Topics for Master Students

Advisor: **Secure Applications area**

Motivation

IAIK'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.

We also research **privacy-preserving computation** techniques like multi-party computation (MPC) and federated learning (FedL).

Example Topics

- What is the implication of quantum computers and the migration to post-quantum crypto on electronic identities?
- How do mobile phone networks combat caller ID spoofing?

Literature

- Jakob Heher
- Edona Fasllija
- Florian Draschbacher
- Stefan More
- Karl Koch
- research@a-sit.at

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
+ DiplomandInnenseminar (CS)
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in **application security, mobile security, privacy, identity management, ...**

Advisor Contact

your.supervisor@iaik.tugraz.at