Undocumented CPU Behavior

Advisor(s): Daniel Gruss and Clémentine Maurice

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Modern CPUs are huge and overloaded with backwards compatibility and features that are not publicly documented. We want to investigate undocumented CPU behavior.
In the past few years there has been a lot of effort in reverse engineering features of the CPU. Such undocumented CPU behavior can undermine software security directly or indirectly. We want to move these reverse engineering efforts to the next layer by automatically detecting undocumented CPU behavior in a large scale.
The aim of this project is to analyze CPU behavior by running program variants and measuring differences.

Goals and Tasks

- Get familiar with the state of the art
- Develop tools to analyze CPU behavior
- Evaluate results from the CPU analysis

Literature

- D. Gruss, C. Maurice, and S. Mangard
  Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript
  DIMVA'16

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- C programming

Advisor / Contact

daniel.gruss@iaik.tugraz.at