CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL Priv.-Doz. Henning Schnoor
Institut für Informatik · AG Software Engineering

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 7

issued: December 15, 2020 **due:** January 7, 2021

Exercise 7.1, the FFGG protototocol: too complicated? (10 Points)

Can you come up with a simpler protocol that is secure when only one session is running, but becomes insecure if the adversary can start as many instances as she wishes? Is there an "advantage" of the ffgg protocol (as an example illustrating the need for the analysis of parallel sessions) over your example?

Exercise 7.2, unbounded instances formalization (10 Points)

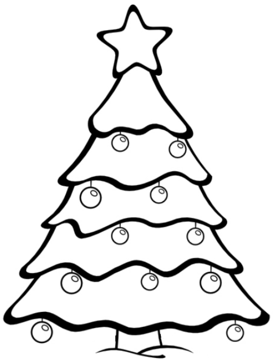
Specify the Needham-Schroeder protocol as an instance of the decision problem UNBOUNDED-INSECURE, and show that it is insecure in this formalization. Discuss the differences between expressing the protocol using this formalism compared to the earlier formalization using the decision problem INSECURE.

Note: You do not need to make your constructions formal. The goal of this exercise is to get a good understanding on how a formal definition of INSECURE (which we did not fully state in the lecture) would look like.

Exercise 7.3, Rusinowitch-Turuani with specified maximal number of sessions (10 Points)

We saw in the lecture that the "unbounded session" version of INSECURE is undecidable. A weaker version of that problem can be obtained by allowing instances to INSECURE to be accompanied by a maximal number of copies in which the adversary may start the corresponding protocol instance (we assume a mechanism that automatically renames variables to ensure that they are "local" to the copy in which they are used). Does the "positive" part of the Rusinowitch-Turuani theorem still hold for this generalization?

Hint: You are not expected to give a formal proof of your conjectures, an informal justification suffices. Also, be explicit about how the "maximal number of copies" is specified in the input to your generalized problem.



The Software Engineering Group wishes you a Merry Christmas and a Happy New Year!