Modeling and analyzing the Corona-virus warning app with the Isabelle Infrastructure framework

Florian Kammüller and Bianca Lutz

Middlesex University London and
Technische Universität Berlin
f.kammueller@mdx.ac.uk|bialut@gmail.com

Abstract. We provide a model in the Isabelle Infrastructure framework of the recently published Corona-virus warning app. The app supports breaking infection chains by informing users whether they have been in close contact to an infected person. The app has a decentralized architecture that supports anonymity of users. We provide a formal model of the existing app with the Isabelle Infrastructure framework to show up some natural attacks in a very abstract model. We then use the security refinement process of the Isabelle Infrastructure framework to highlight how the use of continuously changing ephemeral ids improves the anonymity.

1 Introduction

The German Chancellor Angela Merkel has strongly supported the publication of the mobile phone Corona warning app by publicly proclaiming that the "Corona App deserves your trust" [1]. Many millions of mobile phone users in Germany have downloaded the app with 6 million on the first day. This app is one amongst many similar application that aim at the very important goal to "break infection chains" by providing timely information of users whether they have been exposed to close contact with a person that has been infected.

The Corona-virus warning app has taken a long time to develop being published only on 16th June 2020. It was a quite costly project but this was mainly due to the management of Telekom and SAP being in the driving seat. But the app has been designed with great attention on privacy: a distributed architecture [] has been adopted after a long and heated debate with supporters of a central architecture. The distributed architecture is based on a very clever distributed application design whereby users phones are sending highly anonymized so called "Ephemeral IDs" at physical locations via the Bluetooth protocol. The app saves those IDs of people in close proximity. When at a later date an infected person reports his infection to a central server, the unique root ID is published and in the daily check all mobile phones connecting to the central server can download the root IDs of infected people. Since the Ephemeral IDs can be mapped to the root ID all Ephemeral IDs that have been saved over the last 14 days allow users phones to regularly check whether their user has been exposed to an infected

person and issue a warning to the user. The warning issued by the Corona warning app entitles to having a Corona test done (which at the time of writing is not normally possible).

The Isabelle Infrastructure framework [5] allows modeling and analyzing architecture and scenarios including physical and logical entities, actors, and policies within the interactive theorem prover Isabelle supported with temporal logic, Kripke structures, and attack trees. It has been applied for example to Insider analysis in airplanes [6], privacy in IoT healthcare [2], and recently also to blockchain protocols [4].

[TODO:Motivation: Why bother re-engineering a formal specification for a nicely developed privacy oriented app? physical aspects (adoption rate), formal proof etc]

In this paper, we first provide some background in Section 2: we give a detailed overview of the development history and security and privacy relevant parts of the Corona-virus warning app (Section 2.1) and some essential facts about the Isabelle Infrastructure framework (Section 2.2). We then present our model (Section 3) and analysis of privacy and attacks (Section 4) before drawing some conclusions (Section 5).

The formal model in the Isabelle insider framework is fully mechanized and proved in Isabelle (sources available [3]).

2 Background

2.1 History of Decentralized Architecture

2.2 Isabelle Infrastructure framework

3 Model

4 Analysis

5 Conclusions

References

1. D. Bundesregierung. Die corona-warn-app: Unterstützt uns im kampf gegen corona, 2020. German government announcement and support of Coronavirus warning app.
2. F. Kammüller. Attack trees in isabelle. In *20th International Conference on Information and Communications Security, ICICS2018*, volume 11149 of *LNCS*. Springer, 2018.
3. F. Kammüller. Isabelle infrastructure framework with iot healthcare s&p application, 2018. Available at `https://github.com/flokam/IsabelleAT`.
4. F. Kammüller and U. Nestmann. Inter-blockchain protocols with the isabelle infrastructure framework. In *Formal Methods for Blockchain, 2nd Int. Workshop, colocated with CAV'20*, Open Access series in Informatics. Dagstuhl publishing, 2020. To appear.
5. F. Kammüller. A formal development cycle for security engineering in isabelle, 2020.
6. F. Kammüller and M. Kerber. Applying the isabelle insider framework to airplane security, 2020.