Popular messenger services are extremely insecure - Billions of Users Vulnerable to Privacy Attacks

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 US 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 US 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.

Further Reading
More details: https://contact-discovery.github.io

Involved research groups:
• Secure Software Systems Group at the University of Würzburg: https://go.uniww.de/sss
• Cryptography and Privacy Engineering Group (ENCRYPTO) at TU Darmstadt: https://encrypted.de

About TU Darmstadt
The Technical University (TU) of Darmstadt is one of Germany’s leading technical universities. TU Darmstadt incorporates diverse science cultures to create its characteristic profile. The focus is set on engineering and natural sciences, which cooperate closely with outstanding humanities and social sciences. We are enjoying a worldwide reputation for excellent research in our highly-relevant, focused profile areas: cybersecurity, internet and digitalisation, nuclear physics, fluid dynamics and heat- and mass transfer, energy systems and new materials for product innovation. We dynamically develop our portfolio of research and teaching, innovation and transfer, in order to continue opening up important opportunities for the future of society. Our 312 professors, about 4,500 scientific and administrative employees and about 25,200 students devote their talents and best efforts to this goal. Together with Goethe University Frankfurt and Johannes Gutenberg University Mainz, TU Darmstadt has formed the strategic Rhine-Main Universities alliance.
www.tu-darmstadt.de

(Text by Christian Weinert & Daniela Fleckenstein.)

contact for scientific information:
Prof. Dr.-Ing. Alexandra Dmitrienko
Secure Software Systems Group
University of Würzburg
E-Mail: alexandra.dmitrienko@uni-wuerzburg.de
Tel.: 0931/31-81667
https://go.uniww.de/dmitrienko

Prof. Dr.-Ing. Thomas Schneider
Cryptography and Privacy Engineering Group (ENCRYPTO)
TU Darmstadt
E-Mail: schneider@encrypto.cs.tu-darmstadt.de
Tel.: 06151/16-27300
https://encrypto.de/schneider

Original publication:
All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers by Christoph Hagen (University of Würzburg), Christian Weinert (TU Darmstadt), Christoph Sendner (University of Würzburg), Alexandra Dmitrienko (University of Würzburg), and Thomas Schneider (TU Darmstadt) in 28. Annual Network and Distributed System Security Symposium (NDSS'21). Pre-print: https://encrypto.de/papers/HWSDS21.pdf

URL for press release: https://youtu.be/4vgKHmNaAAw