riscure

What's new in Inspector 2018.3

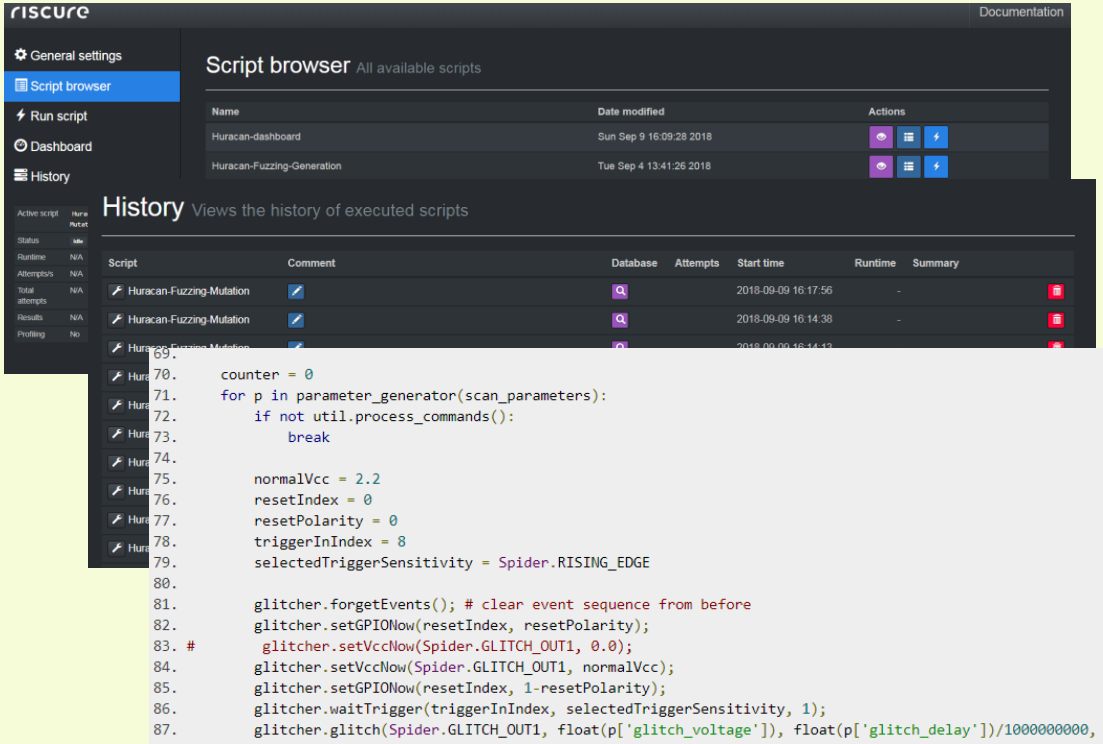
SCA & FI
software update
december2018

Contents

Page 3	**Inspector FI Python**
Page 4	**FI Spotlight**
Page 6	Automation module
Page 7	**Correlation collision**
Page 8	Pipeline
Page 9	Tektronix support
Page 10	**Upgrade procedure & SDK changes**
	• Inspector installation
	• SDK changes

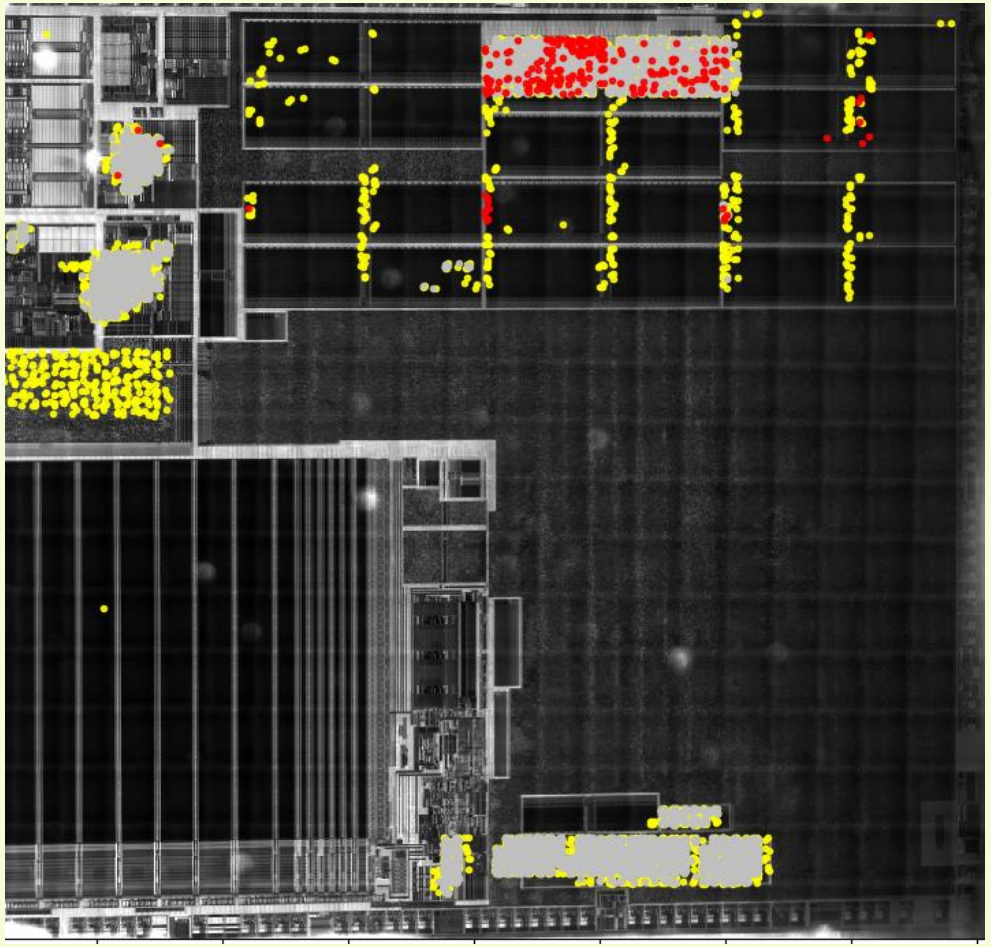
Inspector FI Python

- ✓ Intuitive user interface
- ✓ Example scripts included
- ✓ Build your own scripts
- ✓ For embedded targets
- ✓ In this release support for:
  - ✓ EM probe station
  - ✓ Spider
  - ✓ Riscure lasers
  - ✓ EM-FI
  - ✓ Picoscope



FI Spotlight

- ✓ Visualize FI results in plots or on die
- ✓ Choose out of many different plots like scatter
- ✓ Filter results to get a better view on your successes
- ✓ Use all you glitching parameters to find your sweetspot
- ✓ View during a FI session and see your results evolve

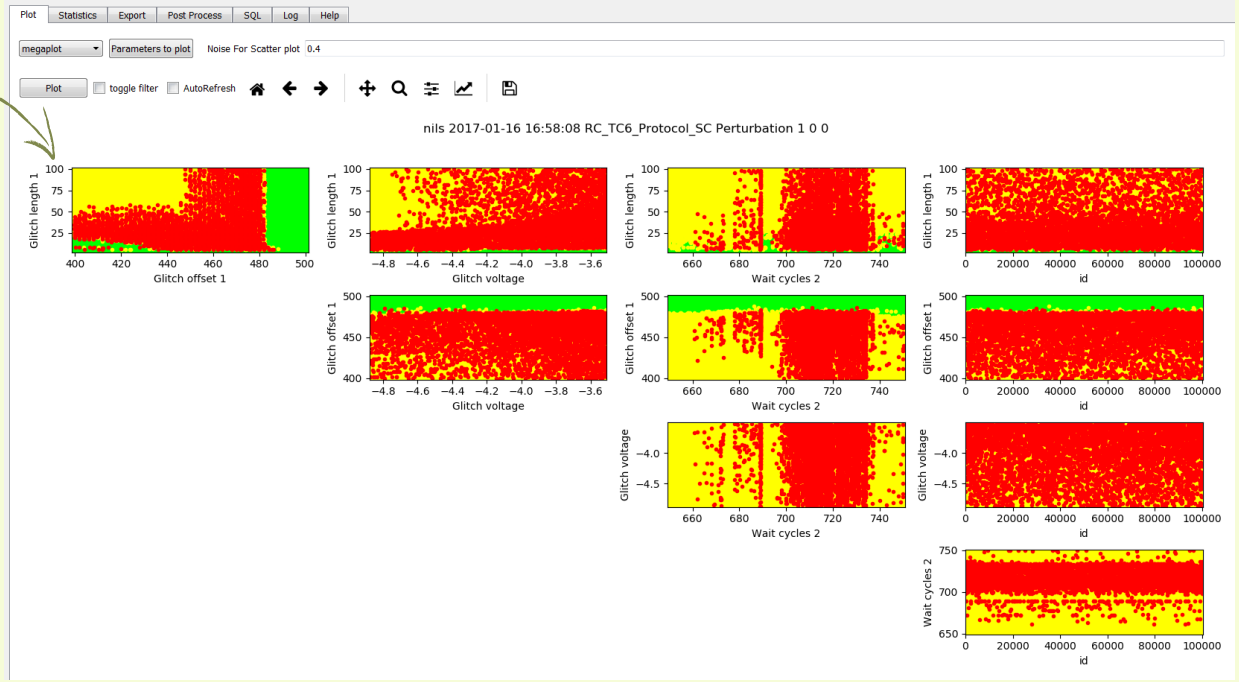


riscure

FI Spotlight

Visualize the results of a fault injection session in a way that analyzing becomes easy!

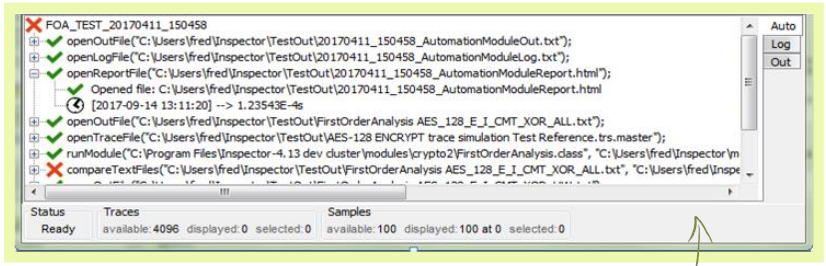
Choose different plot types and X/Y parameters and zoom in on specific area's to get detailed information on FI attempts



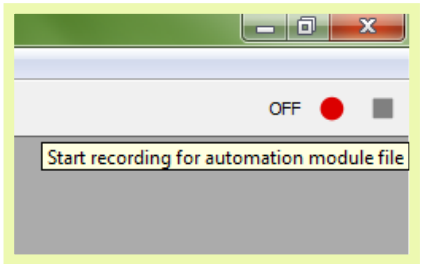
Automation & HPA

- ✓ Generates a programmable user module
- ✓ Build loops to run a automation scenario with multiple settings

- ✓ Premium subscription includes Inspector High performance Analysis
- ✓ Runs on your server
- ✓ Maximum of 10 Inspector instances supported by default
- ✓ Windows and Linux both supported



Progress of the automation scenario is shown in new “auto’ tab

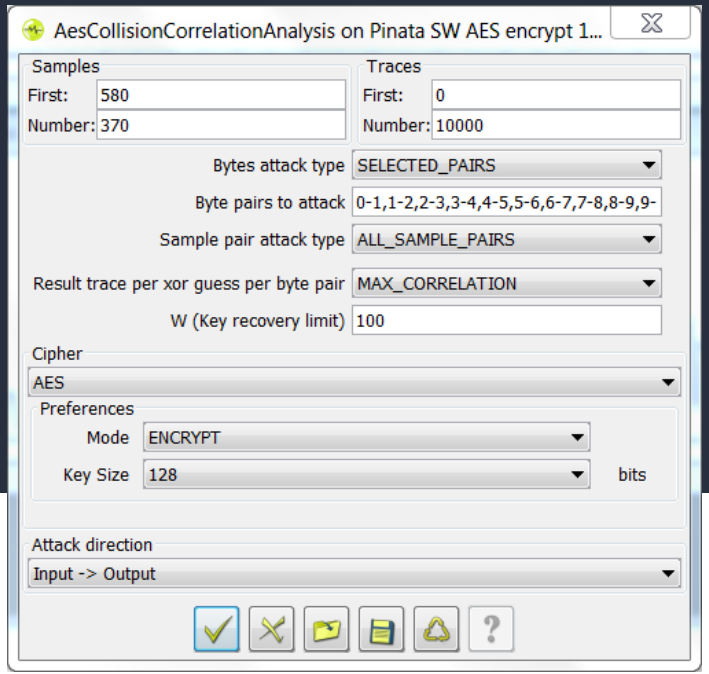


Buttons enable ‘macro like’ recording of automation scripts

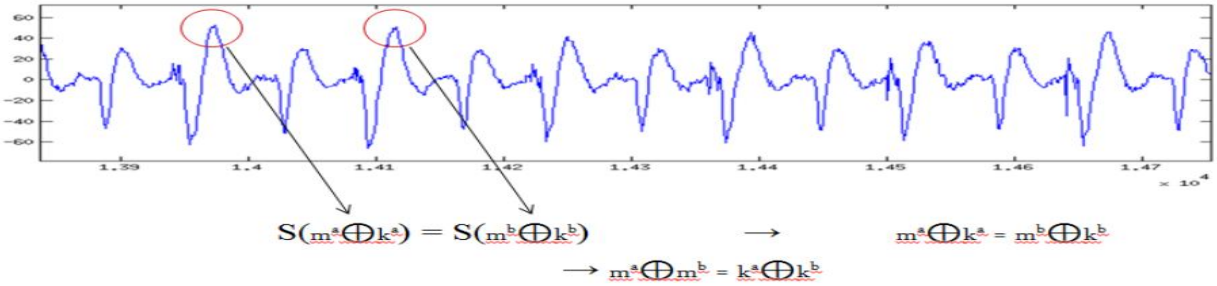
riscure

Collision Correlation module

- ✓ Works for AES cipher
- ✓ Choose to attack the collision correlation between all pairs of key bytes or only selected pairs

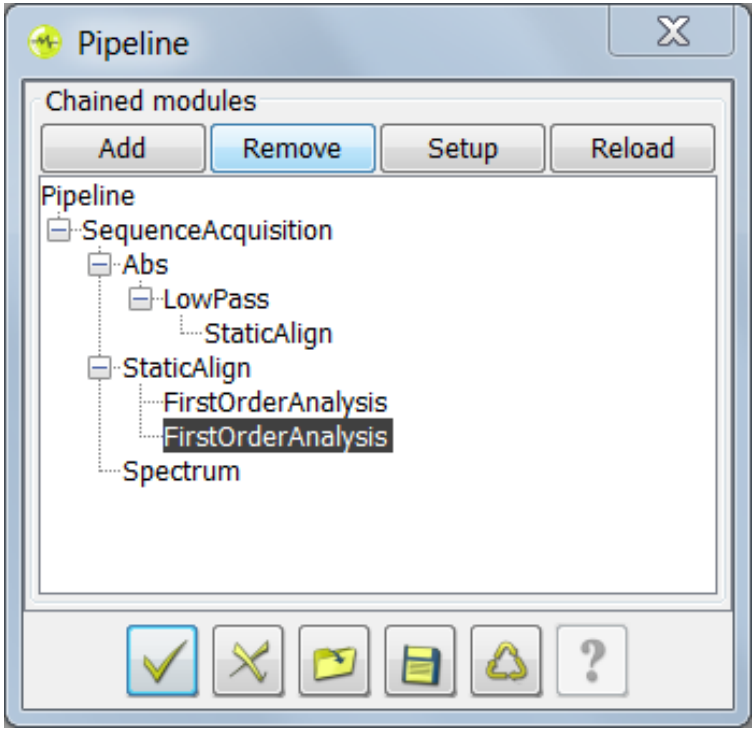


Background : The core idea of the attack is to exploit the fact that the same value after SubBytes lead to similar side channel leakages for different bytes of the input. The figure below tries to capture the theoretical essence of the attack in a visual way.



Pipeline module

- ✓ Pipeline is similar to Chain, only each module can run in a different thread
- ✓ Everything that works in Chain will also work in Pipeline, but faster
- ✓ Speed improvements is depending on the specific use case and the number of cores
- ✓ The console output of each module is redirected to a separate file



riscure

Support for Tektronix

- ✓Tektronix support based on VISA driver
- ✓Support for 5000 and 7000 series
- ✓Fast frame mode to speed up acquisition
- ✓Works next to other supported oscilloscopes: LeCroy and Picoscope

riscure

Inspector installation & SDK updates

Where

- Customers with a Subscription Contract receive a download link
- Download from Riscure license portal

Installation guidance

- Inspector software can be installed on the same PC workstation next to your previous version. You can still revert back to the previous version if you want to.
- You will need a license file next to your dongle to work with Inspector 2018.3.
- API is backwards compatible.

Your own modules & traces

- Inspector software points by default to the same user module folder as previous versions.
- In case you have trouble porting an older module to this Inspector version, please contact our support portal for assistance.

Release notes & bug fixes

For the full list of bug fixes, please refer to the release notes:
https://www.riscure.com/security-tools/inspector-sca/#support

SDK and firmware updates

Spider SDK 1.4.1

- Spider Java classes are now included as Inspector system modules. When compiling any Sequence module operating a Spider device, the system module Spider classes would be used for compilation by default.

- Rounded timing parameters of glitch() method in Spider Chronology class to nearest multiple of 4 to avoid deviation in actual timing generated by Spider device.

Database update

- Inspector 2018.3 uses a SQLite database to capture the perturbation results. The PostgreSQL database has been deprecated. A database migration option is included in the release to migrate previously stored results to the SQLite database.

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

riscure

Challenge your security