ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 4, Issue 1, pp: (47-51), Month: April 2017 – September 2017, Available at: www.paperpublications.org

REVEALING THE LOCATIONS OF IP SPOOFERS FROM ICMP

[1]J Saranya, [2]Dr. A J Deepa

[1]PG student, Department of CSE, Ponjesly College of Engineering, Nagercoil
[2]Assosicate Professor, Department of CSE, Ponjesly College of Engineering, Nagercoil

Abstract: **Forged source IP addresses are used by the attackers to hide the locations. For finding the locations of the attackers IP Traceback Mechanism have been used. IP Traceback approaches can be classified in to Packet Marking, ICMP Traceback, Logging on the Router, Link Testing, Overlay and Hybrid Tracing, Based on the captured backscatter messages spoofing activities are still frequently observed. The IP Traceback system on the internet contain with two critical challenges. The first one is the cost to adopt a traceback mechanism in the routing system. It introduces considerable overhead to the routers generation, packet logging, especially in the high performance networks. The second one is the difficulty to make Internet Service Providers(ISP) collobrate. Attackers spread over every corner of the world, single ISPs to deploy its own traceback system is meaningless. ISPs are generally lack of explicit incentive to help clients of the others to trace attackers in their managed system. There are lot of IP traceback mechanisms and large number of spoofing activities observed , but the real locations of spoofers still remain mystery. Due to the some of the drawbacks it has not been widely used to trace the IP traceback solution. Finally, it was not used to find the locations of the attackers. To overcome the drawback of IP traceback mechanism we propose a Passive IP Traceback Mechanism (PIT). The router may generate an ICMP error message and send the message to the spoofed source addresses. The routers can be close to the attackers, the path backscatter messages may disclose the locations of the attackers. PIT can work in a number of spoofing activities. This technique uses the ICMP features and find the attackers by applying PIT on the ICMP dataset, a number of locations of attackers are captured and presented. As a result, these technique reveal IP spoofing, but it was not well understood. In future, it may be the most suitable mechanism for tracing the attackers on the Internet Level Traceback System.**

Keywords: **IP Traceback, packet logging, path backscatter, hybrid tracing, link testing.**

1. INTRODUCTION

Traceback is the process of tracing something back to its source where the packets have originated. It is the method for reliably determining the tracing of packet on the Internet. With the use of the traceback it can easily identifies the source address where the packet have sent. If the traceback is not used then it cannot identify the source address in the network where the packets are sent.

Internet Protocol has the task of delivering packets from the source host to the destination host based on the IP addresses in the packet headers. The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

IP Traceback determining the origin of a packet on the Internet. Due to the trusting nature of the IP, the source IP address of a packet is not authenticated. The source address in an IP packet can be inaccurate or one-way attacks (IP spoofing). IP traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Passive IP Traceback determine the network in which routers are periodically updated by network administrators or by neighboring routers to find the location of the spoofers. With the use of the Passive IP Traceback the spoofers location are easily identified with the use of the routers. The routers are periodically checked and the spoofers location are easily identified.

Autonomous is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on a single administrative entity. An AS is a heterogeneous network typically governed by a large enterprise. An AS has many different subnetworks with combined routing logic and common routing policies. Each subnetwork is assigned a globally unique 16 digit identification number by the Internet Assigned Numbers Authority (IANA).

An Internet Service Provider (ISP) is an organization that provides services for accessing and using the Internet. The larger ISPs have their own high speed leased lines so that they are less dependent on the telecommunication providers and can provide better services to their customers. The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol. It is used by network devices, like routers, to send error messages. It is an error reporting protocol like routers use to generate error messages to the source IP address when service or host cannot be reached for packet delivery.

2. RELATED WORK

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

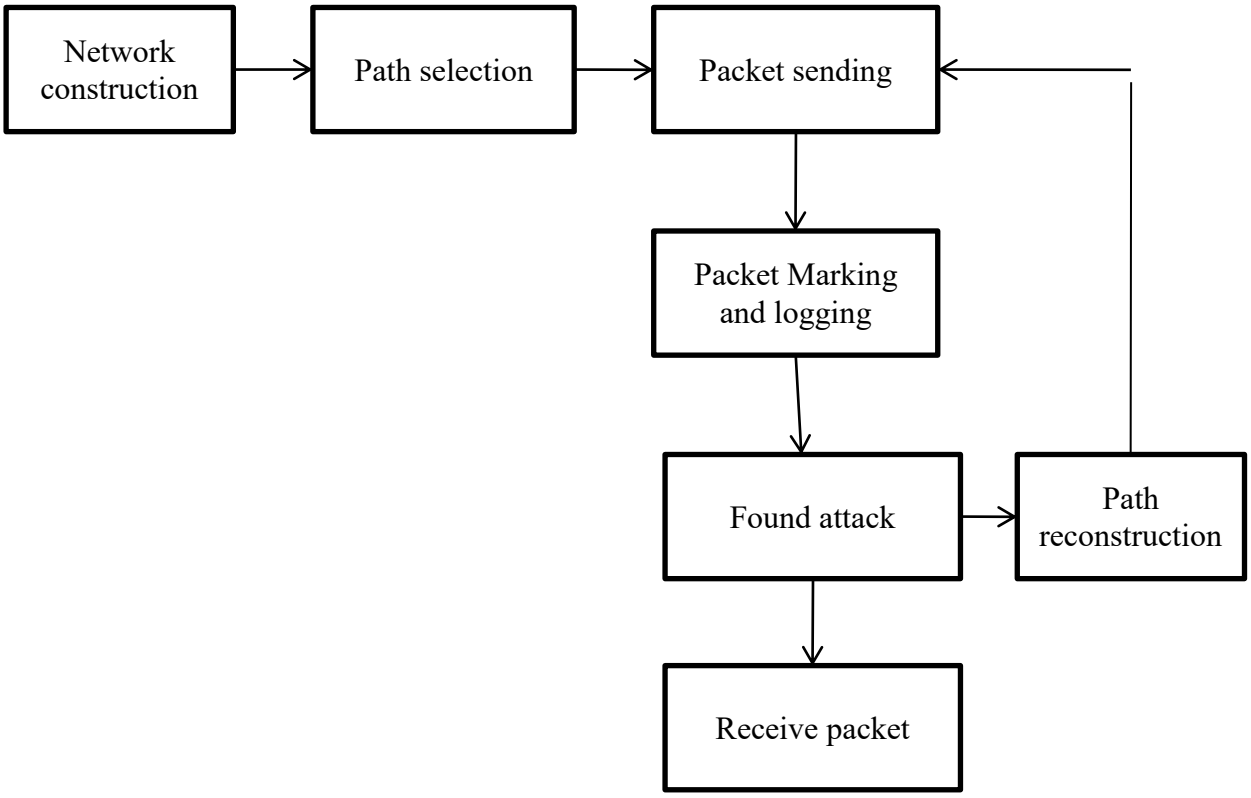
3. PROPOSED SYSTEM

Passive IP Traceback (PIT) is proposed, 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 may deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. A practical and effective IP traceback solution based on path backscatter messages, i.e., PIT, is used. 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.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 4, Issue 1, pp: (47-51), Month: April 2017 – September 2017, Available at: www.paperpublications.org

4. SYSTEM ARCHITECTURE



1. Topology construction:

The topology is the arrangement of nodes in the simulation area. The routers are connected in mesh topology. In which each routers are connected to each other via other routers (Path). It contain 12 nodes as the router node and 20 nodes as the client-server node. Totally we are having 32 nodes in our network. Each host is connected via routers. Each host has multiple paths to reach a single destination node in the network. The nodes are connected by duplex link connection. The bandwidth for each link is 100 mbps and delay time for each link is 10 ms. Each edges uses Drop Tail Queue as the interface between the nodes.

2. Collection of path backscatter messages:

Though path backscatter can happen in any spoofing based attacks, it is not always possible to collect the path backscatter messages, as are sent to the spoofed addresses. The classify spoofing based attacks into categories, and discuss whether path backscatter messages can be collected in each category of attacks.

2a. Single Source, Multiple Destinations:

In such attacks, all the spoofing packets have the same source IP address. The packets are sent to different destinations. Such packets are typically used to launch reflection attacks. The victim captures path backscatter in reflection attacks. Reflection attacks, e.g., DNS amplification, are the most prevalent IP spoofing attacks in recent years. The victim in a reflection attack is the host who owns the spoofed address. The victim itself is able to capture all the path backscatter messages in reflection attacks. All the spoofing packets are set the address of the victim, all the path backscatter messages will be sent to the victim. Then the victim can get the path backscatter messages through checking if it has sent messages to the original destination IP address field in received ICMP messages.

2b. Multiple Sources, Multiple Destinations:

Spoofing attacks can be launched against multiple destination IP addresses belonging to the same website or service provider (e.g., cloud). Generally, such attacks can be regarded as the combination of multiple attacks.

3. Passive IP Traceback mechanism:

PIT is actually composed by a set of mechanisms. The basic mechanism, which is based on topology and routing information. Whenever a path backscatter message whose source is router r (named reflector) and the original destination is od is captured, the most direct inference is that the packet from attacker to od should bypass r. A very simple mechanism in spoofing origin tracking. The network is abstracted as a graph G(V, E), where V is the set of all the network nodes and E is the set of all the links. A network node can be a router or an AS, depending on the tracking scenario. From each path backscatter message, the node r, r ∈ V which generates the packet and the original destination od, od ∈ V of the spoofing packet can be got. Denote the location of the spoofer, i.e., the nearest router or the origin AS, by a, a ∈ V.

With the use of path information, track the location of the spoofer. Use path(v,u) to denote the sequence of nodes on one of the path from v to u, and use PAT H(v, u) to denote the set of all the paths from v to u. Use ϕ(r, od) to denote the set of nodes from each of which a packet to od can bypass r,

ϕ(r, od) = {v|r € path(v, od), path(v, od) € PAT H(v, od)}. Where

ϕ(r, od) - determines the minimal set which must contain the spoofer. An ISP can make this model to locate spoofers in its managed network. Performs tracing does not know the routing choices of the other networks, which are non-public information.

5. CONCLUSION

To find the locations of spoofers based on investigating the ICMP messages. Passive IP Traceback (PIT) which tracks spoofers based on ICMP and public available information. It illustrate causes, collection, and statistical results on path backscatter. It also specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. Two effective algorithms to apply PIT in large scale networks and proofed the correctness. It demonstrated the effectiveness of PIT based on deduction and simulation. It showed the captured locations of spoofers through applying PIT on the path backscatter dataset. Also with the use of the routers capture the location of the spoofers. The most of the spoofers are near the router so the router are periodically updated to find the spoofers location near the router. The spoofers may use of the forged IP address to hide their location. So inorder to find the location of the spoofers the IP address are given higher then the original IP address. And select the node randomly to check the spoofers are available near the router. By using this Traceback the locations of the spoofers are identified by periodically updated in the router. These results can help further reveal IP spoofing, to find the location of the spoofers.

REFERENCES

[1] M. T. Goodrich, “Efficient packet marking for large-scale ip traceback,”in Proceedings of the 9th ACM Conference on Computer and Communications Security, ser CCS ’02.NewYork, NY, USA: ACM, 2002,pp. 117–126.

[2] 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.

[3] 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 International Conference Communication. (ICC), Jun. 2011, pp. 1–6.

[4] B. Al-Duwairi and M. Govindarasu, “Novel hybrid schemes employing packet marking and logging for IP traceback,” IEEE Transaction Parallel Distribution System vol. 17, no. 5, pp. 403–418, May 2006.

[5] H. Wang, C. Jin, and K. G. Shin, “Defense against spoofed IP traffic using hop-count filtering,” IEEE ACM Transaction Network, vol. 15, no. 1, pp. 40–53, Feb. 2007.

[6] C. Gong and K. Sarac, “A more practical approach for single-packet ip traceback using packet logging and marking,” Parallel and Distributed Systems, IEEE Transactions on, vol. 19, no. 10, pp. 1310–1324, Oct 2008.

[7] Daniel B. Faria and David R. Cheriton **"**Detecting identity-based attacks in wireless networks using signalprints"**,** Computer Communcation.vol. 29, no. 4, pp. 251–262, 2006.

[8] Yong Sheng, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", ACM Transaction Computing System, vol. 24, no. 2, pp. 115–139, May 2008.

[9] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," IEEE Computer Communication Society, vol. 2. Apr. 2001, pp. 878–886.

[10] M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," Journal. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.