Research and Implementation of SSH Proxy System for Filtering and Auditing

Zhuxiao Wang¹, Jiaming Zhang¹*, Kehe Wu¹, Wei Li¹ and Wenchao Cui¹
¹School of Control and Computer Engineering, North China Electric Power University
*Corresponding author’s e-mail: 120192227089@ncepu.edu.cn

Abstract. With the rapid development of information technology and network, the informatization level of enterprises is constantly improving, and the security of information system is becoming more and more important. Not only the external intrusion needs to be effectively resisted, but the operation and maintenance of internal personnel also needs to be under security control. Starting from the internal security of enterprise information system, this paper designs and implements the SSH protocol operation and maintenance audit system based on libssh. The forwarding module of the system can meet the requirements of SSH protocol operation and maintenance, and set command parsing, filtering and recording modules, which can correctly identify the commands executed by users and server data, and addition to filter the forbidden commands. In addition, the setting of replay and monitoring module can record the whole process of personnel's operation, so as to ensure that the auditors can monitor in real time or replay afterwards. The system ensures the security of the enterprise internal information system.

1. Introduction

With the continuous development of information technology, enterprises in various industries have carried out information transformation and development. Therefore, reliable and high security business and information system is very important for enterprises. In order to ensure the security of the information network constructed by enterprises, on the one hand, through the construction of network firewall, timely detection and repair of loopholes and other related measures to resist the increasingly hidden and complex external intrusion attacks; on the other hand, the operation and maintenance of "legitimate personnel" in the enterprise also needs to ensure security.

In the information construction of enterprises, with the continuous expansion of system resources, the operation and maintenance personnel not only have more complex system software and hardware maintenance work in the enterprise, but also have higher operation authority. Once they are approved, various operations of the system cannot be effectively supervised, whether it is personnel misoperation or subjective malicious behavior, such as data information leakage, tampering with data, destroying the system and others, may cause varying degrees of harm to the enterprise[1].

Therefore, for the internal security of enterprise information system, not only need to verify the identity of personnel, but also need to establish a safe operation and maintenance environment, and take effective filtering, monitoring and audit measures. In order to meet the above requirements, this paper designs and implements an operation and maintenance audit system based on SSH protocol. The system is deployed in an independent server, independent of the client and server[2].

The main contributions of this paper include: 1) Implement an SSH proxy system based on libssh; 2) Design the command parsing, filtering and recording modules for parsing commands and making
legality judgments, and write data to disk for recording. 3) Replay and monitoring module, which is used for real-time monitoring and post-audit of operation and maintenance personnel.

2. Overview of Secure Shell Protocol and Terminal

2.1. Secure Shell

The SSH (Secure Shell) protocol was originally developed by Tatu Ylonen of the University of Helsinki in Finland, and later developed by the IETF Network Working Group to further develop a standardized SSH protocol. The SSH protocol is a security protocol based on the application layer and the transport layer. By encrypting the communication data, it ensures high security and reliability[3]. The SSH workflow is:

1) Negotiation
   Due to the different SSH protocol versions and key algorithms, after the client initiates a connection request, the two parties negotiate the SSH version and communication algorithm. After successful negotiation, the ID and key of this session are generated, which are used to identify this session and ensure security.

2) Authentication
   The client sends authentication data, and the authentication methods include: public key, password, host-based authentication method, etc. The server responds according to the authentication result.

3) Session request
   After the client is authenticated, it initiates a specific session request to the server. The request types include session, X11, forward-TCP/IP, and direct-TCP/IP. The server processes the request and establishes the corresponding type of channel. Multiple channels can be established in one session.

4) Channel interaction
   The two parties exchange data based on the channel, and the server cyclically processes the data of the client and returns the feedback data. This continues until the session is disconnected.

2.2. Libssh

Libssh is a multiplatform C library implementing the SSHv2 protocol on client and server side. Based on libssh, clients can establish SSH sessions with remote servers and request multiple types of channels, such as session, X11, forward-TCP/IP, and direct-TCP/IP, to meet the needs of interactive sessions. Similarly, the server can respond correctly to the SSH request of the client by using the API provided by libssh. The characteristics of libssh can just meet the needs of building a proxy system[4].

2.3. Terminal

The terminal is a set of equipment for users to interact with the host. On the one hand, it displays the output information of the host, on the other hand, it receives the input and transmits it to the host for processing. The existence form of the terminal can be either directly connected to the display, keyboard and other devices, or connected to other hosts through the serial cable, or carrying the remote terminal through the TCP/IP network protocol. In order to realize the user remote management of host equipment, the system uses a pseudo device file to correspond and bind with the user's pseudo terminal. In the middle, the data can be transmitted through Telnet, SSH protocol and so on to meet the interaction needs[5].

For the pseudo terminal, one is to simulate the interactive environment for the user, control the number of rows and columns of the whole terminal, control the colour of characters, cover the password, etc; The second is to execute the user's special control instructions. When receiving the user's special input instructions, they will not be directly forwarded as data, but capture and trigger control behaviour[6].
3. The SSH protocol operation and maintenance audit system

3.1. System process

The overall structure of the system is shown in the Figure 1, mainly including forwarding module, command parsing, filtering and recording modules, replay and monitoring module. Firstly, the system initializes the service and listen on a port, which is 2222 by default. When the user initiates a connection request at the client, the connection information and authentication data are transmitted; The system calls the authentication module to complete the authentication of the operation and maintenance personnel, the authentication with the operation and maintenance target server, and the establishment of the connection; The system sends the authentication information of the target server back to the client through the forwarding module; In the process of data forwarding, the data will be first transmitted to the command parsing module, and then the command filtering module will query the forbidden command table to determine whether the command is legal. If it is legal, the forwarding module will be allowed to transmit data, otherwise, the forwarding is forbidden[7].

In addition, the command parsing module will send the data to the command recording module synchronously. According to the type and time of the command, the module writes the data to the disk in a specific format to complete the whole process of recording the session. If the auditors need to play back or monitor the session, they can establish a connection with the replay & monitoring module through a specific plug-in. After the authentication, they can read the audit file to complete the review of the operation and maintenance session. The process continues to loop until the customer requests to disconnect.

3.2. Major modules and functions

3.2.1. Forwarding module

The forwarding module is implemented based on libssh. As a forwarding platform, the system needs to be the server of operation and maintenance personnel on the one hand, and the client of enterprise operation and maintenance equipment on the other. Therefore, we need to establish both server and client through libssh.
As shown in the Figure 2, the system establishes service listening, authenticates when a connection request is received, and completes the authentication with the server after identifying the identity of the client. When both authentications are passed, the SSH session is established successfully. After the channel is opened, the operation and maintenance audit system forwards the data of both sides, forwards the client's command to the server, and forwards the information returned by the server back to the client. In this way, the data is circularly forwarded to complete the interaction between the operation and maintenance personnel and the server.

3.2.2. Command parsing, filtering and recording modules

In order to ensure the detection of the operation and maintenance personnel to execute the command and prevent the serious consequences caused by high-risk command, the system needs to record and check the operation of the operation and maintenance personnel.

**Command Parsing**

Through the establishment of buffer, the purpose of temporary storage of operation and maintenance command data is achieved. Therefore, this system uses VT100 terminal as the command analysis platform. Through the analysis of VT100 terminal control code, it can complete the parse of command and server return information, and achieve the purpose of normal acquisition of command and display content.

![Figure 3. Command parsing process](image)

As shown in the Figure 3, the parsing process first needs to initialize an effective terminal control code table to be solved and matched; Then, the characters of buffer are parsed one by one. When the parsed characters match a terminal control code, the output buffer is processed according to the function of the corresponding terminal control code. If the character currently processed is not a control code, it is recorded in the output buffer. When the input buffer processing is completed, the valid command content is output according to the current output buffer and the cursor position.

**Filtering and recording**

In the session establishment stage, the system will load the operation and maintenance forbidden commands corresponding to this session into the memory. The loading source can be in the form of database or file. These commands are written into the current session structure in the form of linked list. The filtering module traverses and matches the parsed data. If there is a match with the contents of the forbidden command set, the forwarding will be stopped, otherwise the forwarding will be normal.

![Figure 4. Audit data file format](image)

For the user's operation command and the data returned by the server, it needs to be persisted to the disk through the recording module, and exists in the form of file. The record file is divided into two parts: one is the operation and maintenance operation execution command, the other is the server echo.
data. For commands in each execution cycle, the specific data format to be recorded is shown in Figure 4.

3.2.3. Replay and monitoring module

**Replay**

Replay for the finished SSH session, the auditor sends the authentication information and the specific session to be played back by sending the playback request to the system, and the system directly reads the audit files to send the data to the auditor for replay, so as to achieve the purpose of the whole process of session review.

**Monitoring**

Similarly, if there is a need for real-time monitoring, the auditor can authenticate and establish a connection with the proxy system, specify the monitoring session, and the forwarding module will open an interface to access the monitoring module, which will not only forward the data back to the operation and maintenance personnel, but also write it into the monitoring module. In order to ensure multi-terminal monitoring, the monitoring module establishes a monitoring set. When receiving the data from the forwarding module, it traverses the set and writes the data to complete real-time monitoring.

4. Demonstration

4.1. Operation and maintenance

As shown in the Figure 5, by connecting the 2222 port of 192.168.100.88, the access to 192.168.100.176 is realized, and the operation and maintenance operation can be carried out.

4.2. Command filtering

This demonstration completes the reading of the operation and maintenance prohibition command by reading the database field. It can be seen from the figure that during the operation and maintenance process, the input of these commands will be connected by the command filtering module, and the
execution will be cancelled, and the user will be informed that the current command is the operation and maintenance prohibition command.

4.3. Replay and monitoring

Figure 7. Replay interface

Through the Replay and monitoring module, the whole operation process of the operation and maintenance personnel can be replayed and monitored, including the specific execution time, command and content display.

5. Summary

In the information construction of enterprises, the internal security of information system cannot be ignored. This paper illustrates the content of SSH protocol, the libssh library and terminal, as well as establishes a SSH protocol filtering and auditing proxy system.

The system builds a forwarding module based on libssh, which can meet the operation requirements. The command parsing, filtering and recording modules are designed and implemented, which can ensure the legality of the operation and maintenance personnel to execute commands and limit their illegal operations. The replay and monitoring modules allow auditors to review the entire operation and maintenance process of personnel. In general, the system realizes the management and control of internal personnel's operation behavior, and ensures the internal security of the enterprise information system.

References

[1] Kevin R. F, W. R. (2012) TCP/IP Illustrated, Volume 1: The Protocols. China Machine Press, Beijing.
[2] Christos Douligeris, Dimitrios N. S. (2007) Network Security: Current Status and Future Directions. Wiley-IEEE press.
[3] Andrew S. Tanenbaum. (2003) Computer Networks 4th Edition[M]. USA:Prentice Hall.
[4] Libssh Library. (2021) Libssh. https://www.libssh.org.
[5] Bolthouse, David (1996). Exploring IBM client/server computing. Business Perspective Series. Maximum Press.
[6] Zhang, Y. (2005) Linux Pesudo terminal device and its application in L2TP. Computer Engineering and Design. 07: 1955-1957.
[7] Zheng. L. (2013) The SSH Protocol Audit System Based on Proxy Technology. International Conference on Computational and Information Sciences. Hubei. 1489-1492.