**.NET Project On Passive IP Traceback Disclosing the Locations of IP Spoofers From Path**

**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. 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.

**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:**

1. Based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed.
2. 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.
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.

**PROPOSED SYSTEM:**

* 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.

**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.

**MODULES:**

1. Topology construction
2. Collection of path backscatter messages
3. Passive IP Traceback mechanism
4. Performance evaluation

**MODULE DESCRIPTION:**

**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). In our simulation, we are using 11 nodes as the router node and 20 nodes as the client-server node. Totally we are having 31 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.

**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 they are sent to the spoofed addresses. We classify spoofing based attacks into four categories, and discuss whether path backscatter messages can be collected in each category of attacks.

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. As illustrated in following figure, because 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.

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 belonging to the above two types.

**Passive IP Traceback mechanism**

PIT is actually composed by a set of mechanisms. The basic mechanism, which is based on topology and routing information, is illustrated below.

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*. We use 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*.

**Performance Evaluation**

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 *?(r, od)*to denote the set of nodes from each of which a packet to *od*can bypass *r*, i.e., *?(r, od)*={*v*|*r*∈ *path(v, od), path(v, od)*∈ *PAT H(v, od)*}*.*  *?(r, od)*actually determines the minimal set which must contain the spoofer. We name the result set of *?(r, od)*by *suspect set*. As illustrated in following figure, 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.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System                          :         Pentium IV 2.4 GHz.
* Hard Disk                      :         40 GB.
* Floppy Drive                 :         1.44 Mb.
* Monitor                         :         15 VGA Colour.
* Mouse                            :         Logitech.
* Ram                               :         512 Mb.

**SOFTWARE REQUIREMENTS:**

* Operating system           :         Windows XP/7.
* Coding Language :         JAVA, .net
* IDE                      :         ECLIPSE KEEPLER
* Database              :         MYSQL