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

Thesis B.Sc. Thesis M.Sc. IDP

Evaluating TLS Certificate Transparency Logs using Active Scans

Motivation

TLS (previously known as SSL) is a fundamental security protocol in the Internet. It provides security guarantees in protocols for web-browsing (HTTPS), email (IMAPS, SMTPS) and beyond.

https://www.certificate-transparency.org/

Due to the design of the TLS PKI every certificate authority (CA) can issue certificates for every domain. This leaves the door open to targeted Man-in-the-Middle attacks by compromising a single CA. To detect these targeted Man-in-the-Middle attacks the *Certificate Transparency* (CT) protocol is being developed in the IETF [a]. Certificate Transparency allows any client to query public CT logs to identify suspicious certificates.

In this thesis you will build a scanner which downloads certificates from CT logs. The goal is to run this CT log scanner as a contiuously running service in order to detect suspicious certificates. You will then evaluate the downloaded certificates and compare them against certificates obtained from active Internet-wide scans as CT log certificates have been found to differ from active scan certificates [b].

[a] B. Laurie et al.: *RFC 6962: Certificate Transparency.* June 2013.
[b] Vandersloot et al.: *Towards a Complete View of the Certificate Ecosystem.* IMC 2016.

Your Task

- Research previous work on CT logs
- Develop new scanner or extend existing one to scan CT logs obtaining new certificates
- Conduct scans, evaluate the results and compare with results from active Internet-wide scans
- Set up regular scanning service

Contact

Oliver Gasser gasser@net.in.tum.de
Benjamin Hof hof@net.in.tum.de

http://go.tum.de/306574