SPECKLING PASSIVE IP INREVEALING LOCALITY FROM REARWARD PATH

Kanda Sridhar[1], Atchyut Kumar Reddy. A[2]
[1]Student of M. Tech (CSE), [2]Assistant Professor
Department of Computer Science and Engineering at Chirala Engineering College, Chirala.

ABSTRACT: IP traceback can be used to find the origin of anonymous traffic; however, Internet-scale IP traceback systems have not been deployed due to a need for cooperation between Internet Service Providers (ISPs). It is long known attackers may utilize fashioned source IP location to cover their real areas. To capture the spoofers, various IP traceback mechanisms have been proposed. However, due to the challenges regarding deployment services, there has been not any widely adopted IP traceback solution, at least at the Internet level. This article presents an Internet-scale Passive IP Trackback (PIT) mechanism that does not require ISP deployment. PIT analyzes the ICMP messages that may scattered to a network telescope as spoofed packets travel from attacker to victim. An Internet route model is then used to help re-construct the attack path. Applying this mechanism to data collected by Cooperative Association for Internet Data Analysis (CAIDA), we found PIT can construct a trace tree from at least one intermediate router in 55.4% the fiercest packet spoofing attacks, and can construct a tree from at least 10 routers in 23.4% of attacks. This initial result shows PIT is a promising mechanism.

Keywords: Denial-of-service, traceback, packet marking.

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 finding their original locations, or enhance the effect of attacking, or launch reflection based attacks. A verity of well known 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. Though there has been a popular prediction 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. To capture the origins of IP spoofing traffic is more important. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks. [1][3] Even just approaching the spoofers, for example, determining the ASes or networks they reside in, attackers can be situated 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 prestige system for ASes, which would be helpful to push the corresponding ISPs to verify IP source address [3] 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. 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 [1], [3].

II. RELATED WORK

Efficient Packet Marking for Large-Scale IP Traceback Author proposed a new approach to IP traceback based on the probabilistic packet marking paradigm [7]. 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. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually. B. Practical Network Support for IP Traceback This paper [8] 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]. Moreover, this traceback can be performed ”post-mortem” after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

III. CONTRIBUTION

Profoundly explores way backscatter messages. These messages are profitable to help comprehend with spoofinging exercises. In spite of the fact that Moore has abused backscatter messages, which are created by the objectives of caricaturing messages, to study Denial of Services (DoS), way backscatter messages, which are sent by moderate gadgets as opposed to the objectives, have not been utilized as a part of traceback. B. A practical and powerful IP traceback arrangement taking into account way backscatter messages, i.e., PIT, is proposed. PIT sidesteps the arrangement troubles of existing IP traceback systems and really is as of now in power. Despite the fact that given the impediment that way backscatter messages are not produced with stable probability, PIT can't work in every one of the assaults, however it work in various satirizing exercises. At any rate it might be the most valuable traceback component before an AS-level traceback framework has been sent in genuine. C. 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.

LITREACHER SURVEY 1) Efficient Packet Marking for Large-Scale IP Traceback (2002) Author: Michael T. Goodrich Abstract:-We 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. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

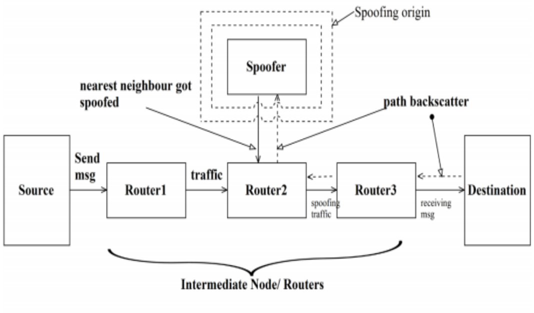

Fig. Architecture Of Proposed Work

IV. CONCLUSION

In this paper a new technique, “backscatter analysis,” for estimating denial-of-service attack activity in the Internet. Using this technique, we have observed widespread DoS attacks in the Internet, distributed among many different domains and ISPs. The size and length of the attacks we observe are heavy tailed, with a small number of long attacks constituting a significant fraction of the overall attack volume. Moreover, we see a surprising number of attacks directed at a few foreign countries, at home machines, and towards particular Internet services. We try to dissipate the mist on the the locations of spoofers based on investigating the path backscatter messages In this, 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 proved that, the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

REFERENCES

[1] G. Yao, J. Bi, and A. V. Vasilakos, “Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, 2015

[2] S. M. Bellovin, “Security problems in the TCP/IP protocol suite,” ACM SIGCOMM Computer Communication Review, vol. 19, no. 2, pp. 32–48, 1989.

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

[4] Labovitz, “Bots, DDoS and ground truth,” Presented at the 50thNANOG, 2010.

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

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM), pp. 295–306, 2000.

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

[8] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F Tchakountio, S. T. Kent, W. T. Strayer, “Hash-based IP traceback,” Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM), vol. 31, no. 4, pp. 3–14, 2001.

KANDA SRIDHAR is pursuing M.Tech (Computer science and Engineering), at Chirala Engineering College, chirala, Prakasam Dist., Andhra Pradesh, India.

Atchyut Kumar Reddy. A is an Assistant Professor in at Chirala Engineering College, Chirala, AP, India.