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 [8] 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 [9], privacy in IoT healthcare [3], and recently also to blockchain protocols [7].

The technical advantage of modeling an application in the Isabelle Insider framework lies in (a) having explicit representations of infrastructures, actors and policies in a formal model that (b) allows additional automated verification of security properties within the interactive theorem prover Isabelle. Although the Corona-virus app has been produced based on a sophisticated security concept conceived by experts in the field, to our knowledge, no formal verification has been involved. Even if a "post-production" formal specification seems pointless, it allows to reveal weak points of the architecture, show that the measures that have been conceived are suitable to cover those weak points. Thereby, we believe that our current work is useful to increase the trust in the Corona-virus app necessary for its wide adoption which in turn is crucial for it to be efficient.

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 [4]).

2 Background

2.1 History of Decentralized Architecture

2.2 Isabelle Infrastructure framework

[TODO:Adapt: this is copied from FMBC paper] The Isabelle Infrastructure is built in the interactive generic theorem prover Isabelle/HOL [10]. As a framework, it supports formalisation and proof of systems with actors and policies. It originally emerged from verification of insider threat scenarios but it soon became clear that the theoretical concepts, like temporal logic combined with Kripke structures and a generic notion of state transitions were very suitable to be combined with attack trees into a formal security engineering process [2] and framework [5].

Figure 1 gives an overview of the Isabelle Infrastructure framework with its layers of object-logics – each level below embeds the one above showing the novel contribution of this paper in blue on the top. The formal model of the

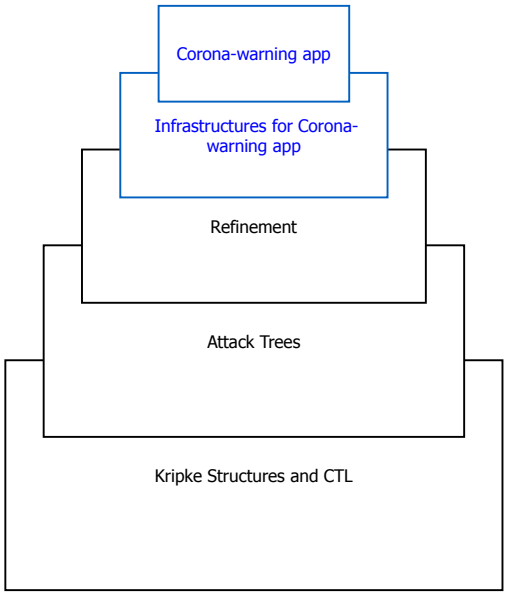

Fig. 1. Generic Isabelle Infrastructure framework applied to Corona-warning app.

Corona-warning app uses the Isabelle Infrastructure framework instantiating it by reusing its concept of *actors* for users and smartphones whereby locations correspond to physical locations. The Ephermeral IDs, their sending and change is added to Infrastructures by slightly adapting the basic state type of infrastructure graphs and accordingly the semantic rules for the actions move, get, and put. The details of the newly adapted Infrastructure are presented in Section 3. Technically, an Isabelle theory file `Infrastructure.thy` builds on top of the theories for Kripke structures and CTL (`MC.thy`), attack trees (`AT.thy`), and security refinement (`Refinement.thy`). Thus all these concepts can be used to specify the formal model for IBC, express relevant and interesting properties and conduct interactive proofs (with the full support of the powerful and highly automated proof support of Isabelle). The IBC theory itself is an adaptation of the Infrastructure theory of the Isabelle Infrastructure framework and reuses (or slightly adapts) existing concepts. In the remainder of this paper, we introduce the model that we conceived for IBC. All Isabelle sources are available online [6].

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. CHIST-ERA. Success: Secure accessibility for the internet of things, 2016. http://www.chistera.eu/projects/success.
3. F. Kammüller. Attack trees in isabelle. In *20th International Conference on Information and Communications Security, ICICS2018*, volume 11149 of *LNCS*. Springer, 2018.
4. F. Kammüller. Isabelle infrastructure framework with iot healthcare s&p application, 2018. Available at `https://github.com/flokam/IsabelleAT`.
5. F. Kammüller. Combining secure system design with risk assessment for iot healthcare systems. In *Workshop on Security, Privacy, and Trust in the IoT, SPTIoT'19, colocated with IEEE PerCom*. IEEE, 2019.
6. F. Kammüller. Isabelle infrastructure framework for ibc, 2020. Isabelle sources for IBC formalisation.
7. 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.
8. F. Kammüller. A formal development cycle for security engineering in isabelle, 2020.
9. F. Kammüller and M. Kerber. Applying the isabelle insider framework to airplane security, 2020.
10. T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer-Verlag, 2002.