Project ID: 731591, Horizon 2020
http://www.reassure.eu

REASSURE

Deliverable D 5 . 6

Advanced SCA Training

Editor:	I.Buhan (Riscure)
Deliverable nature:	OTHER
Dissemination level: (Confidentiality)	PU
Delivery date:	1 April 2020
Version:	1.0
Total number of pages:	7
Keywords:	training, online, side channel analysis

Horizon 2020
European Union funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 731591.

Executive summary

This document is a placeholder for the full training (which can be accessed here https://riscure.talentlms.com/catalog/info/id:245). In this document we present a high level overview of how the course and the online webinar (https://www.riscure.com/news/understanding-leakage-detection-webinar/ are organized and the impact in terms of number of participants.
The decision to dedicate the advanced SCA training to leakage detection is a consortium decision, as the application of leakage detection techniques is a complex topic, not always well understood, of vital interest in the hardware security evaluation industry.

List of authors

Company	Author
Riscure	V. Banciu
UCL	D. Bellizia
Riscure	I. Buhan
UNIVBRIS	C. Whitnall

Revision history

Revision number	Date	Comment
1.0	31 March 2020	Final version of document

Contents

List of authors **3**

Revision history **4**

1 Introduction **6**

2 Understanding Leakage Detection **6**

3 The pocket guide to leakage detection **6**

4 Impact evaluation **6**

1 Introduction

Leakage detection plays an increasingly important role in the security evaluation of cryptographic devices. A particularly popular approach is the Test Vector Leakage Assessment (TVLA) framework, which specifies a suite of simple statistical tests tailored to either confirm or rule out many typical forms of side-channel vulnerabilities. However, if TVLA-style evaluations are performed without an adequate understanding of the statistical theory underpinning them, the risks are that tests may be misapplied, that outcomes may be misunderstood, and that conclusions may be overstated. Evaluating leakage detection methodologies was an active research area for the Reassure consortium.

2 Understanding Leakage Detection

The aim of this course is to help the audience grasp the intuition behind leakage detection methodologies and achieve a sound technical appreciation of how and why they work. In the course, we motivate and describe the current popular practice, including correlation-based tests, and expose some of the limitations, with a special focus on ISO standard 17825. The learning goal of this advanced course is to equip evaluators to carry out leakage detection tests sensibly and interpret the outcomes responsibly.

This course is structured as follows. We start off by introducing the problem, namely the presence of data-dependencies in side-channel measurements, and the most common strategy to exploit such information: Differential Power Analysis (DPA). We then build a case for why statistical methods are necessary and develop the particular rationale behind the t-test before describing it more formally. Finally, we show how the t-test is being applied within the TVLA framework and discuss some of the issues affecting its usefulness.

The online training is available on-demand and free of charge on the project website. The approximate duration of this course is 6 hours. The content of this course can be found here: `https://riscure.talentlms.com/catalog/info/id:245`.

3 The pocket guide to leakage detection

To answer questions from the audience, we organized a free, publicly accessible, live webinar on the 26^{th} of February at 15.00 CET. Through this webinar, which was publicised under the name "The pocket guide to leakage detection", we aimed to help participants from the audience grasp the intuition behind leakage detection methodologies, and walk you through the content of our in-depth online training that is freely accessible. For the already advanced attendees, we reserved time for live questions. The webinar has been hosted by the following members of the consortium:

- Carolyn Whitnall, UNIVBRIS
- Davide Bellizia, UCL
- Valentina Banciu, Riscure
- Ileana Buhan, Riscure

The format of the webinar was interactive discussions where the audience could ask questions to the experts. In figure 1 we have a screenshot of the webinar. A recording of this webinar is available here: `https://www.riscure.com/news/understanding-leakage-detection-webinar/`.

4 Impact evaluation

In this section we report the amount of registered users for both online events.

Title	Launch date	Registered users
Understanding Leakage Detection	22 January 2020	31
The pocket guide to leakage detection	26 February 2020	33

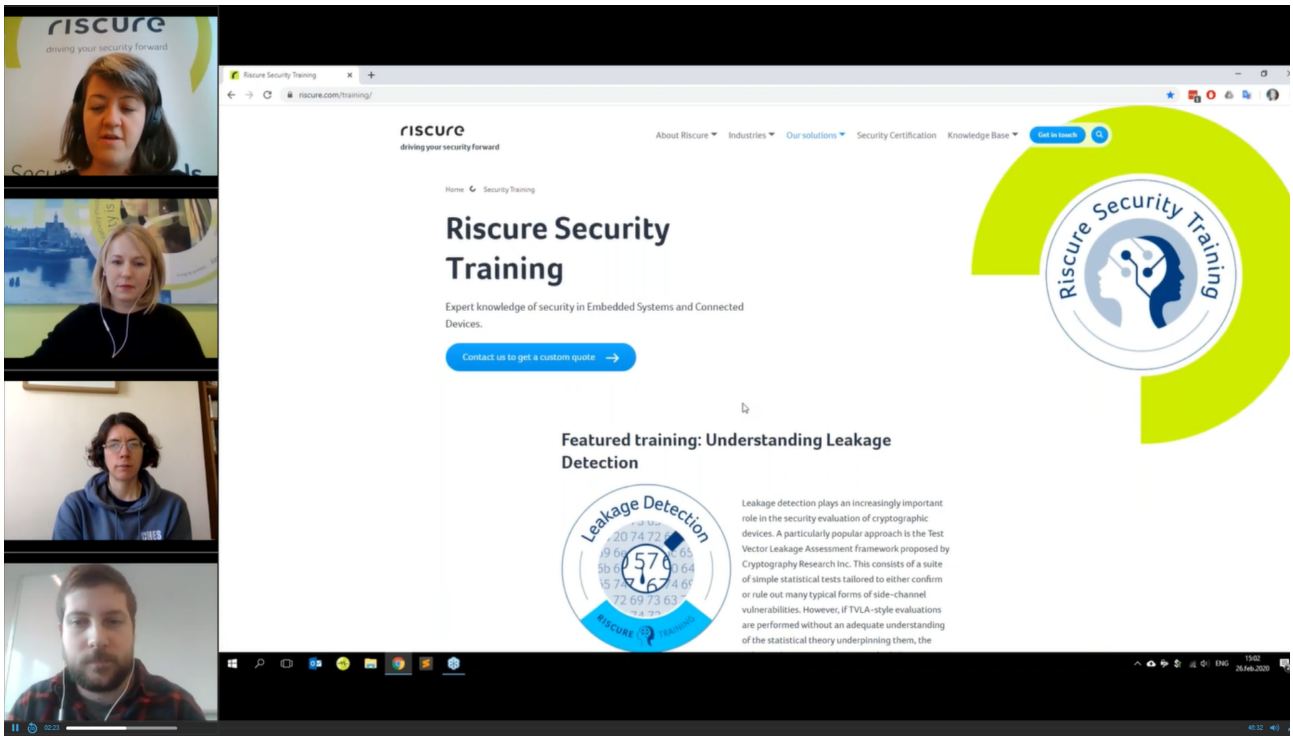

Figure 1: Screenshot from the live webinar

