A Survey of Reactive IP Trace back Techniques

A.Mutharasi[1], Dr .D.J.Evanjaline[2]
[1, 2] Department of Computer Science
[1, 2] Rajah Sarfoji Government Arts of College. Thanjavur

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 IPaddress of a packet is not authenticated. It is long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP trace back 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 trace back 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.*

Keywords- IP Traceback; Spoofed IP address; DDoS Attack; Packet Marking; Logging; Hybrid

I. INTRODUCTION

Denial of Service (DoS) attack attempts to generate a huge amount of traffic to the victim and thereby disrupting the service or degrading the quality of service, by depleting the resources. Distributed Denial of Service (DDoS) attack is a distributed, co-operative and large-scale attack. Attackers can launch the attack traffic from various locations of Internet, exhausting bandwidth. The processing capacity or memory of the target machine or network is drained, taking advantage of the vulnerabilities and anonymous nature of Internet. Both these attacks have been posing a major threat to the Internet for over a decade. Now-a-days these attacks are turning to be more sophisticated. DDoS attack takes place from multiple attack path from numerous zombies controlled by an attacker. According to the recent survey of Arbor networks the impact of DDoS attack is increasing every year. Even the key players such as Microsoft,Yahoo,e-bay are counted in the list of DDoS victims. The packets sent will have spoofed IP addresses [1, 2, 3] which makes it practically difficult to identify the real location of attackers. Defending an attacker with spoofed IP address is more complex and this motivates the research on IP traceback,which is a methodology to trace the true origin of spoofed IP packets.

Traceback methods can be broadly categorized as preventive and reactive . Preventive methods take precautionary steps in preventing DoS attacks. A wide range of solutions has been proposed, however, this problem still remains as open one. The reactive methods solutions aim at identifying the source of the attacks. This is very important because attackers spoof their addresses, thus techniques are needed to trace back to the source to the source of the attack. In this paper the evaluation is based the above two categorized methods.

II. REACTIVE METHODS

The reactive methods solutions aim at identifying the source of the attacks. This is very important because attackers spoof their addresses, thus techniques are needed to trace back to the source to the source of the attack[2].

2.1 Link testing

This Testing starts from the router nearest to the victim and interactively tests its upstream links til they verify that one is utilized to carry the attacker's traffic[2]. Thus this procedure is perennial recursively on the upstream router til the source is reached. Most existing traceback techniques start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. Ideally, this procedure is repeated recursively on the upstream router until the source is reached. Below describe two varieties of link testing schemes, input debugging and controlled flooding. Input Debugging: Many routers include a feature called input debugging, which allows an operator to filter particular packets on some egress port and determine which ingress port they arrived on. This capability is used to implement a trace as follows. First, the victim must recognize that it is being attacked and develop an attack[1].

2.2 Logging

Logging is suggested to log packets at key routers and so use data-mining techniques to see the trail that the packets traversed. It has the valuable property that it will trace an attack long once the attack has completed. This system has drawbacks, and probably huge resource needs and large scale interprovider information integration tough[2]. This scheme

has the useful property that it can trace an attack long after the attack has completed. However, it also has obvious drawbacks, including potentially enormous resource requirements (possibly addressed by sampling) and a large scale interprovider database integration problem. We are unaware of any commercial organizations using a fully operational traceback approach based on logging[1].

2.3 ICMP traceback

Internet Control Message Protocol (ICMP) in would like of trace out full path of the attacks. Typically this scheme is for each router to come upwith an ICMP traceback message or reach directed to the identical destination because the elite packet[2]. The trace message itself consists of consequent and previous hop data and a time stamp. The principle idea in this schemes is for every router to sample with low probability (e.g.,1/20000) and generate an ICMP traceback message or iTrace directed to the same destination as the selected packet. The iTrace message itself consists of the next and previous hop information and a time stamp. In this paper [15], have argued that denial-of-service attacks motivate the development of improved traceback capabilities and have explored traceback algorithms based on packet marking in the network. We have shown that this class of algorithm, best embodied in edge sampling can enable efficient and robust multipart traceback that can be incrementally deployed and efficiently implemented[1].

2.4 Packet marking algorithm

During this scheme, every router within the count for forwarding a packet additionally inserts a mark within the packet[2]. This mark could be a distinctive symbol orthodox to the current specific router. As a result the victim will verify all the shift hops for every packet by observant the inserted marks. There are two variants of this marking scheme. Firstly, Deterministic Packet Marking (DPM) scheme in which each router marks all the packets passing through it with its unique identifier. Secondly, probabilistic packet marking (PPM), DoS attacks may be prevented if the spoofed source IP address is traced back to its origin that lets distribution penalties to the wrong party or isolating the compromised hosts and domains from the reminder of the network[1].

2.5 FDPM traceback

Flexible Deterministic Packet Marking (FDPM) is the enhanced form of DPM that provides more flexible features to trace the IP packets and might acquire higher tracing capabilities over on top of mentioned IP traceback methods[2]. In FDPM schemes, the Types of Services (ToS) fields will be used to store the mark under some circumferences. The two fields in the IP header are exploited, one is fragment ID and other is Reversed flag. An identifying value is assigned to the ID field by the sender to aid in assembling the fragments of a datagram. Given that less than 0.25% of all internet traffic is fragments [20], this field can be safely overloaded without causing serious compatibility problems. FDPM reconstruction process includes two steps: mark recognition and address recovery. Compared to DPM, the reconstruction process is simpler and more flexible. When each packet that is used to reconstruct the source IP address arrives at the victim, it is put into a cache, because in some cases the processing speed is lower than the arrival speed of the incoming packets.

2.6 Hash Based IP Traceback

Hash based approach is called as Source Path Isolation Engine (SPIE). In these methods the forwarding path of a single packet can be reconstructed by querying such routers soon after the packet is observed. More recent work (private communication) moves the processing from the router to a specialized machine observing traffic on a link. This method can be viewed as a special case of Remote Monitors. Attacks on SPIE: Attackers can attack the query/response communication, either the traffic or the endpoints. For that reason access to traceback data will normally be restricted to the administrative domain owning the routers and possibly a few other trusted places.

2.7 Algebraic Approach to IP Traceback

This scheme is based on algebraic techniques. This paper reframes the traceback problem as a polynomial reconstruction problem and uses techniques from algebraic coding theory to provide robust methods of transmission and reconstruction. This has the advantage of providing a scheme that offers more flexibility in design and more powerful techniques that can be used to filter out attacker generated noise and separate multiple paths.

III. EVALUATION OF IP TRACEBACK TECHNIQUES

This section evaluates a representative method in each of the category of IP Traceback techniques based on the following evalution metrics[3].

- Deployability
- Scalability
- Memory Requirement
- Router Processing Overhead
- Protection
- Paraeters needed for traceback

- Applicability on different types of attacks
- Prior knowledge of topology
- Accuracy
- Post Attack Analysis
- Attacker's Challenge Vs Scheme survival
- Router Involovement during traceback
- Number of bits overriden in IP header
- Number of Packets Required to Traceback

3.1 Deployability

Deployability stands for the requirement of hardware or software installation on ISPs either partially or completely. An ideal scheme must have ease of installation on ISPs, without making much change to the existing network infratructure. For e.g., additional hardware to all ISP's for implementation of a methodology will be overhead with respect to this metric. Except ITrace all other traceback schemes require a change in the existing infrastructure to enable IP traceback because packet marking and logging is not presently supported by any of the routers.

3.2 Scalability

Scalability relates to the amount of additional configuration required on other devices needed to add a single device to the scheme. It also measures the ability of the scheme to adapt to increasing network size. The features that depend on configuration on other devices deteriorate scalability.

3.3 Memory Requirement (Network/Victim)

An important metric of a traceback scheme is the amount of additional storage required either at the routers or at the dedicated traceback servers in the network, or at the victim. An ideal scheme should demand negligible or no additional storage on the network devices.

3.4 Router processing Overhead

Almost every traceback scheme requires processing at the routers. Processing overhead on routers is undesirable as it may result in degrading the performance of routers. Though processing occurs during traceback, it is expected to be relatively infrequent. An ideal scheme should have minimal or less processing overhead incurred on the network.

3.5 Reliability

A high level protection is preferred in any traceback scheme. Protection refers to the ability of a traceback scheme to produce reliable traces with a limited number of network elements that have been challenged. An ideal scheme should act as if a device is not part of the scheme when the device becomes subverted.

3.6 Parameters Needed for Traceback

With recent advanced techniques on IP traceback, it is an important criterion to evaluate techniques based on the required paramenters to inititate the traceback process. Attack consists of flooding of attack packets along with normal packets.

3.7 Applicability on Different Types of Attacks

This metric classifies the traceback technique based on the types of attack which it can handle. Attack could be classified into flooding based attacks and software exploit attack.

3.8 Prior Knowledge of Network Topology

A few schemes assume that they are aware of the topology in advance. In this changing environment one cannot always rely on a topology map. So this metric is used to analyse if the scheme requires prior knowledge about the topology.

3.9 Accuracy

Accuracy is the important metric which measures the precision of the scheme. False positive and False negative have to be less in an ideal traceback scheme. False positive is tracing a legitimate node as an attacker node. False negative is missing to identify the attacker node. So the traceback scheme must be able to trace most of the attackers.

3.10 Post Attack Analysis

A few traceback schemes are capable of tracing the attacker even after the attack is stopped whereas some schemes require the attack to be alive till the traceback is completed. A traceback scheme should be able to detect the attack whether it is alive or not because the attack duration cannot be predicted. This metric evaluates whether the traceback scheme supports post attack analysis or not.

3.11 Attacker's Challenge to the Scheme

This metric evaluates how well the proposed scheme sustains the attacker, if the attacker is well aware of the scheme. If the attacker is aware of the controlled flooding

scheme,attacker can very well generate the attack with the signature which matches the normal traffic flow and mislead the traceback scheme.

IV. CONCLUSION

This survey paper thus provides an overview of the evolution of existing reactive IP traceback schemes. The study shows that the focus on traceback scheme has moved from the quick traceback from the victim to the quick detection of attack before the victim is affected as most of the DDoS attacks take place from the stepping stones (compromised intermediate hosts). Traceback schemes using Watermarking technique, Information metrics like entropy, divergence and distance metric are gaining momentum and a brief study of these techniques will be provided in near future.

REFERENCES

[1] A.John , T Sivakumar," DDoS: Survey of Traceback Methods", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[2] K. Arun Kumar K. Sai Ashritha," Analysis of Various IP Traceback Techniques - A Survey, International Journal of Computer Applications (0975 – 8887), Volume 77– No.13, September 2013.

[3] Vijayalakshmi Murugesan, Mercy Shalinie, Nithya Neethimani," A Brief Survey of IP Traceback Methodologies", Acta Polytechnica Hungarica, Vol. 11, No. 9, 2014.

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

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

[6] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[7] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.

[8] R. P. Laufer et al., "Towards stateless single-packet IP traceback," in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160

[9] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A stateless traceback technique for identifying the origin of attacks from single packet," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–6.