

Status Report: a free Group OTR library

Peer-to-Peer Systems and Security, Summer 2014

Markus Teich Jannik Theiß

June 14, 2014

1 Current project status

First we wrote a simple chat client. We wanted to test our library without having to write a huge plugin for an existing chat application. Our client uses UNIX domain sockets and therefore is limited to chatting on the same machine. This also helps us to develop a sane and usable API for our library, so it can be easily adopted to various chat applications used worldwide.

We also started implementing our library. The basic functions like base64 encoding the messages already works. However the understanding of the cryptographic algorithm used for group key agreement took us some time and we just started to implement it.

2 Open tasks

crypto

Also missing is the documentation of libgotr's API and usage. The key exchange protocol has to be fixed and documented as well.

If we find the time, at the end we want to implement a plugin for a widespread chat application using our libgotr.

3 Finalization plan

3.1 June, 16th to June 22nd

The correct implementation of the group key agreement should take up most of the time in this week. Jannik also has to prepare the first talk.

3.2 June, 23rd to June 29th

By the end of this week the crypto stuff should be done and working. Jannik presents related work and the design of our libgotr on June 26th.

3.3 June, 30th to July 6th

During this week we should fix all remaining errors and bugs known to us and start with the documentation.

3.4 July, 7th to July 13th

3.5 July, 14th to July 15th