Practical Cache Side-Channel on Embedded SoC Platforms (AISEC)

Caches are indispensable hardware components of powerful, modern processors. However, their timing characteristics form a challenge to the implementation of secure systems: As they are used concurrently by different processes, they form a side-channel, leaking information about memory access patterns. In addition, misusing cache timings as a deliberate covert-channel between two malicious processes can threaten security, too.

The threat of cache based side-channel attacks has been known and demonstrated for many years. With the increasing performance and complexity of processors throughout all domains, they become more relevant in the domain of embedded SoCs. We want to gain deeper insight in the practical feasibility of cache side-channel attacks on embedded SoCs.

The aim of this work is to help us set up a cache based covert-channel on a modern embedded SoC platform. Therefore we will develop software, which uses the cache to form a covert-channel. Afterwards we will determine the characteristics and reliability of the covert-channel.

Prerequisites

The following skills are valuable for the execution of the project:

* Proficiency in programming in C
* Basic experience with assembly programming (preferably ARM)
* Basic knowledge about cache architectures (e.g., from a university lecture)
* Basic experience with embedded Linux (e.g., Raspberry Pi, BeagleBone, buildroot)
* Basic experience with git
* Basic knowledge in programming in Python3

Contact

If you are interested in this particular HiWi position, please send an email with

* a short CV,
* a short cover letter, and
* your last grading sheet.

If you are interested in working on cache side-channels in some other way, e.g., as research internship (“Forschungspraxis”), please feel free to contact me via email as well.

Kilian Zinnecker, kilian.zinnecker@aisec.fraunhofer.de

Advisors

Georg Sigl
Kilian Zinnecker (Fraunhofer AISEC)