Exploiting ARM Performance Monitors

Advisor(s): Raphael Spreitzer

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

Motivation

Cache attacks have been shown to represent powerful side-channel attacks. By exploiting the different access times within the memory hierarchy, an attacker can break cryptographic implementations and also infer fine-grained information about the user's interaction with the smartphone.

State-of-the-art cache attacks rely on timing information, e.g., based on the cycle counter register. However, ARM platforms also feature other performance monitors, for example, a register keeping track of the number of cache hits and cache misses. Such a metric is perfectly suitable for cache attacks and might help to improve state-of-the-art cache attacks.

The aim of this project is to investigate the ARM performance monitors regarding their applicability for cache attacks and to launch cache attacks, e.g., against scrypt.

Goals and Tasks

- Get familiar with cache attacks
- Investigate ARM performance monitors
- Implement an attack

Possible target device

Literature

- D. Gruß, R. Spreitzer, and S. Mangard
  Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches
  USENIX Security 2015
- M. Lipp et al.
  ARMageddon: Cache Attacks on Mobile Devices
  USENIX Security 2016

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

- Interest in cache attacks
- Programming C/C++ and Java

Advisor / Contact

raphael.spreitzer@iaik.tugraz.at