When Transparency Fails: Lessons from CT Incidents

Advisor: **Edona Fasllija**

Motivation

Despite Certificate Transparency (CT) being designed to make certificate issuance auditable, there have been real-world CT-related failures that undermined trust, such as the recent misissuance of certificates for 1.1.1.1 by Fina CA without Cloudflare's authorization. These incidents reveal gaps in monitoring, alerting, inclusion verification, and root-store trust policies. In this study, you will identify weaknesses in the ecosystem through real incidents and propose potential improvements.

Steps

- Identify and document a few CT-failure incidents (e.g. 1.1.1.1 misissuance, past CA misissuances)
- Analyze where CT and its ecosystem failed (e.g. lack of inclusion checks by clients, monitoring/alerting gaps, root store trust mismatches). Compare across cases to identify recurring patterns.
- Propose potential mitigations

Literature

- J. Abley et al.
  Addressing the Unauthorized Issuance of Multiple TLS Certificates for 1.1.1.1
  Cloudflare Blog 2025
  https://blog.cloudflare.com/unauthorized-issuance-of-certificates-for-1-1-1-1/

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at ISEC (highly recommended), check the full list of topics:

https://www.isec.tugraz.at/bachelor-thesis

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **WebPKI security**

Advisor Contact

edona.fasllija@tugraz.at