Motivation

Current email infrastructure is decentralized, but it does not offer end-to-end encryption out of the box. Therefore, anyone processing an email can read its content. Well known extensions for encrypting and signing mails, such as GnuPG and S/MIME are based on a naive use of asymmetric keys. Namely, they do not provide automated ways to distribute keys and leave this bothersome task to the final user. As a result, using these systems require a high level of technical understanding which limits their adoption for the ordinary user.

In recent years, encryption has spread into the messenger area and lead to fully end-to-end encrypted but centralized protocols which allow asynchronous communication between partly offline participants. Although the technology exists, there is no complete and easy to use solution.

Besides, in the spirit of modern cloud-based solution where most participants utilize several devices concurrently with the same account, it should not matter with which device - as long as all of them are trusted - a key or a message is generated. Moreover, all devices should synchronize their knowledge regularly.
Objective Goals

The goal of this thesis is comprehension of present knowledge, evaluation of existing approaches and, derivation of a suitable scheme to provide such a service. The main focus lays on usability and reliability as such a solution needs to work with almost no user interaction to gain wide acceptance. This research project is spread over a period of six months, from its start date. During the course of this master’s thesis, the student is expected to complete the following milestones:

- Explore and evaluate existing technologies, systems and concepts in relation.
- Developing a decentralized, end-to-end encrypted messaging service working with multiple equally authorized end devices.
- Analysis of the solution prosed.
- Implementation of a prototype if the required level of elaboration is reached.
- Explore further possibilities to extend the approach.

Deliverables include the written code with documentation, a project report, and a final presentation.

Prerequisites

- Proficiency in system level programming.
- General understanding of cryptographic protocols.
- Strong interest in system security and privacy aware protocols.

For further information, please contact David Sommer (david.sommer@inf.ethz.ch)

Supervisors

Prof. Dr. Srdjan Ćapkun (ETH Zürich) (capkuns@inf.ethz.ch)
David Sommer (ETH Zürich) (david.sommer@inf.ethz.ch)