Mike Mishal

mmisha2

Report 3

02/23/2019

Papers Read:

1. Virtualized Execution and management of hardware tasks on a hybrid ARM-FPGA platform

I read this paper to have a better understanding of hybrid platforms and the interactions between Processing System and Programmable Logic.

This paper includes a full design of the virtual execution environment that includes hardware, software and state machines for context switching.

1. How TrustZone could be bypassed: Side-Channel Attacks on a modern System-on-Chip

This paper shows how Arm TrustZone doesn’t protect against Electromagnetic Analyses (EMA). The application that they measure runs on bare-metal without OS. No context switching while measuring computation. 70 hours to perform the attack. They suggest new leakage model for modern SoC as the EM leakage is directly linked to a value instead of Hamming weight.

Papers to Read:

1. Power Analysis attacks and countermeasures
2. TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices
3. Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES 256-GCM via GPU-based analysis

Current Interest:

Differential power analysis attacks on ARM protected world in FPGA-CPU systems. Can FPGA be used to synchronize the operations for better analysis and faster attacks?