Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Jonas Jelten, M.Sc.
Richard von Seck, M.Sc.

Network Security Winter Term 2020/2021
Exercise 2

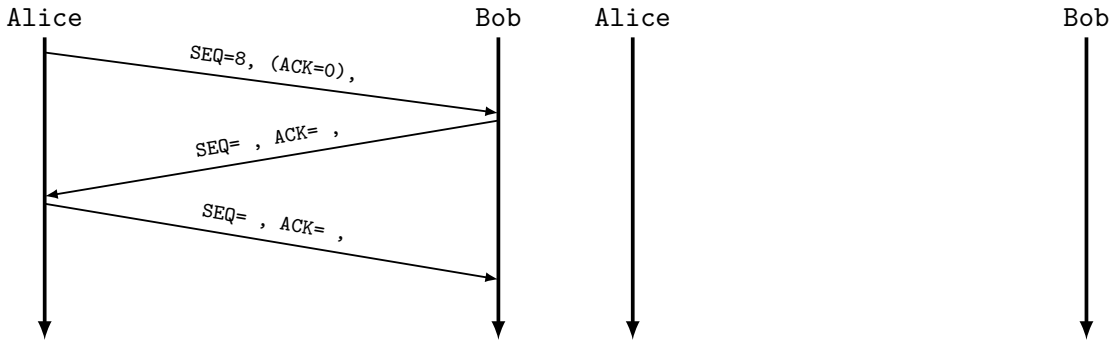
Task 1 TCP SYN Cookies

This task is about TCP SYN Cookies.

a) We prepared four statements about TCP SYN Cookies. Two of them are correct, two are completely wrong. Find out which ones are correct and which ones are wrong. Explain!

1. TCP SYN Cookies work because only valid (not attacking) clients can compute the secure cookie.
2. TCP SYN Cookies are designed such that the server does not need to remember states for half-open connections.
3. With TCP Syn Cookies, the server stores a secure nonce for every client.
4. TCP SYN Cookies were designed such that they are 100% compatible with TCP. A client may not even be aware that the server sent her a TCP SYN Cookie.

b) Complete the diagram of a regular TCP 3-way handshake. Bob thinks 42 is a good random number (where will he need it?)
Now complete the diagram of the same TCP handshake but with SYN Cookies right next to it.



c) A cookie consists at least of three components: $h(K, \text{src})$. Assume an implementation forgot something. Design an attack for every possibly wrong implementation of the cookie:

1. cookie $= K, \text{src}$
2. cookie $= h(\text{src})$
3. cookie $= h(K)$

Task 2 Langsec

a) Messages in your protocol are text-based and consist of two attribute-value pairs. Attributes and values can be any combination of letters and digits. Example: `attribute1:val1;attribute2:val2;` Is the language regular?

b) Is the language still regular if the messages in your protocol can include an arbitrary number of attribute-value pairs?

c) OpenTimeOrg has developed a new time server software and time server protocol to better support community-operated time servers. The timestamps report the time in seconds from a start date and are big fixed-point numbers with microsecond resolution. The protocol has the following operations:

- Client sends "GetTime" and server replies with timestamp
- The client can continue the conversation and report to the server the difference between its timestamp and the received timestamp. The server should ignore all reported deviations larger than 5 seconds. It will store the others for at least one hour.
  - The idea of this exchange is to anticipate the different clock skews and in utilizing the help of many clients to average out the clock skew of the server. It is up to the server, however, how it uses this information to improve its clock skew.
- Clients can request a list of recent timestamp deviations. The server will reply with the reported timestamp deviations from the last hour, at most the 1,000 last reported timestamp deviations.
  - The idea of this exchange is to enable the clients to optimize clock skew themselves and it allows them to have data to research on better algorithms for clock skew improvement.

Considering the concept of weird machines, give an example of using the protocol and server for a different unintended purpose. Note: For the sake of brevity, the protocol description does not provide all details. For the solution, focus on the main operations and fill in missing details reasonably if necessary.

Solution

We will put the solution online, encrypted with the password `weirdm4chines`.