Group OTR

Peer-to-Peer Systems and Security

Summer 2014

1 Introduction

2 Motivation

nsa...

3 Related Work

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

4 Project Plan

The goal of our work 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 planned improvements. 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 we unfortunately can not evaluate the cryptographic correctness of the proposed algorithm. This is left to people with more crypto knowledge.

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