Riscure Inspector 2018.2 Release Notes

Date 22 May 2018

Modified behavior

Issue number	Description
INS-8309	Modified behavior: The context menu to copy/screenshot the known key analysis plot window by right-clicking anywhere in the window, including the 2D plot is restored. Next to that, removing of points shown in the evolution plot is changed from right-click to ctrl+left-click. and a separate button is added to clear the evolution plot (instead of a click outside the image area in the 2D plot).
INS-8494	Modified behavior: Inspector 2018.2 has been upgraded to make use of JNA 4.5.1 to control Riscure devices.
INS-8510	Modified behavior: The Deep Learning module now features an option to indicate if various training and validation progress indicators need to be printed in the output window
INS-8556	Modified behavior: The deep learning module is updated with the Bayes key extraction algorithm to improve key enumeration
INS-8576	Modified behavior: The advanced pattern match and pattern extract modules have been changed so that they can be used for Template Attacks on ECC
INS-8582	Modified behavior: The internal classes of the Deep learning module have been changed so that the results of an attack with the deep learning module is improved
INS-8717	Modified behavior: When the user uses a relative path to define files needed to configure a module (for example, the file where the POI's are located for POI / TA modules), Inspector used to convert this to an absolute path prior to saving the file. This was seen when the module was loaded again.This had the undesired effect that the parameter files are not portable to different machines, with different Inspector work paths (for example, because the user name is different). The parameters files are now saved as entered by the user (with relative paths if necessary), and are only converted to absolute paths each time when running the module.
INS-8738	Modified behavior: When using the Deep Learning module, for the training phase the training and validation fractions both had to be

	determined by the user. Now only one of those need to be assigned. The other fraction will be calculated automatically.
INS-8739	Modified behavior: In the Deep Learning module the Activation function and Loss function for the output layer are now fixed to Softmax and negative Likelyhood. This is based on research that concluded that these settings always give the best results.

Riscure Inspector 2018.2 Release Notes

New features

Issue number	Description
INS-7731	New feature: Running modules on Inspector HPA (multiple instances of Inspector) was only possible when a automation scenario was created forst. This was cumbersome when the intention was only to run one module on Inspector HPA. Now with a specific 'run on cluster' button, a single module can run instantly on Inspector HPA
INS-8513	New feature: The Deep Learning module now has additional features to support MLP (multiple layer perceptron). Please see the section in the manual for more details.
INS-8557	New feature: A new module has been added with data augmentation features. This module can add noise, create random shifts and warp traces. This is especially useful to enhance a trace set so that it is better suited to train a neural network
INS-8558	New feature: The Deep Learning module now uses a genetic algorithm to improve the automated Hyper parameter search option. See the updated manual and tutorial for detailed information
INS-8578	New Feature: Inspector 2018.2 features a new ECC specific pattern extract strategy for AdvancedPatternMatch and AdvancedPatternExtract modules. Please check the 'Whats new in 2018.2" document, the manual and the tutorial for all the details
INS-8620	New feature: The deep learning module is modified so that for DES and AES it is now possible to attack one bit at a time instead of a byte
INS-8623	New feature: The tutorials have been updated to reflect the new options for Template Attacks on ECC and the new features of the Deep Learning module
INS-8650	New feature: Inspector 2018.2 uses a genetic algorithm to simplify the search for hyper parameters for a neural network. The manual will give more details on how to use this.
INS-8699	New feature: A new Pinata sequence is added to support template attacks on ECC cipher
INS-8741	New feature: A threshold on on accuracy, recall, key ranking, and F! scores can now be configured for the Deep Learning training phase which causes the training to stop when the threshold value has bee reached.

Riscure Inspector 2018.2 Release Notes

INS-8742	New feature: The tutorial has been extended with 5 new use cases for the Deep Learning module.
INS-8758	New feature: Inspector 2018.2 features a new Data Augmentation module that can be used to extend a acquired trace set with additional traces based on a user configuration. Please check the manual and tutorial for details.
INS-8761	New feature: Huracan is a new device specifically developed by Riscure to tets the security of devices and chips used in the automotive industry. 2018.2 features a new Java API for this device so that it can be used in sequences for SCA and FI setups

Performance improvements

Issue number	Description
INS-8777	Performance improvement: In Inspector 2018.1 performance issues where reported on trace sets with a lot of traces and trace sets with traces that had a lot of samples. These performance issues were caused by the memory management in 2018.1. This has know been resolved by assigning 2/3 of available to Inspector at startup buy default. For specific use cases, there is an option to exactly assign the amount of memory Inspector uses through a command line parameter.
INS-8727	Performance improvement: Inspector HPA requires a trace set to be imported on the server to be able to process it. The performance of Importing a trace set on Inspector HPA has been improved significantly.

Fixes

Issue number	Description
INS-8509	Fix: The Deep Learning module did not show all possible and relevant leakage model options anymore. This is now fixed.
INS-8555	Fix: When the key was recovered with 1 trace, the module indicated the key was not recovered. This is now solved
INS-8588	Fix: The automation module did not work correctly in combination with a chain. This was reported as a known issue in 2018.1. This issue now has been fixed so that a automation module can be used in a chain without any problem.
INS-8649	Fix: The PicoScope driver reported an exception when the user did not use an external power supply (4 channel mode). This is now fixed.
INS-8694	Fix: There was an issue with license files with a validity date in the future. These license files would not be ;loaded correctly. This is now fixed.
INS-8723	Fix: It could happen that the Deep Learning module threw a NULL pointer exception when the test phase was executed. This was caused by a class declaration in one of the modules. This error is now fixed.
INS-8740	Fix: A issue in the key ranking for the Deep Learning module which caused the ranking to be 256 even in cases when the correct key was recovered is now fixed.
INS-8752	Fix: The AES DFA module used wrong rounds keys when run with decrypt, 192 or 256 key bits and targeting both rounds. This is now fixed.
INS-8755	Fix: The 'Open recent trace set' activity for an automation module was not recorded in the module log. This is now fixed..
INS-8756	Fix: method updateOneProperty(...) -to programmatically change the content of a parameter file in an automation module- gave an error when used with a Chain module parameter file. This is now fixed

Questions and Support

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

https://support.riscure.com/