Title: Attacking TrustZones

Abstract:

The increasing popularity of connected devices in recent years has led manufacturers to put a greater emphasis on security and were then in need of robust designs that would protect their users. From these requirements emerged the ARM TrustZone technology, a system-wide hardware isolation. It introduces a trusted "Secure World" that can process code and data, while ensuring their integrity and confidentiality are maintained. This "Secure World" can watch over the user-controlled, and therefore untrusted, "Normal World" to verify its integrity, similarly to Samsung's TIMA. It can also access hardware peripherals, such as a keyboard, to create a trusted UI, or a cryptoprocessor, to implement a DRM without ever having data pass through the Normal World.

During this practical two-day training, attendees will be introduced to the ARM TrustZone technology, the related problematics and how they can be answered using both hardware and software components. Once the OS running in the Trusted Execution Environment, or TEE-OS for short, has been extracted by the trainees on both Qualcomm and Samsung's Exynos based Android platforms, they will be reverse-engineered to list their entry points, their differences, their communication mechanisms, etc.

The course will then focus on how to extract, reverse-engineer and communicate with trusted applications on both Qualcomm and Exynos. Ultimately, the main objective of the training is for the attendees to get arbitrary code execution in a trusted application on Exynos by exploiting a, now-fixed, vulnerability. The course ends by providing different tips to go further and presents the attack surface offered once code execution is reached in a trusted application.

Description:

Agenda:

Day1

- Introduction to Secure Booting and Trusted Execution Environment (problematics answered, common usages, etc.)
- Introduction to the ARM TrustZone technology
- TEE-OS extraction from Android platforms (Qualcomm and Exynos)
- Basics of TEE-OS reverse engineering, entry points for an attacker and analysis of the attack surface (Qualcomm and Exynos)
- Analysis of kernel components enabling communication with ARM Trustzone elements (Qualcomm and Exynos)
- Trusted Application extraction from Android platforms (Qualcomm and Exynos)

Day2

- Comparison of different Trusted Application formats (Qualcomm and Exynos)
- Reverse engineering of Trusted Applications (Exynos only)
- Development of a tool to discuss with Trusted Applications (Qualcomm and Exynos)
- Vulnerability research and exploitation on a Trusted Application (Exynos only)
- Tips to go further (TEE-OS & drivers attack surface)

Who Should Attend:

The training is optimally suited for:

- Individuals interested by the ARM TrustZone technology, how it works, how it's implemented and how to break it.
- Security researchers who wish to assess the security of ARM TrustZone implementations and its components.
- Software engineers developing on ARM TrustZone who would like to understand how an attacker could compromise the system.

Key Learning Objectives:

This training introduces and details ARM TrustZone technologies through presentations and practical exercises on Samsung's implementation. No pre-requisite in terms of knowledge on ARM TrustZone is needed for this course. At the end of the training, the participants will have gained a solid understanding of the underlying mechanisms used in popular ARM 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 S5/S6/S7 models. The different steps leading up to this objective are described in the agenda.

Prerequisite Knowledge:

- A basic understanding of ARMv7/ARMv8 ISA
- A basic understanding of the main exploitation techniques

Hardware / Software Requirements:

- Python 3.7
- adb
- An IDA license, all tools used and developed for this training are compatible only with IDA 7.0+
- Galaxy S6/S7 (one per participant) -> they will be provided by Quarkslab

biography of the trainers:

- **Joffrey Guilbon**(@patateQbool) is a 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).
- **Maxime Peterlin**(@pandasec_) is a Security Researcher 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.
- **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).