Network attack path Identification and packet filtering with traceback mechanism

Sneha S. Rana, Dr. B.B.Meshram
VJTI, Computer Department, Mumbai

Abstract-
Majority of the network host today are threatened by the network attacks like Denial-of-service(DoS) attack, Distributed DoS(DDoS) attack. The path identification scheme described in this paper can trace back an individual packet back to its source. The routers along the path of the packet mark the packet based on deterministic marking scheme with effective storage requirement by using hash based technique. The attack diagnosis is done at the victim's side and the filtering of the packet is done at the routers near to the source

Index terms- computer attacks, network level security and protection, DoS attack.

INTRODUCTION-

Distributed Denial of Service(DoS), it is an attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

Defending against the DoS attack is very difficult mainly because the attack is done through large number of zombies and the traffic volume sent by single attack might be small but the aggregate traffic volume is huge which is difficult to prevent.

The schemes proposed in [2] [3], requires that when attacks are detecteddownstream close to the victim, the upstream routers closeto the attack sources filter attack packets using summarizedattack signatures sent by the detection module. Theseschemes, however, have either or both of the following twodrawbacks: The first drawback is the need to securelyforward attack signatures to the upstream routers. The second drawback is the dependence on attack signatures to separate attack traffic from legitimate traffic. Using such a signature is very difficult for three reasons. First, in many cases, an attack detection module can only detect the existence of attacks but may not formulate any attack signatures from the observed traffic

The scheme discussed in this paper combines the concept of packet marking and pushback mechanism to defend against the DDoS attack. It first isolates the attacker and then filters all the traffic sent by that attacker. An intrusion detection system(IDS) installed at the victim host detect the attack, the upstream routers are then asked by the victim to start marking the packets with traceback information. Based on those information the victim then separates the attacker from other legitimate users and thereafter trace back to the attack source using the path information obtained by the upstream routers.

I. PACKET MARKING

The basic idea of IP traceback approach based on packet marking is that the router marks packets with its identification information as they pass through that router. The mark overloads a rarely used field in IP packet header, i.e., 16-bit IP identification field. The identification of a router could be32-bit IP address, hash value of IP address, or uniquely assigned number. In the last two cases, the length of identification information is variable and could be less than16 bits. Since the marking space in packet header is too small to record the entire path, routers mark packets with some probability so that each marked packet carries the information of one node in the path. In addition, based on the lengthof router identification and the implementation of marking procedure, the router may only write part of its identificationinformation into the marking space. While each marked packet represents only a small portion of the path it has traversed, the whole network path can be reconstructed by combining a modest number of such packets. This kind of approach isreferred to as probabilistic packet marking (PPM). ThePPM approach does not incur any storage overhead at routersand the
marking procedure (a write and checksum update) canbe easily and efficiently executed at current routers. But due toits probabilistic nature, it can only trace the traffic that consistsof a large volume of packets.

In the PPM a packet stores the information of an edge in the IP header. The pseudocode of the procedure is given below for reference. The router determines how the packet can be processed depending on the random number generated. If x is smaller than the predefined marking probability pm, the router chooses to start encoding an edge. The router sets the start field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field.

```
For each packet w
Let x be a random number from [0..1)
If x <$p_m$ then
Write R into w.node
```

Figure 1: the packet marking algorithm

Below, diagram shows packet marking scheme for the proposed scheme, where the 16 bit identification field is divided into hop count field and Port Identifier(PID) field of the router's interface marked by the routers who mark the packet.

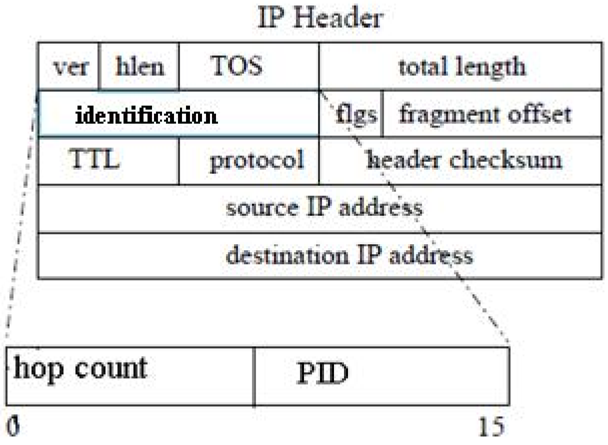

Figure 2: Packet marking in identification field

II. Understanding network topology

To understand the attack diagnosis we first make several assumptions. First, is that every host in the internet is connected to the local edge router, these routers are in turn connected to the core routers. Also we assume that every route from the attacker to the victim follows a constant path, i.e. the router's routing table is hardly updated, and the internet routers are not compromised.Terms like false positive means that the legitimate user's packet which was detected and false negative means that the attacker's packet which went undetected.

The above figure shows the upstream tree for victim V. As observed some of the interface at routers is labeled with unique identifier known as port identifier(PID). This PID is locally unique, in the sense that two interface of same router will have different PID's but two interface of different router can have same PID's.

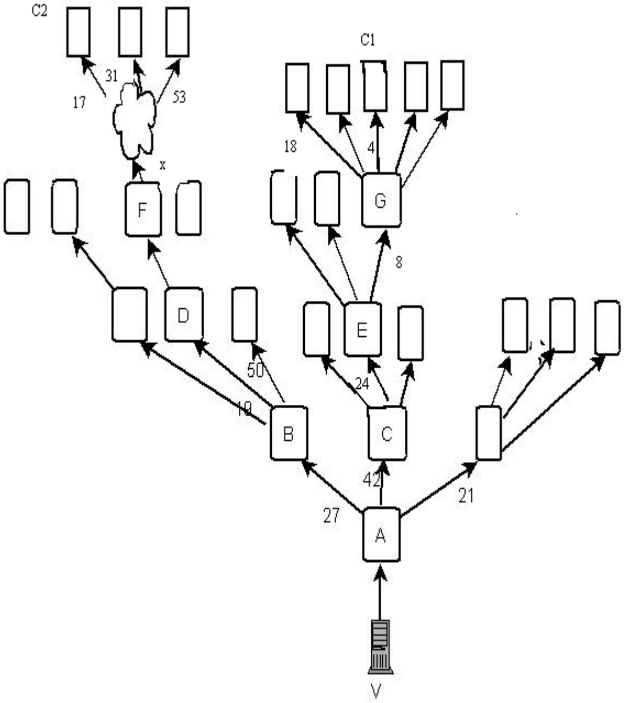

Figure 3: A victim V with its upstream tree

This shows that the PID can be used to uniquely identify the routers or the host that the router connects to. However, there are situations when the interface of the router is connected to multiple hosts via broadcast link channel. As seen in the figure the interface *x* of router F is connected to multiple hosts through a LAN. In such cases the router F maintains a virtual PID table which maps each virtual interface to a MAC address of the hosts connected to it. For example, In the figure the C2's MAC address is map to virtual PID 17.

Since, the PID is unique within a router a string of PID's can be used to identify a path in the network. Like for example, the string 4-8-24-42 uniquely identify the path from C1 to V. the Attack Diagnosis starts from the interface 42 and moves up in the path and the router close to the attacker, say if its C1 perform the filtering process.

III. Attack scrutiny

To scrutinize the attack, the routers need to mark its PID and other traceback information in the IP packet which it forwards. This information is embedded in the 16 bit Identification field and the one bit reserved flag bit of the IP packet. Most of the existing packet marking algorithms overloads this field because of its least contribution in the network traffic. This scheme record two values the hop count, the PID. The hop count field gives the number of hops from the router that first marks the packet to the edge router that is immediately upstream to the victim V. the PID field of the given packet records the PID of the interface port of the router that process the packet.

Two different markings can be done at the router interface. First, in active marking mode the router who process every packets destined for V does the following: 1) Set the hop count field to 0, 2) Records its PID in the PID field of the packet. Whereas in passive marking mode the router performs the following for every packets destined for V 1) Increase the hop count by 1.

Whenever, the victim detects an attack through the IDS installed at the victim's machine, the victim will send the Interface Scrutiny (IS) request to the immediate edge router. This request packet will have the TTL set to 255, so that the edge router can identify that the request has come from the host just one hop away. From the figure, the path C1-G-E-C-A is chosen as the attack path, from the attacker C1. The analysis process is done as follows

1. Upon receipt of the IS request from the victim V the edge router A will send back the response to V to notify that it has begun marking the packets. It set itself to the active marking mode. Hence, now every packet arriving at V will be marked with the hop count field as 0 and the PID field is marked with the PID value of the A's interface that process the packet. In case the IDS at victim identifiy the attack then the edge router should be able to identify the interface which processed the attack packet.

2. When the victim V identifies that the attack traffic is coming through the interface with PID 42 of the edge router A then it sends the scrutiny request for interface 42 to the router A. Router A then set the interface with PID 42 to passive marking mode and later it sends the IS request to router connected to the interface 42, i.e., router C in our example. Also, the TTL value of this request packet should be set to 255.

3. Now, router C performs the same steps as the one done by router A when it received the IS request from the victim V. it also sends the notification back to the victim V. And marks the PID field of the packets with the PID value of the C's interface that process the packet and the hop count field is set to 1 for every packet processed by C, so that the V can identify that the packets are being marked by C. Using this information, now V is able to identify the interface of C which is processing the attack packet which is interface 24 in our example.

4. After identifying the interface of C which is processing the attack packets, the victim V sends the scrutiny request to C for interface 24. C then sets that interface into passive marking mode and its sends the IS request to the router connected to the interface 24 i.e., router E in our example

5. The above procedure is repeated for every router and every identified interface processing the attack packet until the final scrutiny request is send to router G for interface 4. Now, since this interface is connected to the host the router G then will start the filtering process and will filter out the packets sent from the host connected to interface. If this interface is connected to multiple hosts via broadcast link channelthen the router will block all the hosts connected to that interface.

IV. Conclusion

Hence, we have successfully deployed the attack scrutiny module at the victim's end and the filtering module near the attack source's end. However, the presented scheme only works for the DoS attack which comes from the single attack source, this scheme can be further extended to block the parallel attacks in case of DDoS attack. Also, the packet marking process is done only after the victim identifies the attack; hence there is no need to mark every packet coming to the victim even when there is no attack being done on the victim.

References

[1] B. Al-Duwairi and T.E. Daniels, " *Topology based packet marking*", Proc. IEEE Int'l Conf. Computer Comm. and Networks (ICCCN), pp. 146-151, Oct. 2004.

[2] S. Chen and Q. Song, "*Perimeter-Based Defense against High Bandwidth DDoS Attacks,*" IEEE Trans. Parallel and Distributed Systems, vol. 16, no. 6, pp. 526-537, June 2005.

[3] John Haggerty, Qi Shi, MadjidMerabti, "*Early Detection and Prevention of Denial-of-ServiceAttacks: A Novel Mechanism With Propagated Traced-Back Attack Blocking*", IEEE Journal, vol. 23, no. 10, October 2005

[4] Vrizlynn L. L. Thing, Morris Sloman, NarankerDulay, "*Locating Network Domain Entry and Exit point/path for DDoS Attack Traffic*", IEEE Trans. On Network and Service Management, Vol. 6, No. 3, September 2009.

[5] Guang Jin and Jiangang Yang, "*Deterministic Packet Marking based on Redundant Decomposition for IP Traceback*", IEEE Comm. letters, Vol. 10, No. 3, March 2006.