Finding Fake IP Address Attacker Over Network: IP Traceback

[1]Ravindra K V, [2]Prof. H L Shilpa
1PG Scholar (MCA), 2Assistant Professor,
Dept. of MCA, P.E.S.College Engineering, Mandya Karnataka, India

Abstract - 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. As a result, the source address in an IP packet can be falsified (IP address spoofing) allowing for denial-of-service attacks (DoS) or one-way attacks (where the response from the victim host is so well known that return packets need not be received to continue the attack). The problem of finding the source of a packet is called the IP traceback problem. IP traceback is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DoS attack detection. Such solutions require high numbers of packets to converge on the attack path.

Keywords: DoS, IP address spoofing, ISP, TTL, DNS, BWM, ASes, ICMP

I. INTRODUCTION

The goal of IP traceback is to trace the path of an IP packet to its origin. The most important usage of IP traceback is to deal with certain denial-of-service (DoS) attacks, where the source IP address is spoofed by attackers. Identifying the sources of attack packets is a significant step in making attackers accountable. In addition, figuring out the network path which the attack traffic follows can improve the efficacy of defense measures such as packet filtering as they can be applied further from the victim and closer to the source.

Most IP traceback approaches trace the spoofed traffic to the edge of region where traceback is deployed. Unfortunately, the non-cooperation nature of Internet Service Providers (ISPs) means IP traceback approaches are only be deployed in a domain controlled by the single ISP, and can only trace to the edge of this domain. IP traceback approach uses

1 Probabilistic packet marking
2 Deterministic packet marking
3 Router-based approach
4 Out-of-band approaches
5 Trace-back of active attack flows

Probabilistic packet marking: Probabilistic packet marking is a general technique which routers can use to reveal internal network information to end-hosts. Such information is probabilistically set by the routers in headers of regular IP packets on their way to destinations.

Deterministic packet marking: This describes a more realistic topology for the Internet – that is composed of LANs and ASes with a connective boundary – and attempt to put a single mark on inbound packets at the point of network ingress.

Router-based approach: Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. Packet forwarding is the transit of logically addressed network packets from one network interface to another.

Out-of-band approaches: Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only. It is used at console method which is a physical management port that provides out-of-band access to a device.

Trace-back of active attack flows: Trace-back of active attack flows. In this type of solution, an observer tracks an existing attack flow by examining incoming and outgoing ports on routers starting from the host under attack. Thus, such a solution requires having privileged access to routers along the attack path.

II. SYSTEM MODEL

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 mechanism in the routing system. Existing traceback mechanisms are either not widely supported by current commodity routers 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(Application service Element). Since the deployment of traceback mechanisms is not of clear gains but apparently high overhead, 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.

IP traceback techniques are designed to disclose the real origin of IP traffic or track the path. Complete model shows in fig 2.1. 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.

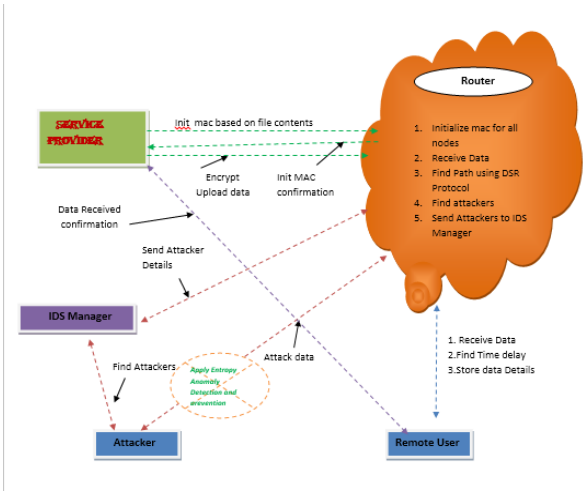

Fig. 2.1 Working process of IP spoofing

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

IV. PROPOSED METHODOLOGY

We propose a novel solution, named Fake IP Traceback, to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL(Time to Living) 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. Fake IP traceback 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. Fake IP traceback is especially useful for the victims in reflection based spoofing attacks, e.g., DNS(Domain Name System) amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic.

V. SIMULATION/EXPERIMENTAL RESULTS

The first step is topology design and bandwidth allocation, and it is concerned with the ability to dynamically reconfigure a network in order to efficiently benefit from network resources. The second step is concerned with flow control and congestion avoidance. Bandwidth management (BWM) protocols are used to prevent congestion, essentially by accepting or refusing a new-arrival cell. The third one, which is the most critical one, is bandwidth allocation, which is concerned with successful integration of link capacities through the different types of services. This case shows in the Fig 5.1 when data is not attack from attacker.

The activity selection problem is a combinatorial optimization problem concerning the selection of non-conflicting activities to perform within a given time frame, given a set of activities each marked by a start time (si) and finish time (fi). The problem is to select the maximum number of activities that can be performed by a single person or machine, assuming that a person can only work on a single activity at a time. When data packet has attacked form attacker this situation is shown in Fig 5.2.

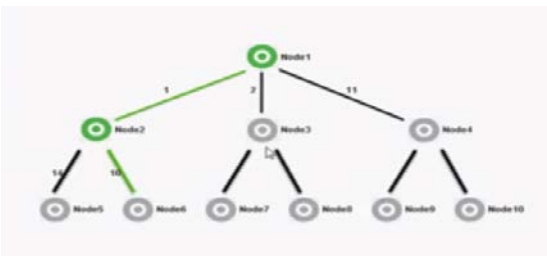

Fig 5.1 The case when data has been not attacked

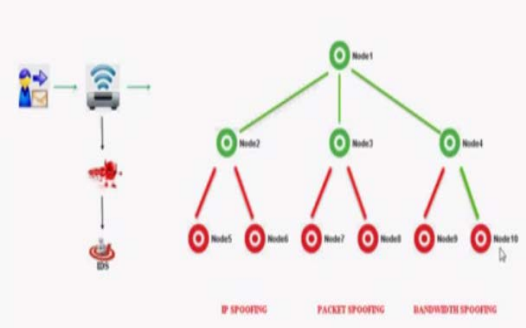

Fig 5.2 The case when data has been attacked

VI. CONCLUSION

We proposed Fake IP Traceback which tracks spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. When path backscatter occurs the traffic is loaded to sender asking to resend the missing packet, immediately ICMP error messages are overloaded to spoofer so automatically Bandwidth Management Protocol (BWM) applies and reroutes through new gateway avoiding spoofer node. We demonstrated the effectiveness of FIT based on deduction and simulation.

VII. FUTURE SCOPES

In future work we can extend this to include more optimize technique. Automatic traceback to speed up tracing and reduce human intervention. Integrating defensive measures with traceback so that on mechanism may perform tracing as well as detection.

REFERENCES

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

[2] ICANN Security and Stability Advisory Committee, “Distributed denial of service (DDOS) attacks,” SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006

[3] K. Park and H. Lee, “On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack,” in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.

[4] Mir, N.F. (2006) Computer and Communication Networks, Prentice Hall.

[5] X. Dimitropoulos et al., “AS relationships: Inference and validation,” ACM SIGCOMM Comput. Commun. Rev., vol. 37, no. 1, pp. 29–40, Jan. 2007.

[6] H. Burch and B. Cheswick, “Tracing anonymous packets to theirapproximate source,” in Proc. LISA, 2000, pp. 319–327.

[7] R. Stone, “CenterTrack: An IP overlay network for tracking DoS floods,” in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.

[8] A. Castelucio, A. Ziviani, and R. M. Salles, “An AS-level overlay network for IP traceback,” IEEE Netw., vol. 23, no. 1, pp. 36–41, Jan. 2009. [Online]. Available:

[9] M. R. Pearlman and Z. J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol, " IEEE Journal on Selected Areas in Communications: Wireless Ad-Hoc Networks, vol. 17, no. 8, p. 1395-1414, August 1999.

[10] Larry Peterson, Tom Anderson, David Culler, and Timothy Roscoe, "A Blueprint for Introducing Disruptive Technology into the Internet," HotNets-I, Oct 2002.