# Exercise for Engineering Secure Software Systems

January 28, 2021: Exercise 9

Henning Schnoor

Institut für Informatik, Christian-Albrechts-Universität zu Kiel

# Oral Exam

**date**

- Tuesday, February 23
- Wednesday, February 24
- let me know if you want to cancel!
- each exam: ≈ 25 minutes

**what to expect?**

- questions cover all lecture aspects
- theory lecture: precise formal knowledge of key definitions required for discussion
- sequence: definitions, results, proofs, alternatives, …

**preparation**

- use available material: slides, notes, exercises
- **“readiness indicator:” review questions**

**organization**

- oral exam via BigBlueButton
- registration until Sunday, February 14:
  `https://www-ps.informatik.uni-kiel.de/pruefungsanmeldung/`, access code: 1O1BIS

# Topics Today

Choice

- Solution to exercise tasks
  - ProVerif modeling, indistinguishability, relationshipp derivability/secrecy/events
- Information-Flow examples

answer

Zoom poll/Chat (don’t cheat ;-))

# Leftovers

# Exercise

**Task (ProVerif example II)**

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).