Breaking TEE by Experience

"Training Description – Classroom – v1.6"

Public

This page was intentionally left blank.

Table of Contents

1 Training information

This section provides information ***meant*** to be public**.**

1.1 Description

A Trusted Execution Environments (TEE) is notoriously hard to secure due to the interaction between complex hardware and a large Trusted Code Base (TCB). The security provided by different TEE implementations has been broken on a wide variety of devices, including mobile phones, smart TVs and even modern vehicles.

The **TEEPwn experience** takes an offensive perspective and dives into the darker corners of TEE security. It's designed with a system-level approach, where you will experience exploitation of powerful vulnerabilities specific for TEE technology. Moreover, it's hands-on, well-guided and driven by an exciting jeopardy-style game format.

Your journey starts with achieving a comprehensive understanding of TEE technology. You will learn how hardware and software cooperate in order to enforce effective security boundaries. You will then use this understanding for identifying interesting vulnerabilities across the entire TEE attack surface. You will be challenged to exploit these vulnerabilities using multiple realistic scenarios.

All practical exercises are performed on our custom emulated attack platform which is using ARM TrustZone to implement multiple TEE implementations.

You will take on different roles, as an attacker in control of:

- the REE, achieving privileged code execution in the TEE
- the REE, accessing assets protected by a Trusted Application (TA)
- a TA, escalating privileges to the TEE OS
- a TA, accessing the protected assets of another TA

You will be guided towards an unexpected range of TEE-specific attack vectors and vulnerabilities, which can be leveraged for novel and creative exploits, allowing you to refine your skills to a new level.

1.2 Format

The **TEEPwn experience** takes your on a journey of 3 days of 8 hours where you will attend lectures and perform exciting hands-on exercises.

You will get access to a personal VM which contains all the required tooling. It's expected that not all of the exercises are finalized within the training hours. Therefore, you will have access to this VM forever so you can continue with the exercises after the training has ended.

Please note, if desired, the format of the **TEEPwn experience** can be adjusted.

1.3 Agenda

During the **TEEPwn experience** we will cover the following topics:

- **Fundamentals**
  - Overview of TEE
  - Security model
- **ARM TrustZone**
  - TEE software
  - TEE attacker model
  - TEE attack surface
- **REE-to-TEE attacks**
  - Secure Monitor (S-EL3)
  - TEE OS (S-EL1)
  - *Identify and exploit vulnerabilities related to:*
    - Vulnerable SMC handlers
    - Broken design
    - Unchecked pointers
    - Restricted writes
    - Range checks
- **REE-to-TA attacks**
  - Communicating with a TA
  - Global Platform API
  - *Identify and exploit vulnerabilities related to:*
    - Type confusion
    - ToCToU / Double fetch
- **TA-to-TEE attacks**
  - TEE OS (syscall interface)

    - Drivers
    - *Identify and exploit vulnerabilities related to:*
        - Unchecked pointers
        - Vulnerable hardware primitives
- **TA-to-TA attacks**
    - State confusion

1.4 Learning objectives

The primary learning objectives of the **TEEPwn experience** are:

- gain a system-level understanding of TEE security
- identify vulnerabilities across the entire TEE attack surface
- gain hands-on experience with TEE-specific exploitation techniques
- gain a solid understanding of ARM TrustZone-based TEEs

1.5 Audience

The **TEEPwn experience** is intended for:

- Security Analysts, Researchers and Practitioners interested in TEE security
- Software Security Developers and Architects interested in an offensive TEE perspective

1.6 What you need to know

The attendees of the **TEEPwn experience** are expected to:

- have experience with C programming
- have experience with the ARM architecture (Aarch64) and ARM64 assembly
- have a solid understanding of modern OSes and related security concepts
- have an understanding of typical software vulnerabilities
- be familiar with reverse engineering (AArch64)
- be familiar with typical exploitation techniques

Don’t worry if you don’t meet all of the above expectations. Less-experienced attendees can rely on our hints and solutions, whereas more-experienced attendees will not.

1.7 What you need to have

The attendees of the **TEEPwn experience** are expected to have:

- any modern computer system or laptop with sufficient memory
- we advise to install and use the Chrome browser
- A virtual machine software (preferably VMware), installed on your laptop
- a stable Internet connection with sufficient bandwidth

1.8 What you will get

The attendees of the **TEEPwn experience** will get access to:

- a personal virtual machine (VM) with all the required tooling installed
- access to the exercise modules and instructions

To continue practicing after the training is completed:

- ability to run the exercise modules forever
- ability to copy the exercise modules and instructions

1.9 About the trainers

Cristofaro Mune is a Co-Founder of Raelize and has been in the security field for 20+ years. He has 15+ years of experience with evaluating the software and hardware of secure products, including numerous TEE designs and implementations.

He has contributed to development of TEE security evaluation methodologies and has been member of TEE security industry groups. His research on Fault Injection, TEE, White-Box cryptography, IoT exploitation and Mobile Security has been presented at renowned international conferences and published in academic papers.

Contact: cristofaro@raelize.com / @pulsoid

Niek Timmers is a Co-Founder of Raelize and has been analyzing the security of embedded devices for over a decade. Usually his interest is sparked by technologies where the hardware is fundamentally present.

He shared his research on topics like Secure Boot and Fault Injection at various conferences like Black Hat, Bluehat, HITB, hardwear.io. and NULLCON.

Contact: niek@raelize.com / @tieknimmers