D7.2

Hands-on trainings for contributors

Project number:	883156
Project acronym:	EXFILES
Project title:	Extract Forensic Information for LEAs from Encrypted SmartPhones
Start date of the project:	1st July, 2020
Duration:	36 months
Programme / Topic:	H2020-SU-SEC-2019 / SU-FCT02-2018-2019-2020 Technologies to enhance the fight against crime and terrorism

Deliverable type:	Other
Deliverable reference number:	SU-FCT02-883156 / D7.2 / V2.0
Work package contributing to the deliverable:	WP7
Due date:	JUL 2021 - M13
Actual submission date:	8th April, 2022

Responsible organisation:	RISCURE
Editor:	Valentina Banciu
Dissemination level:	PU
Revision:	2.0

Abstract:	This report describes the hands-on training for contributors, who are using the lab set-up of D5.2 and the analysis software.
Keywords:	SCA training, FI training

The project EXFILES has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883156.

Editor

Banciu, Valentina (RISCURE)

Contributors (ordered according to beneficiary numbers)

Tabeau, Jasiek (RISCURE)

Disclaimer

Executive Summary

This document describes deliverable D7.2 “Hands-on training for contributors”. As part of this deliverable, RISCURE has made available (and will continue to enable access for the entire duration of the project) two standard, hands-on online training courses to all EXFILES contributors. The training courses in question are:

- Essential SCA with Inspector
- Essential FI with Inspector

In this report, we outline the structure of these training courses and argue the deliverable achievement. Note that throughout the duration of the EXFILES project, updated versions of the training courses will be made available to contributors as and when published by RISCURE. RISCURE periodically updates their training courses in order to match the capabilities of RISCURE’s latest Inspector software release or hardware tools updates.

Table of Contents

List of Figures

Chapter 1 Introduction

This document describes D7.2 “Hands-on training for contributors” and is structured as follows: In this chapter, we describe the structure of this document, and state the intended scope of this deliverable. In 1.1 we go into the specifics of the deliverable: RISCURE has made two training courses available to all EXFILES contributors, namely *Essential SCA with Inspector* and *Essential FI with Inspector*; we outline the structure of each of the training courses and argue the deliverable achievement. Finally, in Chapter 2 we summarize and discuss future work.

1.1 Scope of the deliverable

This deliverable is dedicated to training of the members who are using the lab setup of D5.2 and the analysis software in order to efficiently conduct work in task 5.3. Every applicable member can request standard SCA/FI software to perform analysis of collected data on their own location. The SCA and FI online training courses are made available to all EXFILES contributors during the project to refresh their knowledge, or for new security analysts, who need to work with the SCA/FI software.

Chapter 2 Description of the deliverable

As part of this deliverable, RISCURE has made available (and will continue to enable access for the entire duration of the project) two standard, hands-on online training courses to all EXFILES contributors. More specifically, these courses are:

- *Essential SCA with Inspector* (https://riscure.streamlxp.com/courses/TOOLSSCA-video/home)
- *Essential FI with Inspector* (https://riscure.streamlxp.com/courses/TOOLSFI/home)

Note that Inspector, which is RISCURE's proprietary software, is the state of the art tool for performing Side Channel Analysis (SCA) and Fault Injection (FI), and is used by several organisations worldwide. More information about Inspector can be found here: https://www.riscure.com/security-tools. For best results, learners need access to both Inspector and RISCURE tools in order to complete the training courses; the required tools have been made available by RISCURE to EXFILES contributors. In order to access the contents of the training courses listed above, users must first create an account on the platform. RISCURE controls all accounts and access.

2.1 Essential SCA with Inspector

In this section, we give an overview of the *Essential SCA with Inspector* course.

This course provides the foundation knowledge and skills to evaluate the resistance of cryptographic implementations to side channel analysis. The main learning objective of this training is the methodology of applying SCA to a wide range of devices from the very simple, unprotected smartcards to implementations protected with advanced countermeasures or complex embedded applications.

In the following, we describe the pre-requisites and requirements, give a brief course outline, and list the learning outcomes.

2.1.1 Course pre-requisites and requirements

This course is aimed at new security analysts who aim to perform SCA testing of smart cards or embedded systems. Trainees do not need any specific prior knowledge.

While the concepts we teach are generic and can be replicated using different equipment, during the training we use RISCURE software and hardware tools, as follows:

- software tools: Riscure Inspector SCA
- hardware tools: Riscure Current Probe, Riscure PowerTracer, an oscilloscope (such as PicoScope 5000), Riscure XYZ EM Probe Station, Riscure EM probe, a set of Riscure training cards (2,3,6, and 8), and the Riscure Pinata training board.

2.1.2 Course outline

The training is structured into 15 chapters and consists of pre-recorded video materials as well as interactive exercises and quizzes. The course covers topics such as: an introduction to SCA, power analysis (tools and theory), the process of SCA (building a setup, performing SCA acquisition, signal processing, attacking an implementation), an introduction to cryptography and statistics, practical examples of SCA on smartcards and embedded systems, electro-magnetic analysis, and SCA countermeasures.

A screenshot of the *Essential SCA with Inspector* training as hosted on RISCURE's training platform is reproduced in Figure 1.

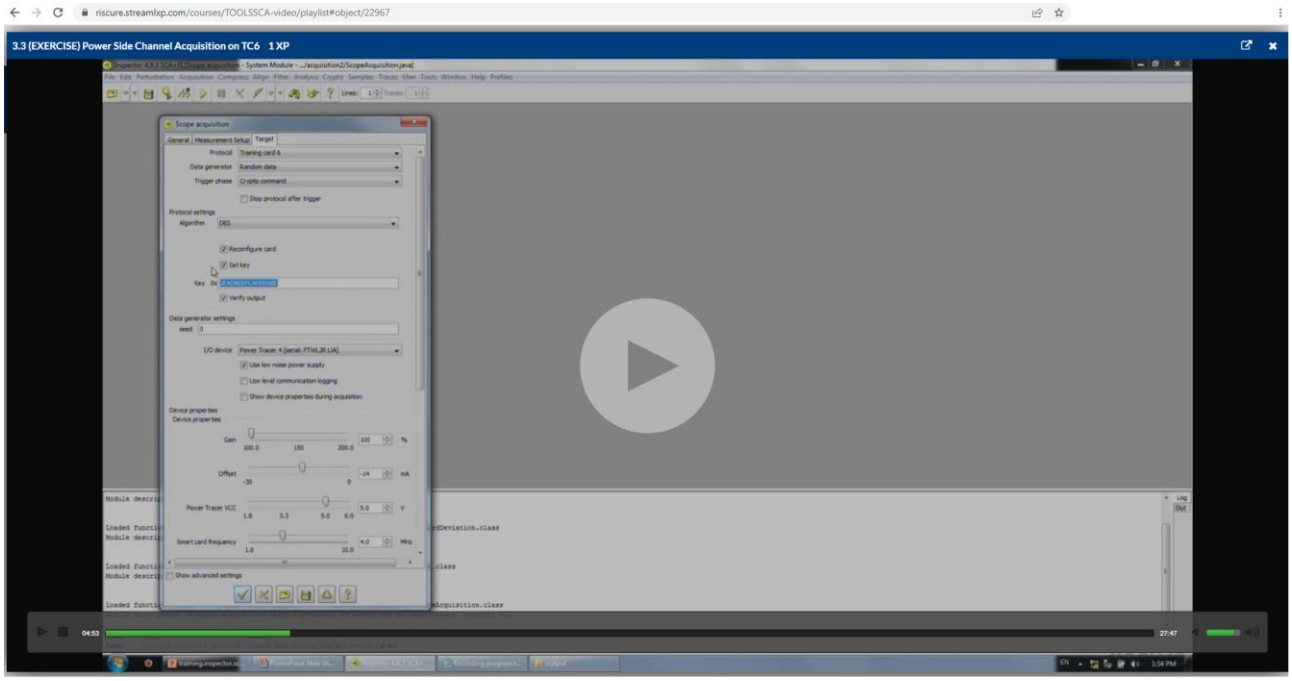

Figure 1: A screenshot of the Essential SCA with Inspector training

2.1.3 Interactive exercises

Figure 1 shows a screen capture of an interactive exercise: the trainee gets step-by-step instructions on how to build a power SCA setup using a smartcard. The trainee must then perform an acquisition campaign and carry out an SCA attack. Tips and tricks for troubleshooting, best practices, and a discussion of the entire process are also available in this exercise. For this exercise, the trainee needs the Riscure PowerTracer, training smartcard #6, an oscilloscope (such as the PicoScope 5000) and the Riscure Inspector SCA software.

The course contains approximately 20 such interactive exercises, accompanied by discussion. If the trainee cannot complete an exercise or if they have further questions, they have the option to contact RISCURE's training team via email.

2.1.4 Learning outcomes

At the end of the training the learner has a thorough understanding of power and electromagnetic analysis methods and is able to perform testing on both smart cards and embedded chips. The learner is able to assess the robustness of chips with no or basic countermeasures of moderate complexity.

2.2 Essential FI with Inspector

In this section, we give an overview of the *Essential FI with Inspector* course.

This course provides the foundation knowledge and skills to evaluate the resistance of cryptographic implementations to fault injection. The main learning objective of this training is the methodology of applying FI to smart cards and embedded systems.

In the following, we describe the pre-requisites and requirements, give a brief course outline, and list the learning outcomes.

2.2.1 Course pre-requisites and requirements

This course is aimed at new security analysts who aim to perform FI testing of embedded systems. Trainees do not need any specific prior knowledge.

While the concepts we teach are generic and can be replicated using different equipment, during the training we use RISCURE software and hardware tools, as follows:

- software tools: Riscure Inspector SCA
- hardware tools: an oscilloscope (such as PicoScope 5000), Riscure Spider, Riscure Glitch Amplifier 2, Riscure XYZ EM Probe Station, Riscure EMFI Transient Probe, Riscure icWaves, and the Riscure Pinata training board.

2.2.2 Course outline

This course is structured into six chapters as follows. In Chapter 1, one will learn the basics of fault injection attacks. In Chapter 2, we introduce the Riscure software tools for fault injection attacks, namely: Inspector FI Python, Inspector FI, and FI Spotlight. In Chapter 3, we introduce the Riscure hardware tools for a basic voltage FI attack (e.g., Spider, Glitch Amplifier 2, etc.), and the Riscure Piñata target board that will be used throughout the training. In Chapters 4 to 7, we walk the learner through building specific FI set-ups and performing different flavours of FI attacks (e.g., icWaves, EMFI, BBI, etc.).

A screenshot of the *Essential FI with Inspector* training as hosted on RISCURE's training platform is reproduced in Figure 2.

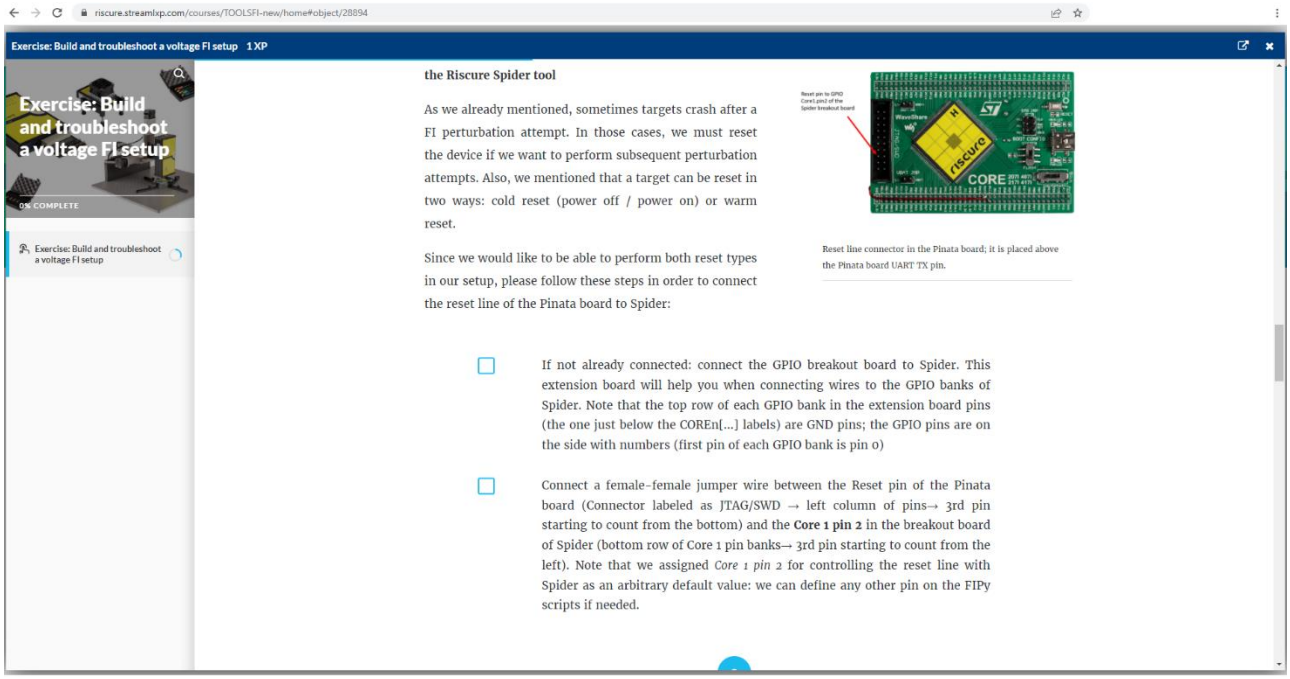

Figure 2: A screenshot of the Essential FI with Inspector training

2.2.3 Interactive exercises

Figure 2 shows a screen capture of an interactive exercise: the trainee gets step-by-step instructions on how to build and troubleshoot a voltage FI setup. The trainee must then perform FI using this setup. Tips and tricks for troubleshooting, best practices, and a discussion of the entire process are also available in this exercise. For this exercise, the trainee needs the Riscure Spider Tool, the Riscure Glitch Amplifier 2, and the Riscure Pinata training board.

The course contains approximately 10 such interactive exercises, accompanied by discussion. If the trainee cannot complete an exercise or if they have further questions, they have the option to contact RISCURE's training team via email.

2.2.4 Learning outcomes

Fault Injection (FI) attacks are implementation attacks designed to influence the intended behavior of a device or application by changing a critical value or by changing the flow of a program. Faults can be used to exploit or bypass robust security features found in secure systems. The end goal of this course is to enable learners to perform voltage and EM fault injection attacks using Riscure software and hardware tools. One will also learn the theory behind FI attacks: the characteristics and effects of faults, different flavours and ways to inject faults, and common vulnerabilities and applications of fault injection attacks.

Chapter 3 Summary and conclusion

RISCURE has created and made available two standard, hands-on online training courses to all EXFILES contributors, namely: E*ssential SCA with Inspector* and *Essential FI with Inspecto*r.

For a learner, the training content of the E*ssential SCA with Inspector* adds up to approximately 12 hours of video content and practical exercises, and we estimate that an additional 4 hours are needed to complete the quizzes. We estimate that it would take a learner approximately 8 hours to go over the E*ssential FI with Inspector* training course materials; completing the practical exercises and quizzes may take up to eight additional hours.

3.1 Future work

Although the training courses that have been provided are technically sound, RISCURE periodically updates their training courses in order to match the capabilities of RISCURE's latest Inspector software release or hardware tools updates. The updated versions of the training courses will be made available to EXFILES contributors as and when published by RISCURE.