Riscure Workshop 2021 - Program

Day 1 – Monday, September 6, 2021 - CET

1-1 **8:00 – 08:30** **R&D 1: What's Hot & What's Happened: Hardware** (Marc Witteman)

During this 30-minute talk, our CEO Marc Witteman will share his thoughts on recent market developments regarding hardware related security topics and gives an insight on his expectations of trends that have a chance to become mainstream in the near future. Topics that will be covered amongst other things: 'What it takes to hack a Tesla' and 'Multi fault attacks are practical'.

1-2 **10:00 – 10:30** **Attacks 1: Security evaluations of a smart device: D-Link DIR 2680 Router** (Yashin Mehaboobe)

Some modern IoT devices have begun the journey into security. Here at Riscure, we are beginning to see more and more devices with locked down UART shells, varying levels of input sanitation and use of dedicated security ICs. Is that enough to secure a modern router? In this presentation, we show you what can go wrong even when security is implemented in IoT devices with the case study of the D-Link DIR2680.

1-3 **13:00 – 13:30** **R&D 2: Failure analysis for SCA Thermal Laser Stimulation** (Dennis Vermoen)

TLS is a method originating from failure analysis. This method is used to heat up the chip surface with the help of a laser source and as it turn out can help with discovering secrets that are stored in memory on a chip. Our principal researcher Dennis Vermoen will share details about this method and the results that we have achieved. Next to that some of the specific products needed to build a TLS setup will be covered.

1-4 **17:00 – 17:30** **SC 1: Fuzzing** (Fred de Beer)

Fuzzing has been around for several years and is a popular method for attackers to hack products. Applying fuzzing in practise for product developers though can be difficult. In this session, we will elaborate on our vision how to integrate fuzzing in the software development lifecycle for embedded software and demonstrate a prototype within True Code that shows how this vision can be made practical.

1-5 **19:00 – 19:30** **Riscure 1: Inspector Updates** (Erwin in 't Veld)

A new release of Inspector has been made available in 2021. In this session our Product Manager, Erwin in 't Veld, will give a wrap up of the most important developments and changes, will demonstrate various features present in the latest release and discuss some of the roadmap topics for the upcoming releases.

Day 2 – Tuesday, September 7, 2021 - CET

2-1 **8:00 – 08:30** **Riscure 2: Hardware Updates** (Erwin in 't Veld)

New hardware products for security testing have been releases in 2021. In this session, Erwin in 't Veld will discuss these new devices and their technical specifications. Next some of the upcoming hardware developments will be discussed.

2-2 **10:00 – 10:30** **R&D 3: Failure Analysis for SCA Optical Beam Induced Current** (Dennis Vermoen)

Yet another method that is often applied in failure analysis. OBIC can help to get detailed information about the assets and power domains present on a chip. Next this information can be used to be more successful in a fault injection attack. Dennis will talk about the specifics of this method and will show some interesting results coming out of experiments conducted at Riscure. Also the setup used to obtain these results will be covered.

2-3 **13:00 – 13:30** **Attacks 2: Exploiting QSEE, the Raelize way! - Part 1** (Niek Timmers & Cristofaro Mune from Raelize)

Raelize identified multiple critical software vulnerabilities in QSEE, Qualcomm's Trusted Execution Environment (TEE), on Qualcomm IPQ40xx SoC devices. Raelize exploited these vulnerabilities in order to execute arbitrary code at the highest privilege. As these vulnerabilities are software vulnerabilities, they were easily fixed by Qualcomm after Raelize disclosed them responsibly. Raelize likes to look further than just software vulnerabilities. Therefore, Raelize decided to analyse the resilience of the Qualcomm IPQ40xx SoC towards Electromagnetic Fault Injection (EMFI) as well.

2-4 **17:00 – 17:30** **R&D 4: Glitch Needle** (Rajesh Velegalati)

This research presentation aims to answer the primary research question: Can an attacker perform fault injection attack on a full featured mobile device under restricted control condition that no hardware modification is allowed on the target? We chose Voltage and Electro Magnetic transient pulses (VFI/EMFI) as the avenues of injecting a fault into the target for our research purposes. We investigate various hardware restrictions present in form factors phones that would restrict the propagation of injected faults (Voltage and EM mediums) and identified the mitigating factors present in full featured phones. Based on our research study, we present a new approach to inject voltage glitches into the form factor target. We present our results and the control conditions under which we can perform VFI using new approach on a form factor smart phone by targeting Proof-of-Concept test applications running on the target devices.

2-5 **19:00 – 19:30** **SC 2: What's Hot & What's Happened: Software** (Marc Witteman)

During this 30-minute talk, our CEO Marc Witteman will share his thoughts on recent market developments regarding software related security topics and gives an insight on his expectations of trends that have a chance to become mainstream in the near future. Topics that will be covered amongst other things: 'Amnesia-33' and 'Obtain remote code execution in Whatsapp'.

Registration: www.riscure.com/riscure-workshop

Access previous workshops and content: www.welove.fi

Contact us: inforequest@riscure.com

Day 3 – Wednesday, September 8, 2021 - CET

3-1 **8:00 – 08:30** **SC 3: Simulation** (Fred de Beer)
Fault Injection simulation has been introduced to True Code last year. Based on customer feedback, behaviour and user interface have been improved. In this presentation, Fred de Beer will explain our choice for a netlist hardware simulator, explain how to use Fault Injection simulation for your software inside True Code and show a comparison of our two netlist simulators for RISC-V and ARM cortex-m0.

3-2 **10:00 –10:30** **Q&A: First Session**

3-3 **13:00 – 13:30** **R&D 5: FIRM – Comparing Pre and Post Silicon** (Erwin in 't Veld)
Fault Injection is a method that is often used by hackers to break into products that need to be secure. Riscure has been working on ways to detect fault injection vulnerabilities in the design phase of a product. In this session we will discuss the similarities between fault injection results obtained from a design simulation compared to fault injection tests on a physical chip. The results will be discussed based on FIRM tests (Fault Injection Resistance Metric), a metric being designed by Riscure to help product vendors to assess the quality of their products against fault injection attacks.

3-4 **17:00 – 17:30** **Attacks 3: Exploiting QSEE, the Raelize way! - Part 2** (Niek Timmers & Cristofaro Mune from Raelize)
Raelize identified multiple critical software vulnerabilities in QSEE, Qualcomm's Trusted Execution Environment (TEE), on Qualcomm IPQ40xx SoC devices. Raelize exploited these vulnerabilities in order to execute arbitrary code at the highest privilege. As these vulnerabilities are software vulnerabilities, they were easily fixed by Qualcomm after Raelize disclosed them responsibly. Raelize likes to look further than just software vulnerabilities. Therefore, Raelize decided to analyse the resilience of the Qualcomm IPQ40xx SoC towards Electromagnetic Fault Injection (EMFI) as well.

3-5 **19:00 – 19:30** **Riscure 3: True Code Updates** (Swetha Yennu)
Several releases of True Code have been made available in 2021. In this session our Product Manager, Erwin in 't Veld, will give a wrap up of the most important developments and changes and will also demonstrate various features present in the latest release.

Day 4 – Thursday, September 9, 2021 – CET

4-1 **8:00 – 08:30** **R&D 6: Automated FI Tuning of FI Parameters** (Erwin in 't Veld)
Building a Fault Injection setup can be challenging by itself, but after the next concern is to find the right set of parameters to increase the chance of being successful. In this session our product manager will show the latest developments in our fault injection software and how these can help find the best possible combination of parameters.

4-2 **10:00 –10:30** **Riscure 4: Training Academy – Effective Learning Approach** (Alex Goumans)
In 2021, Riscure launched a brand new on-line training platform with lots of new training content. In this session, Riscure's Training Academy product manager Alex Goumans, will elaborate on effective learning programs and share details on the new platform and the various training courses that align with modern training practices.

4-3 **13:00 – 13:30** **R&D 7: When Hardware Attacks Scale** (Marc Witteman)
How can a simple FI vulnerability SCALE into a disaster? Many Fault Injection attacks start with something simple but can scale into a logical remote attack.

4-4 **17:00 – 17:30** **Q&A: Second Session**

4-5 **19:00 – 19:30** **Attacks 4: Hackers vs. Security Labs** (Jasper van Woudenberg & Colin O'Flynn from NewAE Technology)
"That's out of scope, said no attacker ever" is a tongue-in-cheek saying that echoes in offensive security circles, and it's true. On the flipside, "We have infinite time and money, said no certification customer ever" is just as true. In practice, this means certified products have a testing scope. In this presentation we take examples of publicly known attacks, explain how they work, and look at them from a security lab perspective.

Day 5 – Friday, September 10, 2021 – CET

5-1 **8:00 – 08:30** **Attacks 5: Drone Attack** (Gabriel Gonzalez - IOActive)
Unmanned aerial vehicles (UAVs) and other unmanned vehicles (drones) are becoming increasingly popular for use by governments, companies, and individuals. Since UAVs are frequently used for illegal or military purposes, there is a requirement for organizations to be able to perform forensic analysis on captured UAVs to gather evidence or intelligence. These vehicles have varying levels of security with more advanced ones being resistant to many typical embedded device attacks. Our interest is in developing one or more side channel attacks on commercially available UAVs to demonstrate the viability of side channel attacks against hardened UAVs.

5-2 **10:00 –10:30** **R&D 8: Research @Riscure** (Durga Ramachandran)
@Riscure we conduct research on several security related topics. This includes research focused on hardware related topics and software related topics as well. In this session, Durga will cover the research that has been conducted in the past year. Tell about the successes that have been reached, but also elaborate a bit on the research of which the results were not what was expected upfront.

5-3 **13:00 – 13:30** **Riscure 5: IoT Certification** (Bernie Rietkerken)
Despite the obvious observation that massive deployment of devices that are connected to the Internet must lead to substantial security risk, we still see hesitance and question marks on IoT device makers side when it comes to investing in security. Absence of a market pull for secure products, in combination with fragmentation in standardization and regulation, don't help. This is where component or platform level security certification comes to the rescue. This presentation is about the options available for IoT component certification and the benefits it brings to component developers as well as device makers.

5-4 **17:00 – 17:30** **R&D 9: Old Skool – 20 ways past Secure Boot** (Job de Haas)
A presentation from 2014 where Job de Haas is showing a live demo of EM-FI on a secure boot and 19 other ways to bypass Secure Boot. Perhaps a bit ahead of it's time but still very relevant. Enjoy this Old Skool Presentation!

5-5 **19:00 – 19:30** **SC 4: Training Academy – Secure Coding** (Rafael Boix Carpi)
Secure coding is becoming more and more important for vendors to properly protect products from hackers with malicious intent. How do you make sure your development team has enough insight and be able to stay at the edge of things to be effective? In this session our Principal Trainer, Rafael Biox Carpi will present Riscure's way to help your development team in the best possible way.

Registration: www.riscure.com/riscure-workshop

Access previous workshops and content: www.welove.fi

Contact us: inforequest@riscure.com

Program Matrix

Start time ▼ / Day ▶	Monday September 6 (Day 1)	Tuesday September 7 (Day 2)	Wednesday September 8 (Day 3)	Thursday September 9 (Day 4)	Friday September 10 (Day 5)
8 am UTC+2 2 pm UTC+8 11 pm UTC-7	**R&D** session 1 1-1	**Riscure** session 2 2-1	**Secure Coding** session 3 3-1	**R&D** session 6 4-1	**Attack** session 5 5-1
10 am UTC+2 4 pm UTC+8 1 am UTC-7	**Attack** session 1 1-2	**R&D** session 3 2-2	**Live Q&A** session 1 3-2	**Riscure** session 4 4-2	**R&D** session 8 5-2
1 pm UTC+2 7 pm UTC+8 4 am UTC-7	**R&D** session 1 1-3	**Attack** session 2 2-3	**R&D** session 5 3-3	**R&D** session 7 4-3	**Riscure** session 5 5-3
5 pm UTC+2 11 pm UTC+8 8 am UTC-7	**Secure Coding** session 1 1-4	**R&D** session 4 2-4	**Attack** session 3 3-4	**Live Q&A** session 4 4-4	**R&D** session 9 5-4
7 pm UTC+2 1 am UTC+8 10 am UTC-7	**Riscure** session 1 1-5	**Secure Coding** session 2 2-5	**Riscure** session 3 3-5	**Attack** session 4 4-5	**Secure Coding** session 4 5-5

Local Hands-On Workshops

Registration: www.riscure.com/riscure-workshop

Access previous workshops and content: www.welove.fi

Contact us: inforequest@riscure.com