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 smart phones 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 expect their face to face conversations to have 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 computer science 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:** The receiver can be sure about the origin of a message.
- **Integrity:** The receiver can be sure, the message has not been modified after it has been sent.
- **Confidentiality:** No entity other than the participants is able to read the content of the messages.
- **Perfect Forward Secrecy:** An attacker is unable to derive ephemeral key material from disclosed long term keys.
- **Deniability:** [1] No entity is able to prove the authorship of a message to a non participating entity.

For just two chat participants the well known and established libotr can be used to achieve these goals. However, currently there is no free and open source library for inclusion in IM clients that provide these properties for conversations with more than two participants such as IRC channels or XMPP conference rooms. Considering groups wanting to have private conversations

[1] Deniability as a property is the direct opposite of what traditional security patterns (e.g. PGP for e-mail) achieve. Typically the signature used to achieve 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.

such as political parties, business partners or whistle blowers, which are unable to meet in person due to legal, time or monetary restrictions, the need for such a tool is given.

3 Related Work

In 2004 Borisov et al. initially proposed the idea of off-the-record communication(OTR) [1]. The OTR protocol amied at providing the beforementioned properties for chats with two participants. However in 2005 Di Raimondo et al. published a paper in which they revealed several weaknesses in the protocol and also provided solutions to fix these [2]. In 2007 Alexander et al. attendet the problem of exchanging public keys

[3]: smp, real life shared secret [4]: virtual server mpOTR: Transcript verification only at the end of a session bad? mpOTR: PFS only per session?

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 usable by 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 the evaluation of the cryptographic correctness of the proposed algorithm is not the subject of our project.

- 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] R. Stedman, K. Yoshida, and I. Goldberg. A User Study of Off-the-Record Messaging. In *Proceedings of the Symposium On Usable Privacy and Security*, SOUPS '07, 2008.

[6] I. Goldberg, B. Ustaoğlu, M. D. Van Gundy, and H. Chen Multi-party Off-the-Record Messaging. In *Proceedings of the ACM Conference on Computer and communications security*, CCS '09, 2009.

[7] Secure Communication over Diverse Transports

[8] Improved Group Off-the-Record Messaging