Security Issues in Hardware/Firmware interaction – Can a formal analysis of (just) the hardware help?

Johannes Müller, Technical University Kaiserslautern, DE

Abstract

This talk describes a formal approach to verify hardware security based on hardware property checking at the register-transfer level (RTL). The approach is based on checking uniqueness of program execution with respect to confidential information. It is therefore called Unique Program Execution Checking (UPEC). UPEC can be used to systematically detect all vulnerabilities to microarchitectural side channels as well as to explicit functional leakages. We summarize results obtained for several open-source RISC-V processors, including Rocketchip and Boom. We then report on our current research activities extending UPEC to detecting security issues in the functionality of hardware/firmware interaction. We present preliminary results for this class of security vulnerabilities at the example of Pulpissimo and sketch future research directions.

Biography

 Johannes Müller received his Dipl.-Ing. degree in Computer Engineering at TU Kaiserslautern in 2018. He is currently pursuing a Dr.-Ing. degree at the chair of Electronic Design Automation, TU Kaiserslautern. His research interests include Hardware Security and Formal Verification methods.