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

Forschungspraxis

# Fuzzing of the Accelerator Coherency Port on Zynq Ultrascale+

**Description**

FGPA-SoC combines a FPGA together with high performance processing units. On the Xilinx Zynq Ultrascale+, the processing units are grouped together inside a Processing System (PS). The reconfigurable logic can access the memory and some peripherals of the PS via dedicated interfaces. In previous works, these interfaces have been used to mount powerful attacks from the reconfigurable logic on the external memory [1,2]. These two works can be extended if an attacker knows which systems components are reachable from these interfaces. This is however not fully documented inside the documentation provided by the manufacturer.

The goal of this research project is to developp a fuzzing framework for the Accelerator Coherency Port (ACP) on the Zynq Ultrascale+. This framework should establish the list of system components reachable from the ACP. The knowledge obtained from this framework could then help to develop attacks scenario from the reconfigurable logic on components contained inside the PS.

**References**

[1] N.Jacob et al., How to Break Secure Boot on FPGA SoCs through Malicious Hardware, CHES 2017

[2] M.Gross et al., Breaking TrustZone Memory Isolation through Malicious Hardware on a Modern FPGA-SoC, ASHES 2019

## Prerequisites

- Good knowledge in VHDL/Verilog and Python
- Knowledge in computer architecture preferred
- Previous experience with Xilinx FPGA-SoCs (Zynq 7000 or Zynq Ultrascale+) preferred

## Contact

Mathieu Gross M.Sc.

Technical University of Munich, Chair of Security in Information Technology

Room N1008, Email: mathieu.gross@tum.de

## Advisors

Mathieu Gross