Tracing the Spoofers Using Passive IP Traceback(PIT)

K Indumathi[1] ,S Anton Pradeep [2],R Gowtham [3,]G Karthikeyan [4]

[1]Asst. Professor, Department of Information Technology, Kings Engineering College

[2,3,4]Student,Department of Information Technology, Kings Engineering College

Abstract— Passive IP Traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol (ICMP) error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers. The causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT. 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

A. Backend

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. As a result, the mist on the locations of spoofers has never been dissipated till now.

B. Innovation

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 mech-anism 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) gen-eration , 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.

C. Our Make

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 sourceaddress. 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 loca-tions 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.

Our work has the following contributions:

1. 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.
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.

I. WORK

Though PIT is used to perform IP traceback, it is very different from existing IP traceback mechanisms. PIT is inspired by a number of IP spoofing observation activities. Thus, the related work is composed by two parts. The first briefly introduces existing IP traceback mechanisms, and the second introduces the IP spoofing observation activities.

A. IP Tracebacking

IP traceback techniques are designed to disclose the real origin of IP traffic or track the path. 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.

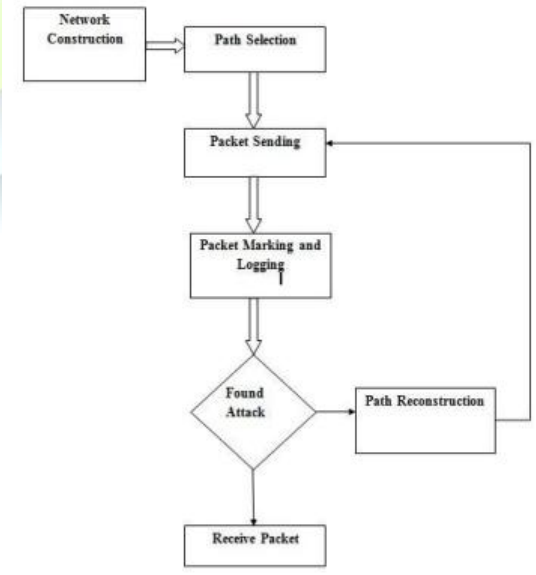
CenterTrack proposes offloading the suspect traffic from edge routers to special tracking routers through a overlay network. Though such a mechanism can reduce the requirement on edge routers, the management of the tunnels and the overlay network will be significantly increase the network management overhead. Ref. proposes building an AS-level overlay to trace spoofers. It is found if hundreds of ASes can join the overlay network, the spoofers can be accurately located. However, the challenge in practice is how to make the ASes cooperate. The intra-domain version of this work can avoid this problem, but it is necessary to update routers to adopt modification on OSPF.

The above mechanisms can be combined to achieve better tracing capacity and/or reduce the cost. There are a number of hybrid mechanisms employ both packet marking and logging . Though the overhead on routers can be reduced, they require the routers to support both mechanisms; thus the barrier to adopt them is higher than adopting a single mechanism.

Though there have been a large number of promising trace-back mechanisms, there is still a long way to get the proposed mechanisms widely deployed, especially at the Internet level. Currently, there is still lack of a ready mechanism to track the spoofers.

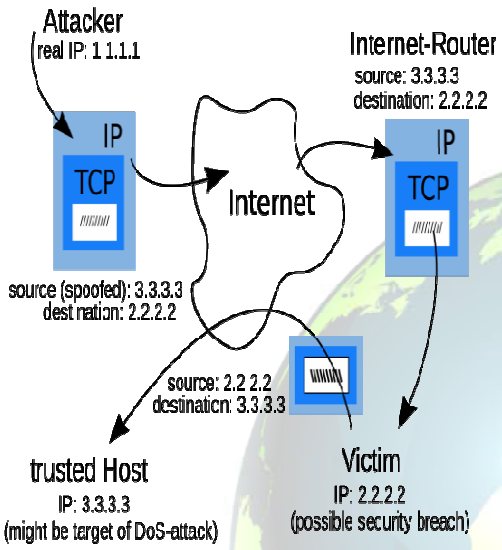
B. IP Spoofing View

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



C. Overview

Not all the packets reach their destinations. A network device may fail to forward a packet due to various reasons. Under certain conditions, it may generate an ICMP error message, i.e., path backscatter messages. The path backscatter messages will be sent to the source IP address indicated in the original packet. If the source address is forged, the messages will be sent to



node who actually owns the address. This means the victims of reflection based attacks, and the hosts whose addresses are used by spoofers, are possibly to collect such messages.

As specified by RFC792 , the format of the path backscatter messages, is illustrated. Each message contains the source address of the reflecting device, and the IP header of the original packet. Thus, from each path backscatter, we can get 1) the IP address of the *reflectingdevice* which is on the path from the attacker to the destinationof the spoofing packet; 2) the IP address of the
originaldestination of the spoofing packet. The original IPheader also contains other valuable information, e.g., the remaining TTL of the spoofing packet. Note that due to some network devices may perform address rewrite (e.g., NAT), the original source address and the destination address may be different.

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.
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.

DISADVANTAGES OF EXISTING SYSTEM:

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.

i. 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.

I. PROPOSED SYSTEM:

1) We propose a novel solution, named Passive IP Traceback (PIT), to bypass the challenges in deployment.

2) 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.

3) Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers
.

4) 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.

5) PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attack. The victims can find the locations of the spoofers directly from the attacking traffic.

The entire work of this paper is divided into five different modules. They are:

Network topology Construction
Path Selection
Packet Sending
Packet Marking and Logging
Path Reconstruction

Network topology Construction

A Network Topology may consist of the no.of routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The no.of routers connected to a single router is called as the degree of a router. This is calculated and stored in a table. The Upstream interfaces of each router also have to be found and stored in the interface table.

Path Selection

The path is said to be the way in which the selected packet or file has to be sent from the source to the destination. The Upstream interfaces of each router have to be found and it is stored in the interface table. With the help of that interface table, the desired path between the selected source and destination can be defined.

Packet Sending

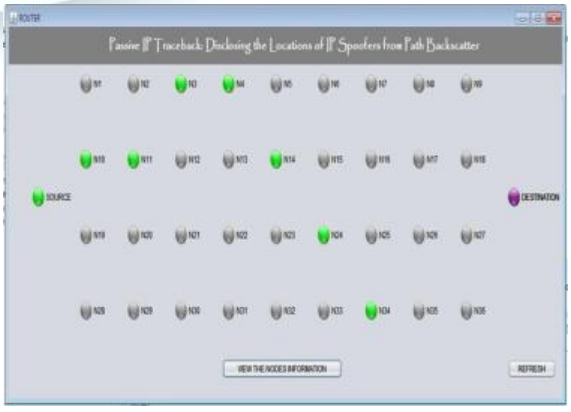
One of the Packet or file is to be selected for the transformation process. The packet is sent along the defined path from the source LAN to destination LAN. The destination LAN receives the packet and checks whether that it has been sent along the defined path or not.

Packet Marking and Logging

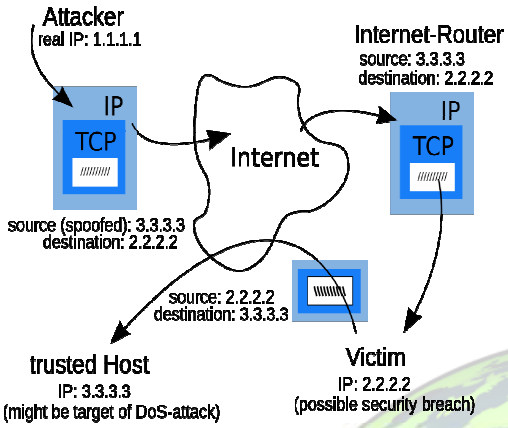
Packet Marking is the phase, where the efficient Packet Marking algorithm is applied at each router along the defined path. It calculates the Pmark value and stores in the hash table. If the Pmark is not overflow than the capacity of the router, then it is sent to the next router. Otherwise it refers the hash table and again applies the algorithm.

Path Reconstruction

Once the Packet has reached the destination after applying the Algorithm, there it checks whether it has sent from the correct upstream interfaces. If any of the attack is found, it request for the Path Reconstruction. Path Reconstruction is the Process of finding the new path for the same source and the destination in which no attack can be made.



IP SPOOFING

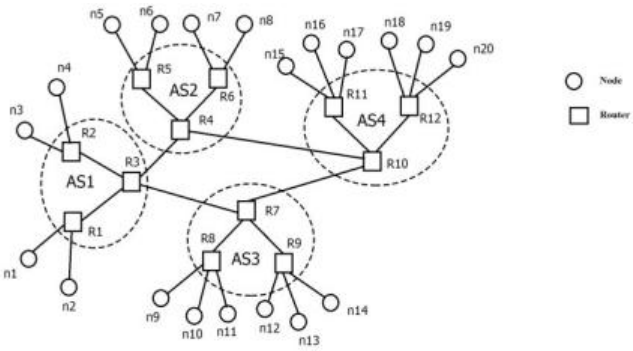



```
1: function GETSUSPECTSET_LOOPFREE(G,r,od)
2:     SuspectSet ← ∅
3:     c ← null
4:     P ←shortest path from r to od
5:     for Vertex v in P do
6:         if v == r then
7:             Continue
8:         end if
9:         G' ← G.remove(v)
10:        if r and od are disconnected in G' then
11:            c ← v
12:            break
13:        end if
14:    end for
15:    SG ← G.remove(c)
16:    for Vertex v in SG do
17:        if v and r are connected in SG then
18:            SuspectSet ← SuspectSet + v
19:        end if
20:    end for
21:    return SuspectSet
22: end function
```

CONCLUSION

We try to dissipate the mist on the the locations of spoofers based on investigating the path backscattermessages. 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

ROUTING



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.

REFERENCE

[1] J. Postel. Internet Control Message Protocol, RFC792[Online].Available:https://tools.ietf.org/html/rfc792, accessed Sep. 1981.

[2] G. Yao, J. Bi, and Z. Zhou, "Passive IP traceback: Capturing the origin of anonymous traffic through network telescopes," in Proc. ACM SIGCOMM Conf. (SIGCOMM), 2010, pp. 413414.[Online].Available:http://doi.acm.org/10.1145/1851182.1851237.

[3] Christo Ananth, M. Suresh Chinnathampy, S. Allwin Devaraj, S. Esakki Rajavel, V. Kulandai Selvan, P. Kannan, "CAPACITY BEHAVIOUR USING WSDV SCHEME OVER WIMAX", ABHIYANTRIKI-An International Journal of Engineering & Technology (AIJET), Vol. 1, No. 2,December 2014,pp:18-27

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

[5] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.484 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.

[6] "Passive IP Traceback: Disclosing the Locationsof IP Spoofers From Path Backscatter" Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE.