



Protecting Against Split View Attacks in Transparency Systems





Advisor: **Edona Faslilija**

Motivation

Transparency Systems, such as Certificate Transparency or Key Transparency, are designed to provide accountability and verifiability of data. However, they are vulnerable to split-view attacks, where adversaries manipulate different versions of data to deceive participants by providing inconsistent views of the system. This thesis focuses on the development of tools and mechanisms to detect, mitigate, and prevent split-view attacks in transparency systems.

As part of this project, you explore cryptographic techniques, such as consistency proofs and data structures, to ensure all participants view the same data. Additionally, the thesis evaluates the effectiveness of consistency protocols and distributed monitoring frameworks (witnessing) to maintain global consistency across the system. Through theoretical analysis and practical implementation, we demonstrate how these tools can enhance the robustness and security of transparency systems, ensuring integrity even in adversarial environments.

Goals and Tasks

-  Get familiar with related literature
-  Design and implement a non-equivocation protocol for Key Transparency
-  Evaluate the compatibility and accuracy of your solution
-  Write down your findings

Literature

- > [S. Meiklejohn et al.](#)
Think global, act local: Gossip and client audits in verifiable data structures
[arXiv preprint arXiv:2011.04551 2020](#)
- > [J. Brorsson et al.](#)
Consistency-or-Die: Consistency for Key Transparency
[Cryptology ePrint Archive 2024](#)

Courses & Deliverables

- Master Project**
Project code
Report
Presentation

– OR –
- Master's Thesis + DiplomandInnenseminar (CS)**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Programming skills (Go, Rust)

Advisor Contact

edona.faslilija@tugraz.at