www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 12 Dec 2015, Page No. 15132-15135

A Survey on Different IP Traceback Techniques for finding The Location of Spoofers

Amruta Kokate, Prof.Pramod Patil

Nutan Maharashtra Institute of Engg. And Technology,Talegoan,Pune
Kokate.amruta@gmail.com
Nutan Maharashtra Institute of Engg. And Technology,Talegoan,Pune
pramodkumarpatil@gmail.com

Abstract: The problem of finding DDoS (Distributed Denial of Service)Attack is one of the threats in the Internet security field. To get the spoofers, a number of IP traceback mechanisms have been proposed. As their attack root is often hidden The problem lies in distinguishing the attack traffic from the normal traffic. Different techniques are used to get and identify the origin of DDoS attack with the help of IP Traceback . The most famous techniques in finding the attack source is the IP traceback . Many kinds of traceback techniques are their with each having its own pros and cons. This paper contain and evaluates some of the existing and recently evolving IP traceback techniques with respect to their advantages and disadvantages.

Keywords: Survey; Review; IP Traceback; Spoofed IP address; DDoS Attack; Packet Marking; Logging; Hybrid

1 Introduction

DDoS attacks can be launched in two forms,namely, direct attacks and reflector attacks . In the Direct attack, the the spoofed packets are floods by attacker to the victim via zombie machines. Direct attack is also classified into Network-layer DDoS attack (e.g. Ping flood, TCP layer attacks, Routing attacks, ICMP flood etc.) and Application-layer attacks (e.g. HTTP flood, HTTPS flood, FTP flood, etc.). The Reflector attack involves sending spoofed request packets to a large number of machines (known as reflectors) that will send reply packets to the requested source. The spoofed request packet will hold the source address of the targeted victim and so the replies from all the reflector machines will flood the source, targetting the victim. ICMP Echo Request attacks commonly known as Smurf attack is a well-known reflector attack.

IP Traceback is one such reactive technique. IP Traceback is used to find the origins and attacking paths of attackers traffic. In IP traceback is not limited only to DDoS attack. The function of IP Traceback is to identifying a source of any packet on the Internet. The task of identifying the original source of a packet is complex as the source IP address can be forged or spoofed. IP traceback techniques neither prevent nor stop the attack, they are used only to identify the source of the packets. Different IP traceback techniques are proposed only to mitigate DoS/DDoS attacks. A survey on existing IP Traceback schemes is already done and evaluated , which has not included the recent developments. This paper focuses on a detailed discussion on various traceback schemes ranging from the traditional Link testing to the newly emerged Hybrid schemes and analyze them with additional evaluation metrics.

2 Classification of IP Traceback Schemes

The intent of IP Traceback mechanism is to locate the source of the packet. As the source IP address of the packet is often forged or spoofed, IP traceback mechanism is inevitable. Traditional traceback mechanisms like Link Testing which includes Input Debugging and Control Flooding [1], have emerged a decade ago and recent techniques that are either combination of or completely different from the traditional ones are discussed here. IP Traceback schemes can be applied in two ways [7] – Intra AS and Inter AS. Intra AS Technique involves traceback within the network and Inter AS technique involves traceback across various networks. The different

types of IP Traceback Schemes and the description of each scheme is given below.

2.1 Link Testing

The overview of link testing starts from the victim and traces till the attack source via upstream links with the assumption that the attack remains active until the completion of the trace. This scheme, therefore, will not be suitable to identify the attack that occurs intermittently or when the attacker is aware of the traceback scheme used. In Input Debugging technique, the victim has to recognize that it is being attacked and has to develop an attack pattern (called attack signature) and check that with each of the incoming packets in the upstream routers and identify the corresponding upstream router and proceed further till the attacker. The most significant problem of this method is the management overhead, the co-ordination from the network admin. If the admin is unavailable or if he lacks the skill to assist the traceback, then the traceback may be slow or its completion could be impossible.

Link Testing which is also known as Hop by Hop Tracing uses an automated Pushback mechanism and it is currently supported by many router manufacturers. This uses statistical and pattern based analysis at the router closer to the victim to identify the upstream router from which the traffic has been forwarded and is repeated until the origin is reached. The statistics suggests the presence of attack and the pattern is used to distinguish the normal packets from the illegitimate attack packets.

2.2 Packet Marking

One of the common and significant techniques of IP Traceback is packet marking. The marking utilizes the rarely used fields of IP header, to store the audit trail where the field size used for marking varies from scheme to scheme. The dawn of packet marking era began with Node append, Node sampling, Edge sampling [1] marking methods etc. Each method emerged with the purpose to overcome the difficulties faced by the other. Packet marking mechanism is broadly classified into Probabilistic Packet Marking and Deterministic Packet Marking.

2.2.1 Probabilistic Packet Marking

Probabilistic Packet Marking method [1] . In this method, each router marks the packet with some probability say p for example p = 1/100 which implies marking one packet for every 100 packets received. The marking field uses 16 bits identification field in the header, of which 5 bits are used for marking hop count, which would be a useful information during reconstruction of attack path, and the remaining bits are used by the router to send its information. If the information is too large, then it is broken into fragments and marked in multiple packets. The marked packets will therefore contain only partial information of the path. This reduces the storage overhead in the packets.

The victim has to receive enough number of packets to re-construct the path. This scheme does not require prior knowledge of the topology. The disadvantage of this scheme is that it produces many false positives and the mark field value written by routers far away from victim might be overwritten by the routers closer to the victim and if the attacker is aware of the scheme, then the traceback fails The main idea of this approach is that each router fragments its message into several words (pieces) and calculates checksum for the whole message named as ‘cord’. The mark value consists of checksum cord and message fragment and an index of the message fragment. The index and checksum are used to identify the message fragment during reconstruction. The total number of bits used for packet marking in this paper is 25. Reconstructing large messages requires more packets. Increasing checksum size increases security, but when the checksum bits are increased, message bits are decreased. Hence reconstruction will be time consuming. The drawback of requirement of large number of packets to traceback an attacker using PPM is addressed with minimum number of packets

Deterministic Packet Marking scheme (DPM) was first proposed to overcome the disadvantages of PPM. Every packet passing through the first ingress edge router is only marked with the IP

address of the router. The IP address is divided into two fragments (16 bits each) and each fragment is randomly recorded into each inflowing packet. The entire IP address is recovered by the victim when the victim obtains both the fragments of the same ingress router. This scheme fails when the source address is spoofed and is also false positive. The enhanced schemes are proposed where the IP address is split into more fragments, and a hash function is used to contain the identity of the ingress router to decrease the false positive. Deterministic packet marking based on redundant decomposition is proposed . The knowledge of topology plays a significant role in DPM scheme's traceback. Consider the DPM scheme suggested where, it is assumed that the topology of the network is known in advance. The packet marking method involves hash of ingress router's IP address. The hash value is split into chunks and each chunk is marked into the packet randomly. With the topology known, the victim performs traceback of the marked routers. Large numbers of packets are not required for traceback in this scheme but it consumes a longer search time to identify the origin. The traceback scheme is challenged, if the topology is modified. When an intermediate router goes off, the traceback can be carried out with the topology but might turn to be false positive. If the attacker modifies the mark field, this scheme will fail to traceback. Instead of IP address respective bit fields were marked .

2.3 ICMP Traceback

A traceback scheme utilizing the explicitly generated ICMP Traceback message was proposed . This field can be null authentication, random strings or even HMACs. TTL is set to 255 for computing distance at the receiving end. During DDoS flooding attack, these ICMP traceback messages are used by the victim to reconstruct the path taken by the attacker. The schematic representation of the scheme . The updated version of the previous iTrace (ICMP Traceback) scheme was proposed . iTrace scheme is considered as an industry standard by IETF. The time taken for path reconstruction by iTrace is minimized in ICMP Traceback with cumulative path (iTrace CP) . This scheme is independent of the attack length. This scheme encodes the entire attack path information (i.e. contains the addresses of all the routers on the attack path) into minimal number of packets, thus minimizing the attack path construction time. This is achieved at the expense of minimal additional overhead in computation, storage and bandwidth.

Logging scheme for IP traceback stores the information like packet's digest, signature, and fields of IP header on all or few routers which forward packets within the domain. When an attack is detected, the victim requests the upstream router to gather information about attack packet. If the information is found, then the router is counted as a hop in the attack path and the process is repeated. The major challenges faced by this scheme is the overhead on the network and the storage requirement at core routers etc. Hash based IP traceback can trace even a single IP packet provided, the copy of the packet, its destination and approximate time of the packet's reception at the victim are available Another scheme for IP traceback with single packet . The disadvantage of false positive errors in traceback due to Bloom Filter is reduced . ID based Bloom Filter (IDBF) is used which requires ID table at every traceback enabled node. During Logging phase, ID table stores the node information (Node ID, Forwarder Address) in positions obtained on applying k hash functions to the payload. During Query phase, the most occurring value of Node ID is retrieved and reverted for traceback. MultipleIDBFs are used on nodes nearer to the sink with high traffic load to avoid false positive errors closer to sink. This, in turn, consumes a lot of memory. The idea of packet logging is combined The idea of hybrid scheme combining marking and logging has been conceived to overcome the disadvantage of individual marking and logging schemes as stated above and a drastic improvement in traceback has been achieved. In, two hybrid schemes of IP traceback are proposed – Distributed Linked List Traceback (DLLT) and Probabilistic Pipeline Packet Marking (PPPM).

3 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.

Controlled flooding is choosen as the representative method of Link Testing, PPM is chosen as a representative method of Probablisitic Packet Marking and FDPM is chosen under Deterministic Packet Marking, ITrace represents ICMP based traceback technique, SPIE is choosen as the representative method of Packet Logging and RIHT represents Hybrid Traceback scheme

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 infrastructure. For e.g., additional hardware to all ISP's for implementation of a methodology will be overhead with respect to this metric.

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. An ideal scheme should be scalable and configuration of the devices should be totally independent of each other.

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. ITrace and marking schemes does not require any storage at the routers whereas logging and hybrid scheme needs logging at the intermediate routers in the attack path. Using SPIE, a core router with 32 OC-192 links requires 23.4 GB and RIHT requires a fixed storage of 320 KB according to CAIDA dataset .

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. Since Link testing involves every router intraceback process,it requires high computation at the routers in the attack path,FDPM and PPM require processing at the routers but it is relatively lesser compared to the logging based SPIE which involves every router and its neighbours in the computation. RIHT involves only the routers in the attack path with minimal arithematic computation.

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.

9.Conclusion

Security is a vital component of every network design. When planning, developing and deploying a network one should understand the importance of a strong security

policy. A security policy defines what people can and can't do with network components and resources. There are different types of attack on internet, passive attack, active attack, Distributed Attack, Insider Attack, Phishing Attack, spoofing attack etc. All these attack have their own characteristics and hence the tester should be very vigilant about the attacker. Even though IDS and firewall are very successful method that ensures network security it does not produce better results in certain cases. Through this paper we can analyze different techniques through which to detect ma-in-the-middle attack and spoofing attack. A comparison of the four methods is made based on complexity and efficiency.

References

[1] S. Savage, D. Wetherall, A. R. Karlin, T. E. Anderson: Network Support for IP Traceback, IEEE/ACM Transactions on Networking, Vol. 9, No. 3, 2001, pp. 226-237

[2]Yaar, A. Perrig, and D. Song: FIT: Fast Internet Traceback, Proc. IEEE INFOCOM, 2005, pp. 1395-1406

[3] D. Moore, C. Shannon, D. Brown, G. Voelker, S. Savage: Inferring Internet Denial-of-Service Activity, ACM Transactions on Computer Systems, Vol. 42, No. 2, 2006, pp.115-139

[4] Hakem Beitollahi, Geert Deconinck: Analyzing Well-known Countermeasures against Distributed Denial of Service Attacks, Computer Comm., Vol. 35, 2012, pp. 1312-1332

[5] R. Stone: Centertrack: An IP Overlay Network for Tracking DoS Floods, Proceedings of the 9th

conference on USENIX Security Symposium, Berkeley, USA, 2000, pp. 199-212

[6] H. Burch, B. Cheswick: Tracing Anonymous Packets to Their Approximate Source, Proceedings of the 14th USENIX Conference on System Administration, New Orleans, LA, USA, 2000, pp. 319-328

[7] J. Ioannidis and S. M. Bellovin: Implementing Pushback: Router
Router-based defense against DDoS attacks, in Proc. Network and Distributed System Security Symp., 2002