



Lab/BA/SA/Group/MA:

Peer-to-Peer Instant Messenger with End-to-End Encryption

Motivation and Informal Description

We all use instant messaging apps like WhatsApp or Skype to communicate with our friends. Unfortunately, most of these apps use a proprietary protocol, which, on the one hand, makes them rather untrustworthy and, on the other hand, forces you to use one specific client. Open alternatives like XMPP (Jabber) are server-based and have a single point of failure. There is no existing solution that uses an open peer-to-peer based protocol.

Only recently people started adding encryption natively into their messengers, also due to the fact that the NSA is eavesdropping on all of us. Most apps still send messages in a way that is easily accessible for anybody with access to the connection. Not to mention that some messaging apps are well-known for having security issues on a regular basis. The few apps trying cope with these issues often implement custom-made cryptography solutions, which usually do not satisfy the high standards requested by cryptographers. And on top of that, those solutions are mostly still server-based.



We think it is about time that this situation changes. Your job is to further improve a prototype messenger developed in previous projects. We already have a peer-to-peer backend and parts of an end-to-end encryption employing the well-established PGP/GnuPG standard such that only the intended recipient is able to read the message. Furthermore, there are existing clients for Android and PC. Depending on the type of thesis, your work could include dealing with malicious nodes that want to delete yet undelivered messages, an efficient and secure implementation of group-messaging, proper handling of offline messages, etc.

Requirements

Good programming skills and some basic knowledge in cryptography. The student(s) should be able to work independently on this topic!

Interested? Please contact us for more details!

Contact

- Philipp Brandes: philipp.brandes@tik.ee.ethz.ch, ETZ G64.2
- Tobias Langner: tobias.langner@tik.ee.ethz.ch, ETZ G61.4