TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Attacking ARM TrustZones

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

This training introduces and details TrustZone technologies through presentations and practical exercises on Samsung's implementation.

At the end of the training, the participants will have gained a solid understanding of the underlying mechanisms used in popular TrustZone implementations as well as developed tools and insights to perform reverse engineering, vulnerability research and exploitation efficiently.

The main objective of this training is to gain code execution in Secure World User Mode (SEL0) by exploiting a, now fixed, vulnerability found in a Trusted Application on certain past Android versions available for the Samsung Galaxy S6/S7 models. The different steps leading up to this objective are described in the syllabus given in the description.

Syllabus

- Introduction to the TrustZone technology
- Analysis of kernel components enabling communication with TrustZone elements (Qualcomm and Exynos)
- Analysis of a TEE-OS attack surface
- TEE-OS extraction from Android platforms (Qualcomm and Exynos)
- Basics of TEE-OS reverse engineering, listing entry points for an attacker (Qualcomm and Exynos)
- Trusted Application extraction from Android platforms (Qualcomm and Exynos)
- Development of a tool to discuss with Trusted Applications (Exynos only)
- Comparison of different Trusted Application formats (Qualcomm and Exynos)
- Reverse engineering of Trusted Applications (Exynos only)
- Vulnerability research and exploitation on a Trusted Application (Exynos only)
- Tips to go further (TEE-OS attack surface)

Requirements

- An IDA license, all tools used and developed for this training are compatible only with IDA 7.0+
- A basic understanding of ARMv8 ISA
- A basic understanding of the main exploitation techniques, software protections and how to bypass them

Provided for the training

- Galaxy S6 (one per participant)

About the Speaker: Maxime Peterlin

Maxime Peterlin (@pandasec_) is a R&D Engineer working in Quarkslab's embedded & hardware team. His day-to-day work includes reverse engineering, studying low-level systems, vulnerability research, binary exploitation and tools development. Occasionally, he enjoys participating in Capture the Flag competitions and pursuing his research during his own time.

About the Speaker: Joffrey Guilbon

Joffrey Guilbon is Security Researcher at Quarkslab working on mobile and embedded systems. His usual work includes low-level systems, reverse engineering (on several targets such as operating systems, trusted execution environment components, secure boot implementations, bootroms, etc.), vulnerability research, binary exploitation, and tools development to ease things out. In his free time, he enjoys participating in Capture The Flag (CTF) competitions and in open-source projects (IDArling for example).

About the Speaker: Alexandre Adamski

Alexandre Adamski (@NeatMonster_) is working at Quarkslab in the Data Analysis team. As an R&D engineer, his work includes reverse engineering, low-level systems, vulnerability exploitation, and his all-time favorite: tools development. In his free time, he develops open-source tools and plugins (IDArling, AMIE, etc.).

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://troopers.de/tickets/

Voucher code: **TR19_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Troopers Organization Team

+49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / info@hmtrainingsolutions.com

+49 6022 5089999 / www.hmtrainingsolutions.com