

# INSPECTOR

## USER WORKSHOP 2009








# PROGRAMME



**Riscure**

**Do you have a strong interest in the latest developments in the field of side channel testing? Would you like to receive tips on how to get the most out of Inspector? In that case, you should attend this year's Inspector User Workshop. On 3 and 4 June 2009, the workshop again takes place in the comfortable setting of the Krasnapolsky hotel in the centre of Amsterdam.**

The two-day workshop, which falls under the Service Contract at no additional cost, has several objectives:

-  Hear the latest developments in side channel testing
-  Exchange ideas on the best approach for side channel evaluation of crypto processors
-  Learn about the new features of Inspector 3.1
-  Learn the ins and outs of the latest Inspector hardware
-  Explore side channel analysis methods
-  Get informed on the product road map
-  Meet with other side channel specialists in an informal setting

Since the work that most of the Inspector users perform is of a sensitive nature, you can attend the workshop anonymously; your first name is what you share, any additional information exchange is up to you. Organisations that use Inspector include manufacturers, solution providers, security laboratories and government agencies.

Riscure's Inspector hardware designers, software developers and side channel cryptanalysis specialists will lead the sessions and be available for questions.



## DAY 1 SESSIONS

### What's hot & what's happened?

A Riscure specialist runs you through the recent side channel discoveries and developments. He shares a relevant selection of the side channel items with you as presented at crypto and security conferences during the past year. Further, side channel topics that got reported in the media will be discussed.

### Inspector 3.1

This session outlines the new features of Inspector 3.1.

-  **Software Modules:** These include the new ECC cryptanalytic modules, several new methods for DES analysis, a module for elastic alignment to deal with clock jitter and random program interrupt, a frequency-time plot to design frequency filters for improved signal quality, a training card with configurable cryptographic countermeasures, and a communication interface to further facilitate the testing of embedded technology.
-  **Software Core:** The updates to the core of 3.1 include GPU support to accelerate Fast Fourier Transforms in frequency filters and alignment, improved dynamic memory allocation, a clear distinction between user and system space, faster data transfer between chained frequency filters, and ten new tutorials to guide how to get the most out of Inspector.

### Hands-on EM analysis

Due to the large number of variables involved with EMA, performing a good measurement takes experience. In this hands-on session, a Riscure specialist shows the ins and outs of taking such measurement and explains what the contributing factors are when EMA yields better results than DPA. Questions from users to Inspector Support during the past year are the basis for this session.

### User experiences

This session gives insight in the experience of two users with Inspector. The user explains what his or her successes and challenges are, what works well, and what he or she would like to see improved.

### Feature requests and discussion

If you have new features that you would like to see, this is a good time to bring them forward. We will further provide an overview of the feature requests that we received from users over the past year, and what our follow up has been on these.

## DAY 2 SESSIONS

### Fault injection with VC Glitch

In 2009, fault injection hardware is added to Inspector to test chip technology. VC Glitch is the new component for performing voltage and clock glitching. The configuration and control of this ultra-fast FPGA-based glitching device is done from the Inspector software. In this session, the architect explains the design principles of VC Glitch, discusses the configuration options and provides a live demonstration on a sample card.

### Tips & tricks

In this interactive session, our specialists present several tips and tricks that can help you improve your side channel testing capabilities. Our tips are triggered by user questions and the security evaluations that we perform ourselves with Inspector.

### Introducing new DES analysis methods

This session covers the new DES analysis features. One feature is the unpublished (1) DES analysis in counter mode module. Other new features that are explained and demonstrated are the (2) DES analysis with masked input data and (3) DES analysis with a known key.

### Experiences in side channel testing of contactless cards

Side channel testing of contactless cards is a relatively new topic and this session aims to share the experiences of Inspector users. A Riscure specialist further reviews the different approaches that are taken by security evaluators and discusses their pros and cons.

### Road map 2009 – 2010

There are many new features on the road map. This session outlines these and provides estimated timelines for new additions to the platform. New features include a laser manipulation station, new cryptanalytic extensions such as template attacks, a power probe for embedded technology, and a reference signal detector for real-time triggering based on a wave form.

## SCHEDULE

### Day 1: Wednesday 3 June 2009

9:00 – 9:30	Coffee & reception
9:30 – 12:30	Sessions
12:30 – 14:00	Lunch
14:00 – 17:00	Sessions
17:00 – 18:30	Cocktail Cruise Amsterdam
19:30 – 22:00	Dinner

### Day 2: Thursday 4 June 2009

9:00 – 12:00	Sessions
12:00 – 13:30	Lunch
13:30 – 15:00	Sessions
15:00	Closing

Riscure hosts the workshop which includes handout material, coffee, lunches, a sightseeing trip, and dinner on Tuesday. As an attendee, you cover your own travelling expenses, such as flight and accommodation costs.

## VENUE

### Krasnapolsky Hotel

Dam 9, Amsterdam  
The Netherlands  
Web site: [www.nh-hotels.com](http://www.nh-hotels.com)

A special Riscure rate applies if you book this hotel before 20 April 2009. Two nearby accommodation alternatives are the NH City Centre Hotel and the Tulip Inn Dam Square. Amanda van den Berg ([vandenberg@riscure.com](mailto:vandenberg@riscure.com)) can provide you with further booking details.

### Riscure B.V.

Phone: +31 (0)15 251 4090  
Fax: +31 (0)15 251 4099  
E-mail: [inforequest@riscure.com](mailto:inforequest@riscure.com)  
Web site: [www.riscure.com](http://www.riscure.com)