International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 10 | Oct -2017 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON IP TRACEBACK TECHNIQUES

Deepthi S[1], Arun P S[2]

PG Scholar[1], Asst. Professor[2]
[1,2]Dept. of Computer Science & Engineering, Sree Buddha College of Engineering, Pattoor, Alappuzha

---

Abstract - *IP traceback is the way of determining the source of IP packet. It is an essential step not only for identifying but also for preventing the attackers. There are several methods are employed for IP traceback. .The IP traceback methods are classified as reactive and proactive. Reactive identifies the traceback information after that the attack has been occurred. Proactive identifies the traceback information when packets are traversed through the network. The methods such as link testing, packet marking, ICMP based traceback, packet logging and so on are used.*

Keywords: IP traceback, proactive, reactive, link testing, ICMP based traceback

1. INTRODUCTION

Attacks on the internet are growing day by day. So there may be chances of increase in crimes. The different types of attacks occurring on internet are IP spoofing, man in middle attack, DoS and DDoS and so on. The Denial of Service (DoS) causes delay on the internet. If the attacker uses a proxy server then normal internet service providers fails to determine the origin. Such types of sources can be traced using IP traceback.

IP traceback is an effective solution for identifying sources as well as the traversed path of these packets. Existing traceback solutions are required to solve the problem of DoS attacks. These types of solutions require many numbers of packets to reconstruct the attack path. The IP traceback can be determined using the techniques such as link testing, packet logging, and packet marking and so on.

2. LITERATURE REVIEW

In paper [1] different IP traceback techniques are used.

1) Link Testing (reactive)

Link testing can be used for determine the packet which carries the attackers traffic. The process starts from the router closest to the target. The procedure is repeated for testing the upstream links to determine which one is carries the traffic.

2) Logging (proactive)

In packet logging based IP traceback, the packet may need to log on each router as it traverses to reach the victim.

3) Packet marking (proactive)

The main idea of packet marking based IP traceback is to mark the packets with its identification information at each router which they pass.

4) ICMP Based traceback (proactive)

In ICMP trace back method, uses iTrace method, and each router selects one packet per 20,000 packets. Then it also generates an ICMP message. The ICMP message has the same destination IP address as the traced packet. The ICMP message also contains the IP header of the traced packet, and the IP addresses of the incoming interface and the outgoing interface of the current router. When the victim receives the sufficient ICMP message it can reconstruct the traversed path of packet.

In this paper [9] it uses a protocol independent DDoS defense scheme. It is based on the principle of smart filtering. The proposed system consists of tree modules. They are Attack Path Re-construction (APR), Filtering router Set Determination (FSD) and Scheduled Packet Filtering (SPF). APR is used to reconstruct attack graphs. It uses IP traceback technique (to check whether or not a network edge is on the path from an attacker). FSD runs on victim. It is used when determining the attack paths and set of routers that should install filters. SPF runs on filtering routers. It uses a self adaptive filter management for filter rewinding. This module mounts filters on the packet processing routine to block the specified packets flows is detected so as to avoid filtering legitimate flows.

Advantage

a) Improves throughput of legitimate traffic during a DDoS attack
b) Faster reconstruction and high accuracy
Disadvantage

a) Provides less security

In paper [6] proposes the RIHT scheme. In RIHT scheme it marks the packets with the interface numbers of router. The interface number is used to trace the traversed path of packets. Here the marking field on each packet is limited. Therefore hash table is used for packet marking scheme. The hash table stores the marking field of the packet and the index corresponding to the marking field is stored on the packet. This procedure is repeated until the packet reaches its destination. For obtaining traceback information

reverse of this process should take place. Thus determine the origin of the packet.

Advantage

a) Does not produce false positives
b) Fixed storage requirement
c) Without need to refresh the logged traceback information

Disadvantage

a) Packet fragmentation problem

In this [3] there are two marking schemes. Scheme 1 marks the packet with hash value of the IP address instead of the IP address itself. An 11 bit hash value is calculated to each IP address in the attack path. In this technique two independent hash functions are used. It is used for distinguishing the order of two routers in the XOR result. The marking scheme 2 uses different number of hash functions. The hash function used for marking is represented by a flag. This flag indicates that which hash function is used. If the ID of flag is known then the router simply calculates the hash function. Thus different FIDs indicated different independent hash functions. In authenticated marking scheme it uses cryptographic MAC computation per marking so that the victim can detect the compromised routers.

Advantages

a) Low network overhead
b) Provides efficient authentication of routers markings
c) Lower false positive rate
d) Computation overhead is small

Disadvantage

a) Network map is needed to reconstruct the attack path

Savage proposed [7] that "practical network support for IP traceback". It is based on two methods. A marking procedure executed by routers in the network and a path reconstruction procedure used by the victim. A router one or more packets by augmenting them with additional information about the path they are travelling. The victim attempts to reconstruct the attack path using only the information in the marked packets. The algorithms used for marking procedure are node append, node sampling, edge sampling.

Advantage

a) Efficient and robust
b) Multiparty traceback that can incrementally deployable
Disadvantage
a) Backward compatibility
b) Distributed attacks
c) Path validation
d) Approaches for determining the attack origin

CONCLUSIONS

IP traceback effectively identify the sources and traversed path of the packets. The various IP traceback techniques such as link testing, packet logging, packet marking, ICMP based traceback, packet filtering, RIHT and network support for IP traceback are described here. Among the techniques RIHT shows better performance. In future by reducing packet fragmentation problem the new traceback techniques need to be developed.

REFERENCES

[1] H. Aljifri, "IP traceback: a new denial-of-service deterrent?" IEEE Security and Privacy, vol. 1, no. 3, pp. 24–31, 2003.

[2] Q. Dong, S. Banerjee, M. Adler, and K. Hirata,Efficient probabilistic packet marking," in ICNP '05, 2005.

[3] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in INFOCOM '01, 2001, pp. 878–886.

[4] 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, 2009.

[5] M.-H. Yang and M.-C. Yang, "RIHT: A novel hybrid IP traceback scheme," IEEE Trans. on Information Forensics and Security, vol. 7, no. 2, pp. 789–797, 2012.

[6] L. Lu, M. C. Chan, and E.-C. Chang, "A general model of probabilistic packet marking for ip traceback," in ASIACCS '08, 2008, pp. 179–188.

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in SIGCOMM '00, 2000, pp. 295– 306.

[8] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in INFOCOM '01, 2001, pp. 878–886.

[9] Minho Sung and Jun Xu,"IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks", IEEE transactions on parallel and distributed systems, vol. 14, no. 9, september 2003

[10] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1310–1324, 2008.