IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Survey of IP Traceback Mechanisms to Overcome DoS Attacks

Sowmya Gibish[1], Uday Babu.P[2]

M. Tech Student, CSE, VAST, Thrissur, Kerala [1]

Assistant Professor, CSE, VAST, Thrissur, Kerala [2]

Abstract: Denial of service attacks are becoming increasingly predominant and serious anonymity that these particular attacks affords the hacker provides no means for a victim to trace the attack. It is essential to protect the resource of the victims and trace the Denial of Service (DoS) attack, but distinguishing of normal traffic and DoS attack traffic is quite challenging because the DoS generally hide their origins. The technique of IP traceback is required to overcome Denial-of-Service attacks. Especially when the attacker's uses incorrect or spoofed source IP address tracing the origin of the Denial of Service is hardest in internet. There are numerous techniques and methodologies are used to trace the DoS attacks. This paper presents several of the mostly used traceback techniques to resolve the problem. The main aim of this paper is to state the various traceback techniques of the DoS attack.

Keywords: IP spoofing, DoS, packet marking, packet logging, IP Traceback methods.

I. INTRODUCTION

Host on the Internet are assigned a unique and an exclusive Internet Protocol (IP) address, which happens to be reported as the original source address in each IP packet header. This header source address is taken as an indication of the originating machine's identity. Attacks against network resources are frequent in the present modern internet dependent world. The most generally known of them are Denial of Service attack [12]. Attacks are launched for several reasons, including monetary gain, maliciousness, fraud, warfare and to acquire a fiscal advantage. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, payments gateways as well as root name servers. Denial of Service attacks and several later forms become one in most of the foremost threatening varieties. It was absolutely reported that DoS traffic within the internet increase number of times in eight years from2002 to 2010. In accordance with Worldwide Infrastructure Security Report 2010 from Arbor Networks, many popular web firms, along with Yahoo, Amazon and CNN were brought down for hours. In Denial of Service attacks, the packets are routed correctly however the destination becomes the prospective of the attackers. DoS attacks are extremely simple to generate and are tough to detect.

In a typical DoS attack the attackers nodes spoofs its IP address and uses multiple intermediate nodes to overwhelm other nodes with traffic. DoS attacks can be classified into flooding attacks and software exploits. Flooding attacks work by flooding a victim with large amounts of packets, while software exploits attack a victim by sending as few as a single packet. A flooding-based DoS attack is a very common way to attack a victim machine by sending a large amount of unwanted traffic. Network level congestion control can throttle peak traffic to protect the network. However, it cannot stop the quality of service (QoS) for legitimate traffic from going down because of attacks. Reflector attacks be owned by the category of the extremely serious DoS attacks. Unlike other DoS attacks, the number of attack packets served by the reflector attacker would be amplified persistently, flooding the victim's network. The attack packets reaching the victim are not direct from the attacker; they will be actually generated by some hosts regarded as reflectors. When such reflectors obtain the envelopes typically reflector attack, they might create persistently more packets with the use of a destination address of the victim IP traceback is the process of identifying the actual source of attack packets. Also, it helps in mitigating DoS attacks either by isolating the identified attack sources or by filtering attack packets far away from the victim.

The rest of this paper is organized as follows are provides. Classifications of traceback methods in Section II. Section III presents different IP traceback methods and conclusion in section IV.

II. CLASSIFICATIONS

IP traceback methods are used to identify the source address of the origin of the packets causing DoS attack and used to restore normal network functionality and preventing reoccurrence. There are many traceback methods in practice to identify the source of the attacker. There are major methods such as reactive or proactive methods.

a. Reactive method is the traceback process in response to an attack. This method is also known as source based mechanism. They must be completed while the attack is active and they become inefficient when attack is inactive. Link testing, ingress filtering/egress filtering and hop count filtering are examples of reactive method. Most of these methods require higher degree of ISP cooperation thus it increases the burden to manage it. Due to these drawback reactive methods suits more for controlled network than internet.

b. Proactive method is referred as destination based mechanism, it record tracing information as packets are routed through the network. The victim can use the resulting traceback data for attack path reconstruction and identifying attacker. Examples of proactive method include logging, ICMP, log based traceback, hash based traceback, distributed link list traceback (DLLT), probabilistic pipelined packet marking (PPPM).

III.DIFFERENT IP TRACEBACK METHODS

1. Link Testing: The link testing method [1] is used to test networks links between routers to determine the origin of the attacker's traffic. This technique usually starts from the router closest to the victim and starts in upstream direction to determine the attack carrying traffic. Link testing is a reactive method and requires the attack to remain active until the trace is completed.

Input debugging: It is one implementation of the link testing approach. This feature lets the administrator determine in coming network links for specific packets. If the router operator knows the attack traffic's specific characteristics (called the attack signature), then it's possible to determine the incoming network link on the router. The ISP must then apply the same process to the upstream router connected to the network link and so on, until the traffic's source is identified.

Controlled flooding: This technique works by generating a burst of network traffic from the victim's network to the upstream network segments and observing how this intentionally generated flood affects the attack traffic's intensity. Using a map of the known Internet topology around the victim, these packet floods are targeted specifically at certain hosts upstream from the victim's network; they iteratively flood each incoming network link on the routers closest to the victim's network.

2. Ingress/Egress filtering: Ingress Filtering is just a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix attached to the ingress router. Egress filtering is definitely an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. An integral requirement for ingress or egress filtering understanding of the expected IP addresses at a specific port. For some networks with complicated topologies, it is challenging to acquire this knowledge. Generally, a router always knows which networks are reachable through any of its interfaces. By looking up source addresses of the incoming traffic, it is possible to test whether the return path to that address would flow out exactly the same interface as the packet arrived upon. Otherwise, they are dropped. It is very difficult to deploy this mechanism in real time.

3. Hop Count Filtering: It is based on packet processing approach for identifying attackers using spoofed source IP address. In this method the packets from the systems at the same hop count passing through the same router are marked with the same identification number which is the combination of 32 bits IP address of the router path and the encrypted value of the hop count. This value is matched with already stored value at receiving router. Thus, attack packets are identified early and spoofing threats are reduced.

4. Network Support for IP Traceback (Packet Marking Approach)

This packet marking approach [3] stores partial path information in the packets, it follows probabilistic packet marking scheme. While each packet represents only a sample of the path it traversed by it. Combining a number of packets together the victim can trace and reconstruct the entire network path .Making algorithm have two steps to follow one is a marking procedure executed by routers in the network and a path reconstruction procedure implemented by the victim. Router will mark the packet by augmenting additional information into the packet that is simply it will append its IP address on the packet and victim uses this augmented information set by the router to reconstruct the path. If the router doesn't mark the packets then obviously it will increase the distance field and cause chaos while reconstructing path by victim.

5. Logging: It is a method of logging the packets at the key routers all throughout the internet and data-mining technique is used to extract information about the attack traffic source. The most predominant drawbacks of this method are amount of processing and storage power and sharing of this information among ISPs poses logistical and legal problems as well as privacy concerns. Packet logs can grow quickly to unmanageable sizes, even over short timeframes in today's high speed network.

6. Hash-based IP Traceback Approach:

To overcome the difficulties of packet marking approach hash based tracing came into effect. This method uses very little space to store the router's address on the packet traversed through it [2]. It uses two methods Source Path Isolation Engine(SPIE) and packet digest technique. SPIE enhanced routers maintain a cache of packet digests for recently forwarded traffic. If a packet is determined to be of intruder by some IDS system, a query is triggered to SPIE which in turn intimate routers for packet digests of the relevant time periods. Packet digest follows an auditing technique, traffic auditing process will compute and store the packet digested value than the packet so it is space efficient. While constructing a packet digest table space-efficient data structure known as Bloom filter is used. This query result is used to initiate an algorithm to construct an attack graph to find source of the packet.

7. FIT: Fast Internet Traceback:

A new packet marking approach i.e., Fast Internet Traceback(FIT)[5],which uses probabilistic packet marking schemes and consists of two major parts: a packet marking scheme to be deployed at routers and path reconstruction algorithms used by victim receiving the packet markings. It improves the traceback methodology by identifying the attack path with high probability, only with two or three packets, it works well and can trace even in the presence of legacy router and it can scale large scattered attacks.FIT scheme uses both upstream router maps and packet markings with the fragment. It employs unique marking and reconstruction algorithms which

generously improve its performance. Firstly it allows the attack victim to generate the upstream router map using packet markings. Second it uses node sampling method greatly reducing the number of false positives and the number of packets required for attack path reconstruction and lastly it uses only 1-bit in the IP id field to mark the distance from the victim at which the packet was marked. While hash based tracing method uses more bits than FIT, which dramatically increases it performance and deploy ability.

8. Advanced and Authenticated Packet Marking (AAPM) scheme:

Advanced and Authenticated Packet Marking (AAPM)[4] is one of the traceback schemes of Denial of Service (DoS) attacks. AAPM uses hash functions to reduce the storage space requirement for augmenting router information in the IP header. A compromised router on the attack path could forge the markings of upstream routers since packets are not authenticated and consequently preventing the victim from detecting and determining the compromised router by analysing the marking distribution. To solve this problem a mechanism to authenticate the packet marking has been introduced. Simplest and straightforward method is to make the router sign digitally the marking of packets. However digital signatures have two major disadvantages, they are very expensive to compute and the space overhead is large. So an efficient technique to authenticate the packet marking is the Authenticated Marking Scheme. This technique only uses one cryptographic MAC (Message Authentication Code) computation per marking thus it is more efficient to compute and can be adapted so it only requires the 16-bit overloaded IP identification field for storage.

9. Novel Hybrid Schemes Employing Packet Marking and Logging (DLLT and PPPM)

There are two techniques namely, Distribute Linked List Traceback (DLLT) and Probabilistic Pipelined Packet Marking (PPPM) used in this approach [9].

Distribute Linked List Traceback (DLLT) is based on the idea of preserving the marking information at intermediate routers and it can be collected using a link list based approach. It combines the features of probabilistic packet marking (PPM) and Hash-based trace back (HBT) schemes i.e., distributed link list trace back (DLLT)=PPM+HBT.DLLT which uses the fixed size packet marking field which is used to store, mark and forward packets. Further marking router will store the content of the marking field in the "marking table" maintained by them or else it forwards those content to the next router. The marking field server has a link to connect the last router did marking to the given packet so a linked list is used; the marking table of that router contain a pointer to the previous marking router and so on. It uses Bloom filter technique as like other tracing approaches and it maintains a Marking Information Table (MIT). MIT contains the IP address of the previous router that marked a given packet which serves as a pointer to that router and the hash function number found from the marked packet i.e. the number used to index the MIT.

Probabilistic pipelined packet marking (PPPM) , based on the pipelined marking concept. The objective of PPPM is, the destination know about all routers that were involved in marking certain packet, using constant space in the IP packet header without requiring long term storage overhead at intermediate routers. The marking information field allocated in each packet consists of two parts: the IP address of the marking router and an ID used to link marking done for a given packet by different routers.

10. A Hybrid Approach for Single-Packet IP Traceback

A practical approach for Single-Packet IP Traceback [10], [11] using packet marking and logging, thus a Hybrid Single-Packet IP Traceback (HIT) Approach has been introduced. This approach in comparison to SPIE has the ability to trace a single IP packet while reducing the storage overhead by half and the access time overhead by the number of neighbouring routers. In this approach the traceback enabled router could do both packet marking and packet logging operations. Router will mark and log each packets forwarded through it depending upon the space availability in packets. In packet logging the router will log current router and every alternate router in its path. The marking field of a packet accommodates the identification information of a single router. While packets are traversing the network, the routers on the path mark each packet but log the packets alternately. In HIT, each traceback enabled router is assigned a 15 bit ID number. The remaining 15 bits are used to store a router ID number. If the logging flag is set to 0, the router chooses to do both logging and marking, if it is set to 1 then the router chooses to do only a marking operation. The traceback process in this approach is managed by traceback servers apparelled with the network topology information. Victim who is attacked by DoS will intimate traceback server with an attack packet and time of attack. From the value of the logging flag bit in the packet, the traceback server can determine whether the last router logged the packet. Further the traceback server will intimate the router which in turn checks all packet digests and also checks according to the time provided by sever. If an entry is found in the packet then that router is considered to be on the attack path, it consist of routing ID which states the upstream routers on the path.

11. ICMP based traceback: ICMP based traceback method [8] will generate iTrace message along with all the packets traversing through router. Since each attacker packet will contribute only partial information about the attacker. An enhanced version of iTrace message is intension driven iTrace messages which is used to separate the iTrace messaging module and decision module. A victim network supplies specific information to the routing table to indicate it requests ICMP traceback message and the decision module would select which kind of packet to use next to generate an iTrace message. The decision module will set a bit in packet-forwarding table which is used to indicate very next packet corresponding to the forwarded packet based on that, iTrace messages are generated. The time taken for reconstructing the attack

path is minimized by using iTrace messages compared to other tracing methods. This method will choose only minimal number of packets to reconstruct the path so its time is reduced. This also reduces other overheads of computation, storage and bandwidth. The iTrace scheme suffers a serious problem on the resource wastage on generating the number of traceback packets which turns out to be neither useful nor informative during traceback but in intentional driven ICMP traceback a bit is set to choose only relevant and informative iTrace packets so it overcomes the drawbacks of other tracing methods.

12. Passive IP traceback:

Passive IP Traceback (PIT) [12], to bypass the difficulties faced by other traceback mechanisms. In some cases router may fail to forward an IP forged packet due to various reasons. In such circumstance, router may generate an ICMP error message named path backscatter and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages eventually disclose the location of the attacker. So these path backscatter messages are used to find the location of spoofer. If the location of the attacker is known the victim can seek help from the corresponding ISP to filter out spoofer from their network or to take any counterattack. PIT also maintains a dataset of already identified spoofer and attack paths, so the victim can find the location of the spoofer directly by analyzing that dataset. PIT uses the ICMP error messages it is widely supported by all ISPs so reducing the deployment difficulties.

IV. CONCLUSION

This paper describes the elaborated survey of different Denial of Service traceback mechanisms. It also describes about the two broad classifications of traceback method and different types of mechanisms under it. Possible DoS attacks in a network and their impacts are identified. There are many traceback methods are available to identify the attacks. The real challenge in security is to pave way to identify the source of unknown attack at the earliest possible which motivate to work on novel traceback mechanism with less computation, storage and costs overhead, with higher scalability and providing best network performance.

REFERENCES

[1] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.

[2] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.

[3] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002,pp. 117–126.

[4] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.

[5] A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005, pp. 1395–1406.

[6] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.

[7] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," in Information and Communications Security. Berlin, Germany: Springer-Verlag, 2003, pp. 124–135.

[8] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, May 2006.

[9] M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid IP traceback scheme," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.

[10] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.

[11] Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE

[12] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.

BIOGRAPHIES

Sowmya Gibish is a postgraduate student at Vidya Academy of Science and Technology, Thrissur, India, affliated to Calicut University. Her area of interest is network security. She received her B.E Degree in Computer Science and Engineering from Anna University, Tamil Nadu, India, in 2012.

Uday Babu P is an Assistant Professor at Vidya Academy of Science and Technology, Thrissur, India, affiliated to Calicut University. His area of interest is security. He received his M. Tech Degree and B. Tech Degree in Computer Science and Engineering from M.G. University, Kerala.

DOI 10.17148/IJARCCE.2015.41299