Your trusted partner in embedded security

Learn how TrustZone® (ARM Security Extensions) works. Focus on a real secure kernel implementation on the Nexus 5 and reproduce an exploit.

TEE TrustZone - Reproducing an exploit

Knowledge is power!

Expand your knowledge and learn from the experts. We share our expertise with you in a hands-on manner to provide a pro-active learning experience. During the training you will get examples of real-case weaknesses and understand how to attack these weaknesses. After the training, you will be able to apply this knowledge straight away to your daily work. We will show you what measures to put in place to break as well as patch these weakness, to avoid future attacks.

TEE TrustZone - Reproducing an exploit

About the course

TrustZone is a hardware based security technique built into SoCs by semiconductor chip designers who want to provide secure end points and roots of trust. During this training youwill learn how TrustZone® (ARM Security Extensions) works. You will learn what composes a TrustZone secure kernel and how it interacts with the rest of the system. Then, you will focus on the real secure kernel implementation of the Nexus 5 smartphone and reproduce an exploit which gives full control over the secure side of the device. You will use a ready-to-use software package provided by eshard so that everyone works in the same environment. At each step you won't have to work from scratch, when necessary code templates will be available so that you don't spend time on uninteresting tasks.

Duration

Three days.

Target audience

Security analysts and software engineers.

Attendees will receive

Copy of the presentation slides and the software package we will be using during the practical exercises.

Pre-requisites

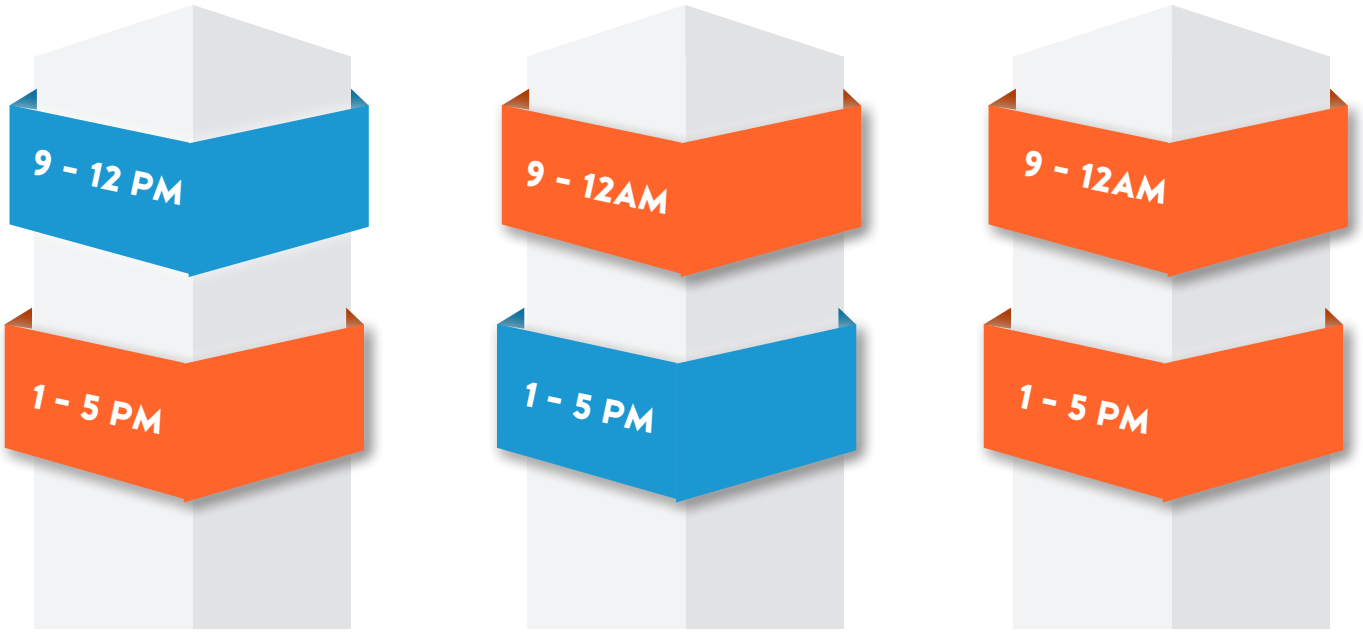
- Basic coding skills in Java, Python, C/C++
- Basic knowledge of Linux environment
- Laptop configuration: 4GB RAM >30GB disk space

Benefits of training with eshard's experts

- Opportunity to work on real life cases. We provide the point of view of an attack.
- Access to hands-on knowledge. Our experts stay up-to-date and have tens of years of cmbined experience in the security field.
- We provide a balanced mix of theory and practical exercises to enhance your understanding of the technology on both levels.
- This course can be hosted on-site or in two locations, in Bordeaux or Marseille in France. It's your call.

Course outline

Practical work Theoretical courses Challenge



Day 1

Day 1 theory:

- How TrustZone compares to other solutions
- ARM reminders
- TrustZone Principles

Nexus 5 - Qualcomm Secure Kernel:

- Architecture & Implementation
- Vulnerabilities

Day 2 theory:

During this part you will learn how TrustZone works and how it compares to other security solutions. We will cover:

- System security solutions
- ARM TrustZone principles - Hardware & Software
- TrustZone vs other solutions
- TrustZone usage examples
- ARM Architecture reminders
- ARM Security Extensions
- Secure & Non-Secure worlds
- Monitor mode
- Boot process
- Secure kernel design

Nexus 5 TrustZone Implementation

During this part the presenter will explain the architecture of the Nexus 5 TEE Implementation based on Qualcomm's Secure Kernel. The presented content is based on reverse engineering.

Day 2

Day 1 practical:

Nexus 5

- TEE Reverse Engineering
- Reproduce Nexus 5 exploit

Qemu:

How to run and debug a simple TrustZone kernel

Day 2 Practical:

During this part you will use a ready-to-use software package provided by eshard so that everyone works in the same environment. At each step you won't have to work from scratch, when necessary code templates will be available so that you don't spend time on uninteresting tasks.

- Device Flashing, custom kernel compilation
- TrustZone image extraction
- TEE Reverse Engineering
- Secure Kernel Exploitation
- Write and run shellcode in Secure context
- Use qemu to run a simple secure kernel, debug with gdb

Day 3

Day 3 Practical:

- All day practical exercises

Want to know more?

@eshardnews

companies/eshard

www.eshard.com
contact@eshard.com

ASIA

19 Keppel Road
#03-07 Jit Poh Building
Singapore 089058

EUROPE

1 Allée Jean Rostand Martillac
Bordeaux 33650 France

7 Rue Gaston de Flotte
Marseille 13012 France