hgi NDS

Analysis of secure Instant Messenger Protocols regarding Group Communication

Bachelor Thesis

GLOBAL

Supervision: Paul Rösler, Christian Mainka

Start date: immediately

DESCRIPTION

Many current instant messenger applications provide end-to-end encryption between the communicating users in order to protect the confidentiality of their communications. The most prevalent application is What's App: the protocol of What's App bases on Signal, invented by Open Whisper Systems. The security of Signal was analyzed multiple times regarding the key exchange and regarding the confidentiality of user-to-user messages. But since group communications require more than confidentiality in order to provide a trustful communication channel, recent analyses do not suffice to proof the security of the respective group communication protocols.

In this thesis the protocols of current widespread instant messengers shall be analyzed. Consequently the main result of the thesis should be a detailed sequence diagram on all protocols of the analyzed system. Typically the protocols include registration, key distribution and retrieval, direct messaging, group management, group messaging and transmission of multimedia files. An example for the analysis of secure instant messenger protocols can be found in the paper *How Secure is TextSecure?* [1].

We propose to analyze one or more of the following applications (depending on the complexity of the analysis):

Telegram, Wickr Me, Wire, Hoccer, iMessage, …

REQUIREMENTS

- Experience in the respective programming language (if open source)
- Experience in traffic analysis
- Knowledge on protocol security

[1] https://eprint.iacr.org/2014/904.pdf