








# INSPECTOR USER WORKSHOP 2008 INVITATION



**Do you have a strong interest in the latest developments in the field of side channel analysis? 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 9 and 10 September 2008, the workshop 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, has several objectives:

-  Hear the latest developments in side channel analysis
-  Exchange ideas on the best approach for side channel testing of crypto processors
-  Learn about the new features of Inspector v3.0
-  Learn the ins and outs of the EM Probe Station and RF Controller
-  Explore side channel analysis methods
-  Get informed on the product roadmap
-  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 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.

**Riscure**

[See next page for activities and schedule](#)

## DAY 1 SESSIONS

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


A Riscure specialist runs you through the side channel discoveries and developments during the past year. Amongst other things, he shares with you a relevant selection of the CHES 2008 papers along with our interpretation as well as the side channel items that the media reported on during the past year. The session further covers the latest on side channel techniques for Elliptic Curve Cryptography, contactless smart cards and crypto processors in embedded devices.


### RF Controller & EM Probe Station

In this session, you will get to know the ins and outs on the new RF Controller for testing contactless smart card technology and on the latest version of the EM Probe Station (v3.0) with automatic hotspot localisation and 3D representation in software. A Riscure specialist explains details on the hardware design and demonstrates how it is used in the most effective manner.

### Inspector v3.0

This session outlines the new features of Inspector v3.0.

 **Software Core:** The new Software Core results in faster execution of complex routines, a new menu structure, and EM surface scan analysis tools with spectral interval selection and 3d intensity display.

 **Software Modules:** These include the XTalClear feature for automatic separation of internal chip signal and external clock related signal, and 2<sup>nd</sup> order DES and 2<sup>nd</sup> order AES analysis modules to test the strength of data and key masking countermeasures.

### 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.

## DAY 2 SESSIONS

### Hands-on exercise

In front of the group, we perform an EM analysis using an interactive step-by-step approach including a data acquisition, filtering, signal processing, dynamic alignment, and cryptanalysis. As a group, you are asked to determine each next step in the analysis, with the objective to have a discussion on the pros and cons of the chosen approach.

### User experiences

This session gives insight in the experience of four 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.

### Roadmap 2009/2010

New features are on the roadmap. This session outlines these and provides estimated timelines for new additions to the platform.

## SCHEDULE

### Day 1: Tuesday 9 September 2008

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: Wednesday 10 September 2008

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

## VENUE

### Krasnapolsky Hotel

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

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. Hotel reservations are made directly with the hotel.

### 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)