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, modelled the Needham-Schroeder protocol as an input to INSECURE such that the attack is detected. However, this required us to already specify the "correct" sessions ("Alice with Charlie, Charlie with Bob") manually. For automatic analysis, such a manual step should not be required. Can you come up with a pre-processing step that makes this manual step unnecessary?

More precisely: Can you come up with a mechanism translating a natural representation of a protocol (e.g., as the list of "intended instances" for a single session) into a protocol P such that

- P can be used as input for the Rusinowitch-Turuani algorithm for INSECURE,
- P contains all relevant protocol instances (i.e., an initiator with Alice's identity expecting to communicate with a responder with Charlie's identity, and a responder with Bob's identity expecting to communicate with an initiator with Alice's identity),
- P is formally insecure if and only if there is a successful attack on any number of sessions with any set of identities in which the original protocol is run?

Note: You do not need to make your constructions formal.