Your trusted partner in embedded security

Learn how attacks on whitebox cryptography can be realised, from the mobile application to the secret key.

Whitebox Security Investigation

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.

Whitebox security investigation

About the course

This training provides a strong introduction of how sophisticated attacks, such as computational data analysis (side-channel) or meaningful fault injection, can affect a whitebox 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 whitebox cryptography can be realised, from the mobile application to the secret key. If you want an extra day for an introduction on statistical attacks (DPA, CPA) and fault injections (DFA), you just ask! Whitebox cryptography has increasingly become an option for implementing strong algorithms in software on non-secure platforms. Quite popular in applications with DRM (Digital Right Management) exposure, it has become a serious option when implementing mobile payment applications, such as HCE (Host-Based Card Emulation). Aiming at maintaining a strong security level while running on non-secure platforms, a whitebox cryptography implementation is potentially subject to sophisticated attacks.

Duration

Two days with possible extra day to learn more about specific details.

Target audience

Anyone interested in learning more about whitebox cryptography security.

Attendees will receive

The attendees will be given the presentation slides.

Pre-requisites

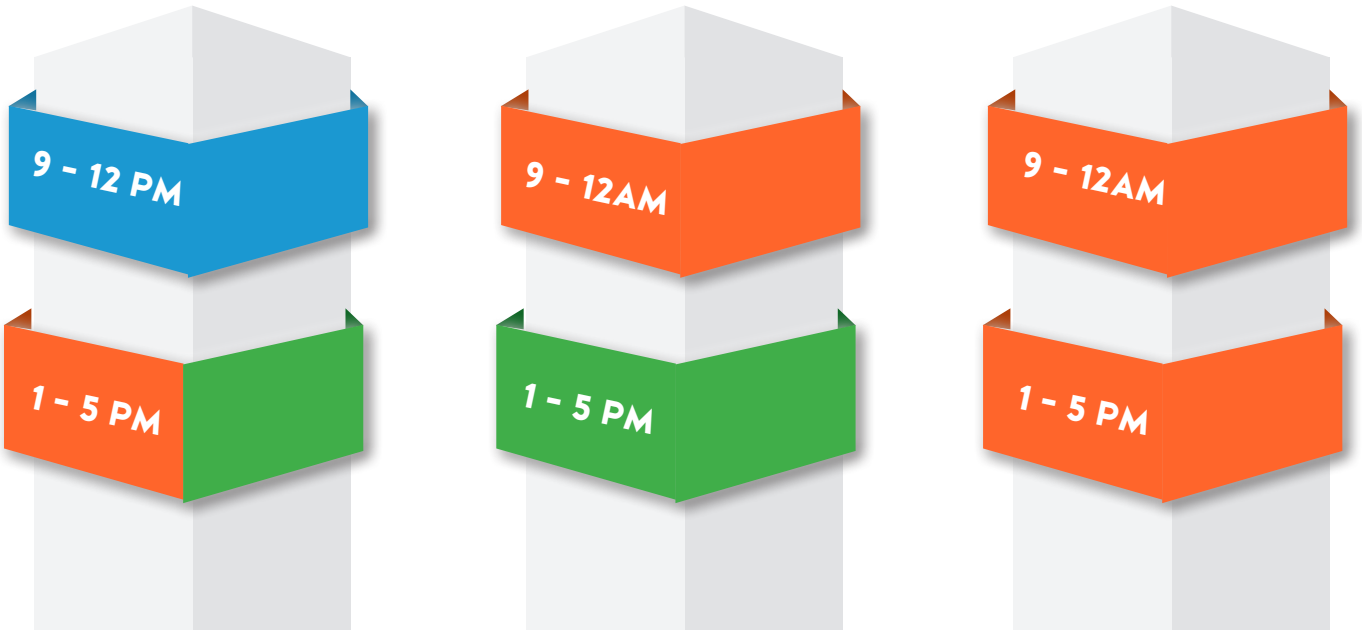
- Basic knowledge of Linux environment
- Basic knowledge of cryptography
- Laptop configuration: 4GB RAM >30GB disk space

Benefits of training with eshard's experts

- Opportunity to work on real life cases.
- Access to knowledge. Our esperts' areas of expertise comprise reverse engineering of android applications and whitebox cryptography and stay on top of the latest developments in these areas, as they are also developing specific tools to perform specific analysis.
- We offer a flexible training program that can be adjusted to your needs.
- We offer our courses on-site or at two locations in Bordeaux and Marseille, France. It's your call.

Course outline

Practical work Theoretical courses Challenge



Day 1

Day 1 AM:

Introduction to the whitebox cryptography:

· Purpose and benefits

· Diversity of existing solutions

· State of the art of the threats and the latest attacks

Extracting a whitebox implementation from an application:

· Overview of the obfuscation methods

· Localisation and extraction of the whitebox

Day 1 PM:

First challenge: extracting a WBC solution from a mobile application

Understanding the computational data analysis (CDA):

· Principle (single power analysis, differential power analysis)

· Different framework

· Executing and tracing a binary

Day 2

Day 2 AM:

Understanding the Computational data analysis (CDA):

· Exploitation of the traces to recover the secret key

Day 2 PM:

Second challenge: tracing a binary, and key recovering

Meaning fault analysis:

· Principle (Differential Fault Attack)

· Different framework

· Faulting a binary execution

· Exploitations of the faulty execution to recover secrets

Third challenge: faulting the extracted binary, and key recovering

Day 3:

An extra day to learn more specific details can be arranged upon request

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