Development of a Software Based Firewall System for Computer Network Traffic Control

Okonigene Robert EHIMEN* and Ikhajamgbe OYAKHILOME

Department of Electrical and Electronics Engineering
Ambrose Alli University, P.M.B. 14, Ekpoma, Edo State, Nigeria.
E-mail: robokonigene@yahoo.com

Abstract

The connection of an internal network to an external network such as Internet has made it vulnerable to attacks. One class of network attack is unauthorized penetration into network due to the openness of networks. It is possible for hackers to sum access to an internal network, this pose great danger to the network and network resources. Our objective and major concern of network design was to build a secured network, based on software firewall that ensured the integrity and confidentiality of information on the network. We studied several mechanisms to achieve this; one of such mechanism is the implementation of firewall system as a network defence. Our developed firewall has the ability to determine which network traffic should be allowed in or out of the network. Part of our studied work was also channelled towards a comprehensive study of hardware firewall security system with the aim of developing this software based firewall system. Our software firewall goes a long way in protecting an internal network from external unauthorized traffic penetration. We included an anti virus software which is lacking in most firewall.

Keywords

Internet Security**;** Software Firewall; Computer Network Security; Hardware and Software Security.

Introduction

Computer network is the engineering discipline concerned with communication between computer system and devices. The purposes of networking are exchange of data and resources sharing. With network, large volume of data can be exchanged through both short and long-range connections. Likewise computer resources such as hardware (printers, scanner etc.) and software can be remotely shared among network hosts [1].

With increase reliance on computer network, calls for serious monitoring of the traffic in and out of the system network. Today there are tools for probing the movement of data or information in and out of networks that has given birth to network security threat. The worst situation occurs when the internal computer network is connected to the Internet. Because of the Internets openness, every corporate network connected to it is vulnerable to attack. Hackers on the internet could break into the network and do harm in a number of ways; they can steal or damage important data, damage individuals computer or their entire network, and use the internal network computer resources [2]. Due to some of these security threats, there was the need to build a defensive mechanism that ensures that hackers and their likes are not allowed into the network. Firewalls are defined as a software or hardware device installed at the point where network connection enters an internal network [3]. Sets of rules are applied to control the type of networking traffic flowing in and out of the system. Firewalls are designed to stop unwanted or suspected traffics from flowing into the internal network. This would ensure that hackers have no access to the internal network. Thus, the basic function of a firewall is to regulate the flow of traffic between computer networks of different trust levels. The Internet is a zone with no trust, and an internal network is a zone of higher trust [4]. Due to the expansion of corporate enterprise network to include Internet connections, this has introduced dangers to the internal (organizational) network. Therefore, in this work we carried out comprehensive literature review on how network traffic can be monitored in order to prevent an unauthorized access to internal network. We examined the weaknesses that characterized some of the existing firewall software's. We proposed and developed an improved software based solution that allows all the inbound and outbound traffic to pass through the firewall. The firewall in turn determines which traffic should be allowed in or out of the network. This software, apart from preventing unauthorized access to the network it also detects and prevents virus attack. The use of Java programming language was considered in order to achieve some of our objectives. Firewall security system can be implemented

either by using the hardware based solution or software based solution [5-6]. This study was focused on software-based solution.

Methodology

The packet filtering systems route packets between internal and external hosts, but they do it relationally. They allow or block certain types of packets in a way that reflects a site's own security as shown in Figure 1. The type of router Firewall used in a packer filtering firewall is known as a screening router.

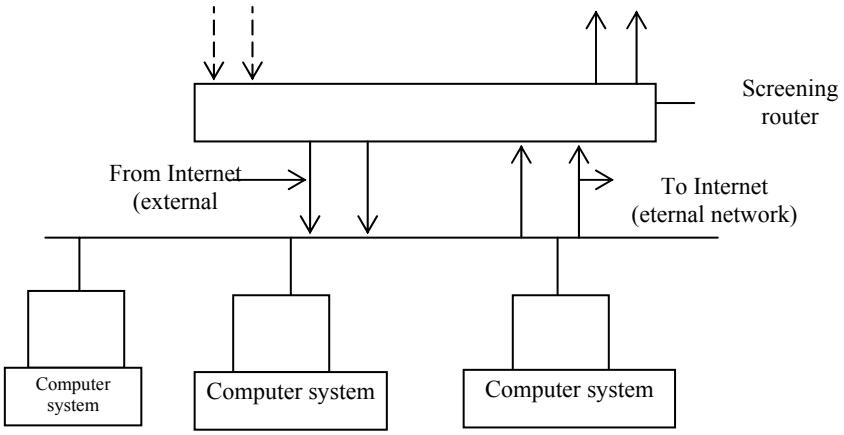

Figure 1. Using firewalls to do packet filtering

Every packet has a set of headers containing certain information. This information is highly essential to the router and it includes; IP source address, IP destination address, Protocol (whether the packet is a TEP, UDP, or ICMP packet, TCP or UDP source port, TCP or UDP destination port, and ICMP message type.

Most of the existing firewall systems are implemented on hardware, that is, they are hardware based. Because of the hardware platform, the firewalls have the following shortcomings: they are very expensive; being hardware based, most of the firewall requires extensive configuration procedure; Network administrators are specially trained to handle the firewall system; each vendor has specific configuration procedures for their firewall systems. The implication of this is that the knowledge in one firewall system may not be applicable in another system; most of the hardware based firewall system cannot be upgraded. The limitations of the hardware based firewall are reasons for our adoption and the implementation of software based approach to firewall development.

Results

A brief description of our designed software based firewall system for network security is as follows. The software firewall system has the following description; it accepts inbound network traffic and analysis the following: IP source address, Protocol destination address, Protocol (TCP or UDP), and ICMP message type. We applied the policy table probe on the traffic information. The results of the probe were passed into the underlying firewall algorithm that initiated the decision making process. Figure 2 is the flow chart for the firewall algorithm. The process determines whether the inbound or outbound traffic should be allowed or denied. This was dilated for the necessary activities and tasks needed in the creation of the proposed software based firewall system. Also contained in this development was the overview of all the development tools needed in the creation of the firewall system. The importance of each trying to achieve some of the design consideration for firewall system includes: Usability, Robustness, Reliability, Fault- tolerance, Security, Maintainability, and Modularity.

The flow pattern of the firewall algorithm was developed using the following basic steps: ▪ Step 1: Acceptance of the inbound traffic; ▪ Step 2: An analyses of the header information; ▪ Step 3: Load the policy table information; ▪ Step 4: Probe the header information using policy table information; ▪ Step 5: If the validation is true then allow the inbound traffic; ▪ Step 6: If the validation is false reject the inbound traffic.

The same 6 steps are needed to filter the outbound traffic and can be implemented in java language using the procedure below:

```
      Socket sock = new socket ();
      Sock accept ();
      Inbound port = sock IN
      Inbound port = socket port ( );
      File = new file ((“policy table”)”txt”);
      Buffer sb = new Buffer (file);
      If (inbound port equals (sb));
{system out port (“connection accepted”)
} else {
      system out port (“connection rejected”) }
      sock. Close ( );
```

The firewall software is compactable with the following operating system; Windows 2000, Windows XP, and Windows Vista. The installed java virtual machine (JVM) requires java runtime environment (JRE) in the range JRE 4.0, JRE 5.0 and JRE 6.0.

After the installation of the firewall software the next step was to switch to command prompt of the operating system. At the command prompt enter 'Java firewall'. This brings up the application interface where the user can interact with the system.

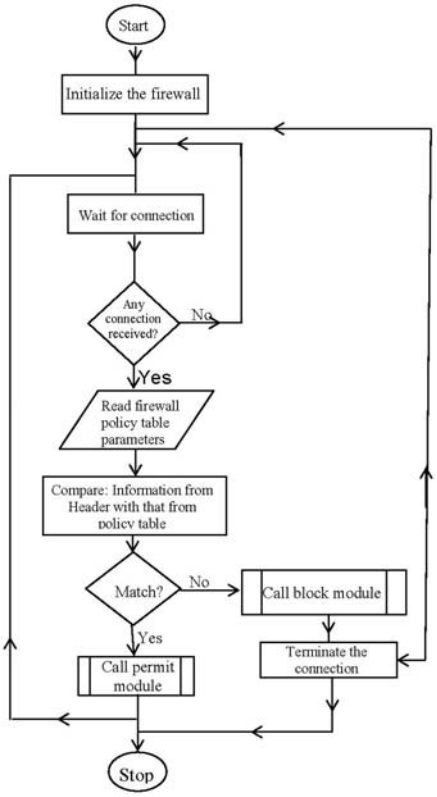

Figure 2. Firewall System Flow Chart

The system interface allows the users to interact with the software. This section gave detailed description of the system that helped to facilitate the effective use of the software. Software based firewall system is a menu driven application, which enables the users to select commands from the menu. The firewall system was composed of two menus namely; Operation and Help. The operation menu contains commands for starting and stopping the firewall system. The two commands cascaded in the menu are: The Start-up command and Shutdown command. The Start-up command starts up the firewall system and prepares it for inbound and outbound connections. All traffics go through the firewall when this command is checked. Furthermore, this command enables the configuration of the firewall IP (Internet protocol) and the firewall port. The firewall listens to connections on the IP and the port. This work is part of a broader ongoing research work. We tested the developed firewall software on 100BaseT Ethernet comprising of sixteen computers. The results were satisfactory. The shutdown command shuts down the firewall. When this is done, traffic does not flow through

the firewall again. At this point, the network becomes an open system without any formal security mechanism.

Conclusions

Information security has become an important concept in any organizations due to the fact that an unprotected information system can be exposed to danger in a network as a result of penetration tools at the disposal of hackers and crackers. Therefore, there was need to ensure adequate protection of internal network from hackers. To achieve this, there are so many tools at the disposal of the network administrator and the security administrator, which include; IPS (Inclusion Prevention System), Firewall Security System and the IDS (Inclusion Detection System). This work focused on the firewall system that filtered what goes in and comes out of the network. It had the ability to block an unauthorized traffic and allow authorized traffic using the IP (Internet Protocol) table. The firewall algorithm was implemented using Java programming language, which was based on java security architecture. It also utilizes the concept of socket programming which enables network communication over the internet. The limitation of this work was the inability of the system to track traffic from dial-up connections. We therefore recommend that future work on this software should solve the problem of tracking down traffic from dial-up connections. The system supports 70 concurrent connections at a time and this can also be improved upon in future software development.

References

1. Kurose J. F., Ross K. IV (20^{th}) Computer Networking: A Top-Dgon Approach, A Press Publication New York.
2. Tamarch D. Network traffic control and management, Boston Massachusetts, 2006.
3. Snikart R. Control Techniques for network traffic, Car bridge University press, 2007.
4. Megn S. P. The Mathematics of network traffic Control-firewall perspective, Birkhauser publishers, Germany, 2007.
5. Dick P. Application of firewall to network security, Pensuin Books, New York, 2001.
6. Pius B. *An effective security control prevent an authorized network traffic*, Journal of information technology, New York, 2003.