A Novel Scheme for Detecting IP Spoofers Using Passive IP Traceback

ANIL KULKARNI
AP in Dept. of CSE
GNDEC
Bidar, Karnataka

SWAROOPA
M.Tech Student
Research Scholar in Dept. of CSE
GNDEC, Bidar, Karnataka

Abstract- **IP spoofing is a attack in which attacker launch the attack by using forged source IP address. It is long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP traceback mechanisms have been proposed. However, due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissipated till now. Here it proposes passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (e.g., topology). In this way, PIT can find the spoofers without any deployment requirement. Here it illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood.**

Keywords: **Computer Network Security; Denial of Service (Dos); IP Traceback;**

I. INTRODUCTION

IP Spoofing, which means attackers launching attacks with forged source IP addresses, has been recognized as a serious security problem on the Internet for long [1]. By using addresses that are assigned to others or not assigned at all, attackers can avoid exposing their real locations, or enhance the effect of attacking, or launch reflection based attacks. A number of notorious attacks rely on IP spoofing, including SYN flooding, SMURF, DNS amplification etc. A DNS amplification attack which severely degrads the service of a Top Level Domain (TLD) name server is reported in [2]. Though there has been a popular conventional wisdom that DoS attacks are launched from botnets and spoofing is no longer critical, the report of ARBOR on NANOG 50th meeting shows spoofing is still significant in observed DoS attacks [3]. Indeed, based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed [4].

To capture the origins of IP spoofing traffic is of great importance. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks[5]. Even just approaching the spoofers, for example, determining the ASes or networks they reside in, attackers can be located in a smaller area, and filters can be placed closer to the attacker before attacking traffic get aggregated. The last but not the least, identifying the origins of spoofing traffic can help build a reputation system for ASes, which would be helpful to push the corresponding ISPs to verify IP source address.

Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding[6]. In such cases, the routers 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 may potentially disclose the locations of the spoofers. PIT exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic. Not all the packets reach their destinations[7]. A network device may fail to forward a packet due to various reasons. Under certain conditions, it may generate an ICMP error message, i.e., path backscatter messages. The path backscatter messages will be sent to the source IP address indicated in the original packet. If the source address is forged, the messages will be sent to the node who actually owns the address. This means the victims of reflection based attacks, and the hosts whose addresses are used by spoofers, are possibly to collect such messages.

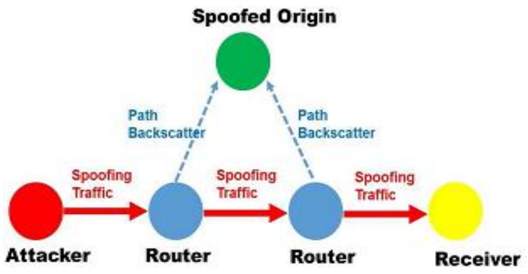

Fig1. Architecture of PIT (Passive IP Traceback)

The above diagram shows the way application works, here first attacker will uses the source IP address of IP packet during this period of time path back scatter messeges are sent to the victim node initially . after some transmission between victim and destination,IP spoofers are detected with the help of passive IP traceback.

II. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before improving the tools it is compulsory to decide the economy strength, time factor. Once the programmer‘s create the structure tools as programmer require a lot of external support, this type of support can be done by senior programmers, from websites or from books.

A. Security problems in the TCP/IP protocol suite (Author: S. M. Bellovin)

S. M. Bellovin has explained The TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. Here the author describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks and also present defenses against these attacks[9].

B. Distributed denial of service (DDOS) attacks (author: Felix Lau Simon)

Felix Lau Simon has discussed about distributed denial of service attacks in the Internet. The has decribed attacks on Yahoo!, Amazon.com, CNN.com, and other major Web sites. A denial of service is characterized by an explicit attempt by an attacker to prevent legitimate users from using resources. An attacker may attempt to: “flood” a network and thus reduce a legitimate user’s bandwidth, prevent access to a service, or disrupt service to a specific system or a user. Some methods and techniques used in denial of service attacks, and provides the list of possible defenses. The study of distributed denial of service attack can be done by using ns-2 network simulator.The algorithms are implemented in a network router to perform during an attack, and whether legitimate users can obtain desired bandwidth[8].

C. Practical network support for IP traceback (Authors: S. Savage, D. Wetherall, A. Karlin and T. Anderson)

S. Savage described a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or “spoofed”, source addresses [10]. Here author describe a general purpose traceback mechanism based on probabilistic packet marking in the network. The approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this traceback can be performed “post-mortem” – after an attack has completed.The implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology [21].

III. METHODOLOGY

A. Mathematical Model

Basic Tracking Mechanism Whenever a path backscatter message whose source is router r (named reflector) and the original destination is od is captured, the most direct inference is that the packet from attacker to od should bypass r.Use a very simple mechanism in spoofing origin tracking. The network is abstracted as a graph G(V, E), where V is the set of all the network nodes and E is the set of all the links. A network node can be a router or an AS, depending on the tracking scenario. From each path backscatter message, the node r,r ∈ V which generates the packet and the original destination od, od ∈ V of the spoofing packet can be got. Denote the location of the spoofer, i.e., the nearest router or the origin AS, by a, a ∈ V[14]. We make use of path information to help track the location of the spoofer [11]. Use path (v, u) to denote the sequence of nodes on one of the path from v to u, and use PAT H(v, u) to denote the set of all the paths from v to u. Use ϕ(r, od) to denote the set of nodes from each of which a packet to od can bypass r, i.e $\emptyset(\mathrm{r}, \mathrm{od}) = \{\mathrm{v} | \mathrm{r} \ \in \mathrm{path}(\mathrm{v}, \mathrm{od}), \mathrm{path}(\mathrm{v}, \mathrm{od}) \in$ PATH(v,od) ϕ(r, od) actually determines the minimal set which must contain the spoofer. We name the result set of ϕ(r, od) by suspect set.If the topology and routes of the network are known, this mechanism can be used to effectively determine the suspect set. For example, an ISP can make this model to locate spoofers in its managed network [12]. However, for most cases, the one who performs tracing does not know the routing choices of the other networks, which are non-public information. Moreover, the topologies of most of the ASes are unknown to the public [13].

Another way to explaine about this project can be done with the help of UML (Unified Modified

Languege) diagram. Figure 2(Fig1) shows UML diagram, provides the graphical representation of functionality which are perfoming in this project.

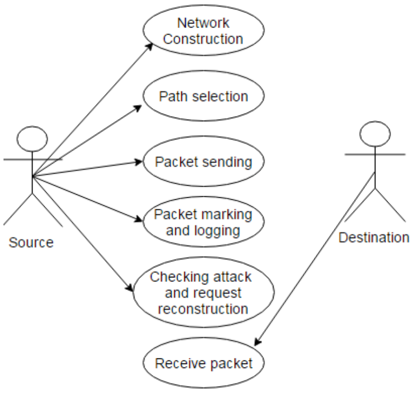

Fig2.UML diagram of PIT

B. Enhancement Model

In order to further enhance the security against the spoofing attacks here accusation method is introduced.

In that, if new node approaches the CA to join, the node should provide the revoked key to the new CA. The new CA would compare the key with previous cluster head. The new CA accepts the new node if only the key is verified. It further prevents the malicious node to join with the new cluster, even after the node detected as malicious.

Since the network has mobility, sensor nodes can move from one cluster to another. The key of the sensor must be updated at each cluster. The old key provided by the previous CA must be revoked and new key should be generated by the current CA [15].

Suppose if a node is found as malicious, then the key should be revoked. The malicious node can move into new cluster to get new keys. The CA had no chance to know that the coming node is malicious. If the new CA provides the key to the malicious node, then it can participate to the communication. There is no method to know the status of the new node [25].

IV. RESULTS AND DISCUSSION

Detecting IP spoofers by using PIT (passive IP Traceback) can be evalueated through graph.

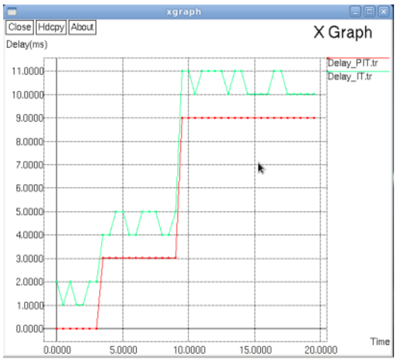

Fig3. End -To –End Delay

Red line show proposed system and green line is for existing system.

Figure 3 shows the end to end delay for both existing and proposed system. Delay after applying PIT is less in proposed system as compard to existing system.

Figure 4. Shows overall performance of the proposed system.

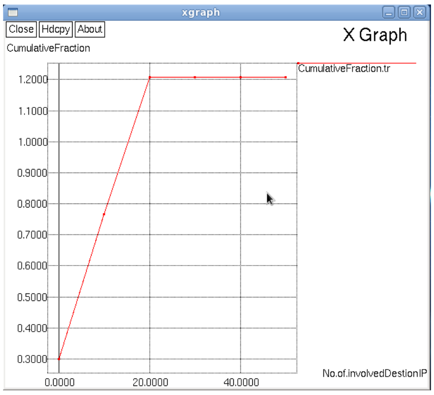

Fig4. CumulativeFraction

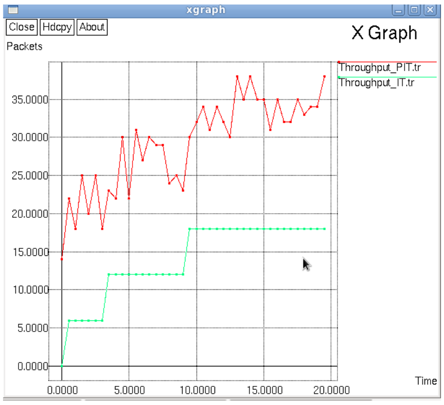

Fig5.Throughput

Figure 5. Shows throughput for existing and proposed system. Throughput is more in proposed system than in existing system.

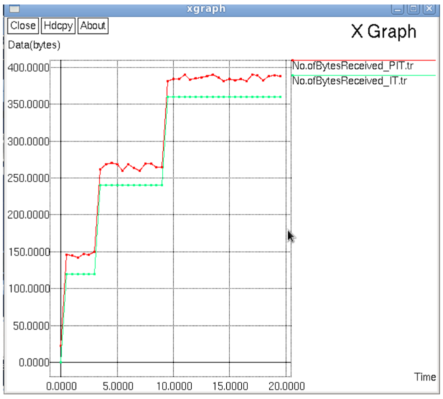

Fig 6. Number Of Bytes Recieved

Figure 6 shows number of bytes recieved in proposed system is more than the existing system. In above graph the No.of bytes recieved is more in proposed system this is achieved by PIT (Passsive

IP Traceback) .

V. CONCLUSION AND FUTURE SCOPE

Here the attempt is try to find the locations of spoofers based on investigating the path backscatter messages. In this article, the Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information.The illustration will provide causes, collection, and statistical results on path backscatter. Here the method is present that how to apply PIT when the topology and routing are either known, or the routing is unknown, or neither of them are known.

In future work we can extend this to include more power full cryptographic technique.

VI. ACKNOWLEDGMENTS

We indebted to management of GNDEC, Bidar for excellent support in completing this work at right time.A special thanks to the authors mentioned in the references.

VII. REFEENCES

[1]. 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.

[2]. ICANN Security and Stability Advisory Committee, “Distributed denial of service (DDOS) attacks,” SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[3]. C. Labovitz, “Bots, DDoS and ground truth,” presented at the 50th NANOG, Oct. 2010.

[4]. 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.

[5]. S. Bellovin. ICMP Traceback Messages. [Online]. Available:

http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

[6]. A. C. Snoeren et al., “Hash-based IP traceback,” SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001. D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage,“Inferring internet denial-of-service activity,” ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027] M. T. Goodrich, “Efficient packet marking for large-scale IP traceback,” in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.

[7]. 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.

[8]. K. Park and H. Lee, “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack,” in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.

[9]. M. Adler, “Trade-offs in probabilistic packet marking for IP traceback,” J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.

[10]. A. Belenky and N. Ansari, “IP traceback with deterministic packet marking,” IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[11]. 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.

[12]. R. P. Laufer et al., “Towards stateless single-packet IP traceback,” in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/LCN.2007.160

[13]. M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, “A stateless traceback technique for identifying the origin of attacks from a single packet,” in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–6.

[14]. A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, “On design and evaluation of ‘intention-driven’ ICMP traceback,” in Proc. 10th Int. Conf. Comput. Commun. Netw., Oct. 2001, pp. 159–165.

[15]. 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.

[16]. H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” in Proc. LISA, 2000, pp. 319–327.

[17]. R. Stone, “CenterTrack: An IP overlay network for tracking DoS floods,” in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.

[18]. A. Castelucio, A. Ziviani, and R. M. Salles, “An AS-level overlay network for IP traceback,” IEEE Netw., vol. 23, no. 1, pp.

36–41, Jan. 2009. [Online]. Available: http://dx.doi.org/10.1109/MNET.2009.4804322

[19]. Castelucio, A. T. A. Gomes, A. Ziviani, and R. M. Salles, “Intradomain IP traceback using OSPF,” Comput. Commun., vol. 35, no. 5, pp. 554–564, 2012. [Online].

[20]. 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.

[21]. 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.

[22]. 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.

[23]. R. Beverly, A. Berger, Y. Hyun, and K. Claffy, “Understanding the efficacy of deployed internet source address validation filtering,” in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), 2009, pp. 356–369.

[24]. G. Yao, J. Bi, and Z. Zhou, “Passive IP traceback: Capturing the origin of anonymous traffic through network telescopes,” in Proc. ACM SIGCOMM Conf. (SIGCOMM), 2010, pp. 413–414. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851237

[25]. J. Postel. Internet Control Message Protocol, RFC792. [Online]. Available:

https://tools.ietf.org/html/rfc792, accessed Sep. 1981.