Traceback Mechanisms to Identify IP Snoofers

Pooja P[1], Vartika Sharma[2], Syed Thouheed Ahmed[3]

[1]MTech student, Dept. of CSE, GSSSIETW, Mysuru.
[2]Associate Professor, Dept. of CSE, GSSSIETW, Mysuru
[3]Sr.Research Engineer, Thinksoft and Information technologies, Bangalore

***Corresponding Email: pujaprabhu7@gmail.com**

ABSTRACT

It is long known attackers may use forged source IP address to conceal 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. The passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques which identifies and deeply investigates path backscatter messages, these messages are valuable to understand spoofing activities. It specifies victims in reflection based spoofing attacks, the victims can find the locations of the spoofers directly from the attacking traffic. Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic,and tracks the spoofers based on public available information. These results can help further reveal IP spoofing, which has been studied for long but never well understood.

Keywords: IP Traceback, Passive IP Traceback (PIT), IP Spoofers.

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 [1]. By using addresses that are assigned to others or not assignedat 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 [2]. Though there has been a popular conventional wisdom that DoS attacks are launched from botnets and spoofing is no longer critical,Indeed, based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequentlyobserved [4].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.

RELATED WORK

(1) Study on UCSD network Telescope

The UCSD network telescope is passive traffic monitoring system built on a globally routed, but lightly utilized, this unique resource provides valuable data for network security researchers. This telescope carries almost no legitimate traffic because there are few provider-allocated IP addresses. After discarding the legitimate traffic from incoming packet, remaining data represents a continuous view of anomalous unsolicited traffic or internet background radiation (IBR).The IBR results from wide range of events, such as backscatter from randomly spoofed source denial of service attack, the automated spread of internet worms and viruses, scanning of address space by attackers looking for vulnerable targets and various misconfigurations [4].

(2) ICMP Traceback Messages

S. Bellovin [6], [8]research focus on a New ICMP message is often useful to learn the path that packets take through the internet, especially when dealing with denial-of service attacks. The majority of IP traceback proposals attempt to either log or insert marks into IP packets as these are forwarded by IP routers, such proposals state that these follow the ‘packet accounting’ paradigm. That is, they try to ‘account’ for IP packets by recording a packet’s identity, based on its content, as well as its route, based on which routers forwarded that packet. This record of identity and route is then used to successively traceback a packet through the routers that forwarded it. The two approaches of marking and logging have different emphasis, with regards to recording packet identity and route [6]. When marking, the route is explicitly recorded by inserting each router’s unique identifier into packets.When logging packets, one must explicitly record the identity of each packet and the route is deduced by querying visited routers. By accounting for packets one can traceback a given packet after this has been delivered and is no longer being forwarded through the network.

(3) Distributed Denial of Service (DDOS) attacks

Distributed Denial of Service (DDoS) attacks are among the most malicious Internet attacks that overwhelm a victim system with data such that the victim response time is slowed or totally stopped. Defending against DDoS attacks has hence become a major priority in the Internet community. Clearly, any defense against DDoS attacks is contingent on the ability of defenders to identify the source of DDoS attacks [3]. This process is known as Traceback [8]. (I.e. tracing back the origin of attack traffic). To date, the best known approach for traceback is to place tracking information into rarely used header fields inside the IP packets as and when the traffic propagates through the Internet. Since, available space in IP header is limited, routers probabilistically marking each packet with their IDs, along with their position in the routing path, called as Probabilistic Packet Marking (PPM) Scheme [2], [5], and [7]. For large number of DDoS packets, if each router probabilistically marks a packet, this approach is expected to provide enough router and path information at victim side in order to traceback the path and hence the source of attack traffic [2].

PROPOSED SYSTEM

A novel solution, named Passive IP Traceback (PIT), is used 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. The victims can find the locations of the spoofers directly from the attacking traffic.

The figure 1, it shows the snoofing process in which there will be sender and receiver with unique IP address for each, in between sender and receiver there will be a snoofer with unique IP address which is not known to sender and receiver. When sender sends the data to receiver, the snoofer will take that data and mask the IP address of sender now snoofer will become the sender as sender IP address will be masked. Snoofer will now have the copy of sender, snoofer will send that data to receiver and receiver believes that it been received from original source as IP address will be masked. Again receiver sends the data to sender there will snoofer in between sender and receiver. Snoofer will going to mask IP address of receiver and sends to sender. Sender receives the data as it comes from original destination. Snoofer is the information bouncing point between sender and receiver, who is going to bounce the data and keep the copy of data with him.

The figure 2 shows the system architecture of snoofer, in which there will be a router fixed for sender and Receiver in between the Reflectors. When sender decided to dispatch the msg to destination there will bouncing point situated in between sender and receiver called as Reflector. Based on information reflected between sender and receiver channel, reflected Traffic, Path Backscatter Messages. The real location of IP Spoofer is determined and tracked the details about Snoofer.

Basic Tracking Mechanism

Whenever a path backscatter message whose source is router r (named reflector) and the original destination is ogd is captured, the most direct inference is that the packet from attacker to ogd should bypass r. The 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 ogd, ogd ∈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. We make use of path information to help 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, ogd) to denote the set of nodes from each of which a packet to od can bypass r, i.e., ϕ(r, ogd) = {v |r ∈path (v, ogd), path (v, ogd) ∈PAT H (v, ogd)}.ϕ(r, ogd) actually determines the minimal set which must contain the spoofer. We name the result set of ϕ(r, ogd) by suspect set.If all the paths are loop-free, the suspect set determined by the path backscatter message is {Attacker, Router A}. If the topology and routes of the network are known, this mechanism can be used to effectively determine the suspect set. For example, an ISP can make this model to locate spoofers in its managed network.

However, for most cases, the one who performs tracing does not know the routing choices of the other networks, which are non-public information. Moreover, the topologies of most of the ASes are unknown to the public.

CONCLUSION

The Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. It shows the causes, collection, andstatistical results on path backscatter.path backscatter messages are captured and locations of spoofers are obtained by applying PIT on the path backscatter dataset. These results can help further reveal IP spoofing.

REFERENCE

[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]UCSD Network Telescope. [Online]: http://www.caidia.org/projects/network_telescope

[5] 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] 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

[8] M. T. Goodrich, “Efficient packet marking for large-scale IP traceback,”in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002,pp. 117–126

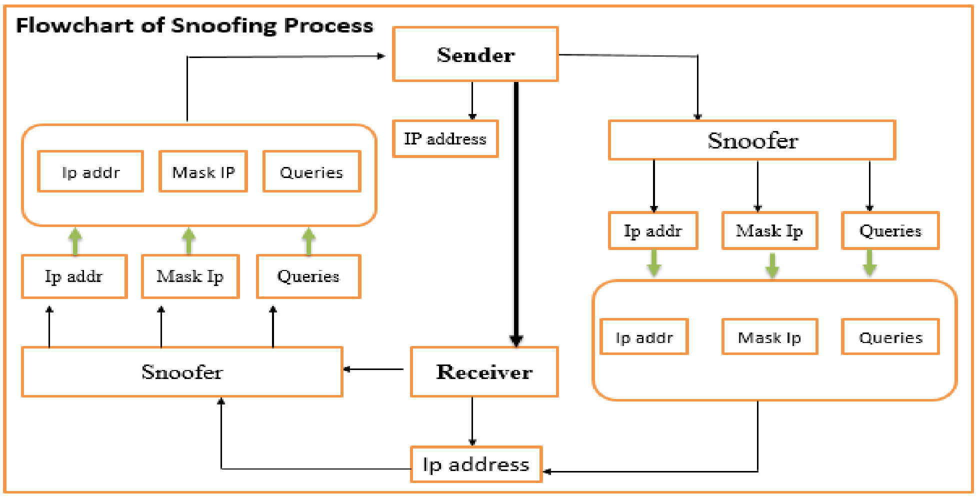

Figure 1: Flowchart of Snoofing Process

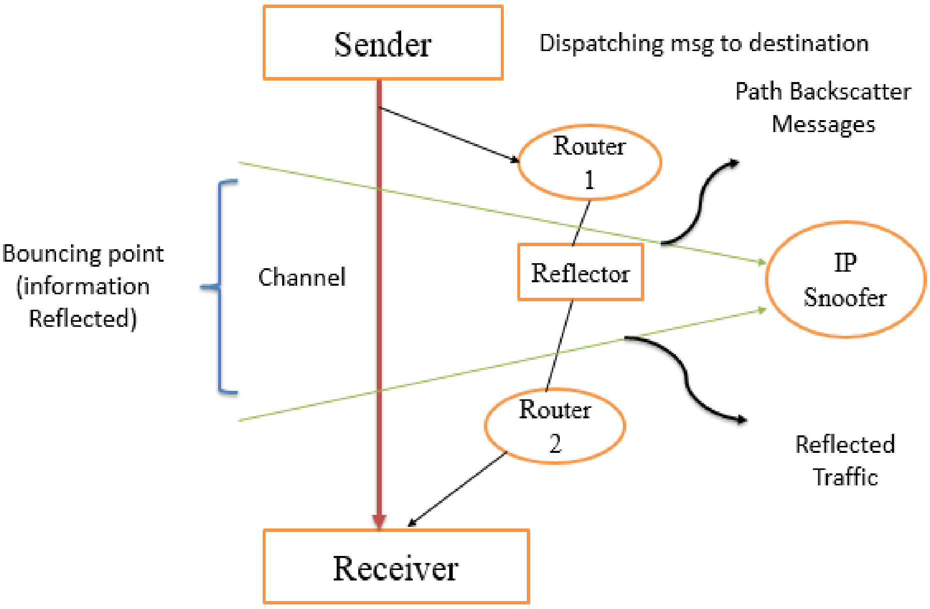
Sender
Dispatching msg to destination
Path Backscatter Messages
Router 1
Bouncing point (information Reflected)
Channel
Reflector
IP Snoofer
Router 2
Reflected Traffic
Receiver

Figure 2: System architecture of Snoofer