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

Engineering Secure Software Systems Winter 2020/21
Exercise Sheet 1

issued: November 3, 2020 **due:** November 12, 2020

Exercise 1.1, exercise git project (1 Points)

Create a git project together with your exercise partner at `https://git.informatik.uni-kiel.de` using the naming scheme `LL-SEM-Lastname1-Lastname2` and add Henning Schnoor (username hs) as a **Maintainer** to your project. Usually, you should have an account from your Bachelor's studies. If you did not obtain your Bachelor in Kiel or do not have such an account for some other reason, see `http://www.inf.uni-kiel.de/de/service/technik-service/accounts` for details on how to obtain such an account. In the project name, LL is an abbrevation for the lecture, (e.g., **SEPVS** for Software Engineering für Parallele und Verteilte Systeme or **ESSS** for Engineering Secure Software Systems), **SEM** is an abbrevation for the semester, like **WS20** for Winter 2020/2021. Lastname1 and Lastname2 are the last names of the two students in the working group. Write an email to Henning Schnoor with the URL of the repository (it suffices for one student in each group to write this mail).

Handing in of exercises and feedback to your tasks will use this git account. For non-programming exercises, answers must be submitted in one of the formats pdf, markdown, or plain text.

Exercise 1.2, WhatsApp Authentication (10 Points)

The instant messenges service WhatsApp for mobile phones uses the following authorization schemes:

1. To activate an account, the user needs to register a phone number. The system then sends a text message (SMS) over the mobile phone network to the user. The message contains a random number, which the user enters into the app. This activates the account.
2. To mirror the mobile app in a web browser, the user visits a special web page, which displays a QR code. The user then scans this code using the app, and can then access her account from the web interface.

Use informal notation and arguments to specify and discuss the security of the protocols underlying these authentication mechanisms. Think about whether encryption and/or signatures are used in the protocols, which (cryptographic) infrastructure is required to run the protocol, and which assumptions the protocol designers made.