Design and Implementation of office automation network security system

Tianwei Nan*
China Railway First Survey And Design Institute Group Co.,Ltd., xi'an 710043, China

*Corresponding author: tianweinan@crfeb.com.cn

Abstract. Socket based network communication is a flexible, easy to implement, low cost method. It can run on a variety of networks that use THE TCP/IP protocol as the communication protocol. So the design in VC++ environment, through the Socket to establish the original Socket, monitoring network traffic, and suspicious data through Access database records, to provide reference for administrators, so as to achieve network security.

Keywords: network traffic monitoring; Network security; The Socket; The Access.

1. Introduction
With the popularity of computers and the rapid development of the Internet, our daily work and data transmission are put on the Internet for transmission, improve the efficiency, reduce the cost, and create a good benefit. However, because of the important security problems of Internet network protocol, there are huge security risks in the transmission of information on the Internet.

2. Fundamentals of Network Monitoring
Know all communication in Ethernet, is broadcast, that is usually in the same network segment of all network interfaces can be accessed in the physical media transmitting all the data, and each network interface has a unique hardware address, the hardware address is the network card MAC address, most systems use 48 bits address, this address is used to represent each device within the network, generally every piece of MFC address on the card is different, each network card manufacturer to get a address, and then use this address assigned to the production of each network card address.

Under normal circumstances, a network interface should respond to only two data frames: the one that matches its own hardware address. The second is broadcast data frames to all machines.

In an actual system, data transceiver is accomplished by the network card, network card to receive data transmission, monolithic applications within the network card MAC address, the purpose of receiving data frames according to the nic driver on the computer to set the receive mode should judge, think the receiver will receive after the interrupt signal to CPU, that shouldn't receive lost no matter, so shouldn't have received data card truncation, computer don't know. CPU gets interrupt signal to produce interrupt, the operating system will call the driver to receive data according to the network card interrupt program address set by the driver of the network card. The driver receives the data and puts it on the signal stack for the operating system to process.
From the sender's point of view, when a computer wants to send data, the data will be gradually shaped into network data frames during the transmission process from the application layer to the physical layer, and then sent to the network line through the network card. The network line will reach their destination machine, and the opposite process will be performed at one end of the destination machine. From the receiver's point of view, the network card generally has four states of receiving data frames:

(a). A single. In this mode, refers to the network card at work, only receive data frames in the destination address is the local MAC address data frame.
(b). The radio. The network card in this mode can receive the broadcast information in the network.
(c). Multicast. The network card set in this mode can receive multicast data.
(d). Mixed. A network card in this mode can receive any data that passes through it, regardless of whether it is passed to it or not.

Normally, a network card simply receives data packets, broadcasts, and group broadcasts sent to it. The reason is that an Ethernet card has a built-in filter called a packet filter, which ignores packets that do not belong to it. In other words, it ignores packets that do not belong to the MAC address. But the sniffer can turn off this hardware feature and set the Ethernet card to "hybrid mode." In other words, it does not do any packet filtering, so that all packets passing through the network can enter smoothly, and be captured and recorded.

3. TCP/IP protocol family

The OSI model divides the network into seven layers, which are respectively used to realize different functions at each layer: application layer, presentation layer, session layer, transport layer, network layer, data link layer and physical layer. And also follow the seven layers of the TCP/IP system standard, but in some the compression on the OSI function, the presentation layer and session layer merging into the application layer, so we actually deal with TCP/IP just five layer, on the network layered structure determines the distribution of protocol in each layer and the realization of functions, thus determines the layers on the use of network equipment.

TCP/IP protocol is actually a complete set of network protocols on a physical network. TCP provides transport layer services and IP provides network layer services. TCP/IP includes the following protocols:

- IP: Internet Protocol is responsible for routing data between hosts and storing data on the network. At the same time for ICMP, TCP, UDP provide packet sending services.
- ARP: Address Resolution Protocol This Protocol maps network addresses to hardware addresses.
- RARP: Reverse Address Resolution Protocol This Protocol maps hardware addresses to network addresses.
- ICMP: Internet Control Message Protocol This Protocol handles custom and host error and transport Control.
- TCP: Transmission Control Protocol is a reliable, full-dual I-stream connection-oriented Protocol for user processes. It provides virtual circuit services for user processes and establishes checks for reliable data transmission.
- UDP: User Datagram Protocol is a connectionless Protocol provided to User processes to transmit data without performing correctness checks.
- FTP: File Transfer Protocol allows users to communicate with another host in the form of File operations (File addition, deletion, modification, search, Transfer, etc.).
- SMTP: The Simple Mail Transfer Protocol (SMTP) Protocol transfers E-mail between systems.
- TELNET: TELNET Terminal Procotol allows the user to access the remote host in virtual Terminal mode.
- HTTP: Hypertext Transfer Protocol.
- TFTP: Trivial File Transfer Protocol.

The HIERARCHY of the TCP/IP protocol family is shown in Figure 1:
4. Database design principles
The goal of database design is to fully meet the business data storage requirements. If a reasonable database model can be designed, it will not only reduce the difficulty of program programming and maintenance, but also improve the performance of the actual operation of the system. Therefore, it is necessary to carefully formulate the design step scheme, understand the design method of the specification and the necessary rules.

A successful management system is composed of: [50% of the business + 50% of the software], and 50% of the successful software is composed of [25% of the database +25% of the program], the quality of the database design is a key. If you compare enterprise data to the blood of life, then database design is the most important part of the application.

For network traffic monitoring management system, has a large number of online personnel need strong database support, but for the system, due to not run in a real environment, so the use of the database can choose easy to use, and easy to maintain, easy access to the database as a background to store information such as Internet cafes database eventually chose to support database as the background.

5. Conceptual structure design
E-r model and relational model are two different descriptions of database. In e-R model, entity sets and relationships are used to represent things in the real world and their relationships with each other. In a relational model, data is organized in a single structure. So, here is the problem of how to turn the E-R model into a relational model. Here are a few guidelines to follow for conversion:

(A). Each entity in the E-R model is transformed into a relationship of the same name, the attributes of the entity set are the attributes of the relationship, and the codes of the entity set are the codes of the relationship.

(B). Each association in the E-R model is also represented as a relationship, and the code of the set of entities associated with the association and the attributes of the association are converted to the attributes of the relationship. The code for this relationship has three cases:
   (a). If the association is 1:1, the code for each entity is a candidate code for the relationship.
   (b). If the relation is 1: n, the code of the relation is the code of the n-terminal entity set.
   (c). If the relation is M: n, the code of the relation is the combination of the code of each entity set.

(C). Relational schemas with the same code can be merged (merge principle).

Here we are going to design the conceptual schema for the database. Based on the analysis of the data flow diagram and data dictionary, we can determine the relationships among the entities, attributes, and entities in the application, as shown in Figures 2 and 3 below.
The design of logical structure is divided into three steps:
(a). Transform the conceptual structure (E-R diagram) into a general relational model;
(b). Transform the converted relational model to the data model supported by Microsoft Office Access 2003;
(c). To optimize the data model, eliminate redundant fields, and minimize processing, the Install information table is shown in Table 1.

| Field   | Data type | Null/primary keys are allowed | Describe                |
|---------|-----------|------------------------------|-------------------------|
| num     | Number    | NO/primary key               | Log rule number         |
| sourceip| Text      | YES                          | The source IP address   |
| sourceport| Text     | YES                          | Source address port     |
| destip  | Text      | YES                          | Destination IP          |
| destport| Text      | YES                          | Destination address port|
| level   | Text      | NO                           | Hazard rating           |
| introduce| Note     | YES                          | Introduce                |

6. Conclusion
This paper introduces the whole process of designing and implementing a network monitoring system under VC++ platform. Through the analysis of more popular network monitoring system development
technology, the characteristics of the system, based on the socket using VC++ development tools to achieve the network monitoring system solution. The intelligent management system design method based on VC++ has a clear design process and a clear hierarchy, which is conducive to the expansion and upgrade of the system and the maintenance and testing of the system.

Reference
[1] Jia Zhiqiang. Network Traffic Monitoring Technology based on TCP/IP [J]. Journal of Shengli College, China University of Petroleum. 2007,(01) : 40-42
[2] Peng Jian. Strategies to Prevent IP Address misappropriation in campus Network [J]. Journal of Changsha Jiaotong University. 2005,(02) : 21-48
[3] Zeng Guangde. Realization and Prevention of Network Monitoring Detection [J]. Journal of Guangxi Youjiang Normal University for Nationalities. 2004,(06) : 34-36
[4] Li Yanyan, Xu An. Sniffing Behavior and Defense Measures in Network [J]. Computer Knowledge and Technology (Academic Communication). 2007,(10) : 65-70
[5] Zhu W. Cluster Queue Structure for Shared-Memory Multiprocessor Systems[J]. The Journal of Super Computing, 2003, 25(3) : 215-236.