Scientific Journal of Impact Factor (SJIF): 3.134

E-ISSN (O): 2348-4470
P-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 12,December -2015

PTI: Expose The Location Through IP Traceback Algorithm

Mohini Ravale[1],Priyanka Ranjan[2], Prof. Sunil Yadav[3]

[1,2,3]Department Of Computer Engineering,Siddhant College Of Engineering,Sudumbare,Pune ,

Abstract *— 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, 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).Along these lines, PIT can discover the spoofers with no arrangement necessity. This paper represents the reasons, accumulation, and the factual results on way backscatter, exhibits the procedures and adequacy of PIT, and demonstrates the caught areas of spoofers through applying PIT on the way backscatter information 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.*

Keywords: Computer network management, 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. 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. 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.

This is the first article known which deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. 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.

A 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.

II. LITERATURE REVIEW

1) Efficient Packet Marking for Large-Scale IP Traceback (2002)

Author: Michael T. Goodrich

Author proposed 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.

2) Practical Network Support for IP Traceback (2002)

Author: Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson

This paper 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). 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.

3) FIT: Fast Internet Traceback (2005).

Author: Abraham Yaar, Adrian Perring, Dawn Song

E-crime is on the rise. 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:

- victims have to gather thousands of packets to reconstruct a single attack path
- they do not scale to large scale attacks
- they do not support incremental deployment

General properties of FIT:

- IncDep
- RtrChg
- FewPkt
- Scale
- Local

4) ICMP Traceback with Cumulative Path, An Ef_cient Solution for IP Traceback (2003)

Author: Henry C.J. Lee, Vrizlynn L.L. Thing, Yi Xu, and Miao Ma

DoS/DDoS attacks constitute one of the major classes of security threats in the Internet today. The attackers usually use IP spoofing to conceal their real location. The current Internet protocols and infrastructure do not provide intrinsic support to traceback the real attack sources. The objective of IP Traceback is to determine the real attack sources, as well as the full path taken by the attack packets. Different traceback methods have been proposed, such as IP logging, IP marking and IETF ICMP Traceback (ITrace). In this paper, we propose an enhancement to the ICMP Traceback approach, called ICMP Traceback with Cumulative Path (ITrace-CP). The enhancement consists in encoding the entire attack path information in the ICMP Traceback message. Analytical and simulation studies have been performed to evaluate the performance improvements. We demonstrated that our enhanced solution provides faster construction of the attack graph, with only marginal increase in computation, storage and bandwidth.

5) Trace IP Packets by Flexible Deterministic Packet Marking (FDPM) (2009)

Author: Yang Xiang and Wanlei Zhou

Currently a large number of the notorious Distributed Denial of Service (DDoS) attack incidents make people aware of the importance of the IP traceback technique. IP traceback is the ability to trace the IP packets to their origins. It provides a security system with the capability of identifying the true sources of the attacking IP packets. IP traceback mechanisms have been researched for years, aiming at finding the sources of IP packets quickly and precisely. In this paper, an IP traceback scheme, Flexible Deterministic Packet Marking (FDPM), is proposed. It provides more flexible features to trace the IP packets and can obtain better tracing capability over other IP traceback mechanisms, such as link testing, messaging, logging, Probabilistic Packet Marking (PPM), and Deterministic Packet Marking (DPM). The implementation and evaluation demonstrates that the FDPM needs moderately a small number of packets to complete the traceback process and requires little computation work; therefore this scheme is powerful to trace the IP packets. It can be applied in many security systems, such as DDoS defense systems, Intrusion Detection Systems (IDS), forensic systems, and so on.

III. SURVEY OF PROPOSED SYSTEM

We propose 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.

1. Advantages of proposed system

1)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.

2) A 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.

3) 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.

IV. PROPOSED ALGORITHM

1. Methodologies Of Problem Solving And Efficiency Issues:
    1. Find the shortest path from source (s) node to destination (d) node.
    2. The messassge can be send from r to d through many intermediate nodes i.e. routers (r).
    3. There may any spoofer origin available in between the path.

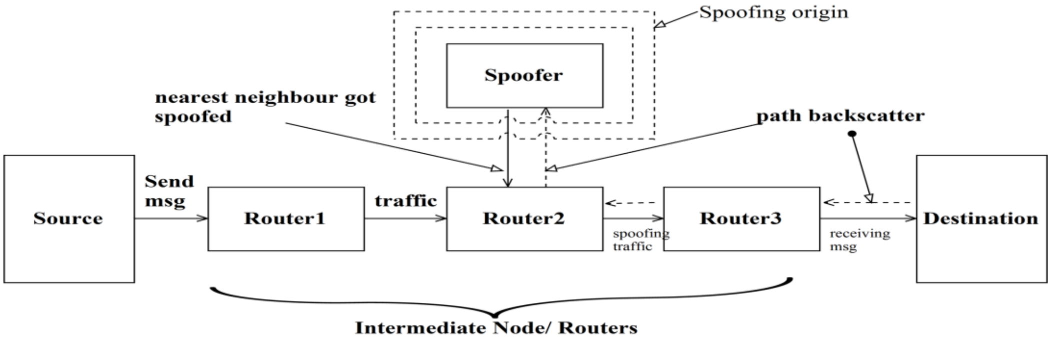
Assume, that ‘sp’ is the spoofer node in the network.
There are two assumptions for locating such spoofing origin while routing the packets in the network.

a. Loop-Free Assumption: This assumption states there is no loop in the paths. This assumption always holds unless misconfiguration or the routing has not converged.
b. Valley-Free Assumption: This assumption states there should be no valley in the some node level network paths. Though the increased complexity of node relationship has reduced the universality of this assumption, it is still the most common model of intermediate network level routing.
c. If suppose any intermediate node has being spoofed by spoofer node then the destination node will send the path backscatter message to all intermediate node indicating that spoofing has occurred at somewhere in the network.
d. Then each node in network will send the acknowledgment for that path backscatter message. The node which fails to give back acknowledgment that will be assumed as spoofer node.

2. Expected Outcome:
    1. We proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information.
    2. 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.
    3. We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness.

4. 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.

V. SYSTEM ARCHITECTURE



.

Fig. Architecture Of Proposed Work

VI. CONCLUSION AND FUTURE WORK

In this article we have presented 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 heavytailed, 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.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

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] 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] *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. 2001.484 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015

[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