Karlsruher Institut für Technologie

Institut für Informationssicherheit und Verlässlichkeit (KASTEL)
Kryptographie und Sicherheit
Prof. Dr. Jörn Müller-Quade

Sicherheitsbegriffe für die digitale Kontaktnachverfolgung (Security Notions for Digital Contact Tracing)

Projektgruppe „Praxis der Forschung“
Sommersemester 2022

1 Motivation

Bluetooth-based digital contact tracing schemes, such as the one implemented by the German Corona Warn App (CWA), contribute to the containment of pandemics while trying to strike a balance between data use and privacy demands. Here, the SARS-CoV-2 pandemic caused a surge of research activity that executed under severe time pressure to find a practical, sufficiently privacy-friendly solution, and subsequently gave rise to the decentralized approach of the Google–Apple Exposure Notification (GEAN) API, which is the predominant mechanism in use.

2 Goal

However, from a research perspective, there is a gap in our understanding of the maximal attainable security and privacy guarantees that would still result in practical schemes, and a proper full-scale formalization of the exact guarantees achieved. In a research project performed within KASTEL, an alternative digital contact tracing approach (called „ConTra Corona“) was presented and proven secure against a strong security formalization in the Real–Ideal model. This scheme uses different assumptions and offers even stronger privacy for infected participants, but was never adopted.

3 Project

Hence, it would be interesting to transfer our strong Real–Ideal security model to the employed GEAN-based approaches (as used in the CWA), and prove these secure against this derived model. Moreover, if time permits, there are plenty opportunities to tweak or extend the model, and/or to compare to existing game-based or UC-based formalizations of security (There is some flexibility w.r.t. the exact research goal.).

Preferably, a team of two or three students could work on the project.

4 Contact

- Felix Dörre <felix.doerre@kit.edu>
- Dr. Alexander Koch <alexander.koch@kit.edu>