Thesis B.Sc.

Thesis M.Sc.

Guided Research

CAA Records
— Can you trick the CAs?

Motivation

Certification Authority Authorization (CAA) is a new DNS record type that allows domain owners to control which Certificate Authoritys (CAs) are allowed to issue certificates for a domain.

The CA/Browser forum has agreed that CAs must check and respect a domain's CAA record when issueing new certifacates. This new agreements becomes effective on September 9th, 2017.

This thesis aims to investigate the details of how CAs check CAA records, and investigates whether and in which circumstances misissuance can be triggered. A different angle, evaluating the deployment of CAA records in the Internet, can be discussed.

Previous knowledge on DNS, DNSSec, and the Web PKI is useful but not required.

Your Task

This is a fun and practical thesis to explore and empirically assess a new security mechanism in the Internet. Your tasks will include:

- Set up a test domain and its name servers
- Set various different CAA records
- Try to obtain certificates from CAs
- Investigate process, technical details of DNS lookup, and effect on certificate issuance

Contact

Quirin Scheitle   scheitle@net.in.tum.de
Oliver Gasser   gasser@net.in.tum.de
Ralph Holz   holz@net.in.tum.de
Johannes Naab   naab@net.in.tum.de