

Introduction to Scientific Working (ISW): Wallet & eID

Advisor: **Secure Applications area**

Motivation

ISEC's "Secure Applications Area" consists of multiple teams, working in the areas of web security, identity and trust management, access control, mobile security, computation on encrypted data, and other fields of applied security and privacy.

A strong focus is **identity management** in the context of eGovernment, e.g., identity wallets and federated identity systems (i.e., ID Austria and eIDAS). Our interest is in how to build these systems in a way that maximizes user **privacy**.

Additionally, we look into techniques to increase user's trust in cryptographic systems (e.g., **key transparency**).

Another focus is **mobile security**. We are interested in innovations that assist application developers in creating secure services, even if they are not security experts themselves.

Example Topics

- When checking identity documents, humans often compare faces with pictures. How reliable are people with unfamiliar face matching ? Are computers better?
  jakob.heher@tugraz.at
- Study mechanisms that prevent identity wallets from communicating with malicious service providers.
  smore@tugraz.at
- How can a server trust an app that it is communicating with? What are reasons and disadvantages of app attestation ? What are alternatives that enable better user freedom?
  smore@tugraz.at

Literature

- Jakob Heher
- Edona Fasllija
- Florian Draschbacher
- Stefan More
- Simon Gutschlhofer
- Dmytro Shvets
- Lukas Treffner
- research@a-sit.at

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in our topics, motivation, communication skills, and some experence with involved techniques.

Advisor Contact

your.supervisor@tugraz.at