An Hybrid IP Traceback Scheme Based on PMPL

Mrs. Sunchu K.S[#1], Dr. Deshmukh P.K.[*2], Prof. Dhainje P.B[#3]

[1] *ME Student, Computer Science and Engineering, Shriram Institute of Technology paniv, Maharashtra, India*
[2] *Principal, Computer Science and Engineering, Shriram Institute of Technology paniv, Maharashtra, India*
[3] *Vice Principal, Computer Science and Engineering, Shriram Institute of Technology paniv, Maharashtra, India*

---***---

Abstract - *Now days a use of internet is growing and it is used in almost every field such as business, industrial, educational systems, banking and military applications. But few applications required more security and some needs less security. Therefore various security problems are arises like Denial of service (Dos), Spoofing, different types of viruses etc, we need to overcome from all these attacks. This paper introduces various IP Traceback schemes :Path Reconstruction Based on PMPL(Packet Logging & Marking, Packet logging),IP Tracing using Hash Table, IP traceback with Deterministic Packet Marking, IP Tracing with 16-bit Marking Field, IP traceback using Huffman Codes. This paper presents merits and demerits of each technique in short.*

Key Words: Security, Hybrid IP traceback, Packet logging, Packet marking, DDos, Spoofing

I. INRODUCTION

As internet is used to complete almost every task. Due to the decreasing cost of Internet access and its increasing availability from a plethora of devices and applications. As Internet is used for different applications, attackers find a way to disturb the services provided by server. Hence, today's network security is often a compulsory need of Internet. In order to develop the businesses of companies, they needs IP Traceback techniques which will ultimately reduce the chances of losses [1]. The goal of IP traceback is to trace the path of an IP packet to its origin. The most important use 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.

There are different types of attacks which disturbs services of internet.

Spoofing: Spoofing is one type of attack, due to this attack the packet was sent by the node specified as the source address in its IP header is not always effective, so other techniques are required to tracing IP addresses for finding their original attacker. Hence effective IP Traceback schemes have to be used to find out the original source of attacks, in order to take any prevention or legal actions against the attackers [1].

Dos: Denial-of-Service (DoS) attack is example of attack deployed against the Internet. It is not easy to prevent from these kinds of attacks because well-crafted DoS attacks do not violate most of the security rules but they definitely cause damage to service provisioning. Inorder to prevent Internet against these kinds of attacks we have to implement defense techniques at necessary locations of the Internet.

Viruses: This is also one of the attacks which disturb services of internet.

IP Traceback Schemes:-

1. Path Reconstruction using packet logging and packet marking.

1.1 Packet Marking:

In this marking scheme, the router marks IP packets with its identification information.

There are basically two types of packet marking techniques are discussed as follows [2].

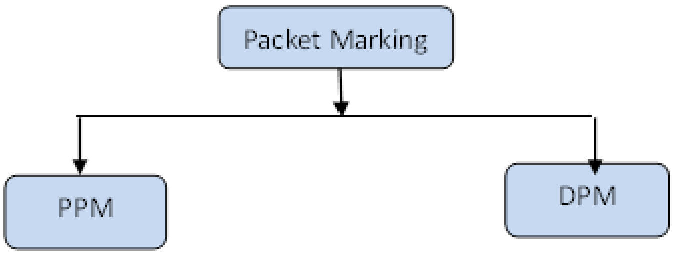

Fig -1: Types of Packet Marking Techniques.

Probabilistic Packet Marking (PPM):

In PPM, routers are treated as atomic units of traceback. We propose to treat interfaces as atomic units of traceback. In fact, the IP address of a router means the IP address of one of its interfaces. Making interfaces the units of traceback enables separation of incoming and outgoing packets with respect to a given interface. This will enable packets travelling in one direction to be treated differently from the packets traveling in another direction [4].

Security issues of PPM schemes arise from the fact that an attacker can inject a packet, which is marked with erroneous information. Such behavior is called mark spoofing. Prevention of such behavior is accomplished by special coding techniques, and is not 100% proof [4].

Deterministic Packet Marking (DPM):

In this marking technique a 32-bit IP address needs to be passed to the victim. From this a17bitsareavailableto pass this information, 16-bit ID field and 1-bit reserved flag. Deterministic nature of the algorithm ensures that once the ingress point has been identified for a particular source address, it will be correct 100% of the time. By design, DPM prevents mark spoofing [4].

2. Enhanced IP traceback using 16-bite marking field (E-RIHT):

This IP traceback scheme will help to detect the spoofing attacker by using packet PMPL scheme. In packet marking technique router marks identification information of its own into the forwarded packets. In packet logging, routers keep the digest information regarding the forwarded packets. Proposed scheme is termed as E-RIHT (Enhanced Routers Interface Hybrid Traceback) in this, memory requirement will be less because we are using marking field of 16-bit, which will also solve the packet fragmentation problem.

3. Marking with Huffman codes:

This is one of the new marking scheme in which router marks a packet with a link that the packet came through Links of router are represented by Huffman codes according to the traffic distribution among the links. If the packet runs out of space allotted for the marking field in the packet header, then the router stores the marking fields in the routers local memory along with the message digest of the packet. We identify the memory requirement of routers to store marking fields, compare the new technique with the other existing techniques, and address practical issues to deploy the new scheme in the internet. The new scheme marks every packet, therefore IP traceback can be accomplished with only a packet unlike in probabilistic markings and also it requires less amount of memory.

II. LITERATURE SURVEY

S.Prathyusha[1] *et al [2]* proposed a novel attack path reconstruction based on packet logging and marking techniques which gives improved accuracy, practicality and low storage and number of routers. For reconstructing the path of a packet and identify the source of the attack, the victim requires a map of the routers. The victim matches packet markings with the routers on the map and can thus reconstruct the attack path. Obtaining or constructing this map is not difficult. A many tools are available that can be used to obtain a map of the the routers and the Internet. If a router commits logging operation on an attack packet, examining digest tables at that router it not only confirm that router is in the attack path, but also find out its upstream router in the attack path.

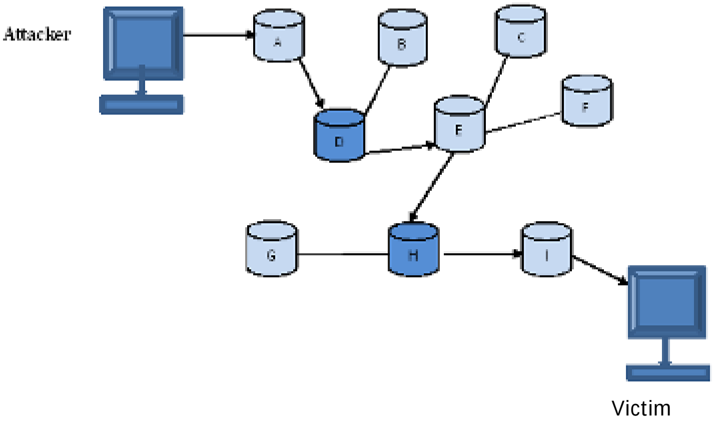

FIG -2: Attack path construction

Advantages: - Reduces the storage overhead and improves accuracy on the access time by a factor of the number of neighbor routers.

SSVR Kumar Addagarla et al [3] discussed a new marking scheme i.e. new hybrid IP traceback scheme with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction. In addition, we use a packet's marking field to censor attack traffic on its upstream routers. Lastly, we simulate and analyze our scheme, in comparison with other related research, in the following aspects: storage requirement, computation accuracy [3].

The entire work of this paper is divided into five different modules:

- Network topology Construction
- Path Selection
- Packet Sending
- Packet Marking and Logging
- Path Reconstruction

Advantages: efficient packet logging and has zero false positive and false negative rates in an attack-path reconstruction [3].

Andrey Belenky and Nirwan Ansari et al [4] propose a new approach i.e. IP Traceback With Deterministic Packet Marking which is essentially a packet marking algorithm, scalable and simple to implement, and introduces no bandwidth and practically no processing overhead. It is backward compatible with equipment which does not implement it [4].

This paper, discussed algorithm i.e. a packet marking algorithm.The16-bit Packet ID field and the reserved 1-bit Flag in the IP header will be used to mark packets. Each packet is marked when it enters the network. This mark remains unchanged for as long as the packet traverses the network [4].

Advantages: Deterministic nature of the algorithm ensures that once the ingress point has been identified for a particular source address, it will be correct 100% of the time. By design, DPM prevents mark spoofing [4].

Chaitanya Kumar Singh et.al [5] This paper is based on IP traceback, which will help to detect the spoofing attacker by using packet marking and packet logging technique In packet marking technique router marks identification information of its own into the forwarded packets. In packet logging, routers keep the digest information regarding the forwarded packets. Proposed scheme is termed as E-RIHT (Enhanced Routers Interface Hybrid Traceback) in this, memory requirement will be less because we are using marking field of 16-bit, which will also solves packet fragmentation problem [5] .This is based on both packet marking and packet logging technique. In E-RIHT, marking and logging of packets is done on the border router and core router. RIHT make use of 32-bit marking field while E-RIHT uses 16-bit marking and logging field in IP packet which solves the packet fragmentation problem. RIHT uses router degree for the calculation of marking value whereas E-RIHT makes use of router id for the calculation of marking value. If attack packet is received by the victim then it automatically discard the packet and send the path reconstruction request to upstream router. For path reconstruction, identification field issued and path towards the attacker is constructed. 16-bit hash table is used for logging the16-bit marking field. Information from the hash table can be retrieved very easily by using the marking field because of the index in the marking field. It is easy to search the particular information and trace back the path [5].

Advantages:- provide efficient IP traceback using single attack packet. E-RIHT make use of router id which is basically IP address of router, there are very less chances of having false traceback. 16-bit marking field is used, so packet fragmentation problem will be reduced and less storage overhead [5].

K.H. Choi and H.K. Daiatel [6] presents new marking scheme (with marking and traceback algorithms) in which a router marks a packet with a link that the packet came through. Links of a router are represented by Huffman codes according to the traffic distribution among the links. If the packet runs out of space allotted for the marking field in the packet header, then the router stores the marking field in the router's local memory along with a message digests of the packet. We analyze the memory requirement of routers to store marking fields, compare the new scheme with other existing techniques, and address practical issues to deploy the new scheme in the Internet. The new scheme marks every packet, therefore IP traceback can be accomplished with only a packet in probabilistic markings; also it requires far less amount of memory compared to logging methods and is robust in case of DDos [6].

III CONCLUSION

A literature survey is carried out on different IP traceback techniques. In this paper, we discussed the pros and cons of more important traceback techniques to highlight the deployment of a particular technique that suits to a particular context.

IV REFERENCES

[1] B. SaiPriyanka and N. SrihariRao ,"IP Traceback Techniques - A Selective Survey "International Journal of Computer Science and Mobile Applications, Vol.1 Issue. 3, September- 2013, pg. 40-44.

[2] S. Prathyusha, M. V. Sruthi and S. Anjani Prasad," A Novel Attack Path Reconstruction Based on Packet Logging & Marking Scheme" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013.

[3] SSVR Kumar Addagarla, Usha Nag S," A hybrid IP Trace Back Scheme Using Integrate Packet logging with hash

Table under Fixed Storage" International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 12, December- 2013, pg. 145-152.

[4] Andrey Belenky and Nirwan Ansari, Senior Member, "IP Traceback With Deterministic Packet Marking" IEEECOMMUNICATIONS LETTERS, VOL. 7, NO. 4, APRIL 2003.

[5] Chaitanya Kumar Singh,SrinivasKoppu, V Madhu Viswanatham, "E-RIHT: Enhanced Hybrid IP Traceback Scheme with 16-bit marking field " ISSN : 0975-4024Vol 5 No 3 Jun-Jul 2013.

[6] K. H. Choi and H. K. Dai," A Marking Scheme Using Huffman Codes for IP Traceback" Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04).