Comparative Study of IP-Traceback Systems for DoS and DDoS Attacks

Suchita Patil[1], Pradnya Rane[2], Pallavi Kulkarni[3] and B. B. Meshram[4]

**[1,2,3] Computer Department, VJTI,
Mumbai, Maharashtra, India**
[1]Suchitapatil26@gmail.com

[2]pradnyarane@gmail.com

[3]Pskulkarni77@gmail.com

**[4] professor, Computer Department, VJTI,
Mumbai, Maharashtra, India**
bbmeshram@vjti.org.in

Abstract

This paper gives the idea of Vulnerabilities present in protocols, Also detail study of DoS attacks and the scenario of how DoS attacks can happen on internet its defence mechanisms. There are many solutions proposed by many author to avoid DoS and DDoS attacks and that are discussed in this paper. This paper provides classification of attacks, and the defence mechanisms that can be used to detect the DDoS and DoS attack.

Keywords: *Network Protocols, DoS attack, DDoS attack, Virus, Worms & Trojan, Ip-traceback.*

1. Introduction

Due to Globalization in the computer networks, Using Internet, the enterprise networks also face anonymous adversaries that may launch attacks from anywhere on the Internet. Today's enterprise security management must expand its scope to monitor the malicious activities on the Internet. Different attacks are possible due to this. Networks expose computers to the problem of transitive trust. Your computers may be secure, but you may have users who connect from other machines that are less secure. This connection-even if duly authorized and immune to direct attack. Security means It should provide secrecy, Integrity, Authentication and non-repudiation. Secrecy is to allow only authorised user to access information. Authentication is to verify the identity of sender and receiver. Integrity is to verify that information has not been altered while transmitting. Non-Repudiation is to verify that the sender has sent a message that he cannot deny latter.

Section 1 gives introduction. Section 2 describes the related work done on the attacks and defense mechanism for DoS and DDoS attacks. Section 3 covers the vulnerabilities and Section 4 gives detection techniques for these attacks. Section 5 gives the discussion about all IP trace back schemes and It's packet marking schemes. Section 6 is conclusion.

2. Related Work

There are different attacks possible due to less security and classification of all these attacks are covered in paper written by Anna Sperotto et. al.

2.1 Classification of Attacks [1]:

These classifications usually distinguish between the following basic categories:

1. *Physical attacks:* attacks based on damaging the computer and network hardware.
2. *Buffer overflows:* attacks that gain control or crash a process on the target system by overflowing a buffer of that process. A buffer is a contiguous area of memory occurring within the memory space allocated by the operating system to a running process. Buffers are created by computer programs. The programmer's intended use of the buffer is to store data of an expected size and format. The run-time system of certain programming language environments do not perform bounds checking, or type checking, on the buffer automatically. Programmer is expected to include program instructions to perform the check when necessary. In many software components these checks do not appear. Consequently, a buffer can be made to overflow in the same way as a bucket of water can be made to overflow. The technique of deliberately

overflowing a buffer to compromise a software system is known as a *buffer overflow attack.*

3. *Password attacks:* attacks trying to gain passwords, keys, etc. for a protected system.
4. *Information gathering attacks:* an attack that does not directly damage the target system, but gains information about the system, possibly to be used for further attacks in the future. This category comprises network traffic sniffing and (port) scans.
5. *Trojan horses*: a program disguised as a useful application, which deliberately performs unwanted actions.
6. *Worms*: a program that self-propagates across a network. Self-propagation is the characteristic that differentiates worms from viruses (see below). A worm spread can be extremely fast: an example is the Sapphire/Slammer worm, which is known to have infected 90% of the vulnerable hosts in 10 minutes.
7. *Viruses*: a virus is regarded as a worm that only replicates on the (infected) host computer. Hence, it needs user interactions to propagate to other hosts. Often, the definition also requires that a virus has to attach itself to files on the host, e.g., executable files, in order to be activated. As a consequence, the speed of spreading cannot be compared with a worm spread.

   i. *Boot Virus:* Boot viruses place themselves in the disk sector whose code the machine will automatically execute during the boot process. When an infected machine boots, the virus loads and runs. After a boot virus finishes loading, it will usually load the original boot code, which it had previously moved to another location, to ensure the machine appears to boot normally.

   ii. *File Virus*: File viruses attach to files containing executable or interpretable code. When the infected code is executed the virus code executes. Usually the virus code is added in such a way that it executes first. After the virus code has finished loading and executing, it will normally load and execute the original program it has infected, or call the function it intercepted, so as to not arouse the victim's suspicion.

   iii. *Macro Virus*: Macro viruses are a specialization of file virus. They copy their malicious macros to templates and/or other application document files, such as those modified by an office productivity software suite. Early versions would place themselves in the macro code that was the first to execute when infected templates or documents were opened. However other macros require the user to invoke an application command, which runs the malicious macro.

   iv. *Script Virus*: Script viruses confuse the victim because they do not appear to be executable files. Standalone Visual Basic Script (VBS) and JavaScript (JS) programs have suffixes that a naïve user does not associate with an executable program. Consequently, script viruses became a popular virus type for attackers launching their attack using mass e-mailing.

   v. *Image Virus*: An image virus attaches itself to compressed image files, e.g., JPEG. Merely viewing the image with a vulnerable web browser could invoke a buffer overflow and activate the virus. The infected image could be distributed via e-mail. It could also be distributed via its presence on a web site.

   vi. *Companion Virus*: Companion viruses do not directly infect boot sectors or executables. Instead, a companion virus simply assumes the same name as a legitimate program but with an extension that will cause an operating system to give it higher precedence for execution. When the file is involved at the command line without the extension, the victim will expect the legitimate program to execute but instead the companion virus will execute.

8. *Scans:* Scans are usually characterized by small packets that probe the target systems. Keeping this characteristic in mind, it is easy to imagine that scans can easily create a large number of different flows. There are three categories of scans:
   (i) A host scanning a specific port on many destination hosts (horizontal scan);
   (ii) A host scanning several ports on a single destination host (vertical scan);
   (iii) A combination of both (block scan).

9. Botnets: Botnets are groups of computers “infected with malicious program(s) that cause them to operate against the owners’ intentions and without their knowledge”. Botnets are remotely controlled by one or more bot-masters. Moreover, Botnets are

the perfect infrastructure for setting up and supporting any kind of distributed attack, such as, for example, DoS attacks and SPAM campaigns. Infected hosts unknowingly become part of Botnets, and take part in malicious activities. The threats posed by Botnets are such that we decided to include them in our attack classification.

10. Denial of service (DoS)[2] : Denial of service (DoS) attacks aim at denying or degrading a legitimate user's access to a service or network resource, or at bringing down the servers offering such services.
11. Distributed DoS(DDoS)[3] : A DDoS attack system can usually be described as a hierarchical model in which an attacker controls a handler (master) that, in turn, dictates the hordes of agents (slaves) to flood the bogus packets to the victim. The communication between the attacker and the handler and between the handler and the agents is called the control traffic, while the communication between the agents and the victim is called the flooding traffic.
12. MITM (Man-In-The-Middle) attack [4]: The address Resolution Protocol (ARP) resolves IP address into hardware or MAC addresses. The ARP poisoning attack targets to modify the IP/MAC address mapping in the ARP cache of remote machine maliciously. The MITM attack is based on ARP poisoning attack. In a MITM attack, an attacker intercepts a legitimate communication between two communicating parties. The attacker then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient.
13. Packet Sniffing [5]: In its most basic form a packet sniffer simply captures all of the packets of data that pass through a given network interface. However, if the network interface card is placed into "promiscuous mode", the packet sniffer is also capable of capturing all packets traversing the network regardless of the source or intended destination.
14. SYN-Flooding[5]: Assume a client process is attempting to perform the aforementioned handshaking process with a server. One point where an attacker can interfere with this process is where the server system has sent an acknowledgment (SYN/ACK) back to client but has not yet received the ACK message. This incomplete handshaking process results in what is referred to as a "half-open" or "partially open" connection. The server operating system has built in its primary memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially open connections. The attacking system sends SYN messages to the victim server system. These messages appear to be legitimate connection attempts but in fact represent attempts to connect by a client system that is unable to respond to the SYN-ACK messages, or simply does not exist. In either case, the final ACK message will never be sent to the victim server system.

3. Vulnerabilities

A denial-of-service attack (DoS), which purports to deny a host, router, or entire network providing or receiving normal services in the Internet, can be launched in many different ways. One classic approach is the ping-of-death and teardrop attacks. System patches are usually issued immediately after discovering such attacks because such attacks are possible due to weaknesses of system design. Another approach of DoS attack is to impose computationally intensive tasks on a target machine, such as encryption and decryption computation, and secret computation based on Diffie-Hellman exchanges. This can be done by simply placing the virus which is a software program to run on target machine. Before actually performing the DoS or DDoS attack first attacker sets up the network of hosts/host and this host (masters/handlers) also known as zombies or Daemons.

There are two types of flooding attacks and DoS is one of the Flooding attack. One method is Direct and another is Reflector method or indirect method.

In Direct method the packets which are sent to the target machine is of TCP/ICMP or UDP.

i. Using TCP packet the SYN flooding attack[7] which is performed and the source IP address is the Spoofed address which is randomly generated, so response i.e. SYN-ACK for these packets are not sent to the attackers machine. Thus, the victim retransmits the SYN-ACK packets several times before giving up. However, these half-open connections will quickly consume all the memories allocated for pending connections, thus preventing the victim from accepting new requests.Now a days there are many attacking tools are available which perform this activity. Other type of TCP-packet based attack is to congest a victim's incoming link. Under these attacks, the victim usually responds with RST packets, except when the attack packets are also RST packets.

ii. Other packet which are used for DoS attacks are ICMP packets [7] echo request packet and timestamp request packet. ICMP floods [8] (e.g ping floods): A stream of ICMP packets is sent to the victim host. A variant of the ICMP floods is the Smurf attack in which a spoofed IP packet consisting of an ICMP

ECHO_REQUEST is sent to a directed broadcast address. The rfc for ICMP specifies that no ECHO_REPLY packets should be generated for broadcast addresses, but unfortunately many operating systems and router vendors have failed to incorporate this into their implementations. As a result, the victim host (in this case the machine whose IP address was spoofed by the attacker) receives ICMP ECHO_REPLY packets from all the hosts on the network and can easily crash under such loads.

iii. UDP floods: A huge amount of UDP packets are sent to the victim host. Trinoo is a popular DDoS tool that uses UDP floods as one of its attack payloads.

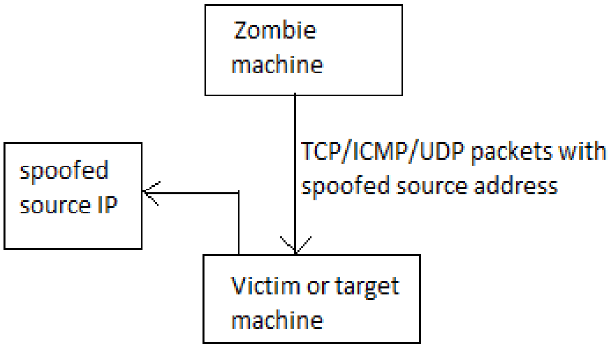

Fig 1. Direct flooding Attacks

A Reflector attack is an indirect attack in that intermediary nodes (routers and various servers), known as reflectors, are innocently used as attack launchers. An attacker sends packets that require responses to the reflectors with the packets' inscribed source addresses set to a victim's address. Without realizing that the packets are actually address-spoofed, the reflectors return response packets to the victim according to the types of the attack packets.

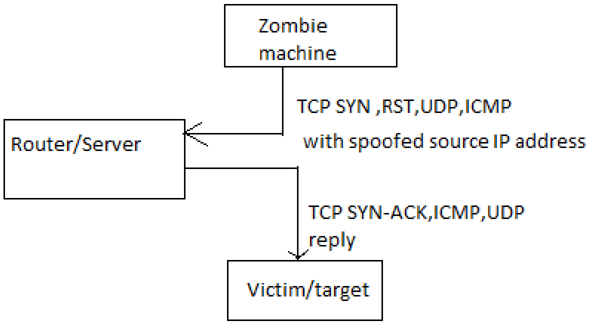

Fig -2 Reflector attack

Table1 : Summary of Reflector attack Method

	Packets send by attackers with spoofed source address of victim	***Packets send by reflector to victim as a response***
SYN flooding	TCP-SYN packet to the server or reflector (eg. Web server)	TCP SYN-ACK packet send by server to the victim
ICMP flooding	ICMP ECHO-REQUEST packets IP packets with low TTL UDP packets to the ports which are not opened	Echo reply packets ICMP time exceeded message Destination unreachable packet(ICMP packet)
RST packets	TCP packets to the non listening ports	TCP RST packets

Spoofing techniques are of following types which are mentioned by Jelena Mirkovic et. al.[6]

i. *Random spoofed source address*: Many attacks spoof random source addresses in the attack packets, since this can simply be achieved by generating random 32-bit numbers and stamping packets with them.

ii. *Subnet-spoofed source address*: In subnet spoofing, the attacker spoofs a random address from the address space assigned to the agent machine's sub-net. For example, a machine which is part of 131.179.192.0/24 network could spoof any address in the range 131.179.192.0 - 131.179.192.255. Since machines at a subnet share the medium (Ethernet) to reach the exit router (¯first hop en route to the outside world), spoofing can be detected by this router using fairly complicated techniques. It is impossibleto detect it anywhere between the exit router and the victim.

iii. *En- route spoofed source address*: An en route spoofed source address attack would spoof the address of a machine or subnet that lies along the path from the agent machine to the victim.

iv. *Fixed spoofed source address*: Attacker performing a reflector attack or wishing to place a blame for the attack on several specific machines would use fixed spoofing. The packet carries the source address chosen from the given list.

4. Detection techniques

4.1 Detection classification [1]

Debar et al. proposed intrusion detection system taxonomy. Their classification focuses on the following elements:

Detection Method: if a system bases the detection on a definition of normal behaviour of the target system, it is called behaviour-based. If it matches the input data against a definition of an attack, it is known as knowledge based. In literature, the community usually refers to these classes with the names of anomaly-based and misuse based solutions.

Behaviour on detection: a system can be proactive and act against the intruder (active system) or can generate alerts that will be later processed by a different system or a human operator (passive system).

Audit source location: the data processed in order to detect intrusion can be host or application logs, network packets or alerts generated by other detection systems.

Detection Paradigm: the IDS can detect the current status of the target system (secure or insecure) or can alert on a state transition (from secure to insecure).

Usage frequency: the system can perform its task in realtime (continuous monitoring) or post-mortem (periodic analysis).

A system is described also on the basis of the following:

Locus of data-processing: a system can be centralized or distributed, irrespectively of the origin of the data.

Locus of data-collection: the data collection can be centralised or distributed.

Security: the intrusion detection system can be itself target of security threats.

Degree of inter-operability: a system can be built to work in conjunction with other systems (exchanging data) or stand-alone.

5. Discussion

Identifying the sources of large-scale distributed denial of service (DDoS) attacks is a challenging task because:

IP routing is based solely on the destination IP address carried by each packet.

IP packets are not authenticated at the moment they are forwarded, enabling spoofed source-IP addresses to be used in DDoS attacks.

Attacker's packets can be sent by zombie hosts (remotely controlled by an attacker), whose owners are unaware that they are participating in a DDoS attack. (Known as Handlers). The information about packet forwarding is not stored at router because It has a scalability issues. Router only forward the packets as it come to it. Only routing Table is stored at the router level. Individual packet information is not stored. And In DoS attack or DDoS attack the attackers address cannot be traced because it is a spoofed IP address which is used or the Zombie computers are used which are under control of attacker. So, only network can be identified because the individual IP address is not visible if firewall is used. In these attacks to trace back the path for incoming packet is very difficult.

There are different attack detection mechanisms proposed by many authors. In which some are based on IP-Trace back scheme, another is AS level BGP overlay structure to identify the path, Firewall. Some author gives idea of Intrusion detection and prevention system. One of the solutions to this is firewall.

The defence against attacks requires three different steps

Intrusion detection, usually performed by intrusion detection and prevention systems. The identification, at least partially, of the route(s) of attacker packets. The filtering or blocking of attacker packets at key points along the route(s).

This attack detection can be done at four levels *at victim's network*, *At upstream router*, *At further stream router*, and *at the source network*.

It increases the effect attack detection as we go on from attacker's network to victim's network. And It increases the effectiveness of packet filtering from victim's network to attacker's network.

One of the solutions to this is Firewall. By using firewall one can detect and prevent the attack and block the address through which some malicious activity is identified. A firewall can be defined as collection of filters, and gateway which satisfies the following properties

All traffic from inside to outside, and vice versa, must pass through the firewall. Only authorized traffic, as defined by the local security policy, will be allowed to pass.

The firewall itself is immune to penetration.

The firewalls are desirable follows 'Many hosts-and more likely, most hosts - cannot protect themselves against a determined attack.

Another solution is to trace the path of incoming packet by using IP-Trace back scheme. In IP trace back scheme Router has to mark the incoming packet by some packet marking scheme and using that packet marking scheme one can identify the network through which that packets are coming. Router has to modify the packet header and it has to insert the identity of intermediate router in the packet header. This packet marking scheme allow to reconstruct the network path from the victim to the attackers. Minho Sung and Jun Xu have proposed the IP-trace back scheme which works independent of protocols used.

When a DDoS attack occurs, most of the traffic is dropped by the upstream routers even before it reaches the victim. In this case, nothing can be done by the victim to improve the throughput of the legitimate traffic. To mitigate the attack, proper action needs to be taken at upstream routers. A set of upstream routers will form a "line of defence," referred to as a perimeter in the sequel. The routers on the perimeter, referred to as perimeter routers, will collaboratively inspect packets going through them. For simplicity of discussion, we assume that all perimeter routers are of the same distance (referred to as perimeter radius) away from the victim. It Contains the Enhance probabilistic marking model (EPM), in which it uses the unused packet header field like IP fragmentation bits to insert the identity of the router. Also it indicates whether the edge is infected or not. Another module is Attack mitigation and Decision making module (AMD) which identify whether the edge is infected or not. And if the edge is infected then it constructs the network path form the marking scheme which is used. IP trace back algorithm is used to reconstruct the path if the edge is infected. And other module which is used is preferential packet Filtering module (PPF). This module is running on every perimeter router. These modules will differentially filter packets (destined for the victim) that contain the aforementioned marks of the first type, based on the instructions issued to them from the AMD module, once an attack is detected. We will show that little processing overhead is incurred at the perimeter routers: Each filter/pass decision requires only the computation of a hash value and a table lookup. This method uses hash value of IP address of the router/node so it is more secure. The hash value is visible to intermediate intruder, IP address is not visible.

The following table gives the comparative study of IP trace back scheme, AS-level IP trace back system and Enhanced IP trace back system.

Table 2 : Comparative study of IP trace back scheme

AS-level Overlay structure for IP-trace back	***IP trace back scheme***	***Enhanced IP-Trace back scheme***
Dependent on BGP protocol	Dependent on IP protocol	Independent of the protocol
No need to install the system on every intermediate router	Need to install it on intermediate router	Need to install it on intermediate router
Use automatic construction of overlays network	Router table for this IP-Trace back scheme is not constructed automatically	Router table for this IP-Trace back scheme is not constructed automatically
In BGP protocol there is update message and community attribute which is used in IP trace back scheme.	In This the packet header is modified by router	In This the packet header is modified by router using fragmentation bits
The information about infected edges are not transferred to the perimeter router.	The information about infected edges are not transferred to the perimeter router.	The information about infected edges are transferred to the perimeter router.
In AS level traceback system the packet marking scheme uses hash value	In IP traceback system, Some of the packet marking scheme uses hash value	In enhanced IP-trace back system the packet marking scheme uses hash value and that is inserted in to the packet header.

For detection of these attacks the systems which are implemented is of two types which are anomaly based detection and misused based detection system.

An anomaly-based system can be described as [1]:

Self-learning: the system is able to automatically build a model of the normal behaviour of the system, or:

Programmed: the definition of normality has to be provided by the system developer.

A misuse-based system, on the other hand, presents a unique subclass, programmed: the system is provided with a knowledge-base of attacks, against which it matches the inputs.

Whenever the DoS or DDoS attacks are detected and confirmed as attack then packet filtering is performed. There are two methods of packet filtering one is Ingress packet filtering and Route based packet filtering. These packets filtering scheme gives different false negative ratio and false positive ratio.

6. Conclusion

When the computer is connected to network, there has to be more security provided to it. There are many tools available now a day's using which many attacks can happen easily. Also the DoS and DDoS attacks are difficult to trace and detect, but easy to make. This paper summarizes the methods which can be used for detection and counter measures of these attacks.

References

[1] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller (2010)"An Overview of IP Flow-Based Intrusion Detection", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 3, THIRD QUARTER 2010

[2] Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari.(2005)"Low Rate TCP Denial-of-Service Attack Detection at Edge Routers" IEEE COMMUNICATIONS LETTERS, VOL. 9, NO. 4, APRIL 2005

[3] Haining Wang, and Kang G. Shin(2003) "Transport-Aware IP Routers: A Built-In Protection Mechanism to Counter DDoS Attacks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEPTEMBER 2003

[4] Seung Yeob Nam, Dongwon Kim, and Jeongeun Kim(2010) "Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks", IEEE COMMUNICATIONS LETTERS, VOL. 14, NO. 2, FEBRUARY 2010

[5] Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing" Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)

[6] Jelena Mirkovic, Peter Reiher “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms”

[7] Forouzan, B.(2003), "TCP/IP Protocol Suite", 2 nd Ed., McGraw-Hill Higher Education, 2003.

[8] Puneet Zaroo,”A Survey of DDoS attacks and some DDoS defense mechanisms”

[9] Rocky K. C. Chang (2002) “Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial”IEEE computer magazine October 2002

[10] Minho Sung and Jun Xu(2003) “IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEPTEMBER 2003