International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Industrial Automation And Computing (ICIAC-12th &13th April 2014)

RESEARCH ARTICLE OPEN ACCESS

IP Traceback Approaches for Detecting Origin of DDoS Cyber Attackers

Mrs. Swati G. Kale *, Mr. Vijendrasinh P. Thakur **,
Mrs. Nisha Wankhade***, Ms.V.Nagpurkar****

*(Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India
Email: s12_kale@yahoo.com)
**(Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India
Email: vijendrapthakur@gmail.com @gmail.com)
***(Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India
Email: nisha.wankhade@gmail.com)
****(Department of Computer Science & Engineering, St. Francis Institute of Technology, Mumbai, India
Email: nvarsha11@gmail.com)

ABSTRACT
Investigating the sources of a denial of service (DoS) and distributed denial of services (DDoS) attack is hardest in the Internet security area, Cyber-attackers often use incorrect source IP addresses in attack packets (spoofed IP packets) to achieve anonymity, reduce the risk of trace-back and avoid detection.. IP traceback system identifies the origin of IP packets when the source address of these packets is spoofed. In this traceback Routers, ISP's play an important role to trace real origin of DDoS Attackers. Our aim is on evaluate & analyze most promising traceback approach for detecting origin of attackers.
Keywords **–** DoS, DDoS - Distributed denial-of-service attacks, IP Address Spoofing, IP Traceback

I. INTRODUCTION

The contents of each section may be provided to understand easily about the paper. Today, the Internet is an essential part of our everyday life and many important and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the Internet. According to recent sources the number of hosts connected to the internet has increased to almost 400 million and there are currently more than 1 billion users of the Internet. Thus, any disruption in the operation of the Internet can be very inconvenient for most of us. As the Internet was originally designed for openness and scalability without much concern for security, malicious users can exploit the design weaknesses of the internet to wreak havoc in its operation. Incidents of disruptive activities like e-mail viruses, computer worms and denial-of service attacks have been on the rise In the distributed form of DoS attacks (called DDoS), the attacker takes control of a large number of vulnerable hosts on the internet, and then uses them to simultaneously send a huge flood of packets to the victim, exhausting all of its resources. There are a large number of exploitable machines on the internet, which have weak security measures, for attackers to launch DDoS attacks, so that such attacks can be executed by an attacker with limited resources against the large, sophisticated sites. The attackers in DDoS attacks always modify the source addresses in the attack packets to hide their identity, and making it difficult to distinguish such packets from those sent by legitimate users. This idea, called IP address spoofing has been used in major DDoS attacks in the recent past, including the attacks on e-commerce.

In this paper we will briefly explain different types of DDoS attacks in section II. In section III we present the existing Traceback Approaches to detect the origin of attacker with their description.

II. TYPES OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

1] ICMP Flood Attacks

ICMP is based on the IP protocol that can diagnose the status of the network. An ICMP flood attack is a bandwidth attack that uses ICMP packets that can be directed to an individual machine or to an entire network. When a packet is sent from a machine to an IP broadcast address in the local network, all machines in the network receive the packet. When a packet is sent from a machine to the IP broadcast address outside the local network, the packet is delivered to all machines in the target network. Other types of ICMP flood attack are the SMURF [5] and the Ping-of-Death [9] attacks.

2] Smurf Attack

One type of DDoS attack is called amplification attack in which the attack traffic actually is amplified in magnitude by compromised intermediary systems before it impacts the victim computer. Smurf is an example of amplification DDoS attack.

A Smurf attack uses a combination of IP spoofing and ICMP to saturate a target network with traffic. The network configuration used in an actual Smurf attack is shown in Fig.1. In smurf based DDoS attack, a large amount of ICMP echo messages i.e. Ping messages are sent to broadcast addresses, and where the Ping messages contain the spoofed source address of the victim computer. Each host of the broadcast domain receives an ICMP echo message, and responds to it by sending ICMP echo reply. Hence for n ICMP echo request messages sent to a broadcast domain, n*m ICMP echo reply messages are sent out of the broadcast domain towards the victim computer where m is the number of hosts in the broadcast domain. In effect, the broadcast domain helps amplify the DDoS attack traffic moving towards a victim computer. If more than one broadcast domains are involved then such DDoS attack traffic can be amplified even further and the victim computer is flooded with ICMP echo reply messages resulting in bandwidth exhaustion and also the resource exhaustion of the victim computer [7].

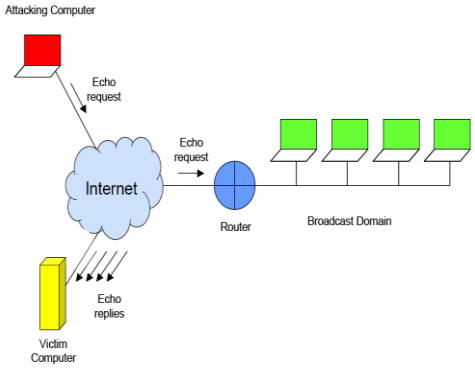

Fig. 1 Architecture of A SMURF Attack

3] Buffer Overflow Attack

A basic buffer overflow attack occurs when a process receives much more data than expected. If the process has no programmed routine to deal with this excessive amount of data, it acts in an unexpected way that the intruder can exploit. Several types of buffer overflow attacks exist, with the most common being the "Ping of Death"[9] (large packet Ping attack) or the use of over 256-character user or file names in email. A large packet Ping attack involves the use of the Internet Control Message Protocol (ICMP) Packet Internet Groper (PING) utility. The intruder sends a "ping" that consists of an illegally modified and very large IP datagram, thus overfilling the system buffers and causing the system to reboot or hang.

In this case, a malformed ping packet flood is sent to the target. Since the TCP stack responds only to a certain type of ping packet, it fails to respond to this, exhausting the system resources.

A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 32 bytes in size (or 84 bytes when the Internet Protocol [IP] header is considered); historically, many computer systems could not handle a ping packet larger than the maximum IPv4 packet size, which is 65,535 bytes. Sending a ping of this size could crash the target computer.

Generally, sending a 65,536-byte ping packet would violate the Internet Protocol as written in [RFC 791], but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.

4] TCP SYN Flood Attack.

A SYN attack occurs when an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when a target system replies to those requests. This causes the target system to "time out" while waiting for the proper response, which makes the system crash or become unusable.

TCP SYN attack makes half-open TCP connection to make the victim wait a certain time after sending SYN/ACK to the attacker.

5] UDP Flood Attack

In case of UDP flood attack, an attacker sends UDP packets to random ports of a victim and then a victim makes a decision that there are no specific applications. After this procedure, a victim sends an ICMP destination unreachable message to the attacker.

III. TRACEBACK

The most common approach in order to effectively defend against a DDoS attack is to try to identify the sources of this attack. This is a very difficult task due to the reasons we have mentioned in the introduction but not impossible. The fact that the source IP address is not a reliable source of information, made the researchers to explore different ways to identify the true sources of an incoming attack.

In the case of DDoS attack, it is more difficult to prevent than DoS attack because there are several distributed attackers. Moreover, it is very difficult to find a real origin of attackers because DoS/DDoS attacker uses spoofed IP addresses.

Once an attack is identified, the immediate response is to identify the attack source and block its

traffic accordingly. There are many approaches that target in tracing and identifying the real attack source. IP traceback traces the attacks back towards their origin, so one can find out the true identity of the attacker and, achieve path characterization. Some factors that render IP traceback difficult is the stateless nature of Internet routing and the lack of source accountability in TCP/IP protocol.

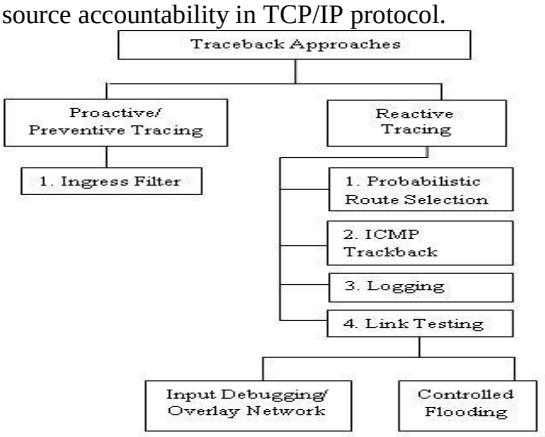

Fig. 2 Classification of IP Traceback Approaches

There are two basic approaches of tracing the real origin of attackers as shown in fig.2. As name indicates in proactive or preventive tracing is implemented before the attack. The focus is on prevention. But reactive tracing focuses on detecting mechanism after the attack. i.e. Reactive actions are made for the detecting the origin of attacker.

A. PROACTIVE/PREVENTIVE TRACING

1. Ingress Filter

In ingress filtering [10], the router checks if an incoming packet in its ingress interface is valid for that interface. The validity of the packet is decided based on the information that the router has about the possible IP ranges that the incoming packets can have as source IP address.[12]

Because routers (or IP level switches) can know which IP addresses originate with which network interface, it is possible for them to identify packets that should not have been received by a particular interface. For example, a border router or gateway will know whether addresses are internal to the network or external. If the router receives IP packets with external IP addresses on an internal interface, or it receives IP packets with an internal IP address on an external interface, the packet source is most likely spoofed.

In the wake of recent denial-of-service attacks involving spoofed attack packets, ISPs and other network operators have been urged to filter packets using the above-described method. Filtering inbound packets, known as ingress filtering, protects the organization from outside attacks. Similarly, filtering outbound packets prevents internal computers from being involved in spoofing attacks. Such filtering is known as egress filtering. It is interesting to note that if all routers were configured to use ingress and/or egress filtering, attacks would be limited to those staged within an organization or require an attacker to subvert a router.

A number of IP addresses are reserved by the IANA for special purposes [RFC5736][RFC6890]. These are listed in table 1. The addresses in the first group are private addresses and should not be routed beyond a local network. Seeing these on an outside interface may indicate spoofed packets. Depending on the particular site, seeing these on an internal address would also be suspicious. The other addresses in table 1 are special purpose, local only addresses and should never be seen on an outer interface.

Many firewalls look for the packets described in this section. Typically they are dropped when received. Because firewalls have been a popular security product, research into routing methods has been active. Most all research has been in this area.

TABLE 1: Special IP Addresses

Private Networks (RFC 1918) --
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
Special / IANA Reserved --
0.0.0.0/8 - Historical Broadcast
127.0.0.0/8 - Loopback
169.254.0.0/16 -LinkLocal Networks
192.0.2.0/24 - TEST-NET
240.0.0.0/5 - Class E Reserved
248.0.0.0/5 - Unallocated
255.255.255.255/32 – Broadcast

One limitation of routing methods is that they are effective only when packets pass through them. An attacker on the same subnet as the target could still spoof packets. When the attacker is on the same Ethernet subnet as the target, both the source IP address and the Ethernet MAC would be spoofed. If the spoofed source address was an external address, the MAC would be that of the router. This implies that other techniques are required.

B. REACTIVE TRACING

1. Probabilistic Route Selection Algorithm

Yim [15] proposed the Probabilistic route selection algorithm to find real origin of DoS/DDos attack.

The requirements of this scheme are:

1. The link status on attack paths will be changed when attacks occur.
2. The inter-arrival time of Internet traffic can be represent as a cumulative exponential distribution.
3. The intermediate router records the number of the incoming packets and outgoing packets traverses each network interface card and calculates the cumulative Poisson packet forwarding probability all the time during running router. After then, a variance of the cumulative Poisson packet forwarding

probability of n seconds period is stored in probabilistic packet forwarding table.
4. Probabilistic packet forwarding table has to be stored in the router.
5. IDS detects a DDoS attack and notify to the victim that DDoS attack occurs.
The probabilistic route selection method is to choose a route one hop by one hop to find attacker's real origin.
Packets and there formats used probabilistic route selection algorithm.
In this method uses three packets an alert packet, an agent packet and a reply agent packet.
Alert packet:-This packet is use to notify to the victim that the DDoS attack occurs.
Agent packet:-This packet is used to find attackers' real origin.
Reply agent packet:-This packet is used to notify to the victim that the agent packet reached the edge router of the attacker.
Fig. 3 shows the example of probabilistic route selection traceback algorithm procedure. An arrow indicates the attack path. A short dotted arrow indicates the path of the alert packet to notify to victim that the DDoS attack occurs. A long dotted arrow indicates the path of the agent packet to find attacker's real origin and a curved dotted arrow indicates the path of the reply agent packet.
After attacks occur, IDS detects the DDoS attack. After then, IDS sends the alert packet to the victim. The victim received the alert packet generates an agent packet to find a real origin of attacker and sends it to the victim's edge router. The source IP address of the agent packet is the IP address of the victim and the destination IP address is NULL value because we do not know the real IP address of the attacker.

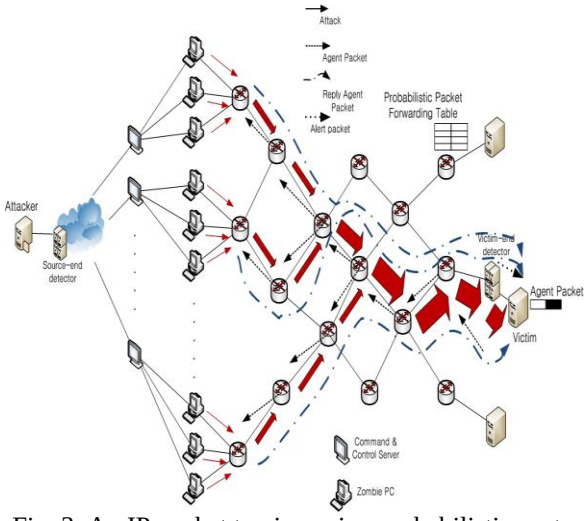

Fig. 3. An IP packet tracing using probabilistic route selection algorithm

The victim's edge router received the agent packet refers to its probabilistic packet forwarding table to forward this packet to next hop router. In this procedure, the edge router checks a variance of cumulative Poisson packet forwarding probability of the row of the interface number, which the agent packet comes into, in the probabilistic packet forwarding table. After this, the edge router chooses the column that has the highest variance of the cumulative Poisson packet forwarding probability to forward this agent packet to next hop router. And then, the edge router forwards this agent packet to next hop router through that interface, which has the column's number, by probabilistic route selection algorithm not by the destination IP address. This column's number is the outgoing interface of the agent packet. The intermediate router that receives the agent packet performs the same procedure. The agent packet finally reaches the attacker's edge router so we can find the origins of attackers refer to this network traffic variation and the probabilistic packet forwarding table as mentioned above.
If the variance of selected row, which the agent packet comes into, has the highest value of its column, this column's number is also selected as an outgoing interface of the agent packet. In other words, several interfaces can be selected as an outgoing interface of the agent packet. In this case, the router copies the agent packet and forwards the agent packet through several interfaces simultaneously.
The attacker's edge router, which receives the agent packet, generates the reply agent packet to send it to the victim. The victim sends the agent packet periodically based on packet round trip time until receiving the reply agent packet.
2. ICMP traceback
ICMP traceback has been proposed by Bellovin [16]. According to this mechanism every router samples the forwarding packets with a low probability and sends an ICMP traceback message to the destination. If enough traceback messages are gathered at the victim, the source of traffic can be found by constructing a chain of traceback messages.
The principle idea in this scheme is for every router to sample, with low probability (e.g., 1/20 000), one of the packets it is forwarding and copy the contents into a special ICMP Traceback message including information about the adjacent routers along the path to the destination. During a flooding-style attack, the victim host can then use these messages to reconstruct a path back to the attacker. This scheme has many benefits compared to previous work and is in many ways similar to the packet marking approach we have taken. However, there are several disadvantages in the current design that complicate its use. Among these: ICMP traffic is increasingly differentiated and may itself be filtered in a network under attack; the ICMP Traceback message relies on an input debugging capability (i.e., the ability to

associate a packet with the input port and/or MAC address on which it arrived) that is not available in some router architectures; if only some of the routers participate it seems difficult to positively "connect" traceback messages from participating routers separated by a nonparticipating router; and finally, it requires a key distribution infrastructure to deal with the problem of attackers sending false ICMP Traceback messages. That said, we believe that the scheme is promising and that hybrid approaches combining it with some of the algorithms we propose are likely to be quite effective[14][16].

3. Logging

An approach suggested to log packets at key routers and then use data mining techniques to determine the path that the packets traversed. This scheme has the useful property that it can trace an attack long after the attack has completed.

However, it also has obvious drawbacks, including potentially enormous resource requirements (possibly addressed by sampling) and a large scale interprovider database integration problem. We are unaware of any commercial organizations using a fully operational traceback approach based on logging [14].

4. Link Testing

i. Input Debugging/ Overlay Network

Several ISPs have developed tools to automatically trace attacks across their own networks. One such system, called CenterTrack, provides an improvement over hop-by-hop backtracking by dynamically rerouting all of the victim's traffic to flow through a centralized tracking router [17] by Stone. Once this reroute is complete, a network operator can then use input debugging at the tracking router to investigate where the attack enters the ISP network.

ii. Controlled Flooding

Burch and Cheswick have developed a link-testing traceback technique that does not require any support from network operators [18]. We call this technique controlled flooding because it tests links by flooding them with large bursts of traffic and observing how this perturbs traffic from the attacker. Using a pregenerated "map" of Internet topology, the victim coerces selected hosts along the upstream route into iteratively flooding each incoming link on the router closest to the victim. Since router buffers are shared, packets traveling across the loaded link including any sent by the attacker have an increased probability of being dropped. By observing changes in the rate of packets received from the attacker, the victim can therefore infer which link they arrived from. As with other link testing schemes, the basic procedure is then applied recursively on the next upstream router until the source is reached.

While the scheme is both ingenious and pragmatic, it has several drawbacks and limitations. Most problematic among these is that controlled flooding is itself a denial-of-service attack exploiting vulnerabilities in unsuspecting hosts to achieve its ends. This drawback alone makes it unsuitable for routine use. Also, controlled flooding requires the victim to have a good topological map of large sections of the Internet in addition to an associated list of "willing" flooding hosts [14] [18].

IV. CONCLUSION

In this paper we tried to analyze different techniques for the development of improved traceback capabilities. We have explored traceback algorithms based on probabilistic route selection, ingress filter & firewall, overlay network like centertrack, ICMP traceback technique. Each approach requires some network support or change to the headers of packets & has some advantages as well as few limitations. Concluding this survey we can say that as per the network infrastructure & its scalability the researchers should proceed with the traceback mechanism.

REFERENCES

[1] Lee Gerber, "Denial of Service Attacks Rip the Internet," *IEEE Computer*, April 2000

[2] Hongbin Yim, Taewon Kim, Jaeil Jung, "Probabilistic Route Selection Algorithm to Trace DDoS Attack Traffic Source", IEEE 2011.

[2] Peter G. Neumann, "Denial-of-Service Attacks," *ACM Communications*, April 2000, vol 43. No. 4.

[3] Kevin J. Houle and George M. Weaver, "Trends in Denial of Service Attack Technology," Computer Emergency Response Team (CERT) ® Coordination Center, v1.0, October 2001

[4] Computer Emergency Response Team (CERT)® Advisory CA-2001-20, Home Network Security, http://www.cert.org/tech_tips/home_networks.html

[5] Sanjeev Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet", Second International Conference on Internet Monitoring and Protection (ICIMP 2007)

[6] Abhrajit Ghosh, Larry Wong, Giovanni DiCrescenzo, Rajesh Talpade, "InFilter: Predictive Ingress Filtering to Detect Spoofed IP Traffic", Proc. of the 25th IEEE

International Conference on Distributed Computing Systems Workshops (ICDCSW'05) 1545-0678/05 , 2005 IEEE

[7] Kavita Choudhary , Meenakshi Shilpa, "Smurf Attacks: Attacks using ICMP" , IJCST Vol. 2, Issue 1, March 2011

[8] Gholam Reza Zargar, Peyman.Kabiri, "Identification of Effective Network Features to Detect Smurf Attacks", 978-1-4244-5187-6/09/2009 IEEE

[9] Ronald L. Krutz, Russell Dean Vines, "The CISSP Prep Guide—Mastering the Ten Domains of Computer Security", Wiley Computer Publishing, ISBN 0-471-41356-9 pp-74-75, Accessed: 23rd Feb13

[10] P. Ferguson and D. Senie, "RFC 2827: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP source Address", May 2000.

[11] K. Park and H. Lee, "On the effectiveness of probabilistic packet making for IP traceback under Denial of Service attack", hoc. IEEE WOCOMM Anchorage, AK, USA, pp. 338-347, Apr. 2WI.

[12] K. Stefanidis, D. N. Serpanos "Countermeasures Against Distributed Denial of Service Attacks", IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 5-7 September 2005, Sofia, Bulgaria.

[13] Steven J. Templeton, Karl E. Levitt ,"Detecting Spoofed Packets",2007

[14] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Network support for IP traceback" in IEEE Transactions on Networking, Vol. 9, No. 3, pp. 226-237, June 2001.

[15] Hongbin Yim, Taewon Kim, Jaeil Jung, "Probabilistic Route Selection Algorithm to Trace DDoS Attack Traffic Source", 2011 IEEE

[16] S. M. Bellavin, "ICMP traceback messages", Internet Draft, 2001

[17] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in Proc. 2000 USENIX Security Symp., July 2000, pp. 199–212.

[18] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. 2000 USENIX LISA Conf., Dec. 2000, pp. 319–327.

[19] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, "Controlling IP Spoofing Through Inter-Domain Packet Filters", IEEE INFOCOM

[20] Wikipedia free Encyclopedia Available online at http://www.wikipedia.org

[21] Network-Based Attacks Available online at http://secret-epedemiology-statistic.org.ua/1587052091/ch01lev1sec3.html

[22] William Stallings, "Cryptography and Network Security principles and practice", Fourth edition, Pearson Prentice Hall, (2006).

[23] Christos Douligeris, Aikaterini Mitrokotsa ,"DDOS Attacks and Defence Mechanisms".