Popular messenger services are extremely insecure

September 15 2020, by Christian Weinert, Daniela Fleckenstein

Credit: Unsplash/CC0 Public Domain

Researchers from the Technical University of Darmstadt and the University of Würzburg show that popular mobile messengers expose personal data via discovery services that allow users to find contacts

based on phone numbers from their address book.

When installing a mobile messenger like WhatsApp, new users can instantly start texting existing contacts based on the phone numbers stored on their device. For this to happen, users must grant the app permission to access and regularly upload their address book to company servers in a process called mobile contact discovery. A recent study by a team of researchers from the Secure Software Systems Group at the University of Würzburg and the Cryptography and Privacy Engineering Group at TU Darmstadt shows that currently deployed contact discovery services severely threaten the privacy of billions of users. Utilizing very few resources, the researchers were able to perform practical crawling attacks on the popular messengers WhatsApp, Signal, and Telegram. The results of the experiments demonstrate that malicious users or hackers can collect sensitive data at a large scale and without noteworthy restrictions by querying contact discovery services for random phone numbers.

Attackers are enabled to build accurate behavior models

For the extensive study, the researchers queried 10% of all U.S. mobile phone numbers for WhatsApp and 100% for Signal. Thereby, they were able to gather personal (meta) data commonly stored in the messengers' user profiles, including profile pictures, nicknames, status texts and the "last online" time. The analyzed data also reveals interesting statistics about user behavior. For example, very few users change the default privacy settings, which for most messengers are not privacy-friendly at all. The researchers found that about 50% of WhatsApp users in the U.S. have a public profile picture and 90% a public "About" text. Interestingly, 40% of Signal users, which can be assumed to be more privacy concerned in general, are also using WhatsApp, and every other

of those Signal users has a public profile picture on WhatsApp. Tracking such data over time enables attackers to build accurate behavior models. When the data is matched across social networks and public data sources, third parties can also build detailed profiles, for example to scam users. For Telegram, the researchers found that its contact discovery service exposes sensitive information even about owners of phone numbers who are not registered with the service.

Which information is revealed during contact discovery and can be collected via crawling attacks depends on the service provider and the privacy settings of the user. WhatsApp and Telegram, for example, transmit the user's entire address book to their servers. More privacy-concerned messengers like Signal transfer only short cryptographic hash values of phone numbers or rely on trusted hardware.

However, the research team shows that with new and optimized attack strategies, the low entropy of phone numbers enables attackers to deduce corresponding phone numbers from cryptographic hashes within milliseconds. Moreover, since there are no noteworthy restrictions for signing up with messaging services, any third party can create a large number of accounts to crawl the user database of a messenger for information by requesting data for random phone numbers. "We strongly advise all users of messenger apps to revisit their privacy settings. This is currently the most effective protection against our investigated crawling attacks," agree Prof. Alexandra Dmitrienko (University of Würzburg) and Prof. Thomas Schneider (TU Darmstadt).

Impact of research results: service providers improve their security measures

The research team reported their findings to the respective service providers. As a result, WhatsApp has improved their protection

mechanisms such that large-scale attacks can be detected, and Signal has reduced the number of possible queries to complicate crawling. The researchers also proposed many other mitigation techniques, including a new contact discovery method that could be adopted to further reduce the efficiency of attacks without negatively impacting usability.

All results are described in the paper "All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers," which will be presented in February 2021 at the 28. Annual Network and Distributed System Security Symposium (NDSS), a top conference for IT security.

More information: All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers: encrypto.de/papers/HWSDS21.pdf

Provided by Technische Universitat Darmstadt