Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Towards Trustless Certificate Authorities

Motivation

X.509 certificates are important building blocks of network security. They provide a secure and trusted method for authenticating entities and enable the establishment of secure TLS/SSL channels between them. Certificates are issued and signed by Certificate Authorities (CAs) after the CA has verified the identity of the certificate holder and other information contained in the certificate, like a Web server's URL. However, this process is often cumbersome and error prone, as it requires the involvement of human actors. Furthermore, the "traditional approach" requires a high level of trust in the CA by owners and users of certificates. Finally, a Web server certificate costs around 100 EUR per year. An alternative to "traditional" CA is *Let's Encrypt*[a] which automatically issues so-called domain validated (DV) certificates for free to Web servers using the *ACME* protocol.

In this thesis we want to research how we can optimize Let's Encrypt in a way that it needs to be trusted less. The approach that we want to follow is to investigate how the Let's Encrypt back end can be distributed. This means, multiple, independent back ends exist that collaboratively issue the certificate. The result is, that if an individual back end is compromized or tricked by an attacker, no bogus but valid looking certificate is issued. The required distribution of the signing functionality can be achieved by using so called threshold signing systems. The key idea is that each back end will only be able to issue a partial signature of the requested certificate. Only if t out of n back ends have independently performed the DV and contributed their partial signature, the certificate can be issued.

[a] https://letsencrypt.org/how-it-works/

Your Tasks

- Analyze Let's Encrypt, the security properties it offers and lacks
- Get familiar with the implementation and set up your own CA
- Design and implement an distributed signing process for Let's Encrypt
- Evaluate the improved system by analyzing its new security properties

Prerequisites

- Knowledge of network security basics (crypto basics, TLS, CA, ACME, ...)

Contact

Kilian Glas	glas@net.in.tum.de
Dr. Holger Kinkelin	kinkelin@net.in.tum.de
Filip Rezabek	rezabek@net.in.tum.de