IERG4130 Assignment3

YU Sihong

1155141630

1 Three types of man-in-the-middle attacks

- Chosen Ciphertext Attack in RSA
- Address Spoofing for network traffic, e.g. HTTPS Spoofing
- TCP Session Hijacking, SSL Hijacking, etc.
- Sniffing, IP Spoofing, Address Resolution Protocol SPoofing...

2 Adversary Model

1. Smurf Amplification attack

Availability, this attack will run out of the resouce of the server. It is a kind of DOS attack.

2. Sniffing

Confidentiality, sniffing is to get packets stealthily without authorization.

Availability, sniffing is based on broadcasting, which will consume the resouce.

3. Man-in-the-Middle attack

Confidentiality, attacker is possible to get the message, where the message can be sensitive.

Integrity, attacker is possible to edit the message in the middle.

Availability, it is possible to disturb the communication.

3 SYN flooding attacks

1. Yes; The attacker will send SYN message to the server, and the server will response and created a listener for the connection, which will consume the resouce. Once there are to many connections is waiting to complete, the server will run out of resouce and freeze.

2. It is easy to be detected and defended if using the same IP. Randomizing the IP will make detection difficult.

3. The SYN package will be dropped, because if the coonection is created, it do not need to handshake again.

4 DNS query

1. Possible Attack

- Spoofing(Hijacking the message); the attack can generate and send a fake reply of the DNS request from futher DNS server to this local DNS server.
- Injection(Hijacking the server); the attack can store the wrong IP address to this local DNS server in advance.

2. Defense

- To prevent receiving fake reply, the authentication between servers and the encryption of message is necessary.
- To prevent being stored wrong message, authentication is necessary. Firewall can be used to filter the unsafe data flows. Programmer needs to be careful with input from user and backdoor, to prevent injection and sniffing.

5 ARP

- ARP Spoofing
- As the line 2 and 4 have the same MAC address, which is an impossible situation for a normal server. The ARP spoofing is able to generate a fake reply and store it into the server. ARP spoofing is possible to cause such result.

6 SQL injection

1. Alice in `$userid`, `123' or '1'=='1` in `$passwd`. (Carefully editing the password so that SQL will return Alice's information without really know the password.)
2. Defense

- Check the user's input is valid or not, e.g. make sure any input is in a confirmed format, translate any dangerous characters.
- Change the SQL query strategy, e.g. just select the password of the user whose userid is Alice, and compare the password with the user input, successful if they are equal.

7 XSS

1. NO, there are many place in website to add js code, excluding `<script>`, e.g. `<button onclick="">`. It is inefficient to only reject the script tag, and it is difficult to reject all kinds of such inputs.
2. Example

- sending cookie/password/secret to the attacker
- running some programmes behind
  - substribe some youtuber...
- redirecting the website to somewhere the attacker wants
  - phishing website, fake login website...
- sending requests to the server with the help of CSRF
  - make a payment for the attacker...

8 SSL/TLS

- Yes and No, because there is a protection method, there will be a new attack method can break it.
- Yes; because SSL/TLS is to authenticate and encrypt the message between the client and the server, making the attacker hard to get the message.
- No; the man-in-the-middle attack is possible to simulate to be a normal server/client and gain trust from the victims. And it is able to do harm to the victims.