Mike Mishal

mmisha2

Report 2

01/27/2019

Papers Read:

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

More Arm TrustZone technology implementations.

This papers introduces a technology that provides a One-Time password implementation and utilized ARM TrustZone to secure it. It relies on duplicating all the components that are need to securely create a One-Time password and display it to the user. It relies on securing the generated OTPs, seed, clock, counter, and drivers by placing them in the secure domain.

An interesting observation is how they secure the Booting sequence of TrustOTP.

1. Hardware-assisted transparent tracing and debugging on arm

This paper introduces several enhancement to NINJA. A transparent Tracing and Debugging malware analysis framework on ARM platform with low artifacts. It solves the current issue with tools that leave footprint (malware split behavior) or relay heavily in virtualizing (performance drawback).

They introduced a remote debugging platform that is connected via secure serial port.

Papers to Read:

1. Understanding the Security of ARM Debugging Features

Current Interest:

Hardware-assisted attacks to bypass secure domain or intercept data during booting or switching