Improvements in Inter-Domain Packet Filtering Method of IP Spoofing

Author - Archit Singh, Co-Authors – Rahul Anand, Pragati Singh

Abstract— The Distributed Denial of Services (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.

We propose an improvement in the inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spooling on the Internet. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers. We are using statistical method for selecting packets to be rejected and detecting the corrupt host.

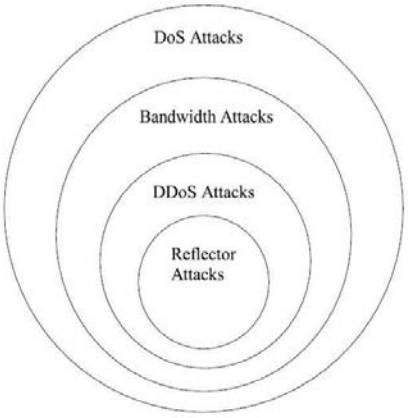
1. Introduction

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. DoS they say is a tool for registering dissent. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy and violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.



The relation of different types of attacks.

The United States Computer Emergency Readiness Team (US-CERT) defines symptoms of denial-of-service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)

- Unavailability of a web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received - (this type of DoS attack is considered an e-mail bomb)
- Disconnection of a wireless or wired internet connection

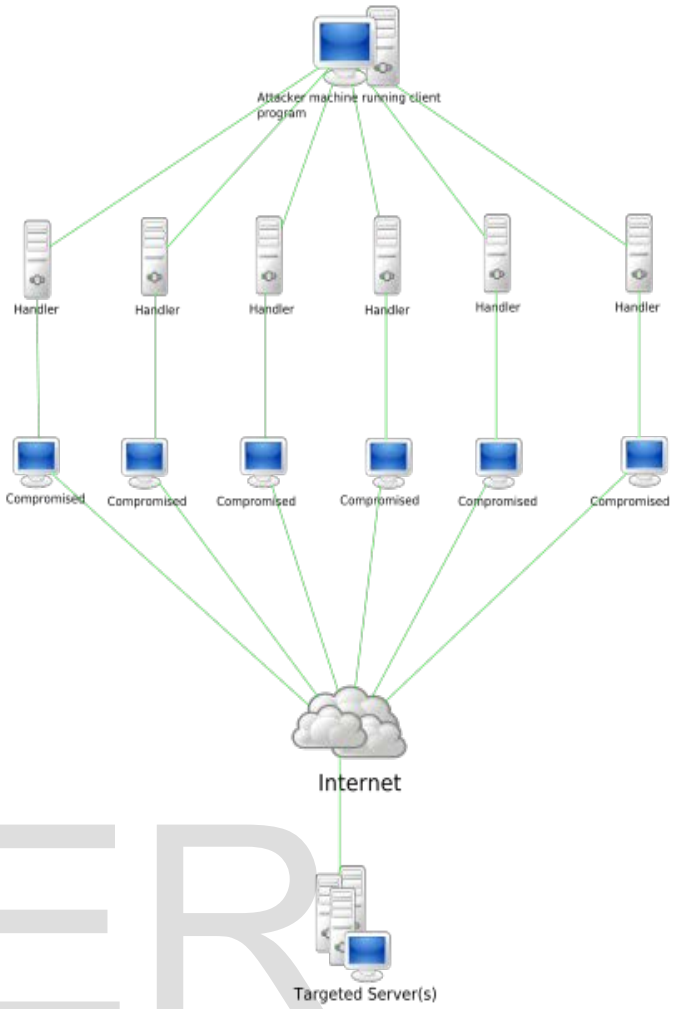
Denial-of-service attacks can also lead to problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by an attack, compromising not only the intended computer, but also the entire network or other computers on the LAN.

If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment.

2. Actual Problem Statement

2.1 Distributed Denial of Service Attack

A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. This is the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted.



The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines.

2.2 IP Address Spoofing

IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

The basic protocol for sending data over the Internet network and many other computer networks is the

Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send a response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

In certain cases, it might be possible for the attacker to see or redirect the response to his own machine. The most usual case is when the attacker is spoofing an address on the same LAN or WAN.

2.3 The Combined Problem

One of the methods used for tackling the Distributed Denial of Service attack problem was blocking the packets from non-trusted IP addresses that were flooding the system. But this method was rendered futile in the cases where the attacker uses IP spoofing to impersonate a trusted user.

Distributed Denial of Service (DDoS) attacks pose an increasingly grave threat to the Internet, as evident in recent DDoS attacks mounted on both popular Internet sites and the Internet infrastructure. Alarmingly, DDoS attacks are observed daily on most of the large backbone networks. One of the factors that complicate the mechanisms for policing such attacks is IP spoofing, which is 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 filtering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofing.

Recently, attackers have increasingly been staging attacks via botnets [4]. In this case, since the attacks are carried out through intermediaries, that is, the compromised "bots," attackers may not utilize the technique of IP spoofing to hide their true identities. It is tempting to believe that the use of IP spoofing is less of a factor. However, recent studies show that IP spoofing is still a common phenomenon: it is used in many attacks, including the high-profile DDoS attacks on root DNS servers in early February 2006. In response to this event, the ICANN Security and Stability Advisory Committee made three recommendations. 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 several 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. Therefore, 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 TCP SYN flood attacks use IP spoofing and require the ability to forge source addresses.

3. Related Terms

Few of the terms that would be used later and need to be discussed:

3.1 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS). The protocol is often classified as a path vector protocol but is sometimes also classed as a distance vector routing protocol. The Border Gateway Protocol does not involve traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule-sets configured by a network administrator. The Border Gateway Protocol plays a key role in the overall operation of the Internet and is involved in making core routing decisions.

The Border Gateway Protocol is the successor to the Exterior Gateway Protocol (EGP) and is currently the most widely used exterior gateway protocol by Internet service providers because BGP allows for fully decentralized routing. BGP was originally designed to help transition from the core ARPAnet model to a decentralized system that included the NSFNET backbone and its associated regional networks.

3.2 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.

3.3 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.

4. An Existing Approach

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.

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, if 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.

4.1 Role of BGP

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 link.

The BGP metric typically is assigned to each 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.

4.2 Role of Packet Filter

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.

4.3 Filtering using IDPF

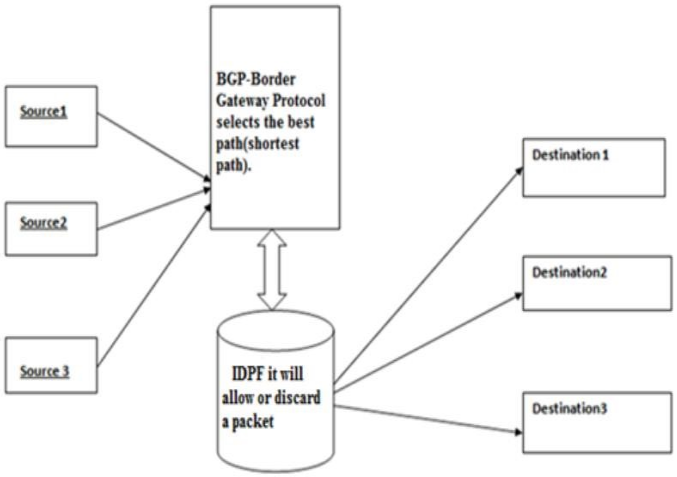
If your site has a direct connection to the Internet, you can use your IDPF to help you out. First make sure only hosts on your internal LAN can participate in trust-relationships (no internal host should trust a host outside the LAN). Then simply filter out *all* traffic from the outside (the Internet)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

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.

4.4 System Architecture



5. Evolution of DDoS

Over the past few years, the attackers have improvised on the DDoS attacks and instead of merely flooding the server with general requests, they now target the specific system intensive operations. These operations require more processing and other system resources and a sudden increase in their volume may destabilize the system. These requests can be of the form of New User signup/login, Product checkout, etc.

In distributed denial-of-service attacks, multiple systems submit as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests. An example is an attack on a victim's phone number. The victim is bombarded with phone calls by the bots, attempting to connect to the Internet.

A botnet is a collection of Internet-connected programs communicating with other similar programs to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a portmanteau of robot and network.

This is how a botnet works:

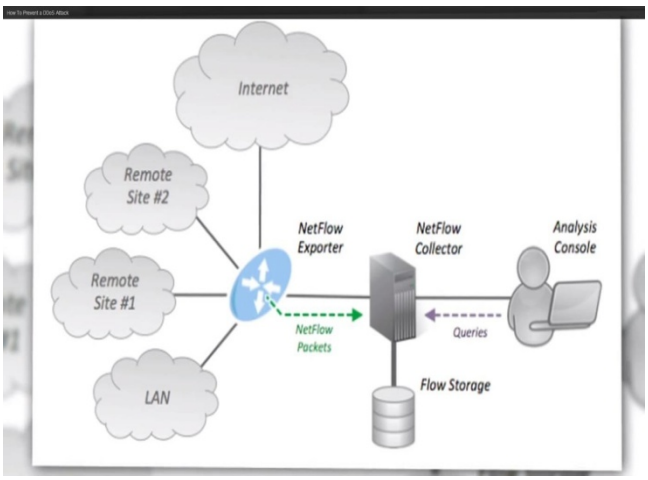
- A botnet operator sends out viruses or worms, infecting ordinary users' computers, whose payload is a malicious application—the bot.
- The bot on the infected PC logs into a particular C&C server.
- A spammer purchases the services of the botnet from the operator.
- The spammer provides the spam messages to the operator, who instructs the compromised machines via the control panel on the web server, causing them to send out spam messages.

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules.

6. An Improved Approach

This approach involves analysis of the network traffic and setting up a baseline for the number of requests for each service provided by the server. In this way, we do not drain away the resources of the server and put a maximum limit to its use.

Our plan is to implement a sentinel tool on the server that puts the above specified analysis. When it sees that things are anomalous and do not comply with the limits set, it realizes that there is a possibility of an attack.



Using the BGP routing protocol, it starts routing the possibly interfering traffic to an application so that it can be analyzed and checked to see if it is bad or interfering. So, from the service provider's perspective, this system analyzes what is going on and tries to automatically shut down the bad traffic.

In this approach, even if the attacker uses IP spoofing to impersonate any trusted client, we can check the new interference coming to the server and block the traffic again. In this way, if there are repeated similar actions from a particular system, we may also block services to the system for a specified period of time.

7. References

- 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.
- International Journal of Students Research in Technology & Management Vol 1(3), May 2013, ISBN 978-93-83006-01-4, Pg 347-352.
- http://en.wikipedia.org/wiki/Denial-of-service_attack
- http://en.wikipedia.org/wiki/IP_address_spoofing
- http://en.wikipedia.org/wiki/Border_Gateway_Protocol