|| Volume 3 || Issue 8 || August 2018 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

A Novel Method for Detecting and Preventing IP Spoofing Attack in Data Network

Dr. N. Arumugam

Lecturer SG, Dept of ECE, Nachimuthu Polytechnic College, Pollachi, Tamil Nadu, South India.

Abstract— **In the Internet, IP source address spoofing is used in many attacks such as some DDOS/DrDoS attacks. Defending against these attacks are the hardest security problems on the internet. One of the methods to thwart these attacks is to trace the source of the attacks because they often use incorrect or spoofed IP source addresses to disguise the true origin. This paper presents a light weight method to detect and prevent the IP spoofing. To validate the incoming IP packet a network Authentication Server (AS) performs a three way verification process for each initiating host. The proposed method which is capable to detect and prevent all types of spoofing packets including subnet spoofing contributes to standard ingress/egress methods in eliminating bogus traffic on the Internet.**

Keywords: *IP spoofing, DDoS, Hop Count, Internet protocol*

I INTRODUCTION

In TCP/IP networks, packets sent from one host to another include an IP header that contains Source IP address, Destination IP address, source port and destination port. The source IP address identifies the sending host and destination IP address identifies the receiving host. The recipient host directs replies to the sender using this Source IP address. However, the IP at the recipient has no means to validate the authenticity of the packet's source address. This vulnerability can be exploited by attackers to send packets with forged or spoofed source IP address. Sending IP packets with forged source addresses is known as packet spoofing or source IP spoofing. IP spoofing is well known vulnerability of TCP/IP suite and has been well described in [1] - [3]. In general a compromised internet host can spoof IP packets by using a raw socket to fill arbitrary source IP address in to packet headers. It is commonly associated with malicious network activities.

Attackers can spoof different types of IP addresses to use as source IP in their spoofed packets. These spoofed source IP addresses can either be a random IP addresses or a subnet IP address [4]. In Random Spoofed Source Address attackers spoofed random Source IP address in attack packets. This is simply achieved by generating random 32-bit numbers and stamping packets with them. Spoofing technique could affect route-based filtering. In Fixed Spoofed Source Address, the attacker performs a reflector attack to place a blame for the attack on several specific machines. The spoofed packets carry a source address chosen from a fixed given list of IP addresses. Fixed spoofing is counted by the same random spoofing techniques. In Subnet Spoofed Source Address, the attacker spoofs a random address from the address space assigned to the attacker machine's subnet. For example, a machine which is part of 192.170.186.0/24/ network could spoof any address in the range 192.170.186.0 – 192.170.186.255.

Many different types of attacks can be classified as packet-spoofing attacks. Attackers relay on IP spoofing either to make the attack possible, such as DoS/DDoS flooding attacks are obscure the attack source to complicate tracing back methods. A key factor in most of these packet-spoofing attacks is that, they overwhelm the target with floods of spoofed packets and render it to an unresponsiveness state. Such attacks do not receive packet replies from the target. Replies are either unimportant, their contents can be inferred, or the packet can be observed in transit [5].

This paper proposes a simple and efficient method for early detection of spoofed packets by validating the received hop count value. For the validation AS performs a non cryptographic authentication process to authenticate the source IP to access the server. The AS was intended to be placed ahead of the edge router in the network architecture so as to accept subnet connection requests before arriving to the network router. On successful primary checks AS requests the host permits to access the server. The rest of the paper is organized as follows. Section 2 discusses the different IP spoofing techniques. Section 3 describes different spoofing prevention methods. Section 4 describes the proposed method. Section 5 explains the performance and result of the proposed method. Finally, conclusions and future work are drawn in section 6.

II THE IP SPOOFING TECHNIQUES

When a client attempts to establish a TCP connection to a server, the client and the server exchange a set of sequence of messages. This connection technique is called TCP three way handshakes. To establish a TCP connection first, the client sends a SYN packet to the server requesting a new connection with initial sequence number (ISN). To acknowledge the receipt of this SYN packet, the server replies the client by sending it a SYN/ACK packet with an Acknowledgment (ACK) number of ISN+1. Finally, the client sends the server an ACK packet acknowledging the receipt of the SYN/ACK packet. If the server does not receive the final ACK packet, it will retransmit the SYN-ACK 5 times, doubling the time-out value after each retransmission. The initial time-out value is 3 seconds, so retries are attempted at 3, 6, 12, 24, and 48 seconds [13].

It is notable that in the above 3-way handshake process, the server will remain in half-open connection state before receiving final ACK packet. Since the server's backlog queue allocated for maintaining half-open connections is finite, so there is a limitation on the maximum number of half-open connections that can be maintained. The TCP SYN flooding attack works just by exploiting the above limitation of three way handshake. The attack begins when the master sends control packets to agents, ordering them to attack a given victim server. The agents then start at the same time to use one of the IP spoofing techniques to send a stream of flooding SYN packets with spoofed IP addresses to the victim's server. These IP spoofing techniques can be classified into three common types [14]:

1. Random spoofed source address: The attacker generates attack packets with random 32-bit numbers as source IP addresses.

2. Subnet spoofed source address: The attacker spoofs a random address from the address space assigned to the agent machine's sub network.

3. Fixed spoofed source address: The attacker chooses
the spoofed IP address from a fixed list and in this case the attacker wants to perform reflector attack.

Since all previous spoofed IP addresses are inaccessible, so the victim's server can not reach them. As a result, many half open connections will be created, leading to an exhaustion of server's backlog queue and thus the dropping of any new legitimate SYN packets (denial of service).

III IP SPOOFING PREVENTION METHODS

A variety of methods that help in determining whether a received packet have spoofed source IP address have been proposed. These include routing based methods that rely on routers and other network devices to identify spoofed packets, and non-routing methods which apply both active and passive techniques a host can use to determine if a received packet is spoofed [5].

Routing based methods are based on the fact that, routers and firewalls can easily distinguish between incoming (inbound) packets and outgoing (outbound) packets, since they deploy different network interface, which make it possible for them to identify packets that should not have been received by a particular interface. Ingress filtering [6] is based on the internal capability of an edge router or a gateway to identify internal IP addresses from external IP addresses. So if a router receives IP packets with external IP addresses on an internal filtering is to block such packets. Egress filtering is archetypal to ingress filtering. If a router or a gateway receives IP packets with an internal IP addresses on an external IP interface, then this is a spoofed packet and should be blocked.

The major drawbacks for ingress and Egress filtering are that; their capabilities in combating IP spoofing is limited and they entail a global deployment. In the last few years, new methods that based on determining validity of a packet's source IP address while it is in the path routers in the Internet are proposed. StackPI [7] is a router based proposed solution in which routers on the packet's path towards its destination are assumed to deterministically mark bits in the packet's IP Identification field. The deterministic marking are assumed to guarantee that packets traveling along the same path will have the same marking. Another yet new marking approach is MASK [9]. Source Address Validity Enforcement Protocol (SAVE) [8], employ a mechanism to construct router table that map ranges of IP address to the proper incoming interface for packets with those source address.

It proposed that routers would learn this information on the fly, and maintain an incoming routing table, where the valid incoming interface, for a given source address would be stored. TTL field in the IP header is used to play a role in filtering spoofed packets as in [10] [11]. Filtering in [10], [11] is done differently, but they share the same concept that packets originating at the same source traverse the same route. The Spoofing Prevention Method [12], proposed the use of a filtering key that is a function of the Source IP and IP destination pair and it is filtering technique is independent to the route the packets traverse.

With exception to ingress/egress filtering which prevent spoofing at source, all of the above mentioned proposed solutions are destination-based solutions that detect spoofing at destination to prevent victims from spoofed attacks. Our contribution in this paper is to improve filtering capabilities at source by detecting and blocking all types of source IP spoofing packets including subnet spoofing and TCP/SYN flooding attack pack

IV PROPOSED METHODOLOGY

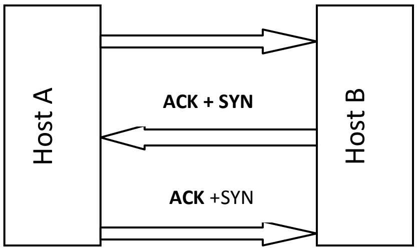
The proposed method is designed to detect and denied both subnet and external spoofed packets at the leaf router before reaching the network server. The design characteristics that have been considered in designing are simple and light weighted. To realize these characteristics, the proposed method was designed to constitute an uncomplicated databases and routines, and to use techniques that lessen network overhead. One of the databases is Subnet Host Information Database

(SHID), which stores the subnet hosts assigned IP addresses and their corresponding MAC addresses.

The proposed design was centered on an Authentication Server (AS), which has to authenticate incoming IP packets without using any cryptographic methodology or router support. The goal of the proposed method is to screen out most of the bogus request. To perform these functionalities, AS acts as a connection service provider and receives all SYN packets that initiated by client hosts prior reaching the network gateway. To identify the forged IP packets, AS employ a three way authentication process with the initiating host.

TCP Connection Establishment- Normal

When making a TCP connection one host send a TCP packet with a SYN flag bit on in order to request connection establishment. Immediately up on receiving the packet destination host sends back a TCP packet with ACK and SYN flags bits on to accepts the request and to establish the connection in the reverse direction. The negotiation ends when the first host sends back an ACK packet. Logically TCP tries to make both upstream and downstream connection separately to achieve full duplex transmission. This process is called 3-way handshake [15].



Figurer 1: 3-Way Handshake

The ACK packet is sent back immediately after the SYN packet is received, the ACK packet can be regarded as an ECHO packet of the SYN packet. There fore the difference between the time when the SYN packet is sent and the time when the ACK packet returns can be used as the approximation of the packet transfer time between two hosts.

TCP Connection Establishment- Proposed Method

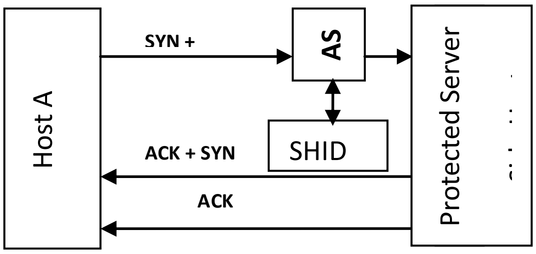


Figure: 2 TCP Connection Establishment

In the proposed method AS compute the exact hop value to the source IP of the received packet. Based on the difference it identifies the spoofing of the packets. Fig 2 shows the connection establishment scenarios.

Primary Check Routine

To protect the server side hosts from any type of spoofing an initial verification carried out by AS on the received hop count called primary check routine. FIG.3 shows the flowchart approach of the routine. During this routine the incoming hop count value is checked, if it is equal to 0 the subnet spoofing verification routine is executed. Otherwise external spoofing verification routine is executed.

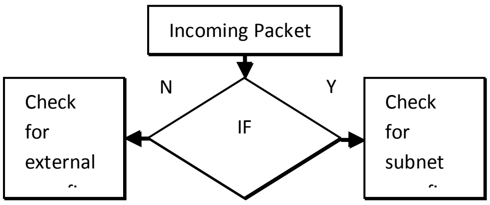


Figure 3: Primary Check Routine

Algorithm for Primary Check Routine

```
/* When AS receives a SYN packet */
Begin
{
Check the hop count value of the received packet details;
if (Hop value == 0)
{
/* call the subnet spoofing verification routine */
}
else
{
/* call the External spoofing verification routine */
}
End ;}
```

Subnet Spoofing Verification Routine

In this routine, AS send a request to the received source IP to send its MAC address. The received MAC address is compared with the stored MAC address in the SHID database. Both the records are equal AS confirmed the request as a legitimate and permit to access otherwise the request is denied to access further.

Algorithm for Subnet Spoofing Verification Routine

```
/* When receives a SYN packet hop value is zero*/
Begin
{
Begin
Send a request to the source IP host to send its MAC address;
if (Received MAC address == MAC address of SHID)
{
/* no subnet spoofing */
Permit the request;
}
else
{
/* Subnet spoofing detected */
Deny the request;
}
End ;}
```

External spoofing verification routine

The validation of the initial request is performed by the primary check routine. Since the received packet hop count value *r-hop* is more than zero it is understood that the request hails from external source and hence to verify its genuineness the external spoofing verification routine is executed. During the verification, AS send a trace route to the received source IP and get back the hop count value denoted as *t-hop*.

The legitimate of the request is validating by comparing the above said hop values and difference among the hop value is denoted as d-hop.

d-hop= (r-hop ~ a-hop)

When the d-hop value is zero, it is understood that the request is a legitimate and the request is permit to access. Otherwise the request is a fake and it is not to permit to access. But it is not possible to confirm the bogusness fully. Based on the traffic and congestion in the network, the hop count value may change. Thus by observation in the proposed method the difference in the hop value (d-hop) up to 2 is permitted. Rest of the difference in d-hop treated as illegal and the access is denied.

```
/* When AS receives a SYN packet t */
Begin
{
Workout the hop count value of the received packet(r-hop);
Start:
        {
        Procedure to
          Trace route the received Source IP hop count (t-hop);
        }
/*Find out the difference among the two hop*/
d-hop=(r-hop ~ a-hop)
If (| (d-hop==0) | | (d-hop== (+2)) | | (d-hop== (-2)))

 {
  no external spoofing found:
   permit the request;
   }
 else
 { declare: partial spoofing found
 Start:
        Routine to filter the request;
  }
End;
}
```

V PERFORMANCE AND RESULT

This section present the performance measurements conducted using the stimulation setup. The performance of the proposed method is compared with correlation between the request and the response time. In normal TCP connection the time required for connection establishment is based on the three way handshake period in the range of seconds. According to Karn /Partridge algorithm the RTT estimation is important and it is neither underestimate nor overestimate.

Estimate RTT= α. Estimate RTT +β. Sample RTT

Sample RTT is computed by sender using timer

Let $\alpha + \beta = 1$; then the range of α and β are

$0.8 <= \alpha <= 0.9$; $0.1 <= \beta <= 0.2$

In addition to the TCP connection establishment time the proposed method required an additional searching time for verification of legitimateness.

VI CONCLUSION AND FUTURE WORK

This paper proposed a simple and passive approach to prevent IP spoofing. This method overcomes the limitation in preventing subnet spoofing and provides an efficient mean for detecting and eliminating SYN flooding attacks. In this method, requisite gets response after verification, thus the response time is more than normal TCP connection. Second constraint is the memory consumption of SHID and DCSD data bases. In the future work, new methodologies can be implemented to minimize the problems described above.

REFERENCES

[1] S. Bellovin, “Security Problems in the TCP/IP Protocol Suite”. *Computer Communications Review*, vol. 19, no. 2, pp. 32-48, April 1989.

[2] Computer Incident Advisory Committee (CIAC), Advisory Notice F-08, “Internet Spoofing and Hijacked Session Attacks”, USES 1995.

[3] Daemon9“IP Spoofing Demystified”, *Phrack Magazine Review*, Vol 7, No. 48, 48-14, June 1996.

[4] Jelena MirKovic, Peter Reiher, “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”, *ACM SIGCOMM Computer Communications review*, Volume 34, Number 2, April 2004, pp.39-54

[5] Steven J. Templeton and Karl E. Levitt, “Detecting Spoofed Packets”. *In proceedings of DISCEX03*, 2003.

[6] P. Ferguson and D. Senie.“Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing,”RFC2827. May 2000.

[7] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against ddos attacks," *in Proc .IEEE Symposium on Security and Privacy*, 2003.

[8] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "Save: Source address validity enforcement protocol," *in Proc. INFOCOM 2002.*

[9] LU XiCheng, LÜ GaoFeng, ZHU PeiDong & CHEN YiJiao, "MASK: An efficient mechanism to extend interdomain IP spoofing prevention". Springer, Science in China series, 2008.

[10] C. Jin, H. Wang, and K. Shin, "Hop-count filtering: An effective defense against spoofed ddos traffic," *in Proc. ACM Conference on Computer and Communications Security*, 2003.

[11] G. Pazi, A. Bremler-Barr, R. Rivlin, and D. Touitou, "Protecting against distributed denial of service attacks," 2002, Patent Application 20030110274.

[12] Bremler-Barr, A. Levy, H, "Spoofing Prevention Method",*proceedings of 24th Annual Joint Conference of IEEE computer and communications societies*, INFOCOM 2005, V1, Pages 536-547.

[13] V.Paxson and M. Allman, "RFC 2988 Computing TCP's Retransmission Timer", Nov.2000.

[14] J. Mirkovic and P. Reiher, "Taxonomy of DDoS attack and DDoS defense mechanisms," in Proc. Conf. ACM SIGCOMM Computer Communications Review, April 2004.

[15] W.Richard Stevens, "TCP/IP Illustrated, Volume 1" Addison Wesley Longman, Inc., 1994.