Asian Journal of Applied Science and Technology (AJAST)
(Open Access Quarterly International Journal) Volume 2, Issue 2, Pages 835-839, April-June 2018

A Novel Approach to Disclose the Locations of IP Spoofers Using ICMP

V.S.Vidhya[1], S.Ragavi[2], R.Gayathri[3], R.Vinothini[4] and Mr.K.Selvaraj[5]

[1,2,3,4]*Student, Department of Information Technology, V.S.B Engineering College, Karur.*
[2]*Assistant Professor, Department of Information Technology, V.S.B Engineering College, Karur.*

Article Received: 01 March 2018 *Article Accepted: 09 April 2018* *Article Published: 28 April 2018*

ABSTRACT

There are many assaulters who are using forged source IP address to hide their real locations. To capture the assaulters, a number of traceback techniques have been introduced. Due to the challenges of implementation, there has been not a widely used IP traceback solution, at least at the Internet level. As a consequence, the mist on the locations of spoofers has never been dissolute till now. This paper offers passive IP traceback which neglects the implementation difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol error messages triggered by spoofing traffic, and tracks the spoofers based on public available information such as topology. In this way, PIT can find the attackers without any implementation needs. This project explains the processes and efficiency of passive IP traceback, and shows the captured locations of spoofers through the path backscatter data set. As because of some limitations PIT cannot work in all the spoofing attacks, it may be a helpful mechanism of tracing spoofers before an Internet-level traceback system has been deployed in real.

Keywords: Computer network management, computer network security, denial of service (DoS), IP traceback.

1. INTRODUCTION

Network security combines multiple layers of defenses at the edge and in the network. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats. Network security consists of the policies and practices adopted to prevent unauthorized access, misuse, modification or denial of a computer network and network accessible resources. This paper represents the reasons, accumulation, and the factual results on way backscatter, exhibits the procedures and adequacy of PIT, and demonstrates the caught areas of spoofers through applying PIT on the way backscatter information set. PIT can discover the spoofers with no arrangement necessity.

1.1. Background

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. 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.

1.2. Network management

Network management is the process of administering and managing computer networks. Various services provided by this discipline include fault analysis, performance management, provisioning of networks, maintaining the quality of service, and so on. Software that enables network administrators to perform their functions is called network management software.

1.3. Denial of service

A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests being fulfilled.

1.4. Computer network security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

1.5. IP traceback

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated.

2. EXISTING SYSTEM

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

2.1. Drawbacks of Existing System

1) The real locations of spoofers are not disclosed. 2) Attackers cannot be deterred from launching further attacks. 3) Due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level.

3. PROPOSED SYSTEM

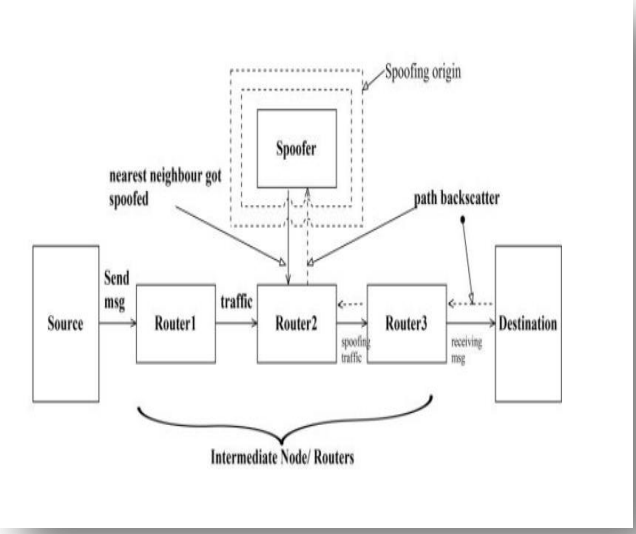
Instead of proposing another IP traceback mechanism with improved tracking capability, propose a novel solution, named Passive IP Traceback (PIT), to bypass the challenges in deployment. Routers may fail to forward an IP

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.

3.1. 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.

4. SYSTEM ARCHITECTURE



5. MODULE DESCRIPTION

1. Topology construction
2. Collection of path backscatter messages

3. Passive IP Traceback
4. Performance evaluation

5.1. 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). In our simulation, we are using router node and 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.

5.2. 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 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. 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

5.3. Passive IP Traceback

The Distributed Denial of Service (DDoS) attacks are launched synchronously from
multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP
traceback.

5.4. Performance evaluation

We make use of path information to help track the location of the spoofer. 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.

6. ALGORITHM

Loop-Free Assumption

1. no loop in the paths
2. G(V,E) V-Vertices E-Edges
3. This algorithm first finds a shortest path from r to od r-router, od-original destination

4. Checks if the removal of the vertex can break r and od
5. If such vertex is found ,it remove the vertex from G
6. The set containing all the verticals which are still connected with r is just the suspect set

7. CONCLUSION

In this article we have presented a new technique, backscatter analysis, for estimating denial-of-service attack activity in the Internet. Using this technique, we have observed widespread DoS attacks in the Internet, distributed among many different domains and ISPs. The size and length of the attacks we observe are heavy tailed, with a small number of long attacks constituting a significant fraction of the overall attack volume. Moreover, we see a surprising number of attacks directed at a few foreign countries, at home machines, and towards particular Internet services. We try to dissipate the mist on the actual locations of spoofers based on investigating the path backscatter messages. In this, 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 proved that, the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

REFERENCES

[1] Y. Bhavni, V.Janaki, R. Sridevi “IP Trackback through modified probabilistic packet marketing algorithm intense rapid assumption,” in Engineering Journal Volume 6,Issue 2, June 2015.

[2] K. Munivara prasad, A. Rama mohan reddy, V. Jyothsna “IP Trackback for flooding attacks on Internet Threat Monitors using Honeypot” remaining at the International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.

[3] W. Caelli, S. Raghavan, S. Bhaskar, and J. Georgiades, “Policy and law: denial of service threat,” in An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, pp. 41–114, Springer, 2011.