Your trusted partner in embedded security

Mobile Application Security Track

Android Security - Level 1
Android Security - Level 2

Mobile Device Security Track

Reproducing a TEE TrustZone Exploit
Principles of TrustZone V7-A, V8-M & Trusty
Using Rowhammer Against TrustZone Implementations

Cryptography and Security Track

Side-Channel Introduction
White-Box Cryptography Security Analysis

Understanding risks and analysing threats will enable you to make informed decisions on your product's security

Training Course Catalog

Knowledge is power!

Expand your knowledge. Learn from the experts. We share our expertise with you in a hands-on manner to provide a pro-active learning experience. During our training we will give you examples of real-case weaknesses (know how to attack these weaknesses). Apply this knowledge straight away to your daily work. We will provide you with the full software so that you can practice as often as you wish when you are back in the office, thus enabling you to maintain your newly acquired knowledge after the training course.

Mobile Application Security Track — 5 days

1 - Android Security - Level 1

2 days

Android applications can be easily reverse engineered unless appropriate protections are properly set up. During this training, you will learn techniques and tools for reverse engineering Android applications. We will see from the Java world to the Native one, how to statically and dynamically reverse a given application in the Android environment. You will also discover some of the different techniques that make reverse engineering harder. Focus will be particularly put on practical exercises that you will have to do all along during the training.

On-site or at our offices in Bordeaux or Marseille, France
In English or French
enquiry: contact@eshard.com

2 - Android Security - Level 2

3 days

Take your knowledge in mobile application attack techniques to the next level. During this training, you will learn advanced techniques and reverse engineering frameworks that can be used by powerful attackers to target Android applications. This training is intended for seasoned reverse engineers that are familiar with IDA and binary reverse engineering. Focus will be split in theoretical and practical parts. This course is particularly designed for those willing to extend their skills for conducting in-depth analyses and for improving the security of their developments.

On-site or at our offices in Bordeaux or Marseille, France
In English or French
enquiry: contact@eshard.com

Cryptography and Security Track — 5 days

1 - Side-Channel Introduction

3 days

Side-channel analysis offers a way to uncover cryptographic keys and other sensitive information from hardware and embedded software. This is achieved by listening to and understanding the information that (hardware) channels emit when processing information. This introduction to side-channel training will give you an an understanding of the possibilities and impact of side-channel analysis and explains how you can protect against it through a hands-on approach. Besides theory, you will be offered practical exercises to fully grasp the concept of side-channel analysis.

On-site or at our offices in Bordeaux or Marseille, France
In English or French
enquiry: contact@eshard.com

2 - White-Box Cryptography Security Analyis

2 days

This training provides a strong introduction of how sophisticated attacks, like computational data analysis (side-channel) or meaningful fault injection, can affect a white-box cryptography implementation. Not a cryptography expert? Don't worry! With balanced theoretical and practical sessions, this training course will provide you with a strong understanding of how attacks on white-box cryptography can be realised, from the mobile application to the secret key.

On-site or at our offices in Bordeaux or Marseille, France
In English or French
enquiry: contact@eshard.com

eshard

Why choose eshard as your training partner

We offer three specific training tracks that are designed to provide full overview of a specified security topic. These are designed for both entry-level and experts in the field. Our courses give you the following:

- Opportunity to work on real life cases.
- Access to years of hands-on knowledge.
- We are flexibile regarding timing, customization and location.
- Follow a course on-site or from two locations in France (Marseille and Bordeaux). It is your call.

Mobile Device Security Track

7 days

1. Reproducing a TEE TrustZone Exploit

TrustZone is hardware-based security built into SoCs by semiconductor chip designers who want to provide secure end-points and roots of trust. During this training you will learn how TrustZone® (ARM Security Extensions) works. We will show you how to design a basic TrustZone secure kernel. After, you will focus on a real secure kernel implementation on the Nexus 5 device and reproduce an exploit which gives full control over the secure side of the device. The training consists of a theoretical part as well as a hands-on practical part.

3 days

On-site or at our offices in Bordeaux or Marseille, France

In English or French

enquiry: contact@eshard.com

2. Principles of Tustzone V7-A, V8-M & Trusty

During this training you will learn how TrustZone® (ARM Security Extensions) works on ARM Architecture v7-A and v8-M. You will learn in detail what composes a TrustZone v7-A secure kernel and how it interacts with the rest of the system. You will then focus on the real world secure kernel implementation "Trusty" open-sourced by Google. You will modify Trusty in order to implement a Trusted Applet which will communicate with non-secure Linux applications.

2 days

On-site or at our offices in Bordeaux or Marseille, France

In English or French

enquiry: contact@eshard.com

3. Using Rowhammer Against TrustZone Implementations

During this training you will learn the principles of TrustZone (ARM Security Extensions). In particular, you will learn how the 'Rowhammer effect' can be used against a particular TrustZone implementation. During the practical part of this session, you will work on your own Rowhammer implementation and target a TrustZone OS prepared for this purpose.

2 days

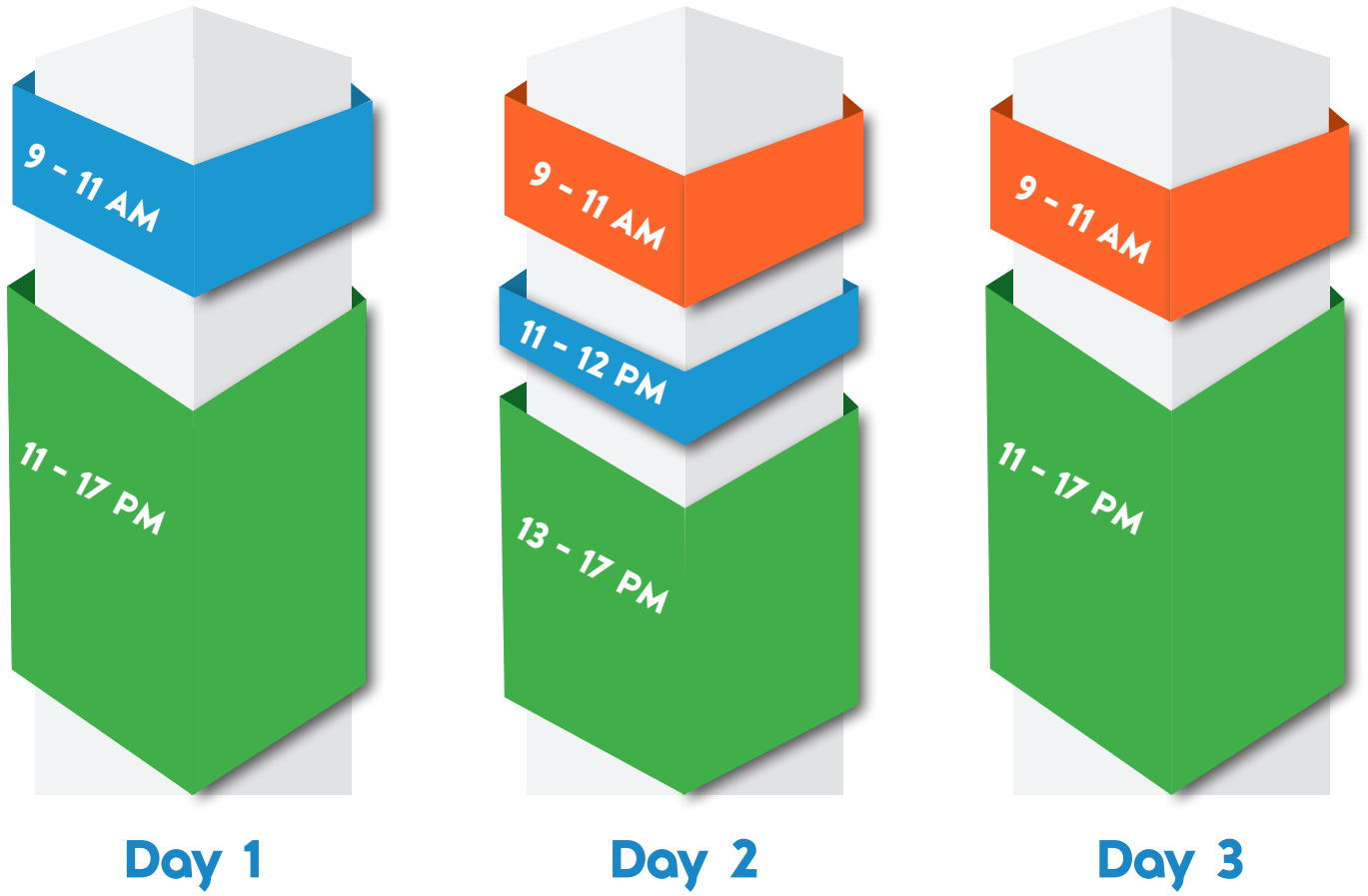
On-site or at our offices in Bordeaux or Marseille, France

In English or French

enquiry: contact@eshard.com

eshard

Our Methodology



How to sign up

We schedule courses regularly throughout the year in our offices in Bordeaux and Marseille. However, we're quite flexible in when, where and how we deliver our training. Should you require an expert to come to your site, we can make that happen. We offer our courses in English, however we are also able to provide training in French if necessary.

You can simply check our website (www.eshard.com) for the most up-to-date training dates and locations or send us an email (contact@eshard.com) if you would like to discuss how we can facilitate a training course at your premises, tailored to your needs.

@eshardnews

companies/eshard

1 Allée Jean Rostand Martillac
33650 Bordeaux France

7 Rue Gaston de Flotte
13012 Marseille France

www.eshard.com
contact@eshard.com