

Introduction to Scientific Working (ISW): AI & Agents

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

- Analyze and understand Apple's Private Cloud Compute and similar systems.
  smore@tugraz.at
- A security harness is used by AI agents to find vulnerabilities in your codebase. How is a security harness working?
  smore@tugraz.at
- Do you trust your local coding agent? How can you prevent it from doing bad stuff on your computer? Let's study sandboxing approaches and mechanisms!
  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