riscure

Program

Riscure User Workshop 2018 - Korea

9:00 Reception

9:15 What's Hot & What's Happened / Research @ Riscure

During this 60 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 and combine this with our current research at Riscure.

10:15 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

11:00 Coffee Session 1

11:45 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.

12:30 Lunch

13:30 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

14:15 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.

15:00 Coffee Session 2

15:45 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.

16:15 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.

16:45 Question and Discussion

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