eshard

Your trusted partner in embedded security

Learn techniques and tools for reverse engineering white-boxed Android applications. Specific focus will be put on practical exercises.

Android Security - Level 1

Benefits of training with eshard

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.

Android Security - Level 1

About the course

Android applications can easily be reverse engineered unless appropriate protections are properly set up. During this course, 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 throughout the course.

Duration

Two days.

Target audience

Anyone interested in Android application security.

Attendees will receive

The attendees will be given the presentation slides and tools to perform the exercises with.

Pre-requisites

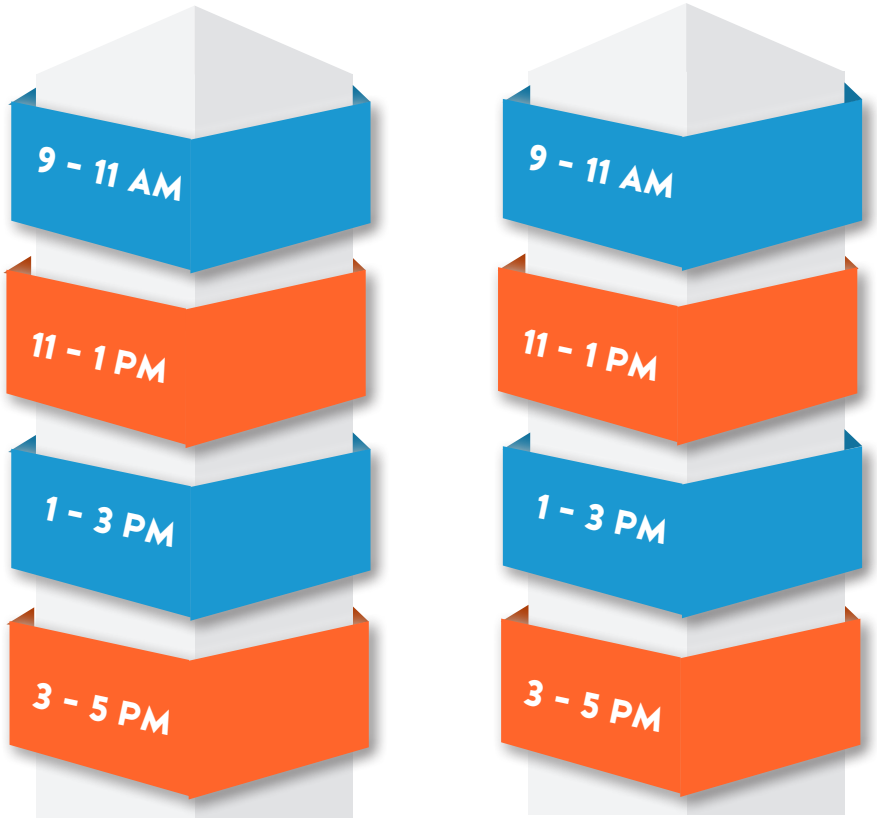
- Basic coding skills in Java, Python, C/C++
- Basic knowledge of Linux environment
- Minimum laptop configuration: 4GB RAM, >50GB free disk space

Why choose eshard as your trainer?

- Opportunity to work on real life cases.
- Access to years of hands-on knowledge. eshard's engineers have been working on several evaluation of SDKs and sensitive Android applications to measure their resilience against reverse engineering and tampering attacks.
- Having several engineers coming from the evaluation area provide a very good combination between evaluation methodology and reverse engineering expertise.
- We are flexibile regarding timing, customization and location. Training can be done onsite or hosted from two locations - Bordeaux and Marseille, in France. It's your call!

Course outline

Practical work Theoretical courses Challenge



Day 1

Day 1:

On the first day, we cover:

The basics

- Android apps lifecycles
- Anatomy of an Android application
- Introduction to DalvikVM and ART
- Introduction to Android Debug Bridge
- Introduction to SMALI syntax

Static analysis of the Java side

- Finding entry points
- Disassembling and decompiling
- Reassembling, recompiling and repakaging
- Static analysis with Android Studio
- Static analysis with radare2
- Reverse engineering obfuscated code

Static analysis of the Native code

- Introduction to Android NDK and JNI
- Introduction to ARM assembly

Day 2

Day 2:

On the second day, we cover:

Dynamic analysis of the Java side

- Debugging release applications
- Debugging with Android Studio
- Runtime instrumentation with Xposed
- Runtime instrumentation with Frida

Dynamic analysis of the Native code

- Remote debugging with GDB
- Runtime instrumentation of native code with Frida

Throughout both days we will mix theory with 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