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

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 6

issued: December 8, 2020 **due:** December 17, 2019

Exercise 6.1, applying the Rusinowitch Turuani Theorem (10 Points)

In the lecture, we discussed how to model the Needham-Schroeder protocol formally as an input to INSECURE such that the attack can be detected. However, this modeling required us to already specify the "correct" sessions ("Alice with Charlie, Charlie with Bob") as the input. For a complete automatic analysis, such a manual step should not be necessary. Can you come up with a general mechanism translating a natural representation of a protocol (for example, as the list of "intended instances" for a single session) into an instance that can be used as input for INSECURE? If not, why not?