ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

Controlling IP Spoofing Through Inter Domain Packet Filter

J. Selvakumar, S. Manikandan

Assistant Professor, Department of ECE, Karpagam College of Engineering, Coimbatore, Tamil Nadu, India

ABSTRACT: The Distributed Denial-of-Service (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 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 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.

I. PROBLEM DEFINITION

The first and long-term recommendation is to adopt source IP address verification, which confirms the importance of the IP spoofing problem. IP spoofing will remain popular for a number of reasons. First, IP spoofing makes isolating attack traffic from legitimate traffic harder: packets with spoofed source addresses may appear to be from all around the Internet. Second, it presents the attacker with an easy way to insert a level of indirection. As a consequence, substantial effort is required to localize the source of the attack traffic. Finally, many popular attacks such as man-in-the-middle attacks, reflector-based attacks, and attackers use IP spoofing and require the ability to forge source addresses. Although attackers can insert arbitrary source addresses into IP packets, they cannot control the actual paths that the packets take to the destination.

Based on this observation, we have proposed the route-based packet filte rs as a way of mitigating IP spoofing. The idea is that by assuming single-path routing, there is exactly one single path between the source node and the destination node. Hence, any packet with the source address and the destination address that appear in a router that is not in path source and destination address should be discarded.

The Internet consists of thousands of network domains or autonomous systems (ASs). Each AS communicates with its neighbors by using the Border Gateway Protocol (BGP), which is the de facto inter-domain routing protocol, to exchange information about its own networks and others that it can reach. BGP is a policy-based routing protocol in that both the selection and the propagation of the best route to a destination at an AS are guided by some locally defined routing policies.

Modules:

- **Check and lookup the local network**
- **Content Selection**
- **Encryption**
- **BGP**
- **Hackers**
- **Decryption**

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

II. MODULE DESCRIPTION

Check and lookup the local network

This is module, which executes at the loading time to check and lookup the local network. It gets all the systems, which are connected, to that local network. This helps to the gets current working nodes that means which are active and ready for access in the network.

Content Selection

It uses a dialog box to open a required file format, but it mainly supports only for the text support files. The file loaded to a file variable, Then it send to the next stage Encryption area.

Encryption

In this the original data is converted to some other format using chips algorithm so that incase some intruder may hack the file at any reason or at any cost, but they won't get the original data unless it decrypted in proper format.

BGP

In this Modules BGP (Border Gateway Protocol) is a protocol that communicates across the network and also monitoring the client present in the network. It has all client details as a table. The connection is established with the client and the Router. The Encrypted data is transmitted to the Router which can send or redirect to the correct destination address. The Router checks whether the sender and receiver are proper to the network. Incase the sender (hacker) is not a proper member in the network then that node is said to the attacker node, then the message will not sent to the destination. Otherwise the message will send to the destination address.

Hackers

The hacker will act as a client in the distributed network. The hacker may have false name in the network and virtually seems to be present within the current network. It selects the destination address which original present in the network.

Decryption

At the destination the received encrypted data will under go decryption to get the original data, which was sent by the sender. Decryption using chips algorithm for the decryption of the received data to the original content. After decryption only the data will be meaningful. The Encryption and Decryption gives the security to data while transferring.

III. MODULE INTERACTION

Module 1:
Given Input:
Neigbouring Node Address
Output
Individual Node Routing Table
Module 2:
Given Input:
1. Destination
2. File
Output:
Routing table for the selected Destination.
Module 3:
Given Input:
Routing Table
Output:
Feasible path
Module 4:
Given Input:
Feasible path
Output:
Filtering the spoofing packet

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

Proposed System

- In our project we propose and study 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.
- It correctly works without discarding any valid packets

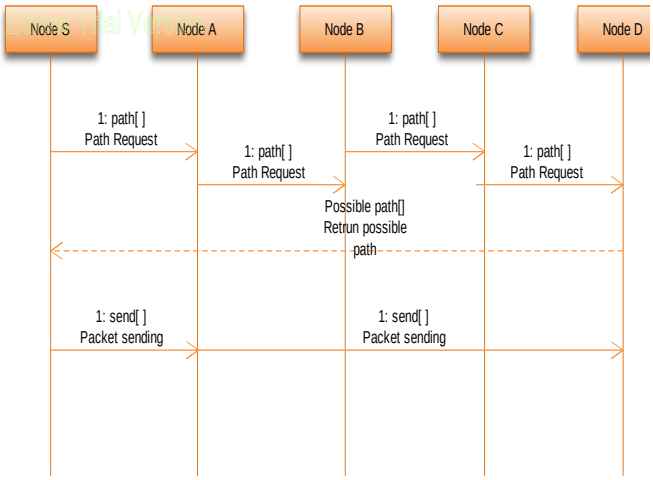
Two distinct sets of routing policies are typically employed by a node:

❖ **Import policies** -- Neighbor-specific import policies are applied upon routes learned from neighbors

❖ **Export policies**.-- whereas neighbor-specific export policies are imposed on locally selected best routes before they are propagated to the neighbors.

BGP is an incremental protocol

A downhill path is a sequence of edges that are either provider-to-customer or sibling-to sibling edges
An uphill path is a sequence of edges that are either customer-to-provider or sibling-to-sibling edges



Challenges:

The first and long-term recommendation is to adopt source IP address verification, which confirms the importance of the IP spoofing problem. IP spoofing will remain popular for a number of reasons. First, IP spoofing makes isolating attack traffic from legitimate traffic harder: packets with spoofed source addresses may appear to be from all around the Internet. Second, it presents the attacker with an easy way to insert a level of indirection. As a consequence, substantial effort is required to localize the source of the attack traffic. Finally, many popular attacks such as man-in-the-middle attacks, reflector-based attacks, and attackers use IP spoofing and require the ability to forge source addresses. Although attackers can insert arbitrary source addresses into IP packets, they cannot control the actual paths that the packets take to the destination.

Based on this observation, we have proposed the route-based packet filters as a way of mitigating IP spoofing. The idea is that by assuming single-path routing, there is exactly one single path between the source node and the destination node. Hence, any packet with the source address and the destination address that appear in a router that is not in path source and destination address should be discarded.

The Internet consists of thousands of network domains or autonomous systems (ASs). Each AS communicates with its neighbors by using the Border Gateway Protocol (BGP), which is the de facto inter-domain routing protocol, to exchange information about its own networks and others that it can reach. BGP is a policy-based routing protocol in that both the selection and the propagation of the best route to a destination at an AS are guided by some locally defined routing policies.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

IV. LITERATURE REVIEW

In recent years, more and more networks with sensitive or even business critical data on them are being interconnected. Simultaneously, hacker activity has grown tremendously because of freely available hacker tools. In order to protect networks, so-called firewalls are deployed that protect against hacker activities. One of the ways to implement a firewall is to make use of so-called packet filters. Packet filtering has proved to be a handy tool to put access controls to IP traffic. Packet filters can be used to block IP packets based on certain criteria such as the protocol used and various protocol characteristics. In early packet filters, filtering decisions were made based solely on the packet that is currently inspected. Data like the source and destination addresses and in UDP and TCP cases the source and destination ports could be used in the filtering decisions. Even the well known 'established' keyword, was based on static information (it inspected the presence of the ACK and RST flags in TCP return traffic. Such filtering could be very well used to protect against spoofing attacks where the attacker would send packets that seem to originate from systems on the inside of the packet filter.

"The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet", Robert Beverly MIT CSAIL , Steven Bauer

Forging, or "spoofing," the source addresses of IP packets provides malicious parties with anonymity and novel attack vectors. Spoofing-based attacks complicate network operator's defense techniques; tracing spoofing remains a difficult and largely manual process. More sophisticated next generation distributed denial of service (DDoS) attacks may test filtering policies and adaptively attempt to forge source addresses. To understand the current state of network filtering, this paper presents an Internet-wide active measurement spoofing project. Clients in our study attempt to send carefully crafted UDP packets designed to infer filtering policies. When filtering of valid packets is in place we determine the filtering granularity by performing adjacent netblock scanning. Our results are the first to quantify the extent and nature of filtering and the ability to spoof on the Internet. We find that approximately one-quarter of the observed addresses, netblocks and autonomous systems (AS) permit full or partial spoofing. Projecting this number to the entire Internet, an approximation we show is reasonable, yields over 360 million addresses and 4,600 ASes from which spoofing is possible. Our findings suggest that a large portion of the Internet is vulnerable to spoofing and concerted attacks employing spoofing remain a serious
concern.

"Botz4Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds" Srikanth Kandula, Dina Katabi,Matthias Jacob ,Arthur Berger

Recent denial of service attacks are mounted by professionals using Botnets of tens of thousands of compromised machines. To circumvent detection, attackers are increasingly moving away from bandwidth floods to attacks that mimic theWeb browsing behavior of a large number of clients, and target expensive higher-layer resources such as CPU, database and disk bandwidth. The resulting attacks are hard to defend against using standard techniques, as the malicious requests differ from the legitimate ones in intent but not in content. We present the design and implementation of Kill-Bots, a kernel extension to protect Web servers against DDoS attacks that masquerade as flash crowds. Kill-Bots provides authentication using graphical tests but is different from other systems that use graphical tests. First, Kill-Bots uses an intermediate stage to identify the IP addresses that ignore the test, and persistently bombard the server with requests despite repeated failures at solving the tests. These machines are bots because their intent is to congest the server. Once these machines are identified, Kill-Bots blocks their requests, turns the graphical tests off, and allows access to legitimate users who are unable or unwilling to solve graphical tests. Second, Kill-Bots sends a test and checks the client's answer without allowing unauthenticated clients access to sockets, TCBs, and worker processes. Thus, it protects the authentication mechanism from being DDoSed. Third, Kill- Bots combines authentication with admission control. As a result, it improves performance, regardless of whether the server overload is caused by DDoS or a true Flash Crowd.

"An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks" Vern Paxson

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 7, July 2013

Attackers can render distributed denial-ofservice attacks more difficult to defend against by bouncing their flooding traffic off of reflectors; that is, by spoofing requests from the victim to a large set of Internet servers that will in turn send their combined replies to the victim. The resulting dilution of locality in the flooding stream complicates the victim's abilities both to isolate the attack traffic in order to block it, and to use traceback techniques for locating the source of streams of packets with spoofed source addresses, such as ITRACE [Be00a], probabilistic packet marking [SWKA00], [SP01], and SPIE [S+01]. We discuss a number of possible defenses against reflector attacks, finding that most prove impractical, and then assess the degree to which different forms of reflector traffic will have characteristic signatures that the victim can use to identify and filter out the attack traffic. Our analysis indicates that three types of reflectors pose particularly significant threats: DNS and Gnutella servers, and TCP-based servers (particularly Web servers) running on TCP implementations that suffer from predictable initial sequence numbers. We argue in conclusion in support of "reverse ITRACE" [Ba00] and for the utility of packet traceback techniques that work even for low volume flows, such as SPIE.

"Practical Network Support for IP Traceback", Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson

This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or "spoofed", source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this traceback can be performed "post-mortem" – after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

"Inferring Internet Denial-of-Service Activity" David Moore

In this paper, we seek to answer a simple question: "How prevalent are denial-of-service attacks in the Internet today?". Our motivation is to understand quantitatively the nature of the current threat as well as to enable longer term analyses of trends and recurring patterns of attacks. We present a new technique, called "backscatter analysis", that provides an estimate of worldwide denial-of service activity. We use this approach on three week-long datasets to assess the number, duration and focus of attacks, and to characterize their behavior. During this period, we observe more than 12,000 attacks against more than 5,000 distinct targets, ranging from well known ecommerce companies such as Amazon and Hotmail to small foreign ISPs and dial-up connections. We believe that our work is the only publically available data quantifying denial-of-service activity in the Internet.

REFERENCES

[1] R. Beverly and S. Bauer, "The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet," Proc. First Usenix Steps to Reducing Unwanted Traffic on the Internet Workshop, July 2005.
[2] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds," Proc. Second Symp. Networked Systems Design and Implementation, 2005.
[3] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," ACM Trans. Computer Systems, vol. 24, no. 2, May 2006.
[4] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson, "Characteristics of Internet Background Radiation," Proc. ACM Internet Measurement Conf., Oct. 2004.
[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," Proc. ACM SIGCOMM Computer Comm. Rev., vol. 30, no. 4, Oct. 2000.
[6] P. Watson, "Slipping in the Window: TCP Reset Attacks," Proc. Fifth CanSec West/core04 Conf., 2004.
[7] J. Stewart, "DNS Cache Poisoning—The Next Generation,"technical report, LURHQ, Jan. 2003.
[8] V. Paxson, "An Analysis of Using Reflectors for Distributed Denialof- Service Attacks," ACM Computer Comm. Rev., vol. 31, no. 3, July 2001.
[9]. Srinivas Aluvala M.Tech (CSE) Jayamukhi Institute of Technological Sciences Warangal (AP), India P.Srinivas Rao Asst.Pof. CSE dept Jayamukhi Institute of Technological Sciences Warangal (AP), India ."Constructing IDPFs to control IP Forging"