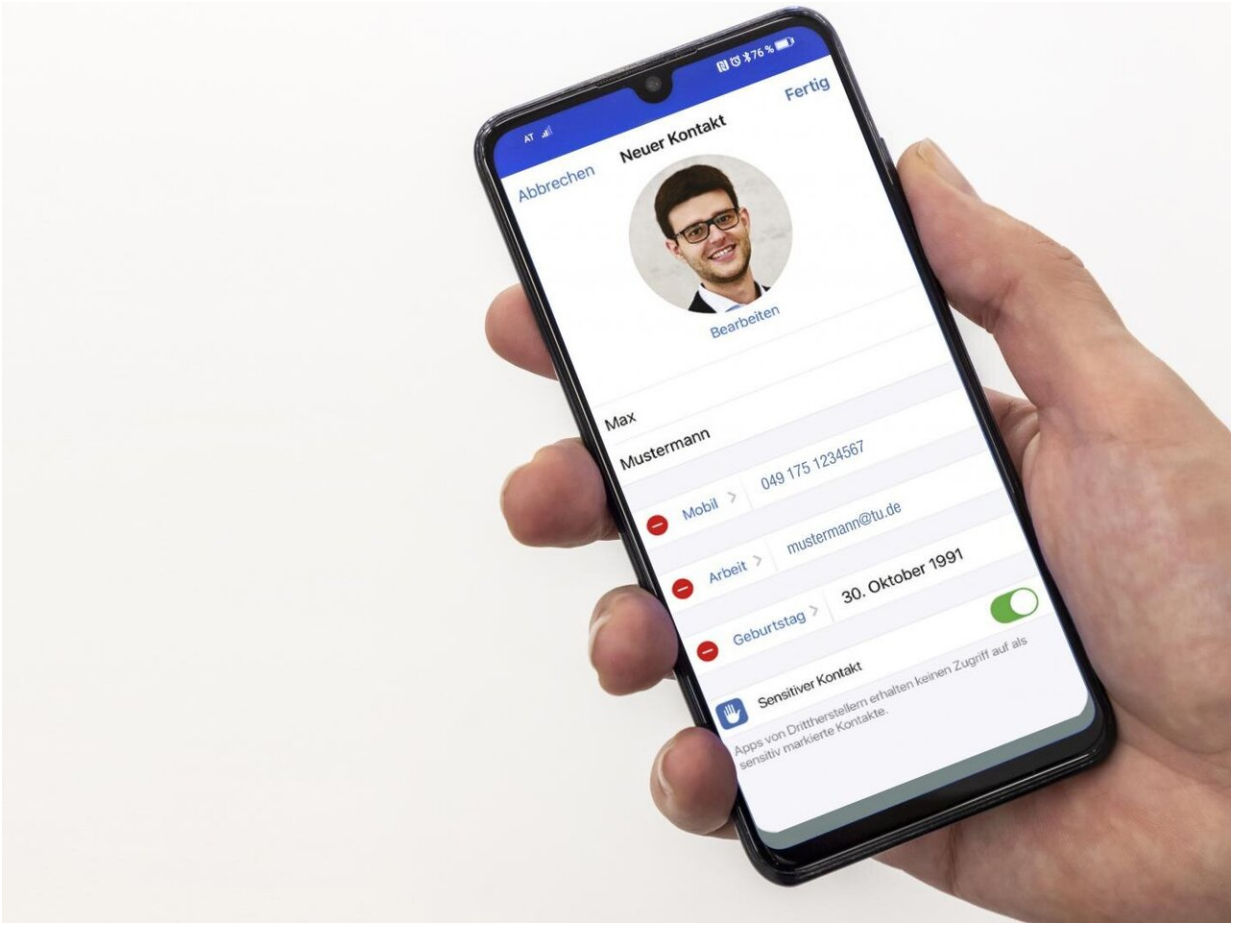
More privacy when using WhatsApp, Signal and others

February 16 2021, by Christoph Pelzl



This is how the planned ContactGuard integration in the address book application could look: Activating a "sensitive contact" function denies messenger services and third-party providers access to the data. Credit: Lunghammer - TU Graz/TU Darmstadt

When installing a messaging service on a smartphone, users are usually prompted to give the app access to their own phone address book. This will automatically connect them with those contacts from their address book who already use the messaging service. For this purpose, the service provider matches the telephone address books with its own contact database. This process currently uploads the complete address books to the service provider's servers.

This so-called 'mobile contact discovery' process constitutes a massive invasion of privacy. Service providers thus not only obtain the data of those individuals who have consented to the data processing themselves, they also obtain the data of those affected who have not installed the respective messaging service at all and thus have not given their consent to the processing and storage of their data.

New method of contact discovery

"There are currently no satisfactory solutions for a contact discovery process by mobile messaging services. All previous options are either completely insecure or at least do not offer any significant protection," says Christian Rechberger, summarizing the problem. The cyber security expert is professor at the Institute of Applied Information Processing and Communications at Graz University of Technology and area manager for Data Security at the Know Center. Rechberger has developed 'ContactGuard' together with his Institute colleague Daniel Kales and with the two researchers Christian Weinert and Thomas Schneider from TU Darmstadt. This is a new method of contact discovery that significantly limits or completely avoids privacy threats and critical scenarios such as spying on contacts or reselling data and exploiting sensitive relationships.

More efficiency and higher safety

The ContactGuard application is based on new encryption protocols that are many times more efficient and secure than all previously existing approaches. The shared contacts between the service provider and those people who use the messaging service are determined using intersection calculations. The service provider's encrypted database is sent to the user in a resource-saving manner—thanks to a compression technique specially developed by the researchers—and stored on the mobile phone. There, the address book entries are encrypted with the service provider's secret key, but without the users being able to see the secret key. Conversely, the service provider also does not receive any information about the address book entries of the users. This bilateral data encryption also means that no further information or sensitive data is revealed from the address books.

Successful tests should pave the way for more privacy

Additional efficiency is promised by the use of modern security chips which are included in most smartphones that have come onto the market in the past seven years. Compared to older chip generations, these chips speed up cryptographic calculations by a factor of 35. Prototype tests have shown that even with 100 million data records, data matching is within a tolerable time frame. There may be some latency due to the cryptographic calculations and data transfers only during the initial registration. "However, this is in the range of a few seconds even in mobile networks for the synchronization of up to 1000 contacts," said Rechberger. He now hopes that, with knowledge of the technical possibilities, policymakers will improve global data protection laws in the medium term in the interests of greater privacy: "This could prompt messaging services to act or for new offerings to emerge."

This research is anchored in the Field of Expertise Information, Communication & Computing, one of the five research foci at Graz University of Technology.

For the development of ContactGuard, the research group has now been awarded second place in the prestigious IT Security Award 2020 of the Horst Görtz Foundation on Feb. 11, 2021. In keeping with the sponsor's wishes, the researchers intend to use the prize money of 60,000 euros to further develop the security software to market maturity.

Since 2017, TU Graz and TU Darmstadt have had a strategic partnership that enables close networking between the two universities at all levels. In research, the close ties are reflected in numerous joint projects between different departments—including a research agreement on cyber security.

Provided by Graz University of Technology