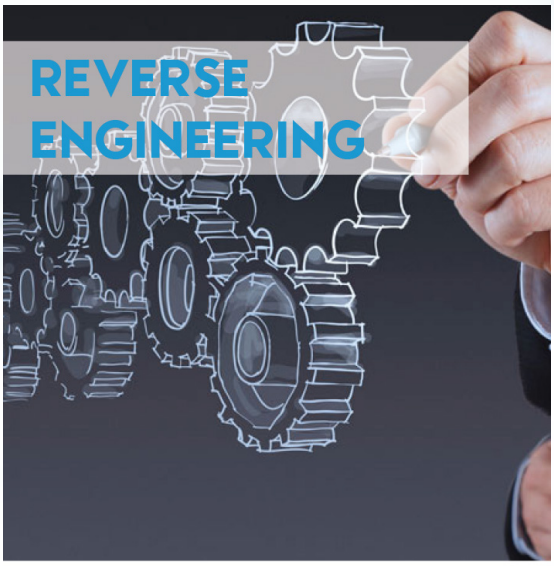
Your trusted partner in embedded security



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

Reverse Engineering of Android Apps

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.

Reverse engineering of Android applications

About the course

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 practica exercises that you will have to do all along the training.

Duration

Two days.

Target audience

Anyone interested in learning more about Android application security.

Attendees will receive

The attendees will be given the presentation slides and a provisionned VM with a set of open source security tools and an evaluation version of IDA Pro 6.9.

Pre-requisites

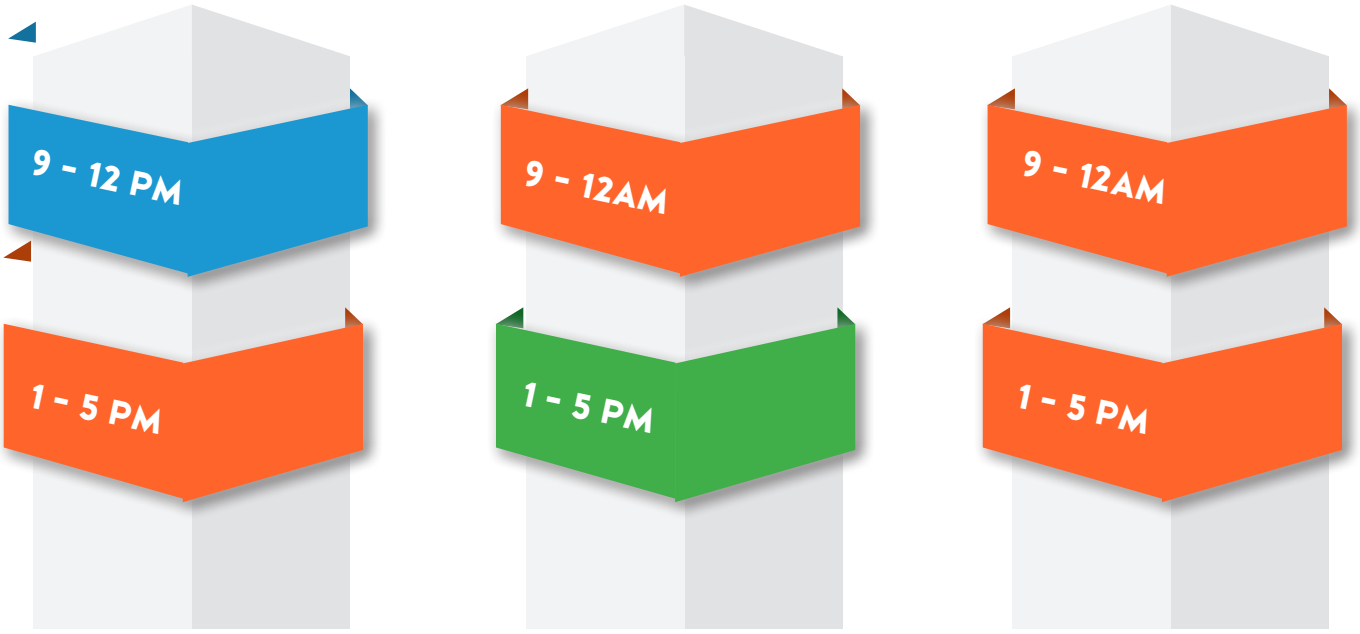
- Basic coding skills in Java, Python, C/C++
- Basic knowledge of Linux environment
- Laptop configuration: 4GB RAM >30GB disk space

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 AM:

In the morning, we cover the basics, including:

- Anatomy of an Android Application
- Android life cycles
- The Dalvik virtual machine
- The Dalvik byte code
- Android debug bridge
- Dalvik Debug monitor server
- Native development
- ARM assembly
- Rooting

Day 1 PM & Day 2 AM:

We cover hands-on static analysis tools for:

- Disassembling/decompiling
- Inspecting/modifying
- Reinstalling patched APK
- Static analysis automation

Static analysis of native libraries:

- Hands-on Linux tools for reverse engineering purpose
- Hands-on IDA tools for reverse engineering native code

Day 2

Day 1 AM/PM:

In the afternoon, we will cover code and data protection, inluding:

- Obfuscation
- Anti-tampering
- Jailbreak detection
- Anti debug
- Packers

During dynamic analysis, we cover:

- Debug an application
- Debug the native code
- Runtime instrumentation and manipulation (code injection, hooking, instrumentation)

Day 2 PM

The whole afternoon is spent on the security challenge 'crack me if you can'.

Upon request

Want to know more?

@eshardnews

companies/eshard

1 Allée Jean Rostand Martillac
Bordeaux 33650 France

21b, Avenue Du Docteur Heckel Bat H
Marseille 13011 France

www.eshard.com
contact@eshard.com
www.linkedin.com/companies/eshard
eshardnews