Computer Security (COM-301)

Network Security - TLS TCP

Interactive Exercises

TLS security

Suppose an attacker steals the private key of a website that uses TLS, and remains undetected. What can the attacker do using the private key?

a) Decrypt recorded past TLS sessions that used RSA key exchange.
b) Successfully perform a MITM attack on future TLS sessions.
c) Impersonate the client on future TLS sessions.
d) Decrypt recorded past TLS sessions that used Diffie–Hellman key exchange.

a) Yes: in RSA Key exchange, the key is sent by the client, which means that session keys are encrypted to the private key of the server. Thus, once adversary has this key they can recover the key of any past session and decrypt the content.
b) Yes, can sign for the server
c) No, the client does not use the SK of the server. But, when combined with (b) to steal credentials of user: in that case yes.
d) No, those are really ephemeral

State-?

Alice has designed a private file-sharing protocol over HTTPS (on the same port as typical applications). Which of the following **header-based firewall types** could block file-sharing connections over Alice's protocol without impacting other protocols over HTTPS?

a) Stateless
b) Both stateful and stateless
c) Stateful
d) Neither stateful nor stateless

Alice's service runs on the port of all other HTTPS connections. You cannot filter based on the port: **stateless does not work.**

Stateful can neither detect the protocol. That requires reading content to know what is going on

d) **True.** You need Deep Packet Inspection to detect this protocol (which is difficult for a HTTPS connection).

Flipagram

Flipagram is a website that allows clients to share photos with friends. Flipagram requires clients to login before using the system. To reduce the number of fake users on the platform, Flipagram restricts the number of users registered per IP to a maximum of 5.

When a client logs onto Flipagram, the server sends to the client all new pictures recently posted by this client's friends. The photos are then displayed by the client's browser.

Every time a client posts a photo on Flipagram, a TCP connection is created from the client's device to Flipagram's server. This connection is used to send the photo to the server who will store it. To increase the number of visits, clients can only upload one photo per hour.

Give two examples of Denial of Service attacks on Flipagram's server: one that would exhaust the server's bandwidth, and one that would exhaust the server's kernel and CPU resources. For each attack, state clearly (in one or two sentences) how the adversary performs the attack and what capabilities they need to perform the attack.

Sample answers:

- Server bandwidth:
- create a huge amount of clients on different IPs and post one photo per client
- create a huge amount of clients on different IPs that are friends with a lots of other users, so that when all the clients log on simultaneously, the server will try sending the new pictures to all fake clients, making it impossible for honest clients to get updates from their friends.

- Server kernel and application:

- Use fact that the website server listens to incoming TCP connection requests to launch a syn flood attack, or a teardrop attack, to exhaust the amount of TCP connections the kernel can create and make it impossible for other users to connect to the server
(A teardrop attack is a type of denial-of-service (DoS) attack (an attack that attempts to make a computer resource unavailable by flooding a network or server with requests and data.) The attacker sends fragmented packets to the target server, and in some cases where there's a TCP/IP vulnerability, the server is unable to reassemble the packet, causing overload.)
- With just one client, send millions of high resolution pictures to exhaust the server's memory (would require a huge amount of data)

Sawit

Bobby works at AcmeCorp. Bobby feels that during working hours he needs a break from time to time. He enjoys visiting Sawit, a site that allows users to post their favorite memes. Bobby does not want AcmeCorp's IT team to learn about his meme-related activities. He decides to use DNSSEC to resolve Sawit's IP address, and then HTTPS to connect to Sawit. Evaluate whether Bobby's setup will ensure that the following scenarios do not happen

1. AcmeCorp observes that an anonymous user has been posting memes making fun of AcmeCorp on Sawit. By inspecting the network traffic of AcmeCorp employees, the IT team finds out that it was Bobby who has posted these memes. The IT team informs his boss, who fires him.

1. The IT team hears from Bobby's colleague that he is visiting Sawit during his work time. They catch him in the act of posting memes about AcmeCorp by replacing Sawit's DNS record returned by the DNS resolver with an IP address of AcmeCorp's fake Sawit site. When he visits the fake site and posts memes about AcmeCorp, they inform his boss who fires him. Assume that the IT team only has access to Bobby's network traffic, and their fake server.

Justify your answer. If your answer is no in any of the scenarios, explain what Bobby could do to protect himself.

1. Potential answer: Yes, the setup ensures that this does not happen. Bobby is protected because he uses HTTPS which encrypts the contents of his messages. Thus, the IT team can only observe who has been visiting Sawit but not what they have posted.
2. Potential answer: Bobby is protected because DNSSEC provides protection against tampering of DNS records.

(Note: With a correct justification, the opposite answer could be correct as well for both 1 and 2.)