International Journal of Students Research in Technology & Management
Vol 1(3), May 2013, ISBN 978-93-83006-01-4, pg 347-352

CONTROLLING IP SPOOFING THROUGH INTER DOMAIN PACKET FILTERS

Yash Suresh Paluskar, Prashant Mahesh Agarwal, Rajesh Ravsaheb Tambe, Sumit Nandkumar Agarwal
Department of Computer Engineering
P.E.S Modern College of Engineering, Pune
yashpaluskar@gmail.com, prashantagarwal2002@gmail.com,
tamberajesh876@gmail.com, sumitagrwal@gmail.com

Abstract

IP Spoofing is a serious threat to the legitimate use of the Internet. By employing IP spoofing, attackers can overload the destination network thus preventing it from providing service to legitimate user. In this paper, we propose an inter domain packet filter (IDPF) architecture that can minimize 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 Border Gateway Protocol (BGP) route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses. 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- IP spoofing, DDoS, BGP, ANT Colony Algorithm, network-level security and protection, AES algorithm

I. INTRODUCTION

IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without any authentication. By pretending as a different host, an attacker can hide its true identity and location, rendering source based packet filtering less effective.

IP spoofing can also be a method of attack used by network intruders to defeat network security measures, such as authentication based on IP addresses. It works in such a way that the proposed System uses Inter domain Packet filters (IDPFs) architecture, a system that can be constructed solely based on the locally exchanged BGP updates. Each node only selects and propagates to neighbors based on two sets of routing policies. They are Import and Export Routing policies.

The IDPFs uses a feasible path from source node to the destination node, and a packet can reach to the destination through one of its upstream neighbors. Such a filtering will not discard the packets with valid source address. An ideal packet filter should discard spoofed packets while allowing legitimate packets to reach the destinations. Since, even with the perfect routing information, the route-based packet filters cannot identify all spoofed packets, a valid packet filter should focus on not dropping any legitimate packets while providing the ability to limit spoofed packets.

Border Gateway Protocol (BGP) is used to determine path very easily. By using the BGP protocol we establish communication between multiple autonomous systems and Different service providers.

We are controlling IP Spoofing and in order to provide additional security we are encrypting as well as decrypting the message that is being sent between the nodes. By implementing this feature the message will also get secured making it difficult for an intruder to track the message. Thus by controlling IP Spoofing along with encryption and decryption of message the overall security is being improved.

Advanced Encryption Standard (AES) algorithm will be used for encryption and decryption purpose.AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. We will be using 256 bit key in AES algorithm which will make it strong.

II. RESULTS AND DISCUSSION

A. Existing system

a. Ingress system:

Ingress filtering is a computer security technique that relies on scanning incoming packets to confirm their validity. If a packet does not appear to match its purported source, the network can hold it and may refuse to allow the information through it. This can protect users from malicious attacks based on spoofing, where a hacker attempts to make a packet look like it originated from somewhere else. Internet service providers (ISPs) typically use ingress filtering to defend their customers and an individual home or office network can have additional safety measures in place.

b. Egress system:

In computer networking, egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is controlled. TCP/IP packets that are being sent out of the internal network are examined via a router or firewall

B. Related work

To help develop a secure system, we are 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).

The idea of IDPF is influenced by the work carried out by Park and Lee who evaluated the relationship between network topology and the effectiveness of route-based packet filtering. They showed that packet filters constructed based on the global routing information can significantly limit IP spoofing when deployed in just a small number of Autonomous Systems (AS's). In this work, we extend the idea and demonstrate that filters that are built based on local BGP updates can also be effective. If the policy does not match, the packet is dropped.

A packet is forwarded, as long as the source IP address is in the forwarding table. However, the loose mode is less effective in detecting spoofed packets. In Hop-Count Filtering (HCF), each end system maintains a mapping between IP address aggregates and valid hop counts from the origin to the end system. Packets that arrive with a different hop count are suspicious and are therefore discarded or marked for further processing.

In the Network Ingress Filtering proposal, traffic originating in a network is forwarded only if the source IP in the packets belongs to the network. Ingress filtering primarily prevents a specific network from being used for attacking others.

C. Proposed System

Considering all the facts faced by the IP Spoofing last few years, we have come up with a proposal to develop a comprehensive approach with methodological guidance to analyze, develop and implement a logical and effective program to obtain security objectives of the organization. It works such a way that the proposed System use Inter domain Packet filters (IDPFs) architecture, a system that can be constructed solely based on the locally exchanged BGP updates. Each node only selects and propagates to neighbors based on two set of routing policies. They are Import and Export Routing policies. The IDPFs uses a feasible path from source node to the destination node, and a packet can reach to the destination through one of its upstream neighbors. Such a filtering will not discard the packets with valid source address.

Advantages of the Proposed System:

- Minimize the denial of service attacks.
- For finding possible path we don't need global routing information.
- Reducing the IP spoofing through BGP updates, this will overcome the drawback of finding BEST route
- Encrypting a message to improve overall security.

a. BGP Routing:

As with any routing protocol, BGP maintains routing tables and it doesn't require global routing information, transmits routing updates, and bases routing decisions on routing metrics. The basic function of a BGP system is to exchange network reachability information, including information about the list of possible paths, with other BGP systems. This information can be used to construct a graph of AS connectivity from which routing loops can be pruned and with which AS-level policy decisions could be enforced. Each and every BGP router maintains a routing table that lists all possible paths and feasible paths to a particular network. The BGP router does not refresh the routing table, however instead of that, the routing information received from peer routers is retained until and unless an incremental update is received.

The BGP protocol devices exchange routing information upon initial data exchange and after incremental updates. When a router first connects to the network, BGP routers exchange their full BGP routing tables. Similarly, when the routing table changes occur, routers send the portion of their routing table that has changed. The Border Gateway Protocol does not send regularly scheduled routing updates, and the Border Gateway Protocol routing updates advertise only the optimal path to a network. The BGP uses a single path routing metric to determine the feasible path or best path to a given network. This metric contains of an arbitrary unit number which specifies the degree of preference of a particular link.

The BGP metric typically is assigned to each and every link by the network administrator. The value assigned to a link could be based on any number of criteria, including the number of ASs through which the path passes stability, speed, delay, or cost.

b. Packet filtering:

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.

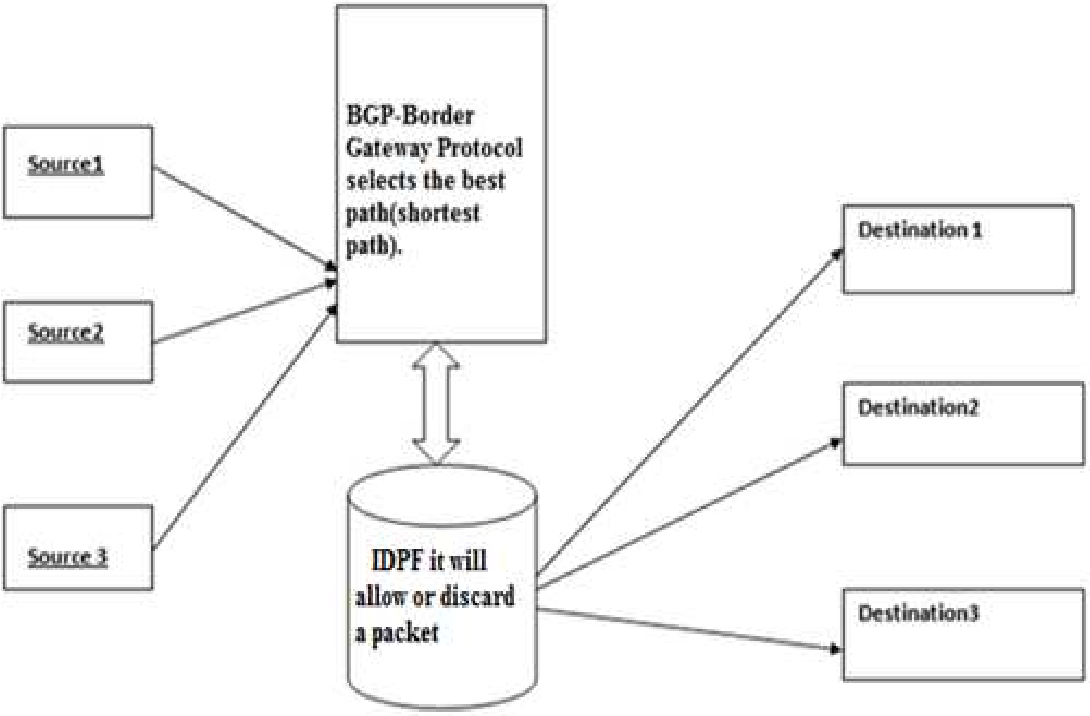
Egress filtering checks the source IP address of packets to ensure they come from a valid IP address range within the internal network. When the router receives a packet that contains an invalid source address, the packet is simply discarded and does not leave the network boundary. Ingress filtering 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.

c. Filtering using IDPF:

If your site has a direct connection to the Internet, you can use your IDPF to help you out. First make sure only hosts on your internal LAN can participate in trust-relationships (no internal host should trust a host outside the LAN). Then simply filter out *all* traffic from the outside (the Internet) that purports to come from the inside (the LAN).

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.

D. System Architecture


Source1
Source2
Source 3
BGP-Border Gateway Protocol selects the best path(shortest path).
IDPF it will allow or discard a packet
Destination 1
Destination2
Destination3

The packets from source machine will be first sent to BGP. BGP will select the best(shortest) path to the destination. From here the packets will go to IDPF .Filtering of packets is done by IDPF. The invalid packets are discarded here and valid packets are sent to destination.

III. CONCLUSION

In this project, we have proposed to establish a network within which first we will be showing how IP spoofing will be done. We will be defining rules(incoming and outgoing policies) based on which filtering process of IDPF will be done.BGP will be used to select the best path that will take the packet to destination. Thus implementing all these things the overall network security will be increased against the DDoS attack which will improve server security. Thus all clients will get proper service from server. The project developed by us is cost efficient.

IV. FUTURE SCOPE

We are showing DDoS Attacks only, in future development other attacks can be covered . Currently four nodes are set for incoming and outgoing policies therefore for N nodes incoming and outgoing policies should dynamically get generated. The system can be made distributed i.e if one of the nodes fail then the system will not crash, other nodes will continue to interact with each other.

V. ACKNOWLEDGEMENT

We hereby take this opportunity to express our deep sense of gratitude to the whole team, from guides to well wishers for their guidance, encouragement and motivation.

Our sincere thanks to our Principal Prof. Mrs. K.R.Joshi and Head Of Department Prof. Mrs. S.A.Itkar for their consistent supervision and encouragement .

We thank our internal project guide Prof. Mrs. A.A.Junnarkar for her encouragement, valuable guidance, keen interest towards the project and supporting us in all aspects.

VI. REFERENCES

1. Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, *Controlling IP Spoofing through Interdomain Packet Filters, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 5, NO. 1, **January-March 2008**
2. J. Stewart, *BGP4: Inter-Domain Routing in the Internet*. Addison-Wesley, **1999**.
3. Herbert Schildt, *The Complete Reference JAVA* 7th Edition,Tata McGraw Hill,**2010.**
4. K. Park and H. Lee, *"On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets*," Proc. ACM SIGCOMM, **Aug. 2001.**