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

OPPORTUNISTIC PIGGYBACK MARKING: A SURVEY

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

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

---

Abstract - *IP traceback is a solution for identifying the sources and traversed path of these packets. There are a number of techniques employed for determining the IP traceback. It is not only identifying the source but also for preventing the attackers. 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 technique such as packet filtering, Fast Internet Traceback, PPM, DPM and FDPM are described below.*

***Key Words*: IP Traceback, reactive, proactive, PPM, DPM**

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 trace back.

There are a number of techniques has been proposed for determining the traceback. The techniques such as packet marking, logging, link testing, ICMP, hash method and so on. The marking based traceback has received considerable attention. The main idea of MBT is that routers may send their traceback message to the victim by marking on passing packets. So that the victim can construct a graph of network paths traversed by these marked packets regardless of source IP address spoofing. It is know packet-level marking to be applied on all the time on all traffic flows is unnecessary and it suffers the scalability problem when the routers marking on by passing packets. In many proposed solutions, traceback mechanisms are activated in a reactive manner when any unusual traffic flow is detected.

1.1 OPPORTUNISTIC PIGGYBACK MARKING

In MBT method it assumes that the message fragments are only carried by the packets that belong to the flow being traced. Since a sequence numbers of packets are needed to convey a single traceback message to the destination. So it may take a long time for an end-host to collect all traceback messages from routers to reconstruct the network path of these packets. The situation that fragments buffered in individual routers can be delivered faster to the end-host without incurring extra message overhead. It is known as the opportunistic piggyback marking.

2. LITERATURE REVIEW

M Sung proposes [1] that "IP traceback based on intelligent packet filtering". It uses a protocol independent DDoS defense scheme. It works by performing smart filtering. There are three modules in the system. They are Attack Path Reconstruction (APR), Filtering router Set Determination (FSR) and Scheduled Packet Filtering (SPF). APR is used to reconstruct attack graphs. Also checks whether or not a network edge is on the path from an attacker. FSR runs on victim. It is used for determining the attack paths and set of routers that should install filters. SPF runs on filtering routers. It uses self adaptive filter management for filter rewinding. It mounts the filters packet processing routine to block the specified packets.

Advantage

a) Improves throughput of legitimate traffic flows during a DDoS attack

Disadvantage

a) Provides less security

This paper [9] based on probabilistic marking schemes. There are two methods. One is Packet marking scheme used by the routers. And second is Path reconstruction algorithms used by the victims. FIT uses both upstream maps and packet marking of that fragment. It contains three steps.

a) In FIT, the packet marked from the attack victim can be used to generate the upstream router map.

b) FIT allows the node to be sampled this method is more effectively reducing the number of false positives and it reconstruct the number of packets required for attack path.

c) In FIT, when the packet is marked it uses one bit in the IP id field to mark the distance from the target.

Advantages

a) Reduces false positive

b) Improves scalability

c) Shows better performance in legacy routers

Disadvantage

a) It is difficult to identify the packet if the number of attack packet is high

PPM [3] algorithm is used by the victim for reconstructing the traversed path of the attack packets. In this technique each router in attack path marks the packet with its partial IP address information. This information is called the marking information. This marking information is placed into the IP header of the packet with some fixed probability. After receiving the partial path information from the marked packets the victim reconstructs the attack path of these packets.

Advantages

a) Reduces the number of packets required almost two orders of magnitude

b) Used to convey any network information to destination end hosts.

c) The attack source to location can be done after the attack has stopped.

Disadvantage

a) False positive rate is high

b) If the attacker is aware of the scheme then traceback fails

c) The traceback process requires large number of packets.

This technique [6] was proposed to overcome the disadvantages of PPM. It focuses on the source of the attack packet. It does not depend on the traversed path of the attacker's packet to the target. When the packet arrives at the first source edge router is marked with the IP address of the router. The IP address can be divided into two fragments. Each fragment is randomly recorded into each ongoing packet. So the victim recovers the entire IP address when the victim obtains both the fragments of the same source router. During the packets pass through the network this mark stays not changed.

Advantages

a) Traceback process requires small number of packets

Disadvantages

a) Packet header size increases

b) It takes long time delay to identify the source

c) Scalability problem

d) Does not provide overload prevention

FDPM [1] uses various bits in the IP header. It is based on two methods. They are flexible mark strategy and flow based marking scheme. In flexible mark strategy the packet is marked. The mark has a flexible mark length. It depends on the network protocols used. When an IP packet enters the protected network it by the interface close to the source of the packet on an edge ingress router. The source IP address is stored in the marking field. When the packet traverses through the network the intermediate routers will not be overwritten the mark. In flow based marking scheme, the router selectively marks the packet depending on the flow of information. So it can reduce the packet marking load but still maintain the marking and traceback function .

Advantages

a) Reduce packet marking load

b) Does not consume any bandwidth

c) It marks in packets but does not increase their size

d) Overload prevention capability

Disadvantage

a) Maximum forward rate

b) Maximum marked rate

3. CONCLUSION

The paper describes the advantages and disadvantages of packet filtering, FIT, PPM, DPM, FDPM and OPM. From these analyses we can observe that Opportunistic piggyback marking shows better performance than other traceback techniques. In OPM we do not specify the available space for marking in IP header. For further improvement by avoiding the marking based traceback new traceback technique 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] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP

traceback," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, 2006.

[5] 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.

[6] 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.

[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.