ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

End-to-end Encryption in a Messenger

A recent change in its terms of service has pushed millions of WhatsApp users to adopt alternative services such as Signal and Telegram. As reported by The Guardian[1]: "Over the first three weeks of January, Signal has gained 7.5 million users globally, according to figures shared by the UK parliament's home affairs committee, and Telegram has gained 25 million". Even the Tesla CEO Elon Musk has jumped into the fray, tweeting "Use Signal" to his more than 42 million followers. This and many other incidents show us that in the age of mass surveillance and information breach, private messaging is becoming more important every day.

As secure messaging protocols are executed on the not-so-secure end-user devices, and because their sessions are long-lived, they aim to guarantee strong security even if secret states and local randomness can be exposed. The most basic security properties, including forward secrecy, can be achieved using standard techniques such as authenticated encryption.

WhatsApp belongs to Facebook, Telegram does not offer encrypted group chats, Signal, Threema and WhatsApp only allow one device per account, or their web applications only communicate via the app. In short, no messenger offers all of the features. In this project, we want to investigate the most popular messaging applications such as WhatsApp, Telegram, Signal, Threema, Zoom and possibly others and see what are their main features that they provide and what can be done to improve them.

Requirements: Prior experience or a strong interest in programming and cryptography.

Interested? Please contact us for more details!

Contact

- Ard Kastrati: kard@ethz.ch, ETZ G61.3
- Karolis Martinkus: martinkus@ethz.ch, ETZ G 60.1

[1] https://www.theguardian.com/technology/2021/jan/24/WhatsApp-loses-millions-of-users-after-terms-update