riscure

What's new in Inspector 2018.2

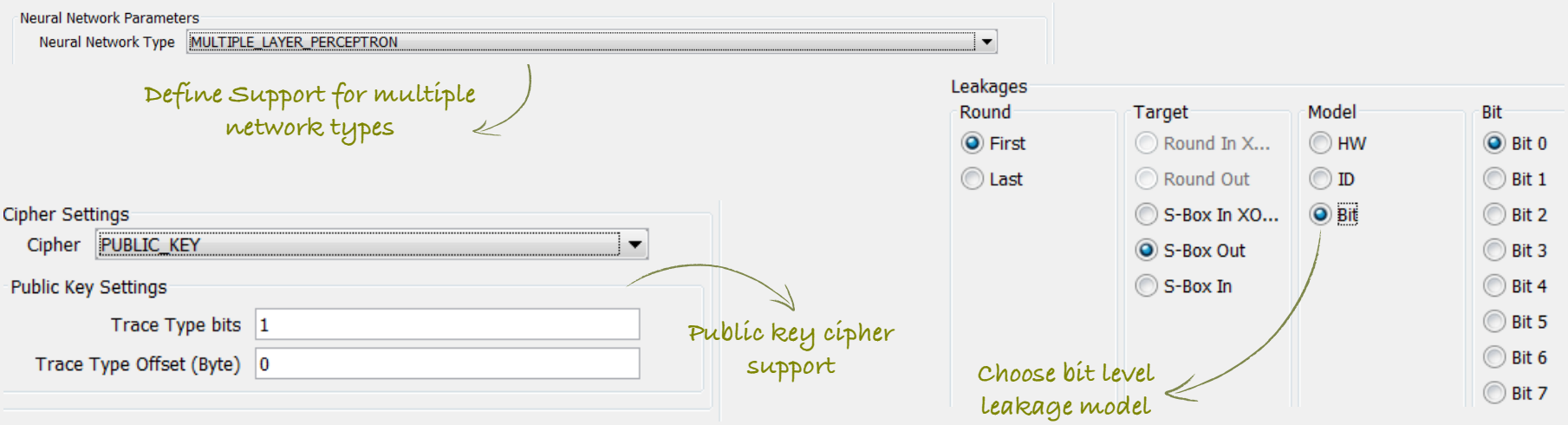
SCA & FI
software update
May 2018

Contents

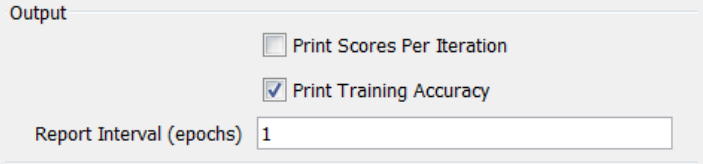
Deep Learning

The Deep Learning module introduced in Inspector release 2018.1 has been extended with a lot of features that extends the possible usage of this module and improved usability. Next to AES and DES the module now also supports RSA and ECC ciphers.
Multiple options to search for hyper parameters have been added. A genetic algorithm can be used to optimize the search for hyper parameters and the quality of the network. Next to that thresholds can be set to stop searching for parameters when certain conditions are met.

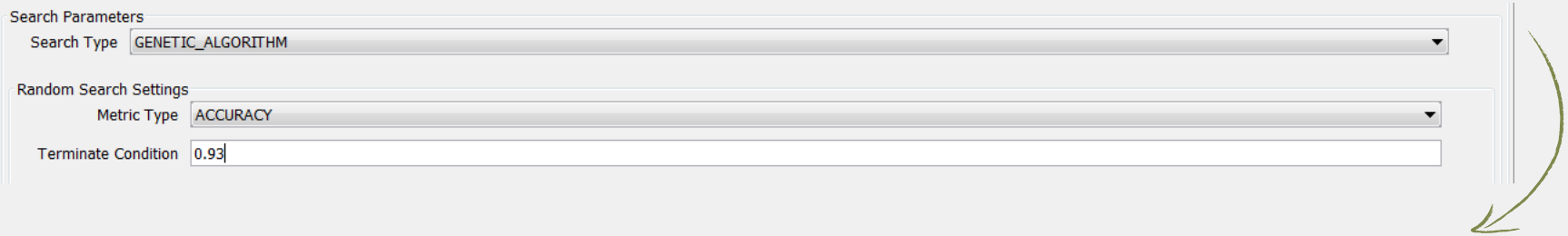
- ✓ Support for RSA and ECC ciphers
- ✓ Use genetic algorithm to search for hyper parameters
- ✓ Choose to attack AES and DES for each bit separately
- ✓ Choose a convolutional neural network or multi layer perceptron
- ✓ Reuse result processors for public key ciphers from template attack module



Deep Learning

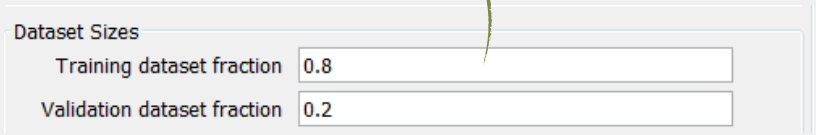


Control output to get a better overview of network performance



Hyper parameter search is improved on several points. Now you can choose to use the benefits of a genetic algorithm to optimize parameter search. Next to that thresholds can be set on accuracy, F1 score, recall, loss function and key ranking to stop searching when the network reaches this chosen value. Early stopping based on time is also still available

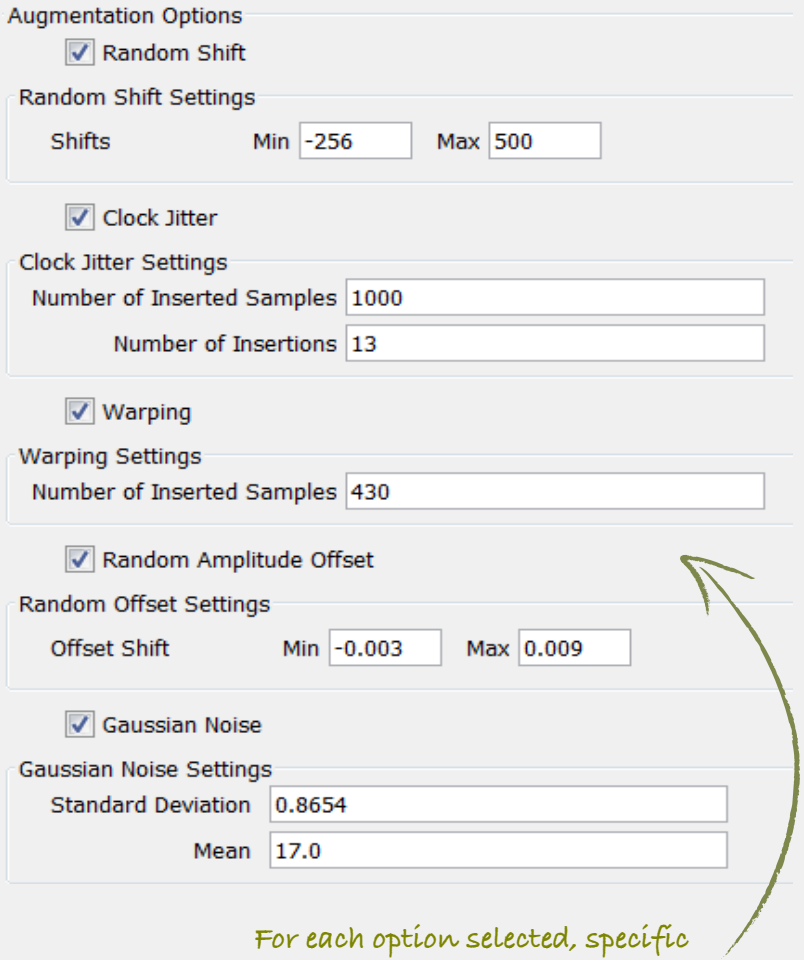
Training and validation fractions are auto calculated when one of them is chosen



Trace augmentation

This new module enables you to extend your trace set with additional traces that have shifts or jitter added to them. This is particularly useful for training a deep learning network since training a network on more traces with small differences will result in a network that is better able to generalize when it is used in an attack (test) phase on just a few traces with an unknown key. The module allows to select and configure various options to generate the additional traces based on the trace set acquired through normal acquisition and also allows to configure the target number of traces.

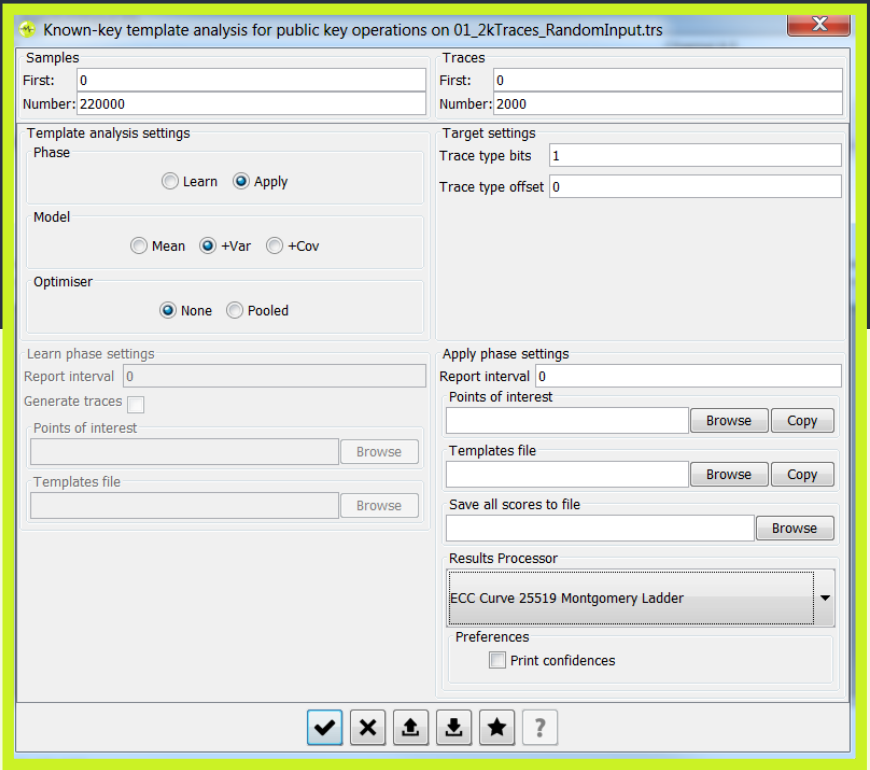
- ✓ Extend your trace set in a fraction of the time compared to normal acquisition
- ✓ Improve the training of your neural networks
- ✓ Select and configure trace generation options
- ✓ Create an automation scenario to automatically generate traces after acquisition and train your deep learning network accordingly



For each option selected, specific settings can be configured

riscure

Template attack for ECC



- ✓ New template analysis module allows user to classify traces containing different operation types from a public key implementation
- ✓ User selectable results processor
- ✓ User can develop new results processors for custom implementations using the module wizard

Operations that are used for template attacks on DES and AES also apply for ECC

Piñata

- ✓ Piñata 2.3 release support ECC 25519 scalar multiplication commands
- ✓ New sequence can be used for acquisition to demonstrate Template Analysis on ECC

riscure

Huracán

Huracán is a new device specifically designed for security assessments on ECU's and other automotive electronics

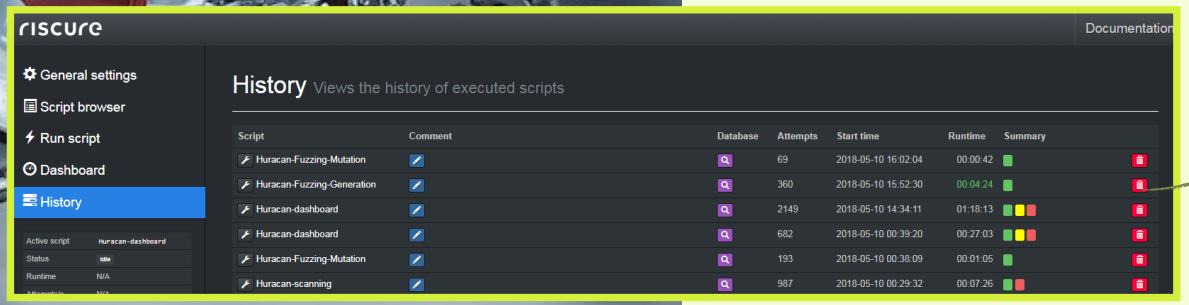
- Use Huracán in SCA and FI setups to generate traffic and triggers
- Use fuzzing to test the robustness of ECU's in an easy and straight forward way
- Shipped with various connectors to easily adapt to the pin layout and power needs of the target ECU

Integrate in Inspector sequences through the java API

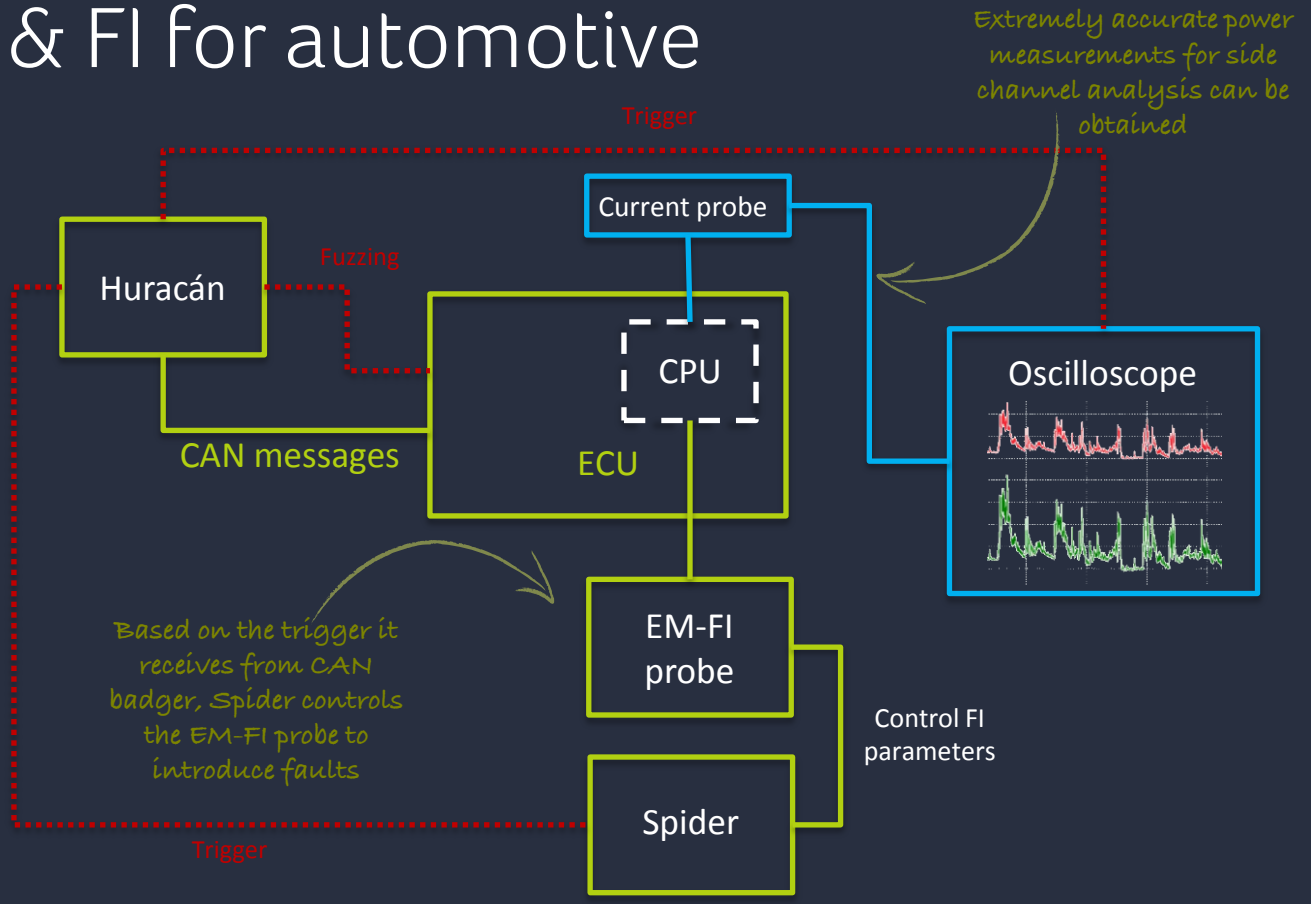
- Huracán can be integrated as a serial device in an easy way based on the easy to understand and described API
- Examples are available to get you up to speed as fast as possible

Use the Python API to easily create scripts and extend them

- On request Riscures new web based Python GUI is available as beta



Huracán: SCA & FI for automotive

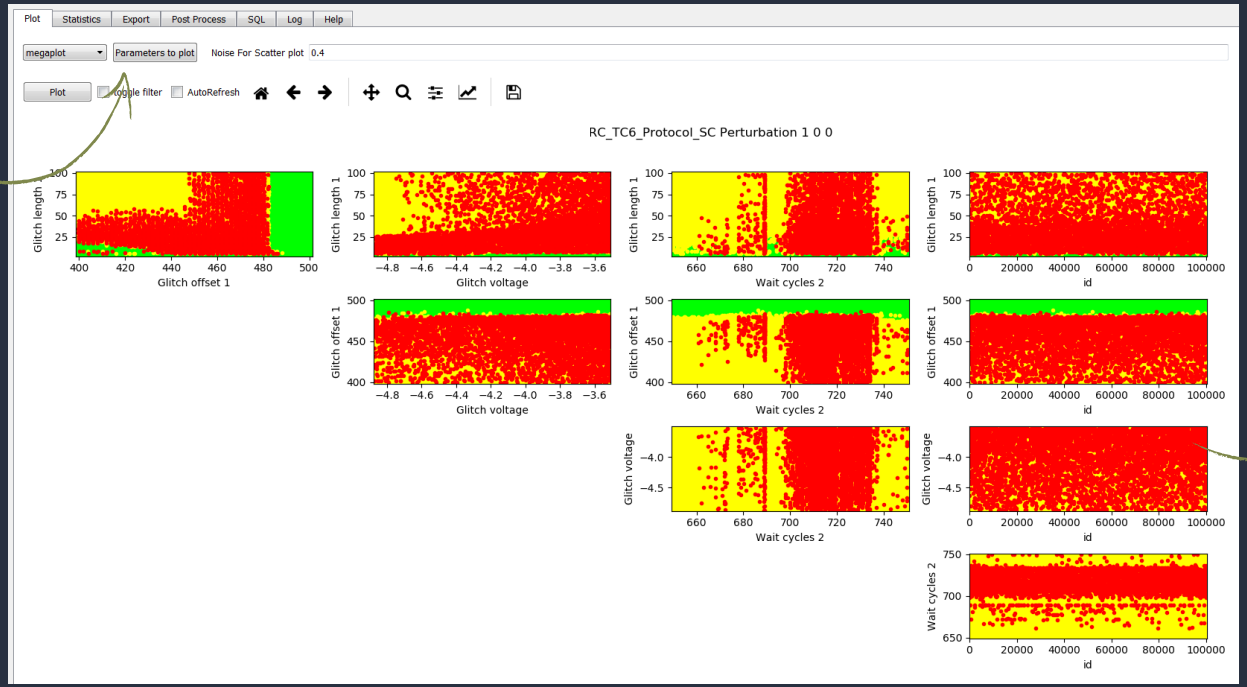


Release version planned for Inspector 2018.3

Available as beta: 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



Bases on a SQL lite database so results from older FI session can easily be imported and analyzed

New support portal

Riscure has a new support portal! The portal can still be found at https://support.riscure.com or by choosing the link from our homepage.

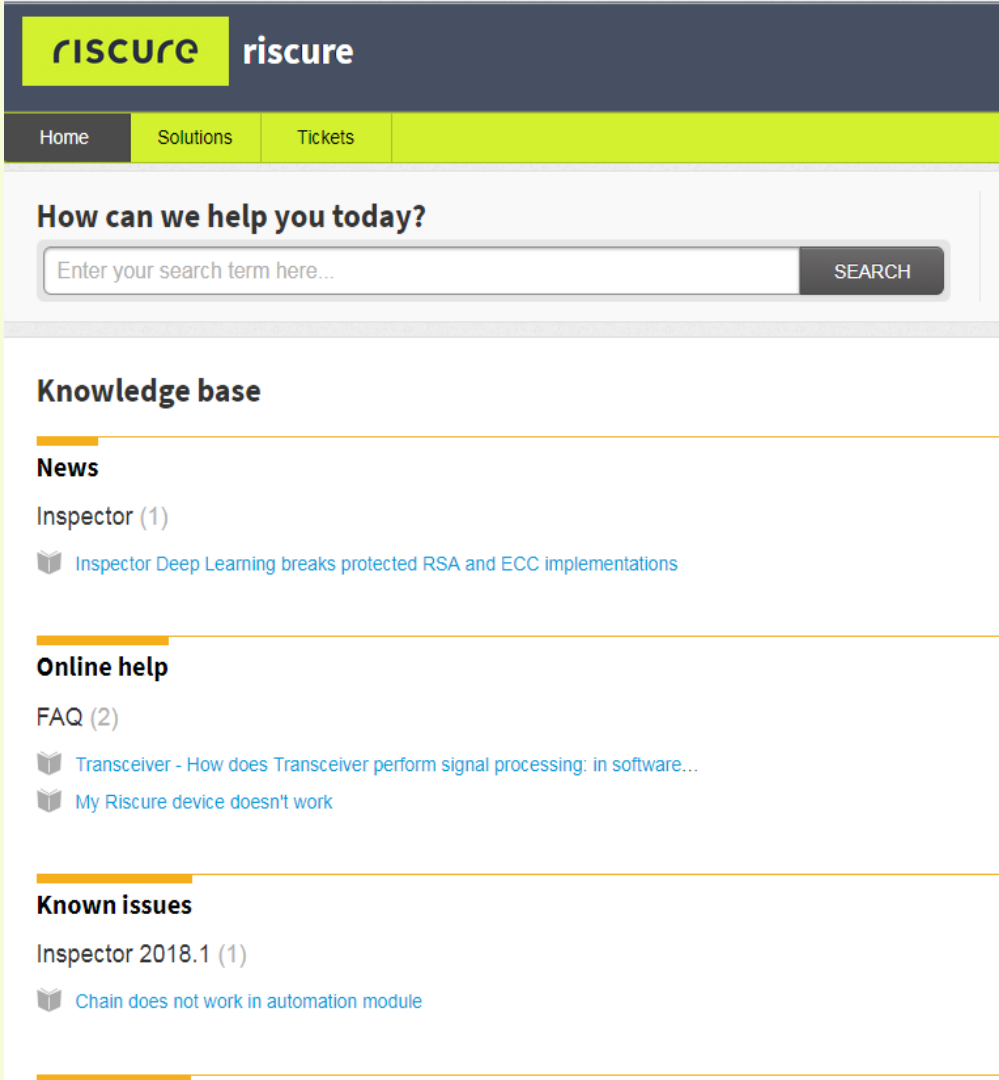
The new portal is very easy to use and not only to raise a support issue, but also to find information on new released modules, frequently asked questions and known issues, for which we also mention when these will be solved!

The new support portal makes it easy to submit a ticket and to have an overview of all your support tickets, open and closed. It even works on your mobile phone or any other device.

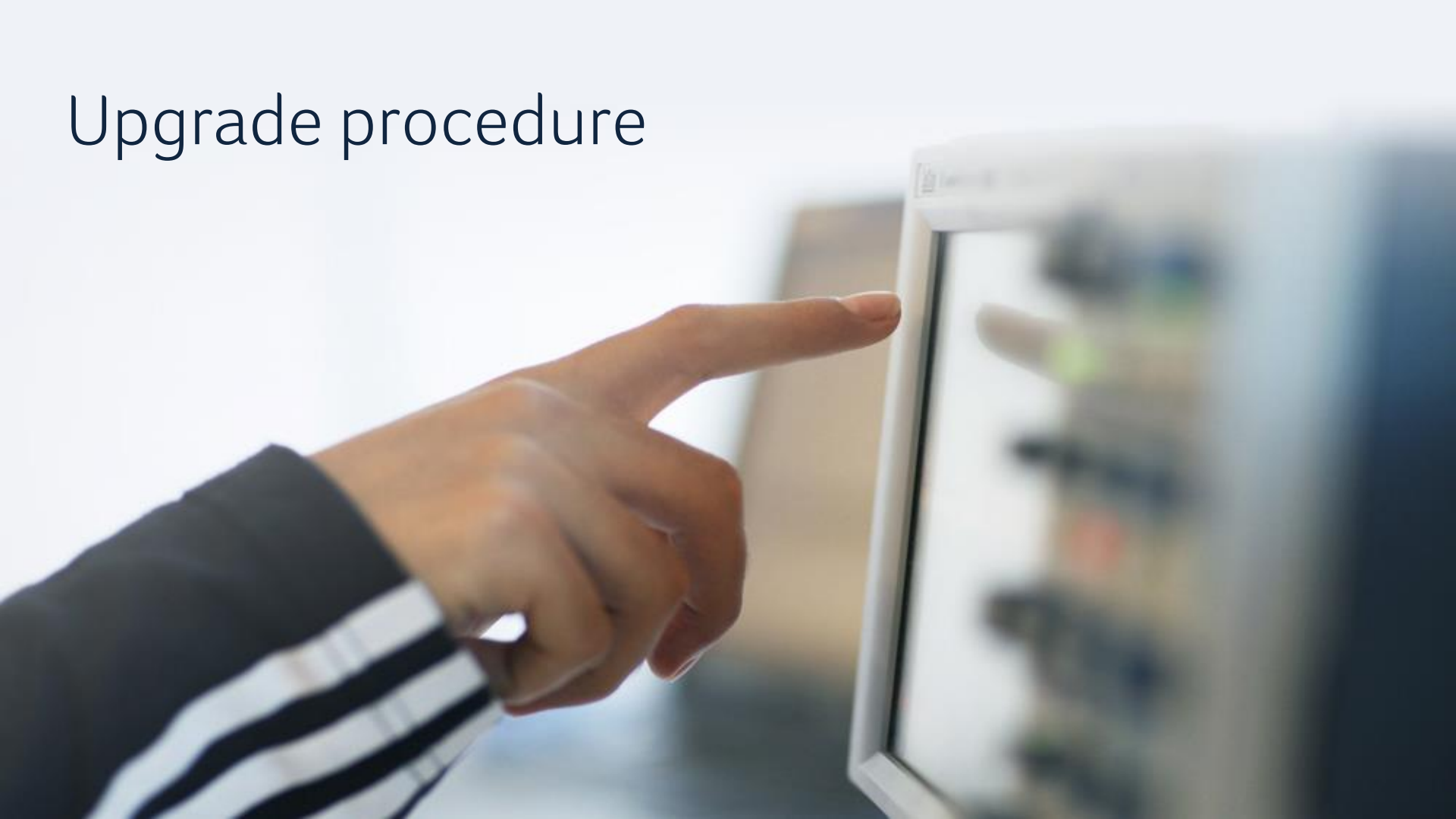
For just a quick question it is possible to chat with one of our specialists and when they are unavailable your chat request will automatically be transferred to a support ticket, so we can get in contact with you as soon as possible.

Sending an email to support@riscure.com is also an option. Your email will end up as a ticket in our system and we will get back to you as soon as possible.

riscure



Upgrade procedure



Inspector installation

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 2018.2.
- 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

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