Riscure Workshop 2019 Program

Day 1:

8:45 Reception

9:15 What's Hot & What's Happened

During this 45-minute talk, our CEO Marc Witteman will share his thoughts on recent market developments and gives an insight on his expectations of trends that have a chance to become mainstream in the near future.

10:00 ARM PSA, SESIP and other IoT certification initiatives

The ARM Platform Security Architecture (PSA) offers a framework for securing connected devices. It provides a step-by-step guide to building in the right level of device security, reducing risk around data reliability, and allowing businesses to innovate on new ideas to reap the benefits of digital transformation. The Security Evaluation Standard for IoT Platforms (SESIP) defines a standard for trustworthy assessment of the security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains. In this session we will share our view on emerging IoT certification initiatives and discuss how Riscure can help customers with implementing and verification.

10:45 Inspector Cloud

Cloud computing is emerging all around us. Riscure developed a cloud environment for side channel analysis, first aimed at the IoT market and universities. During this session we will discuss the workflow principles to do side channel analysis in our cloud environment, the brand new user interface, have a live demo and give a preview on future developments.

10:45 Coffee break – 'take a close look at our demo setups'

11:30 Deep learning

During this talk our Deep Learning expert Guilherme Perin will discuss the latest developments on Deep Learning for side channel analysis including Neural Network Model Assessment for Side-Channel Analysis and he will share some of the research topics we have on our agenda for the upcoming months.

12:30 Lunch

13:30 Lateral laser fault injection attack

Our valued customer Applus will host this session on laser attacks and specific positioning of the target.

14:00 Inspector releases

In 2019 Inspector version 2019.1 is already released, Inspector 2019.2 will be available soon and towards the end of the year yet another Inspector release is planned. During this session we will cover the highlights of both releases, show short demonstrations and give guidance on how to start using them. We will also share what is in the upcoming release and roadmap topics for 2020.

15:00 Coffee break – 'take a close look at our demo setups'

15:30 Fuzzing

In this talk we present a syzkaller inspired fuzzing framework for OP-TEE using an unmodified version of AFL with coverage tracking integrated in the TEE kernel using compile-time injected hooks. This framework can be used to test any code running in the kernel such as the interface exposed to the non-secure the world, as well as trusted applications embedded in the kernel and the system call interface by providing the coverage data to the non-secure world. We discuss the challenges of fuzzing a (trusted) operating system running nonvirtualized on an actual device as well as our approach that allows using an unmodified version of AFL running as Linux application in the non-secure world. Additionally, we discuss how we created a useful set of initial inputs to seed AFL. The approach discussed in this talk is not limited to OP-TEE but could be used for any (trusted) operating system.

16:45 Drinks and a guided tour through the automobile museum

18:45 Gather for transfer to dinner location in the harbour of Scheveningen

Riscure Workshop 2019 Program

Day 2:

8:45 Reception

9:15 Finding security vulnerabilities in software

A lot of software being written needs to be secure. Secure against all kinds of attacks that would allow an attacker to gain control over the system in a way that it could compromise the legitimate user of the software and the device it is running on. To prevent this code reviews are being done to find vulnerabilities and give feedback to the development team so that they can resolve them. This however is not an automated process and therefor a good candidate to improve efficiency and quality. In this session one of our principal developers will discuss Riscures view on efficiently end (semi) automated review of source code.

10:15 Simulation – secure devices during development

Check SCA and FI resistance during development. Gaining insight in vulnerabilities during development could not only save a lot of time but is also very cost efficient. Riscure is developing a solution that will allow you to discover vulnerabilities early and easy. During this session we will discuss our approach and show a demo.

11:00 Coffee break – 'take a close look at our demo setups'

11:30 Hardware & Tools Update

During 2019 Riscure will introduce several new upgrades for the hardware tools that enable side channel analysis or fault injection. In this session we will cover all new developments and discuss their practical use cases and give a demonstration.

12:30 Lunch

13:30 Injection FI countermeasures in Software

Preventing fault injection vulnerabilities in software is important but difficult. Developers need to keep track of a lot of things and besides that the number and type of attacks and vulnerabilities constantly change. Helping out by injecting countermeasures automatically could be a way to make life easier. In this talk we will demonstrate a prototype and discuss our approach.

14:00 Riscure prototypes

At Riscure we develop a lot of prototypes to test new things or improve our current features. Not all of them end up in one of our Inspector releases that fast. In this session we want to share a couple of our prototypes and discuss specifics. Customers can indicate if they would be interested to try.

14:45 Coffee break – 'take a close look at our demo setups'

15:30 Brain

Security evaluations are usually difficult and there are a lot of things that you will need to keep track of. How do you make sure you don't forget important things and how do you cope with efficiently guiding juniors in your team. We will show Riscures approach and tool to inspire you and to get feedback on our direction.

16:00 Research @ Riscure

17:00 Closing