Scribe: Cryptography and Network Security (Class.1.A)

Ritik Kumar

23-Sep-2020

1 Introduction

In this class we discussed basics of networks and TCP and then learnt about the various network attacks which could happen like attacking host to host, attacking network infrastructure.

2 Basics of Networks

Lets take an example to understand it. When a computer A tries to connect to a server B. There are mainly 4 stages of it:

1. At first, we need to know the IP addresses of these machines (ie A and B). This is IP addressing and allocation.
2. To get the IP address of the destination (here it is IP address of B). It is done by DNS.
3. To find a path between A and B. It is done by Routing.
4. To decide how data should be send between them, decide the format and headers. This is done by TCP, UDP.

The attacker always lie. That is the attacker can send wrong data, wrong DNS record, wrong IP addresses. and the attacker always lies.

3 Basics of TCP communication

Two types of protocols exist in network layer: TCP and UDP.

TCP is a Transport layer Protocol and it sends data in a reliable way. So one always know if the packets sent by it reached to receiver or not, receiver always know that it is you that send the packets.

For this, each TCP connection has 3-way handshake. First client sends a SYN packet with Sequence number A. Then the server sends a SYN packet with

sequence number B+ ACK packet with sequence number A+1 which can be verified by client that packets reached the right server. Then Client sends ACK packet with sequence number B+1 which can be used by server to client.

The authentication or key root of security here is that the sequence number is random. And so no one else can send the same sequence number.

4 Blind Spoofing

It is an attack in which attacker A tires to pose as a client C to server S. A sends a SYN packet with seq = x and src: C's IP. Then S will send the packet with seq=y to C. But C will drop the packet since he never the send the packet with seq=x.
Now the attacker will try to guess and send ack=y+1. If it is able to guess and so 3-way handshake is complete. So now attackers can receive the packets related to C.

Earlier this sequence was dependent on time, so was easy to guess. The solution was to make it completely random and so makes it very difficult for attacker to guess it. But still non-blind spoofing could happen in the open WiFi or WiFi sharing. So the attacker have a idea of what are the possible sequence numbers someone can receive by looking the previous sequence numbers received by client from that server.

5 RST hijacking

RST is a special packet which resets the connection. That is used to stop present connection, drop all packets and initiate a new connection. Even if a attacker knows a port=p, he has very low probability of guessing sequence number y and closing connection.

One way to do this: Flood the network with RSTs.
It is hard to do it by individual attackers. But rather done by nation states for censorship. The nation state can reset the connection between VPN and user by sending RST packets to VPN with all sequence numbers.

6 Attacks on DNS

To connect to a server, we need IP address. And DNS is a way to convert URLs to IP addresses. If we can compromise the DNS server, then we can own a part of internet.

6.1 How DNS works

When user A tries to load a website "example.com". His browser will go to DNS server to ask IP address of "example.com" and DNS server might not know and so will go to high level DNS server like Authoritative name server. So Authoritative dns server will send the IP address to DNS server and DNS server sends it to the user.
But if we have to do this every time someone ask for "example.com" and then have to repeat this process every time which could be expensive and time consuming. So local server stores the IP address in cached data with an expiry date.

6.2 DNS Poisoning

The attacker can ask for IP address for say "example.com" and then will also send the fake IP address of "example.com" to DNS server repeatedly. While DNS server ask the IP address with Authoritative server. So whoever respond, its value is stored.
If attacker is successful. Then each time user asks for the IP address, DNS server will send the malicious address IP instead of the real one.

DNS poisoning changes the IP addresses for specific websites in the DNS servers. This works because DNS uses UDP. So no authentication is needed between DNS and authoritative servers.

Challenges with DNS Poisoning:
1. The attacker need to know which DNS queries are not cached. Because if it is already cached, the DNS server will drop the packages send by the attackers.
2. The attackers need to know the IP address of authoritative name server.
3. The attackers need to send it before the response of authoritative server. So it has very less time (only few milliseconds).

Solution to DNS Poisoning:
Add a random 16 bit query ID(QID) to every request. So authoritative nameserver will send the response with same QID. Now a attacker needs to race with the response from name server and also has to guess the QID correctly. (so chances come to very low).

6.2.1 Kaminsky Attack(2008)

This attack broke the security provided by the QID in the DNS attacks. In this a attacker can even own a whole domain.

Glue Records: Authoritative nameservers provide some DNS servers which the DNS server should go to get the required IP address. For example: Local DNS server will go to name servers which are related to query(say example.com).

Authoritative server will send the IP address along with these glues records. So next time you might directly go to get these glued DNS server address, to get the IP address.

Attackers Javascript resides on user's machine.This happens mostly when we load some malicious sites or try using torrent. This Javascript will just do a get request say for "doesnotexist.example.com".
The attacker also sets a DNS server which also send responses like this: doesnotexist.example.com has IP address of this. but also has a glue record of example.com with its IP address.

This glue record is problematic. Since DNS server will cache it and next time, when users will ask for example.com and it will return with this cache record. So here a authoritative DNS server is replaced by one set by attackers. So all sub-domain traffic will go to attacker instead of original authoritative DNS server. so it's like hijacking the whole domain.