

Research and Implementation of RDP Proxy Proxy-based Audit System

Xiao-Liang ZHANG¹, Xiao-Yu WU², and Wu-Xia ZHANG³

^{1,2,3} School of Computer Science and Technology North China Electric Power University Beijing, China

¹zhanghino@126.com

Keywords: RDP protocol, The agency agreement, The audit system, The operation playback, Security.

Abstract. Using the Windows RDP protocol developed by Microsoft Inc to connect and operate the remote machines which base on the same system become a trend. However, the RDP has caused many security problems. It is necessary to design and implement a audit system to ensure the system's security and guarantee the machines run correctly. It points out improper methods than before and accomplishes the RDP proxy proxy-based audit system to solve the problems.

Introduction

The expansion of Business Scale have a influence on the working place and implementation in the different workplaces. The operator operate the remote servers in accordance with RDP protocol. RDP provides a graphical interface to help the maintain staffs interact with the remote server system. In comparison to the former, the operations become easier and the efficiency of workers' operation become better[1]. Using the remote desktop client we can connect any server that support the remote control and can decrease the workload. Remote desktop procedure just convey the information of the user's mouse, keyboard and other device to the remote server system and never involved in the data processing, so that the level of hardware requirements commonly. It is a kind of the Gospel for the users.

Currently, RDP is the most popular graphical remote access protocol in the market. Comparing with other protocols, RDP was initially used in the Windows Ins interior and was not publicly released details about themselves, and the implementation procedure of RDP has been a trade secret. Fortunately, the Ins has disclosed the detail about the protocol now. As a kind of terminal services network protocol, RDP adopt the typical C/S architecture. The client runs on the local machine, and the server-side on the remote server machines [2]. With the widespread use of the RDP protocol, it not only apply to the server machines which based on the Windows system, but also fits the Linux system. There are many Linux clients providing remote desktop control, such as Winconnect, Linrdp, and Rdesktop.

The Agent Technology is a kind of special network service, that allowing one network terminal typically represent the client connect the other network terminals typical represent the service indirectly through the service[3]. The agent technology usually apply to the fortress parts in the entire system. The fortress between the client and the server, and consists of the agent client and server. First, the client establishes a relationship with the server, then according to the content of the protocol adopted by the agent server, requesting a connection with the target server or obtaining the source which the target server specifies(for example: documents)^[4].

The agent records the client's requests and the server's feedback, and offers data for the maintain system to audit. At present, the agent maintain the system's operations which record int the logs through audit techniques, then finds the illegal operations or analysis the logs to conclude the reason why the application system crashed. However, this way can not provide a direct manner to audit the system, and it is difficult to guarantee the logs's security [5].

Under the background of this topic in the above requirements and the research. Basing on the RDP protocol and agent techniques and by means of the audit session, it is extremely urgent to design and implement a remote desktop audit system.

The Key Technology Research

A. RDP Protocol Analysis

Followings are the several important points about RDP protocol:

Based on the TCP Protocol:

Based on the strength of TCP protocol, the RDP protocol can avoid the packet loss problem.

Data Encryption

According to the RDP protocol rules, before transfer the data are encrypted from one point to another and thus avoid criminals to intercept the plain text.

Multi-Channels

When using the remote desktop to connect the target, both of the clipboard in the desktop can be used mutually, even copy the files from virtual desktop to the physical machine. Generally the protocol open many channels to implement different functions during the operation time. According to the format of RDP we can see, its each channel has a unique id to identify itself. The id consists of a field of 16 bits and uniquely for the channel.

Based on the Graphic Command

Based on the remote display graphics protocol, the RDP realize the graphic data transfer through frame buffer[6]. Due to the huge graphic date, the data need to compress or filter when transfer. The RDP fits the follow steps and finally successfully guarantee the efficiency of data transmission[7].

General Principles

The designer who designed the protocol tried their best to reduce the transmission of traffic.

The application layer prepared the data entirely, and then delivered the data to the next layer to encapsulation. According to the protocol rules, adding data to the both ends of link layer of the corresponding information. As other network protocols, at initialization time of the RDP, the next layer start to initialize and the formal layer come to connect through the pipes which have been built.

Based on the Hierarchy Protocol

The RDP protocol consists of five layers, such as network connection layer, ISO data layer, virtual channel layer, encryption and decryption layer and function data layer^[8]. The function of each layer show in the following table 1:

Table 1. RDP protocol hierarchy

name	function
Network connect	Define a complete and logical package of RDP data, in order to avoiding the network package data losing because of the packet are so long.
ISO data layer	To ensure the connection of RDP data communication normal.
Virtual channel layer	Above the ISO data layer, a virtual channel layer defined by RDP protocol, in order to divide the virtual channel by the different data, to speed up the client's procession and save time avoid to occupy the network interface.
Encrypt decrypt layer	To encrypt or decrypt data about all the functions.
Function data layer	Processing data from all the functions, such as data processing function, image information functions, local resources transformation , voice data and print data. Dividing into different layers accord to the data type.

B.System Design

The Design of Overall System Structure

The function of the system structure as shown in the figure below. The whole system is composed of three parts, including WEB page management module, RDP agent module and maintain operation replay module. Besides, the WEB module and proxy process are deployed in the Linux Centos system[9].Based on Windows system the playback function module usually are deployed in the auditor's local machine.

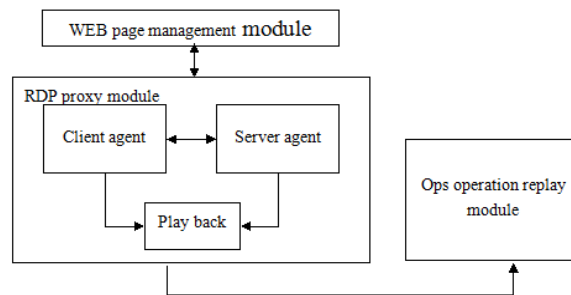


Fig.1 Overall system structure design

RDP Proxy

The RDP proxy is composed of three parts, the RDP proxy client, RDP proxy server and data storage module.

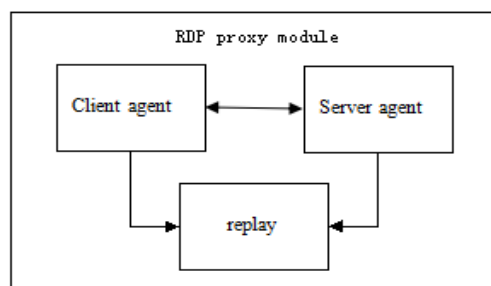


Fig.2 RDP agent module diagram

1.RDP Proxy Client

The RDP proxy client's main functions lie in the following aspects. One receives the user's data packets that proxy send, one connects the target server and sends the data packets to the destination, and the other store the content and audit later.

2.RDP Proxy Server

The main function about RPD proxy server receives the data from users, transfers the packets to the RDP proxy client, and waits the agent client return message.

3.Data Store

The main function of this part store the message which are analyzed by the RDP proxy client and server[10]. The type of storing is a kind of file which can playback through video player.

The RDP proxy is layered[11], and each level has its special functions, as shown in the figure below, and each layer at the location in the agent.

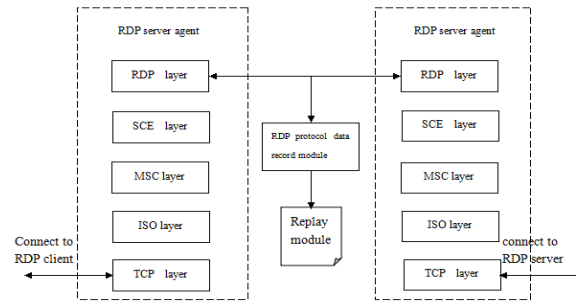


Fig.3 RDP agent general structure

Implementation

The RDP Agent Module

The RDP proxy consists of three parts, the main program Rdpdproxy[12], the RDP proxy library Librdpproxy. The basic library also named Libcommon. so. Besides, the Rdpdproxy is the main program in the agent, makes up the main body of RDP agent framework. In the agent, there is a monitor thread and many connect threads. The function of the connect threads is to resolve the problems between the client and server, at the same time to deal with the data transfer[14]. After the connection, keeping the connected status. The RDP proxy stack consists of two parts, the server protocol stack and the client. The server protocol stack aims at the basic library between the Rdpdproxy and Librdpproxy. so, while the client protocol stack to solve the communication problems between the client and server. The library Libcommon.so is the basic library for the main program, because it provides the threading encapsulation, signal encapsulation and socket communication, and supply service for the other parts.

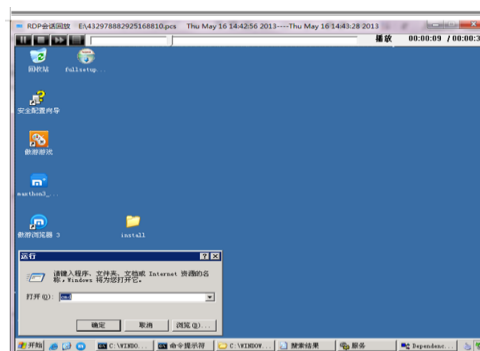


Fig.4 RDP agent rdpproxy overall flow chart

The Realization of Rdpdproxy. The main thread in the Rdpdproxy is used to monitor whether exist connections from client, if client want to connect to the server, after identifying the client and agree the client's request, the server allow the request and

create thread to process the connection. The connection thread acquire the socket from the client, which is usually called `ser_sock`, then call the stack processing library that is `librdpproxy`. so to initialize the connection function for the client. After the initialization, call the function `rdpproxy_connect` to deal with the connection of server. The return from the function is named `socket`, also called `client_sock`. At the end, the connection program has finished the duty to initialize the connection between client and server. Transferring data between client and server will be remain.

Judging whether the client transfers data to the server, if dose, call the `librdpproxy`. so functions to process, if not, jump to the next step. Judging whether the server transfers data to the client, if dose, also call the functions, if not, sleep the thread and repeat to judge. It means the thread is running all the time to monitor whether there is a transfer data between the client and server. The whole process as shown in the figure below:

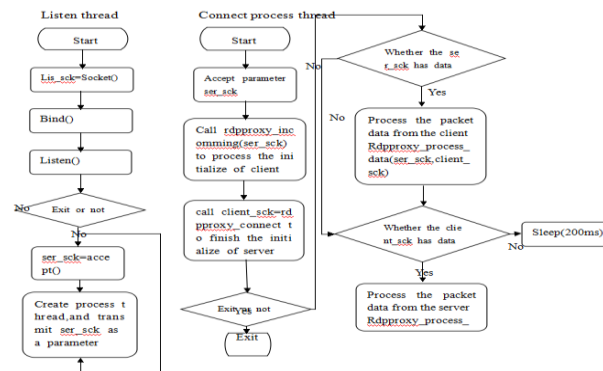


Fig.5 RDP agent rdpproxy overall flow chart

The Playback Module

Based on the Windows system, the video playbacks the file to store the operations by the maintain stuffs, then provide an intuitive way to the auditors for auditing operations. Following the table shows the file header.

Tab.2 Playback File Header Format

0	31
version	
start_time(s)	
...continue	
start_time(s)	
...continue	
end_time(s)	
...continue	
end_time(s)	
...continue	

The table shows the file header, and under the version number is the start and end time which are alternating.

The playback program composed of three threads, are the main thread, drawing thread and time control thread. The main thread creates windows and all kinds of buttons, also creates the draw thread; the draw thread is responsible for reading the playback commands and drawing in the windows, finally, creates the time control thread; the time control thread set the trigger cycle and the perform which need being triggered timer processing routines.

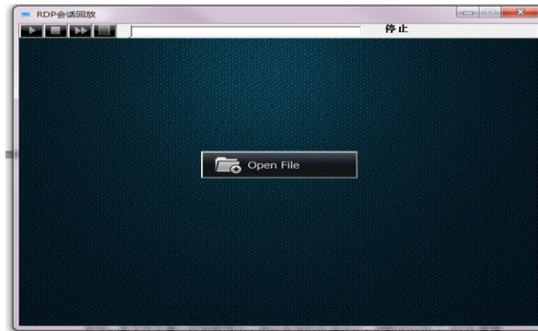


Fig.6 Playback Program Rendering

Conclusions

The paper aims to research the RDP protocol which is used frequently in the remote log and access process, and adopt a systematic study for this parts, hierarchy structure of RDP protocol, connection initialization, connection status keeping and graphic data transmission and so on. Based on a deep learn about the work principle about RDP protocol, designing and implementing a RDP audit system which based on the agent techniques. The system includes WEB management module, the RDP proxy and video playback part. The research focus on the RDP protocol theory and the audit system's design and accomplish.

- 1) Researching the RDP protocol deeply.
- 2) Designing the WEB and implementing the functions.
- 3) Designing the RDP proxy programs and finally accomplishing the functions

Although this article has learn the RDP protocol deeply, but still can't display all of the comment about the protocol, and there are some parts have not been researched. For the RDP proxy, there are many shortcomings, and the audit system's safety level is not the highest compare with other mature products.

Acknowledgment

This work is supported by "The Fundamental Research Funds for the Central Universities 2015MS34"

References

- [1] Chen Yanjun, Liu yan, Chen Yinyin etc. Instruments of remote desktop base on the IPV6 system circumstance. Computer knowledge and techniques, 2012.8;
- [2] Wang yue, The RDP protocol security analysis and middle attack[j]Beijing: Beijing university of posts and telecommunications. 2008.
- [3] Wikipedia. Agent server [http://zh.wikipedia.org/zh/agent server](http://zh.wikipedia.org/zh/agent%20server). 2008. 10.
- [4] Wikipedia. Agent server [http://zh.wikipedia.org/wiki/agent server](http://zh.wikipedia.org/wiki/agent%20server). 2008. 10.
- [5] Lin Yishui, a kind of implementation method based on Java proxy server functions. Information security and techniques. 2013. 4(5): 59-62.
- [6] Tan Z, Wu X, Wen Q, et al. Design and Implementation of proxy-based SSO and security audit system for remote desktop access[C]. Advanced Intelligence and

Awareness Internet(AIAI 2010), 2010 International Conference on. IET, 2010: 341-344.

[7] Ikawa K, Akada K, Morikawa N. Development of a pharmacokinetic analysis program based on nonlinear least square method available in Microsoft Windows XP(MULTI-Win)[J]. Japanese Journal of Pharmacy and Health Care Sciences, 2004, 30: 438-444.

[8] Rdesktop: about A Remote Desktop Protocol Client Proxy [J/OL]. <http://www.rdesktop.org> 2011.08.

[9] Winrdesktop: A Remote Desktop Protocol Client for windows[J/OL].

[10] Roland M. RSC-Remote System Controller[J].

[11] Microsoft Corporation. Remote Desktop Protocol 8.1 Update for Windows 7 SP1 released to web [J/OL]. <http://www.winrdesktop.org>.

[12]Xrdp. A Remote Desktop Protocol Proxy[J/OL]. [http:// github.com/ FreeRDP/ xrdp](http://github.com/FreeRDP/xrdp).

[13] Wang Dong. The fortress machine system to solve the technology risk management of internal control[j]. Financial technology era.

[14] Zong Bo. Analyses the fortress machine concept and work principle[j]. Computer CD software and application. 2012. 18: 070.