SCA, FI and Secure Boot Workshop – May 2019

May 14-17, Delft, The Netherland

Tuesday May 14	Wednesday May 15	Thursday May 16	Friday May 17
Side Channel Analysis (SPA/DPA)	Fault Injection (FI) – Day 1	Fault Injection (FI) – Day 2	Hardening the Secure Boot
Rambus Cryptography Research	riscure driving your security forward	riscure driving your security forward	riscure driving your security forward

Workshop

Riscure, together with Rambus (Cryptographic Research) are hosting a 4 days workshop at Riscure in Delft, The Netherlands. The aim of the workshop is to introduce the concepts of Side-Channel Analysis, Fault Injection and hardening Secure Boot.

Audience

This course is intended for developers, security evaluators and researchers focused on hardware security testing, government organizations seeking to analyze threats posed by state-of-the-art side channel attacks or fault injection, Rambus DPAWS customers and Riscure Inspector customers. The course does not require any specific existing experience. Having general knowledge about embedded systems architecture is welcome.

Pricing 4 day workshop

- € 1.000 per trainee (Outside US)
- $1.100 per trainee (US customers)
- Maximum 25 trainees

Location

Riscure Head Office
Delftechpark 49
2628 XJ Delft
The Netherlands

45 min by car or train from Amsterdam or Schiphol Airport

riscure
driving your security forward

Rambus
Cryptography Research

Learning Objectives

Day 1 – Side Channel Analysis

This course provides you the foundations and skills to evaluate the resistance of cryptographic implementations against Side Channel Analysis. The main learning objective is to understand the basic principles of SPA and DPA,

Day 2 and 3 – Fault Injection

During these 2 days you learn how to inject faults for the purpose of security testing and you will apply these techniques in practice on real-world targets. You will also learn how to recognize when and where to inject a fault, what parameters are relevant, and how to use statistics to analyze faults.

Day 4 – Hardening the Secure Boot

This workshop covers the most common pitfalls of secure boot implementation based on our extensive security evaluation experience. We discuss common logical vulnerabilities that allow attackers to bypass secure boot and also more sophisticated attack techniques such as fault injection. These attacks are extremely effective against any code which has not been specifically hardened against FI attacks making the manufacturers take on additional cost of re-developing the code of high enough quality too meet the rising industry standards.

Registration

www.riscure.com/training
www.rambus.com/security/dpa-countermeasures/training/

Agenda – May 14 - 15

Tuesday – May 14 – SPA/DPA - Rambus

9.00 – 75 min
- Welcome and Simple Power Analysis (SPA)

10.30 – Break – 15 min

10.45 – 60 min
- SPA Modular Exponentiation Exercise

11.45 – 30 min
- Electromagnetic Analysis Demonstration

12.15 – Lunch – 60 min

13.15 – 90 min
- Differential Power Analysis (DPA)

14.45 – Break – 15 min

15.00 – 75 min
- Differential Power Analysis Hands-on Exercise

16.15 – 30 min
- Preventing DPA: Countermeasures

16.45 – 45 min
- Testing and Certification

17.30 – End of day 1

Wednesday – May 15 – FI Intro – Riscure

Introduction to Fault Injection
- What is a fault (or glitch)?
- Types of fault injection
- Tools for fault injection
- Basic notions of cryptography

Bypassing a security check (practical assignment)
- Finding a exploitable point in the code
- Building a setup for fault injection on smart cards
- Efficiently tuning parameters

Differential Fault Analysis (practical assignment)
- Finding a exploitable point in the code
- Efficiently tuning parameters
- Recovering the key

Countermeasures (practical assignment)
- Common countermeasures
- Coding guidelines
- Bypass a protected security check

Practical information

- Workshop start every day at 9.00 and ends at 17.30
- Lunch and breaks are provided at Riscure office
- Coffee, snacks, drinks are included
- Free parking is available next to our office

Hotel suggestions

- **Hamshire Hotel Delft Centre**
  - www.hoteldelftcentre.nl
  - 2.9 km from Riscure
- **Hotel Casa Julia**
  - www.casajulia.nl
  - 2 km from Riscure
- **WestCord Hotel Delft**
  - www.westcordhotels.nl
  - 2.7 km from Riscure

- Most hotels offer bikes for rent or free to use with a booking
- In the Netherlands biking is the easiest way to travel since we have excellent biking lanes and distances are relatively short

riscure
driving your security forward

Rambus
Cryptography Research

Agenda – May 16 - 17

Thursday – May 16 – FI Embedded – Riscure

Module development (practical assignment)

- Writing simple modules for device communication

Optical Fault Injection (practical assignment)

- How does it work?
- Practicalities
  - Safety
  - Target Preparation
- Different wavelengths and laser types
- Building a setup for smart cards

Fault injection on embedded targets

- Differences compared to smart cards
- Building a setup for embedded targets

Module development (practical assignment)

- Writing simple modules for device communication

Electro Magnetic Fault Injection (practical assignment)

- How does it work?
- Building a setup for embedded targets

Advanced topics

- Smart triggering

riscure
driving your security forward

Rambus
Cryptography Research

Friday – May 17 – Secure Boot - Riscure

Introduction to secure boot

- Anatomy of a secure boot implementation
- Secure boot and firmware integrity

Logical attacks on secure boot

- Most common issues
- Vulnerability Identification exercise

Introduction to Fault Injection

- Overview of FI attacks
- Fault models
- Fault location identification exercise

Common Vulnerable Code patterns

- Infinite loops
- Single points of failure

Combined attacks

- Create your own buffer overflow
- Hijack control flow with FI

Hardening secure boot

- Software countermeasures
- Compiler optimization & FI
- Hardening exercise

Final exercise

- Interactive game to test & implement your counter measures to create the most secure implementation!

For more information

Bartek Gedrojc
Senior Director Global Tools

+31 15 251 4090 / +31 6 48 19 39 86
gedrojc@riscure.com or inforequest@riscure.com