Analyzing the local Citizen Card Environment

Advisor: **Jakob Heher and Stefan More**

Motivation

These days, the most common form of eGovernment authentication is the "ID Austria". But – before the ID Austria, before even the Handysignatur, there was the Citizen Card. It was a smart card-based authentication model which never really took off; it required users to buy a smart card reader device, and install specialized software. Eventually, it was phased out in favor of the far more usable mobile phone based models of today.

However, the Citizen Card never went away, and is still seeing active use in public sector administrations. In this project, want to take a look at the local Citizen Card Environment, which is the software that users install for communication with the smart card. Among other things, this software also listens for HTTP connections on a local loopback address. This allows other applications to request signatures from the Citizen Card.

We would like to look at this local application, and in particular on the functionality it offers via HTTP. What safeguards are there? Can we access the application from arbitrary web pages? If yes, what does this let us do?

Goals and Tasks

- Learn how the protocols underlying CCEs work
- Analyze a particular common CCE implementation
- Find vulnerabilities & exploit them

Relics from a different time.

Literature

- A. Hollosi et al.
  Die österreichische Bürgerkarte
  https://sl.eid.egiz.gv.at/

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Experience with Reverse Engineering (C++)

Advisor Contact

jakob.heher@iaik.tugraz.at