B. Sai Priyanka *et al*, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 3, September- 2013, pg. 40-44 **ISSN: 2321-8363**

IP Traceback Techniques – A Selective Survey

B. Sai Priyanka [1], N. Srihari Rao[2]
[1]M.Tech Student, CSE Dept, CMR Institute of Technology, Hyderabad, A.P
Email-id: saipriyanka04@gmail.com
[2]Associate Prof., CSE Dept., CMR Institute of Technology, Hyderabad, A.P., MIAENG, MCSI
Email-id: raon2006@gmail.com

Abstract

Since many years Internet has been used broadly in several fields, network security problems are the major concern. A literature survey is carried out in this context to explore different IP Traceback techniques. This paper presents several techniques to perform IP Traceback. The pros and cons of each technique are explained briefly in this paper.

Keywords: IP Traceback; Denial-of-service (DoS) attacks; Packet marking; Packet logging

I. Introduction

Internet is widely used now-a-days to complete almost every task. As Internet is used for many tasks, attackers find a way to disturb the services provided by it. Hence, today network security is often a compulsory requirement for Internet. Even though many security measures are adapted by the security people to ensure security for the customers, still Internet is open for many attacks. The attacks have become so prevalent that no security measure can prevent all of them.

In order to strengthen the business of companies, they need methods such as IP Traceback techniques which will ultimately reduce the chances of losses. IP Traceback is an attempt to trace the true origin of a packet or a stream of packets. Because of IP Spoofing, merely assuming that the packet was sent by the node specified as the source address in its IP header is not always effective, so other methods of tracing packets to their origin are required. Hence effective IP Traceback techniques have to be used to find out the true source of attacks, in order to take any preventive or legal actions against the attackers.

Denial-of-Service (DoS) attacks are examples for attacks deployed against the Internet to disrupt the services provided by them. It is not so easy to prevent these kinds of attacks because well-crafted DoS attacks do not violate most of the security rules but they definitely cause damage to service provisioning. In order to prevent Internet against these kinds of attacks we have to implement defense techniques at necessary locations of the Internet.

We can classify the attack defense methods into two categories: Proactive attack defense method and reactive attack defense method. Proactive attack defense methods take the precautionary steps in preventing the attacks. Reactive attack defense methods either try to respond to the attack after detection of attack situation or aim to identify the source of attacks which means they employ some traceback techniques. Existing technologies for preventing network attacks focus on access control and attack detection. Firewalls use access control based on source IP address, destination IP address, protocol type, source port number, and destination port number. Intrusion Detection System based on attack signatures, anomaly-based attack detection, or a combination of these two (hybrid detection) can be used. Our consideration in this paper is on IP Traceback a technique which comes under reactive attack defense method. Currently possible solutions for IP Traceback

problem include Packet Marking, Packet Logging, and Hybrid Traceback approach. These solutions are explained below.

Packet Marking Technique: This solution relies on the routers in the network to send their identities to the destinations either by encoding this information directly in rarely used bits of the IP Header, or by generating new packet to the same destination. They have the drawback in that they require large number of attack packets to be collected by the victim to infer the attack paths.

Packet Logging technique: This solution involves storing packet digests or signatures at intermediate routers. The drawbacks of this technique include significant amount of resources have to be reserved at intermediate routers and hence large overhead on the network, complexity, centralized management.

Hybrid Traceback technique: This solution achieves the best of both the worlds: small number of attack packets to conduct the traceback process and small number of resources to be allocated at intermediate routers for packet logging purposes.

The remainder of the paper is organized as follows. In Section II, literature survey is explained. Section II concludes the paper. Section III presents the future work.

II. Literature Survey

Abraham Yaar et al. [1] proposed a new packet marking approach i.e., Fast Internet Traceback (FIT),is one among the PPM (Probabilistic Packet Marking) traceback schemes and consists of two major parts: a packet marking scheme to be deployed at routers, and map and path reconstruction algorithms used by end hosts receiving the packet markings. Hence this scheme improves IP traceback in several ways:

1. Victims can identify attack paths with high probability after receiving only tens of packets, a reduction of 1–3 orders of scale.
2. FIT performs well even in the presence of legacy routers, allowing every FIT-enabled router in path to be recognized.
3. FIT scales to large scattered attacks with thousands of attackers.

FIT scheme uses both upstream router maps and packet markings with the fragment/number/distance format. It employs unique marking and reconstruction algorithms which dramatically improve its performance. Steps to be followed in FIT firstly, FIT allows the attack victim to generate the upstream router map using packet markings. Second FIT uses node sampling instead of the commonly used edge sampling, greatly reducing the number of false positives and the number of packets required for attack path reconstruction and lastly FIT uses only 1-bit in the IP ID field to mark the distance from the victim at which the packet was marked. This allows 4 extra bits to be used for hash fragment marks, which both greatly reduces false positives and increases the effective marking probability. And the main significance of this method is it represents a step forward in performance and deployability.

K. H. Choi et al. [2] discussed a new marking scheme with marking and traceback algorithms in which a router marks a packet with a link that the packet came through. And the Links of a router are represented by Huffman codes according to the traffic distribution among the links.
A marking scheme needs to have a:
(i)When a router marks a packet with address information, the information is not of the router that is marking but of a router that sent the packet to the current router.
(ii)It uses a special table called link table, which shows all the links between the router and its adjacent routers. The router appends to the marking field a Huffman codeword representing the link number of the link (router) through which the packet arrived. When the marking field of a packet converts short of space left to join the corresponding Huffman codeword for the link number, the router stores the content of the marking field with a message digest of the packet into the router's local memory, and then clears the field and appends the

codeword. The stored link sequence can be retrieved via the message digest of the packet from the intermediate router. And also it requires far less amount of memory compared to logging methods and is robust in case of Distributed Denial of Service (DDoS). But the current IP header is not appropriate for marking, using either the Identification field or the Option field of IP header has its own limitation.

Chao Gong et.al [3] proposed a novel scheme to improve the practicality of log-based IP traceback by reducing its overhead on routers and makes an intelligent use of packet marking to help improve the scalability of log-based IP traceback.

This method depends on the availability of free space in the marking field of the forwarded packets, routers decide where to record network path information. If there is free space available in the marking field, routers write their identification information into the packets; otherwise, routers compute and record the packet digests, and then clear the marking field. Some of the expansions of our approach to the state-of-the-art log-based approach called Source Path Isolation Engine (SPIE). It reduces the storage overhead of packet digests to one half and secondly reduces the access time requirement by a factor of the number of neighboring routers.

Here the storage overhead and access time requirement for recording packet digests are fairly high at high-speed routers.

*Linfeng Zhang et al.[4]*outlined a technique called Bloom filter-based topology-aware single packet IP traceback system, namely TOPO, which utilizes router's local topology information, i.e., its immediate predecessor information, to traceback. It can significantly reduce the number and scope of unnecessary queries and thus, significantly decrease the false attributions to innocent nodes.

Partial deployment is a significant and desired property when designing and implementing IP traceback systems. When Bloom filters are applied in IP traceback systems, it is difficult to decide their optimal control parameters a priori and thus achieve the lowest false positive rate. Here we design a k-adaptive mechanism to dynamically adjust parameters of Bloom filters such that our IP traceback system can achieve the best performance in terms of false attribution rates, storage space requirement and also reduces the number of unnecessary queries.

S. Malliga et al.[5] discussed a packet marking algorithm, which follows hybrid marking scheme to solve IP traceback problem where the packets travel through the network, and they are marked with router information using modulo technique. Upon traceback request, to reconstruct the path traversed by the packets we use reverse modulo. In particular, this method reconstructs the attack path with one packet and acquires very less overhead on the network and router. It requires logging at routers, so the storage overhead on the routers is also significantly reduced. And stores the entire path traversed in a single packet and thus leads to less convergence time to find the attack path at the victim.

Alex C. Snoeren et al. [6] developed a hash-based technique for IP traceback that generates audit trails for traffic within the network. Source Path Isolation Engine (SPIE) is used to enable IP traceback, the ability to identify the single IP packet to be traced, its destination, and an approximate time of receipt.

Tracing individual packets has required prohibitive amounts of memory. One of SPIE's key innovations is to reduce the memory requirement through the use of Bloom filters. By storing only packet digests, and not the packets themselves, SPIE also does not increase a network's susceptibility to eavesdropping. Therefore it allows routers to efficiently determine if they forwarded a particular packet within a specified time interval while maintaining the privacy of unrelated traffic. In this method it will support traceback of large packet flows for longer periods of time in a fashion similar to probabilistic marking schemes rather than discard packet digests as they expire.

Stefan Savage et al. [7] discuss a novel strategy for which tracing anonymous packet flooding attacks in Internet back towards their source. It is motivated by the increased frequency and sophistication of denial-of-service (DoS) attacks and by the difficulty in tracing packet(s) with incorrect, or "spoofed", source addresses. Here a general purpose traceback mechanism based on probabilistic packet marking in the network is used and performs a "post-mortem" – after an attack has completed. We trace attacks back towards their origin and ideally stopping an attacker at the source. Determining the source generating attack traffic is surprisingly difficult due to the stateless nature of Internet routing. As these packets traverse the Internet their true origin is lost and a victim is left and it does not require interactive cooperation with ISPs and therefore avoids the high management overhead of input debugging. As we reuse of the IP identification field, we must address issues of backwards-compatibility for IP fragment traffic.

Chao Gong et al. [8] proposed a new Probabilistic packet marking (PPM) approach that improves the current state of the art in two practical directions: (1) It improves the efficiency and accuracy of IP traceback (2) It provides incentives for ISPs to deploy IP traceback in their networks.

PPM approach employs a new IP header encoding scheme to store the whole identification information of a router into a single packet. This eliminates the computation overhead and false positives due to router identification fragmentation. There is a problem hindering the deployment of PPM approaches in the Internet. This approach has limited efficiency and accuracy in tracing large-scale distributed DoS (DDoS) attacks, in order to avoid this problem a new approach an accurate and secure PPM (ASPPM) has been used which addresses the above-mentioned problem. The process of ASPPM identifies routers with assigned ID numbers instead of IP addresses. ASPPM also employs a new IP header encoding scheme to store the complete router identification information into a single packet. In ASPPM, if a marked packet is to be forwarded to a customer not purchasing IP traceback service, the marking information in the packet will be removed. Hence, it is suitable to be deployed by ISPs as a value- added service. The Significance of this method, it stores the entire identification information of a router in a single packet and therefore, the router does not need to split its identification information into multiple fragments.

III. Conclusion

A literature survey is carried out on different IP traceback techniques. In this paper, we discussed the pros and cons of more important traceback techniques to highlight the deployment of a particular technique that suits to a particular context.

IV. Future Work

As the internet has been used widely throughout the world, security plays crucial role for data communications. However, hackers often hide themselves by spoofing their own IP addresses and then blastoff attacks. For this paper, we gathered and studied different existing research methods and technologies and performed a survey. To overcome drawbacks of the existing IP traceback methods we are trying to propose a novel IP traceback scheme which we would be doing in future course of our dissertation work.

References

1. A. Yaar, A. Perrig, and D. Song, “FIT: Fast internet traceback,” in Proc. IEEE INFOCOM2005, Miami, FL, Mar. 2005, pp. 1395–1406.

2. K. H. Choi and H. K. Dai, “A marking scheme using Huffman codes for IP traceback,” in Proc. 7th Int. Symp. Parallel Architectures, Algorithms Networks (SPAN’04), Hong Kong, China, May 2004, pp. 421–428.

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

4. S. Malliga and A. Tamilarasi, “A proposal for new marking scheme with its performance evaluation for IP traceback,”WSEAS Trans. ComputerRes., vol. 3, no. 4, pp. 259–272, Apr. 2008.

5. L. Zhang and Y. Guan, “TOPO: A topology-aware single packet attack traceback scheme,” in Proc. IEEE In. Conf. Security Privacy Communication Networks (SecureComm 2006), Baltimore, MD, Aug. 2006, pp. 1–10.

6. S.Savage, D.Wetherall, A.Karlin, and T.Anderson, “Practical network support for IP traceback,” in Proc. ACM SIGCOMM2000, Stockholm, Sweden, Aug. 2000, pp. 295–306.

7. A.C.Snoeren, C.Partridge, L.A.Sanchez, C.E.Jones, F.Tchakountio, B.Schwartz, S.T.Kent, and W.T.Strayer, “Single-packet IP traceback,” IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.

8. C.Gong and K.Sarac, "Toward a practical packet marking approach for IP traceback," Int. J. Network Security, vol. 8, no. 3, pp. 271–281, Mar. 2009.

9. http://en.wikipedia.org/wiki/IP_traceback

10. http://dslab.csie.ncu.edu.tw/93html/paper/pdf/IP%20Traceback:A%20New%20Denial-of Service%20Deterrent.pdf

11. http://cseweb.ucsd.edu/~savage/papersTon01.pdf

12. http://www.cs.plu.edu/courses/netsec/arts/w2020.pdf

13. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.4574&rep=rep1&type=pdf

Authors' Biography

B. Sai Priyanka had B.Tech from SR engineering college, Warangal. She is an M.Tech Student in CSE Department of CMR Institute of Technology, Hyderabad. She is currently working for her M.Tech. Research project work under the guidance of Mr.N.Srihari Rao. Her areas of interest include Network Security, Computer Networks, and Programming Languages.

N.Srihari Rao had his B.E. from C.B.I.T., Hyderabad, and he had M.E. from Karunya Deemed University, Coimbatore. He is currently working as Associate Professor in CSE Department of CMR Institute of Technology, Hyderabad. He is working for Ph.D. in CSE Discipline at JNTUA University, Anantapur. His areas of interest are Network Security, Data Mining, Image Processing, and ICT for various fields.

