ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

IP Spoofing Attack Detection using Route Based Information

Sneha S. Rana[1], T. M. Bansod[2]

[1] Department of Computer Technology, VJTI Mumbai, India
[2] Department of Computer Technology, VJTI Mumbai, India
[1] rana.sneha9@gmail.com
[2] tmbansod@gmail.com

***Abstract*— IP spoofing is almost always used in one of the most difficult attack to defend against – Denial of Service (DoS) attack. DOS attack is evolving due to proliferation of diverse network application. Researchers have performed studies on online/offline network devices such as routers and IDS/IPS. While, the task of deep packet inspection is powerfully handled by IDS/IPS, the real time processing requirement is best suited for routers. The IP packet header information is efficiently handled by routers, hence proposing a technique the uses the router specific features will be best suited for real time processing. In this paper we introduce a technique which uses the router specific information to identify the IP spoofing based attack and mitigate it using that information.**

***Keywords*— Dos attack, IP Spoofing, Network security**

I. INTRODUCTION

Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. IP spoofing is one of the most common forms of on-line camouflage.

The concept of IP spoofing was initially discussed in academic circles in the 1980's. While known about for some time, it was primarily theoretical until Robert Morris, whose son wrote the first Internet Worm, discovered a security weakness in the TCP protocol known as sequence prediction. Stephen Bellovin discussed the problem in-depth in Security Problems in the TCP/IP Protocol Suite, a paper that addressed design problems with the TCP/IP protocol suite. Another infamous attack, Kevin Mitnick's Christmas Day crack of Tsutomu Shimomura's machine, employed the IP spoofing and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, spoofing can still be used and needs to be addressed by all security administrators.

IP spoofing is commonly associated with malicious network activities, such as Distributed Denial of Service (DDoS) attacks which block legitimate access by either exhausting victim servers' resources or saturating stub networks access links to the Internet. Perpetrators of DoS/DDoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. DDoS attacking tools spoof IP addresses by randomizing the 32-bit source-address field in the IP header which conceals attacking sources and dilutes localities in attacking traffic.

The recent "backscatter" study, which quantifies DoS activities in the current Internet, has confirmed the widespread use of randomness in spoofing IP addresses. Moreover, some known DDoS attacks, such as smurf and more recent Distributed Reflection Denial of Service (DRDoS) attacks are not possible without IP spoofing. Such attacks masquerade the source IP address of each spoofed packet with the victim's IP address. Overall, DDoS attacks with IP spoofing are much more difficult to defend.

Route-based and host-based are two different approaches taken by researchers to thwart DDoS attacks. The former installs the defense mechanism inside IP routers and hence trace the source of attack and block the corresponding traffic originating from that source. However, the drawback of this approach is that it requires coordination among different routers and networks, and also a widespread deployment to reach the proximity of the attacker. The host-based approach can be deployed immediately. Also, a much stronger incentive is required to deploy the defense mechanism at the end system compared to that of network service provider.

The current host-based approaches protect an Internet server either by using sophisticated resource-management schemes or by significantly reducing the resource consumption of each request to withstand the flooding traffic such as SYN cookies and Client Puzzle. Without a mechanism to detect and discard spoofed IP traffic at the very beginning of network processing, spoofed packets will share the same resource principals and code paths as

legitimate requests. Under heavy attacks, current approaches are unlikely to be able to sustain service availability due to resource depletion caused by spoofed IP packets. Furthermore, most of existing host-based solutions work at the transport-layer and above, and cannot prevent the victim server from consuming CPU resource in servicing interrupts from spoofed IP traffic. At high speed, incoming IP packets generate many interrupts and can drastically slow down the victim server. Therefore, the ability to detect and filter spoofed packets at the IP layer without any router support is essential to protection against DDoS attacks. Since filtering spoofed IP packets is orthogonal to the resource-protection mechanisms at higher layers, it can be used in conjunction with advanced resource-protection schemes.

The scheme introduced in this paper filters out the bogus traffic with very less false positive rate. It scans the incoming IP packet without using any cryptographic technique. The basic idea behind the scheme is to use the packet information – the route that packet travels along with the TTL field. The TTL field of the packet is used to determine if the packet has travelled the right number of hops before reaching the destination. In IP spoofing the attacker can falsify the IP address of the source but he cannot ideally alter the number of hops the packet would travel to the destination.

In this paper we discuss the related work by other researchers, the present system for detecting the IP Spoofing based attack and then we put forward our scheme to detect IP spoofing based attack.

II. Related Work

The two basic detecting mechanism of IP spoofing based attack is packet filtering and packet traceback at the node level. Many techniques have been proposed by various researchers based on the above mentioned two mechanisms. The partial path of the packet is inspected in order to find the true origin of the attack packet. This task of finding the true source of the malicious packet is called traceback mechanism. The first step towards the necessary legal action to discourage such attack in future is to identify the source address correctly. Savage et al. proposed to let routers mark packets probabilistically, so that the victim can collect the marked packets and reconstruct the attack path. One enhanced scheme of probabilistic packet marking has been proposed by Song et al. to reduce the false positive rate for reconstructing the attack path. Another enhanced scheme of probabilistic packet marking has been proposed to reduce the computational overhead.

As a proactive solution to such attacks, several filtering schemes, which must execute on IP routers, have been proposed to prevent spoofed IP packets from reaching intended victims. The ingress filtering blocks spoofed packets at edge routers, where address ownership is relatively unambiguous, and traffic load is low. However, the success of ingress filtering hinges on its wide deployment in IP routers.

Park and Lee proposed the route-based packet filters as a form of International Journal of Database Theory and Application mitigating IP spoofing, which assumes that there is one single path between one source node and one destination node, so any packet with the source address and the destination address that appear in a router that is not in the path, should be discarded.

Subsequently, a new method which is Hop-Count Filtering (HCF) proposed another novel simplified scheme to identify packets whose source IP addresses is spoofed. The information about a source IP address and its responding hops from a server (victim) are recorded in a table at the server side when there are attacks free. Once an attack alarm is raised, the victim will inspect the incoming packets' source IP addresses and their responding hops to differentiate the spoofed packets.

To validate that an IP packet carries the true source address, SAVE, a source address validity enforcement protocol, builds a table of incoming source IP addresses at each router that associates each of its incoming interfaces with a set of valid incoming network addresses. SAVE runs on each IP router and verifies whether an IP packet arrives at its expected interface. By matching incoming IP addresses with their expected receiving interfaces, the set of IP source addresses that any attacker can spoof is greatly reduced.

In attack situations where a large number of infected hosts are utilized, the information from a large number of network devices should be combined to induce a meaningful decision.

III. Detection Mechanism

In this paper we describe the IP spoofing detection mechanism which will first identify if the packet is malicious or not and if found malicious it will then try to identify the true source of the IP packet from where the packet has originated. IP packet header fields – the TTL and the ID field of the packet will be used to help find the attack source. The TTL of an IP header is a record of how many routers the packet has traversed and the ID is a serial number that is used in de-fragmentation.

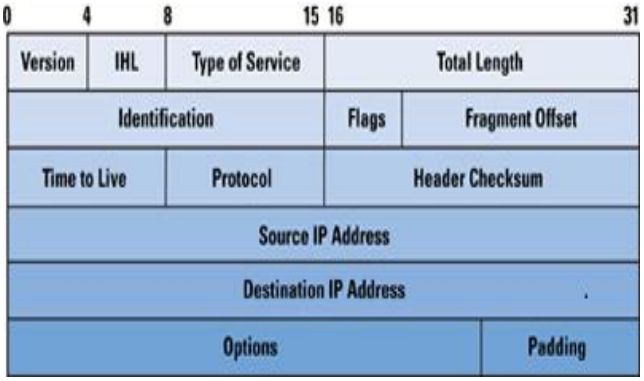

Fig 1: IP Header

A. *Detection Mechanism based on TTL*

One most common attack based on IP spoofing is DDoS attack. Such attack is initiated when the attacker compromise various botnets using some malicious way. These compromised hosts then spoof the attack packet by inserting some random IP address in the source address field of the IP packet. This detection mechanism keeps track of the packet flow information embedded in the IP header (figure1). TTL is a 8 bit field in IP header determines the maximum lifespan of an IP packet. As the IP packet transit through the network each intermediate node decrements the TTL value by one before forwarding it to the next node. Hence, this mechanism uses the number of Hop the packet travelled to detect if the packet is legitimate or not. This information is obtained by subtracting the final TTL with the initial TTL value. This hop count value is then compared with the stored hop count corresponding to the source address. If both the values are same then the packet is malicious.

The fact that the ID increases monotonically for the given session can be utilized for the detection. Since the rates from the spoofed victim and that of the zombie/bot are different, at certain point the ID should be less that the value of the previous packet. In the case when ID values decreases abnormally, the Source-IP Based Lookup Table is updated and the packet is forwarded based on the dropping probability routing.

B. *Detection Mechanism based on ID field*

The utilization of Identification field in IP header is done in case of packet assembly when large data is sent across the network. This field is set to a large value initially during the transmission session and steadily increases to 65,535 to 0.

```
For each received packet:
    analyze and extract the final TTL(TTLf) and the Source addres (S);
    find the initial TTL value (TTLi)
    compute the hop count Hc = TTLi - TTLf;
    use the S to find the stored Hop count value (Hs);
    if (Hc = Hs)
        the packet is legitimate:
    else
        the packet is spoofed;
```

Fig 2: TTL based detection

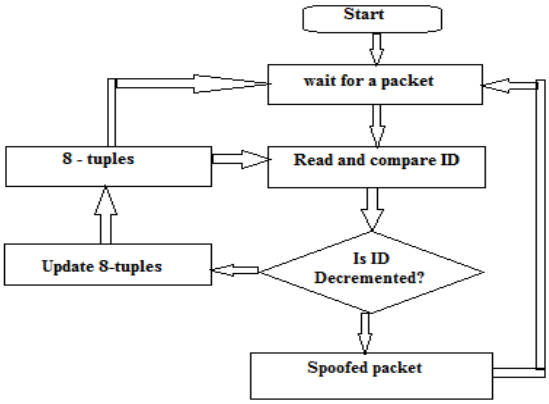

Fig 3: ID based detection algorithm

IV. TRACEBACK MECHANISM

The basic idea of IP traceback approach based on packet marking is that the router marks packets with its identification information as they pass through that router. The mark overloads a rarely used field in IP packet header, i.e., 16-bit IP identification field. The identification of a router could be 32-bit IP address, hash value of IP address, or uniquely assigned number. In the last two cases, the length of identification information is variable and could be less than 16 bits. Since the marking space in packet header is too small to record the entire path, routers mark packets with some probability so that each marked packet carries the information of one node in the path. In addition, based on the length of router identification and the implementation of marking procedure, the router may only write part of its identification information into the marking space. While each marked packet represents only a small portion of the path it has traversed, the whole network path can be reconstructed by combining a modest number of such packets. This kind of approach is referred to as probabilistic packet marking (PPM). The PPM approach

does not incur any storage overhead at routers and the marking procedure (a write and checksum update) can be easily and efficiently executed at current routers. But due to its probabilistic nature, it can only trace the traffic that consists of a large volume of packets. In the PPM a packet stores the information of an edge in the IP header. The pseudocode of the procedure is given below for reference. The router determines how the packet can be processed depending on the random number generated. If x is smaller than the predefined marking probability pm, the router chooses to start encoding an edge. The router sets the start field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field.

```
For each packet w
    Let x be a random number from [0..1)
    If x <  then
    Write R into w.node
```

Figure 4: the packet marking algorithm

V. CONCLUSION

In this paper we discussed the IP spoofing based attack detection using route based information present in IP packet header i.e. the TTL and ID field of the packet also we introduced a traceback mechanism to trace back the attacker right at its origin. . The IP packet header information is efficiently handled by routers, hence proposing a technique the uses the router specific features will be best suited for real time processing. We found the algorithm is well suited to detect the DDoS attack situations as long as the network is stable, i.e., the routing information is not changed.

REFERENCES

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

[2] C.Jin, H.Wang, and K. G. Shin, Hop- count filtering: An effective defense against spoofed DDoS traffic, *In Proc .of the 10th ACM conference on Computer and communications security*, 2003.

[3] K. Park and H.Lee, On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets, *In Proc. of ACM SIGCOMM*, 2006.

[4] Z.Duan, X.Yuan, and J. Chandrashekar, Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates, *IEEE Transactions On Dependable And Secure Computing, Vol. 5, No. 1, January-March 2008.*

[5] A.Bremler-Barr and H.Levy, Spoofing Prevention Method, *In Proc. of INFOCOM*, 2005.

[6] S.Savage, D.Wetherall, Anna Karlin, and Tom Anderson, Network support for IP Traceback. *IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001*.

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

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

[9] Stefan sevage, Anna karlin and Tom Anderson, Network Support for IP traceback, *IEEE/ACM Transactions on Networking, VOL 9., NO. 3 , June 2001.*

[10] 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.*

[11] 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.*