

New side-channel analysis tool helps manufacturers and labs

Since the beginning of 2005, Riscure has offered companies a software tool to perform side-channel analysis (e.g. Power Analysis). It is the first side-channel analysis tool on the market with a fully graphical user interface. Evaluation labs and manufacturers can use the tool to test a smart card against susceptibility to side-channel attacks and to rapidly implement their own new side-channel analysis techniques. This article discusses the existing problems of manufacturers and labs with side channel analysis tools and it explains how Inspector addresses these problems.

Side-channel analysis has been a dangerous smart card attack technique since its discovery about seven years ago (see Figure 1). With less than US\$ 10,000 of investment, fraudsters and security professionals have been successful in retrieving secret keys from smart cards. The basics of this class of attacks are now well understood by the industry, but new attack variations and improvements are introduced regularly. Manufacturers and evaluation labs spend therefore each year considerable research efforts to ensure that new smart cards are not vulnerable to the latest side-channel attacks. Each manufacturer and evaluation lab develops its own proprietary side-channel analysis testing software.

What is side-channel analysis?

Side-channel analysis is a method for extracting information from electronic devices through analysing their physical characteristics. Rather than using the regular I/O interface, physical phenomena like timing, power consumption and electro-magnetic emissions are used. The analysis is often applied to cryptographic devices in order to investigate the leakage of secret data, such as keys and PIN codes. The results are used to identify weaknesses in the implementation of hardware and software. Side-channel analysis is an important instrument in the product development and evaluation cycle of smart cards and other secure devices and contributes to reaching a high level of security.

Figure 1 Side-channel analysis explained

These existing tools have several problems. First of all, they show a lack of flexibility to implement new side-channel attacks. Second, development and maintenance can be expensive for relatively small manufacturers and labs. Third, these tools are usually not very user-friendly as they are command-line driven. Fourth and final, effective operation is usually limited to the one or two experts that were involved with coding the tool from the beginning. So, although in the last couple of years, side-channel analysis has moved from an experimental and exotic attack class to an accepted and relatively mature one, the development of tools has lagged behind.

Another problem exists with the smaller card manufacturers that did not develop their own side-channel analysis software and therefore rely on external test labs. This has proven to be costly and time-consuming for a manufacturer that is in the process of developing a new card. In addition, the importance of protection against side-channel attacks has become paramount and sole dependence on an external lab gives a manufacturer understandably an uneasy feeling.

Riscure developed a new side-channel analysis tool called *Inspector* (see Figure 2). With Inspector, a security test professional can analyse any set of traces. A typical trace set is obtained with an oscilloscope measuring the power consumption of a smart card. Inspector supports a

variety of techniques, including Power Analysis (SPA & DPA), Timing Analysis and Electromagnetic Analysis (SEMA & DEMA). The graphical representation and manipulation of traces is intuitive to work with. Further, the tool has an open API which allows the test professional to add his own attack modules written in the Java programming language.

According to Marc Witteman, Chief Scientist at Riscure, “most existing tools for side-channel analysis are not very flexible in their design. They are cumbersome when it comes to development of new attacks, keeping in mind the trial-and-error nature of side-channel analysis research. Therefore, as an evaluation lab we decided that we needed a flexible integrated development environment. With Inspector a security analyst can boost his analysis work by updating his analysis code and testing its results within seconds.”.

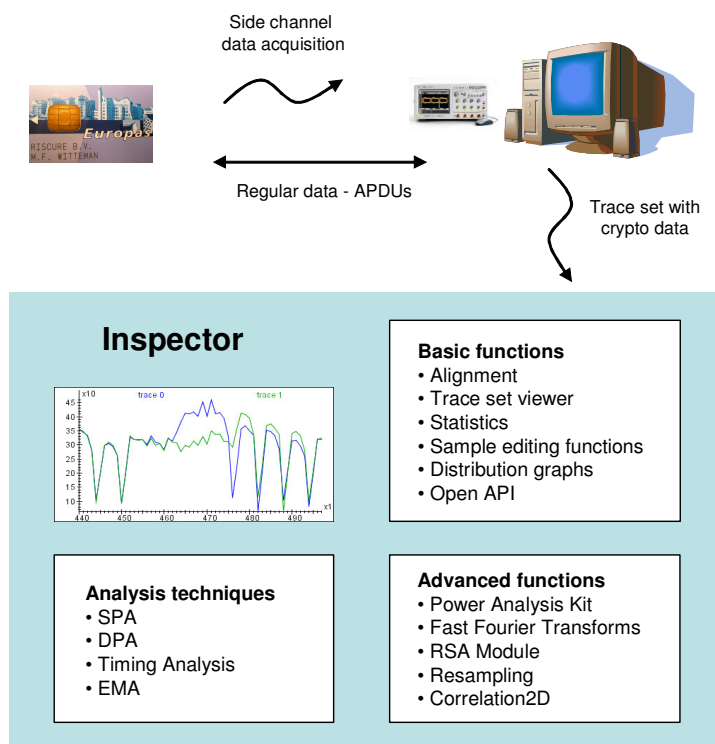


Figure 2 Overview of the Inspector tool

To get a better idea of how Inspector works, let's consider the following seven steps that a test professional typically takes when performing a side-channel attack:

	Activity	Description	Support from Inspector
1.	Data acquisition	Manufacturer or evaluation lab uses his own preferred hardware for data acquisition	Various <i>trace set formats</i> are supported. Encryption data can be combined with the trace. An acquisition module can be integrated within Inspector.
2.	Visual inspection	The test professional visually inspects one trace (e.g. what chip technology is used, wave shape, clock speed, noise)	<i>Trace set viewer</i> with graphical user interface (e.g. zoom in on a specific part of the trace with one mouse click)
3.	Identify target of attack	Identify process building blocks in the trace	Same as Activity 2. Use <i>Correlation2D</i> to analyse building blocks and program structure.

	Activity	Description	Support from Inspector
4.	Acquire a trace set	Perform large scale data acquisition from chip under attack (e.g. several days)	Same as Activity 1.
5.	Signal processing	Perform filtering, alignment and further signal processing of traces. Resampling is possibly required.	Static and dynamic <i>alignment</i> . The red part in Figure 3 is the selection of the trace to be aligned. Figure 4 shows the results. Other features are <i>Averaging, Standard Deviation, Resampling, Editing and Distribution Graphs</i> .
6.	Execute the attack	Execute the side-channel analysis attack (e.g. SPA, DPA, Timing Analysis, EMA)	<i>Correlation, Fast Fourier Transforms, Power Analysis Kit, RSA module</i> . Figure 5 shows the output of a DES attack with Inspector.
7.	Development of attack techniques	Tune existing attack techniques and develop new attacks	Attack modules are written in Java. The source code is edited inside Inspector. <i>Compiling and running new source code</i> take one button-click.

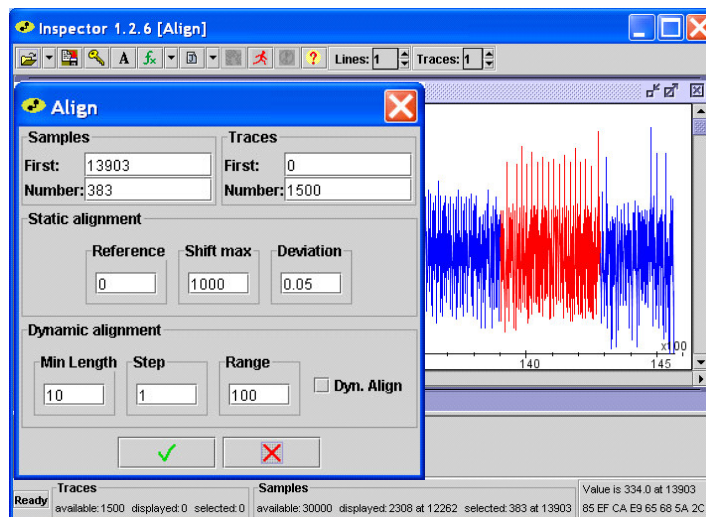


Figure 3 Alignment to be applied to the mouse-selected red section of the trace

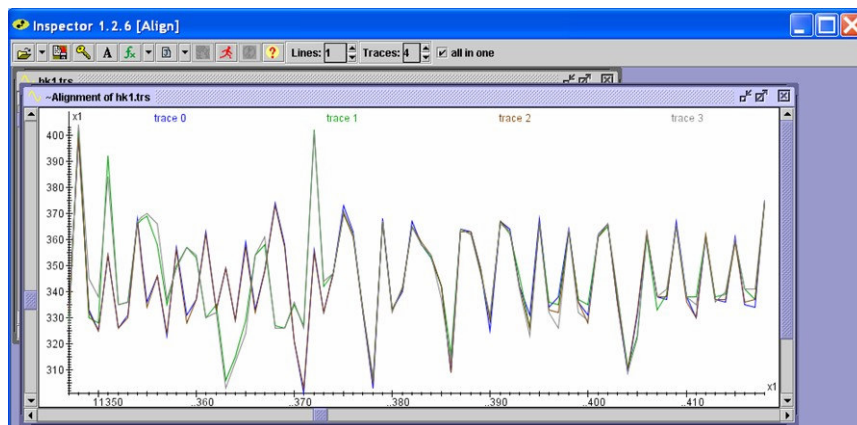


Figure 4 Multiple traces in one window after performing static alignment

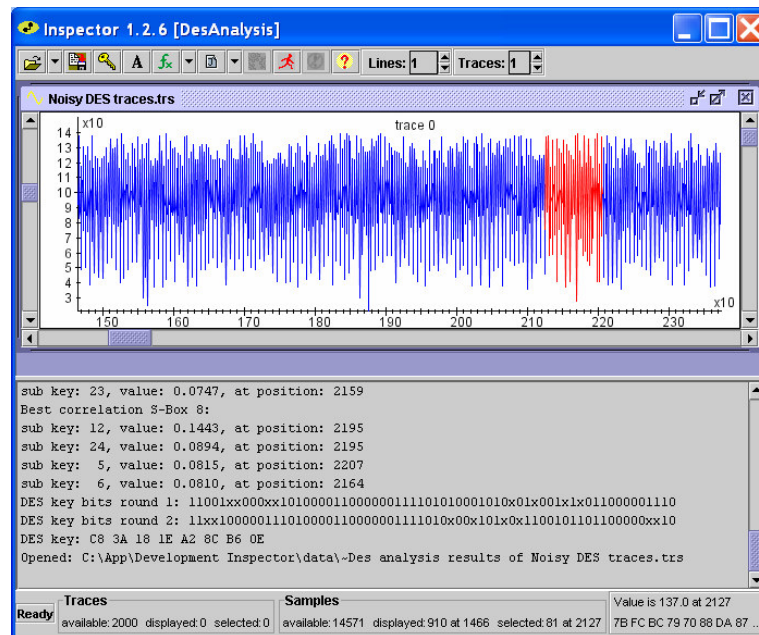


Figure 5 The output of DPA: a DES secret key obtained from the power trace of a card

After analysing Inspector, a technical manager at one of Riscure’s clients said: “When we saw Inspector, we decided to stop the development of our in-house side-channel analysis software. The time required for our own implementation of the signal processing features alone would have taken us months. With Inspector, we have more time to focus on evaluating smart cards and researching new attack techniques. The open framework of the tool is unique and it allows us to implement and tune our own attack techniques. Further, we created the option to outsource the development of new techniques which was very difficult to do when we were operating our own software.”

A card manufacturer in Western Europe commented: “We were looking for a side-channel tool that would accelerate our testing of new countermeasures. Further, the tool had to come with several existing side-channel analysis techniques to enable us to get started with this tool very quickly and expand from there. Getting our traces in the right format for the tool proved a straightforward exercise and the open API allowed us to implement our own secret analysis techniques whilst we could still use the powerful signal processing features of Inspector.”

Listening to the feedback that we received from clients, we realised that one fixed solution does not work for a side-channel analysis tool. Labs and manufacturers use different flavours of attack techniques and have different requirements for data acquisition. Therefore, we decided to customise the delivery of the tool specific for each client. This also means that the client only pays for the Inspector modules that he has selected. Looking forward, we are continually expanding a library of analysis modules to support clients that want to keep up-to-date with the newest attacks. For example, various new modules for high order analysis are under development.

About the author

Harko Robroch is director at Riscure based in the Netherlands. He has an MSc in Business Mathematics & Computer Science. Before working at Riscure, he was the Technical Security Manager at the mobile telco Orange Netherlands and worked for several years at Ernst & Young as an information security specialist. In this capacity, he conducted several research projects on the security risk of emerging internet technologies and was a speaker at several security conferences in South Africa. For years, Harko has also been a regular attendee of the Security Workgroup meetings of the GSM Association.