TEE Offensive Core

Cristofaro Mune

Description

Trusted Execution Environments (TEEs) are notoriously hard to secure, due to the interaction between complex hardware and a large trusted code bases (TCB)

Would you like to gain a system-level understanding of TEE security? Identify new vulnerability classes? Learn new exploitation techniques? Understand how the underlying hardware (HW) may become a powerful resource for SW exploitation?

Then, this is THE training for you.

“TEE Offensive Core”, with its system-level approach, where HW and SW concur to SW exploitation, provides a unique experience for a thorough understanding of TEEs and their SW security. The training is modeled around ARM TrustZone based TEEs, but the discussed concepts are often applicable to non-TrustZone TEEs as well.

The training is organized in a methodical flow, with an attacker-oriented perspective.

TEE SW vulnerabilities are discussed across the entire TEE attacks surface, along with non-conventional exploitation techniques. A solid understanding of TEE system security is built step by step, in light of multiple threat models.

You are guided through the topics by means of new content, analysis of public vulnerabilities and exploits, as well as tailored exercises. The training is supported by widely used codebases, such as OP-TEE and ARM Trusted Firmware (ATF), which have been purposely modified for supporting classroom exercises. Public attacks, up to the most recent ones, are ported to the training codebase allowing for close simulation of real vulnerabilities. Specially crafted exercises support discussion of attack vectors, impacts and applicable techniques. The training codebase runs in an emulated ARMv8 (AArch64) target, where exploitation is performed for some of the vulnerabilities.

The exploitability of all vulnerabilities is analyzed taking the overall system into account. Techniques for"HW augmented" exploitation, where the underlying HW is used for novel and creative SW exploits, are introduced and discussed in details.

Presentations, interactive sessions, open questions and exercises are all mixed into a high intensity training. An in-class, jeopardy-style CTF supports the training during all its phases, from understanding theoretical concepts, to identification of vulnerabilities and exploitation.

Course Agenda

- TEE Security Intro
  - Fundamentals
  - Security model
- ARM TrustZone-based TEEs
  - TEE HW primitives
  - TEE SW components
  - Attacker models
- TEE SW attack surfaces
  - Communications
  - TCB
- TEE runtime attacks and exploitation [Advanced]:
  - REE --> TEE
  - REE --> TA
  - TA --> TEE
  - TA --> TA
- Crypto primitives attacks
- HW-augmented exploitation [Advanced]
- TEE initialization attacks
- TEE configuration attacks

Intended Audience

The training is intended for:

- Security Analysts and Researchers, interested in new techniques, or
- SW Security Developers/Architects interested in defenses against attacks combining HW and SW.

Goals

The main training goals are:

- *Add "new creative books" to your TEE offensive library*

    - *Vulnerabilities, attacks and exploits*
- *Extend your accessible TEE attack surface*
- *Understand how HW subsystems may be used in SW exploitation*
- *Gain a system-level understanding of TEE security.*

Although not explicitly focused on reverse engineering or ARM exploitation, this training may also benefit such areas.

Prerequisites

You are expected to have:

- knowledge of C/C++ programming [Advanced]
- sound knowledge of modern OS security concepts [Intermediate]
- familiarity with typical SW vulnerabilities and their exploitation [Intermediate]
- knowledge of ARM architecture (AArch64) and related assembly [Basic]

Although not mandatory, experience with the following may be helpful during the overall course

- OS-level source code reviews
- binary reverse engineering
- SoC-level HW security

HW/SW requirements

You are expected to bring a laptop:

- capable of running VMware Fusion, Workstation or the free VMware Player
- with one of the above VMWare products installed *(latest version preferred)*
- with 40GB available disk space
- with Wi-Fi connectivity

Bio

Cristofaro has been in the security field for 15+ years. He has 10 years of experience with evaluating SW and HW security of secure products, as well as more than 5 years of experience in testing and assessing the security of TEEs.

He works as an independent Product Security Consultant, providing support for design and development of secure products. He also performs device-level security testing with advanced SW

and HW techniques. Finally, he provides security training on low-level topics, usually lying at the boundaries of SW and HW.

He has contributed to development of TEE security evaluation methodologies and has been member of TEE security industry groups.

Research on Fault Injection, TEEs, White-Box cryptography, IoT exploitation and Mobile Security has been presented at renowned international conferences and in academic papers.
You can contact him on Twitter (@pulsoid).