

bright sight®



your
partner
in security
approval

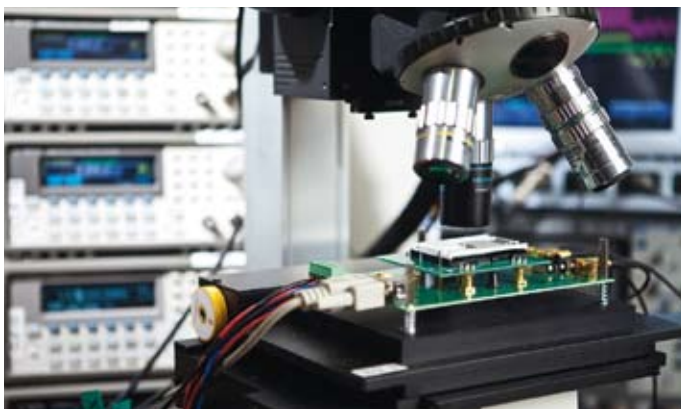


Unique Tools
from the
Security Lab

Brightlight security analysis tools – all-inclusive packages with built-in added value

Our evaluation and consultancy services facilitate a highly efficient design of secure IT products according to individually specified security conditions. During product development we provide our customers with additional security tests, which rule out potential product risks prior to the large-scale rollout and make an official approval easier.

All our expertise flows continuously into the development of innovative analysis and testing methods which, combined with sound technological knowledge in the field of data security, has created a range of unique methods and tools.



The Brightlight hardware mounted in a laser set-up.

Brightlight

Improving resistance against laser manipulation

Secure micro controllers are designed to protect the confidentiality and the integrity of sensitive information. Laser manipulation disturbs the normal hardware and software operations with the risk of bypassing security functionality or dumping secret information.

Product profile

- Brightlight is a state-of-the-art laser manipulation tool for testing the susceptibility of secure micro controllers and investigating the resistance of a final product to laser-controlled perturbation.
- Brightlight was developed by the Brightsight experts in 2004 and is today one of the most reliable test tools worldwide in the area of laser manipulation for embedded systems.

Features

- Brightlight controls a number of peripherals that are necessary for laser manipulation:
 - Function generators to accurately trigger laser pulses
 - Oscilloscopes for real-time power consumption analysis of program execution
 - XY-table for automated surface scanning
 - Physical interface for communication with the micro controller.
- Brightlight is fit for metal as well as silicon side attacks.
- Brightlight combines standard, commercially available equipment with unique Brightsight hardware and software:
 - MATLAB® scripts and graphical user interface to control the hardware components of a laser set-up
 - Physical interface to connect the micro controller with the MATLAB® environment.

Benefits

- Brightlight is the ultimate tool to get meaningful results with laser manipulation techniques and to verify the strength of implemented countermeasures.
- Brightlight creates a flexible workbench and an easy to use environment for laser manipulation in combining MATLAB® with customized Brightlight scripts and off-the-shelf hardware.

Sideways

Safeguard against side channel attacks

Side channel analysis (SCA) is used to test whether cryptographic devices are leaking information as well as to validate the level of resistance against side channel attacks, such as power analysis (DPA) or electromagnetic analysis (DEMA).

Product profile

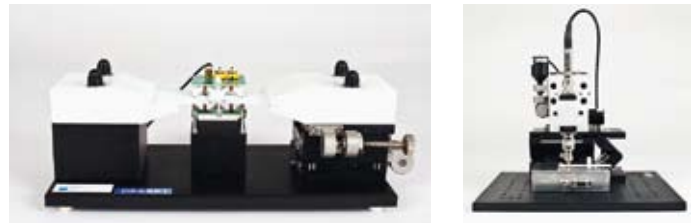
- Sideways offers chip manufacturers and software developers a tool to validate the quality of countermeasures against realistic security threats like DPA and DEMA.
- Sideways was developed in 1998 and has been continuously adapted to the latest relevant security requirements.

Features

- Sideways supports the analysis and evaluation of a range of physical data from cryptographic devices like
 - Power consumption profiles (SPA/DPA)
 - Electromagnetic data (SEMA/DEMA)
 - Contact and contactless interfaces (DPA on contactless)to test whether confidential or secret information is leaked at the point of use.
- Sideways includes software modules for data acquisition and data analysis as well as a dedicated card reader.
- The Graphical User Interface (GUI) is configured as a multi-document interface, providing an intuitive and practical way of working.
- All Sideways software modules are compatible with Microsoft Windows.

Benefits

- Incorporating Brightsight's Sideways as an integral part of the development process ensures maximum product integrity and effectiveness.
- Early application of Sideways contributes to completing a secure product on time and on budget.
- Research laboratories and government agencies benefit from the use of Sideways in their decision-making processes, when evaluating or acquiring secure IT products.



The Sideways evaluation board in a running set-up (top). Balanced measurement set-up for DPA on contactless (left). EM measurement set-up (right).

Integrated approach when it comes to proving security

The Brightsight security analysis tools are provided as all-inclusive package solutions, exclusively for internal use. The tools have been developed in-house and are successfully put to test in literally hundreds of complex high-standard evaluations (Common Criteria). Each tool generally includes:

- Software for data collection and software for data processing
- All the necessary electronics and hardware that cannot be bought off-the-shelf
- Documentation of the used hardware and software
- Installation and training at the site of the customer (including shipment and travel costs)
- Support for the first year

Every installation comes with several days' comprehensive training and hands-on experience on the use of each tool. The training program can be tailor-made to meet specific customer needs. Optionally, on request, we develop and load every single tool with additional customer-specific features.

Brightscan

Effective risk management against voltage manipulation

Susceptibility to voltage manipulation is an inherent vulnerability in most micro controller designs. It is a powerful attack on secure micro controllers as nowadays found in products like pay-TV and payment cards.

Product profile

- Brightscan enables a fully automated, fast, reliable and highly repeatable execution and analysis of perturbation driven devices.
- Brightscan was introduced in 1998. The security experts of Brightsight have been using the tool very successfully in their daily work to date.

Features

- Brightscan systematically tests secure micro controllers for their resistance against voltage perturbation attacks.
- Brightscan can be applied in different types of perturbation set-ups, including light, power, probe and electromagnetic fields.
- Brightscan supports a variety of trigger sources and combinations, including reset, external trigger and IO.
- The Brightscan software is based on flexible MATLAB® scripts and controls the entire measurement set-up.

Benefits

- As successful manipulation depends primarily on perturbation timing, supply voltage, pulse duration and pulse amplitude, Brightscan explores the micro controllers' behaviour in response to changes in exactly these parameters.
- The high level of automation leads to
 - Fast results
 - Reliable reproducibility.
- The MATLAB® scripts provided with Brightscan can be fully customized and – to save money – can be integrated in individual test set-ups.



The Brightscan perturbation interface board.

Brightsight tools – saving time and money

Manufacturers, operators and research laboratories of secure IT products can utilise Brightsight's security analysis tools to their best advantage. As all tools have been continuously adapted to the latest standards, they are internationally recognized to validate state-of-the-art security products. In employing the tools from Brightsight, manufacturers can perform high-level, in-house testing during the development phase with the very same tools as used for formal evaluations. This ensures that products meet the required level of security before large-scale production.

Brightsight is your globally recognized partner in security approval of IT products

Security Evaluations and Audits, Training, Consultancy, Tools

delftechpark 1
2628 xj delft, the netherlands
p (+31) 15 269 2500
f (+31) 15 269 2555
info@brightsight.com
www.brightsight.com