CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

HiWi Position –Prototyping of Remote side-channel Attacks on FPGAs and Defenses

Background

Currently cloud service providers offer Field Programmable Gate Arrays (FPGAs) to users to implement their hardware-based accelerators or Intellectual Property (IP) for better performance. The FPGAs in cloud are envisioned to be shared among several users. Nevertheless, remote power side-channel and fault-injection attacks against shared FPGAs in the cloud are serious threats, since these attacks require neither physical access to the FPGAs nor expensive equipment to be launched. The only requirement of such attacks is that both victim's logic and attacker's logic reside in the same physical FPGA fabric, i.e., the attacker architects malicious logic that co-resides with the victim logic on the same FPGA. Several attacks have been demonstrated in the literature to reveal secret keys or confidential information of a victim user. State-of-art defenses are failing to prevent such attacks without violating the confidentiality of users' IP. One such project involves architecting new defense that prevents fault-injection attacks from corrupting victim's data while also protecting the confidentiality of users' IP.

Tasks

The tasks required involve 1) implementing/prototyping the new defense on an FPGA, 2) evaluating the defense against state-of-the-art remote fault-injection attacks, and 3) evaluating the overhead of the defense (performance and area).

Position

- Available immediately
- Duration: 3-months

Requirements

- Verilog and/or VHDL knowledge and basic digital design and integration
- Hands-on FPGA experience
- Hands-on Xilinx Vivado Synthesis toolchain and RTL simulation experience
- Familiar with microprogramming for Xilinx microcontrollers (Picoblaze)

Contact

Please send your application (incl. CV and certificate(s)) via email to:

Shaza Zeitouni
shaza.zeitouni@trust.tu-darmstadt.de

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

October, 2019