Security of Instant Messaging

Bachelor or Master Theses

GLOBAL

Supervision: Paul Rösler **Start date:** immediately

DESCRIPTION

There are a lot of open questions regarding the security and reliability of Instant Messengers like

WhatsApp, Signal, iMessage, Telegram, … .

If you are interested in a practical or theoretical analysis of their implementations or protocols, we may find a topic for a theses.

While practical analyses could focus on the new group chat protocol of Signal [1], theoretical analyses may be concerned with modeling or proving the security of protocols [2,3]. A practical work could also focus on the implementation of protocols that have only been published theoretical yet [4]. Combining practice with theory could be achieved by reproducing and validating automatically generated proofs [5,6] with tools like ProVerif [7], CryptoVerif [8], and Tamarin [9].

REQUIREMENTS

Depending on the focus of your desired thesis you should have

- Good knowledge and experience in source code analysis and debugging and
- Good grades in Network Security 1 & 2

or

- Interest in practical aspects of cryptography
- Good grades in Cryptography, Authenticated Key Exchange or other courses of Theory in IT-Security

[1] https://github.com/WhisperSystems/Signal-Android/

[2] https://eprint.iacr.org/2016/1013

[3] http://noiseprotocol.org/

[4] Ask me; it is not published yet ;)

[6] https://eprint.iacr.org/2017/666

[6] https://github.com/Inria-Prosecco/proscript-messaging

[7] http://proverif.inria.fr/

[8] http://cryptoverif.inria.fr/

[9] https://tamarin-prover.github.io/