ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

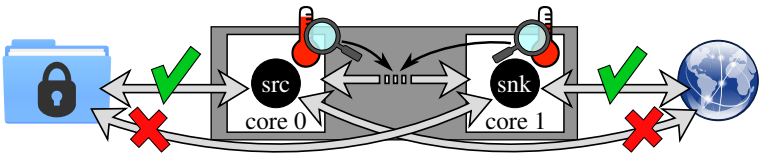
TIK Institut für Technische Informatik und Kommunikationsnetze
Computer Engineering and Networks Laboratory

Prof. L. Thiele

Semester/Group Thesis:

Un-Covert - Evaluating Physical Security Leaks

Context



Mobile devices (smartphones, tablets, ...) have evolved into general purpose computing devices that can handle multiple applications, which might have access to sensitive information, for example mobile banking or health data. Today's mobile devices leverage multi-processor systems on chip (MPSoCs) that put several components (cores, caches, accelerators, ...) onto the same piece of silicon.

While various sandboxing and segregations techniques exist to ensure the security of sensitive information, the applications still share the physical silicon of the MPSoC. We are studying how attackers could leverage this physical property to leak information from an infected authorized app to an unauthorized one, which is otherwise isolated at the software and architecture level. In particular, we are trying to demonstrate how applications can communicate through *covert channels* established through temperature and power draw measurements. Our goal is to evaluate the quality of the transmission, learn to understand the channel, and find its limits.

Tasks

The student will extend our work focusing on different representative mobile platforms (e.g. a Samsung Galaxy S5 smartphone). The main tasks to complete the thesis will be:

- Get to know the existing measurement framework (Matlab, C, C++, UNIX Shell Scripts)
- Port the framework to Android
- Build a case study to demonstrate successful communication through the targeted covert channels
- Run the case study on the target devices and demonstrate a sensitive data leak

Requirements / Skills

- C / C++ / Java development / UNIX Shell
- Familiarity with system programming for Linux (Script Languages)
- Data Analysis (MATLAB or similar)
- Basic Android application programming
- Curiosity and interest in security and in systems research

Interested? Please have a look at http://www.tec.ethz.ch/research.html and contact us for more details!

Contacts

- Philipp Miedl: philipp.miedl@tik.ee.ethz.ch, ETZ G76