Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Bachelor's Thesis

Microarchitectural Effects in Sub-Sampled Indirect Side Channels

Despite any theoretical strength a cryptographics algorithm might offer, a real-world application can only be as good as the eventual implementation. For example, side channel leakage is a common problem: unless particular care is taken during the implementation, any computation running on real hardware leaks information about the processed secrets. Common examples include timing side channels, where the execution time depends on secret bits, or power side channels, where e.g. a CPU's power draw depends on the processed data.

Often, these side channels are governed by a complex interplay of subcomponents and -circuits within the device. However, in most cases, very simple models for the exploitable signals' data dependencies are sufficient to mount side-channel attacks. For example, the most common power side channel attack merely correlates the power trace with the secret's hamming weight.

On some cases, only limited data is available and an attack's prospects might benefit from a better understanding of the leakage's underlying principles. When power traces are only available with a comparatively low sample rate (i.e. subsampled) or the system's power draw can only be observed indirectly, the suboptimal data might be compensated by better modelling of the secret dependencies.

The aim of this work is a structured exploration of the observable leakage of different instructions when executed on a microcontroller. Measurements on real hardware will be carried out, which can then help create better models for the leakage's data dependency.

Prerequisites

Necessary: Experience programming in Python
Necessary: Experience programming microcontrollers in assembly (preferrably ARM Cortex-M)
Optional: Basic understanding of cryptographics algorithms and side channel attacks

This work can either be conducted in German or in English. I am happy to provide more details and answer your questions upon request.

Contact

If you are interested in this work, please contact me via email with a short CV and grade report. We will then arrange a short meeting where we can discuss the details.

Jonas Ruchti, M.Sc.
Technical University of Munich, Chair of Security in Information Technology
Room N1014
E-Mail: j.ruchti@tum.de

Advisors

Jonas Ruchti