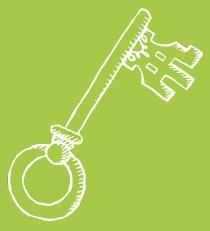

Zero-Knowledge Group Membership: Hiding communication patters in MLS

Advisor: **Lena Heimberger**

Motivation

The thesis focusses on how to deploy metadata-hiding group messaging in a client/server setting. The thesis will focus on the MLS protocol, which enables more efficient group messaging while avoiding secure 1:1 channels. More concretely, in the standard MLS protocol every message is wrapped in a struct that includes a sender index and a signature. While the sender index is encrypted, traffic analysis from a server may still be feasible. The thesis splits into the following parts:

In your thesis, you will

- Discuss the possible limitations (even security vulnerabilities?) and scope of improvement in the existing protocols.
- Implement your ideas and discuss the results.

Contact me to discuss further about the topic specifics and your personal interest.

Goals and Tasks

Analyzing the feasability of traffic analysis Formally model the threat of traffic analysis by a server and look at the security guarantees.

Reading about existing proposals from the literature You will start by reading about Clarion, a system which uses shuffling protocols to enable metadata-hiding comunication, and see how it could be applied to MLS.

Design and implement a solution for MLS Based on your literature research, you will design, analyze and implement a prototype of your protocol.

Literature

- R. Barnes et al.
  The Messaging Layer Security (MLS) Protocol
  RFC 9420 2023
  doi:10.17487/RFC9420
  https://www.rfc-editor.org/info/rfc9420
- S. Eskandarian and D. Boneh
  Clarion: Anonymous Communication from Multiparty Shuffling Protocols.
  NDSS

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Read https://heimberger.xyz/supervision.html#apply.

Advisor Contact

lena.heimberger@tugraz.at