Riscure Inspector 4.11 Release Notes

Date 28 November 2016

Release Highlights

4.11

- Introduction of TVLA modules
- Introduction of Template Analysis Key Schedule attacks
- Introduction of Template Analysis DPA and Key Loading Unknown Key attacks
- Template Analysis tutorial updates
- DPSS motor driver upgrade
- Added software support for the PicoScope 3206D
- Bug fixes as detailed in table below

Questions and Support

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

https://support.riscure.com/

Riscure Inspector 4.11 Release Notes

Issue Key	Release Note
INS-6634	Decreased the default joystick speed for XYZ stage to improve accuracy and added persistence of user configured speed settings when reloading a module.
INS-6694	Improved performance of AdvancedDifferentialAnalysis by making it more cache friendly
INS-6745	Added tutorial of Spider Vcc FI Pinata
INS-6746	Added tutorial of Spider EMFI on Pinata
INS-6761	Added support for the PicoScope 3206D
INS-6783	Fixed exception when using dummy XY table (in framework 2)
INS-6814	Added icWaves 3 live tuning procedure to the manual
INS-6821	Support for new VC Glitcher FIFO mode in perturbation 1 driver avoiding unnecessary read time outs.
INS-6822	Increased read timeout for the VCGlitcher in perturbation1 to avoid exceptions
INS-6847	Introduced unknown-key for Template Analysis DPA-like for AES and DES (new technique / feature)
INS-6874	Clarified in the manual the meaning of the Timed Out parameter in the perturbation log
INS-6926	Bug fix for the error "Not a multiple of 0.0002" which was caused by spinners inside the Perturbation tab of a Perturbation module
INS-6927	Fixed the issue that previous result keys from First Order Analysis could have been lost when a new run failed if you forgot to copy the previous round key
INS-6928	User gets a warning if zero oscilloscope channels are selected
INS-6930	Fixed a regression with inclusion of MP300 and MP500 Micropross drivers

Riscure Inspector 4.11 Release Notes

INS-6935	Fixed manipulation of sample array in Distribution and added warning to Trace API
INS-6951	Fixed the loss of the global trace title when running certain modules (Abs, Reverse, Low pass etc.) on trace sets
INS-6954	Upgraded the installer software to be able to handle more Java versions
INS-6962	Fixed a bug for Picoscope 3000 series to display lowest supported ranges (like 10mV and 50mV range)
INS-7034	Introduced unknown-key for Template Analysis on key loading for AES and DES (new technique / feature)
INS-7068	Added support for the new DPSS power controller
INS-7073	Fixed a display bug in the built-in editor when ending a string in \\"
INS-7074	The Perturbation History window is kept open after selection of a perturbation record. Further the user can now manually close the perturbation history via a close button.
INS-7097	Fixed a bug (out of bound exception) when saving a partial trace from a large trace set (e.g. 3M traces)
INS-7112	Added FTDI driver 2.08.28 to the hardware folder to ease Pinata and laser Twin Scan installation
INS-7126	Fixed a bug where using icWaves as scope throws "For 1M" exception
INS-7134	Removed single threaded versions of CorrelationAnalysis and DifferenceOfMeanAnalysis
INS-7155	Adapted AES/DES Pinata Sequence modules to use the new Sequence built-in data generators
INS-7173	Added the AES Equivalent Inverse implementation to Crypto2 cipher
INS-7208	The memory usage for (multi) trace display is reduced. For single trace display memory usage is again as (efficient as) before Inspector version 4.10.
INS-7225	Updated and extended the tutorial for Template Analysis to match current feature set in Inspector
INS-7235	Reduced memory usage when Module Log Viewer is not used.

INS-7250	Fixed bugs in the GUI of Spectrogram and Core
INS-7251	Performance improvement when displaying and saving traces
INS-7269	Fixed issue which occurred when a user manually dragged (shifted) a channel with logic signals (e.g. coming from an icWaves 3)
INS-7283	Introduced new Template Analysis attack for DES Key Scheduling, including Point of Interest selection, learn and apply for known key scenarios (new technique / feature)
INS-7306	Tips added to set parameters in Pattern tab of icWaves configuration
INS-7310	Introduced Test Vector Leakage Assessment (TVLA) methods for DES and AES including semi-constant data set generation and T-testing (new technique / feature)
INS-7315	Fixed a memory leakage of module log viewer
INS-7329	To ease icWaves configuration in Inspector FI, a Scope Only module was added to run an oscilloscope without target communication
INS-7361	Added AES Equivalent Inverse Cipher support to Template Analysis (new technique / feature)
INS-7376	Fixed a bug where trace zoom will intervene mult-trace display during acquisition
INS-7387	Added Spider tutorials performing EMFI and Vcc FI on Pinata board