Delegated Credentials Implementation

Advisor: **Lukas Alber**

Motivation

CDNs and TLS play a significant role in today's world. Combining the end-to-end security of Transport Layer Security (TLS) with Content Delivery Networks (CDNs) while ensuring the authenticity of connections results in a challenging delegation problem. When CDN servers provide content, they have to authenticate themselves as the origin server to establish a valid end-to-end TLS connection with the client. In standard TLS, the latter requires access to the secret key of the server. To curb this problem, multiple workarounds exist to realize a delegation of the authentication.

Delegated Credentials [1] is one approach to achieve authentication by delegation. Backed by Facebook, Cloudflare, and Mozilla, it has a great chance to be standardized soon.

Goals and Tasks

In this project, we want to extend the IAIK's TLS library by Delegated Credential. For that, we need to implement a TLS extension, an X.509 certificate extension, and some further logic. The goal is to present a working showcase of the Delegated Credentials at the end of the journey.

- Understand the CDN & TLS context
- Read on Delegated Credentials and competitors
- Implement an extension to the IAIK's TLS library
- Implement a demo showcase of your work

For a short overview read the Cloudflare Blog [2].

Literature

- R. Barnes et al.
  Delegated Credentials for TLS
  Internet-Draft
  IETF, June 2020
  https://datatracker.ietf.org/doc/html/draft-ietf-tls-subcerts-09
- Cloudflare
  Delegated Credentials for TLS
  https://blog.cloudflare.com/keyless-delegation/

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Java programming
- Basic understanding of TLS is beneficial

Advisor / Contact

lukas.alber@iaik.tugraz.at