RESEARCH ARTICLE OPEN ACCESS

DNS Backscatter Prevention Using Perturbation Methodology

Mrs. S.Selvi [1], Mrs.S.Nirmalajancy [2]
Assistant Professor [1], Research Scholar [2]
Department of Computer Science
Tiruppur Kumaran College for Women, Tiruppur
Tamil Nadu - India

ABSTRACT

The Backscattering is one of spammer spoofing technique used in domain by legitimate ones, thus the spam is send by anyone to us, we cant realize it is spam, the Non delivery report is accessed mechanism is called out when the sender sends the spoofing content to all, for the legitimate users bounce messages are send to innocent one those email or DNS servers etc, thus the DNS address is spoofed it is known as DNS Backscatter, The Non-Delivery Report makes ones proof of send mail or packets to server is doubt, thus we have an Perturbation methodology to made secure based packet sending through networks, also bounce messages can give harm to the sender, thus we need to propagate wide technology to overcome using perturbation, in that we have introduce the stages, that gives an very effective to prevent backscatter in network, it also gives headers, of messages previously send through that we can easily identify it is non delivery messages (bounced) or send by victim, this title defines thoroughly of prevention.

Keywords:- Backscatter, Non-Delivery Messages, DDoS Attacks, Perturbation

I. INTRODUCTION

The main objective of any flooding attack is the speedy use of dangerous system resources in order to paralyze the afford services and make them occupied to its rightful users. Assuming that such an attack takes place against or use a critical part like the DNS it is very likely that would quickly harm the overall network's services making it unavailable to any rightful user. Many researchers have sketch out the threat of flooding attacks using recursive DNS name servers open to the world. For instance, according to a recent study, which is based on case studies of several attacked ISPs report to have on a volume of 2.8 Gbps, one event point to attacks achievement as high as 10 Gbps and used as many as 140,000 broken name servers. Flooding attacks against DNS are similar to other well documented Internet services flooding attacks and could be launched in two discrete ways. In the first case the attacker sends a huge number of fake DNS requests either from a single or numerous sources, depending on the flooding architecture utilized. An instance of numerous sources flooding architecture attack against a DNS is depicted in figure. According to this development, the attacker arrange usually innocent hosts, called bots, to concurrently make fake DNS needs aiming at troublesome the normal DNS operation by consuming its resources; mainly memory and CPU.

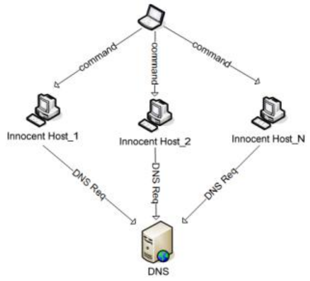

Fig 1.1. DNS Backscattering

On the additional hand, the most complicated and "modern" attacks use the DNS method themselves in a try to enlarge flooding attack consequences. Putting it one more way, in a DNS magnification attack state, the attacker exploits the information that little size requirements could produce better answer. Particularly, new RFC condition behind IPv6, DNS Secure, Naming Authority Pointer (NAPTR) and other extensions to the DNS system, need name servers to go back much better responses to queries. The relation among a request and the parallel response is known as the strengthening factor and is calculate.

The attacker use a discrete plan similar to that obtainable in obvious that the bandwidth and resources use rate at the victim boost very fast. Furthermore, it should be famous that the attacker featly spoof all query wants to include an precise type of DNS provide in order the dependable DNS server to make large responses. This task could be managed either by determine which DNS servers accumulate RRs that when request create large responses or by cooperate a DNS server and consciously include a precise record – also known as the intensification record - that will make a large reply. An illustration of this method, exploiting large TXT records which is introduced in wide DNS (EDNS). As stated in by combining dissimilar reaction types, the strengthening effect can reach up to a feature higher than 60. After that, the attacker collects a list of open recursive name servers that will recursively query for, and then return the strengthening record he/she created. Even a list of known name servers may be more than sufficient. As stated in there is a 75% chance that any known name server is an open resolver too, thus a copy of a TLD zone file may be enough.

Protection Mechanisms

In here the protection mechanism is countermeasure using the strengthening of network and defend against the attacks, in general the system is given very secured against the DNS DDos attacks and other protection is coped are deployed in each network, The work of acting parallel is very big opinion to build more inattentive thing of robust DNS infrastructure and the protection in our network is before attack.

DNS server now can occupy transportation with response, such as malign user is fitted to produce the suitable spoofed DNS requests in the name of very clear. The level of protection is should be introduced in spoof detection mechanism and implemented in firewall as well. Moreover, to mitigate DNS cache poison and Man-In-The-Middle (MITM) attacks, which usually are launch at the near the beginning stages of a DNS intensification attack, additional safety mechanisms should be employed. These are necessary in order to ensure the truthfulness and origin verification of the DNS data that reside either in RR cache or in the region file. Apart from well conventional practices to strongly configure DNS servers, one more effective remediation, at least against outsiders, is to immobilize open recursion on name servers from outside sources and only tolerant recursive DNS create from trusted sources. This method significantly diminishes the intensification vector. Obtainable data until now disclose that the majority of DNS servers operate as open recursive servers. The dimension factory reports that more than 75% of domain name servers of about 1.3 million sampled permit recursive name service to random querying sources. This leaves deserted name servers to both cache poisoning and DoS attacks.

Amplification Factor = size of (response) / size of (request)

The bigger the intensification factor is, the quicker the bandwidth and resource expenditure at the victim is induced. Consequently, in the case of DNS amplification attack the aggressor is based on the fact that a single DNS request (small data length) could generate very larger responses (bigger data length). For example, in the initial DNS specification the DNS answer was restricted up to 512 bytes length, while in even bigger. The attack unfolds as follows: The invader falsifies the source address field in the UDP datagram to be that of a host on the victims' network. Using the spoofed address, a DNS query for a valid reserve record is crafted and sent to a middle name server. The last entity is usually an open recursive DNS server, which forwards the final response towards the target machine.

II. RELATED WORK

Inferring Internet Denial-of-Service Activity: "How common are denial-of-service attacks in the Internet?" Our incentive is to quantitatively appreciate the nature of the present threat as well as to allow longer-term analysis of trend and chronic patterns of attacks. We present a new technique, called "backscatter analysis," that supplies a conservative approximation of worldwide denial-of-service movement. We use this move toward on 22 traces (each covering a week or more) gather over three years from 2001 through 2004. Crosswise these corpuses we quantitatively assess the number, length, and focus of attack, and qualitatively typify their behavior. In total, we observed over 68,000 attacks directed at over 34,000 distinct victim IP addresses---ranging from well-known e-commerce company such as Amazon and Hotmail to small foreign ISPs and dial-up connections. We believe our technique is the first to provide quantitative approximation of Internet-wide denial-of-service activity and that this article describes the most complete public measurements of such activity to date. A framework for classifying denial of service attacks: Initiation a denial of service (DoS) attack is small but discovery and reply is a painfully slow and often a physical process. Automatic classification of attacks as single- or multi-source can help focus a response, but current packet-header-based approach are vulnerable to spoofing. The work introduces a structure for classify DoS attack based on header content, and novel techniques such as transient ramp-up behavior and spectral analysis. Although headers are easily forged, we show that characteristics of attack ramp-up and attack spectrum are more difficult to spoof. To evaluate our framework we monitored access links of a regional ISP detecting 80 live attacks. Header analysis identified the number of attackers in 67 attacks, while the remaining 13 attacks were classified based on ramp-up and spectral analysis. We validate our results through monitoring at a second site, controlled experiment, and simulation. We use experiments and simulation to understand the underlying reasons for the characteristics observed. In addition to helping understand attack dynamics, classification mechanisms such as ours are important for the development of realistic models of DoS traffic, can be packaged as an automated tool to aid in rapid response to attacks, and can also be used to estimate the level of DoS activity on the Internet. "Study of a Denial of Service Attack on TCP:" This research sketch out a network-based denial of service attack for IP (Internet Protocol) based networks. It is popularly called SYN flooding. It works by an attacker sending many TCP (Transmission Control Protocol) connection requests with spoofed source addresses to a victim's machine. Each request causes the targeted host to instantiate data structures out of a limited pool of resources. Once the target host's resources are exhausted, no more incoming TCP connections can be established, thus denying further legitimate access. The research contributes a detailed analysis of the SYN flooding attack and a discussion of existing and proposed countermeasures. Furthermore, we introduce a new solution approach, explain its design, and evaluate its performance. Our approach offers protection against SYN flooding for all hosts connected to the same local area network, independent of their operating system or networking stack implementation. It is highly portable, configurable, extensible, and requires neither special hardware, nor modifications in routers or protected end systems. A taxonomy of DDoS attack and DDoS defense mechanisms: Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This research presents two taxonomies for classifying attacks and defenses, and thus provides researchers with a better understanding of the problem and the current solution space. The attack classification criteria was selected to highlight commonalities and important features of attack strategies, that define challenges and dictate the design of countermeasures. The defense taxonomy classifies the body of existing DDoS defenses based on their design decisions; it then shows how these decisions dictate the advantages and deficiencies of proposed solutions. A Path Identification Mechanism to Defend Against DDoS Attacks: Distributed denial of service (DDoS) attacks continue to plague the Internet.

III. BACKGROUND STUDY

3.1. Problems In Present System

Denial-of-service attack can be simply explained with the analogy of the telephone network. A telephone number can be easily attacked by calling to that number by a number of people simultaneously, which in turn not give access to a legitimate caller. A denial-of-service attack is a malignant attempt by a single person or a group of persons to disrupt an online service. Denial-of-service attacks have caused huge financial losses in recent years in the Internet. Denial-of-Service attacks a businesses on websites like eBay.com, amaon.com, yahoo.com, ZDNet.com, Buy.com and a lot of other similar websites

Most of the attacks that come under a denial-of-service are bandwidth attacks. The attackers generate a huge traffic in the network and overload the network with unwanted or bogus Internet packets. Detection of bandwidth attack is difficult when the detector is far from the victim. But it becomes easier when the detector is placed near to the victim. Recently, a lot of denial-of-service attack detection schemes have been proposed. Most of these schemes come under volume-based scheme or feature-based scheme. Volume-based scheme needs a detectable disruption in the traffic volume. When the attack is done gradually, then there is a possible vulnerability in some volume based scheme. On the other hand, feature-based scheme detects the attack by inspecting the header information. It checks the header, and some schemes even check the data parts as well to detect any possible anomaly in the traffic. But the checking of every single packet is time consuming and if the traffic is very high, it becomes very difficult. Feature based-schemes are most accurate in detection, but they are notoriously processor hungry. This thesis focuses on another approach, which takes the positive sides of both volumes-based approach and feature-based approach, detecting denial-of-service attack using packet size distribution. The method only uses the entropy of the packet size, and when there is a spike in the packet size entropy- time series, it could be a potential denial-of-service attack.

Network Attacks

- Reconnaissance Attacks
- Access Attacks
- Denial-of-Service Attacks

These attacks are not discrete. These attacks can be used in combination to meet the goals of the malicious attacker

Reconnaissance Attacks

Reconnaissance attacks are used to gather information about a target network or a system. Such an attack may seem harmless at the time and may be overlooked by network administrators as network noise, but it is usually the information gained through reconnaissance attack that is used in subsequent access or denial-of-service attack. Several means may be used to gather information about an organization and could include automated and technological attacks as well as human social attacks. Examples might include ICMP ping sweeps against a network or SNMP walking technologies to gather network map and device configuration data. Likewise, application level scanners could be used to search for vulnerabilities such as web server CGI or ASP weakness.

Access Attacks

Access attack can be manual or automated and may be composed of unstructured or structured threats. Access attacks are categorized into data retrieval attacks, system access and privilege escalation. The first form of access attack is the unauthorized data retrieval in which information is read, copied or moved to a system. The data retrieval access attack is a common form of internal threats and is largely the result of poorly configured file and directory permissions. For instance, world readable Windows file shares or Unix NFS directories are relatively simple ways for unauthorized users to gain access to potentially sensitive data such as accounting or human resource information. Use of proper mounting or access permission and even encryption could prevent such access.

Denial-of-Service Attacks

A third form of network attack is known as denial-of-service attack. Here the attacker seeks to prevent the legitimate use of service or system. Often times, this is accomplished by overwhelming an infrastructure with bogus requests for service. Denial-of-service attacks can also be caused by corrupted data or configurations. For instance, a denial of service attack could be the result of an intentionally corrupted BGP protocol routing configuration.

ICMP flooding Attack or Ping to death

A Denial of Service attack that sends large amounts of ICMP packets to a victim in order to crash the TCP/IP buyer on the victim's machine and cause it to stop responding to TCP/IP requests is called an ICMP flooding attack or Ping flooding attack.

IP Spoofing

An application program fills the header fields of the IP packet with any IP address it wants while writing to a raw socket. Root permission is required to do such actions which is always known to a user running Linux on a PC. If routing is purely based on the IP destination address only, it won't check the Source IP address. In Re detection attacks, attackers use one specific IP source address on all outgoing IP packets to make all returning IP packets go to the unfortunate owner of that address. The main use of IP spoofing is to hide the location of attacker in the network.

IV. PROPOSED METHODOLOGY

4.1. BACKSCATTER:

Recipients of such messages see them as a form of unsolicited bulk email or spam, because they were not solicited by the recipients, are substantially similar to each other, and are delivered in bulk quantities. Systems that generate email backscatter may be listed on various email blacklists and may be in violation of internet service providers' Terms of Service.

Backscatter occurs because worms and spam messages often forge their sender addresses. Instead of simply rejecting a spam message, a misconfigured mail server sends a bounce messageto such a forged address. This normally happens when a mail server is configured to relay a message to an after-queue processing step, for example, an antivirus scan or spam check, which then fails, and at the time the antivirus scan or spam check is done, the client already has disconnected. In those cases, it is normally not possible to reject the SMTP transaction, since a client would time out while waiting for the antivirus scan or spam check to finish. The best thing to do in this case, is to silently drop the message, rather than risk creating backscatter.

Measures to reduce the problem include avoiding the need for a bounce message by doing most rejections at the initial SMTP connection stage; and for other cases, sending bounce messages only to addresses which can be reliably judged not to have been forged, and in those cases the sender cannot be verified, thus ignoring the message (i.e., dropping it).

4.1.1. DoS Attack Prevention in Backscattering:

Most of the time the attacker launches a DoS attack by sending a large amount of bogus data to interfere or disrupt the service on the server. Using a volume-based scheme to detect such attacks would not be able to inspect short-term denial-of-service attacks, as well as cannot distinguish between heavy load of legitimate users and huge number of bogus messages from attackers. Enabling early detection of Denial-of-service (DoS) attacks in network traffic is an important and challenging task because Denial-of-Service attacks have become one of the most serious threats to the Internet. There are methods based on packet size entropy detection. Here what we are introducing is a hybrid approach which will use address distribution as well as packet size entropy.

An discoverer is a particular IP address that touches many destination. In the application classes we study, originators interact with their targets. In principle the originator could be the victim of spoofed traffic (such as a DNS server as part of an amplification attack); we have not recognized such originators in our data.

The movement prompts the target’s interest in discovering the originator’s domain name from its IP address: a reverse DNS mapping that causes a requester to make a reverse query if the result is not already cached. This query may be for logging (as by firewalls), to perform domain-name based access control, or to characterize the originator (for example, mail servers that consider the sender’s hostname as part of anti-spam measures). The requester is defined as the computer that does resolution of the reverse name. That the target and the requester may be the same computer, or the requester may be a dedicated recursive resolver shared by several targets.

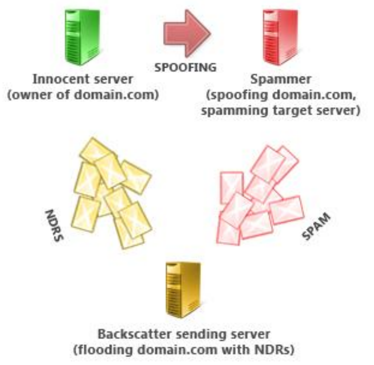

Fig 4.1. DNS Spoof with Backscatter

The Non delivery report of network packets are very harmful to the user agent, In some cases, the reecipient server realizes the email cannot be delivered only after the SMTP conversation has ended, and it tries to notify the sender by sending an NDR email. This practice was OK before the time of spammers and email forgery (even the RFC says it should be done this way), but nowadays, it is strongly discouraged. Such thing may occur if the email was relayed through a secondary MX or front-end server to a primary MX/back-end server, (so the email has already been accepted from the original sender by the secondary MX/front-end), but the relay target server (primary MX/back-end) cannot deliver the email.

a) DNS Setup Stage: This phase takes place right after DNS is established, but before any packets are transmitted over the network. In this phase, Sender decides on a symmetric-key crypto-system (encryptkey, decryptkey) and Receiver symmetric keys key1, . . . , keyK, where encryptkey and decryptkey are the keyed encryption and decryption functions, respectively. S securely distributes decryptkey and a symmetric key keyj to node nj on PSD, for j = 1, . . . , K. Key distribution may be based on the public-key crypto-system such as RSA: Sender encrypts keyj using the public key of node nj and sends the cipher text to nj . nj decrypts the cipher text using its private key to obtain keyj . Sender also announces two hash functions, H1 and HMAC key , to all nodes in PSD. H1 is unkeyed while HMAC key is a keyed hash function that will be used for message authentication purposes later on. Besides symmetric key distribution, Sender also needs to set up its Perturbation keys. Let e : G × G → GT be a computable bilinear map with multiplicative cyclic group G and support Zp, where p is the prime order of G, i.e., for all α, β ∈ G and q1, q2 ∈ Zp, e(α q1 , βq2) = e(α, β) q1q2 . Let g be a generator of G. H2(.) is a secure map-to-point hash function: {0, 1} ∗ → G, which maps strings uniformly to G. S chooses a random number x ∈ Zp and computes v = g x . Let u be another generator of G. The secret PERTURBATION key is sk = x and the public PERTURBATION key is a tuple pk = (v, g, u).

b) Backscatter Avoiding methodology: After the completion of DNS setup phase, source generates signatures and add these signatures to the packets and send to the route. Each node stores signature for the proof of reception in its database for the future purpose. Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes ri = H1(Pi) and generates the PERTURBATION signatures of ri for node nj , as follows sji = [H2(i||j)u ri] x , for j = 1, . . . , K

where || denotes concatenation. These signatures are then sent together with Pi to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes. More specifically, after getting sji for j = 1, . . . , K, S iteratively

c) Spoof Checking Stage: This phase comes into research when receiver receives ACK message from the source. Each node sends the bitmap of packet received and also the signature and it compares the signatures with the stored signatures. If it is correct then it will prove that node has received all the packets. Here node cannot tell that it has received a packet when it does not receive it.

d) Virtual Circle Enable: While sending and receiving of packets the virtual circle is to be enable between certain DNS server, sender and receiver through this circle no IP spoofing is enter and make backscatter through this is done by the above three phases reservedly.

V. CONCLUSION

We believe that the flourishing conclusion of this attempt will create basic insights into the nature of malicious behavior on the Internet and therefore the best instructions for mitigating that behavior. In less than three years, large-scale Internet attacks such as denial-of-service flooding and self-propagating worms have emerged as critical threats to our communications transportation. Moreover, during this same period these attacks have undergone rapid evolution and refinement. We can no longer afford to analyze each new attack innovation post facto with microscope and tweezers. It has become essential for the Internet community to develop meaningful and up-to-date quantitative characterizations of attack activity such as those that we have proposed. Defending distributed denial of service attacks is challenging, due to their multifaceted natures: dynamic attack rates, various kinds of targets, big scale of message hackers etc. he DDoS problem could be very difficult. The journal involves that how to overcome of Distributed Denial of Service and backscatter in DNS using Perturbation methodology.

REFERENCES

[1] Sandoval, G. ; Wolverton, T.(2000, February 9). \Leading Web sites under attack" [online].Available: http://news.cnet.com/2100-1017-236683.html

[2] Wikipedia, Free Encyclopedia.(2012, July 11). \Timeline of Internet conflicts" [online].Available:http://en.wikipedia.org/wiki/Timeline of Internet conflicts#2000

[3] Udhayan, J. ; Prabu, M.M. ; Krishnan, V.A. ; Anitha, R. \Reconnaissance Scan Detection Heuristics to disrupt the pre-attack information gathering ". In International Conference on Network and Service Security, N2S '09, pages 1 - 5, June 24-26 2009.

[4] Carl, G. Kesidis, G. ; Brooks, R.R. ; Rai, S. "Denial-of-service attack-detection techniques". Internet Computing, IEEE (Volume:10 , Issue: 1), pages 82 - 89, Jan.-Feb. 2006

[5] Udhayan, J. ; Anitha, R. \Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis". IEEE International Advance Computing Conference, pages 558 - 564, March 6-7 2009.

[6] Kumar, S. ; Azad, M. ; Gomez, O. ; Valdez, R. \Can Microsofts Service Pack2 (SP2) Security Software Prevent SMURF Attacks?". International Conference on Internet and Web Applications and Services/Advanced International Conference on Telecommunications, AICT-ICIW '06, page 89 February 19 -25 2006.

[7] Cert Advisory CA-1996-26, "Denial of Service Attack via ping", http://www.cert.org/ advisories/CA-1996-26.html, Dec. 1997.

[8] Gibson, S., "DRDoS Distributed Reflection Denial of Service",http://grc.com/dos/ drdos.htm, 2002.

[9] Glenn C., Kesidis, G., Brooks, R. R. and Suresh Rai, "Denial-of-Service Attack-Detection Techniques" IEEE Internet computing 2006.

[10] Peng, T., Leckie, C. and Kotagiri, R., "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", to appear in ACM Computing Surveys.

[11] Mirkovic, J. et al., Internet Denial of Service: Attack and Defense Mechanism.

[12] Security and Stability Advisory Committee, "DNS Distributed Denial of Service (DDoS) Attacks",

http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf, March 2006.

[13] Mockapetris P., "Domain Names – Concepts and Facilities", RFC 1034, November 1987.

[14] Mockapetris P., "Domain Names – Implementation and Specification", RFC 1035, Nov. 1987.

[15] Vixie P., "Extension Mechanisms for DNS", RFC 2671, August 1999.

[16] Arends, R., Austein, R., Larson, M., Massey, D., Rose, S., "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[17] Arends, R., Austein, R., Larson, M., Massey, D., Rose, S., "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[18] Guo, F., Chen, J., and Chiueh, T., "Spoof Detection for Preventing DoS Attacks against DNS Servers", In Proceedings of the 26th IEEE international Conference on Distributed Computing Systems , July 2006

[19] Chandramouli, R. and Rose, S. "An Integrity Verification Scheme for DNS Zone file based on Security Impact Analysis", In Proceedings of the 21st Annual Computer Security Applications Conference, Dec. 2005.

[20] Atkins, D., Austein, R., "Threat Analysis of the Domain Name System (DNS)", RFC 3833, Aug. 2004.