ENGINEERING AND TECHNOLOGY IN INDIA
Volume 1 Issue 2 (October, 2010) Page : 110-114

REVIEW ARTICLE

Accepted : *June, 2010*

A method to prevent IP spoofing attacks

R. ABIRAMI ARASI, K. KUPPUSAMY AND T. RAJENDRAN

Key words : I.P. spoofing, Spoofing attack

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 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 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. 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. 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 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 TCP SYN flood attacks use IP spoofing and require the ability to forge source addresses. Based on this observation, Park and Lee 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 p (s, d) between the source node s and the destination node d. Hence, any packet with the source address s and the destination address d that appear in a router that is not in p (s, d) should be discarded.

These study mainly concentrate on following objectives to describe how can practically construct IDPFs at an AS by only using the information in the locally exchanged BGP updates; to establish the conditions under which the proposed IDPF framework works correctly in that it does not discard packets with valid source addresses; and to evaluate the effectiveness of the proposed architecture, we conduct extensive simulation studies based on AS topologies and AS paths extracted from real BGP data.

Content on a spoofed page, the highjacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The highjacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam. Web site administrators can minimize the danger that their IP addresses will be spoofed by implementing hierarchical or one - time passwords and data encryption / decryption techniques. Users and administrators can protect themselves and their networks by install ting and implementing firewalls that block outgoing packets with source addresses that differ from the IP address of the user's computer or internal network.

Methods of attack:

A "denial - of - service" attack is characterized by an explicit attempt by attackers to prevent legitimate users

Abirami Arasi, R., Kuppusamy, K. and Rajendran, T. (2010). A method to prevent IP spoofing attacks, *Engg. Tech. India,* **1** (2) : 110-114

of a service from using that service. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

– Consumption of computational resources, such as bandwidth, disk space, or processor time

– Disruption of configuration information, such as routing information.

– Disruption of state information, such as unsolicited resetting of TCP sessions.

– Disruption of physical network components.

– Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to:

– Max out the processor's usage, preventing any work from occurring.

– Trigger errors in the microcode of the machine.

– Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock - up.

– Exploits errors in the operating system to cause resource starvation and/or thrashing, *i.e.* to use up all available facilities so no real work can be accomplished.

– Crash the operating system itself.

– iFrame (D) DoS, in which an HTML document is made to visit a webpage with many KB's of information many times, until they achieve the amount of visits to where bandwidth limit is exceeded.

ICMP flood:

A smurf attack is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination. To combat Denial of Service attacks on the Internet, services like the Smurf Amplifier Registry have given network service providers the ability to identify misconfigured networks and to take appropriate action such as filtering.

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping - t" command from unix like hosts (the - t flag on Windows systems has a far less malignant function). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim. SYN flood sends a flood of TCP / SYN packets, often with a forged sender address. Each of these packets is handled like a connection request, causing the server to spawn a half - open connection, by sending back a TCP / SYN - ACK packet, and waiting for a packet in response from the sender address. However, because the sender address is forged, the response never comes. These half - open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

Teardrop attack:

A Teardrop attack involves sending mangled IP fragments with overlapping, over - sized, payloads to the target machine. A bug in the TCP / IP fragmentation re - assembly code of various operating systems causes the fragments to be improperly handled, crashing them as a result of this. Windows 3.1x, Windows 95, and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.

Peer - to - peer attacks:

Attackers have found a way to exploit a number of bugs in peer - to - peer servers to initiate DDoS attacks. The most aggressive of this peer - to - peer - DDoS attacks exploits DC++. Peer - to - peer attacks are different from regular botnet - based attacks. With peer - to - peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a 'puppet master,' instructing clients of large peer - to - peer file sharing hubs to disconnect from their peer - to - peer network and to connect to the victim's website instead. As a result, several thousand computers may aggressively try to connect to a target website. While a typical web server can handle a few hundred connections / sec before performance begins to degrade, most web servers fail almost instantly under five or six thousand connections / sec. With a moderately big peer - to - peer attack a site could potentially be hit with up to 750,000 connections in a short order. The targeted web server will be plugged up by the incoming connections.

While peer - to - peer attacks are easy to identify with signatures, the large number of IP addresses that need to be blocked (often over 250,000 during the course of a big attack) means that this type of attack can overwhelm mitigation defenses. Even if a mitigation device can keep blocking IP addresses, there are other problems to consider. For instance, there is a brief moment where the connection is opened on the server side before the signature itself comes through. Only once the connection is opened to the server can the identifying signature be sent and detected, and the connection torn down. Even tearing down connections takes server resources and can harm the server. This method of attack can be prevented by specifying in the p2p protocol which ports are allowed or not. If port 80 is not allowed, the possibilities for attack on websites can be very limited.

Permanent denial - of - service attacks:

A permanent denial - of - service (PDoS), also known loosely as phlashing, is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.[6] Unlike the distributed denial - of - service attack, a PDoS attack exploits security flaws in the remote management interfaces of the victim's hardware, be it routers, printers, or other networking hardware. These flaws leave the door open for an attacker to remotely 'update' the device firmware to a modified, corrupt or defective firmware image, therefore bricking the device and making it permanently unusable for its original purpose. The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacker communities such as Hack a Day.

PhlashDance is a tool created by Rich Smith (an employee of Hewlett - Packard's Systems Security Lab) used to detect and demonstrate PDoS vulnerabilities at the 2008 EUSecWest Applied Security Conference in London.

Application level floods:

On IRC, IRC floods are a common electronic warfare weapon. Various DoS - causing exploits such as buffer overflow can cause server - running software to get confused and fill the disk space or consume all available memory or CPU time.

Other kinds of DoS rely primarily on brute force, flooding the target with an overwhelming flux of packets, oversaturating its connection bandwidth or depleting the target's system resources. Bandwidth - saturating floods rely on the attacker having higher bandwidth available than the victim; a common way of achieving this today is via Distributed Denial of Service, employing a botnet. Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs. A "banana attack" is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets. An attacker with access to a victim's computer may slow it until it is unusable or crash it by using a fork bomb.

Nuke:

A Nuke is an old denial - of - service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

In online gaming, nuking is used by spamming another user, or all other users, with random repeated messages in quick succession. Such techniques are also seen in instant messaging programs as repeatedly sending text can be assigned to a macro or Apple Script. Modern operating systems are usually resistant to these nuke attacks, and online games now have third party "Flood control". A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out - of - band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death

Proposed IP spoofing method:

Personal information:

The personal information form is just that: a place where we can define personal information about ourself. Along with some standard information like user name and email address, we also allow us to specify the location of an icon and a profile picture. If user does not have images for these fields, just leave them blank.

Change password:

It is highly recommended that users change their passwords regularly. Some important rules to follow when creating a new password. Do not use birth - dates, bank - card pin numbers, telephone numbers, or anything that can be easily guessed.

Forum preferences:

The forum preferences form allows user to define how site appears and functions for user. Any changes made on this form take place immediately, and user do NOT need to press a save button. When we make a change on this form, a status message should appear on our screen to notify us when the changes have been completed.

Discussions:

The registered user can add the discussion topics using discussion tab. Administrator can also add the discussion topics by click "Start new Discussion" link. For each discussion, user can see "how many comments are there under the discussion? Who did post comment first?" such like that.

Comments:

The registered user can add the comments. The user edits and deletes their comments only.

Advanced searching:

If we click on the search tab, we might notice the little "Advanced" button to the left of the search inputs. If we click this button, we'll see an expanded version of the three different types of searches. If we tinker around with these inputs and run a few different searches, we'll see some interesting things show up in the search input when we're viewing results. For example: under the "Discussion topic search" heading, enter our username into the "where the author was" input and click search. When the results come up, the search input will contain: If we take it a step further and select a category from the category dropdown AND enter our username in the "where the author was" input, we'll see something like this in the search input when we run the search: This time the search results will contain all discussions that we started in the "Random" category. Take it even further and enter "test" in the "find discussion topics containing" input and we'll see something like this: This time the search results will contain all discussions that we started in the "Random" category where the word "test" appears in the discussion topic. When it came to doing searches.

Password retrieval:

If we forget our password, we can reset it by clicking on the "Forgot your password?" link on the sign - in page. We will be prompted to enter your username. Password reset instructions will then be emailed to the email address associated with that username. Using this form does not change our password. If we are the owner of that email address, you will receive an automated message from the application that will contain a link back to the server where we can change our password.

Discussion and control panel listings:

In this area, it can find options for the maximum number of items a user can see in discussions, discussion lists, searches or in their side bar panel. Each of the controls listed is fairly self explanatory, and offers a variety of options to choose from depending on the list in question. By default, each of these will be set to a fairly reasonable value which should strike a balance between the numbers of items displayed while keeping server performance in mind. If we run a busy forum, keeping these numbers down will result in faster page loads and less overall page cluttering.

Post privilege:

Administrator can set the status as De - Active for user comments that base on the word filter. After the user post their comments. The comments will be checked by the word filter function that whether there is any other bad word contained in the Comments. If the bad words are contained in the post comments means that post status is set as De - active. So this post comments are not displayed on the site and user could not see this De - active post comments. Only active post comments will be displayed on the site and user can see the post. The administrator can see like this post comments via control panel. The administrator can delete this type of comments by delete link on the Post privilege page. Suppose the administrator wants to post this comments, they can change the status as Active. Then this active post will be displayed on the site.

IP blocking:

This feature is used for security purpose. Administrator can block the user temporarily by IP Address. When the user log into the site, the IP Address is captured. If the administrator wants to block the particular user, they can block user by enter the IP Address in the IP Blocking Field text box and click the Save button. The administrator can see the blocked IP address details through View IP blocks link. In this View IP Block page, we have displayed status and delete link. If the IP address's status is Active, the blocked user can access the site. If the IP address's status is DeActive, the blocked user can not access the site. The IP Address is deleted by delete link.

User blocking:

It is same as IP blocking. Administrator can block the user temporarily by their username. Here also have displayed Status and delete link.

Membership applicants:

Use this form to approve or decline new membership applicants. If there is any new user as member, that user will be displayed here for getting approved by the admin. Once approved, the permission will be set to the new user. That new member can access the site now. Otherwise that new member could not access the site because of the access permission.

Conclusion:

In this dissertation, a new method has been devised to prevent IP spoofing. This method includes many ways to secure the public forums, through Filtering concept. It has been implemented in PHP and MY - SQL. Using this method, the attackers can be identified automatically and banned without administrators Need. The effective filtering gives more control to the administrator. The administrator can block the attackers using the IP address, user name or e - mail.

The most effective IP Blocking method has been implemented in this research work. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet server. IP banning is commonly used on to protect against attacks. On an Internet forum or Web site an IP ban is often used as a last resort to prevent a disruptive member from access, though a warning and / or account ban may be used first. Dynamic allocation of IP addresses can complicate incoming IP blocking, rendering it difficult to block a specific user without blocking a larger number of IP addresses, thereby risking collateral damage caused by ISPs sharing IP addresses of multiple internet users. IP banning is also used to limit the syndication of content to a specific region. To achieve this IP - addresses are mapped to the countries they have been assigned to. The system is thus effective and simple. The implementation of new method devised blocks the unwanted messages also can block the misbehaved users and stop advertisers from spamming the system.

REFERENCES

compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm___http://technet.microsoft.com/en-us/library/cc261825.aspx_http://en.wikipedia.org/wiki/IP_address www.google.com/support/appsecurity/bin/answer.py?hl=en&answer_searchnetworking.techtarget.com/sDefinition/0,,sid7_gci http://en.wikipedia.org/wiki/Routing

Address for correspondence :
R. ABIRAMI ARASI
Govt. Arts College for Women
RAMANATHAPURAM (T.N.) INDIA
Email : abiramiarasi6@yahoo.co.in

Authors' affiliations :
K. KUPPUSAMY
Department of Computer Science and Engineering
Alagappa University,
KARAIKUDI (T.N.) INDIA

T. RAJENDRAN
Department of Social Sciences,
Horticultural College and Research Institute
(Tamil Nadu Agricultural University)
PERIYAKULAM (T.N.) INDIA
Email : rajae06@gmail.com

****