International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey on IP Traceback Mechanisms

Aparna C Bhadran[1], Maria Joy[2]

[1]M.Tech, KMEA, Computer Science and Engineering, Mahatma Gandhi University, Kerala, India

[2]Assistant Professor, KMEA, Computer Science and Engineering, Mahatma Gandhi University, Kerala, India

Abstract: ***Security is used to protect the vital information by allowing those who have the right to access and denying the access to those who don't have right. IP spoofing is one of the network attacks. The attackers will launch an attack by forging the source address. So they will be able to enhance the attacking without exposing their real location. The attacker's uses fake source IP address to hide their actual places. To find the attackers so many IP traceback mechanisms have been proposed in this paper.***

Keywords: Ingress Filtering, Link testing, Logging, ICMP traceback ,Packet Marking

1. Introduction

IP Spoofing is a major security problem on Internet. In IP Spoofing the attackers will launch an attack by forging their source IP address. These addresses can be either an already allotted address or those addresses that are not allotted at all. By IP Spoofing the attackers can conceal their real location so thereby increase the outcome of attacking.

There are various notorious attacks that rely on IP Spoofing including SYN Flooding, DNS amplification etc.

SYN Flooding is commonly used in denial of service attack. The attackers need only a few resources to launch the attack and it is difficult to trace the source address. The attackers send the succession of the SYN request to the target system to consume resources of the server to make the system unresponsive to the legal users.

DNS amplification attack is a popular distributed denial of service. The attackers use openly accessible DNS server to overflow a target system with DNS response traffic. The attacker sends a DNS name lookup request to an open DNS server with the source address of the attackers as target"s address. The response of the DNS is sent to the target address.

It is of great importance to obtain the origin of IP spoofing traffic. If the real location of the IP Spoofers are not known then they cannot be prevented from initiating further attacks.

Obtaining the origin of IP Spoofers on Internet is difficult. The study of identifying the source of IP Spoofers are known as IP traceback. There are two challenges to construct IP Traceback system on the Internet:

1) The Cost to adopt traceback mechanism on routing system is high. The existing traceback mechanisms are not supported by current routers and will introduce a considerable overhead to the routers.

2) It is difficult to make the different Internet Service Provider (ISP) to work together. The attackers can be in every corner of the world so a single ISP to deploy its own traceback mechanism is pointless.

2. Literature Survey

The Traceback mechanism can be generally divided into two preventive and reactive methods. The preventive method uses defensive steps to prevent DoS attack. The reactive method aims to find the source of the attacker.

2.1 Ingress Filtering

Ingress Filtering is a preventive method .One way to overcome the problem of an unknown attacker is by illuminating the capacity to forge source address. The routers should be designed in such a way that it should block all the packets that arrives with illegal source address [1]. This requires the router with adequate power to inspect the source address of every packet and adequate knowledge to distinguish between genuine and illegal address.

Ingress filtering is most practicable in that network where the address ownership is explicit and traffic load is low like in customer network or at the border of Internet Service Provider (ISP).

Ingress Filtering restricts the routing of traffic that starts from a downstream network to recognized and advertised prefixes. The router must drop the packets whose source address does not fit to one of the advertised networks.
Disadvantages:

1) The efficiency depends upon widespread, if not universal deployment.

2)Even if ingress filtering were universally deployed at the customer to ISP level, the attackers can still forge address from 100 or 1000 hosts within the legal customer network.

In figure 1 the router R1 drops those packets that are coming from subnet spoofed source address to the victim. The spoofed source address must exist in the 10.0.0.0/16 prefix. But the IP address of neighbor address can be used as the sources address of attack packet.

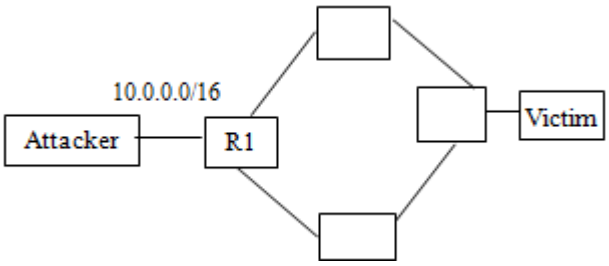

Figure 1: Ingress Filtering

2.2 Link Testing

Link Testing works by testing network links between routers to decide the source of attacker‟s traffic. The technique starts from the router nearby to the victim and interactively test its upstream link to decide which one carries the attacker‟s traffic. This procedure is repeated recursively until it reaches traffic source as in figure 2.

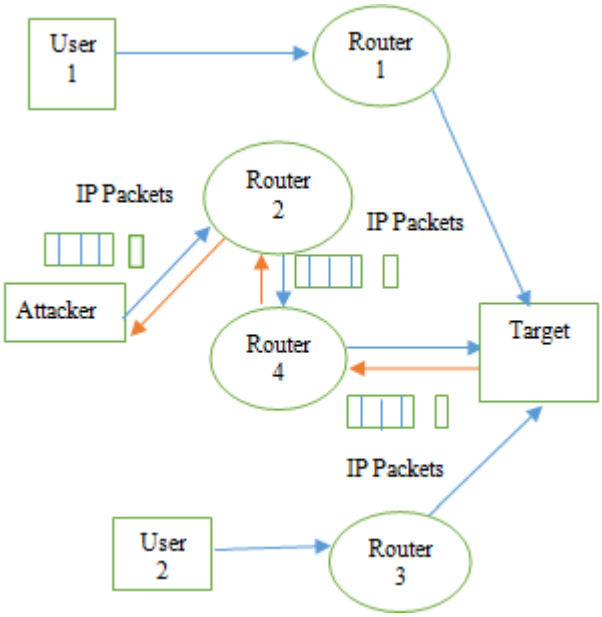

Figure 2: Link Testing

Link testing can be done in 2 methods:
1) Input debugging
2) Controlled Flooding

2.2.1 Input debugging

In input debugging [2] if the router recognizes the attack signature (attacking traffic‟s specific characteristics) then it is possible to decide the arriving network link on the router. The ISP must then apply the same procedures to the upstream router joined to the network link and so on, until the attacker is identified or the trace leaves present ISP‟s boundary. If the process leaves the present ISP then the administrator must contact the upstream ISP to carry on the tracing processes.

Link testing method can be performed manually or using any automated tools that are developed by ISP to trace attackers at their own network.

Advantages:
1) Well-suited with existing protocol.
2) Irrelevant network traffic overhead.
3) Supports incremental application.
4) Well-matched with existing routers and network infrastructure.

Disadvantage:
1) Considerable management overhead in communication and organizing efforts across multiple network boundaries and ISP.
2) Needs time and personnel on both the victim‟s and ISP side.
3) For successful trace, the attack should last until the tracing is over.
4) Less appropriate for distributed DoS.

2.2.2 Controlled Flooding

Controlled Flooding [3] works by creating a burst of network traffic from the victim‟s network to the incoming network segment and sees how this purposefully made flood affects the attack traffic‟s intensity. It uses a map which is a known internet topology around the victim [2]. These floods are targeted specifically at certain hosts that are coming from the victim‟s network. There will be changes in attack traffic‟s frequency and intensity so the victim can deduce the incoming network link on the upstream router. This process is repeated one level above on the router.

The controlled flooding technique is a kind of DoS attack which can disturb the genuine traffic on the unsuspicious upstream router and network. This will make it inappropriate for extensive routine usage on the Internet.

Advantages:
1) Well-suited with existing protocol.
2) Supports incremental application.
3) Well-matched with existing routers and network infrastructure.

Disadvantages:
1) Controlled Flooding works efficiently only if there is an accurate map of the network topology.
2) For successful trace, the attack should last until the tracing is over.
3) ISP cooperation is required

2.3 Logging

Logging method works by storing the packets at the important routers all over the internet and uses data mining methods to extract the information about the source of the attackers as in figure 3. This method allows accurate analysis of attack traffic. It needs high processing and storage overhead to store the packets. It also has the legal and statistical problem to store and share the information among different ISP.

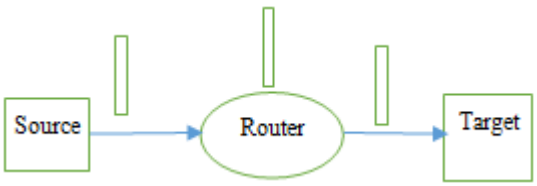

Figure 3: Logging

Alex Snoeren and colleagues [4] proposed Source Path Isolation Engine (SPIE).Here the entire packets will not be stored in the router instead hash digest of the appropriate invariant portion is stored in an efficient memory structure called Bloom Filter. To extract significant packet data a network of data collection and analysis agent covering the different network can be used and then suitable attack graphs can be produced so that the attacker‟s source can be identified.

Tatsuya Baba and Shigeyuki Matsuda [5] proposed a different method for logging. This method consists of 1)an overlay network that is built of sensors to detect possible attackers,2) tracers (tracing agents) that can store packets on request and 3)managing agents that can coordinate the tracer‟s and sensors and can communicate with each other. It stores only certain features that are required. It supports high speed and less storage.

Logging method uses sliding time window for storing data in the router. So it can avoid excessive storage and analysis requirement.

Advantages:
1) Well-suited with existing protocol.
2) Irrelevant network traffic overhead.
3) Supports incremental application.
4) Well-matched with existing routers and network infrastructure.
5) Allows tracing even if attacks are stopped.
6) Can trace even a single packet.

Disadvantages:
1) Resources are required for processing and storage.
2) There is legal and logistics issues for sharing information among different ISP.
3) Less appropriate for Distributed DoS.

2.4 ICMP Traceback

The ICMP traceback method works by iTrace.In iTrace method, the victim receives router generated messages in addition to information from the regular traffic as shown in figure 4. The router generated messages contain information that shows the source of the packet, the time the packet was sent and the authentication of the packet. The network manager will combine all the information to trace the path to its source. To limit the extra traffic, the router will generate ICMP traceback message for only one in 20,000 packets passing through that router. This method limits the extra traffic on the network.

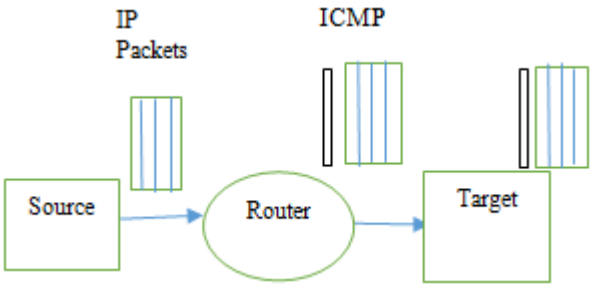

Figure 4: ICMP Traceback

The enhancement of iTrace method is intension-driven ICMP traceback [6]. This method separates the messaging function between decision module and iTrace generation module. Based on the information that is stored in the routing table the decision module will decide which type of packet can be used in the next iTrace generation module. Based on this decision the decision module will set a special bit in packet forwarding table. This special bit indicates that the immediate packet corresponding to the particular forwarding entry will be selected to generate iTrace message. The iTrace generation module then process this selected packet and sends a new iTrace message.

Advantages:
1) Well-suited with existing protocol.
2) Supports incremental application.
3) Well-matched with existing routers and network.
4) Allows tracing even if an attack is stopped.
5) ISP coordination‟s are not required.

Disadvantages:
1) Creates additional network traffic.
2) The attackers can use false ICMP traceback message into the packet stream to hide the attacker‟s original source.
3) The organizations are filtering the ICMP traffic due to attack scenarios.

2.5 Packet Marking

Each router in the network puts a mark in the packet in addition to the packet forwarding as shown in figure 5. This mark is a unique identifier representing the router. So by observing the mark, the victim can find out all the internal hops for each packet.

There are 2 variants for packet marking:
1) Deterministic Packet marking (DPM)
2) Probabilistic Packet marking (PPM)

In DPM [7] each router marks all the packets passing through the router with a unique identifier. So the reconstruction of attack pattern at the victim is easy. But the routers are having additional overhead. If an attacker is controlling a trusted router then it can make any path up to that router unless an authentication mechanism is used. If authentication methods are added then it will add cost in terms of both processing time and space. Some of the packets will not be overwritten by the routers. So the attacker will write fake information knowing that these packets will confuse the victim. This method does not work for DoS because it needs large amount of packets to converge. In PPM [8] DoS attack can be avoided if spoofed source IP address is traced back to its origin which allows assigning penalties to the wrong parties or separating the wrong host or network from the rest of the network.

Advantages:
1) Can be installed incrementally.
2) Low cost
3) Effective against Distributed DoS.
4) Does not require ISP cooperation.
5) Allows tracing even if the attack is stopped.

Disadvantages:
1) Needs change in the protocol.
2) Produce paths which are not attacking paths.
3) Victims receive a minimum number of packets.
4) Does not handle fragmentation.

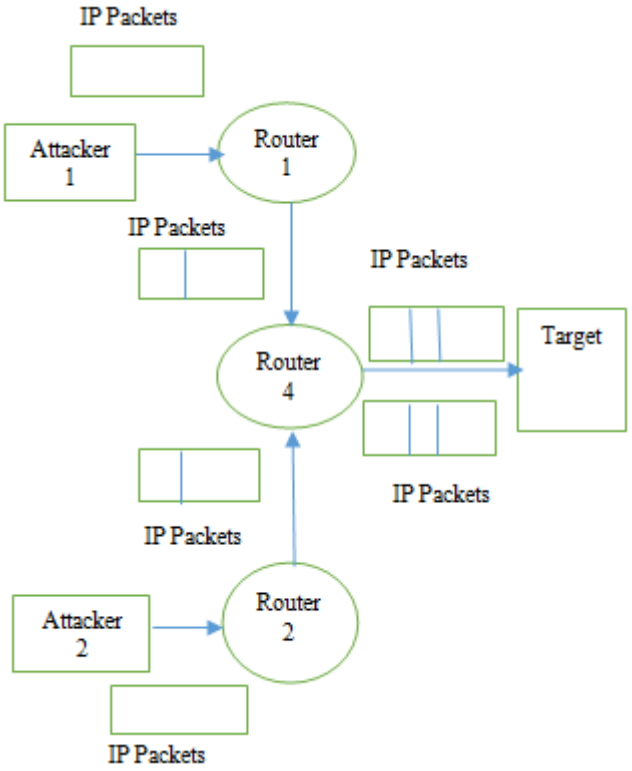

Figure 5: Packet Marking

3. Comparison Study

Table 1 shows the comparison study of various existing systems.

Table 1: Comparison Study

Categories	IF	LTID	LTCF	L	IT	PM
Implementation	Fair	Easy	Fair	Fair	Easy	Easy
Router Overhead	Moderate	Large	High	Large	High	Large
Network Topology	Low	Low	High	Low	Low	Low
Network Overhead	Low	Low	High	Low	Low	Low

IF-Input Filtering
LTID-Link Testing Input Debugging
LTCF-Link Testing Controlled Flooding
L-Logging
IT-ICMP Traceback
PM-Packet Marking

4. Conclusion

In this paper various IP traceback mechanisms are discussed. Thiese IP traceback mechanism comes under either preventive or reactive methods. Each method has its own merits and demerits. The main difficulty is in deployment. So to overcome the deployment problems Passive IP Traceback (PIT) mechanism is proposed.

References

[1] E Ferguson and D. Senie, "Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing,", RFC 2827, 2000R.
[2] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," Proc. 9th Usenix Security Symp.,Usenix Assoc., 2000, pp. 199–212.
[3] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. 2000 USENIX LISA Conf., Dec. 2000, pp. 319-327
[4] A.C. Snoeren et al., "Single-Packet IP Traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, 2002, pp.721–734. IP Packets
[5] T. Baba and S. Matsuda, "Tracing Network Attacks to Their Sources," IEEE Internet Computing, vol. 6, no. 3,2002, pp. 20–26.
[6] A. Mankin et al., "On Design and Evaluation of „Intention-Driven" ICMP Traceback," Proc. IEEE Int'l Conf.Computer Comm. and Networks, IEEE CS Press, 2001. pp.159–165.30 IEEE
[7] Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters,vol. 7, no. 4, pp. 162-164, 2003.
[8] M. Adler, "Trade-Offs in Probabilistic Packet Marking for IP Traceback," J. ACM, vol. 52, no. 2,pp. 217-244, 2005.

Author Profile

Aparna C Bhadran received the Bachelor of Technology degree in Computer Science and Engineering from Sree Narayana Guru Institute of Science and Technology in 2014 and currently doing Master of Technology in Computer Science and Engineering from KMEA Engineering College, Edathala.

Maria Joy received the Bachelor of Technology degree in Computer Science and Engineering from Toc H Institute of Science and Technology, Arakkunnam in 2008 and Master of Technology in Computer Science and Engineering (Specialization in Data Security) in 2011.She is currently working as Assistant professor in Computer Science Department, KMEA Engineering College, Edathala.