A Brief Analysis on the Measurement of Network Sniffer

ZHANG Hao[1]
Tongling College Anhui, Tongling, 244000
hao19825@tlu.edu.cn

ZHANG Lin[2]
Dept. of Computer Science and Technology
AnHui SanLian University HeFei,AnHui, P.R.C., 230000
sirenrabbit@sina.com

***Abstract*—The network wiretap biggest challenge to the network safety. Chaperonage network technique of continuously development, make ether net safety problem research more and more importance, involve a network safety the realm have many safety technique, but these technique of realization all demand depend on a network data pack to succeed in catching. The network wiretap checks a side technique to discover wiretap behavior in time and stop wiretap of further development, decrease customer loss. This text to under the system of the data pack succeed in catching a technique to carry on a research, and put forward a few data pack of succeeds in catching a method.**

Keywords—network wiretap, discover wiretap, network safety

I. Introduction

Computer network security, meaning the network system hardware, software and data information can be protected, keeps the network service not to be interrupted, destroyed or changed by accident or malicious reasons. With the rapid development of network technology and the age of the Internet coming, the security of network and information is increasingly emerged, which more and more are concerned. In this context of the recent network security problem, there are many network security technologies have been applied for solving these problems, such as network intrusion detection, network security scanning, and protocol analysis, etc. The primary task of these safe systems is to collect data and information sources by capturing the network data packet. Network packet capture technology can capture all or specific network packets information from the network for the corresponding network security system operating. Which also involves network address and port transformation problems. The article presented here will give a attention of these problems mentioned above, and try to analyses Ethernet Packet capture technology.

II. The Operating System to Provide Network Capture Mechanism

A. SOCK PACKET

SOCK PACKET is a socket type, which is one of the Linux socket types, can receive all data packets of the network. SOCK PACKET is implemented by using Application Programming Interface provided by the operating system. The main purpose to apply the socket is to access the network data link layer.

B. Data Link Provider Interface（DLPI）

Data Link Provider Interface[2], a standard interface between data link providers and users, defines the service which is from the data link layer to the network layer. The data link users can be the applications of the users, also can be the high-level protocol that can access data link service, like TCP|IP etc.

C. Berkeley Packet Filter（BPF）

Berkeley Packet Filter（BPF）[3][5] is a efficient mechanism to capture specific packets. It works in the kernel layer of operating system. BPF mainly consists of two parts: the Network Relay part and the Packet filtering part. According to specific filtering rules, Packet filtering part keeps part of network packets for normal network switching, and the other part is filtered. The two parts, which work in the kernel layer, offer the filtered packets to application layer. Therefore, the process of capturing and filtering data packets is completed in the kernel layer. And Hierarchical Caching is used to cache capturing data packets in the kernel layer by BPF. when they achieve a certain amount, these data packets will transfer to application. In this way, it increases the processing efficiency greatly.

III. A Few Network Data Packs Succeed in Catching a Technique

A. Libpcap

Libpcap (the Packet Capture Library), with a independent platform, has nothing to do with operation system platform. It can access to the network link layer, and reads the data of link layer independently, so it is the most used network packet capture technology. Libpcap, as a high-level programming interface, can hide the details of the operating system，also can capture any packets of network including the packets that get to other hosts. Libpcap used the BPF filtering mechanism, and supports DLPI and SOCK PACKET[4], It can filter useless packets, and capture the packets users are interested in. Using Libpcap can save filtered data packets in particular documents, also can read the packets information from the file at any time, and the results is completely same as the data from the captured network packets.

The specific working process of Libpcap, as shown in figure 1.

Published by Atlantis Press, Paris, France.

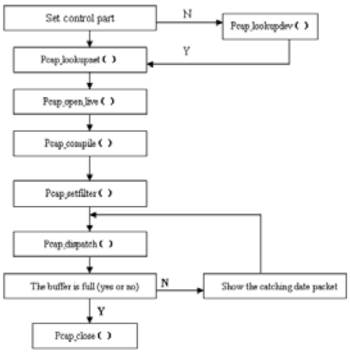

Figure 1 Libpcap Succeed in catching the workflow of function database

When the network port for monitoring is not set, also it finds several network ports, Libpcap will choose the smallest sequence number port to operate. If the network interface is specified, the system will transfer the interface directly to the application.

To sum up, Libpcap can：

- The primary function of Libpcap is capturing network packets, which is a professional function library of capturing network packets. Using Libpcap can convenient to capture the network packets, also the operation process is simple and effective. The data packet can be analyzed in different ways.
- There is a network packet filter module in BPF, which can filter different packets. The module works in the kernel layer, also the BPF filtering rules is optimized, so the efficiency is high.
- After capturing the data packets, Libpcap will analyse them. Using Libpcap can simplify the operator work, as Libpcap provides internal analysis function. Although the data packet captured by Libpcap is a kind of bytes stream information, it provides its basic information, such as time, length, etc. Developers can do further analysis based on these information. It is also the primary work the developers should do.
- The captured data packets can be stored, and do not have to be analyzed immediately. Libpcap provides packets storage function, it will store these captured packets in the computer hard drive. The users, who need the data packets, will read the packets and then do further analysis. These data packets will not be changed.

B. *Winpcap*

Winpcap(Windows Packet Capture) is designed for Libpcap capturing data packets under the Windows platform. They have a same interface, and the user just needs to call corresponding function.Winpcap mainly consists of three parts [2][3]:

First part: It is Net group Packet Filter (NPF) of Kernel Layer, which is the core part of Winpcap, could be considered as Berkeley Packet Filter (BPF) used by Libpcap. Its main functions are capturing, sending, and storing data packets, also accounting, analyzing the network. So BPF can realize the statistical functions of Kernel Layer, and complete capturing and filtering the network packets efficiently. The working principle of NPF is basically same as said above BPF's, which is a capturing mechanism evolved from BPF. This Filter is actually a driver.

The second part: Dynamic link library--packet.dll, it offers a interface to the developers. By using this interface, which is just a lower level interface, can invocate the function of Winpcap directly.

The third part: Dynamic link library--wpcap.dll, it offers a interface to the developers as well, but it is a higher level interface. Call of this interface has nothing to do with the system. Because it is designed based on Libpcap, its function of call is almost completely similar to Libpcap, function name and the definition of parameter are also similar.

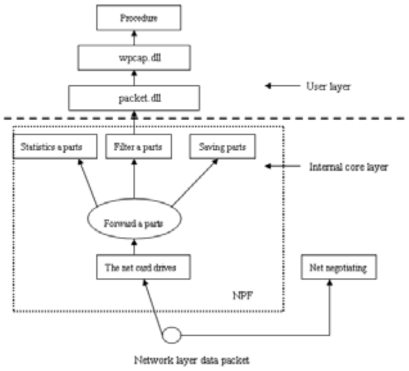

Figure 2 Winpcap Succeed in catching the workflow of function database

As shown in the above picture, network driver gets data packets directly from the network link layer, and eventually transfers to the application in user layer without any modification during the process of counting, storing, and filtering these data packets. Low-level dynamic linking data is isolated from the kernel layer to make the application operate in different Windows systems without any modification.

The benefits of using Winpcap:

- Winpcap provides the programmer a complete set of programming interfaces to capture network packet. Also as Winpcap can be compatible with Libpcap, many security procedures of Libpcap can be directly transplanted to the Windows system.
- Given optimizing all sorts of performance, Winpcap captures and filters the data packets in kernel layer. It promotes the efficiency on this application, and all of this is done by NPF.
- Winpcap also provides a powerful capacity for sending data packet. It promotes the efficiency on packet transmission. Winpcap makes the detail analysis to these packets in the process, and the packets can be distributed clearly to the link bases to intensify the reliability of the application.

ACKNOWLEDGMENT

This paper mainly discusses the network monitoring process of Winpcap I owe my sincere gratitude to Teacher Chen who gave me his help and guidance.

REFERENCE

[1] Chen Yanfeng.Visual Basic database item the case navigate[M].Peking:Chin Hua university publisher, 2004.

[2] Yao Xiaolan.The network safety manages and technique protection.Peking:Tech university publisher in Peking, 2002:pp47-99.

[3] [USA]Roberta Bragg, Keith Strassberg.Network safe complete hand then.Electronics industrial publisher, 2006

[4] Shao Bao,Wang Qihe network safe technique and application[M].Peking:Electronics industrial publisher, 2005:pp105-144

[5] Li Siqi,Weng Yang.The way of safety-the Internet safety set up a depth application.Peking:Electronics industrial publisher, 2006:pp46