Mike Mishal

mmisha2

Report 4

03/4/2019

Papers Read:

1. Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis

I read this paper to confirm that there are commercial implementations of secrets being stored as a trustlet in the TrustZone. Runs attacks under root privileges and focuses on the first AES-256 rounds. They attacked an AES-256 code used by Samsung’s Keymaster trustlet. The attack is carried out in several phases and accelerated using a GPU to minimize the time it takes to complete the attacks.

1. <http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf>

This paper lists down the details of how ARM TrustZone works. Gained a better understanding on how ARM security works.

Papers to Read:

1. Power Analysis attacks and countermeasures
2. Template Attacks in Principal Subspaces

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?