Disclosing The Locations Of IP Spoofers From Pathway Backscatter In Passive IP Traceback

T. RAMA
PG Scholar, Department of CSE
G.K.C.E, Sullurpet, Andhrapradesh, INDIA.

K. SUDHA
Assistant Professor, Department of CSE
G.K.C.E, Sullurpet, Andhrapradesh, INDIA.

Abstract: **It is very long known attackers may use forged source IP address to obscure 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. This paper 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. This paper 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. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level traceback system has been deployed in real.**

Key Words: **Computer Network Management; Computer Network Security; Denial Of Service (Dos); IP Trace Back**

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. 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 degraded the service of a Top Level Domain (TLD) name server is reported in this system. 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. Indeed, based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed.

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. 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.

However, to capture the origins of IP spoofing traffic on the Internet is thorny. The research of identifying the origin of spoofing traffic is categorized in IP traceback. To build an IP traceback system on the Internet faces at least two critical challenges. The first one is the cost to adopt a traceback mechanism in the routing system. Existing traceback mechanisms are either not widely supported by current commodity routers (packet marking), or will introduce considerable overhead to the routers (Internet Control Message Protocol (ICMP) generation, packet logging), especially in high-performance networks. The second one is the difficulty to make Internet service providers (ISPs) collaborate. Since the spoofers could spread over every corner of the world, a single ISP to deploy its own traceback system is almost meaningless. However, ISPs, which are commercial entities with competitive relationships, are generally lack of explicit economic incentive to help clients of the others to trace attacker in their managed ASes.

Since the deployment of traceback mechanisms is not of clear gains but apparently high overhead, to the best knowledge of authors, there has been no deployed Internet-scale IP traceback system till now. As a result, despite that there are a lot of IP traceback mechanisms proposed and a large number of spoofing activities observed, the real locations of spoofers still remain a mystery.

II. LITREACHER SURVEY

1) Efficient Packet Marking for Large-Scale IP Traceback

It present a new approach to IP traceback based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to “link” message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori.

2) Practical Network Support for IP Traceback

It describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work 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. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs).

3) FIT: Fast Internet Traceback

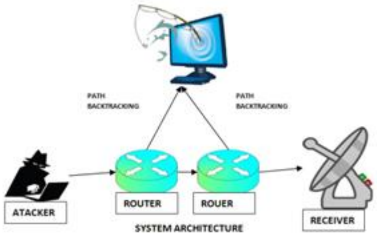
The costs of the damages are often on the order of several billion of dollars. Traceback mechanisms are a critical part of the defense against IP spoofing and DoS attacks. Current traceback mechanisms are inadequate to address the traceback problem Problems with the current traceback mechanisms

III. RELATED PROBLEM

Though PIT is used to perform ip TRACEBACK, it is very different from existing ip TRACEBACK mechanisms. PIT is inspired by a number of ip spoofing observation activities. Thus, the related work is composed by two parts. The first briefly introduces existing ip TRACEBACK mechanisms, and the second introduces the ip spoofing observation activites.

3.1. IP Traceback

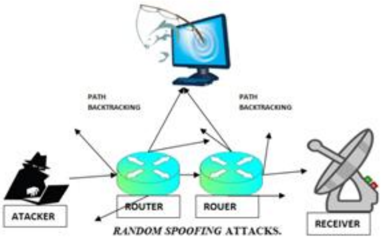
Information processing TRACEBACK IP TRACEBACK techniques square measure designed to disclose the important origin of information processing traffic or track the trail. Existing information processing TRACEBACK approaches are usually classified into 5 main categories: packet marking, ICMP TRACEBACK, logging on the router, link testing, overlay, and hybrid tracing. Packet marking strategies need routers modify the Header of the packet to contain the info of the router and forwarding call. So the receiver of the packet can then reconstruct the trail of a packet from the received packets. There are two Classes of packet marking schemes: probabilistic packet marking and settled packet marking. Packet marking methods are generally considered to be lightweight because they do not price storage resource on routers and the link bandwidth resource. However, packet marking is not a wide supported operate on routers; so, it's tough to switch packet marking TRACEBACK at intervals the network.



SYSTEM ARCHITECTURE

3.2. IP Spoofing Observation

Network telescope may be a basic technique for Passive observation of spoofing activities on the internet. Network telescope captures non-solicited messages, which area unit in the main generated by victim attacked by traffic with source prefix set in the scope closely-held by the telescope. Then, it can be Determined a part of nodes which area unit attacked by spoofing traffic. Currently, the largest scale telescope is the CAIDA UCSD telescope, which owns 1/256 of all the ip addresses and is in the main used to observe DDoS activities and worms. More el at. Conferred a method namely “back-scatter analysis” that uses the feature of DoS attacks based mostly on traces collected by the network telescope. Though ICMP error message provides publicly accessible information. A recent report from Arbor network based mostly on additional than 5000 attacks shows an intriguing result unreasonable per IP traffic of 4Gbps is determined in 100% attacks, and significant rate of TCP connections area unit launched from just a few validated hosts. Though this is not direct evidence of spoofing, it suggests spoofing could be used in such attacks



RANDOM SPOOFING ATTACKS.

IV. PROBLEM ANALYSIS

a novel solution, named Passive IP Traceback (PIT), to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding. 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.

This is the first article known which deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. Though Moore has exploited backscatter messages, which are generated by the targets of spoofing messages, to study Denial of Services (DoS), path backscatter messages, which are sent by intermediate devices rather than the targets, have not been used in traceback.

Practical and effective IP traceback solution based on path backscatter messages, i.e., PIT, is proposed. PIT bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force. Though given the limitation that path backscatter messages are not generated with stable possibility, PIT cannot work in all the attacks, but it does work in a number of spoofing activities. At least it may be the most useful traceback mechanism before an AS-level traceback system has been deployed in real.

Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. Though this is not a complete list, it is the first known list disclosing the locations of spoofers.

V. IMPLEMENTATION

Service provider:

The service provider will browse the data file, initialize the router nodes, for security purpose service provider encrypts the data file and then sends to the particular receivers (A, B, C, D…). Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

Router

The Router manages a multiple nodes to provide data storage service. In router n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and routing path details. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then flow will be send to IDS manager and router will connect to another node and send to particular receiver.

IDS Manager

The IDS Manager detects introducer and stores the introducer details. In a router any type of attacker (All Spoofers like source, destination, DOS Attacker) is found then details will send to IDS manager. And IDS Manager will detect the attacker type (Active attacker or passive attacker), and response will send to the router. And also inside the IDS Manager we can view the attacker details with their tags such as attacker type, attacked node name, time and date.

Receiver (End User)

The receiver can receive the data file from the router. Service provider will send data file to router and router will accept the data and send to particular receiver (A, B, C, D, E and F). The receivers receive the file in decrypted format by without changing the File Contents. Users may receive particular data files within the network only.

Attacker

there are a two types of attacker is present one is who is spoofing the Ip address. Active attacker is one who is injecting malicious data to the corresponding node and also passive attacker will change the destination IP of the particular node. After attacking a node we can view attacked nodes inside router.

VI. CONCLUSION

It try to dissipate the mist on the locations of spoofers based on investigating the path backscatter messages. In this article, we proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. We specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness. We demonstrated the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset. These results can help further reveal IP spoofing, which has been studied for long but never well understood.

VII. REFERENCES

[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]. CANN 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]. The UCSD Network Telescope. [Online]. Available:http://www.caida.org/projects/network_telescope/

[5]. 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.

[6]. S. Bellovin. ICMP Traceback Messages. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

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

[8]. 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

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

[10]. 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.

[11]. 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.

[12]. J. Liu, Z.-J. Lee, and Y.-C. Chung, “Dynamic probabilistic packet marking for efficient IP traceback,” Comput. Netw., vol. 51, no. 3, pp. 866–882, 2007.

[13]. 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.

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

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

AUTHOR’s PROFILE

T. Rama has received her B.Tech degree in Computer science Engineering from JNTU Anantapur in 2014 & She is now Pursuing the M.Tech degree at Gokula Krishna College of Engineering (GKCE) at sullurpet, Nellore (D.T), Andhra Pradesh, INDIA. Her areas of research include

K.Sudha has received her B.Tech degree in Information Technology from SASTRA UNIVERSITY Thanjavur in 2007 & M.Tech degree in Computer Science Engineering from PRIST UNIVERSITY Thanjavur in 2010.She is a life member of ISSE, she is dedicate to teaching field from the last six years, her last research areas included Mobile computing and Wireless Sensor Network. At present she is working as assistant professor in Gokula Krishna College of Engineering (GKCE) at sullurpet, Nellore (D.T), Andhra Pradesh, INDIA.