RESEARCH ARTICLE OPEN ACCESS

Passive IP Traceback: Disclosing the Locations of Man in the Middle from Path Backscatter

Aman Shekhar [1], Krishan Yadav [2], Krishna Yele[3]
Utpal Chirag [4], Ms. Santhi K. Guru [5]
Research Scholar [1], [2], [3] & [4], Assistant Professor [5]
Department of Computer Engineering
D Y Patil College of Engineering, Akurdi
Pune – India

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, due to the challenges regarding deployment services, there has been not any widely adopted IP traceback solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissolute till now. This paper proposes passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques and comes up with a solution to the problem. PIT investigates Internet Control Message Protocol (ICMP) error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information such as 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. As because of some limitations PIT cannot work in all the spoofing attacks, it may be a helpful mechanism of tracing a 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 thus protecting them from being traced, or enhance the effect of attacking, or launch reflection based attacks. A number of scandalous attacks rely on IP spoofing, including SYN flooding, SMURF, DNS amplification etc. A Domain Name System (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 [1] 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 [2], spoofing activities are still frequently observed. To capture the origins of IP spoofing traffic is of great importance. As long as the actual and real locations of spoofers are not disclosed, they cannot be deterred, stopped and prevented from launching further attacks. Even just approaching the spoofers, for example, determining the ASes or networks they reside in, attackers can be located and traced in a smaller area, and filters can be placed and arranged 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].

This is the first article known which deeply investigates path backscatter messages. These messages are important and valuable to help understand and analyze the spoofing activities. Backscatter messages, which are produced and generated by the targets of spoofing messages, to study Denial of Services (DoS) [4] [5], path backscatter messages, which are sent by intermediate devices during the information exchange and transfer 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 [6] 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 SURVEY

A. 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.

C. FIT: Fast Internet Traceback

[9] 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

D. ICMP Traceback with Cumulative Path, An Effcient Solution for IP Traceback

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 [10], we propose an enhancement to the ICMP Traceback approach [11], 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.

E. Trace IP Packets by Flexible Deterministic Packet Marking (FDPM)

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) [12], 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) [13] [14], and Deterministic Packet Marking (DPM) [15]. 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 [4], Intrusion Detection Systems (IDS), forensic systems, and so on.

III. EXISTING SYSTEM

Existing IP traceback approaches can be classified into five main categories: packet marking [7] [16], ICMP traceback [11] [10], logging on the router, link testing, overlay, and hybrid tracing.

1) Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision.
2) Different from packet marking methods, ICMP traceback generates addition ICMP messages to a collector or the destination.
3) Attacking path can be reconstructed from log on the router when router makes a record on the packets forwarded.
4) Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the attack is in progress.
5) Center Track proposes offloading the suspect traffic from edge routers to special tracking routers through a overlay network

IV. DISADVANTAGES OF EXISTING SYSTEM

1) Based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed. 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
2) Supported by current commodity routers, 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.
3) Since the spoofers could spread over every corner of the world, a single ISP to deploy its own traceback system is almost meaningless.
4) 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.
5) 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.
6) 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.

V. 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.

VI. PROPOSED SYSTEM ARCHITECTURE

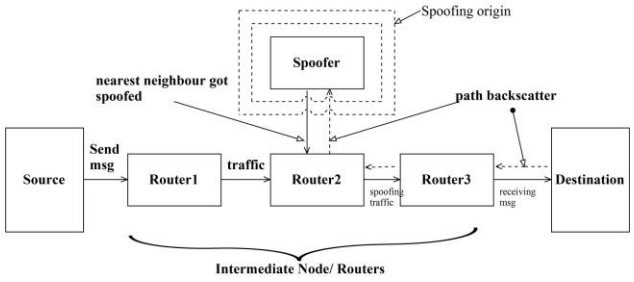

Fig. 1. Architecture of proposed work

A. Problem Statement

The Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP traceback.

B. Goals and objectives

1) Designing the IP traceback techniques to disclose the real origin of IP traffic or track the path.
2) A practical and effective IP traceback solution based on path backscatter messages.
3) Passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques.
4) Packet marking methods to modify the header of the packet to contain the information of the router and forwarding decision.

C. 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 noloop in the paths. This assumption always holds unless misconfiguration or the routing has not converged.
b) Valley-Free Assumption: This assumption states thereshould 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.

1) 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.
2) 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.

VII. EXPECTED OUTCOME

We proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. 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.

A. Applications

1) IP traceback is a method to traceback to the source of the packets.
2) Packet marking schemes are the most successful implementation towards preventing DoS attacks by tracing to the source of attacks.

VIII. CONCLUSION

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 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 actual 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.

ACKNOWLEDGEMENT

We are grateful to Prof. M. A. Potey, Head of Department of Computer Engg., D.Y.P.C.O.E. for always being ready to help with the most diverse problems that we have encountered along the way. We express our sincere thanks to all our staff and colleagues who have helped us directly or indirectly in completing this project. She patiently discussed the ideas with us and gave indispensible suggestions.

REFERENCES

[1] C. Labovitz, "Bots, ddos and ground truth," *NANOG50, October*, vol. 5, 2010.

[2] "The ucsd network telescope."

[3] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," *ACM SIGCOMM Computer Communication Review*, vol. 19, no. 2, pp. 32–48, 1989.

[4] W. Caelli, S. Raghavan, S. Bhaskar, and J. Georgiades, "Policy and law: denial of service threat," in *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks*, pp. 41–114, Springer, 2011.

[5] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.

[6] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-based ip traceback," in *ACM SIGCOMM Computer Communication Review*, vol. 31, pp. 3–14, ACM, 2001.

[7] M. T. Goodrich, "Efficient packet marking for large-scale ip traceback," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 117–126, ACM, 2002.

[8] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for ip traceback," in *ACM SIGCOMM Computer Communication Review*, vol. 30, pp. 295–306, ACM, 2000.

[9] A. Yaar, A. Perrig, and D. Song, "Fit: fast internet traceback," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 2, pp. 1395– 1406, IEEE, 2005.

[10] H. C. Lee, V. L. Thing, Y. Xu, and M. Ma, "Icmp traceback with cumulative path, an efficient solution for ip traceback," in *Information and Communications Security*, pp. 124–135, Springer, 2003.

[11] draft-bellovin itrace, "Icmp traceback messages," 2003.

[12] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An ip traceback system to find the real source of attacks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 20, no. 4, pp. 567–580, 2009.

[13] J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient ip traceback," *Computer Networks*, vol. 51, no. 3, pp. 866–882, 2007.

[14] M. Adler, "Trade-offs in probabilistic packet marking for ip traceback," *Journal of the ACM (JACM)*, vol. 52, no. 2, pp. 217–244, 2005.

[15] A. Belenky and N. Ansari, "Ip traceback with deterministic packet marking," *IEEE communications letters*, vol. 7, no. 4, pp. 162–164, 2003.

[16] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for ip traceback," in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, pp. 878–886, IEEE, 2001.