Karlsruhe Institute of Technology

Practical Introduction to Hardware Security

Lab Course 1: Introduction

Instructors: Mehdi Tahoori, Dennis Gnad, Jonas Krautter

INSTITUTE OF COMPUTER ENGINEERING (ITEC) – CHAIR FOR DEPENDABLE NANO COMPUTING (CDNC)

Acknowledgement for Lab Tasks

- Some of the lab experiments are based on joint research with Ruhr-University Bochum

Organization

- Dynamically organized
  - After initial more basic tasks
  - Later students can be involved in deciding which task
    - For example: Power Analysis, or
    - Fault Attacks
- Partially project or task based
  - Tasks are narrowed down to a core element
    - e.g. filling an important gap in code, developing components of a larger framework
  - Projects need more involvement
    - e.g. also read up on a method by yourself

Module/Exam Organization

- Important: Sign up within first few weeks
  - Please check the online campus system on the actual deadline until which you need to sign-up
- Slots and FPGA boards are limited
  - First come, first serve (based on sign-up)
    - Erasmus/Exchange/other Faculty: Contact us when you can not sign-up online
- Lab+Lecture are a single module/mark together
  - Labs are checked during the Semester
  - Final exam includes everything from lab and lecture

Hardware and Organization

- FPGA platforms for most experimentations and practices
  - Implementation on both Verilog (hardware description language) and software codes
  - The platforms can be borrowed
    - You need to sign some document
    - Legal binding that you have to bring the board back
- Computers
  - You can use those in our lab (please ask for an account)
  - We recommend you use your notebook
- We only support Linux
  - Windows can work (just python and fpga tools are needed)
  - Linux VM might be of use
    - Try Ubuntu LTS releases!
- Depending on your interest, we might be able to discuss topics beyond what is planned until now
  - Just let us know your idea!

Overview of Course Content

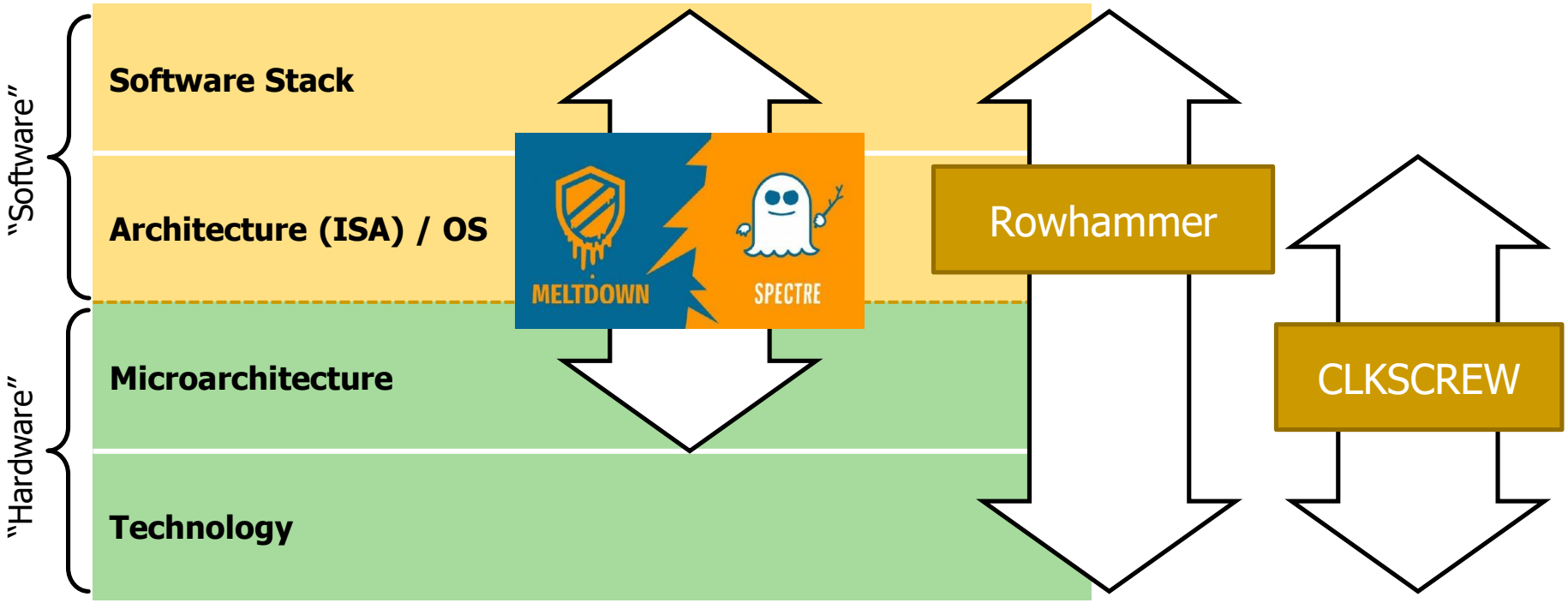
- Hardware security primitives (at least one of)
  - Physically Unclonable Functions (PUF),
  - True Random Number Generators (TRNG)
- Hardware Implementation of encryption modules (AES)
- At least one of:
  - Passive Attack with power side channel (on AES)
  - Active fault attack (on simple circuits, if feasible also on AES)

(Some) Lab Goals

- Extended view on security
  - Mathematically proven vs. secure in implementation
- Primitives for specific tasks in secure hardware
  - Used in smartcards, etc.
  - Used in dedicated security chips
  - Hardware implementation of common algorithms

Some of the recent developments..

- Software-involved, but not software-only breaches
- Increasingly interesting to attackers
  - Algorithmic security is very high
  - Attacks a system from its fundaments (below OS level)



→ Power Analysis might not be local!

- Increasingly amount of physical attacks can also be performed through software “remotely”
  - Even more interest in HW security!
- …
- Some methods used here are directly based on recent research results