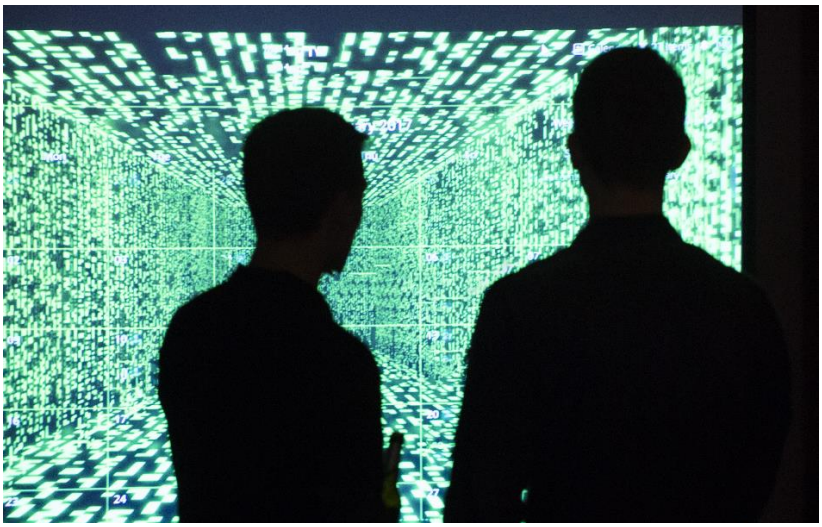
Privacy-aware Corona Tracing App

Researchers of KIT and FZI Propose to Combine a Central and a Decentralized Solution to Enhance Privacy



Researchers of KIT and FZI propose privacy-aware app for digital tracking of potential infection chains. (Photo: Irina Westermann, KIT)

Identification of contacts is one of the most important measures to mitigate the spread of the Corona virus. Tracing apps are to help. They will inform people who stayed near an infected person during a defined period of time. Technical implementation, however, is associated with the risk of data misuse and the approaches presented so far do not sufficiently protect privacy. Researchers of Karlsruhe Institute of Technology (KIT) and of the FZI Research Center for Information Technology, an innovation partner of KIT, have now proposed an app that combines the advantages of a central and a decentralized approach and, thus, enhances privacy. The results are published in a technical report.

In the past weeks, potential centralized or decentralized solutions for tracing apps and their data security triggered extensive discussion. Debates mainly focus on the question of whether these approaches sufficiently protect the privacy of users. For this reason, scientists of KIT's Competence Center KASTEL and FZI's Competence Center for

Monika Landgraf
Chief Press Officer,
Head of Corp. Communications

Kaiserstraße 12
76131 Karlsruhe, Germany
Phone: +49 721 608-21105
Email: presse@kit.edu

Press contact:

KIT:
Sandra Wiebe
Press Officer
Phone: +49 721 608-21172
Email: sandra.wiebe@kit.edu

FZI:
Johanna Häs
Head | Division Manager
Communications (COM)
Phone: +49 721 9654-904
Email: haes@fzi.de

Additional material:
Technical report:
https://eprint.iacr.org/2020/505.pdf

IT Security have developed a dual approach that guarantees enhanced privacy also against active attackers.

Combination of Central and Decentralized Solutions

“To exclude, if possible, the risks to the privacy of persons infected by the Corona virus, there should not be any central register of all persons infected and users of the system should not be able to draw any conclusions with respect to the person infected when they receive a warning,” says Professor Thorsten Strufe, Head of the “Practical IT Security” research group of KIT. “This is achieved by dividing the tracking information into information applied to warn the users and information required for tracking proper.” Moreover, the data should be distributed to several independent servers, each of which receives a small volume of sensitive information only.

The scientists plan to store the data locally on the mobile phones similar to the decentralized approaches presented so far. Then, these data will be loaded onto central servers in case of a positive diagnosis only. “On the servers, matching of the contacts will take place. In this way, we can conceal the person infected. This would be impossible when using a purely decentralized concept,” says Jörn Müller-Quade, Professor for Cryptography and IT Security at KIT and Director of FZI. “At the same time, we have divided the server such that no individual party alone can retrieve any sensitive information. For example, one server might be run by the Robert Koch Institute, while others are operated by large companies.” Even if all these servers would be compromised, this method would still reach the same security level as approaches presented so far – as long as they do not cooperate maliciously.

Protection against Unnecessary and Fake Warnings

The proposal of the scientists also includes the feature that users can reliably prove to medical experts that they had contact to an infected person before they are tested for COVID-19. Without this function, anybody could ask for a test by presenting a screenshot of a warning from another person’s smartphone. To prevent unnecessary and potentially panic-inducing warnings of contacts, the information about an infection risk will only be given after a certain period of time. This is to prevent that a person is warned after having passed a car in which an infected person was sitting, for instance.

“Our approach is practicable, scaled, and offers additional security features that have not yet been implemented in any other method,” Müller-Quade says. “Finding an optimum compromise between use,

privacy, robustness, and performance for applications, however, is a delicate matter that requires further work on data protection and security technology as well as thorough validation not only by scientists, but also by society as a whole."

The FZI Research Center for Information Technology which is based in Karlsruhe and has a branch office in Berlin is a non-profit institution for applied research into information technology and technology transfer. It provides businesses and public institutions with the latest research findings in information technology and qualifies young researchers for their career in academia or industry as well as for self-employment. The FZI is an innovation partner of Karlsruhe Institute of Technology (KIT).

Being "The Research University in the Helmholtz Association," KIT creates and imparts knowledge for the society and the environment. It is the objective to make significant contributions to the global challenges in the fields of energy, mobility and information. For this, about 9,300 employees cooperate in a broad range of disciplines in natural sciences, engineering sciences, economics, and the humanities and social sciences. KIT prepares its 24,400 students for responsible tasks in society, industry, and science by offering research-based study programs. Innovation efforts at KIT build a bridge between important scientific findings and their application for the benefit of society, economic prosperity, and the preservation of our natural basis of life. KIT is one of the German universities of excellence.

This press release is available on the internet at http://www.sek.kit.edu/english/press_office.php.

The photo in the best quality available to us may be downloaded under www.kit.edu or requested by mail to presse@kit.edu or phone +49 721 608-21105. The photo may be used in the context given above exclusively.