Mike Mishal

mmisha2

Report 1

01/21/2019

Papers Read:

1. SKEE: A Lightweight Secure Kernel-level Execution Environment for ARM

This papers introduces a technology that provides kernel isolation at the same privilege level of the kernel itself. It does that by protecting a portion of the address space and prevent direct access to it from the kernel. These technologies allow access to the protected address space to the kernel through a well-controlled switch gate.

Doesn’t include any hardware protection level, but compares SKEE to KVM/ARM which is a hardware-assisted ARM hypervisor that is used to host security tools.

1. ARM Security Technology - Building a Secure System using TrustZone Technology Chapter 3: TrustZone Hardware Architecture.

Read this chapter to review some of the core components in ARM processors and the TrustZone Hardware Architecture. The modes in ARM core that implements the Secure and Normal world and how they interact with each other. How interrupt requests are handled between both worlds is interesting. ARMv6 and ARMv7 has a Performance Monitor on CP15 that can be used for timing code execution and counting processor events.

Wondering what areas of the architecture can be enhance to boost performance. Especially the part of memory mapping for both worlds.

Papers to Read:

1. TrustOTP: Transforming Smartphones into Secure One-time Password Tokens.

More Arm TrustZone technology implementations.

Current Interest:

Attack-based research to one off the new implementation.

Enhance the performance of one of the new implementation.

Come up with a new implementation.