network equipment, database, middleware, and other resources for operational management purposes. Users can pre-set password change cycles, password complexity, and password change ranges, and trigger the password change plan manually or automatically to change the passwords of specified resource accounts. For password change attachments, two recipients can be set, and the attachment is encrypted. The two recipients receive the first half and the second half of the account password, respectively, and the complete password can be obtained by combining the two halves.

(4) Secure storage of accounts: The PAM system provides secure storage of account passwords and credentials, making it easier to manage and protect various types of privileged account credentials. Data isolation can be achieved based on departments, and administrators from different departments cannot access data across departments, achieving isolation of audit, resource, and account data.

(5) Account management policies: The system can quickly and flexibly formulate global policies for privileged account management and provide fine-grained special policies to meet the special requirements of different devices and operating systems. Various policies, such as access control policies, one-time-password policies, and exclusive policies, can be used to set mandatory management measures for privileged accounts, ensuring their security and reliability.

2.2 System Architecture and Workflow

The architecture of the privileged account management system is shown in Figure 1:

The process for using the account management system is as follows:

(1) Administrators access the PAM web console through a web browser.

(2) The privileged accounts are added to the password vault.

(3) Password policies are configured.

(4) The policy executor automatically changes the passwords and performs inspections on target assets based on the password policies.

(5) After the password is changed, the updated password is stored in the password vault.

ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

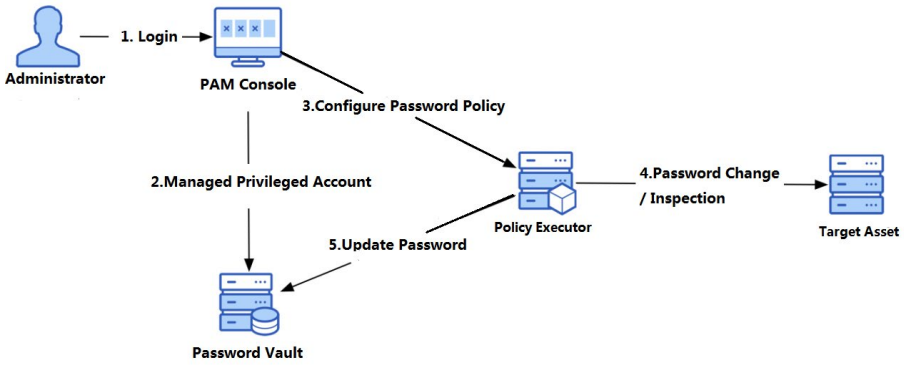

Figure 1: Logical Architecture of the Privileged Account Management System

This process provides a secure and efficient way to manage privileged accounts in university information systems. By using the PAM system, administrators can easily configure password policies and automate the password change process, reducing the risk of security incidents caused by weak or compromised passwords. The password vault provides a secure and centralized location for storing and managing privileged account credentials, making it easier to track and control access to these accounts.

2.3 Characteristics of the Fortification Machine System

According to the "Basic Requirements for Information Security Technology - Network Security Level Protection" (GB/T22239-2019), the fortification machine has become a necessary device for campus information construction. Without the fortification machine, it is impossible to complete the work of operational security auditing or clearly record and manage the access of operations personnel to campus resources. Therefore, the introduction of a fortification machine can effectively achieve the integration of prevention, control, and auditing functions. The fortification machine is a common operational security auditing device, which mainly includes two functions: core system operation and security auditing control. In addition, it also includes functions such as identity authentication, account management, authorization control, and single sign-on [4]. The fortification machine separates the system operations personnel from the target device. The system operations personnel log in to the fortification machine using their username and password, and then the fortification machine jumps to the authorized target device. Device administrators can authorize the target device to the system operations personnel through the fortification machine, and password administrators are responsible for updating the real passwords of the device. The system operations personnel cannot access unauthorized devices through the fortification machine or obtain the real passwords of the target device, thereby achieving access authorization management of the target device. In addition, the fortification machine automatically records the entire operation process of the system operations personnel, facilitating post-event security auditing and timely discovery of violations by operational personnel. Therefore, by using the fortification machine, the excessive concentration of operational personnel power can be effectively avoided, reducing the operational security risks of the information system.

The fortification machine has a comprehensive operational security risk control capability in the security management and auditing field, supporting the operation and auditing of resources such as network devices, databases, security devices, and host systems. By using centralized operational control, real-time supervision of operational processes, compliance control of operational access, and graphical auditing of operational processes, a complete operational process security management system can be constructed, including prevention before an event, monitoring during an event, and auditing after an event [9].

The user authentication management mode, resource management mode, authorization management mode, and operation auditing function of the fortification machine can greatly enhance the operational security risk control capability of an organization. Practical research shows that relying solely on the fortification machine system cannot complete the diversified operational auditing tasks of a campus network. How to solve the contradiction between refined operational requirements and isolated operational auditing defects has become one of the current research hotspots [10]. Implementing the linkage between the privileged account security management system and the fortification machine can further enhance the standardization and security of privileged account management and operations [4].

ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

The architecture of the fortification machine system is shown in Figure 2:

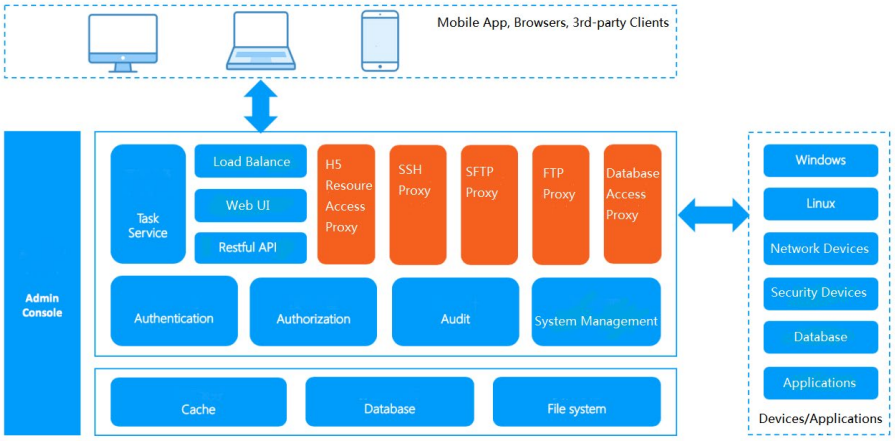

Figure 2: The architecture of the fortification machine system

The fortification machine system has become an indispensable tool for managing privileged accounts and controlling operational access in university information systems. By using the fortification machine, administrators can implement access control policies, enforce password policies, and audit all operational activities in a centralized and secure manner. The fortification machine can effectively reduce the risk of security incidents caused by unauthorized access and compromised passwords, safeguarding the confidentiality, integrity, and availability of campus resources.

3. A Privileged Account Management System Linked with the Fortification Machine

3.1 Design Principles

Due to the isolation between the internal network and the Internet in universities, a network path between the two must be established to remotely handle faults in internal network information systems. Therefore, the following principles must be adhered to in the design process, given the importance of the internal network in universities:

1) Do not change the existing core network structure of the internal network. The internal network of universities has been running stably for many years, and important information systems are deployed according to a unified network plan. Therefore, the original network structure of the internal network cannot be changed, as this would bring uncontrollable network security risks.

2) Ensure the security of the overall network. The internal network of universities plays a crucial supporting role in teaching management and other businesses, hosts multiple important information systems, and meets the requirements of Network Security Level Protection Level 2. Therefore, the security protection level of the overall network cannot be affected, and the security protection capability of the network must be ensured.

3) Adhere to the principle of granting the minimum access privileges to remote operational personnel for accessing internal network resources. To reduce the external threats faced by internal network resources and minimize the losses caused by malicious users utilizing PAM, the minimum privilege principle should be followed when assigning permissions. Whether it is the operational privileges of operational personnel or the addresses and ports of network connections, only the necessary privileges should be granted to reduce the network security risks faced.

Adhering to these principles can effectively ensure the security of the internal network of universities and reduce the risk of unauthorized access and compromised passwords. By linking the privileged account management system with the fortification machine, a more comprehensive and secure approach can be established for managing privileged accounts and controlling operational access in university information systems.

3.2 System Architecture

The privileged account management system and the fortification machine can achieve a seamless

ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

linkage mode. In this mode, PAM is responsible for the full lifecycle management of privileged accounts, while the fortification machine serves as the unified entry point for operational access. When the fortification machine needs to use an account to connect to a target device for operational purposes, it will dynamically retrieve the account password from PAM. The fortification machine does not store account passwords locally, which comprehensively solves the problems of password changes and conflicts in account usage. Account-related issues such as password changes, verification, and account discovery are handled by the privileged account management system, while account operational use is handled by the fortification machine. The linkage and integration of the two systems can comprehensively solve the problems of privileged account lifecycle management and operational process management.

The seamless linkage mode between the privileged account management system and the fortification machine can effectively improve the security and efficiency of operational access in university information systems. By integrating the two systems, administrators can centrally manage and control privileged accounts, enforce password policies, and audit operational activities in a secure and efficient manner. Operational personnel can access target assets through the fortification machine, with the access privileges granted and monitored by the privileged account management system. This approach can effectively reduce the risk of security incidents caused by unauthorized access and compromised passwords, safeguarding the confidentiality, integrity, and availability of campus resources.

The Architecture of the linkage between PAM and the fortification machine is shown in Figure 3 :

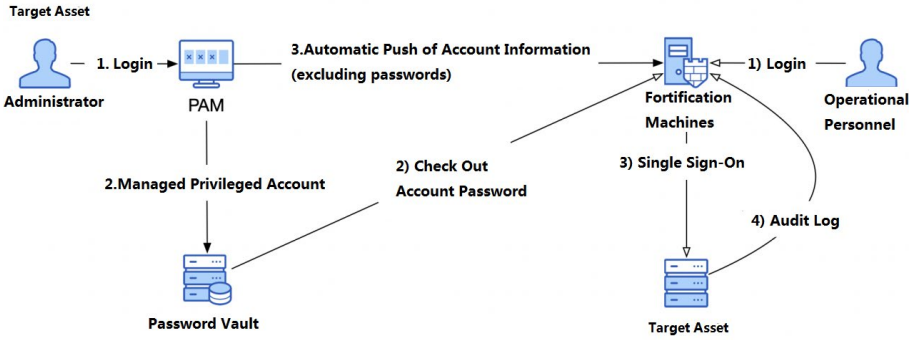

Figure 3: The Architecture of the linkage between PAM and the fortification machine

The seamless linkage mode between the privileged account management system and the fortification machine can provide a comprehensive and secure approach to managing privileged accounts and controlling operational access in university information systems. This approach can effectively improve the security and efficiency of operational access, reducing the risk of security incidents and ensuring the stable and reliable operation of campus resources.

3.3 Account Operational Process

In this system, the account operational process is as follows:

(1) The operational personnel access the fortification machine through a browser;

(2) The fortification machine retrieves the account password from the password vault;

(3) The operational personnel single sign-on to the target device and perform operational activities;

(4) The fortification machine records the operational audit log.

As can be seen, compared to the previous approach, the security is higher while the process becomes simpler.

This approach can improve the security and efficiency of operational access in university information systems. By implementing strict access control and monitoring measures, the risk of unauthorized access and compromised passwords can be effectively reduced, safeguarding the confidentiality, integrity, and availability of campus resources. The simplified process can also improve the usability and convenience of operational access, enabling operational personnel to perform their duties in an efficient and effective manner.

ISSN 2616-5902 Vol. 5, Issue 13: 127-132, DOI: 10.25236/AJBM.2023.051318

4. Conclusion

The privileged account security management system and the fortification machine have different technical characteristics. By linking the two, their advantages can be fully utilized, forming a more standardized architecture system and more convenient operational access process, effectively solving the problems of privileged account lifecycle management and operational process management. The privileged account management system linked with the fortification machine can be widely applied to servers, cloud servers, network devices, databases, middleware, application systems, big data platforms, and other scenarios, eliminating privileged account management security risks and comprehensively improving the IT operational capabilities of organizations.

In summary, the integration of the privileged account management system and the fortification machine provides a comprehensive approach to managing privileged accounts and controlling operational access in university information systems. This approach can effectively improve the security and efficiency of operational access, reduce the risk of security incidents, and ensure the stable and reliable operation of campus resources. By adhering to the design principles and implementing strict access control and monitoring measures, universities can establish a secure, efficient, and convenient approach to managing privileged accounts and controlling operational access, promoting the development and innovation of university information systems.

References

[1] Liu Qi. Research on Privileged Account Threat Analysis System [J]. Electronic World, 2020(24): 75~77.
[2] Liu Qi. Research and Analysis of Privileged Account Security Management System [J]. Information and Computer (Theory Edition), 2020, 32(21): 198~200.
[3] Liu Xiaoxiao. Establishing a Secure Management System for Information System "Privileged Accounts" [J]. Financial Electronicization, 2009(07): 67.
[4] Liang Haowei. Operational Security Management Based on Fortification Machine [J]. China Informatization, 2021(04): 80~81.
[5] Xu Shenglin. Strengthening the Construction of University Campus Network Operational System to Improve User Experience [J]. Information Systems Engineering, 2021(09): 112~114.
[6] Xuan Hui, Chen Xing. Application of Fortification Machine in Campus Information System [J]. China New Communications, 2018, 20(06): 81.
[7] Peng Guifen, Zhe Mingwei, Han Hua. Preliminary Exploration on the Construction and Application of Fortification Machine in Medical Colleges and Universities [J]. Modern Information Technology, 2019, 3(10): 152~154.
[8] Feng Kuan. Research on Key Technologies and Systems for Privileged Access Security Integration Data Platform [D]. Harbin Institute of Technology, 2020.
[9] Lin Zhida, Zhang Huabing, Cao Xiaoming, et al. Enterprise Information Network Security Protection Model Based on Fortification Machine Technology [J]. Electronic Design Engineering, 2022, 30(18): 179~183.
[10] Zhang Zhe. Application of Fortification Machine and VPN Technology in the Remote Disposal of Emergency Information System Faults in the People's Bank [J]. Heilongjiang Finance, 2021(02): 48~50.