DISTRIBUTED DENIAL OF SERVICE (DDoS)

Prachi Shah
School of Informatics and Computing
Indiana University Bloomington
Email: pracshah@indiana.edu

Abstract--- Distributed Denial of Service attacks are executed by an attacker that uses numerous zombie machines to launch an attack against the victim system. The purpose is to exhaust the connection bandwidth thereby, making a network resource or a service temporarily or indefinitely unavailable to its intended users.

Keywords
DoS, DDoS, bandwidth, networks, zombie, botnet

1. INTRODUCTION

1.1 Computer Security and Privacy

One of the most challenging and important issues faced in the computer networks domain since a very long time now are network security and privacy issues. These issues have been haunting network administrators, engineers and system managers. Due to the ever increasing number of cyber attackers and the use of more sophisticated tools and techniques of attack, these issues seem to be growing day by day and becoming more challenging.

Different types of attacks like Man in the middle, Tear drop, IP spoofing, Phishing, Denial of Service cause significant damage to the target systems and/or interrupt services.

1.2 Denial Of Service [DoS]

The purpose of this classic attack is to prevent legitimate users from using network resources and/or computer system services. Traditionally, DoS attack was executed using SYN packets wherein a multitude of SYN packets were sent continuously to a target system eventually, enabling the target system to shut down its services temporarily or permanently. Previously, routers would implement FIFO method for storing SYN packets. Once new (bogus) SYN packets enter the system, old (legitimate) packets are dropped off. Thus, the server memory gets overwhelmed by storing illegitimate packets and cannot accept new (legitimate) SYN requests from its intended users thereby, denying services to its intended users. Over the time, routers became smarter. They use rate-based filtering. After a certain limit of packets are accepted, routers don't further accept packets. Also, routers don't implement FIFO methods anymore. They only accept and store packets from computers that send an ACK as response to their SYN-ACK and complete the 3-way handshake. Incoming packets from a computer system that do not complete a 3-way handshake are dropped.

1.3 2nd generation DoS attacks

As the routers got smarter, attackers felt the need to improve their techniques. The 2nd generation DoS attack called **Distributed Denial of Service** attack is much more sophisticated than the traditional DoS attack. The attacker uses one or more controller systems and targets a few thousand computer system to convert them into zombies. Zombies are computer systems that have been infected by an external entity like a hacker, trojan horse or a computer virus and possess a security hazard. The owners of the zombie machines are not aware of their system being compromised. A simple spam email, a malware download or a simple phishing attack can convert a computer system into a zombie. Malware downloads enable automatic download and installation of a zombie program/file into the victim's system without victim's knowledge. The victim's system acts as a host to the zombie program. An army of these zombie machines called Botnets are then used to launch Distributed Denial of Service attacks on the target victim's system. Since, thousands of compromised computer systems are used to launch an attack, this type of attack is called a **Distribute** Denial of Service attack.

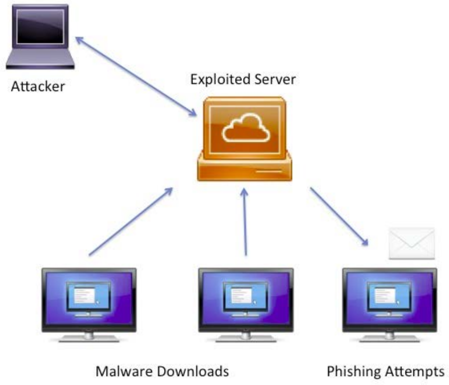
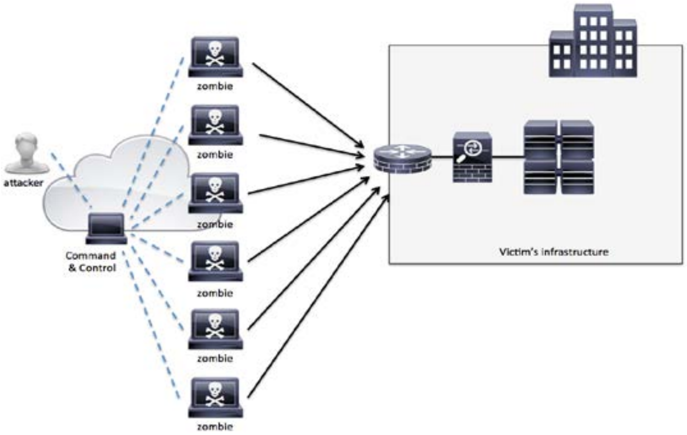


Figure: DDoS components. [6]

2. DISTRIBUTED DENIAL OF SERVICE [DDoS]

Distributed Denial of Service attacks are executed with the purpose of overwhelming the bandwidth of the target servers/computer systems. Multiple zombie machines send a flood of traffic to the target system in order to compromise their bandwidth, if not necessarily exhaust the target system resources. The main motive is to disrupt the normal services of the target system to its internal or external users, temporarily or indefinitely. The attacker with the use of one or more handler systems that manage botnets or an army of zombie machine, launches an attack on a system with usually high bandwidth. Attackers launch attacks multiple times for several hours over a span of few weeks.

As shown in the figure below, a controller/handler will instruct the zombie machine to launch attacks from time to time on the victim. The victim's bandwidth is disrupted or lost as a result of the attack.



2.1 Motive

DDoS attacks are one of the most common and disruptive attacks. The motives for DDoS attacks are multiple. DDoS attacks are generally carried out for political, religious, extortion, financial, retribution, competition, personal reasons and often just for fun! [1] Lately, extortionist attacked tech companies in order to receive bitcoin ransom.[2] Extortionist demanded around $300 of cryptocurrency[2]. Vimeo, Shutterfly and Evernote are some of the companies that have been victims of such attacks that are driven by extortion as a motive.[2] The Estonia DDoS attacks in April-May 2007 were launched for political reasons against the Estonian government by Russian youth groups.[1] The attacks lasted for 10 hours, the traffic data rate was close to 100 Mbps and the government had to bear a loss of ~$100,000. [1] Botnets were used to launch this attack. [1]

2.2 Methods

2.2.1 IP spoofing: The attackers sends request packets to the zombie machines with the spoofed source IP address of the target system. The zombies in turn send heavy responses to the target system thereby flooding them with heavy traffic.

Mitigation: Networks should implement ways to validate the authenticity of the source of the packets.

2.2.2 Ping of death: Different types of maximum-sized packets are send continuously to the target system using the simple ping command in order to clog the network bandwidth.

Mitigation: The ping of death is one the most common and serious attacks. Routers can implement rate-based filtering.

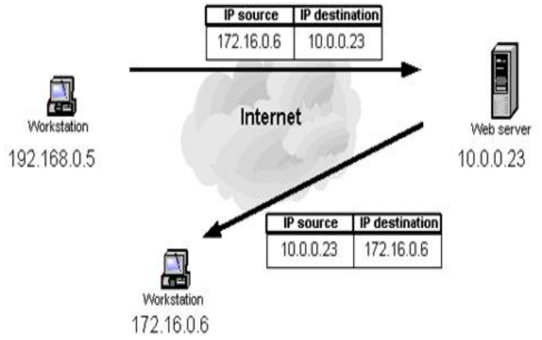


Figure: Spoofed source IP address [7]

2.2.3 Protocol Abuse:

2.2.3.1 UDP Floods: A large number of User Datagram Protocol packets are sent to the target system using a ping of death method.

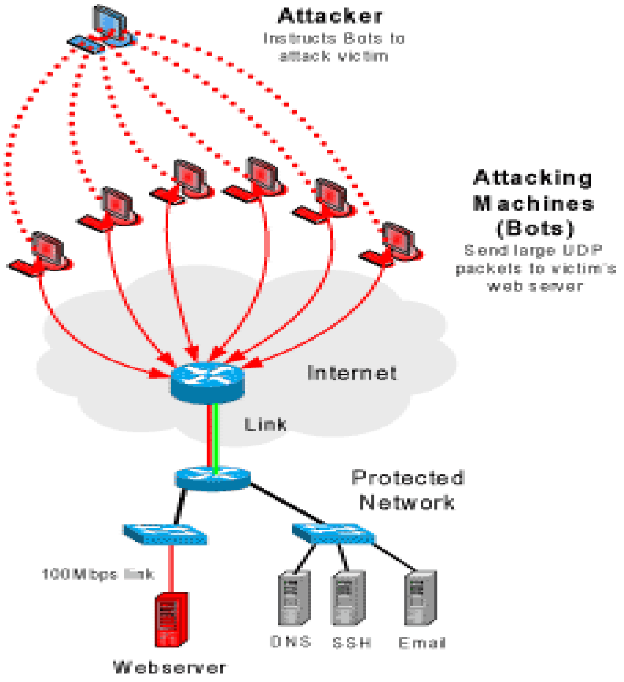

Attacker
Instructs Bots to attack victim
Attacking Machines (Bots)
Send large UDP packets to victim's web server
Internet
Link
Protected Network
100Mbps link
Webserver
DNS
SSH
Email

Figure: UDP Flood [4]

Since, the UDP packets do not implement a 3-way handshake (unlike TCP communication) and the protocol is connectionless/stateless, there is no way to determine the genuineness of the source of the packets. DNS amplification attacks are amongst those attacks that use UDP packets to launch a DDoS attack.

Mitigation: One solution is to enable routers to block/drop all UDP packets. This will enable border routers to disallow illegitimate UDP packets to enter the target network, thereby weakening the DDoS attack.

2.2.3.2 ICMP Floods: It is easy to spoof Internet Control Message Protocol packets with target system's IP address as the source IP. Since, ICMP packets don't have a structure similar to TCP communication hence, there is no specific way to determine if the source IP address is from a genuine source or that from a potential attacker. Generally, ICMP echo request packets are sent with spoofed IP address.

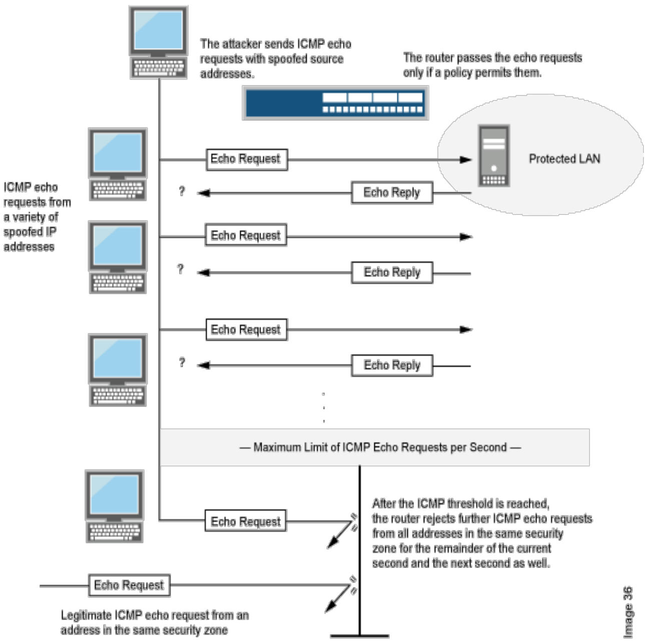

The attacker sends ICMP echo requests with spoofed source addresses.
The router passes the echo requests only if a policy permits them.
Protected LAN
ICMP echo requests from a variety of spoofed IP addresses
Echo Request
Echo Reply
?
Echo Request
Echo Reply
?
Echo Request
Echo Reply
?
— Maximum Limit of ICMP Echo Requests per Second —
After the ICMP threshold is reached, the router rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second and the next second as well.
Echo Request
Echo Request
Legitimate ICMP echo request from an address in the same security zone
Image 36

Figure: ICMP flooding [3]

Mitigation: Similar to UDP packets, a solution is to enable routers to block/drop all ICMP packets. This will enable border routers to disallow illegitimate ICMP packets to enter the target network, thereby weakening the DDoS attack. A DDoS attack on 13 root name servers few years ago, was a flood of ICMP packets. Since, the root servers were instructed to drop all ICMP packets, the damage caused was minimal.

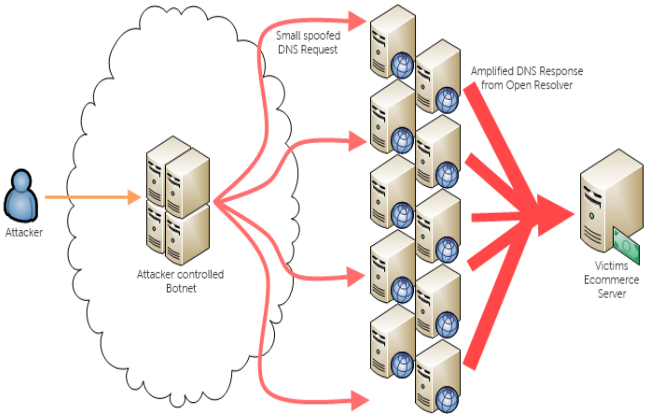
2.2.4 Amplification attacks:

2.2.4.1 DNS Amplification:

Amplification methods are advanced methods to launch DDoS attacks with the sole purpose of amplifying traffic. Publicly accessible open recursive Domain Name System servers are exploited to launch DDoS attacks. These servers accept DNS requests from computer systems that resides in any subnets around the world. They are open servers and hence, do not restrict their services to specific private subnets. Any malicious attacker can send a DNS request of around 60-90 bytes with the victim's spoofed source IP address to the DNS server. Since, the DNS server's response is huge (as it contains zone information), the response packets are nearly of 2000-4000 bytes. The amplification factor is nearly 50 times the original value of the request packet size. Generally, attackers sent spoofed queries of type “ANY”. DNS servers return maximum zone information as response to these type of queries thereby directing substantial amount of traffic towards the victim. The Spamhaus project, that is responsible for filtering around 80% of the daily spam messages all over the Internet, was affected by a DDoS attack in March 2014. Spamhaus distributes its blocklists of spammers using DNS servers. The method used for attack was DNS amplification.

Mitigation: Unfortunately, since the DNS responses that come from valid servers seem legitimate traffic, it is difficult to mitigate such an attack. One solution is for DNS servers to reject any traffic that contains spoofed addresses. Another solutions is to disable recursion on authoritative name servers for external clients and allow resolution to private authorized clients/organizations only. Response rate limiting feature has been implemented that limits the maximum number of responses/second to a client from the name server.

Figure: Botnet used to launch a DDoS attack.[8]


Small spoofed DNS Request
Amplified DNS Response from Open Resolver
Attacker
Attacker controlled Botnet
Victims Ecommerce Server

2.2.4.2 NTP Amplification:

An attacker spoofs the source IP address and sends a large number of UDP packets to the Network Time Protocol [NTP] server (port 123). The server supports a MONLIST command. This command sends a list of up to last 500 IP addresses that have accessed the NTP server. Since the UDP packets require no handshake, in a scenario where the server has its list fully populated, the response to the request can be 206-times larger than the request. [9] An attacker with a connection 1 Gbps can theoretically generate close to 200 Gbps or more of data traffic.[9]

Mitigation: One should check if their network contains NTP servers. If yes, they should check if the servers support MONLIST. This feature can be disabled. One can ensure that their network follows BCP38 – network ingress filtering tool and try to prevent packets with spoofed source IP addresses from passing through your network.

FACTS AND FIGURES [1][9]

1. Attacks History:

1.1 Primitive attacks: In year 1998, the traffic data rates were as small as 200 Mbps.

1.2 Modern attacks: In 2014, the DDoS attack traffic data rate was as large as 400 Gbps.

2. Attack Subtypes:

2.1 DNS

2.2 IP Fragment

2.3 Private IP Space

2.4 IP Null Protocol

2.5 TCP NULL Flag

2.6 TCP Reset

2.7 TCP SYN

3. Time takes:

3.1 1 year of global measured attack data

3.2 1128 attacks per day on an average

3.3 30 attacks per deployment/ day

4. Attacks by Protocol

4.1 TCP

4.2 ICMP

4.3 UDP

5. Top 5 countries that source DDoS attacks:

5.1 United States

5.2 Germany

5.3 Great Britian

5.4 South Korea

5.5 Sweden

6. Top 5 countries that source DDoS attacks:

6.1 Switzerland

6.2 United States

6.3 Sweden

6.4 Asia Pacific region

6.5 South Korea

2.3 Tools

2.3.1 Trinoo

The DoS Project's "trinoo" also called as “trin00”, is a set of master/slave programs that implement DDoS attacks. A user account is set on a repository that hosts trinoo daemon and master programs, lists of previously compromised hosts and list of possible vulnerable hosts, etc.[11] A scan is performed on multiple networks in order to identify potential target systems. Once identified, these systems are used to create scripts that will eventually perform the attack by executing sniffers and/or trinoo daemons or masters. On August 17, 1999 a trinoo network attack consisting a minimum of 227 systems, 114 out of these were at Internet2 sites, flooded a single system at the University of Minnessota, rendering the system unusable for over two days.[11]

2.3.2 Tribe Flood Network

Currently, Tribe Flood Network or TFN is developed and tested on several compromised UNIX systems on the Internet.[12] TFN is a powerful tool that can implement ICMP floods, UDP floods, Smurf attacks, SYN floods, as well as provide a root shell bound to a TCP port for attack, on demand. TFN consists of client programs. A command line execution of the client program control the TFN network remotely. This connection is established using different connection methods. ICMP_ECHOREPLY packets are used to establish a communication between the TFN client and daemons. This communication is not at all TCP or UDP based.

2.3.3 Stacheldraht

Stacheldraht tool combines features of the trinoo and TFN tool. Additionally, it provides communication encryption between the attacker and stacheldraht masters and, enables automated update of the handlers.[13] Stacheldraht consists of trinoo's handler features, as well as TFN's features of ICMP flood , UDP floods, SYN flood, and Smurf attacks.

Classic tools used to launch a DDoS attacks were Supper DdoS and NetBot attacker.

2.3.4 Timings

Typically, these attacks last from a minimum of an hour to a maximum of several weeks that consists of multiple attacks that's lasts a few hours.

2.3.5 DDoS attacks

2.3.5.1 GRC.com

Steve Gibson's Gibson Research Corporation, a provider of security and privacy software solutions, was attacked by a massive DDoS attack in May 2001. The attack lasts for three weeks. Their website grc.com was attacked by a total of 474 Windows PC's.[14] Approximately, 2.4 Billion packets were filtered by the Verio border gateway routers they used to protect their website.[14] The attacks were a simple brute force of ICMP and UDP packets. The UDP packets were aimed at GRC.com's bogus port "666". [14] GRC.com was connected to the Verio router using two 3.08 Mbps trunks (1.54 Mbps per each trunk). The Verio router was used to connect to the rest of the internet. The first attack launched on May 4th, 2001 knocked the website for over 17 hours. There were several attacks over the next few days on May 13th, 14th, 15th, 16th, 17th, 18th, 19th and on 20th May that knocked over the website for several hours. The mastermind behind this attack was a juvenile of 13 year old with the alias **"wicked"**. "wicked" and Steve Gibson were members of a common newsgroup. Steve Gibson particular comment on hacker newbies offended "wicked". As per "wicked", Steve had apparently called them "script kiddies". The motive of the attack was then to avenge against the comment. The attacker used an Internet Relay Chat [IRC] server in order to convert Windows PC's into zombies. These zombies were used to launch several attacks against GRC.com. The attacker implemented two commands on the ITRC server:

1) ***!p4 207.71.92.193*** [14]

These commands were executed as simple "ping" commands on windows systems:

ping.exe 207.71.92.193 –l 65500 –n 10000

This allowed zombies to launch 10000 packets of 655 Megabytes of data to the mentioned IP address. (GRC.com)

2) ***!udp 207.71.92.193 9999999 0*** [14]

This enabled zombies to launch 9,999,999 maximum-sized packets with 0 delay to the mentioned IP address. (GRC.com)

There was nothing much that Steve and his team could do to handle the attacks. This type of DDoS attack was powerful and rendered significant losses.

2.3.5.2 CloudFlare, Inc.

The biggest DDoS attack so far has been the one that was launched in the year 2014 against CloudFlare, Inc., a content delivery network and a distributed DNS. Attackers launched an NTP amplification attack of 400 Gbps, the maximum traffic data rate so far! The attackers used 4,529 NTP servers running on 1,298 different networks that generated on an average 87Mbps of traffic/server.[9]

3. Conclusion:

DDoS attacks are amongst the ones that are the toughest to mitigate. Since, the attack is based on sending innumerable packets to the target system, it is important to establish strong packet filtering techniques to avoid all illegitimate traffic. Packet filtering is difficult. Traditionally, attackers would send enormous number of packets from one computer system. Routers would implement two techniques to avoid packet floods. Routers would implement rate-based filtering that enabled them to stop accepting further packets after a certain limit of packets are accepted. Also, if a lot of packets are being sent from one source IP address, routers dropped further incoming packets from that source. But, attackers have got smarter. They send millions of maximum-sized packets from multiple sources using multiple zombie armies/ botnets. Hence, it is difficult to quickly understand if the system is under attack.

TCP packets implement a 3-way handshake. A SYN flood of TCP packets can be avoided since router will drop packets that do not complete the handshake. On the contrary, UDP and ICMP packets do not implement a 3-way handshake, making it difficult to validate the authenticity of such packets.

Another solution is to implement maximum security measures and rules at the border gateway routers, so that only legitimate traffic enters the internal network, as shown in figure. The internal network firewalls can implement additional rules to further filter incoming traffic. Implementing maximum security at the border gateway routers enables filtering maximum illegitimate traffic thereby, saving the resources and time needed to apply such security features internally.

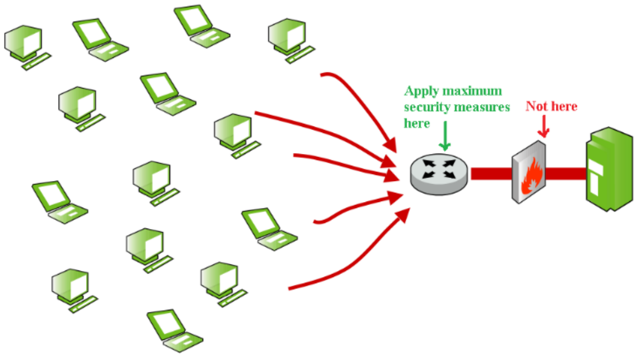


Figure: arbor network [1]

The primary difficulty is packet filtering, making it tougher to mitigate DDoS attacks. Once under attack, one can only implement smart packet filtering techniques in order to avoid further damage.

4. REFERENCES

[1]https://www.usenix.org/legacy/event/sec08/tech/slides/nazario-slides.pdf

[2]http://pando.com/2014/06/20/bitcoin-bandits-are-holding-tech-companies-for-ransom-with-ddos-attacks/

[3]https://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/understanding-icmp-flood-attacks.html

[4]http://areshelpusersrhb.blogspot.com/p/ataques-dos-syn-icmp-udp-flood.html

[5]http://www.betterhostreview.com/ddos-attack-protected-hosting.html

[6]http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

[7]http://people.scs.carleton.ca/~dlwhyte/whytepapers/ipspoof.htm

[8]http://www.secureworks.com/resources/blog/research/dns-amplification-variation-used-in-recent-ddos-attacks-update/

[9]http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

[10] http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

[11]http://staff.washington.edu/dittrich/misc/trinoo.analysis

[12]http://staff.washington.edu/dittrich/misc/tfn.analysis

[13]http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

[14]http://www.crime-research.org/library/grcdos.pdf