Scribe: Cryptography and Network Security (Week 5 Class 1)

Rutwik Pandit (20CS60R13)

Class 17 : Wed 30th September 2020

1 Introduction to DDoS

A Distributed Denial of Service attack is an attack orchestrated by an ACTIVE attacker to reduce or eliminate the Availability of a certain service. The motivations for a DDoS attack can be to cause financial harm by reducing the revenue of a business, cause a loss of credibility to that business , or simply restrict access to information.The standard procedure in a DDoS attack is to overwhelm the application resources thus blocking legitimate users from your application.

2 DDoS Fundamentals

2.1 Resource Problem and Asymmetry

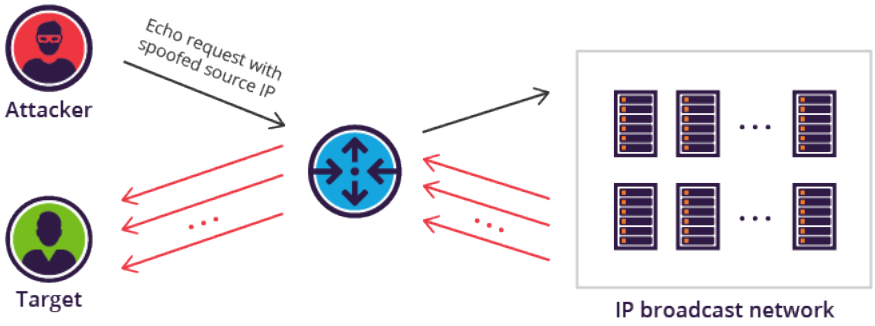
A victim server will always have a finite amount of computational and network resources i.e. Memory , CPU capacity , Network Bandwidth etc.A DDoS attack is then about winning the resource arms race. A fundamental question for a potential DDoS attacker is how do I muster the resources to overwhelm the victim , who will have substantial resources to serve his regular clients.This is where the Distributed aspect of the attack comes into view , because the victim is singular in nature , but the attacker can use a distributed net of machines.The attacker can ask for donations of computation resources , pay for the resources or use other nefarious methods like using botnets.
The attacker can also use Asymmetry.Asymmetry is when the attack only needs small amount of resources to then cause greater amount of damage to the victim. This property of amplifying damage is called amplification.

2.2 Amplification Factor

Amplification factor is the amount of output data that can be generated to head towards the victims machine for a certain X input data.If the amplification factor is high then we can use this to overload the victims machine using low amount of

input resources.There are various ways of generating these amplification factors which will be discussed below.

3 Smurf Attack



A Smurf Attack is a DDoS attack that involves sending ICMP echo requests to the broadcast address of routers in large computer networks with a spoofed source address, since the ping request does not validate the source IP. Since the router receiving the original ICMP echo request broadcasts it to every other device it's connected to, each one of these devices sends out an echo reply to the victims IP address.
Thus an attacker can get an amplification factor upto :

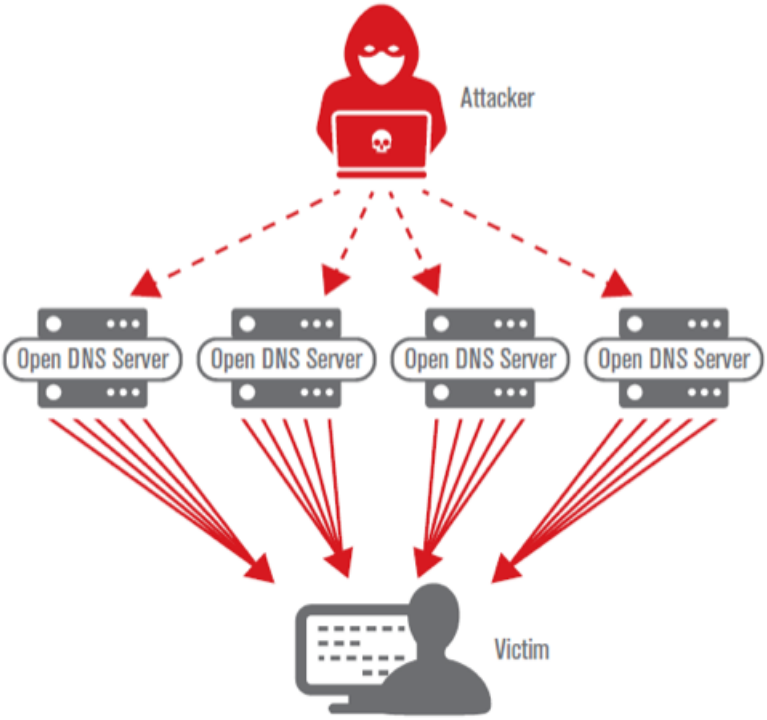
$$\frac{254 * SizeofPong}{SizeofPing}$$

After 1999, however, most routers do not forward packets sent to their broadcast addresses by default, this means the attack is now highly improbable.

4 Fraggle Attack

Fraggel attack is very similar to smurf attack.Fraggle attack replaces the ICMP request by a UDP request on port 7(Echo) and 13(Chargen).
Echo has an Amplification factor of 1.
Chargen has an Amplification factor of 360.

5 DNS Reflection Attack

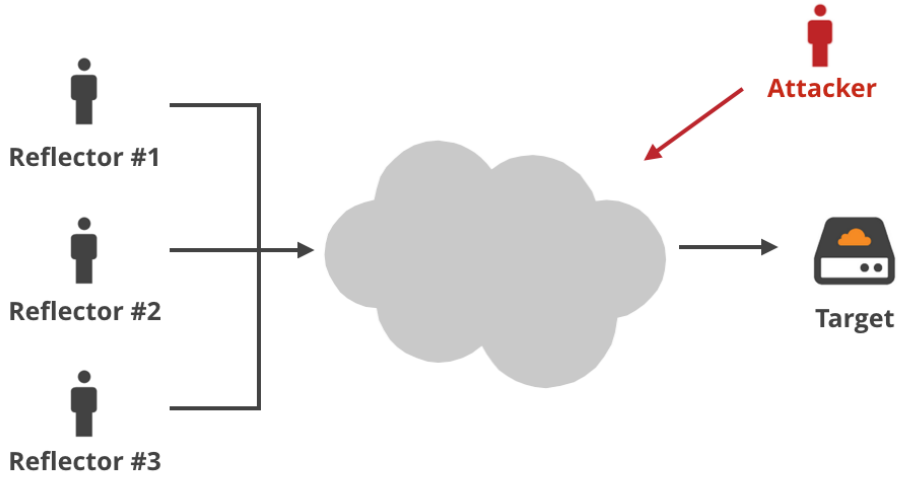


A DNS Reflection Attack uses the open DNS resolver servers available to amplify the attack.There are millions of DNS servers open to everyone on the internet.DNS queries are sent using UDP, thus it does not verify the IP of the source request.DNS requests with the "ANY" extension can generate upto 6000 bytes of response for 64 bytes of input.The attacker can also regsister a ficticious domain with a large DNS record which can be used to achieve a high amplification factor.
Thus the using DNS Reflection we can achieve an Amplification factor of upto 93.75.

6 NTP Reflection Attack

The NTP reflection attack is similar to DNS Refelction attack.NTP refection attack uses the open NTP servers to generate a large amplification factor.The NTP server accepts UDP packets and thus the victims IP can be spoofed.The "monlist" query on an NTP server generates a response 560 times larger than the input response.
Thus the using NTP Reflection we can achieve an Amplification factor of upto 560.

7 Memcached Reflection Attack



Memcached Reflection aka Memcrashed Attack is an attack which exploits the memcache service. Memcached is a memory-caching system which helps with increasing the speed of webservices.The attacker spoofs requests to a vulnerable UDP (port 11211) memcached server, because of the UDP request , the server cannot authenticate source IP and sends the response to victims IP.The memcache server can generate a large response ie multiple 1 MB for a small 1460 byte input query.
The Amplification factor ca be upto 50,000.

8 Conclusion

As we can see from the above examples , many of the Amplification attacks rely upon the unsecured nature of the UDP protocol.
DDoS mitigation can be achieved with the help of many service providers , but as IOT devices start to explode , the computational power available to attackers will continue to increase.

References

1. Lecture Slides
2. https://blog.verisign.com/security/dns-based-threats-dns-reflection-amplification-attacks/
3. https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/