ISSN 2229-5518

THE LOCATIONS OF IP SPOOFERS FROM PATHWAY BACKSCATTER IN PASSIVE IP TRACEBACK

[1]S. Mahesh Babu, K. Sreenivas [2]
[1]*(CSE, GIST/ JNTU ANANTHAPURAMU, INDIA)*
[2]*(CSE, GIST / JNTU ANANTHAPURAMU, INDIA)*

ABSTRACT:

It isvery 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.

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.

Given the difficulties of the IP traceback mechanisms deployment, we are considering another direction: tracking the spoofers without deploying any additional mechanism. In another word, we try to disclose the location of spoofers from the traces generated by existing widely adopted functions on commodity routers when spoofing attacks happen.

Instead of proposing another IP traceback mechanism with improved tracking capability, 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.

The system presents PIT, which tracks the location of the spoofers based on path backscatter messages together with the topology and routing information. We discuss how to apply PIT when both topology and routing are known, or only topology is known, or neither are known respectively. We also present two effective algorithms to apply PIT in large scale networks. In the following section, at first we show the statistical results on path backscatter messages. Then we evaluate the two key mechanisms of PIT which work without routing information. At last, we give the tracking result when applying PIT on the path backscatter message dataset: a number of ASes in which spoofers are found.

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

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.RELATED PROBLEM

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.

Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision.

Different from packet marking methods, ICMP traceback generates addition ICMP messages to a collector or the destination.

Attacking path can be reconstructed from log on the router when router makes a record on the packets forwarded.Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the attack is in progress.

CenterTrack proposes offloading the suspect traffic from edge routers to special tracking routers through a overlay network ,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 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.

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.

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.

III.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.

IV.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.

V.CONCLUSION

We try to dissipate the mist on the 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.

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.

[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. IEEEComput. 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. IEEE20th 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.

[16] Y. Xiang, W. Zhou, and M. Guo, “Flexible deterministic packet marking: An IP traceback system to find the real source of attacks,” *IEEE Trans.Parallel Distrib. Syst.*, vol. 20, no. 4, pp. 567–580, Apr. 2009.

[17] R. P. Laufer*et al.*, “Towards stateless single-packet IP traceback,” in *Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN)*, Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/LCN.2007.160

[18] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, “A stateless traceback technique for identifying the origin of attacks from a single packet,” in *Proc. IEEE Int. Conf.Commun. (ICC)*, Jun. 2011, pp. 1–6.

[19] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, “On design and evaluation of ‘intention-driven’ ICMP traceback,” in *Proc. 10th Int.Conf. Comput. Commun. Netw.*, Oct. 2001, pp. 159–165