Packet Filtering Technique for Network Security

T. Divya Rai
Department of CSE
PCEM Bhilai
CG India

Ritu Verma
Department of CSE
PCEM Bhilai
CG India

Abstract— **Packet filtering is a useful tool for the security conscious network administrator but its effective use requires a thorough understanding of its capabilities & weakness & of the quirks of the particular protocols that filters are being applied to.In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. The explosive growth in computer systems and their interconnections via networks has increased the dependency of both organizations and individual on the information stored and communicated using these systems. This has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and to protect systems from network based attacks. A firewall is a security guard placed at the point of entry between a private network and the outside Internet such that all incoming and outgoing packets have to pass through it.**

The paper concludes packet filtering is a viable network security mechanism but that its utility could be greatly improved with the extension proposed.

Keywords- ***Network Security, Firewall, Packet filtering***

I. INTRODUCTION

The rapid increase in internet has connected millions of computers worldwide, in order to communicate with the external world companies need to connect to the internet. The private networks of individual organizations known as Intranet which is a private network have to be connected to the public network i.e. Internet. The individual networks of the organizations need to be protected from public access in order to provide security to their private data. Packet filtering generally is inexpensive to implement. However it must be understood that a packet filtering device does not provide the same level of security as an application or proxy firewall. All except the most trivial of IP networks is composed of IP subnets and contain routers.

How does a packet filter work?

All packet filters function in the same general fashion. Operating at the network layer and transport layer of the TCP/IP protocol stack, every packet is examined as it enters the protocol stack. The network and transport headers are examined closely for the following information.

- **protocol** (IP header, network layer) – In the IP header, byte 9 (remember the byte count begins with zero) identifies the protocol of the packet. Most filter devices have the capability to differentiate between TCP, UPD, and ICMP.
- **source address** (IP header, network layer) – The source address is the 32-bit IP address of the host which created the packet.
- **destination address** (IP header, network layer) – The destination address is the 32-bit IP address of the host the packet is destined for.
- **source port** (TCP or UDP header, transport layer) – Each end of a TCP or UDP network connection is bound to a *port*. TCP ports are separate and distinct from UDP ports. Ports numbered below 1024 are reserved – they have a specifically defined use. Ports numbered above 1024 (inclusive) are known as ephemeral ports. They can be used however a vendor chooses. For a list of “well known” ports, refer to RFP1700. The source port is a pseudo-randomly assigned ephemeral port number. Thus it is often not very useful to filter on the source port.
- **destination port** (TCP or UDP header, transport layer) – The destination port number indicates a port that the packet is sent to. Each service on the destination host listens to a port. Some well-known ports that might be filtered are 20/TCP and 21/TCP - ftp connection/data, 23/TCP - telnet, 80/TCP - http, and 53/TCP - DNS zone transfers.
- **connection status** (TCP header, transport layer) – The connection status tells whether the packet is the first packet of the network session.The ACK bit in the TCP header is set to “false” or 0 if this is the first packet in the session. It is simple to disallow a host from establishing a connection by rejecting or discarding any packets which have the ACK bit set to “false” or 0.

Packet filtering involves parsing the header information of the packets and making decision whether to drop or route the packet. The decision can be based on several parameters. Packet filtering implementations allow the administrator to specify the rules that are to be followed in making the decision. The rules specified by the administrator can be based on either inbound or outbound packets. Ability to specify the rules based on both inbound and outbound packets will give the administrator significant control over the appearance of the router in the filtering scheme and will help filtering on routers consisting of more than two interfaces. Attackers from the outside world can fake the internal source addresses and can claim to be from internal host, to make sure this does not happen the administrator should have knowledge of the source from where the packets are coming, by knowing the interface from where the packet came we can drop all the packets which fake the internal source addresses.

II. STRATEGIES OF PACKET FILTERING

The main advantages of packet filtering are being able to reduce the unwanted packet traffic and to protect from malicious and unwanted use of network sources. Several strategies can be used to implement packet filtering. Some of them are

Routing Table Solutions

In this scheme the decision to route or drop the packet is based on the routing table lookup. The routing table entries decide to which destinations packets may be routed to and to which they are not supposed to. This Solution is helpful when static routes are used. Routing Protocols like RIP are used but these are not secure. Routers can choose from which sources they want to accept the RIP information, this is helpful in preventing incorrect information that was provided accidentally.

Input and Output Filtering

In this scheme filtering is done on the external interface of a network in both input and output directions. By doing this the network security is achieved without slowing down the internal routing in the network.

Source Address Filtering

In this scheme the internal network connections will have one authentication scheme and the connections to the outside network will have another. Internal connections constitute the connections with in the organizations internal address space. If a filter is applied to the external interface that rejects the packets which claim to be from inside but actually are from the outside connection i.e. the source and destination addresses are in the internal address space but the packet arrives from outside the network.

Protocol Port Filtering

In this scheme the destination port is examined to decide which set of destination ports can be accessed from the external network by applying a filter restricting the services that can be accessed from the external network. For example any of the TCP services like SMTP, nntp, ftp-data, ftp, finger, telnet, login and shell can be denied access to the external networks.

Advanced Filtering Strategies

Some Other strategies followed by commercial vendors like Novell in its Border Manager 3.7 are Static Packet Filtering and Advanced features like TCP ACK bit filtering, Dynamic Packet filtering, and Fragmented packet filtering.

Static Packet Filtering

In Static Packet filtering each packet that crosses the border between the internal networks i.e. intranet and the external network i.e. internet is examined. The static packet filter examines the header information of each packet to identify the parameters such as Protocol ID, Source and destinations IP addresses and Port numbers, router interface for the incoming and outgoing packets.

These parameters are examined and then the decision of forwarding or dropping the packet is done following the fixed set of inbound and outbound rules.

TCP ACK bit filtering

In TCP ACK bit filtering only the packets with the TCP ACK bit set are allowed into the network. TCP ACK filtering prevents all the external hosts from initiating TCP connections to internal hosts without authentication.

Dynamic Packet filtering

In Dynamic packet filtering also known as stateful packet filtering keeps track of the outgoing packets which it has allowed passing and allows only those corresponding packets to return. A return filter is dynamically created to allow the response packet whenever a packet is transmitted to the public network .This scheme supports both connection less and connection oriented protocols.

Fragmented packet filtering

Packets are divided in to small chunk called fragments, the first fragment has the complete header information, previously only the first packet was dropped assuming that the following packets cannot be reassembled without the header information, but these subsequent packets can be used to flood the network consuming the bandwidth to avoid this the filtering discards the first packet as well as all the subsequent packets if they have the same source and destination addresses and interfaces.

III. PROBLEMS WITH CURRENT PACKET FILTERING IMPLEMENTATIONS

Packet filtering can be as a tool to improve total network security. An increasing number of IP routers offer this possibility. Packet filtering can be a very secure and useful tool if administrators properly use it. Currently, a number of difficulties arise in the design and implementation in order to make packet filtering firewall secure and efficient.

Some of the problems that need to be addressed are listed below:

- **Wrongly classify:** A packet filter may wrongly classify a packet when the source IP address be spoofed. Filtering based on source port faces similar problem, such as the source machine might be running an unsuspected client or server on that port.
- **Variable header length:** The options field makes the IP packet header length variable. So, locating the higher level protocol information can be difficult, such as TCP/UDP headers, when using simple offset-based pattern matching techniques.
- **Fragment packet :** When a packet is fragmented, some packet filters just drop the first fragment, assuming that the other fragments will be useless to the receiver. However, risks arise here, hackers may find ways to fool the system. However, it can significantly make the packet filtering process complicate.
- **Predefined header fields:** This has severe impact on flexibility. Unless the administrator can specify precisely which header fields are to be used in decision making, the desired security policy cannot be effectively implemented. For instance, one may wish to block packets with TCP “SYN” flag set, but the packet filter may not allow this field to be used for filter specification.

Possible Solutions for Current Packet Filtering Problems:

1) Improve syntax of filter specification
2) Make all relevant header fields as filtering criteria available
3) Allow outbound filters also inbound filters
4) Make developing, testing, and monitoring filters tools available
5) Simplify specification of common filters

Advantage of Packet Filters:

- These firewalls are low cost, have only a small effect on the network performance,
- They do not require client computers to be configured in any particular way.
- Application independence
- Scalability
- Packet filtering is fast, flexible and transparent (no Changes are required at the client).
- They can process packets at very fast speeds.
- They easily can match on most fields in Layer 3 packets and Layer 4 segment headers, providing a lot of flexibility in implementing security policies.

Disadvantage of Packet Filters:

They are not considered to be very secure on their own because they do not understand application layer protocols. They cannot make content-based decisions on the packets. They are stateless and do not retain the state of a connection. They also have very little or no logging capability which makes it hard to detect if the network is under attack. Testing the grant and deny rules is also difficult which may leave the network vulnerable or incorrectly configured.

Applications of packet filtering

A packet filtering device can be the first-line of defense in the network and used to block in-bound packets of specific types from ever reaching the protected network. This is known as ingress filtering. Although not a robust firewall, it can be used to reduce the load on the proxy or application firewall. The following diagram illustrates a simple example of using the packet filter and proxy or application firewall.

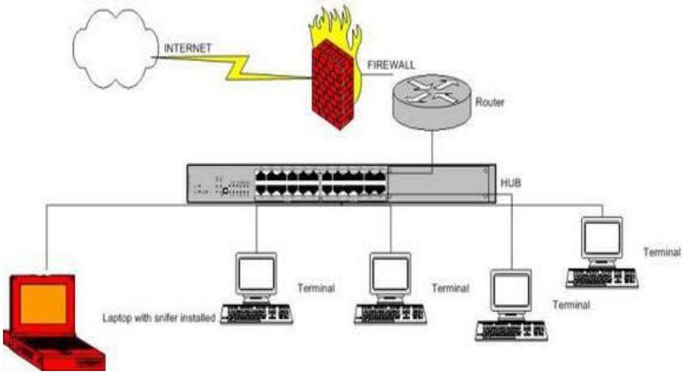

Figure 1. Packet Filtering Firewall

IV. CONCLUSION

A firewall is a security guard placed at the point of entry between a private network and the outside Internet such that all incoming and outgoing packets have to pass through it. In this paper packet filtering firewall has been discussed. How we can define the rule set in packet filtering firewall, how they are work, what are the advantages and disadvantage of the packet filtering firewall. The concepts filtering and classification are generally referenced together. According to specified filter rules, Filtering requires the ability to classify packets. The rules can be viewed as logical] functions on the packet header fields. Classification of packets also arises in other areas of computing, such as routing, policy based routing, differentiated Quality of Service, traffic billing, etc. [Gupta & McKeon,1999]. However, not all of them use classification based on multiple fields in the packet header. Packet filtering is currently Packet filtering is a very useful technique for computer security. Some simple improvements to filter specification mechanisms could greatly make the lives of network administrators simplify and increase their confidence. When combined with other techniques, a very secure system can be developed ..

REFERENCES

[1] M. Bishop, “Early computer security papers, part 1”, http://csrc.nist.gov/publications/history/index.html.1998.

[2] Mohamed G. Gouda, Alex X. Liu Structured firewall design, Computer Networks 51 (2007) 1106–1120

[3] Matt Curtin Introduction to Network Security March 1997

[4] Firewall Architecture Understanding the purpose of a firewall when connecting to ADSL networ

[5] Network (In) Security through IP Packet Filtering D. Brent Chapman (great circle associates) Published in proceedings of the Third USENIX UNIX security symposium, Baltimore, MD; September, 1992.

[6] Novell Border Manager 3.7 Documentation http://www.novell.com/documentation/lg/nbm37/index.html?page=/documentation/lg/nb m37/over/data/ae70ppq.html

Corbridge, B., Henig, R., & Slater, C. (1991). Packet filtering in an IP router