Riscure Inspector 2018.1 Release Notes

Date 15 January 2018

Modified behavior

Issue number	Description
INS-7594	Modified behavior: During module execution it was possible to start another module by choosing one from the recent modules drop down list. This causes Inspector to crash and therefor the behavior is modified. The recent modules drop down in the menu bar will now be disabled during module execution and when the module finishes the drop down will be enabled again.
INS-7593	Modified behavior: When a module was running it was possible to compile another module by pressing the F9 key. This could cause instability. The behavior as been modified so that it is not possible anymore to compile a module while another module is running.
INS-7709	Modified behavior: When starting an acquisition the default number of samples was very low (e.g. 100 samples) . This is changed so now for all scopes the default number of samples is set to 10k.
INS-7620	Modified behavior: In the "Embedded Glitch Setup" tab of any Embedded Perturbation module there was an option "Wait for glitch to complete" option. This option is now removed because it caused problems related to other timeout setting also present. The functionality is taken over by the "Timeout" field present in the "Glitcher properties" options.
INS-7427	Modified behavior: Not all modules that implemented a brute force key search behaved the same when this process was aborted. The behavior of all these modules is synchronized so that when a user aborts, all modules generate by default all possible result traces and then stop processing. Modules : First Order Analysis, AES chosen input FOA and Template analysis DPA unknown-key have been modified
INS-7576	Modified behavior: During acquisition, if the received data length is smaller or larger than expected, instead of aborting the acquisition with an exception, Inspector will pad or truncate the data to expected length, store it into the trace, log a warning "Received more/less data than expected" and move on to acquire the next trace.

Riscure Inspector 2018.1 Release Notes

INS-7613	Modified behavior: When scanning a target with EM Probe Station there was a chance that the target or probe tip could be damaged because the probe was first moving in a horizontal direction and then in a vertical direction. Especially with a tilted chip this could cause problems. To avoid that the target or probe tip is damaged during EM Probe Station movement, the movement is now split in moving first aside and then down or moving first up and then aside.
INS-7600	Modified behavior: When the perturbation log was opened via the perturbation history window, an opened trace set could not be brought to the front by selecting Window -> "trace set name". This is now fixed so that trace sets can be brought to front.
INS-7538	Modified behavior: The visualization of Known Key Analysis results have been improved on several points: 1) When using a non-zero report interval with "Generate Plot" enabled, a single window will be opened, which allows the user to scroll back and forth through the results after each report interval. Additionally, an evolution graph can be generated to show the change in rank over time for a single, or several sub keys at a time. 2) Hovering the mouse over a section will show the actual rank. 3) The evolution graph shows the point where the rank reached 1 (the top value), or the user can extrapolate easily based on this graph. 4) A confidence evolution graph can be generated which shows the confidence of the correct key candidate plotted against all others.
INS-7481	Modified behavior: The default modulus and public exponent values of the RSA CRT analysis are now set to match those used by Pinata board.
INS-8359	Modified behavior: The splash screen will be displayed right after the application startup and will show a progress bar to show that the application initialization is in progress.
INS-7404	Modified behavior: We have added a global key to limit the brute force part of the key recovery process. The key reflects the maximum number of remaining entropy bits after which a brute force will be done.

INS-8227	Modified behavior: The format of the parameter files that Inspector uses to save the parameters for modules to a human readable xml format. This is the same for the module parameter in the module Log. This is also changed to a human readable format.
INS-6819	Modified behavior: Previously for analysis, Inspector read a trace, processed it and (optional) wrote the processed trace to disk. Now trace reading and writing is done by 2 separate threads.

Riscure Inspector 2018.1 Release Notes

New features

INS-7265	New feature: To be able to filter on elapsed time, a column which indicates the elapsed time since the start of the perturbation run is added to the perturbation log.
INS-7032	New feature: In the result list for First Order Analysis, the relative distinguishing margin (RDM) for the top candidate is added. The RDM is calculated as follows : RDM = (top candidate - 2d candidate) / stdev(all candidates)
INS-7358	New feature: In trace view, the X-axis label text no longer overlaps with the trace signal. This is especially helpful when including trace screenshots in reports
INS-7965	New feature: It can be useful for a statistics component (correlation or differential) to request to see the traces twice. We have added support for a statistics component in crypto2 to be able to make multiple passes through a trace set.
INS-7863	New feature: The Perturbation History view has been improved and filter possibilities for the Perturbation Log view are expanded
INS-7875	New feature: When developing an Inspector Protocol module the user can use the addLogData() method to add data to perturbation log.
INS-7614	New feature: When a null byte (0x60) was received after a fault injection attempt an indefinite stream could hang Inspector. For the T=0 smart card protocol a timeout is now introduced on the reception of NULL (0x60) bytes.. The timeout is 10 seonds by default and configurable in the Expert view of the T=0 protocol panel.
INS-7578	New feature: Support has been added for the Chinese SM4 block cipher algorithm with leakages for First Order Analysis, Known Key Analysis and Simulation.
INS-8339	New feature: Deep Learning Module added to Crypto menu in Inspector. Please refer to the 'What's new' document, the manual and tutorial to get familiar with the specifics of this new module.
INS-8366	New feature: Deep Learning Module added to Crypto menu in Inspector. Please refer to the 'What's new' document, the manual and tutorial to get familiar with the specifics of this new module.

Riscure Inspector 2018.1 Release Notes

INS-8329	New feature: Inspector 2018 works with a new licensing system. Next to your dongle you will also need a license file to be able to work with the software. Please see the 'What's new in Inspector 2018" document and the manual for more information on this.
INS-7626	New feature: In trace IO data, resulting from a perturbation 2 module an extra byte was appended. This extra byte is used by AES/DES DFA modules to skip trace data corresponding to a perturbation attempt ended with INCONCLUSIVE status. Not all modules though use this extra byte and some of them even produce wrong results because of this extra byte (RSA/CRT DFA). Users now have control over the Perturbation 2 module behavior where they can set if appending an INCONCLUSIVE status byte to trace IO data is needed.
INS-8356	New feature : Inspector 2018.1 supports template analysis on RSA. This includes a new Pinata sequence, two new modules : pattern match and extract, the template analysis module and new tutorials. Please see the ‘What’s new’ document, the manual and tutorial for more information.
INS-7184	New feature: Inspector 2018.1 supports the 24 mathematical methods/variants for performing a DES Key Scheduling template attack as discussed in Mathias Wagner's Des Key Scheduling Attack paper.

Riscure Inspector 2018.1 Release Notes

Performance improvements

INS-6665	Performance improvement: Wait delays in Perturbation and Acquisition modules are removed or optimized to improve performance for Riscure devices
INS-7219	Performance improvement: Some of the screens to enter acquisition or perturbation parameters took very long before they were displayed (sometimes even close to 10 seconds). The performance of Inspector has been improved for this resulting in a decrease to approximately 1 second to display such configuration screens
INS-7880	Performance improvement: Inspector was configured in a way that it always used 2/3 of the available memory. When a lot of memory is available this is not optimal for performance because Inspector leaves a lot of memory unused. JVM memory usage on system with more than 3GB of system memory is improved in a way that all memory available except for 1GB is used by Inspector.

Riscure Inspector 2018.1 Release Notes

Fixes

INS-8154	Bug Fix: The XYAcquisition was not aborted with an exception when a Picoscope was used as an oscilloscope. This issue is solved.
INS-8049	Bug fix: The the entire DES round key also appeared as a sub-key in the Key Intermediates panel, and its value could have been updated separately from the values of the 8 sub keys. Next to that, when running First Order Analysis on a DES and the key was retrieved, the Key Intermediates panel displayed "96 bits retrieved" and those values would also be copied. This is now corrected to 48 bits.
INS-7159	Bug fix: Fixed the local title detection on right-mouse click for the trace sets in both overlap and non-overlap modes.
INS-8170	Bug fix: Fixed an issue that occured when a chain was loaded that contains user modules. When the chain contained user moduels that where not part of a package null pointer exeptions wheree generated.

Questions and Support

- Please contact Riscure support If you experience problems or need help:

https://support.riscure.com/