riscure

Program

Riscure User Workshop 2018

Day 1

9:00 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 Deep learning: tuning your network efficiently

Deep learning is a promising technology that already shows some good results in side channel analysis. Setting up a neural network that is optimized for a side channel analysis though can be quit complicated. How to approach this will be explained in this session with practical examples on how to best tune your network and get results in the shortest time possible.

10:45 Coffee Session 1

11:30 Invited Speaker: Daniel Gruss PhD – Graz University of Technology

Software-based Microarchitectural Attacks: Meltdown and Spectre

In this talk, we will discuss software-based microarchitectural attacks, with a focus on Meltdown and Spectre. We will discuss memory timing and cache attacks. After building our first cache attack we will directly continue with Meltdown and Spectre. We will also discuss the more recently discovered Foreshadow attack. The talk will provide a detailed explanation of how these attacks fundamentally work. We will discuss countermeasures to protect against these attacks. Finally, we will discuss how we got into this situation with microarchitectural attacks and what we can learn from this development.

12:30 Lunch

13:45 Find software vulnerabilities efficiently

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.

14:30 Extracting secrets from "secure" devices

In this practical session we will use the Riscurino hardware platform to run a secure storage. We will attack the provided implementation and show a complete attack path, from receiving a black-box device, to extracting its content. We will explain why it is possible to extract secrets from secure software running on insecure hardware

15:15 Coffee Session 2

16:00 Accelerating fault injection with Python

Riscure has developed a Python framework that can be used execute FI attacks efficiently and in a flexible, extendable way. This framework will be available for customers in the upcoming Inspector release. In this session we will show you the framework and demo the possibilities. Next to that we will show some upcoming features that are planned for 2019

16:45 FI in Automotive: Attacks on the UDS protocol

For years, attackers exploited trivial vulnerabilities in these diagnosis protocols to bypass this authentication, but state-of-art implementations make it impossible to simply logically bypass the security. This talk presents fault injection as a technique to bypass the security of diagnosis protocol implementations, with special focus in UDS, that is protected against traditional logical attacks because they do not contain any logical vulnerabilities. This also illustrates the risk of an implementing a vulnerable diagnosis protocol since it could serve as entry point for a scalable attack.

17:30 Closing

19:00 Dinner

Day 2

9:00 Reception

9:15 Deep learning: Leakage assessment in protected AES implementations

Deep learning is currently more and more used in side channel attacks. Most examples though are on unprotected, simple targets, In this session we will show how we have applied deep learning on a protected AES implementation. Next to that we will discuss general deep learning techniques and show some visualization features on neural networks that will become available in the next Inspector releases.

10:00 Inspector releases

In 2018 Inspector version 2018.1 and 2018.2 were released and towards the end of the year yet another Inspector release is planned. During this session we will cover the highlights of both releases and give guidance on how to start using them. We will also share what is in the upcoming release and roadmap topics for 2019

.

10:30 Coffee Session 3

11:15 Invited speaker: Paul Wooderson, Cybersecurity Principal Engineer & Team Leader, Vehicle Resilience HORIBA MIRA

Security and resilience for cyber-physical automotive systems

12:15 Lunch

13:30 Practical Application of BBI

BBI (body-bias injection) is a relatively new technique in fault injection which has been adopted by several security testing schemes. In this session we will explain the characteristics of these attacks, when to use it compared to other attack methods, specifics about BBI equipment and how to use it in a setup.

14:00 Hardware & Tools Update

During 2018 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

14:45 Coffee Session 4

15:30 Guiding development: Fault injection simulation in hardware and software

Fault Injection can be a way that attackers can use to compromise a device or extract key material. Vulnerabilities for these attacks though are quite often are discovered in the last stages.

16:00 Research @ Riscure

17:00 Closing

Amsterdam,
The Netherlands

Seoul,
South Korea

Shanghai,
China

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road, Shanghai
200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com