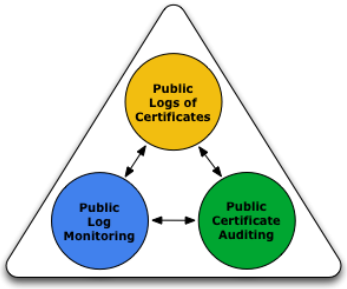
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

IDP

Performant Certificate Transparency Monitoring

Motivation

Certificate Transparency (CT) [1] makes communications in the TLS ecosystem more trustworthy by publicly logging X.509 certificates and thus allowing to detect mis-issued certificates more easily. The certificates are kept in so-called CT logs. Domain owners and other parties can monitor those public logs for mis-issued certificates and take appropriate actions, e.g. revoking the certificate. This makes attacks on TLS users (e.g. man-in-the-middle) harder to carry out.



CT ecosystem [1]

In addition to the increase in trustworthiness, the data from CT logs provides valuable insight into the TLS ecosystem. For example, the adoption of new security standards or the market share of Certificate Authorities can be analyzed.
Your task is to implement a continously running service that retrieves data from CT logs and performs automatic analyses on this data.

[1] https://www.certificate-transparency.org/what-is-ct

Your Task

- Familiarize with core concepts of CT (Merkle Trees, . . .)
- Implement a continously running service that retrieves data from CT logs
- Implement periodically running analyses on the CT data

Requirements

- Experience with Linux
- Experience with Go and Bash
- Beneficial to have experience with PostgreSQL

Contact

Max Helm helm@net.in.tum.de
Patrick Sattler sattler@net.in.tum.de