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

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 9

issued: January 12, 2021 **due:** January 21, 2021

Exercise 9.1, ProVerif example I (10 Points)

Consider the following protocol:

1. $A \to B$ $\quad \mathsf{enc}^{\mathsf{s}}_{k_{AB}}(N_A)$
2. $B \to A$ $\quad [\mathsf{enc}^{\mathsf{s}}_{k_{AB}}(N_B), N_A]$
3. $A \to B$ $\quad N_B$

Here, k_{AB} is a long-term symmetric key shared by Alice and Bob. Is the protocol secure in the sense, that it can only be completed correctly if both Alice and Bob participate in the protocol run? Analyse the protocol "by hand" and using ProVerif.

Note: If you use the standard ProVerif **query attacker**(FAIL) modeling, you need to express the "participation property" as secrecy property. We will study a different method using events later in the lecture.

Exercise 9.2, ProVerif example II (10 Points)

Choose a cryptographic protocol and use ProVerif to analyze its security properties, that is:

1. Specify the protocol in ProVerif (including the required cryptographic primitives),
2. specify the security property in ProVerif,
3. run ProVerif to search for attacks. Does the result match with your expectations?

You can use any protocol you find interesting—all the protocols mentioned in the course so far are good candidates. The following is an incomplete list:

- your modeling of the WhatsApp authentication protocol in the first exercise,
- the (broken) authentication protocols presented in the first exercise class and their fixes,
- the Needham-Schroeder(-Lowe) protocol,
- the Woo-Lam protocol,
- the ffgg protocol,
- the repaired version of the handshake-protocol from the ProVerif tutorial (the broken version was discussed in the lecture).

Remember that most protocols are only insecure if the "correct" sessions are initiated. You can use a generic mechanism to start sessions, or use hard-coded sessions in your evaluation.