ConTra Corona: Contact Tracing against the Coronavirus by Bridging the Centralized–Decentralized Divide for Stronger Privacy

Wasilij Beskorovajnov
FZI Research Center for Information Technology, Karlsruhe

Felix Dörre Gunnar Hartung Alexander Koch
Jörn Müller-Quade
Thorsten Strufe
Competence Center for Applied Security Technology (KASTEL),
Karlsruhe Institute of Technology (KIT)

32nd Crypto Day, 15 January 2021

Contact tracing is one of the most important interventions to mitigate the spread of any epidemic. Smartphone-facilitated *digital contact tracing* may help to increase tracing capabilities and extend the coverage to those contacts one does not know in person. Most implemented protocols use local Bluetooth Low Energy (BLE) communication to detect contagion-relevant proximity, together with cryptographic protections, as necessary to improve the privacy of the users of such a system. However, current decentralized protocols, including DP3T Troncoso *et al.* (2020), do not sufficiently protect infected users from having their status revealed to their contacts, which raises fear of stigmatization.

We alleviate this by proposing a new and practical solution with stronger privacy guarantees against active adversaries. It is based on the upload-what-you-observed paradigm, includes a separation of duties on the server side, and a mechanism to ensure that users cannot deduce which encounter caused a warning with high time resolution. Finally, we present a simulation-based security notion of digital contact tracing in the real–ideal setting, and prove the security of our protocol in this framework.

References

Carmela Troncoso *et al.* (2020). Decentralized Privacy-Preserving Proximity Tracing. *ArXiv e-prints* 2005.12273. First published 3 April 2020 on `https://github.com/DP-3T/documents` where companion documents and code can be found.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-43