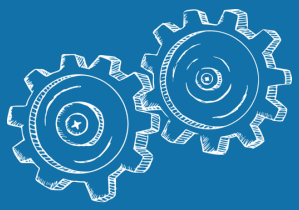

Mobile Application Fingerprinting via Physical Side-Channels

Advisor: **Hannes Weissteiner**

Motivation

Smartphones provide access to many sensors (accelerometer, gyroscope, microphone, light sensor, etc.). Different applications may cause different sensor readings, allowing to fingerprint which application the user is currently using. Some sensors may leak even more information about the user or their environment, such as location or movement patterns.

This project is fairly open, and aims to explore different sensors and their potential to leak information.

Goals and Tasks

- Learn about smartphone sensors and prior work on device- and application fingerprinting.
- Design small experiments to test which sensors leak identifying patterns.
- Build a prototype (app or website) to collect and analyze sensor data.
- Train a machine learning model on the collected data to classify applications

Literature

- Y. Chen et al.
  POWERFUL: Mobile app fingerprinting via power analysis
  INFOCOM
- N. Matyunin et al.
  MagneticSpy: Exploiting Magnetometer in Mobile Devices for Website and Application Fingerprinting
  ACM Workshop on Privacy in the Electronic Society

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

- Basic knowledge of mobile systems
- Some programming experience (ideally mobile or JavaScript)
- Interest in system security

Advisor Contact

hannes.weissteiner@tugraz.at