riscure

inspector 4.9

SCA & FI software update

February 2016

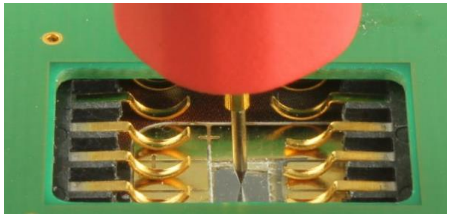
Contents

What’s new in 4.9?

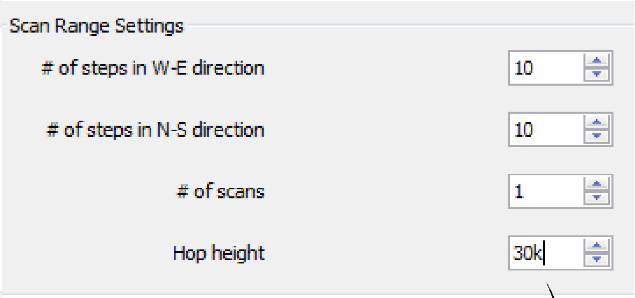
New FI hardware support

BBI probes

The needles of the new BBI probes touch the chip surface for fault injection. To avoid scratching the surface they require a hopping motion when moving to the next location.



Hop height is relative, e.g. 30k gives about 1 mm hop height for EMPS XYZ. Use 0 (default) for a traditional XY scan without hops.



Scan Range Settings

# of steps in W-E direction 10

# of steps in N-S direction 10

# of scans 1

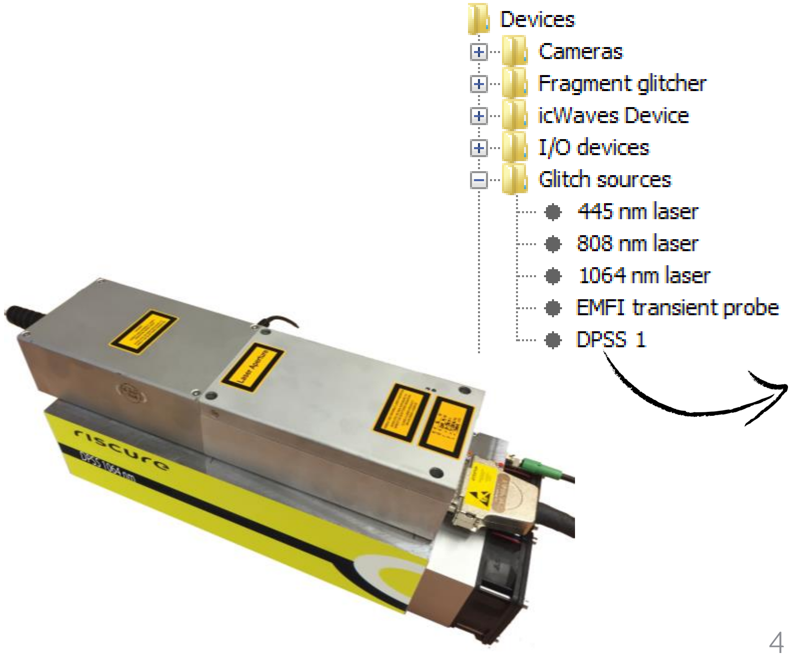
Hop height 30k

Hop height for a BBI scan

DPSS lasers

For the new green and NIR DPSS lasers you control the power output and offset as you are used to with our other laser sources. “Laser cutter type” fault injection has never been so easy!

Installation instructions are provided in the manual; note these are specific so please follow them.

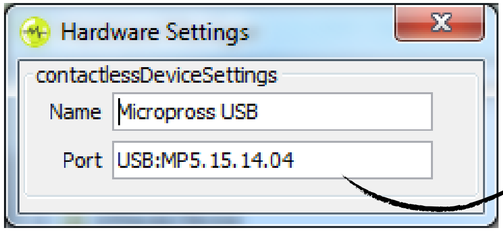


New

New settings for contactless

USB support added

In addition to TCP you can now use USB to connect to a Micropross contactless reader (MP300 and MP500). No more hub and TCP configuration issues.



Hardware Settings

contactlessDeviceSettings

Name: Micropross USB

Port: USB:MP5.15.14.04

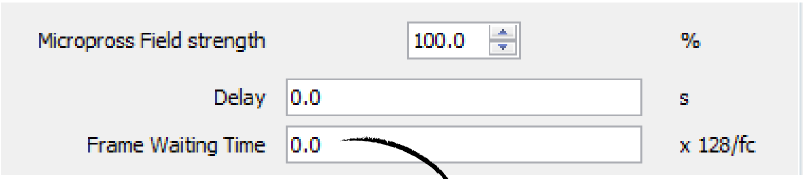
USB: add MP serial# for multiple MP devices

MP500

The MP500 TCL3 product can be used with Inspector for contactless smart cards.

Frame waiting time

When testing contactless smart cards that are unresponsive (slow) you can manually configure the frame waiting time.



Micropross Field strength 100.0 %

Delay 0.0 s

Frame Waiting Time 0.0 x 128/fc

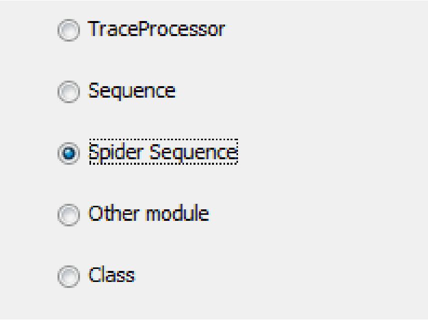
Increase for unresponsive cards

Spider & Piñata

Spider support added

A module wizard for Spider Sequence has been added. It helps you to get started with the new Spider. Further two advanced tutorials are provided for interacting with an embedded chip.

Module wizard



○ TraceProcessor

○ Sequence

● Spider Sequence

○ Other module

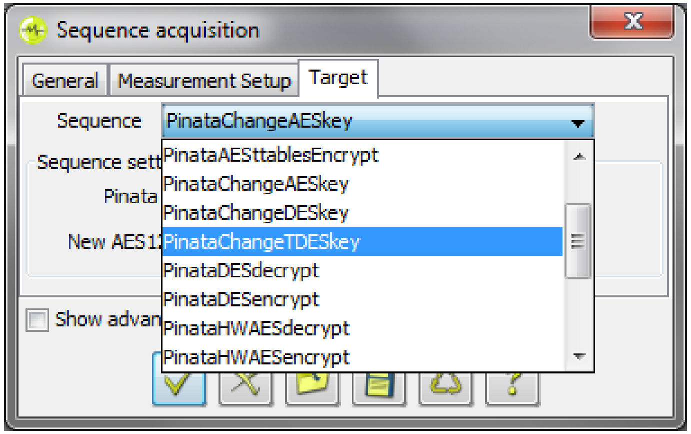
○ Class

Spider installer separated

When purchasing Spider you receive a separate software installer. It was separated from the main Inspector installer in order to improve the software distribution to you; it is more flexible for updates and you get what's relevant.

Piñata

The training board Piñata that we introduced last year has a full suite of Sequence examples for popular encryption algorithms.



Sequence acquisition

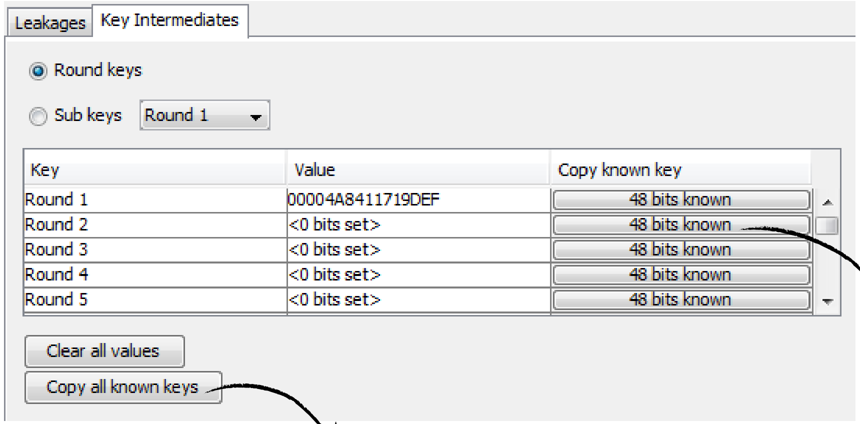
Sequence: PinataChangeAESkey

SCA crypto improvements

Manual selection of round keys

Remember getting a pop up window saying “attacked key already known” in First Order Analysis?

The approach was changed: after running DPA on one round the software does not automatically fill in the recovered round key. Instead you select what key or subkey bytes to take to the next round. Or of course, you keep analyzing the previous round.



● Round keys

○ Sub keys   Round 1

Key	Value	Copy known key
Round 1	00004A8411719DEF	48 bits known
Round 2	<0 bits set>	48 bits known
Round 3	<0 bits set>	48 bits known
Round 4	<0 bits set>	48 bits known
Round 5	<0 bits set>	48 bits known

Click to take key to next round

Copy all

Performance improvements

- Fixed the delay when starting a first order & known key analysis, when switching between encrypt / decrypt, and when switching between ciphers.
- Improved memory management when performing crypto analysis calculations, avoiding runtime failures which sometimes occurred after hour long calculations.
- More efficient implementation of the known key analysis resulting in less time to get the results.

icWaves fixes

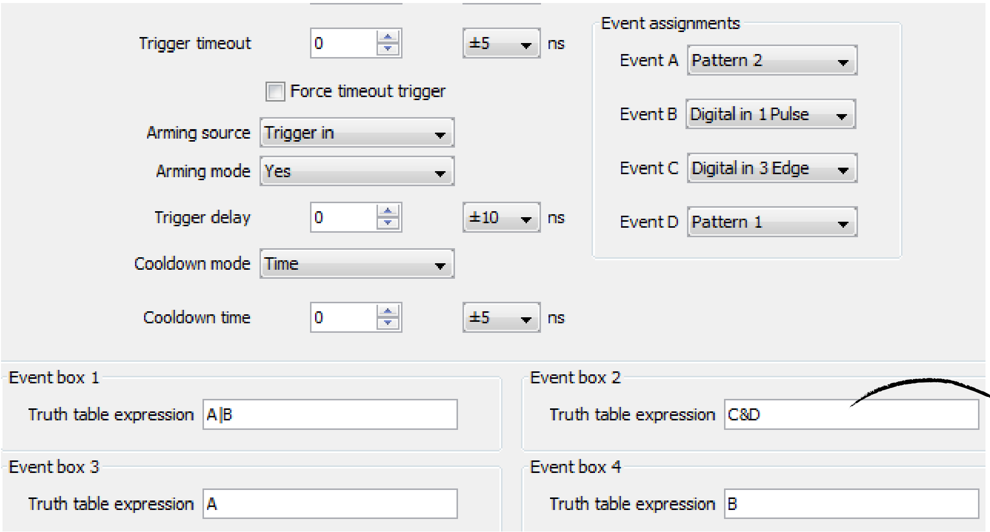
Internal state transparent

In "Expert" mode: the user now has a direct view on the internal event parameters also after disconnecting the icWaves. So you can always verify the internal state of the icWaves.

In the next few months we will work on more improvements in the icWaves GUI.

Bug fixes:

- Fixed a problem where the FPGA firmware could accidently get erased.
- We have seen cases in which the software loaded the wrong pattern into the icWaves resulting in ineffective triggering. This issue was fixed.



Trigger timeout 0 ±5 ns

□ Force timeout trigger

Arming source: Trigger in

Arming mode: Yes

Trigger delay 0 ±10 ns

Cooldown mode: Time

Cooldown time 0 ±5 ns

Event assignments

Event A: Pattern 2

Event B: Digital in 1 Pulse

Event C: Digital in 3 Edge

Event D: Pattern 1

Event box 1

Truth table expression: A|B

Event box 2

Truth table expression: C&D

Event box 3

Truth table expression: A

Event box 4

Truth table expression: B

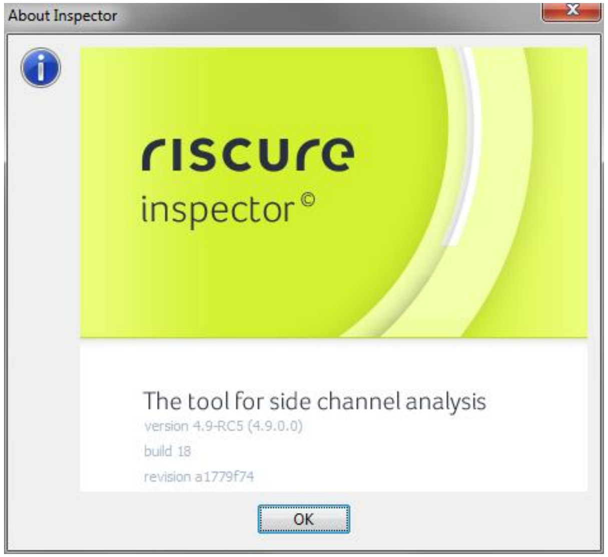
Event parameters inside icWaves are displayed (expert mode)

Miscellaneous

Version from main taskbar

We removed the version number display from the main taskbar because it caused confusion in our training material, manual and tutorials.

Click “about” to check your version number!



The tool for side channel analysis
version 4.9-RC5 (4.9.0.0)
build 18
revision a1779f74

Tutorials updated

Seven tutorials are out of date and marked “deprecated” in the tutorial section.

More replacements will follow, but in the mean time two tutorials can be used:

- Optical fault injection on a pin verification
- DPA on AES on embedded chip Piñata

which you find **in the following location** on your Inspector PC:
%PROGRAMFILES%\Inspector-4.9\doc\tutorials\AdditionalTutorials\

What’s new in 4.8.x?

4.8 was the last major release. Here we summarize the improvements in 4.8.1, 4.8.2 and 4.8.3.

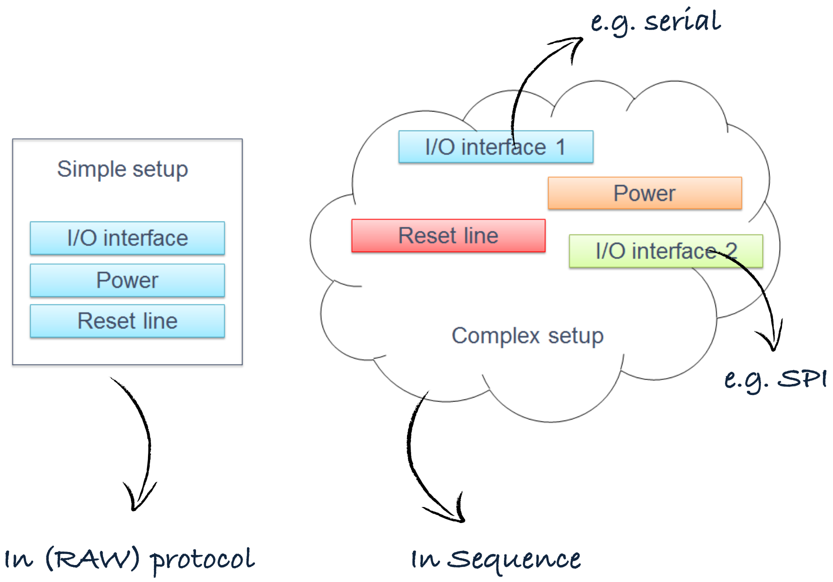
Sequence improvements

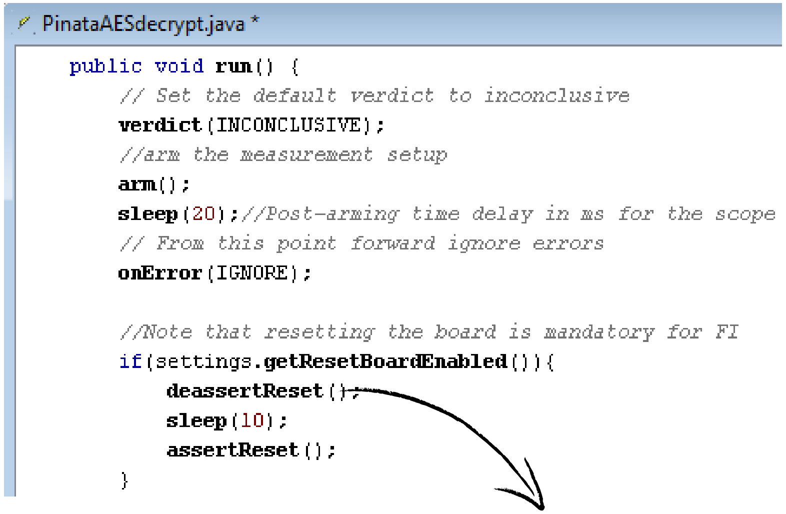
Crypto chips get more complex, and so does your side channel test environment. We made Sequence easier to use so that you can now control a complex setup with minimal effort.

Choose to have zero, one or many I/O interfaces in one setup. The same applies to power lines and reset lines.

This means that you can:

- Talk to e.g. serial, SPI and ethernet in one setup
- Run external scripts, e.g. call your external Python script
- Support and logging of additional FI parameters (e.g. voltage of each of 3 power lines)
- Script the events that you want to happen (e.g. see below)




PinataAESdecrypt.java *

```
    public void run() {
        // Set the default verdict to inconclusive
        verdict(INCONCLUSIVE);
        //arm the measurement setup
        arm();
        sleep(20);//Post-arming time delay in ms for the scope
        // From this point forward ignore errors
        onError(IGNORE);

        //Note that resetting the board is mandatory for FI
        if(settings.getResetBoardEnabled()){
            deassertReset();
            sleep(10);
            assertReset();
        }
```

Reset line control

Crypto fixes and tutorials

HMAC-SHA1 and ECC

A change to round key handling had introduced a bug not allowing you to run the HMAC-SHA1, DSA and ECDSA crypto modules. This was fixed.

Also added a new tutorial on attacking an ECDSA implementation.

High order analysis on k-ary RSA

A bug in the grouped exponentiation caused only a subset of the solution space to be searched leading to suboptimal results. This impacts only implementations with bit group size > 2.

In addition, tutorial trace and instructions were updated with a more representative example.

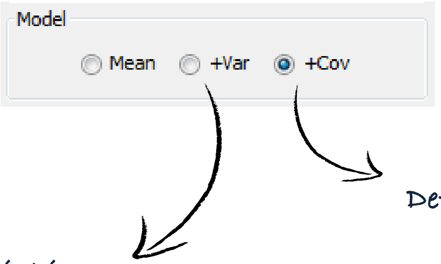
Optimized crypto attacks

Several fixes to avoid memory leaks during analysis operations and to improve the performance of the calculations. Further the brute force function works faster.

Template analysis

A method in the “blue book” (www.dpabook.org) has a bug which Inspector inherited. The blue book selects the **closest to zero** as the best value (for negative and positive key score values). However, the best key candidate is the one with the **highest** score (no matter negative or positive) as shown in the paper "Efficient Template Attacks", CARDIS 2013, section 5.1. This has been fixed.

It is an uncommon scenario in practice, we have only occasionally observed an impact from this bug in cases where the “+Var” option was selected. For impact on previous results rerun the analysis that used this option (which is not default).



Model

○ Mean ○ +Var ● +Cov

Default option

Potential impact
only with +Var

Improvements hardware support

Piñata board

Directly plug the new embedded training target Piñata into your Inspector software to start practicing your skills.

Piñata training board

Support malformed APDUs

You can send malformed APDUs to PC/SC readers in order to communicate with non-standard smart cards (e.g. FeliCa).

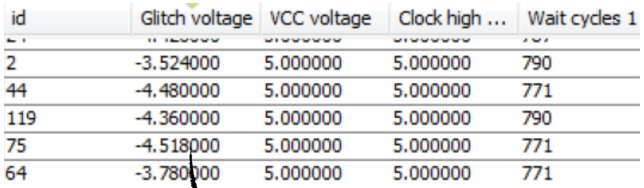
USB for EM Probe Station

EM Probe Station is now delivered with USB connection. No more serial anymore.

Finer control voltage level FI

We increased the minimum step size in perturbation modules for finer fault injection control:

- 1mV for Clock FI
- 2mV for VCC FI



id	Glitch voltage	VCC voltage	Clock high ...	Wait cycles 1
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	-3.524000	5.000000	5.000000	790
44	-4.480000	5.000000	5.000000	771
119	-4.360000	5.000000	5.000000	790
75	-4.518000	5.000000	5.000000	771
64	-3.780000	5.000000	5.000000	771

in millivolts
(0.001 V)

Upgrade procedure

Old API changes in 4.6 and 4.7

The issue

- Significant API changes were introduced in the past in 4.6 and 4.7 which caused many custom developed modules to stop running
- We did not properly document and communicate the changes, so it was very hard for you to port your custom modules
- We don't know how many users are still impacted by this

The impact

- If you keep running an old software version, you don't benefit from bug fixes and new features
- It is challenging for us to support your questions on these old software versions
- We are aware that several users still occasionally use 4.5 and 4.6, but we do not know how many of you are in this situation

The solution

- If you have custom modules in 4.5 and 4.6 that are still relevant for you, we will help you fix them to work in 4.9, free of charge! Contact our Support Portal for this
- If you use an old Inspector version for a different reason, please let us know why

In the future

We will not make undocumented changes anymore. Changes to the API will be properly communicated to you! It should not be hard to update a custom module to a new version.

Inspector 4.9 installation

Where

- Customers with Support Contract receive download link
- Download from Riscure download portal

Installation guidance

- Inspector 4.9 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.
- API is backwards compatible with Inspector 4.7

My own modules & traces

- Inspector 4.9 points by default to the same user module folder as previous versions.
- Your own modules and traces from Inspector 4.7 are compatible with Inspector 4.9.
- In case you have trouble porting an older module to this Inspector version, please contact our support portal for assistance.

SDK and firmware updates

- icWaves 3: SDK 3.6. When first using icWaves 3 with Inspector 4.9, a firmware upgrade is performed to prevent accidental firmware corruption.
- Power Tracer 4: SDK 1.4. When first using Power Tracer 4 with Inspector 4.9, a firmware upgrade is performed to prevent accidental firmware corruption.
- VC Glitcher 2: SDK 2.5. When first using VC Glitcher 2 to Inspector 4.9, firmware upgrade is performed to prevent accidental firmware corruption.

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

Please contact Riscure for more information.

You can reach us by email : inforequest@riscure.com,

by phone : +31 15 251 4090   US: +1 650 646 9979

Or on the web : riscure.com.

riscure