International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

Forensic Spoofer Location Detection Using Passive IP Traceback Techniques

Pritish Deshpande[1], Virandra Patil[2], Mahesh Talekar[3], Swapnil Tapkir[4], Dhanajay Khade[5], Nitin Humbir[6]
[1, 2, 3, 4, 5, 6]Department of CSE, Dr. D. Y. Patil School of Engineering, Pune, India-412105
Email address: [1]mr.pritish2013@gmail.com

Abstract**—** *It is long known attackers may use designed source IP area to cover their real regions. To catch the spoofers, different IP traceback systems have been proposed. Then again, however, because of the difficulties of arrangement, there has been not a generally received IP traceback arrangement, in any event at the Internet level. Accordingly, the fog on the areas of spoofers has never been scattered till now. This paper proposes passive IP traceback (PIT) that sidesteps the sending challenges of IP traceback strategies. PIT examines Internet Control Message Protocol blunder messages (named way backscatter) activated by mocking movement, and tracks the spoofers in light of open accessible data (e.g., topology). Along these lines, PIT can find the spoofers with no game plan need. This paper represent to the reasons, accumulation, and the authentic results on way backscatter, displays the systems and adequacy of PIT, and shows the got regions of spoofers through applying PIT in transit backscatter data set. These outcomes can assist further with uncovering IP spoofing, which has been examined for long however never surely known. In spite of the fact that PIT can't work in all the spoofing attacks, it might be the most valuable instrument to follow spoofers before an Internet-level traceback framework has been sent in genuine.*

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 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].

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 [3].

II. EXISTING SYSTEM

Existing IP traceback approaches can be classified into five main categories: packet marking, ICMP traceback, logging on the router, link testing, overlay, and hybrid tracing.

A. Packet checking strategies require routers alter the parcel's header to contain the routers data and sending decision.

B. Different from packet stamping routines, ICMP traceback creates expansion ICMP messages to an authority or the destination.

C. Attacking way can be recreated from log on the switch when switch makes a record on the packets sent.

D. Link testing is a methodology which decides the upstream of assaulting activity jump by-bounce while the attacker is in advancement.

E. Center Track proposes offloading the suspect activity from edge routerts to uncommon following switches through an overlay system.

III. DISADAVNTAGE OF EXISITNG SYSTEM

A. Figures and tables Based on the caught backscatter messages from UCSD Network Telescopes, caricaturing exercises are still as often as possible observed. To assemble an IP traceback framework on the Internet faces no less than two discriminating difficulties. The first is the expense to embrace a traceback component in the directing framework. Existing traceback instruments are either not generally

B. Supported by current item switches, or will acquaint impressive overhead with the switches (Internet Control Message Protocol (ICMP) era, parcel logging, particularly in elite systems. The second one is the trouble to make Internet administration suppliers (ISPs) work together.

C. Since the spoofers could spread over each side of the world, a solitary ISP to convey its own particular traceback framework is verging on useless.

D. However, ISPs, which are business substances with focused connections, are by and large absence of unequivocal financial motivating force to help customers of the others to follow assailant in their oversaw ASes.

Pritish Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 40-43, 2016.

IV. PROPOSED SYSYTEM

A. This paper introduces an approach to, named Passive IP Traceback (PIT), to bypass the difficulties in organization. routers may fail to forward an IP spoofing packet because of different reasons, e.g., TTL surpassing. In such cases, the switches may produce an ICMP lapse message (named way backscatter) and send the message to the caricature source address. Since the switches can be near the spoofers, the way backscatter messages might conceivably reveal the spoofers' area

B. PIT exploits these way backscatter messages to discover the spoofers' area. With the spoofers' areas known, the casualty can look for assistance from the relating ISP to filters through the attackers packets, or take different counterattack

C. PIT is particularly valuable for the victims in reflection based spoofing attack, e.g., DNS amplification attack. The casualties can discover the spoofers' areas specifically from the attacking moveme.

V. CONTRIBUTION

A. 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.

VI. SYSTEM ARCITECTURE

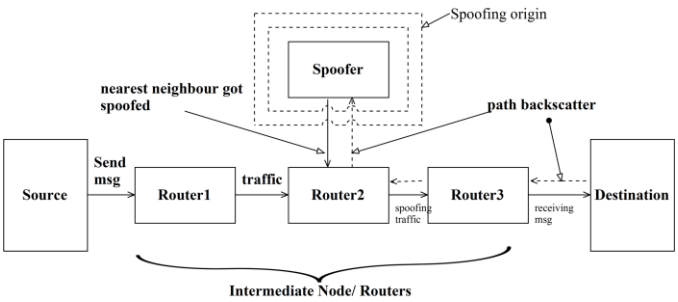

Fig. 1. Architecture of proposed work

VII. 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.

2) Practical Network Support for IP Traceback (2002)

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

*Abstrac*t:-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

Abstract:-E-crime is on the rise. The costs of the damages are often on the orderof several billion of dollars. Traceback mechanisms are a critical part of thedefense against IP spoofing and DoS attacks. Current traceback mechanisms are inadequateto address the traceback problem Problems with the current traceback mechanisms:

– victims have to gather thousands of packets toreconstruct 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

British Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 40-43, 2016.

4) ICMP Traceback with Cumulative Path, AnEf_cientSolution for IP Traceback (2003)

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

Abstract: DoS/DDoS attacks constitute one of the major classes of securitythreats in the Internet today. The attackers usually use IP spoofing to concealtheir real location. The current Internet protocols and infrastructure do not provideintrinsic 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 bythe attack packets. Different traceback methods have been proposed, such as IP logging, IP marking and IETF ICMP Traceback (ITrace). In this paper, we proposean enhancement to the ICMP Traceback approach, called ICMP Tracebackwith Cumulative Path (ITrace-CP). The enhancement consists in encoding the entireattack path information in the ICMP Traceback message. Analytical and simulationstudies have been performed to evaluate the performance improvements. We demonstrated that our enhanced solution provides faster construction of theattack 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*

Abstract: Currently a large number of the notorious Distributed Denial of Service (DDoS) attack incidents make people aware ofthe importance of the IP traceback technique. IP traceback is the ability to trace the IP packets to their origins. It provides asecurity 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 trace back 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.

VIII. MATH

Let S is the Whole System Consists:

S= {V, E, P, G}.

Where,

1. V is the set of all the network nodes.
2. E is the set of all the links between the nodes in the network.
3. P is path function which defines the path between the two nodes.
4. Let G is a graph.

Suppose, G (V, E) from each path backscatter, the node u, which generates the packet and the original destination v,

Where u and v are two nodes in the network. i.e. u∈V and v ∈ V of the spoofing packet can be got.

We denote the location of the spoofer, i.e., the nearest router or the origin by s,

Where, s∈ V.

IX. PROCEDURE

A. For each path backscatter message, at first we check whether it belongs to the classes i.e. dataset or source list. If yes, the reflector should be near the attacker.

B. We simply use the source AS of the message as the location of the spoofer. If the message does not belong to the types, it is mapped into an AS tuple.

C. We determine whether the AS tuple can accurately locate the source AS of the attacker based on our proposed mechanisms. Then if the AS tuple can accurately locate the source AS of the message, the source AS of the spoofer is just this AS.

D. Then we also use the source AS as the location of the spoofer.

We assume some Probability for Accurate Locating on Loop-Free for spoofer based on the Loop-free assumption, to accurately locate the attacker from a path backscatter message (v, s),

There are three conditions:

1) LF-C1: the degree of the attacker sis 1;
2) LF-C2: v is not s;
3) LF-C3: u is s.

Based on the Assumption I, the probability of LF − C1 is equal to the ratio of the network nodes whose degree is 1.

To estimate our assumptions of probability, we introduce the power law of degree distribution from,

$$f_d \propto d^{\mathcal{O}}$$

Where f_d is the frequency of degree d, and O is the out degree exponent.

Transform it to

$$f_d = \lambda d^{\mathcal{O}} + b_d$$

Where λ and b_d are two constants. Then,

$$f_1 = \lambda + b_d.$$

Based on the Assumption II, the probability of LF − C2 is simply (N − 1)/N.

Based on the Assumption III, the probability of LF −C3 is equal to 1/(1+len(path(u, v)).

Because sand uare random chosen, the expectation of len (path (u,v)) is the effective diameter of the network i.e. =1+len(path((u,v)).

Based on our three assumptions, these conditions are mutually independent. Thus, the expectation of the probability of accurate locating the attacker is

$$E(P_{LF-accurate}) = \frac{N-1}{N} * \frac{\lambda + b_d}{1 + \delta_{ef}}$$

Pritish Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 40-43, 2016.

This form gives some insight on the probability of accurate locating of spoofer. If the power-law becomes stronger, λ will get larger and δ_{ef} will get smaller. Then the probability of accurate locating will be larger.

X. 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.

ACKNOWLEDGMENT

Authors are cordially giving thanks to Prof. Nitin Humbir for her valuable and constructive suggestions. We sincerely thank Head of Department (Computer Engineering) Prof. Somitra S. Das for his reassuring encouragement throughout the preparation of our Paper. Also thanking to all others who have tried hard to make their work easy to accomplish.

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 50th NANOG*, 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.

Pritish Deshpande, Virandra Patil, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, and Nitin Humbir, "Forensic spoofer location detection using passive IP traceback techniques," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 2, pp. 40-43, 2016.