International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

Controlling IP Spoofing with SBGP

A.Manjula [#1], R.Geethanjaly [*2]

[#1] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
mnjlarumugam@gmail.com

[*2] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
geethanjaly91@gmail.com

Abstract— **IP address spoofing refers to the creation of Internet Protocol packets with a forged source IP address, called spoofing, it is a method of attacking a network in order to gain unauthorized access. The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. The attack is based on the fact that Internet communication between distant computers is routinely handled by routers which find the best route by examining the destination address. 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 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. Based on extensive simulation studies, we show that, even with partial employment 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.**

Index Terms— Border gateway protocol, symmetric key distribution protocol, Inter Domain Packet Filter

1.INTRODUCTION

IP spoofing can evade detection and put a substantial burden on the destination network for policing attack packets from the attackers. In this Project, 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 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. Based on extensive simulation studies, we show that, even with partial employment on the Internet, IDPFs can proactively limit the spoofing capability of attackers.

Distributed Denial of Service (DDoS) attacks pose an increasingl grave threat to the Internet, as evidenced by recent DDoS attacks mounted on both popular Internet sites and the Internet infrastructure. Alarmingly, DDoS attacks are observed on a daily basis on most of the large backbone networks . One of the factors that complicate the mechanisms for policing such attacks is IP spoofng, the act of forging the source addresses in IP packets. By masquerading as a different host, an attacker can hide its true identity and location, rendering source-based packet fltering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofng [3]. Recently, attackers are increasingly staging attacks via *botnets* [4]. In this case, since the attacks are carried out through intermediaries, i.e., the compromised .bots., attackers may not utilize the technique of IP spoofng to hide their true identities. It is tempting to believe that the use of IP spoofng is less of a factor. However, recent studies [1], [5], [6] show that IP spoo_ng is still a common phenomenon:

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

it is used in many attacks, including the high-pro_le DDoS attacks on root DNS servers in early February 2006 [1].

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. The IP protocol specifies no method for validating the authenticity of the packet's source. This implies that an attacker can forge the source address to be any desired. This is almost exclusively done for malicious or at least inappropriate purposes. Given that attackers can exploit this weakness for many attacks, it would be beneficial to know if network traffic has spoofed source addresses.This is a well-known problem and has been well described In all but a few rare cases, sending spoofed packets is done for illegitimate purposes Sending IP packets with forged source addresses is known as packet spoofing and is used by attackers for several purposes. These include obscuring the true source of the attack, implicating another site as the attack origin, pretending to be a trusted host, and hijacking or intercepting network traffic, or causing replies to target another system Because none of these are desirable, it is useful to determine if a packet has a spoofed source address. In cases where an

Ongoing attack is occurring it is beneficial to determine if the attack is from a particular location. In many cases we are able to determine when packets are spoofed, and generally from where they originate. Spoofing of network traffic can occur at many layers. Examples include network layer spoofing as well as session and application layer spoofing (e.g. email spoofing). All of these have significant security concerns. However, for the purposes of this paper we will focus only IP packet spoofing. A related issue is attacks that cause packets to be routed to a different host than the sender intends. These are attacks on routing] and the DNS system. Packet spoofing is restricted to false source addresses in the IP packet header.Although attackers can insert arbitrary source address into IP packets, they cannot, however, control the actual paths that the packets take to the destination. Based on this observation, Park and Lee [5] proposed the route-based packet filters as a way to mitigate IP spoofing. The intuition in this scheme is that, assuming single-path routing, there is exactly one single path p(s; d) between source node s and destination node d. Hence, any packets with source address s and destination address d that appear in a router not in p(s,d) should be discarded. However, constructing a specific route-based packet filter in a node requires the knowledge of global routing decisions made by all the other nodes in the network, which is hard to reconcile on the current BGP-based Internet routing infrastructure. Inspired by the idea of route-based packet filters, we propose an Inter-Domain Packet Filter (IDPF) architecture. The IDPF architecture takes advantage of the fact that while network connectivity may imply a large number of *potential* paths between source and destination domains, commercial relationships between ASes act to restrict to a much smaller set the number of *feasible* paths that can be used to carry traffic from the source to the destination. In this paper we focus our attention on the construction of IDPFs based solely on locally exchanged BGP updates. We will investigate how other AS relationship and routing information may help further improve the performance of IDPFs in our future work.

Based on the authentication model described above, we use two forms of key distribution protocols for securing routing protocols. In the first type of key distribution protocol, each sender is responsible for generating and distributing the symmetric keys to the receivers. In the second type of key distribution protocols, a centralized authority is responsible for distributing the necessary keys to the users.

II RELATED WORK

2.1 BGP OVERVIEW

The Border Gateway Protocol (BGP) is an interautonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP). BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

optimal path to a destination network. Contrary to popular opinion, BGP is not a necessity when multiple connections to the Internet are required. Fault tolerance or redundancy of outbound traffic can easily be handled by an IGP, such as OSPF or EIGRP. BGP is also completely unnecessary if there is only one connection to an external AS (such as the Internet). There are over 100,000 routes on the Internet, and interior routers should not be needlessly burdened. BGP should be used under the following circumstances:Multiple connections exist to external AS's (such as the Internet) via different providers. Multiple connections exist to external AS's through the same provider, but connect via a separate CO or routing policy. The existing routing equipment can handle the additional demands. BGP's true benefit is in controlling how traffic entersthe local AS, rather than how traffic exits it

As a BGP peer session is forming, it will pass through several state. This process is known as the BGP Finite-State Machine (FSM)

Idle
– the initial BGP state
Connect
- BGP waits for a TCP connection with the remote peer. If successful, an OPEN message is sent. If unsuccessful, the session is placed in an Active state. Active
– BGP attempts to initiate a TCP connection with the remote peer. If successful, an OPEN message is sent. If unsuccessful, BGP will wait for a ConnectRetry timer to expire, and place the session back in a Connect State.
OpenSent
– BGP has both established the TCP connection
And sent an OPEN Message, and is awaiting a reply OPEN Message. Once it receives a reply OPEN Message, the BGP peer will send a KEEPALIVE message.
OpenConfirm – BGP listens for a reply KEEPALIVE message.
Established – the BGP peer session is fully established. UPDATE messages containing routing information will now be sent.

2.1.1 BGP WORKING

Each node only selects and propagates to neighbors a single best route to the destination, if any. Both the selection and the propagation of best routes are governed by locally defined routing policies. Two distinct sets of routing policies are typically employed by a node: import policies and export policies. Neighbor-specific import policies are applied upon routes learned from neighbors, whereas neighbor-specific export policies are imposed on locally selected best routes before they are propagated to the neighbors. In general, import policies can affect the "desirability" of routes by modifying route attributes. Let r be a route (to destination d) received at v from node u. [1]We denote by import (v <- u) [{r}] the possibly modified route that has been transformed by the import policies. The transformed routes are stored in v's routing table. The set of all such routes is denoted as candidateR (v, u);

CandidateR (v, d) = {r: import (v <- u) [{r}]! = {} r.prefix d u E (v)} .Here, N (v) is the set of v's neighbors.

Among the set of candidate routes candidateR (v, d); node v selects a single best route to reach the destination based on a well-defined procedure. To aid in description, we shall denote the outcome of the selection procedure at node v, that is, the best route, as bestR (v, d) which reads the best route to destination d at node v. Having selected bestR (v, d) from candidateR (v, d) v then exports the route to its neighbors after applying neighbor-specific export policies. The export policies determine if a route should be forwarded to the neighbor and if so, they modify the route attributes according to the policies. We denote by export (v <- u) [{r}] the route sent to neighbor u by node v after node v applies the export policies on route r[1].

BGP is an incremental protocol: updates are generated only in response to network events. In the absence of any event, no route updates are triggered or exchanged between neighbors, and we say that the routing system is in a stable state.

2.2 Attacks

From the point of view of intrusion detection and response, we need to observe and analyze the anomalies due to both the consequence and technique of an attack. While the consequence gives evidence that an attack has succeeded or is unfolding, the technique can often help identify the attack type and even the identity of the attacker. Attacks in MANET can be categorized according to their consequences as the following:

Blackhole: All traffic are redirected to a specific node, which may not forward any traffic at all.

Routing Loop: A loop is introduced in a route path.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

Network Partition: A connected network is partitioned into k (k >= 2) sub networks where nodes in different sub networks cannot communicate even though a route between them actually does exist.

Selfishness: A node is not serving as a relay to other nodes.

Sleep Deprivation: A node is forced to exhaust its battery power.

Denial-of-Service*:* A node is prevented from receiving and sending data packets to its destinations

Some of the common attacking techniques are :

Cache Poisoning: Information stored in routing tables is either modified, deleted or injected with false information.
Fabricated Route Messages: Route messages (route requests, route replies, route errors, etc.) with malicious contents are injected into the network.

Specific methods include:

a) False Source Route: An incorrect route is advertised into the network, e.g., setting the route length to be 1 regardless where the destination is.

b) Maximum Sequence: Modify the sequence held in control messages to the maximal allowed value. Due to some implementation issues, a few protocol implementations cannot effectively detect and purge these “polluted" messages timely so that they can invalidate all legitimate messages with a sequence number falling into normal ranges for a fairly long time

Rushing*:* This can be used to improve Fabricated Route Messages. In several routing protocols, some route message types have the property that only the message that arrives first is accepted by a recipient. The attacker simply disseminates a malicious control message quickly to block legitimate messages that arrive later.

Wormhole*:* A tunnel is created between two nodes that can be utilized to secretly transmit packets.

Packet dropping: A node drops data packets (conditionally or randomly) that it is supposed to forward.

Spoofing: Inject data or control packets with modified source addresses.

Malicious Flooding: Deliver unusually large amount of data or control packets to the whole network or some target nodes.

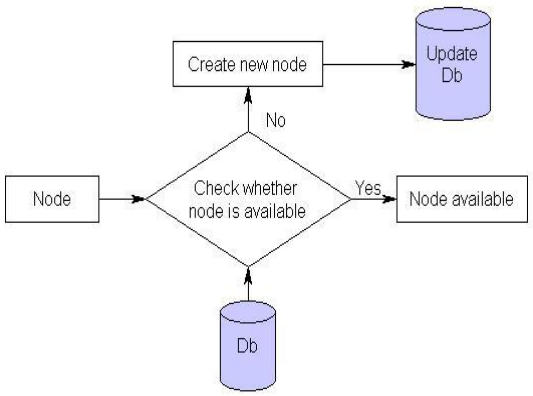
III MODULES

In our project we have four modules; based on the module we implement our project.

- Topology Construction.
- BGP Construction.
- IDPF Construction.
- Control the Spoofed Packets

3.1 TOPOLOGY CONSTRUCTION

In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user.While getting each of the nodes, their associated port and ip address is also obtained.For successive nodes, the node to which it should be connected is also accepted from the user.While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.



MODULE 1:

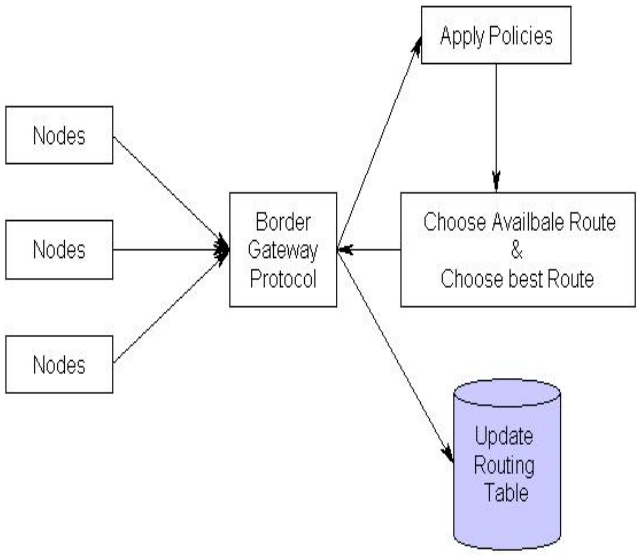
3.2 BGP CONSTRUCTION

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

Definition 1: (stable routing state). A routing system is in aStable state if all the nodes have selected a best route to reach other nodes and no route updates are generated (or propagated).

Each node only selects and propagates to neighbors a single best route to the destination, if any. Both the selection and the propagation of best routes are governed by locally defined routing policies. Two distinct sets of routing policies are typically employed by a node: import policies and export policies. Neighbor-specific import policies are applied upon routes learned from neighbors, whereas neighbor-specific export policies are imposed on locally selected best routes before they are propagated to the neighbors. In general, import policies can affect the "desirability" of routes by modifying route attributes.

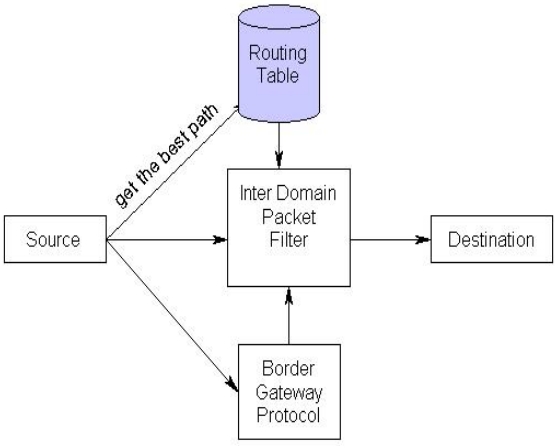


3.3 IDPF CONSTRUCTION

IDPFs can independently be deployed in each AS. IDPFs are deployed at the border routers so that IP packets can be inspected before they enter the network. By deploying IDPFs, an AS constrains the set of packets that a neighbor can forward to the AS: a neighbor can only successfully forward a packet M (s, d) to the AS after it announces the reachability information of s. All other packets are identified to carry spoofed source addresses and are discarded at the border-router of the AS.

Definition 2: (route-based packet filtering). Node v accepts packet M(s, d) that is forwarded from node u if and only if e(u,v) belongs to R(s,d). Otherwise, the source address of the packet is spoofed, and the packet is discarded by v.In the context of preventing IP spoofing, 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 [5], a valid packet filter should focus on not dropping any legitimate packets. Accordingly, we define the correctness of a packet filter as follows.

Definition 3: (correctness of packet filtering). A packet filter is correct if it does not discard packets with valid source addresses when the routing system is stable. Clearly, the route-based packet filtering is correct, because valid packets from source s to destination d will only traverse the edges on best R(s, d) when the routing system is stable.



3.4 CONTROL THE SPOOFED PACKETS

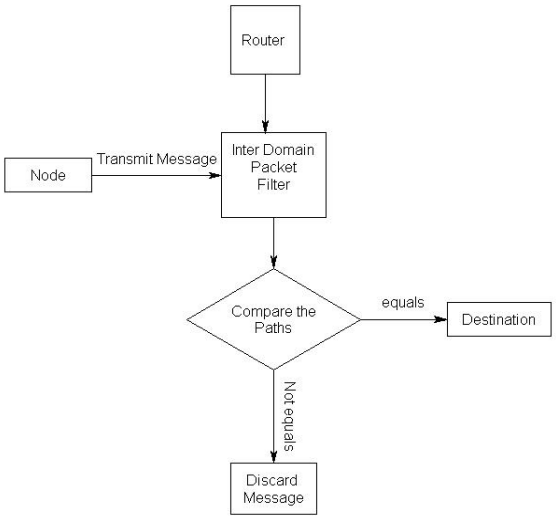
Based on the IDPF and BGP we will identify the packet will be spoofed or correct. If it's correct the messages allow to the destination or its spoofed means the packets will be discarded. IDPF framework works correctly in that it does not discard packets with valid source addresses.

IDPFs can significantly limit the spoofing capability of an attacker.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-007 PAGE NO: 034-039

Moreover, they also help pinpoint the true origin of an attack packet to be within a small number of candidate networks, thus simplifying the reactive IP trace back process.



IV CONCLUSION

In this paper, we have proposed and studied IDPF architecture as an effective countermeasure to the IP spoofing-based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbor. We showed that IDPFs can easily be deployed on the current BGP-based Internet routing architecture. We studied the conditions under which the IDPF framework can correctly work without discarding any valid packets. Our simulation results showed that, even with partial deployment on the Internet, IDPFs can significantly limit the spoofing capability of attackers. Moreover, they also help pinpoint the true origin of an attack packet to be within a small number of candidate networks, thus simplifying the reactive IP traceback process.

V FUTURE ENHANCEMENTS:

It also helps pinpoint the true origin of an attack packet to be within a small number of candidate networks, thus simplifying the reactive IP traceback process.

VI REFERENCES

[1] Routing Protocol Security Using Symmetric Key Based Techniques. Bezawada Bruhadeshwar and Kishore Kothpalli and M.Poornima and M.Divya International Institue of Technology Hydrabad.
[2] K. Park and H. Lee. On the e_ectiveness of route-based packet _ltering for distributed DoS attack prevention in power-law internets. In Proc. ACM SIGCOMM, San Diego, CA 2000
[3] ICANN/SSAC, .ICANN SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks,. Mar. 2006.
[4] C. Labovitz, D. McPherson, and F. Jahanian, .Infrastructure attack detection and mitigation,. SIGCOMM 2005, August 2005, tutorial.
[5] R. Beverly and S. Bauer, .The Spoofer Project: Inferring the extent of Internet source address _ltering on the internet,. in *Proceedings of Usenix SRUTI*, Cambridge, MA, Jul. 2005.
[6] S. Kandula, D. Katabi, M. Jacob, and A. Berger, .Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds,. in *NSDI*, 2005.
[7] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, .Inferring internet Denial-of-Service activity,. *ACM Transactions on Computer Systems*, vol.24, no. 2, May 2006.
[8] J.Stewart, .DNS cache poisoning - the next generation,. LURHQ, Technical Report, Jan. 2003.
[9] Paxson, .An analysis of using re_ectors for distributed denialof- service attacks,. *ACM Computer Communications Review (CCR)*,vol. 31, no. 3, Jul. 2001.
[10] K. Park and H. Lee, .On the effectiveness of route-based packet _ltering for distributed DoS attack prevention in power-law internets,. in *Proc.ACM SIGCOMM*, San Diego, CA, Aug. 2001.
[11] Y. Rekhter and T. Li, .A border gateway protocol 4 (BGP-4),. RFC 1771, Mar. 1995.
[12] L. Gao, .On inferring autonomous system relationships in the internet,. *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, Dec. 2001.

Published by SK Research Group of Companies (SKRGC).