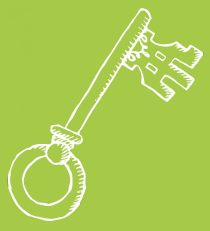

Anonymous KT State Lookups in Deployed Messengers

Advisor: **Lena Heimberger**

Motivation

Key Transparency (KT) servers may serve conflicting views to different parties, enabling man-in-the-middle attacks on end-to-end encrypted messengers. A possible detection method is *anonymous state retrieval*, which tries to detect differences between the KT states served to different users. Rather than expensive cryptographic approaches like Private Information Retrieval (PIR), we observe that a cheap mechanism for state retrieval is available: account creation. A fresh account is likely to be served the locally-correct KT state, and since the server cannot reliably distinguish a legitimate new signup from one created purely to probe KT state, particularly when performed over a network that does not trivially identify the user, such as WiFi, comparing the KT view of a fresh account against an existing account can detect a partition.

The core questions are:

- How hard is it to create a second account?
- What network-level signals does the server have to distinguish a probe account from a genuine one?
- Does the messenger's account model allow cross-account KT comparison at all?

Some messengers, like Signal, WhatsApp, and iMessage, require phone numbers for registration; others may require device attestation. Additional anti-abuse measures such as rate limiting will also affect whether this approach is viable in practice. The thesis aims to characterize the threat model under which anonymous state lookup via account creation is sound, identify which deployed systems it applies to, and assess whether it can be integrated into existing gossip-based KT verification schemes such as those discussed in the context of MINGLE [3].

Literature

- B. McMillion
  Key Transparency Architecture
  Internet-Draft
  Internet Engineering Task Force, 2026
  https://datatracker.ietf.org/doc/draft-ietf-keytrans-architecture/08/
- T. K. Yadav et al.
  Automatic Detection of Fake Key Attacks in Secure Messaging
  2022
  https://arxiv.org/abs/2210.09940
- E. Fasllija, L. Heimberger, and K. Paul
  Signal and Ready to MINGLE: In-Band Gossip for Key Transparency Split-View Detection in E2EE Messengers
  Manuscript 2026

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.