Project Proposal: a free Group OTR library

Peer-to-Peer Systems and Security

Summer 2014

Markus Teich, Jannik Theiß

1 Introduction

In recent years instant messaging (IM) gained a lot in popularity. Virtually everyone uses one or more IM solutions (e.g. WhatsApp, Skype, iMessage, Facebook Messenger etc.) for private conversations. Especially the ease of use that comes with this kind of online communication combined with the high availability through the popularity of smartphones makes IM attractive for a broad audience. Also companies have discovered IM as a suitable solution for online business meetings, particularly because it causes no additional costs.

At its heart IM emulates the behavoir of a private conversation held in person. Naturally people expecet their face to face conversations to satisfy several properties. For example for any party that did not participate the conversation the (hopefully) honest word of the participants is the only proof of what was said during the conversation (given that no one recorded it). To be a suitable alternative to face to face conversations IM should also satisfy

these properties. It is also not astonishing that people without a strong knowledge in informatics and/or cryptography already expect their private online conversation to be held under these constraints.

However, the dominant IM solutions do not satisfy all of these properties. Security concerns fueled by the revelation of surveillance activities of government institutions last year have lead to a more wide spread awareness for the need to secure communication over the internet.

2 Motivation

Ideally it should be possible to have secure, face to face like conversations over the internet without additional effort. To properly emulate the security of a face to face meeting, an IM conversation should satisfy the following properties:

- **Authenticity:**
- **Inegrity:**
- **Confidentiality:**
- **Deniability:** [1]

Currently there is no free and open source library for inclusion in existing IM protocols or building new ones that provide these properties.

3 Related Work

mpOTR: Transcript verification only at the end of a session bad? mpOTR: PFS only per session?

[1] Deniability as a property is the direct oposite of what traditional security patterns (e.g. PGP for e-mail) achive. Typically the signature used to achive authenticity also provides a proof of who the author of a message was. On the other hand this property makes such patterns suitable for messages of legal relevance such as contracts or bills.

4 Project Plan

The goal of our project is to implement a free and open source library which is independent of a specific IM client and provides the user with the group OTR functionality proposed in [8]. The existing proof of concept implementation for pidgin serves as reference to our work. We aim to provide the group OTR algorithm under a standardized interface usableby various existing IM clients as well as new IM concepts based on OTR only communications. Further the correct functionality of our library is to be tested with a simple "client". However we unfortunately can not evaluate the cryptographic correctness of the proposed algorithm. This is left to people with more crypto knowledge.

- generalize

References

[1] N. Borisov, I. Goldberg, and E. Brewer. Off-the-record communication, or, why not to use PGP. In *Proceedings of the ACM workshop on Privacy in the electronic society*, WPES '04, 2004.

[2] M. Di Raimondo, R. Gennaro, and H. Krawczyk. Secure off-the-record messaging. In *Proceedings of the ACM workshop on Privacy in the electronic society*, WPES '05, 2005.

[3] C. Alexander and I. Goldberg. Improved User Authentication in Off-the-Record Messaging. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, WPES '07, 2007.

[4] J. Bian, R. Seker, and U. Topaloglu. Off-the-Record Instant Messaging for Group Conversation. In *Proceedings of Information Reuse and Integration*, IRI '07, 2007.

[5] A User Study of Off-the-Record Messaging

[6] Multi-party Off-the-Record Messaging

[7] Secure Communication over Diverse Transports

[8] Improved Group Off-the-Record Messaging