Controlling IP Spoofing Through Inter-Domain Packet Filters

Archana verma
Department of Computer Science Engineering
Parthivi College Of Engineering And Management
Bhilai-3, Chhattisgarh, India

Prerna Dewangan
Department of Computer Science Engineering
Parthivi College Of Engineering And Management
Bhilai-3, Chhattisgarh, India

Abstract — *The Distributed Denial of Services (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge, or spoof, the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, we propose an inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework works correctly in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks.*

Keywords — *Spoofing; IP; legitimate user; PF; Router ; encipher ; DDoS ; malwares ; drive-by-attack.*

I. INTRODUCTION

What is IP Spoofing

IP spoofing is the creation of IP packets using somebody else’s IP source addresses**.** Using one of several tools, an attacker can easily modify these addresses – specifically the “source address” field. A common misconception is that IP spoofing can be used to hide our IP address while surfing the Internet, chatting online, sending e-mail, and so on

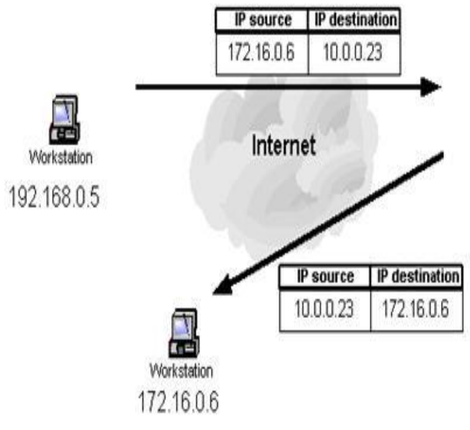

Fig.1.

Valid source IP address, illustrates a typical interaction between a workstation with a valid source IP address requesting web pages and the web server executing the requests. When the workstation requests a page from the web server the request contains both the workstation’s IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address (172.16.0.6) and its own and its own IP address as the source IP address (10.0.0.23).

Spoofed source IP address illustrates the interaction between a workstation requesting web pages using a spoofed source IP address and the web server executing the requests. If a spoofed source IP address (i.e. 172.16.0.6) is used by the workstation, the web server executing the web page request will attempt to execute the request by sending information to the IP address of what it believes to be the originating system (i.e. the workstation at 172.16.0.6). The system at the spoofed IP address will receive unsolicited connection attempts from the web server that it will simply discard

A. Asymmetric routing (splitting routing)

Asymmetric routing means traffic goes over different interfaces for directions in and out. In other words, asymmetric routing is when the response to a packet follows a different path from one host to another than the original packet did. The more correct and more general answer is, for any source IP address ‚A’ and destination ‚B’, the path followed by any packet (request or response) from ‚A’ to ‚B’ is different than the path taken by a packet from ‚B’ to ‚A’.

B. Spoofing attacks

There are a few variations on the types of attacks that successfully employ IP spoofing. Although some are relatively dated, others are very pertinent to current security concerns.

- Blind Spoofing: Usually the attacker does not have access to the reply, abuse trust relationship between Hosts. For example: Host C sends an IP packet with the address of some other host (Host A) as the source address to Host B. Attacked host (B) replies to the legitimate host (A).

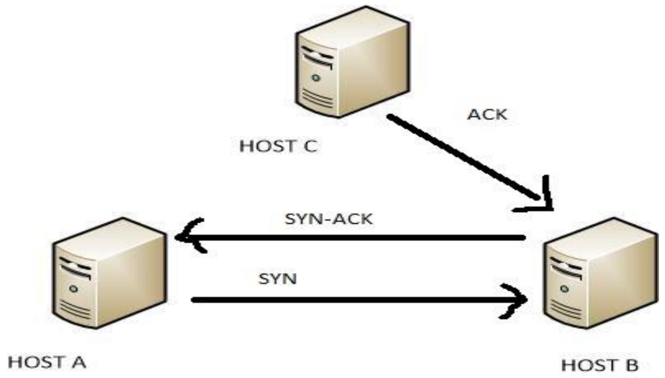

Fig. 2.

- Non-blind Spoofing: This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.

- Man in the middle attack: Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender, who is presumably trusted by the recipient.

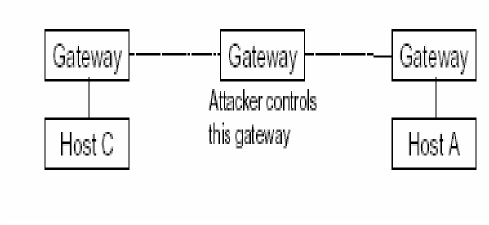

Fig.3.

- Denial of service: IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DoS. Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions. Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DoS as difficult as possible. When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block traffic.

C. Defending against spoofing

There are a few precautions that can be taken to limit IP spoofing risks on your network, such as:

Filtering at the Router –

Implementing ingress and egress filtering on your border routers is a great place to start your spoofing defense. You will need to implement an ACL (access control list) that blocks private IP addresses on your downstream interface. Additionally, this interface should not accept addresses with your internal range as the source, as this is a common spoofing technique used to circumvent firewalls. On the upstream interface, you should restrict source addresses outside of your valid range, which will prevent someone on your network from sending spoofed traffic to the Internet.

Encryption and Authentication : Implementing encryption and authentication will also reduce spoofing threats. Both of these features are included in Ipv6. Which will eliminate current spoofing threats. Additionally, you should eliminate all host-based authentication measures, which are sometimes common for machines on the same subnet. Ensure that the proper authentication measures are in place and carried out over a secure (encrypted) channel.

1) Inter domain

Inter domain is data flow control and interaction between Domain Controller (PDC) computers. This type of computer uses various computer protocols and services to operate. It is most commonly used to multicast between internet domains.

2) Packet filter

A packet filter is a first generation firewall that processes network traffic on a packet-by-packet basis. Its main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network. The router that connects a network to another network is known as a border router. One way to mitigate the threat of IP spoofing is by inspecting packets when they the leave and enter a network looking for invalid source IP addresses. If this type of filtering were performed on all border routers, IP address spoofing would be greatly reduced. Outgoing filtering checks the source IP address of packets to ensure they come from a valid IP address range within the internal network. When the router receives a packet that contains an invalid source address, the packet is simply discarded and does not leave the network boundary.

Incoming filtering checks the source IP address of packets that enter the network to ensure they do not come from sources that are not permitted to access the network. At a minimum, all private, reserved, and internal IP addresses should be discarded by the router and not allowed to enter the network.

3) Limits of packet filtering

Packet filtering normally may not prevent a system from participating in an attack if the spoofed IP address used could fall within the valid internal address range. However it will simplify the process of tracing the packets, since the systems will have to use a source IP address within the valid IP range of the network. Instances where you might need to disable packet filtering include:

- If you want to do asymmetric routing (accepting returning packets inbound an interface other than the outbound interface).

If the box has multiple interfaces up on the
Same network.

- If you are using special VPN interfaces to tunnel traffic (e.g. Free S/WAN) Another problem is that many ISPs do not have the technical ability to arrange packet filtering to block packets with spoofed source addresses. Also, packet filtering reduces equipment performance.

II. RELATED WORK

Research in time-sharing is provided by a collection of programs whose elaborate and strange design outgrowth of many years of experience with earlier versions. To help develop a secure system, we have continuing competition to devise new way to attack the security of the system (the bad guy) and, at the same time, to device new techniques to resist the new attack (the good guy) . This competition has been in the same vein as the completion of long standing between manufactures of armor plate and those of armor –piercing shells. For this reasons, the description that follows will trace the history of IP Spoofing and packet routing rather than just sending a data normally without any encryption in the network.

A. Detecting Spoofed Packets

Packets sent using the IP protocol include the IP address of the sending host. The recipient directs replies to the sender using this source address. However, the correctness of this address is not verified by the protocol. They did research to know if network traffic has spoofed source addresses and a wide variety of methods for detecting spoofed packet. By using routing and non-routing methods they are trying to detect the spoofed packet various methods are used like

□ Spoofed detection method
□ Non Routing Method
□ OS Fingerprinting
□ IP Identification Number
□ Zombie control

Steven and Karl conclude that the intricacies of the modern computer networks can create situations that complicated detecting spoofed packets. Also, an attacker who knows that a system is being monitored for spoofed packets may craft more sophisticated packets to defeat the spoofed packet detector.

B. Practical Network Support for IP Traceback

In This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source by using general purpose traceback mechanism based on probabilistic packet marketing in the network. Traceback can be performed "post-mortem" – after an attack has completed.

□ Ingress filtering
□ Link testing
□ Logging
□ ICMP Traceback

That said, we believe that the scheme is promising and that hybrid approaches combining it with some of the algorithms we propose are likely to be quite effective.

C. Introduction to Blowfish Algorithm

Blowfish Algorithm is used for encryption and decryption. Blowfish is a symmetric block cipher that can be effectively used for encryption and safe guarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times.

The block size is 64 bits, and the key can be any length up to 448 bits. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. It performs data encryption via 16-round feistel network. Each round consist of a key-dependent permutation, and a key-and data dependent substitution. All operations are XOR and additions on 32-bit words. The only
addition operations are four indexed array data lookups per round.

Sub-keys : Blowfish uses a large number of subkeys.
These keys must be per computed before any data
encryption or decryption.
Blowfish has 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32-bit halves: xL, xR.

```
Then, for i = 1 to 16:
 xL = xL XOR Pi
    xR = F(xL) XOR xR
    Swap xL and xR
      After the sixteenth round, swap xL and xR again
      to undo the
      last swap.
```

Then, xR = xR XOR P17
and xL = xL XOR P18.
Finally, recombine xL and xR to get the ciphertext.

III. CONCLUSION

IP Spoofing is a problem without an easy solution, since it's inherent to the design of the TCP/IP suite. Understanding how and why spoofing attacks are used, combined with a few simple prevention methods, can help protect your network from these malicious cloaking and cracking techniques.

A. Comparison

During the previous paper review we observed that many of the alerts generated were false positives and could be eliminated if corroborating information were available. The ability to know if the packets that generated the alerts were spoofed is just one example of supplemental information that would help in filtering out those alerts of low significance. Only strong end-to-end authentication can prevent packet spoofing .

Preventing spoofing through Packet filtering alone is a tough work to do, can prevent the frequency but for have a secure network and secure session of the user during network communication need to have better idea. IP encryption is another way to prevent the security of the IP address and if unauthorized user is not able to have original IP address then they will not be able to spoof that. For IP encryption ciphering techniques can be used.

IV. FUTURE WORK

Detecting spoofed packet and trying to prevent Source IP address is just half of the solution of the problem: we need to be able to localize the true source of the packets. A number of projects have looked at this, but either required specially instrumented routers, or changes in the underlying network protocol that will predefine having a support to IP address encryption. While these are possible solutions, we feel that methods that do not have these requirements are more attractive. We believe that for some spoofing attacks, it is possible to use search techniques built upon some of the active detection methods described in this paper to accomplish this.

REFERENCES

[1] Steven J. Templeton, Karl E. Levitt "Detecting Spoofed Packets". Department of Computer Science U.C. Davis, Jan 2004

[2] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, "Controlling IP Spoong Through Inter-Domain Packet Filters" IEEE members

[3] Dr. Rengarajan Alwar, Dr. Sugumar Rajendran, Dr. Sarvankumar Selvaraj, "optimization of blind spoofing using discrete model"

[4] Yogesh Singh, Hariom Awasthi,"controlling ip spoofing through packet filtering using simulation in blowfish algorithm"

[5] S. Staniford-Chen and L. T. Heberlein. Holding Intruders Accountable on the Internet. Proc. of the 1995IEEE, Symposium on Security and Privacy, May 1995 Oakland, CA, pages 39-49.

[6] Hikmat Farhat, Zouk Mosbeh, A Scalable Method to Protect From IP Spoofing, 978-1-4244-2624-9/08/$25.00 ©2008 IEEE.

[7] Ruiliang Chen, Jung-Min Park and Randolph Marchany, A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks,IEEE Transactions On Parallel And Distributed Systems, Vol. 18, No. 5, May 2007.

[8] Jieren Cheng, Jianping Yin, Zhiping Cai and Chengkun Wu, Dos Attack Detection using IP address Feature Interaction, 2009 International Conference on Intelligent Networking and Collaborative Systems.

[9] A. Perrig, D.Song, and A.Yaar, StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks, Technical Report CMU-CS-02-208, CMU Technical Report, February 2003.

[10] Stefan savage, Anna karlin and Tom Anderson, Network Support for IP trace back, IEEE/ACM Transactions on Networking, VOL 9, NO. 3, June 2001.

[11] Pierluigi Rolando, Riccardo Sisto, SPAF: Stateless FSA-Based Packet Filters, IEEE/ACM Transactions on Networking, Vol. 19, No. 1, February 2011.