Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Exercise 11

Total number of points obtainable: 16.

1 Challenge-Response

The following protocol was given in the lecture as a variation of the standard challenge-response protocol:

$$\begin{aligned} \text{Alice} &\longrightarrow \text{Bob} &:&\quad \mathit{Alice} \\ \text{Bob} &\longrightarrow \text{Alice} &:&\quad \{R\}_K \\ \text{Alice} &\longrightarrow \text{Bob} &:&\quad R, \end{aligned}$$

where R is a random challenge.

1.1 Reversible Crypto Needed?

(2 points) It was claimed that, in contrast to the standard challenge-response protocol, this protocol required reversible cryptography (i.e., a way to compute R from $\{R\}_K$ and K) in order to work. Doesn't the standard protocol also require reversible cryptography? After all, doesn't Bob need to decrypt $\{R\}_K$?

1.2 Mutual Authentication With Challenge-Response

It was claimed in the lecture that authentication was mutual if R was a recognizable quantity with a limited lifetime.

- **(2 points)** Why is this so? Describe how two parties can mutually authenticate themselves.
- **(2+2 points)** Suggest two different ways to create R values which have that property.

2 Timestamp-Synchronized Authentication

The following protocol was given as another variation of the challenge-response protocol that eliminates the challenge altogether:

$$\text{Alice} \longrightarrow \text{Bob} \quad : \quad \mathit{Alice}, \{t\}_K.$$

- **(1 point)** Assume that the server doesn't keep any state (i.e., doesn't remember past messages). Explain how Eve could impersonate Alice.
- **(3 points)** We said that when using the same secret K for multiple servers, Eve can impersonate Alice at the other servers. Fix the protocol so that this can't occur anymore. Keep the assumption that the same secret K must still be used for communication with all the other servers.

3 Foiling Reflection Attacks

(4 points) In the lecture, we claimed that we could foil reflection attacks if we insisted that the challenges looked different for Alice and Bob. Suggest two ways of modifying the challenges so that reflection attacks don't work anymore. Show why a reflection attack cannot work.