Scribe: Cryptography and Network Security (Class.13.B)

AKASH KUMAR GANGWAR

24-September-2020

1 Introduction

In this scribe, I will explain about three type of attacks. First one is DNS poisoning attack- Kaminsky Attack and the second one is attacks on BGP(Border Gateway Protocol) and the last one is DoS attacks. So we will understand these one by one.

2 Kaminsky Attack

Kaminsky Attack was launched in 2008. It mainly meant for cache poisoning. In this attack, Attacker try to poison DNS cache in such a way that victims dns machine could have a wrong glue record.Glue records are record which tells dns server which machine to go or which authenticate name server to go for all the url to ip mapping for a given domain.

2.1 Working of kaminsky Attack

The attackers javascript resides on the victim's machine by different methods for example when we open website of movie downloading and torrent websites then many unwanted sites open simultaneously that may contain attackers javascript. In this attack the attacker send javascript will ask for a url and also create its own DNS server which continuously send the DNS response for same url so by this way Attacker can control victims' javascript.

Now the only thing attacker need query identification number that is quid and no authentication needed for quid as it use UDP protocol for sending query.

The QID can be guessed in following way
1. flood of responses with different QID
2.Just send responses with QID X and let the javascripted queries 1000 times. In this case $1000/2^{16}(1/65)$ chance that domain will be owned.

2.2 Solutions of kaminsky Attack

2.2.1 Immediate solution

1. Use QID size 32 bit instead of 16 , so there will be more search space for attacker to guess QID. But it can not be widely deployed because everyone have to update his application and many people do not want to update his application or system.
2.Another solution is to randomize the UDP port. That is used in present . For example Microsoft's updated DNS server is said to pre-allocate 2,500 UDP ports to use for these random queries . So by this method we can increase our search space for QID guess from $2^{16} to\ 2^{16} * 2500$that is 2^{27}almost. Then it will be more difficult for attacker to guess QID.

2.2.2 Better solution: DNSSEC

DNSSEC uses Cryptography for sign the DNs responses. Using cryptography you can ensure that from where the requests are coming from. You can authenticate every single path. So I will know that i request QID from which nameeserver and if that name server response back i will accept that otherwise reject that. So you can ensure Integrity of your request packet by DNSSEC. This is definite solution but it is costly.

3 Attacks on BGP

3.1 Border gateway protocol (BGP)

BGP is a protocol which is used to route packet between two autonomous systems. autonomous system can be BSNL, vodaphone etc. These AS have their own advertised paths for example if you want to connect IIT KHARAGPUR site you should have to come by this path and router.

3.2 BGP hijacking

In BGP hijacking mainly means changing the path to short path from original and trusted path but that was a bluff you may go to long route and on wrong route . It is very harmful attack as there packet may be lost and your confidential information can be leaked to someone on that path.

3.3 BGP hijacking in the real world

1."in April 2018, a Russian provider announced a number of IP prefixes (groups of IP addresses) that actually belong to Route53 Amazon DNS servers. In short, the end result was that users attempting to log in to a cryptocurrency site were redirected to a fake version of the website controlled by hackers." - the impact of this attack was 152 million dollars.
2."In 2008, the Pakistani government-owned Pakistan Telecom attempted to

censor Youtube within Pakistan by updating its BGP routes for the website. Seemingly on accident, the new routes were announced to Pakistan Telecom's upstream providers, and from there broadcast to the whole Internet. Suddenly, all web requests for Youtube were directed to Pakistan Telecom" - The impact of this hijacking was that youtube was down and they actually created denial of services on them.

3.4 S-BGP

So the solution to avoid BGP is S-BGP that is secure- BGP . S-BGP use cryptography and say these IPs and routes are under my control you need to sign this and verify from the root means previous hop authorize next hop and Higher level vouch for lower level So just use crypto to provide integrity. So S-BGP ensures that everything is vouched by trusted entities like ICANN, ARIN. and it only publish its root public key.
S-BGP is costly and not so popular as its adaption is very slow.

3.5 TLS/SSL certificates

TLS/SSL certificate is one way to solve this problem of DNS and fake IP. This certificate is used as a trusted and secure communication. For this you have to use public key certificates issued by certificate authority(CA) to know if you are really talking to the domain you intend and the list of Certificate Authority's are shipped with the browser.

4 DoS attacks

The full name of DoS is Denial of services . DoS is used to prevent users from being able to access a specific computer, service, or piece of data. So we can say shorty is will violate availability. It can be possible for the following vectors -
1. Exploit bugs that lead to crashes means you will crash the server

2. Exhaust the resources of a target means every server in this world has a limit of bandwidth if you will send them data more than that bandwidth then it will be unavailable.

4.1 DoS Attacker Goals Threat Model

In DoS, attacker may send arbitrary packets to anybody. and Goal of attacker is to reduce the availability for the victim means make the victim server slow.

4.2 DoS Attacker model

1. Attacker should have available bandwidth more than the server which he want to attack
2. Attacker can attack from many points and server is just one.

3. Attacker should send packet with minimum effort and risk of attacker while also maximizing the damage to victim

4.3 Standard DDoS(Distributed Dos)

In standard DDos you want to send packet from all over the place means from multiple people. and more ideally DDoS should use UDP that is connection less becuase it is very tough to spoof TCP connections.

4.4 When would DoS attack work?

DoS attack work when the effort of victim is much higher than the effort of attacker. Here effort means computation or work and memory resources.

4.5 TCP SYN flood

This is very simplest attack and a example of DDoS. TCP stack keeps track of connection state in data structures called Transmission Control Blocks (TCBs) . TCB wants to know quick SYN packet. Whenever you send a new SYN request you create a new TCB and essentially you put it in a queue and same happen when you receive a SYN request.

4.5.1 ATTACK

Attacker flood the victim with SYN packets. so attacker exhaust memory for TCBs, prevent legitimate clients from connecting. Or attacker crash the server OS by overflowing kernel memory .

4.5.2 Advantages for the attacker

1. As there is no connection so no need to hear responses
2. Attacker does not need to allocate TCBs means attacker machine would not be crashed

5 Conclusion

So in today class we learn about some popular attacks . These attacks violate mainly availability for victim. There should be many prevention to avoid these attacks which victim server should follow. Server should use cryptography for authentication and integrity so that if there will be any anonymous activity in server , server can know.