EPFL

SPRING

SECURITY AND PRIVACY ENGINEERING LABORATORY

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.

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

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.

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.

2. 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.