Topics for Master Students

Advisor: **Edona Fasllija, Lena Heimberger**

Motivation

Very recently, modern messengers started to deploy key transparency to ensure the cryptographic keys are publicly verifiable and resistant to tampering, making meddler-in-the-middle attacks significantly harder. A method to decentralize protocols like key transparency is *gossip*, where information is spread across the network by the parties participating instead of a central entity. In the case of messaging, these parties are the messenger users. Your task is to implement a proof-of-concept key transparency protocol in an existing messenger, e.g. Signal.

Literature

- Edona Fasllija
- Lena Heimberger

Courses & Deliverables

- ☑ **Master Project**
  - Project code
  - Report
  - Presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **application security, mobile security, privacy, messengers, identity, cryptography**

Advisor Contact

edona.fasllija@tugraz.at,lena.heimberger@tugraz.at