EDSA-201

ISA Security Compliance Institute — Embedded Device Security Assurance

Recognition process for communication robustness testing tools

Version 1.21

November 2010

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision history

version	date	changes
1.1	2010.06.03	Initial version published to http://www.ISASecure.org
1.21	2010.11.11	Modified for CRT specification changes for versions noted in Clause 2

Contents

1. Purpose

This document describes the process for ISCI (ISA Security Compliance Institute) recognition of a CRT (communication robustness testing) tool for the ISASecure Embedded Device Security Assurance (EDSA) certification program. ISASecure EDSA certification has been defined by the ISCI interest group organized under ASCI (Automation Standards Compliance Institute). A certifier must use a test tool for CRT that has achieved recognized status under this process, in order to be accredited by ASCI as an ISASecure EDSA chartered laboratory as defined in [EDSA-200].

The goal of the CRT tool recognition process is to provide confidence that a tool offers adequate functionality to support a certifier in performing CRT in accordance with the ISASecure EDSA CRT specifications. The list of current CRT specifications and versions is maintained on the ISCI web site http://www.ISASecure.org.

This document includes guidance for tool suppliers on applying for CRT tool recognition. It is used in conjunction with the CRT specifications cited in the following section. An application form to apply to ISCI for recognition of a CRT tool, and general information about the ISASecure program is available at http://www.ISASecure.org.

2. References

The most current versions of these documents can be obtained as noted below. The versions that correspond to this document are noted in parentheses after each reference.

[EDSA-200] *ISA Security Compliance Institute Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org (version 1.3)

The ISASecure EDSA CRT specifications current at the time of publication of this document are listed below. The overarching document [EDSA-310] contains references to the protocol-specific documents listed after it.

[EDSA-310] *ISA Security Compliance Institute Embedded Device Security Assurance – Common requirements for communication robustness testing for IP based protocol implementations* as specified at http://www.ISASecure.org (version 1.7)

[EDSA-401] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols,* as specified at http://www.ISASecure.org (version 2.01)

[EDSA-402] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4,* as specified at http://www.ISASecure.org (version 2.31)

[EDSA-403] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol,* as specified at http://www.ISASecure.org (version 1.31)

[EDSA-404] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol,* as specified at http://www.ISASecure.org (version 1.3)

[EDSA-405] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org (version 2.6)

[EDSA-406] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org (version 1.41)

3. Overview of CRT Tool Recognition Process

This section provides a high level description of the recognition program for CRT tools.

3.1. Scope of Evaluation for Tool Recognition

The CRT tool recognition process will evaluate coverage of the following general technical capabilities of a tool:

- Tests for all ISASecure certifiable protocols
- Basic and load stress robustness tests
- Capability to monitor the control loop
- Reproducibility of test results

ISCI will evaluate a test tool solely on its technical capabilities to carry out CRT. This means that for the initial CRT tool recognition program, ISCI will not evaluate the user friendliness of the tool, the future prospects for maintenance and support of the tool, the tool development process or the financial and organizational standing of the provider of the tool. However, these criteria are relevant to organizations when selecting a CRT test tool, as for any software purchase.

The CRT specifications listed in Clause 2 place requirements on the CRT process. These requirements have impact on either the chartered laboratory performing CRT or the CRT tool the laboratory uses, and in some cases on both. ISCI evaluates CRT tools against a defined subset of the requirements in the CRT specifications. A requirement will fall outside of this subset if (1) it applies only to test laboratories and so does not impact CRT tools, (2) it is not practical or feasible to address in a CRT tool, or (3) it may be reasonably met by means other than a CRT tool. In particular, a CRT tool is not required to cover:

- Interface surface testing (finds resident protocols on a device) – because standard tools are available that may be used for this, such as nmap
- Monitoring for adequate maintenance of upward essential services (e.g. view, alarms) – because methods for this vary significantly for various devices under test, so that a generic “packaged” capability is not envisioned

The ISCI recognition process for a CRT tool will not include evaluation of these non-required functions, even if they are supported by the tool. Thus if a user plans to use the tool for these functions, they should independently evaluate the tool functionality in these areas relative to the ISASecure CRT specifications.

3.2. Overview of Evaluation Approach

To apply for recognition of a CRT tool, a tool supplier submits evidence to ISCI that shows that the tool meets each of the applicable requirements in the CRT specifications. A small subset of tool behavior is then directly verified by requesting the tool supplier to create and analyze specific samples of test traffic generated by the tool.

This document provides the list of requirements in the CRT specifications that are applicable to CRT tool evaluation. For some requirements, the form of the evidence required to show compliance with the requirement is also specified here. Required evidence includes design information, user documentation, test results and pcap (packet capture) files. Additional forms of evidence as deemed useful by the tool supplier are permitted. After receiving technical training on the tool arranged by the tool supplier, ISCI's evaluation team verifies the evidence provided by the tool supplier. Tool names, versions, identifying hash values and suppliers for CRT tools that have been recognized are posted on the ISCI web site at http://www.ISASecure.org. A tool is recognized for a specific version of ISASecure, for example, it might be recognized for ISASecure 2010.1 CRT. A chartered laboratory verifies the version and hash of the tool they are using against information provided on this site.

4. Tool Evaluation

4.1. Overview of Evaluation Criteria

The evaluation of a CRT tool takes place in four steps, as shown in the left column of Table 1. The first three steps focus on design level analyses of the tool. The fourth step verifies a sample of tool features based upon actual tool outputs.

For the first three steps the applicant will provide to ISCI:

- For each requirement in the CRT specifications that is marked in Annex A of this document as associated with this step, the CRT tool supplier will provide documented evidence to show that the tool meets this requirement. This evidence will take a form determined by the tool supplier as most appropriate to demonstrate compliance, subject to the guidelines provided in Annex A.

- All items in the basic evidence column of Table 1; and

- Supplemental evidence as deemed necessary by the applicant to demonstrate compliance with CRT tool requirements.

For the fourth step, the evaluation team will request a small set of pcap files from the tool supplier that are generated using specified functions supported by the tool. The evaluation team will ask the tool supplier also to provide analyses of these files that show they have certain characteristics – for example, they contain certain kinds of malformed packets or particular packet sequences. The purpose of this step is to validate the conclusions that the evaluation team has reached regarding how the tool functionality supports the CRT requirements, using actual network traffic generated by the tool. This step should be considered a sanity check covering a small sample of expected tool performance and is not a comprehensive test of the tool.

The overall intent of the evidence requested for each step in the evaluation process is described in the "Evaluation Criteria" column of Table 1.

Table 1 - Overview of Evaluation Criteria

Step	Basic Evidence	Evaluation Criteria
1 - Initial technical analysis	• User documentation for the tool • Test report (as would be provided to the user of this tool) for a CRT test on a sample device selected by the tool supplier	• All certifiable protocols are covered • Tool will support reporting requirements • Test approach covers general test type requirements • Test tool addresses control loop monitoring
2 – Detailed test coverage analysis	• Coverage mapping created by tool supplier, that shows how each numbered test listed in Section 7 of each ISASecure protocol-specific CRT specification can be carried out using the tool • Training provided to ISCI evaluation team members	• Tool supports all tests required by Section 7 of all CRT specifications for individual protocols • Tool covers required types of field value errors • Control loop monitoring functionality meets technical requirements
3 - Testing features analysis	• Initial and reproduced test results illustrating compliance with reproducibility requirements	• Tool meets reproducibility requirements • Tool supports adequate traffic rate and other test timing requirements • Tool supports process to vary source IP addresses
4 – Sample validation	• pcap files generated by tool and analyses of these as requested by ISCI	• Tool outputs are consistent with tool design in evidence and meet CRT requirements

The above table serves as an overview of the evidence required from a tool supplier. Annex A to this document provides detailed guidance regarding the evidence required for the tool evaluation process.

4.2. Evaluation Process

The evaluation of a CRT tool proceeds from left to right and top to bottom though the cells in Table 2. The process is designed to first determine broad applicability of the candidate tool and then successively examine it in more detail. The column heading is the organization that performs the tasks described in that column. The application form that starts the process is found on the web site http://www.ISASecure.org .

Table 2 - Overview of Evaluation Process

	ISCI	CRT Tool Supplier	ISCI
1 - Evaluation of initial technical information	Specify required initial technical information. This is specified in this document. Publish application form at http://www.ISASecure.org .	Submit filled in application form and initial technical information for Step 1, as per Table 3 in Annex A.	Evaluate application and initial technical information.
2 - Evaluation of test coverage	If initial technical information is found compliant, request Step 2 detailed test coverage information and training for ISCI evaluation team.	Submit detailed test coverage evidence for Step 2 as per Table 3 and Table 4 in Annex A. Train ISCI evaluation team on the tool.	Assess test coverage evidence against completeness criteria, then proceed with further evaluation of this evidence.
3 - Evaluation of testing features **4 - Sample validation**	If test coverage evidence shows compliance, request Step 3 evidence regarding testing features, as well as pcap files and analyses for Step 4.	Submit evidence regarding testing features for Step 3 as per Table 3 and Table 4 in Annex A. Submit pcap files and analyses as requested for Step 4.	Evaluate Step 3 and 4 evidence.
Recognition	If compliance has been shown for all requirements, request permission from tool supplier to register tool as recognized for ISASecure CRT.	Grant permission for public posting of tool recognition status.	Post name, version and hash of recognized tool and name of tool supplier on ISASecure website.

12 of the 13 requirements identified in Table 3 of Annex A for Step 1, must be found by ISCI to be compliant after one iteration of the tool supplier's Step 1 evidence, in order for the application process to proceed to step 2.

Table 2 notes that completeness criteria are assessed before evaluation of Step 2 evidence will begin. In particular, all requested evidence as identified in Annex A for Step 2 must be provided before Step 2 evaluation begins. Further, the mapping that shows that the tool supports all required CRT tests must cover all of these tests before the Step 2 evaluation will proceed further. This mapping is the evidence described in Table 4 that shows compliance to the requirement "Ethernet".R14 and to the parallel requirements for other protocols.

For recognition to be granted, the tool supplier must show that the CRT tool is compliant with all applicable requirements in the ISASecure EDSA CRT specifications as enumerated in Annex A of this document.

4.3. Maintenance of Tool Recognition

If the ISASecure EDSA CRT specifications have not changed, and the tool supplier provides a tool update to its users, the tool supplier shall advise ISCI of the nature of the changes provided in the update. If ISCI judges the changes to be significant relative to CRT requirements, the tool supplier will be asked to re-submit its application form, and the Steps 1-3 evidence as described in overview in Section 4.1. The supplier will also identify any differences in this evidence from that for the previous tool version as part of this submission. At ISCI's discretion, if the tool has undergone major changes, the evaluation of sample test outputs per Step 4 may also be required to maintain tool recognition.

Since chartered laboratories are required to use recognized CRT tools, and recognition applies to a specific tool version, this process should be initiated by the tool supplier as early as possible relative to the release of the updated tool.

Suppliers of recognized CRT tools are encouraged but not required to be part of the working group that maintains and improves the CRT specifications. When changes to ISASecure EDSA CRT specifications are planned for release, ISCI will inform the suppliers of recognized CRT tools of the expected date of release. If these changes add new protocols, then in order for a tool to be recognized for that year's certification, ISCI and the tool supplier will go through the steps described in Section 4.1 and Section 4.2 relative to the new protocol(s). If the specification changes relate to protocols previously covered, the supplier will provide evidence that their tool meets the modified requirements. The format of this evidence may be specified by ISCI as appropriate for each change.

5. Annex A - Guidelines for CRT Tool Evaluation Evidence

5.1. General

Table 3 and Table 4 below detail the evidence required from a CRT tool supplier for evaluation under the ISASecure EDSA CRT tool recognition program. The evaluation step during which this evidence is requested is also defined in these tables. Section 4.1 describes these steps. In addition to the evidence listed here, as the last step in the evaluation, the evaluation team will request traffic generated by the CRT tool in pcap format (packet capture) together with analyses of that data that further supports the compliance of the tool with the ISASecure requirements. This final evaluation step 4 serves as a validation of the design level evidence requested in the first three steps.

The CRT specifications listed in Section 2 apply to the overall CRT process, which involves both the CRT tool and the CRT tool user. Hence the descriptions in the tables below detail the aspects of each requirement in these specifications that should be addressed by the CRT tool. In some cases a specific form for evidence of compliance is requested, or some examples of forms for evidence are offered. In all cases, it should be noted that the phrase "show that…" will be satisfied by a convincing argument that the requirement to be shown holds under all applicable circumstances. Compliance cannot normally be adequately shown by demonstrating that the required functionality or characteristic holds in one particular case.

5.2. Evidence for Compliance with Common CRT Requirements

The table below describes evidence required for tool compliance with the requirements in the common CRT specification [EDSA-310]. The last column shows the step of the tool evaluation for which this information is needed.

Table 3 - Evidence for tool compliance with [EDSA-310], common CRT requirements

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
CRT.R1	Types of CRT tests	Provide pointers to tool user or design documentation that show the tool covers all required protocols, and complies to the protocol reference standards cited in the CRT specifications for individual protocols listed in Section 2 of this document.	1
CRT.R2	Applicable protocols for CRT	Not required for CRT tool	
CRT.R3	Interface surface tests precedence	Not required for CRT tool	
CRT.R4	Core protocol tests precedence	Not applicable at this time	
CRT.R5	Criterion for CRT pass	Not required for CRT tool	
CRT.R6	Single configuration DUT	Not required for CRT tool	
CRT.R7	Submission of essential service opt-outs	Not required for CRT tool	
CRT.R8	Submission of definition of essential history data	Not required for CRT tool	
CRT.R9	Submission of upward essential service monitoring criteria	Not required for CRT tool	
CRT.R10	Submission of method to achieve maximum recommended device load	Not required for CRT tool	
CRT.R11	Submission of cycle time and control jitter tolerance	Not required for CRT tool	
CRT.R12	Submission of device hardware and software	Not required for CRT tool	
CRT.R13	Submission of monitoring hardware and software for downward essential services	Provide pointers to user or design documentation that show how the tool provides monitoring for digital (binary or discrete multi-valued) and analog control outputs, regardless of method of conveyance. For example, this may be achieved via a test harness interface as described in this requirement, or direct support of monitoring functionality, or a combination of these approaches.	1
CRT.R14	Submission of monitoring hardware and software for upward essential services	Not required for CRT tool	
CRT.R15	Submission of end user device documentation	Not required for CRT tool	
CRT.R16	Submission of list of accessible network interfaces	Not required for CRT tool	

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
CRT.R17	Submission of implemented protocols	Not required for CRT tool	
CRT.R18	Submission of description of intended embedded device defensive behavior	Not required for CRT tool	
CRT.R19	CRT report summary	Not required for CRT tool.	
CRT.R20	Test report administrative information	Show how tool user will determine version of ISASecure specification supported. Show how tool user will determine which tests have been run and the date of the test runs.	1
CRT.R21	Report CRT test case descriptions	Show that the CRT tool documentation contains sufficient information to allow the test laboratory to document high level test case descriptions and to map the tests in Section 7 of each of the protocol specific CRT specifications to their test procedures.	2
CRT.R22	Report CRT methodology summary	Show that the CRT tool documentation contains sufficient information to allow the tool user to document the test methodology in a manner useful to a device vendor.	1
CRT.R23	Report CRT configuration	Show that the tool provides a method to output the configuration of the tool that was used for a test run or series of runs.	1
CRT.R24	Report ISASecure reference for test failure	Show how a tool user will determine a specific requirement of the CRT specifications that has failed when a test encounters a failure condition.	2
CRT.R25	Report test failure analysis	Not required for CRT tool	
CRT.R26	Report conditional branches of test execution	This requirement applies if the CRT tool employs logic such that it executes some test branches based upon encountering specific types of anomalous results. For such test tools, show that the tool reports the anomalous results and the tests that were therefore executed.	1
CRT.R27	Report test software version	Show that the CRT tool user can determine the version of	3

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
		the CRT tool, and can validate that this software is unchanged using a hash mechanism.	
CRT.R28	Report test identification and parameters for reproducibility	Show that the CRT tool user can determine based upon tool outputs, all tool parameters required to reproduce robustness test runs for all protocols required by CRT. For example, this might take the form of a sample test report plus step by step instructions for reproducing the results, and then a demonstration that initial and reproduced results are identical.	3
CRT.R29	Basic interface surface test configuration	CRT tool requirement covered by CRT.R30	
CRT.R30	Configuration for downward essential services monitoring during interface surface test	Show that the CRT tool provides a method to support calculation of jitter meeting the requirement in CRT.R30 part c. For example, this may be achieved via a test harness interface as described here or direct support of monitoring functionality, or a combination of these approaches. Show how this functionality can be used during the interface surface test to allow the tool user to determine the conditions associated with a failure.	1
CRT.R31	Configuration for firewalls during interface surface test	Not required for CRT tool	
CRT.R32	UDP port scan	Not required for CRT tool	
CRT.R33	TCP port scan	Not required for CRT tool	
CRT.R34	Use of DUT- based utilities for determining active ports	Not required for CRT tool	
CRT.R35	IP protocol type scan	Not required for CRT tool	
CRT.R36	Scan coverage of all accessible network interfaces and device modes	Not required for CRT tool	
CRT.R37	High rate port and protocol scans	Not required for CRT tool	
CRT.R38	Reproducibility of determination of ports that may be active	Not required for CRT tool	
CRT.R39	Test criteria for “adequately maintain control capability”	Show that the control jitter monitoring approach demonstrated under CRT.R30 can monitor control outputs as	2

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
		described in this requirement and describe the measurement accuracy that the tool supports. Describe the process used for estimating measurement accuracy.	
CRT.R40	Test criteria for “adequately maintain upward essential services”	Not required for CRT tool	
CRT.R41	Criteria for “pass interface surface test”	Not required for CRT tool	
CRT.R42	Reproducibility of interface surface test failure	Not required for CRT tool	
CRT.R43	Report basic interface surface test information	Not required for CRT tool	
CRT.R44	Report UDP ports that may be active	Not required for CRT tool	
CRT.R45	Report TCP ports that may be active	Not required for CRT tool	
CRT.R46	Report IP protocol types	Not required for CRT tool	
CRT.R47	Report behavior of essential services during scans	Not required for CRT tool	
CRT.R48	Test configuration 1 – switched IP connection from TD to DUT	Per CRT.R48 item d), show how the control jitter monitoring functionality described under CRT.R30 can be used during robustness testing of individual protocols to allow the tool user to determine the conditions associated with a failure.	1
CRT.R49	Test configuration 2 – non-switched IP connection from TD to DUT	Describe the difference (if any) in the use of jitter monitoring functionality in this network environment vs. that described for CRT.R48. If there is a difference, show how the tool user can use this functionality to determine the conditions associated with a failure in this network environment.	1
CRT.R50	Robustness testing phases	Provide a high level description of the approach used by the tool for covering basic and load stress robustness testing.	1
CRT.R51	Test coverage for devices with redundant configurations	Not required for CRT tool	
CRT.R52	Test coverage of field values	Show that the test approach embodied by the tool meets this requirement.	2
CRT.R53	Robustness testing with IP address blacklisting	Show how a tool user could meet this requirement.	3

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
CRT.R54	TD traffic rate	Show that the CRT tool can generate traffic at the rate specified in this requirement.	3
CRT.R55	Required test values used in testing fixed-length fields representing integers or enumerations	Show that the CRT tool generates traffic with these characteristics for all protocols tested. As examples, the tool supplier may furnish tool design information that supports compliance with this requirement, or provide a sample packet capture with associated analysis results that demonstrates compliance with this requirement, and an argument that this generated traffic is representative for all uses of the tool.	2
CRT.R56	Required test values used in testing determined-length fields containing varying-length self-delimiting strings	Show that the CRT tool generates traffic with these characteristics for all protocols tested.	2
CRT.R57	Testing fields with a varying sequence of fixed-size subfields	Show that the CRT tool generates traffic with these characteristics for all protocols tested.	2
CRT.R58	Testing fields with substructure and self-defining length	Show that the CRT tool generates traffic with these characteristics for all protocols tested.	2
CRT.R59	Protocol-specific load testing	Describe the CRT tool approach for generating traffic of the types mentioned in this requirement.	2
CRT.R60	Criteria for protocol specific robustness test pass	Show that CRT tool output allows the tool user to determine pass or fail per the criteria of this requirement, for each protocol covered by CRT.	2
CRT.R61	Reproducibility of protocol-specific robustness test failure	Show how a tool user would reproduce a failure based on output from the tool.	3
CRT.R62	Generation of reproducible robustness tests	Show that the tool approach to robustness testing meets this requirement.	3
CRT.R63	Pseudo-random seed value	If a pseudo random seed is used by the CRT tool, show that it meets the size and reporting requirements stated here.	3

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
CRT.R64	Pseudo random seed reuse	If a pseudo random seed is used by the CRT tool, show that it can be reused and duplicate test data as described in this requirement.	3
CRT.R65	Report basic protocol specific robustness test information	Covered for CRT tool by CRT.R20 - CRT.R28.	
CRT.R66	Robustness results summary over all protocols	Not required for CRT tool	
CRT.R67	Report robustness failures	Show that the CRT tool reports CRT failures as defined in CRT.R39 and detected by the jitter monitoring function described in CRT.R30 part c.	1
CRT.R68	Report robustness failure conditions	Show that the CRT tool reports test conditions for CRT failures as determined per the processes described under CRT.R30, CRT.R48 and CRT.R49.	1
CRT.R69	Report robustness test case results listing	Describe how the CRT tool supports the test tool user in creating this report.	1

5.3. Evidence for Compliance with Protocol-Specific CRT Requirements

Table 4 below describes evidence required for tool compliance with the requirements in the protocol specific specifications [EDSA-4nn], as listed in Section 2 of this document. The table is divided into two sections. The first section covers requirements that have the same name and are very similar and (in some cases identical) across all specifications. The second section lists requirements that are unique to one protocol specification.

Table 4 - Evidence for tool compliance with [EDSA-4nn], protocol specific CRT requirements

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
Requirements parallel across all protocols			
"Ethernet".R1 ARP.R1 IPv4.R1 ICMPv4.R1 UDP.R1 TCP.R1	Criteria for robustness test failure	The second bullet of this requirement discusses unique failure conditions for each protocol. Describe these conditions, if any, and show that the CRT tool recognizes and reports them for each protocol. (The first bullet in this requirement is covered for the CRT tool by [EDSA-310] evidence.)	2
"Ethernet".R2 ARP.R2 IPv4.R2 ICMPv4.R2 UDP.R2 TCP.R3	Preconditioning of DUT, TD and any firewalls between the DUT and TD	Covered for CRT tool by CRT.R1 in [EDSA-310]	
"Ethernet".R3 ARP.R3 IPv4.R3 ICMPv4.R3 UDP.R3 TCP.R4	Demonstration of baseline operation	Not required for CRT tool	
"Ethernet".R4 ARP.R5 IPv4.R4 ICMPv4.R4 UDP.R4 TCP.R6	Equipment vendor disclosure of proprietary protocol extensions	Not required for CRT tool	
"Ethernet".R5 ARP.R6 IPv4.R5 ICMPv4.R9 UDP.R5 TCP.R7	Testing of each message field for sensitivity to invalid content	Show that each protocol violation listed in the specification for each CRT protocol is covered by the test traffic generated by the CRT tool. Examples of possible evidence for this are: instructions for running a test together with the analysis of a resulting pcap file showing these violations are present; pointers to product test documentation and results that show that testing of the tool itself verified that these violations are covered by the tool traffic generation algorithms. (Populating values in erroneous fields is addressed by CRT.R55-58.)	2

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
"Ethernet".R6 ARP.R7 IPv4.R11 ICMPv4.R10 UDP.R6 TCP.R8	Constituent elements in basic robustness tests	Show that the CRT tool can generate each type of network traffic described in this requirement for each CRT protocol.	2
"Ethernet".R8 ARP.R8 IPv4.R12 ICMPv4.R11 UDP.R7 TCP.R9	Documentation of self-protective rate limiting behavior	Not required for CRT tool	
"Ethernet".R9 ARP.R9 IPv4.R13 ICMPv4.R12 UDP.R8 TCP.R10	Constituent elements in load stress tests	Show that the CRT tool can generate each type of network traffic described in this requirement for each CRT protocol.	2
"Ethernet".R10 ARP.R10 IPv4.R14 ICMPv4.R13 UDP.R9 TCP.R11	Testing of saturation rate-limiting mechanism(s)	Show how a user would use the CRT tool to support testing for required time durations as described in this requirement.	3
"Ethernet".R11 ARP.R11 IPv4.R15 ICMPv4.R14 UDP.R10 TCP.R12	Reproducibility of robustness testing	For each protocol covered by CRT, show how the testing approach used by the CRT tool meets this requirement.	2
"Ethernet".R12 ARP.R12 IPv4.R18 ICMPv4.R15 UDP.R11 TCP.R23	Overall reproducibility	Covered for CRT tool by related requirements in [EDSA-310]	
"Ethernet".R13 ARP.R13 IPv4.R19 ICMPv4.R16 UDP.R12 TCP.R24	Specific test cases	Not required for CRT tool	

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
"Ethernet".R14 ARP.R14 IPv4.R20 ICMPv4.R17 UDP.R13 TCP.R25	Test tables	Create a mapping that shows that each numbered test (each table) listed in Clause 7 of each protocol specific CRT specification is addressed by the CRT tool. Specifically, the mapping shows how each test is carried out using the CRT tool, and points to the description of this method in the tool user documentation.	2
Requirements unique to specific protocols			
"Ethernet".R7	Specific focus of basic robustness testing	Show that the CRT tool covers the required implementations of "Ethernet"	1
ARP.R4	Susceptibility to cache poisoning	Covered for CRT tool by mapping of test ARP.T01 per ARP.R14 evidence above	
IPv4.R6-IPv4.R10 and IPv4.R16	Various	Identify the Clause 7 table(s) in the IPv4 CRT specification that are mapped to each of these requirements as a Reference Requirement. Then either show that the CRT tool implementation of those tests (as identified per IPv4.R20) fully meets this requirement, or show how additional tests implemented by the tool augment those tests to fully meet this requirement.	2
IPv4.R17	Specific focus of robustness testing	Show how the CRT tool test approach meets this requirement.	2
ICMPv4.R5 - ICMPv4.R8	Various	Identify the Clause 7 table(s) in the ICMPv4 CRT specification that are mapped to each of these requirements as a Reference Requirement. Then either show that the CRT tool implementation of those tests (as identified per ICMPv4.R17) fully meets this requirement, or show how additional tests implemented by the tool augment those tests to fully meet this requirement.	2

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
TCP.R2	Conditional test report notice of limited TCP robustness testability	Not required for CRT tool	
TCP.R5 TCP.R13 - TCP.R22	Various	Identify the Clause 7 table(s) in the TCP CRT specification that are mapped to each of these requirements as a Reference Requirement. Then either show that the CRT tool implementation of those tests (as identified per TCP.R25) fully meets this requirement, or show how additional tests implemented by the tool augment those tests to fully meet this requirement.	2