Mike Mishal

mmisha2

Report 3

02/11/2019

Papers Read:

1. FPGA-Based Remote Power Side-Channel Attacks

This paper is extremely interesting. It demonstrates remote power side-channel attacks for systems with integrated FPGA. On-Chip power monitor using programmable logic on an FPGA can both allow to measure dynamic power consumption and allow remote access to the data. They show an FPGA-FPGA attacks as well as FPGA-CPU attacks.

The attacks and research are on FPGAs and CPUs that have a limited type of security. It doesn’t include any information about what would happen if ARM security technology is deployed. Only basic power protection (timing-channel protection schemes with delays outputs) that can be easily filtered with a few cycles.

1. Rendering Insecure: GPU side channel attacks are practical

This paper shows that GPU side channel attacks using performance counters and resource tracking API. Parallelism and resource sharing in GPUs are what makes these attacks a bit different compared to CPUs. Reading this paper shows another example of how side channeling attacks works for GPUs but my interest is in integrated systems.

These attacks require colocation of attackers and victims in the resource space.

Papers to Read:

1. Power Analysis attacks and countermeasures
2. TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices
3. https://www.arm.com/products/silicon-ip-security/cryptoisland

Current Interest:

Differential power analysis attacks on ARM protected world in FPGA-CPU systems.