ISBN 978-93-5156-328-0
International Conference of Advance Research and Innovation (ICARI-2015)

Developing A Simple Net Shield for Securing Personal Computer Using IP Filter Hook Driver

Sahana Lokesh R [a *], H. S. Saraswathi [b]
[a] Department of Computer Science, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
[b] Department of Computer Science, Jain Institute of Technology, Davanagere, India

Article Info
Article history:
Received 9 January 2015
Received in revised form
15 January 2015
Accepted 22 January 2015
Available online 31 January 2015

Keywords
Net-Shield,
Internet Protocol,
Filter-hook Driver

Abstract

A simple net-shield tool provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted. It differs from a conventional firewall in terms of scale. A simple Net-shield is typically designed for use by end users as a result, a simple Net-shield will usually protect only the computer on which it is installed. A filter-hook driver is a kernel-mode driver that is used to filter network packets. Filter-hook drivers extend the functionality of the system-supplied internet protocol(IP) filter driver.

1. Introduction

Internet is a network of interconnected network with a boundary. Because of this fact, the organizational network becomes accessible and vulnerable from any computer in the world. As companies become internet business, new threats arise from person who no longer requires physical access to a company's computer assets. The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within.The Internet is insecure for a variety of reasons. Those factors include:

- Lack of education
- The Internet's design
- The trickling down of technology
- Human nature

A. Types of Attacks

Before deciding what to do, it is important to understand what types of attacks may occur and how they will affect you and your computer system. The following list (which is by no means complete) gives the general classes of attack along with some common or well- known examples and specific solutions to these problems:

- **External Attacks**

Attacks originating from outside your home or office computer/network

- **Denial of Service (DOS)**

The purpose of this type of attack is not to gain control over your computer, rather it is to prevent anyone from making use of one or more of the services that the attacked computer provides. Some examples include:

- **SYN Attack-** A "SYN" packet is used to initiate a connection between computers using the TCP protocol, it is part of a three way handshake used by TCP to set up a connection. In this attack, repeated "SYN" packets are sent to the computer under attack, the attacked computer sends its response handshake packet, and waits for the final handshake packet from the attacking computer (which never sends it). Each of these incomplete connection attempts ties up one network port on the computer until it times out, if enough are sent before the timeout occurs, the system runs out of ports and/or other resources at which point no one else can connect.
- **Process Table Overflow-** Most computers have some kind of limit on the total number of processes that can be active at one time, in many cases if this limit is ever reached, the system will crash or at least become virtually unusable. One way to do this is to simply establish as many connections as possible to as many different system services as possible. Many standard services will create a new process for each connection, quickly using up all space in the process table.
- **Network/Server Overload-** No matter how fast your connection to the internet is, someone else has a faster one, and if they make requests faster than your server or internet connection can handle them, your site will become virtually unusable to everyone else. Even if the person attacking you doesn't have a faster link, they can use other computers that they have compromised to launch multiple attacks which, when combined, exceed the capabilities of your server.
- **Ping of Death-** This one should be fixed in any computer operating system which has been updated in the last couple of years, but it is a classic example of how easy it can be to knock a system off-line. In this attack, a person simply sent a 64k+ byte "ping" packet to the target system. This would overflow the receive buffer and crash the network link if not the entire computer. On the bright side, for these kinds of attack your data is not in any danger of being stolen or corrupted and in some cases the simplest course if you are not running an E-commerce or other high availability site, may be to just ignore the problem until you get enough attacks to be irritating.
- **Break-in**

Corresponding Author,
E-mail address: sahana.lokesh@gmail.com

The reasons for this type of attack are virtually unlimited; it can be anything from just proving they can break into your system, to revenge.

- **Standard accounts and password scans-** This type of attack simply attempts to log-in using any available login service (telnet, ssh, rsh, etc.) using common account names (root, games, mail, etc.) or the names of users discovered by looking at internet discussion groups, company web sites and other sources. Armed with a potential list of account names, the attacker will use a list of common passwords or simply words from the dictionary in an automated attempt to log-in to the system. A more serious attacker dedicated to breaking into your computer specifically, will research people with accounts on the system and apply birth dates, names of children and other personal information in order to find a working account and password. This type of attack is also a common internal attack, but is even more likely to succeed since personal information is even more readily available to those on the inside.
- **Known bugs, common bugs and security holes-** In this type of attack, the attacker looks for bugs or system security holes in your computer which can be used to gain access. Once they have one of these bugs or holes, it is used to break into the computer.
- **Computer viruses-** Many people today only think of computer viruses and worms as an irritation which may delete files on their hard disk or display silly messages, unfortunately, many of them are very discrete and instead gather information to send out to their originator so that they can better attack your network, or even just install a program to give their originator direct access to your network.

B. Internal Attacks

If you have a large network shared by many people, an internal attack should be a major concern, since most networks are least protected against this. Small or single user networks generally do not give this any consideration at all, but it could be a big mistake to do so. Once your Net-Shield is breached by an outside attack, the next stage of the attack is in fact an internal attack! There are far too many different kinds of internal attacks to list them all here, but some of the more common general approaches include:

- Password Cracking
- Symlink
- Temp file
- Buffer Overflow

Thus to prevent all these types of attacks or to keep the computer safe from all these types of attacks the net-shield is used. Net-shield provides security to the computer by performing several security functions.

2. Net-Shield

Using a simplified definition, a Net-Shield is a tool that implements security policy to Control traffic between two or more networks. A Net-Shield can be a special network appliance or adevice that is configured using a desktop computer, operating system (e.g., Microsoft Windows2000, Sun Solaris, Open BSD, Linux) and a network Net-Shield application.

The Net-Shield performs several security functions. Primarily, a Net-Shield monitors, inspects and controls

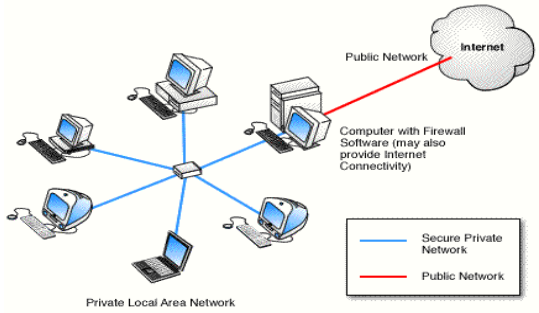

Fig: 1. Computer Running Net-shield Software

Inbound/outbound network traffic. The Net-Shield implements user-defined security policies to determine whether to permit or deny particular network traffic. The security policies define the characteristics of acceptable and unacceptable network traffic based on packet criteria at the IP level and above. Typically, network traffic that or delete information is proactively denied by the Net-Shield represents hostile intrusion attempts, denial of service attacks and/or unauthorized attempts to read, modify or delete information is proactively denied by the net-shield. A Net-Shield examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A Net-Shield filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Net-Shields can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Net-Shields can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependent upon the protocol used, for example HTTP, ftp or telnet. Net-Shields can also filter traffic by packet attribute or state.

3. Working of Net-shield

There are two access denial methodologies used by Net-Shields. A Net-Shield may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of Net-Shield to another.

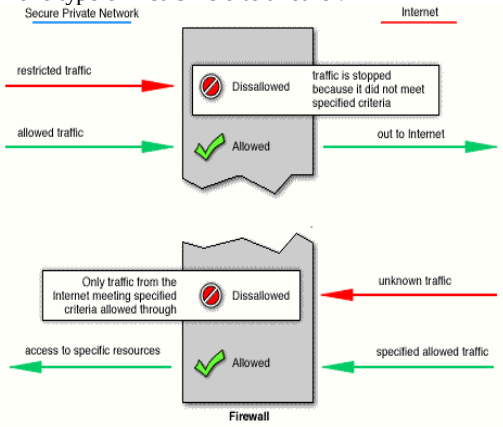

Fig: 2. Basic Net-shield Operation

Net-Shields may be concerned with the type of traffic, or with source or destination addresses and ports. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a Net-Shield determines what traffic to let through depends on which network layer it operates at. The traffic is allowed only if it satisfies the certain criteria or else it is stopped. As the figure shows the restricted traffic is stopped because it did not meet the specified criteria, and in case of unknown traffic only the traffic from internet meeting certain criteria is allowed and the traffic other than that is stopped.

4. Filter-Hook Driver

A *filter-hook driver* is a kernel-mode driver that is used to filter network packets. Filter- hook drivers extend the functionality of the system-supplied Internet Protocol (IP) filterdriver. A filter-hook driver can only be installed on the Microsoft® Windows® 2000 operating system and later versions. A filter-hook driver can only register itself with the IP filter driver if the pointer to the extension hook for the IP filter driver is set to NULL. After the filter-hook driver is registered, the IP filter driver assigns the file object for the filter-hook driver to the extension hook for the IP filter driver, thereby ensuring that it can only accept and use a single filter-hook driver.

A) Implementation of Filter – Hook Driver

In fact, Filter-Hook Driver isn't a Network driver; it is a Kernel Mode Driver. Basically, in this Filter-Hook driver we implement a callback function, and then, we register this callback with the Ip Filter Driver. When we do this, the Ip Filter Driver calls our callback function when a packet is been sent or received. We can summarize then in the following steps:

- Create a Filter-Hook Driver. For this, you must create a Kernel Mode Driver,
- If we want to install the filter function, first we must do it's get a pointer to Ip Filter Driver. So, It will be the second step.
- We already have the pointer, now we can install the filter function. We can do it sending a specific IRP. The data passed in this "message" included a pointer to the filter function.
- Filtering Packets!!!!
- When we decided to finish filtering, we must deregister the filter function. We can do it, "registering" as filter function the null pointer.

B) Create the Kernel Mode Driver

Filter-Hook driver is a Kernel Mode Driver, so if we want to do one, we have to make a Kernel Mode Driver. The structure of the Filter-Hook driver is the typical Kernel Mode Driver Structure:

- A driver entry where we create the device, set the standard routines in order to process IRPs (Dispatch, load, unload, create....) and create the symbolic link for communication with user applications.
- The standard routines to manage IRPs. Implement four IOCTL Codes: START_IP_HOOK (registers the filter function), STOP_IP_HOOK(deregisters the filter function), ADD_FILTER(install a new rule) and CLEAR_FILTER (free all rules).
- For our driver, we must implement one more function: the filter function as explained below.

C) Working of Filter

Filter is the most important part of the Net-Shield. Main aim of the filter is to grab the packet collecting all the header information from the header and to decide whether to leave or pass the packet according to the rules applied. Working of filter is implemented by an important function named as "PF_FORWARD_ACTION cbFilterFunction". This function contains seven parameters as shown under: The callback function looks like this:

```
PF_FORWARD_ACTION
cbFilterFunction (
unsigned char *PacketHeader, // Ip Packet Header
unsigned char *Packet,       // Packet. Don't include Header
unsigned int PacketLength,   // Packet length. Don't Include
                             // length of ip header
unsigned int RecvInterfaceIndex, // Index number for the
                             //interface adapter over
                             // which the packet arrived
unsigned int SendInterfaceIndex, // Index number for the
                             //interface adapter over
                             //which the packet will be
                             //transmitted
IPAddr RecvLinkNextHop,      //IP address for the
                             //interface adapter that
                             // received the packet
IPAddr SendLinkNextHop);     //IP address for the
                             //interface adapter that will
                             // transmit the packet)
```

5. Advantages of Net-shields

Net-Shields protect private local area networks from hostile intrusion from the Internet. Consequently, many LANs are now connected to the Internet where Internet connectivity would otherwise have been too great a risk. Net-Shields allow network administrators to offer access to specific types of Internet services to selected LAN users. This selectivity is an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what. Privileges can be granted according to job description and need rather than on an all-or-nothing basis.

6. Disadvantages of Net-Shields

Net-Shields introduce problems of their own. Information security involves constraints and users don't like this. It reminds them that Bad Things can and do happen.Net-Shields restrict access to certain services. The vendors of information technology are constantly telling us "anything, anywhere, anytime", and we believe them naively. Of course they forget to tell us we need to log in and out, to memorize our 27 different passwords, not to write them down on a sticky note on our computer screen and so on.Net-Shields can also constitute a traffic bottleneck. They concentrate security in one spot, aggravating the single point of failure phenomenon. The alternatives however are either no Internet access, or no security, neither of which are acceptable in most organizations.

7. Conclusion

Net-Shields based on Packet Filters are one of the most powerful and widely used techniques which is used in

networking security. Our Net-Shield is based on this technique but it lags various features in its working. In raw sense it is a complete Net-Shield but considering the modern definition it lacks a lot of features such as

- Content Checking of Packets
- Log Files for later inspection
- Unable to inform the user about any attempt of hack

Since it is able to provide a control to an end user on the traffic on his machine therefore it complies to basic definition of the Net-Shield. The user has the facility to allow only certain packets while denying others. He can use the facility of denying all the traffic and can also allow all the traffic to his computer.

References

[1] Zhichun Li, Gao Xia, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Junchen Jiangand Yuezhou Lv, Net Shield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense, ACM SIGCOMM 2010, New Delhi, India, 2010

[2] Zhichun Li, Gao Xia, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Net shield: Matching with a large vulnerability signature ruleset for high performance network defense, Technical Report NWU-EECS-08-07, Northwestern University, 2009

[3] M. Becchi, P. Crowley. A hybrid finite automaton for practical deep packet inspection. In *Proc. of ACM CoNEXT*, 2007

[4] M. Becchi, P. Crowley. Efficient regular expression evaluation: Theory to practice. In *Proc. of IEEE/ACM ANCS*, 2008

[5] N. Borisov, D. J. Brumley, H. J. Wang, J. Dunagan, P. Joshi, and C. Guo. A generic application-level protocol analyzer and its language. *NDSS*, 2007.

[6] D. Brumley, J. Newsome, D. Song, H. Wang, S. Jha. Towards automatic generation of vulnerability-based signatures. *IEEE Security and Privacy Symposium*, 2006

[7] B. Chazelle. Lower bounds for orthogonal range searching. i: The reporting case. *Journal of the ACM*, 37(2): 200–212, 1990

[8] B. Chazelle. Lower bounds for orthogonal range searching. ii: The arithmetic model. *Journal of the ACM*, 37(3): 1990, 439–463

[9] M. Costa, J. Crowcroft, M. Castro, A. Rowstron, L. Zhou, L. Zhang, P. Barham. Vigilante: End-to-end containment of internet worms. *ACM SOSP*, 2005.

[10] W. Cui, M. Peinado, H. J. Wang, Locasto. Shieldgen: Automated data patch generation for unknown vulnerabilities with informed probing. *IEEE Security and Privacy*, 2007

[11] Sahana lokesh R, Srikanth T N, *Shortcomings of Quantum and the usage of Classical Cryptography: A Review* in proc International Journal on Advance research Innovation, 2015