CRT Test Tool Recognition

**Background**

產品認證包括評估步驟, ISCI特許實驗室（CB）對提交的設備/系統進行穩健性測試, 嵌入式設備在EDSA認證過程中經受通信穩健性測試Communication Robustness Testing（CRT），且控制系統在SSA認證過程中經受CRT測試和系統穩健性測試System Robustness Testing（SRT）

測試工具必須能夠成功測試/驗證ISASecure認證規範中公佈的所有ISASecure嵌入式設備安全保障（EDSA）CRT要求和/或系統安全保障（SSA）SRT要求。 測試工具必須證明他們能夠執行具有一致結果的ISASecure認證測試

**CRT Tool Recognition Options**

**1. ISCI政策允許CRT工具供應商提交其工具以供僅用於EDSA認證的認可EDSA-201,包含CRT工具供應商為EDSA所需的所有CRT工具識別過程信息和文件參考（添加了EDSA-102勘誤表規範）**

**2. ISCI政策允許CRT工具供應商提交CRT工具，以便在SSA認證中使用,** **EDSA-201包含工具供應商（增加EDSA-102）所需的所有CRT工具識別過程信息和文件參考**

注意：截至2016年8月，除了支持SSA CRT和SRT測試所必需的EDSA CRT工具之外，還有一個額外的SSA CRT工具技術能力。

**ISCI Staff Processes the Tool Submittal for Recognition**

CRT test tool recognition process是ISCI技術人員對CRT測試工具的評估，以確保測試工具滿足ISCI CB使用的必要功能,讓供應商在其產品開發測試過程中使用，以提高其產品的安全性能，並確保其產品符合ISASecure CRT認證要求

滿足ISCI認可要求的CRT工具列在www.isasecure.org網站上，為您的產品擴大市場曝光率並提高可信度。

**Process**

有關CRT工具識別的流程步驟在EDSA-201通信穩健性測試工具識別流程文檔中有詳細說明

**Fees and Expenses**

申請人將收取測試工具提交的行政申請費（參見下面的費用表）。 申請人還將收取ISCI技術人員花費的時間（見下面的小時費用）以及相關的旅行和生活費用（按實際費用計算）。

**First Step**

第一步是聯繫ISCI總經理，他將向您發送一份官方的ISCI CRT工具識別申請表EDSA-203（此表格僅可直接從ISCI工作人員處獲得）。 ISCI強烈建議申請人在聯繫總經理之前審查EDSA-201通信穩健性測試工具認可流程

**CRT Tool Recognition Requirements**

**EDSA-201**

Purpose:

A certifier must use a test tool for CRT that has achieved recognized status under this process, in order to be accredited by ASCI

認證機構必須使用已在此過程中獲得認可狀態的CRT測試工具，以便獲得ASCI認可

實驗室認證在與這些程序相關的200系列文件中定義（例如[EDSA-200]，[SSA-200]）

The list of current CRT specifications and versions is maintained on the ISCI web site <http://www.ISASecure.org>.

當前的CRT規範和版本列表保存在ISCI網站http://www.ISASecure.org上

**References**

**[EDSA-200,310,401,402,403,404,405,406,102 , SSA-200]**

**Overview of CRT Tool Recognition Process**

Scope of Evaluation for Tool Recognition (工具的評估範圍)

CRT工具識別過程將評估工具的以下一般技術能力的覆蓋範圍:

(1) Tests for all ISASecure certifiable protocols (測試所有ISASecure可認證協議)

(2) Basic and load stress robustness tests(基本和負載應力穩健性測試)

(3) Capability to monitor the control loop(能夠監控控制迴路)

(4) Reproducibility of test results(測試結果的再現性)

ISCI將僅根據其執行CRT的技術能力評估測試工具, (最初)將不會評估該工具的用戶友好性，工具的維護和支持的未來前景

**Overview of Evaluation Approach**

**Tool Evaluation**

**Overview of Evaluation Criteria**



CRT工具的評估分四個步驟進行, 前三個步驟側重於工具的設計級別分析。 第四步根據實際工具輸出驗證工具特徵的樣本

對於與本步驟相關的本文件附錄A中標記的CRT規範中的每個要求, CRT工具供應商將提供書面證據以證明該工具符合此要求 (附錄A=ch5)

對於第四步，評估團隊將請求工具供應商提供的一組pcap文件和相關測試報告，這些報告是為該工具支持的指定測試生成的

Table1:

Step1: 初始化技術分析:

- 基礎證明:

此工具的使用者說明(User documentation)

測試報告(Test report): 在供應商選擇的sample device上進行CRT測試的測試報告

- 評估標準:

涵蓋所有可認證的協議

工具必需要支援產出報告的需求

測試的方法將涵蓋一般測試類型的要求

測試工具可進行控制迴路監控

Step2: 測試涵蓋率細節分析:

- 基礎證明:

供應商將提出涵蓋率,其展示了有關於在第7章中關於每個ISASecure的特定協議CRT規範所列出的每個編號的測試是如何利用工具完成的

工具的技術設計概述(提供給ISCI評估團隊成員)

- 評估標準:

工具能夠提供所有在第7章提出的所有個別的CRT規範需要的測試

工具擁有需要的field的值的容錯能力

控制迴路監控功能符合技術要求

Step3: 測試特徵分析:

- 基礎證明:

- 評估標準:

工具需滿足可再現要求

工具支援足夠的流量速率及其他測試時間要求(應是指在限定時間內完成)

Step4: 輸出驗證:

- 基礎證明:

pcap檔案及工具所產生的相關測試報告

- 評估標準:

工具的輸出須和原本的工具設計相符且符合CRT要求

**Evaluation Process**

該過程旨在首先確定候選工具的廣泛適用性，然後更詳細地連續檢查它, 列標題是執行該列中描述的任務的組織



Step1: 初始化技術資訊評估

- ISCI: 指定了所需的初始化技術資訊,此在這篇文件中指定,並提供給供應商申請表

- CRT Tool Supplier: 需要根據在Annex A中的Table3來填寫申請表和此步中需要的初始化技術資訊

Step2: 測試涵蓋率評估

- ISCI: 若前一步驟之初始化技術資訊合乎規定,則請向評估組要求詳細測試覆蓋率資訊及技術設計概述

- CRT Tool Supplier: 提交在Annex A中的Table3, Table4中每個和Step2相關的測試涵蓋率的證據。提供有關於工具的技術設計概述給評估團隊

Step3: 測試特徵評估

Step4: 樣本驗證

- ISCI: 若step2測試涵蓋率沒問題,則要求提供有關測試特徵的證據以及step4的pcap文件及分析結果

- CRT Tool Supplier: 依照Annex A中的Table3, Table4,提交相關的測試特徵的證據,並提交在step4中要求的pcap檔

ISCI會在step1中確定Table3中相關要求都滿足後才會進到step2,而在table2中說明在評估step2的證據之前必需要先評估完整性準則。特別是AnnexA中和step2相關的所有要求的證據需要在評估前先提供。此外,顯示此工具能支援所有必須的CRT tests的mapping必須涵蓋所有測試在step2評估前,且此mapping就是table4中所提到的項目的證據,表明其符合相關並行要求

為了被承認,需要證明tool符合Annex A中提出的ISASecure EDSA CRT規範的相關所有要求

**Maintenance of Tool Recognition**

若ICRT規範並未變化,但工具供應商想要提供更新檔,則應主動告知ISCI其更新中變動的性質,若ISCI認定變動的部份影響程度重大則會要求重新提供4.1節中所提的step1~3證據,且視情況也可能再對step4中的output進行再評估。因為Lab需要使用CRT工具且要對應的版本,因此相對應的流程處理(process)需由工具供應商盡早提出申請

**Ch5:** **Annex A - Guidelines for CRT Tool Evaluation Evidence**

因此，下表中的描述詳細說明了CRT工具應解決的這些規範中每個要求的各個方面。 在某些情況下，要求提供符合證據的特定表格，或提供證據表格的一些例子。 在所有情況下，應該指出的是，“表明......”這一短語將通過一個令人信服的論點來滿足，即在所有適用的情況下都要求顯示的要求

**Evidence for Compliance with Common CRT Requirements**

Table3 列出了符合ERT規範[EDSA-310]要求所需的證據，該規範列出了第7, 9.1 和9.3條中所有協議的通用CRT要求(ERT. R1~R78)

當中和CRT tool無關或不需要的有: 2~13, 15~19, 22~29, 31~33, 37, 44, 50~56, 62, 66~72, 76~78

R1: Types of CRT tests, 提供指標指向工具使用者或可證明工具涵蓋所有需要的協定的設計文檔, 1

R14: 提交用於監視基層功能的硬件和軟件, 顯示該工具如何提供對數字（二進制或多值）和模擬控制輸出的監視,必須直接支持規定的二進制數字和模擬電壓範圍,此外監控可能可以透過需求中所述的介面但超出電壓範圍或以離散多值完成, 1

R21: 測試期間監視基層功能的配置, 顯示在界面測試期間如何使用此功能，以允許工具用戶確定與故障相關的條件, 1

R30: “充分保持控制能力”的測試標準, 表明在R21下演示的方法可以監視控制輸出,並描述工具支持的測量精度 - 轉換之間測量的時間,顯示測試工具本身可以確定或者輸出可確定是否已經滿足測試,以保持要求的控制能力,2

R34: Test configuration 1 – switched IP connection from TD to DUT, 根據ERT.R34項目d說明如何在測試期間使用R21的功能以允許工具使用者確定與故障相關的條件, 2

R35: Test configuration 2 – non-switched IP connection from TD to DUT, 描述在此網路中使用之功能與ERT.R34中的差異,如果有差, 說明工具使用者如何使用此功能確定在此網路環境中的故障相關的條件, 2

R36: 穩健性測試階段, 提供工具的描述包含基本和負載應力穩健性測試的方法, 1

R38: 測試字段值的覆蓋範圍, 表明工具的測試方法符合要求, 2

R39: 在測試表示整數或列舉的固定長度字段時使用的必需測試值, 顯示CRT工具為所有測試協議產生具有這些特徵的流量, 2

R40: 在測試包含不同長度自定義字符串的確定長度字段時使用的必需測試值, 同R39, 2

R41: 測試具有不同固定大小子字段序列的字段, 同R39, 2

R42: 測試具有子結構和自定義長度的字段, 同R39, 2

R43: Protocol-specific load testing, 顯示該工具允許配置流量速率限制，並且生成的流量符合該限制(工具可以在64B網路中維持生成的60Mbps流量速率2分鐘),若為軟體則需提供可支持此流量速率的硬體用戶指南, 2

R45 單協議特定穩健性測試通過的標準, 顯示CRT工具輸出允許工具用戶根據此要求的標準確定通過或失敗, 這包括該工具每次測試的開始和結束時需驗證被測設備是否正在與測試工具通信,測試需全數通過,此外對於長時間的測試，通信還應每10秒驗證一次, 2

R46: 協議特定的穩健性測試失敗的再現性, 顯示工具使用者如何根據工具的輸出重現故障, 3

R47: 產生可重現的穩健性測試, 表明穩健性測試的工具方法符合此要求(含隨機過程), 3

R48: 偽隨機種子值, 表明CRT工具使用的偽隨機種子符合所需的大小和報告要求, 3

R49: 偽隨機種子重用, 顯示CRT工具使用的偽隨機種子可以重複使用，並且可以按照此要求中的描述複製測試數據, 3

R57: 測試報告管理信息, 顯示工具使用者如何確定支持的ISASecure規範的版本, 顯示工具使用者將如何確定使用的置信度,已運行的測試以及測試運行的日期, 1

R58: 報告CRT測試範例說明, 證明CRT工具文檔包含足夠的信息，允許測試實驗室記錄高級測試用例描述, 並將每個協議特定CRT規範的第7章中的測試映射到他們的測試程序, 2

R59: 報告CRT方法摘要, 顯示CRT工具文本包含足夠的信息,以允許工具使用者以對設備供應商有用的方式記錄測試方法, 1

R60: 報告CRT配置, 證明該工具提供了一種方法，用於輸出用於測試運行或一系列運行的工具的配置, 1

R61: 報告ISASecure測試失敗當作參考, 顯示工具使用者如何確定CRT規範中的特定要求或一組要求，這些要求在測試遇到故障情況時失敗, 2

R63: 報告測試執行的條件分支, 如果CRT工具採用的邏輯使得它基於遇到特定類型的異常結果而執行一些測試分支, 對於此類測試工具，請顯示該工具報告異常結果和因此執行的測試, 1

R64: 報告測試軟體版本, 顯示CRT工具用戶可以從工具測試報告中確定CRT工具的完整版本號,並且可以使用hash值驗證此軟件是否未更動, 3

R65: 報告測試標識和重複性參數, 顯示CRT工具使用者可以根據工具輸出確定，運行CRT所需的所有協議的工具參數來重現穩健性測試, 3

R73: 報告穩健性故障, 顯示CRT工具報告顯示證明符合R45的故障, 1

R74: 報告穩健性故障情況, 顯示CRT工具報告CRT故障的測試條件，根據R21，R34和R35中描述的過程確定, 1

R75: 報告穩健性測試用例結果列表, 描述CRT工具如何在產生此報告時支持測試工具使用者, 1

**Evidence for Compliance with Protocol-Specific CRT Requirements**

Table4描述了工具符合協議特定規範[EDSA-4nn]中要求的證據，如本文件第2章所列。 該表分為兩部分。 第一部分涵蓋了所有規範中具有相同名稱且非常相似且（在某些情況下相同）的要求。 第二部分列出了一個協議規範所特有的要求

和CRT tool無關或不需要: “Ethernet”.R2, “Ethernet”.R4,

R1: 穩健性測試失敗的標準, CRT工具中要求的第一個要點被[EDSA-310]證據涵蓋,第二個要點討論了每個協議的唯一故障條件,這些條件需要維護TD和DUT之間的通信，並且被證據R45涵蓋, 2

R3: 演示基礎操作, 描述為所有協議實施T00測試的方法, 2

R5: 測試每個消息字段對無效內容的敏感性, 解釋為什麼創造測試的技術方法將導致覆蓋每個CRT規範中列出的每個協議違規(錯誤字段中的值由R39-42解決), 2

R6: 基本穩健性測試中的組成元素, 顯示CRT工具可以為每個CRT協議生成此要求中描述的每種類型的網絡流量, 2

R9: 負載壓力測試中的組成元素, 顯示CRT工具可以為每個CRT協議生成此要求中描述的每種類型的網絡流量, 2

R10: 飽和速率限制機制的測試, 顯示用戶如何使用CRT工具支持測試所需的持續時間，如此要求中所述, 3

R11: 穩健性測試的再現性, 對於CRT涵蓋的每個協議，顯示CRT工具使用的測試方法如何滿足此要求，包括在適用的情況下使用種子偽隨機過程, 1

R14: 測試表格, 具體來說，映射顯示如何使用CRT工具執行每個測試，並指出工具用戶文檔中此方法的描述, 此外,還要在使用的出版物中，提供了有關如何設置所有可配置測試工具參數以運行ISASecure認證所需的CRT測試集的說明, 2

R7: 基本穩健性測試的具體重點, 證明CRT工具涵蓋了“以太網”所需的實現, 1

IPv4.R17: 穩健性測試的具體重點, 展示CRT工具測試方法如何滿足此要求, 2

1. report related: R57, R58, R59, R60, R63, R73, R74, R75

“Ethernet”.R1 – Criteria for robustness test failure

基本穩健性和負載壓力測試的通過或失敗應由以下因素確定：

創建的網絡流量條件下是否充分維護基本服務

在這些測試中，如[CRT.Essential\_services]中所定義

導致本文檔中指定的測試強制通過/失敗的任何特定條件

TCP 4.2.4 Mandatory protocol aspects

Conveying IP NPDU: TCP fixes the value of one of the header fields of any conveying IP NPDU

For IPv4, the NPDU header SHALL specify the TCP protocol in its ProtocolType field-> ProtocolType: 0x06 (TCP)

For IPv6, the last header in the NPDU SHALL specify the TCP protocol in its NextHeader field -> NextHeader: 0x06 (TCP)

4.2.4.2Checksum procedure

checksum field is the 16-bit one's complement (big-endian), virtual TCP TPDU = (extra 4 bits = pseudo header)+actual TPDU | pseudo header = source ip addr + destination ip addr + ip protocol ID for TCP + length in octets of conveyed TCP TPDU

**EDSA-406 (測試IETF TCP傳輸協議實現的穩健性)**

內容大綱:

1 規模

2 規範的參考文獻

3 定義及縮寫

4 在測試中的協定的要素

一般

TCP TPDU

強制及可選擇的協議功能

5 測試中所需要的其他協定的要素

從下層的protocol來的

從上層的protocol來的

6 穩健性測試

推動測試要求的目標

測試概述(觀)

在測試中的協定堆疊

Phase0 : DUT前處理

Phase1 : 基本處理

Phase2 : 基本穩健性測試

Phase3 : 負載壓力測試

可重現性

7 特定測試案例

============================================

文中若有和之後更新的部份存在衝突的情況下,以ch7的表格為準

對於每個RFCnnn，控製版本可以在http://tools.ietf.org/html/rfcnnn找到

嵌入式設備穩健性測試的要求，詳見<http://www.ISASecure.org>

[Port\_numbers] IANA端口號，在http://www.iana.org/assignments/port-numbers中指定

2 規範的參考文獻

RFC793，傳輸控制協議

RFC1122，互聯網主機要求 - 通信層（僅4.2節）

RFC1146，TCP備用校驗和選項

RFC1191，路徑MTU發現（僅3.1和6.4節）

RFC1323，用於高性能的TCP擴展

RFC1644，T / TCP - 事務的TCP擴展 - 功能規範

RFC1693，TCP的擴展：部分訂單服務

RFC1812，IP版本4路由器的要求（僅6.2節，僅適用於也作為IP路由器的DUT）

RFC2018，TCP選擇性確認選項

RFC2385，通過TCP MD5簽名選項保護BGP會話

RFC2883，TCP的選擇性確認（SACK）選項的擴展

RFC2988，計算TCP的重傳定時器

RFC3168，向IP添加顯式擁塞通知（ECN）

（僅6.1，它將CWR和ECE標誌及其過程添加到TCP）

RFC3390，增加TCP的初始窗口

RFC5681，TCP擁塞控制

RFC5482，TCP用戶超時選項

RFC5925，TCP認證選項

RFC6247，將未部署的TCP擴展RFC 1072，RFC 1106，RFC 1110，RFC 1145，RFC 1146，RFC 1379，RFC 1644和RFC 1693移至歷史狀態

RFC862，Echo協議

3 定義及縮寫

定義(3.1.1~3.1.13):

3.1.1: CC\* <-> TCP option CC, CCNEW, CCECHO

3.1.2: device under test <-> 在測試期間被刺激和觀察的裝置

3.1.3: erroneous (message or PDU or option) <-> PDU(or PDU選項)違反結構之語法或內容違反語義規則或是兩者皆是

3.1.4: Ethernet <-> IETF Ethernet II協議或IEEE 802.3上的IEEE 802.2 Type1 LLC上的IEEE 802 SNAP

3.1.5: fragmenting <-> IPv4的功能, 在傳輸之前將一個未分段的NPDU映射到多個較小的分段NPDU

3.1.6: inferior <-> 比參考協議更低層或子層的協議

3.1.7: lower tester <-> 控制和觀察DUT中的協議層實現的測試器

3.1.8: malformed (message or PDU) <-> PDU違反結構的語法規則

3.1.9: reassembling <-> IP接收後用於從多個小NPDU重建一個未分段的NPDU

3.1.10: superior <-> 比引用的協議更高層或其子層的協議

3.1.11: testing device <-> 概念性單個網絡連接設備, 但也可能是由多個可連接實體網路的設備組成,用以測試被測設備的穩健性

3.1.12: upper tester <-> 通過控制和觀察來控制和觀察DUT中的協議層實現的測試器

3.1.13: vulnerability <-> 系統的設計，實施，操作或管理中的缺陷或弱點，可能被利用來違反系統的完整性或安全策略

縮寫(看table) 以快照拼一起看較佳

縮寫字串列表: ACK,APDU,CRT,CWR,DPDU,DUT,ECE,ECN,FIN,FSM,GPL,IANA,ICMP,IETF,IP,IPv4,IPv6,NIST,(N)PDU,NPDU,PSH,RFU,RST,STS,SYN,TCP,TD,TPDU,URG

4 在測試中的協定的要素

4.1 一般: 本文檔規定了IETF TCP協議的穩健性測試，IETF TCP協議是一種有狀態傳輸協議，提供有序，可區分(1)優先級(2)可靠的(3)端到端 通信通道

4.2 TCP TPDUs:

TCP TPDU 結構: 展示於Fig 1. (big-endian octet order)

結構=Header + Data, Header(32 bits),組合均列於Fig 1.

強制區(fields):

以下字段是每個TCP TPDU的必需組件（其中字段大小以八位byte（B）或位元bit（b）指定）

(a) SourcePort (SP): (2B)

(b) DestinationPort (DP): (2B)

(c) SequenceNumber (SN): (4B)

(d) AcknowledgmentNumber (AN): (4B)

(e) DataOffset (DO): (4b)

(f) RFU: (4b)

(g) TCP flags: (8b)

CWR=ECE=URG=ACK=PSH=RST=SYN=FIN (1b)

(h) Window (W): (2B)

(i) Checksum: (2B)

(j) UrgentPointer (UP): (2B)

(k) Options: (0B .. 40B length)

(l) Data: (varying length ≥ 0B, granularity 1B, not padded to a multi-octet boundary)

選擇區(fields):

TCP定義了兩種類型的選項，每種選項通常使用big-endian八位字節順序進行結構化，如圖2所示(single-octet options, multi-octet options)

為TCP定義了17個特定選項，如圖3和圖4。

EOS (1B), PAD (1B), MSSN (4B), WSN (3B), SACKN (2B), SACK (2+8n B), ECHORQ (3B), ECHORP (3B), TS (10B), POCR (2B), POCSP (3B), CC (4B), CC.NEW (4B), CC.ECHO (4B), ACR (3B), ACD (2+n B), MD5 (18B)

### The status of TCP options is summarized at https://www.ietf.org/mail-archive/web/tcpm/current/msg03199.html

!!! 只有在同一TCP TPDU中設置SYN標誌時，MSSN選項才有意義。 要求發送方和接收方都支持此選項，並且當所需的MSSN值與默認值536 B不同時，使用此選項

強迫協定方面(Mandatory protocol aspects)

Conveying IP NPDU (修復IP NPDU)

-IPv4

-IPv6

校驗程序(checksum)

Checksum field: 2bytes=16bits (big-endian octet order) , 在虛擬TCP TPDU中通過為實際TPDU加前綴由額外4 B組成的偽標頭創建, for IPv4-> Fig 5., for IPv6->Fig 6.

每個偽標頭包含Source IP Address; the Destination IP Address; the IP protocol ID for TCP and the length in octets of the conveyed TCP TPDU

在虛擬TCP TPDU內，在計算校驗和時，包含的變長TCP TPDU的校驗和字段被設置為零, 虛擬header的第三個4B字中的TCP TPDU長度是由關聯網絡層呈現或報告的TPDU的長度。 這通常是TCP頭長度加上八位字節的計算數據長度，不包括虛擬TCP TPDU的額外前綴或填充後綴八位字節

TCP state machine:

表示其狀態的列表列在圖7,其轉換則列在表1

**Sequencing concepts**

一般: Sequence numbers are unsigned 32-bit values, 表3列出了與TCP連接相關的概念狀態變量，以及作為TCP TPDU的隱式或顯式參數傳送的相關變量。Table3大致分成3類,傳送seq 變數,接收 seq 變數, 目前階段(segment)變數

**TCP connection sequencing concepts and constraints**

Table4: TCP連接：接收段的可接受性

**Elements of procedure: Connection establishment via 3-way handshake**

**Optional TPDU components and elements of procedure**

一般:

The only optional TPDU components are the options of the TCP option field唯一可選的TPDU組件是TCP選項字段的選項

**Receiver maximum segment size**(接收器最大段大小)

**TCP echo (deprecated for timestamp use)**

**Timestamp**

**Window scaling**

**Selective acknowledgment**

**Partially ordered connection (experimental, obsolete)**

**Transaction support (experimental, obsolete)**

**Alternate checksum**

**MD5 signature (obsolete)**

**User timeout**

**Authentication option**

RFC5925規定使用加密消息認證碼（MAC）作為消息摘要，以支持TPDU完整性並防禦重送攻擊

**Mandatory and optional protocol features**

TCP協議的強制功能是

**Elements of other protocols required for the testing**

**Protocol(s) from inferior layers used by this protocol**

**Protocol(s) from superior layers used to test this protocol**

RFC768的TCP協議被指定為在IPv4上操作，因為圖5的虛擬TCP TPDU使用來自傳送IPv4 NPDU的信息, RFC792（已修改）的無法到達終點現象，超時和參數問題ICMP錯誤PDU被用於報告由DUT的TCP實現檢測到的接收TCP TPDU中的錯誤情, RFC2460,8.1通過使用圖6的替換虛擬TCP TPDU來指定TCP如何適用於IPv6，該TCP TPDU使用來自傳送IPv6 NPDU的信息。 對於IPv6，RFC4443（修訂版）是相應的控制ICMP規範

**Protocol(s) from superior layers used to test this protocol**

一般

**Robustness testing**

**Goals that drive testing requirements**

本文檔中描述的測試目標是評估：

a）具有一組已實現協議的嵌入式控制設備的穩健性，以及

b）設備的抗攻擊能力，包括在持續發生此類攻擊時對設備報告和控制功能的影響

如[EDSA-310]中的具體要求所述，隨後的要求是進行此測試

1）在測試開始之前確定DUT和測試配置的其他部分是否滿足正常的操作期望;

2）確定DUT是否能夠在接收到無效幀的同時繼續在自動化環境中按預期運行; 和

3）確定DUT是否能夠維持長時間大量通信負載的間隔

**Testing overview**

必須對DUT進行預處理:

1）滿足[EDSA-310]的要求，以證明測試期間的持續正確操作;

2）如果在DUT的默認操作配置中被阻止，則取消阻止TCP Echo服務器協議（port 7）

穩健性測試發生在可能重疊的三個概念階段，加上測試環境預處理階段(total=4)

第一個概念階段，Baseline操作，試圖在嘗試進行任何協議模糊測試或壓力測試之前，表現用於測試的選定的DUT協議套件在低網絡通信負載下對於簡單測試案例似乎正常運行

注1：這種明顯正確行為的初步證明表明，假設在附加測試期間發生故障是由於被測試的特定協議的漏洞，而不是測試套件中的其他協議

第二個概念階段，即基本穩健性測試，探討實作的能力是否不會因單獨或組合地接收任意錯誤幀而造成傷害。 對於存在狀態性的協議，該階段還測試對各種狀態相關的正確和不正確的PDU序列的回應的實作成果

注2：該概念階段側重於簡單的協議穩健性/模糊測試

第三個概念階段，負載壓力測試，探討對包含有效PDU的高流量速率的實作的回應。 對於存在狀態性的協議，該階段還測試對各種狀態相關的正確和不正確的PDU序列的實作的回應

注3：這個概念階段側重於負載/性能測試，首先是在高但可能是可持續的接收器網絡通信負載下，然後是大規模過載

**Requirement TCP.R1 – Criteria for robustness test failure**

基本穩健性和負載壓力測試的通過或失敗應由以下因素確定：

(1)在這些測試下所產生的網絡流量中是否能充分保持必要功能,如同在[CRT.Essential\_functions]中定義一樣

(2導致本文檔中指定的測試強制通過/失敗的)任何特定條件

TCP協議是具有簡單觸發 - 應答機制的有狀態協議

**Protocol stack used for testing**

**Protocol(s) from inferior layers used by this protocol**

IP is used to convey TCP TPDUs, 最初的EDSA CRT測試協議包括IPv4而不是IPv6或其他網絡協議, RFC793（修訂版）中指定此規範下測試的是IPv4, 該選擇會影響TCP校驗和計算中使用的地址字段值。 本文檔還規定在IPv6上運行TCP測試所需的必要調整

**Protocol(s) from superior layers used to test this protocol**

TCP是一種有狀態傳輸協議，可用於傳遞兩個不同優先級的混合APDU, TCP的某些方面只能通過使用具有查詢/回復機制的高層協議來觀察,測試DUT TCP實現的穩健性的最簡單方法是讓DUT提供並使TD在port 7（RFC862）上使用標準TCP Echo服務器, 此服務器接受具有well-form header，交換源和destination IP地址以及source and destination ports的TCP TPDU

**Requirement TCP.R2 – Conditional test report notice of limited TCP robustness testability (DUT: Device Under Test)**

如果在DUT中沒有TCP Echo服務器協議，則只能進行有限的TCP穩健性測試。 在這種情況下，測試結果應該說明DUT中TCP Echo服務器的不可用性，因此DUT的TCP實現對基於序列號的攻擊的穩健性只是部分可測試的

**Phase 0: DUT preconditioning**

**Requirement TCP.R3 – Preconditioning of DUT, TD and any firewalls between the DUT and TD (Test Device)**

a）如果可能，DUT應該通過啟用DUT作為TCP Echo協議（RFC862）上的服務器進行穩健性測試，可能僅用於協議測試目的，在DUT內啟用該協議

b）DUT協議堆疊實現，DUT中的任何防火牆以及DUT和TD之間的任何中間防火牆應該通過禁用任何阻止從DUT到TD的ICMP錯誤PDU的傳輸或傳播的規則來進行穩健性測試

c）測試系統中的DUT，TD和可能的其他設備應配置為允許在測試條件下根據[CRT.Essential\_functions]中的要求觀察嵌入式設備的基本功能的性能

[CRT.Essential\_functions]中定義的基本功能包括控制迴路，控制設備配置的命令，如設定值和過程警示。 獲得可觀察性的關鍵方法是，作為測試配置的一部分，使用其他自動化系統元件，這些元件已被設計為與DUT通信並監視DUT

**Phase 1: Baseline operation**

**Requirement TCP.R4 – Demonstration of baseline operation(演示基本操作)**

在TD開始穩健性測試之前，DUT應證明其在測試環境中按預期運行的能力，包括DUT協議堆疊的TCP組件存在且運行，以及DUT可以保持基本功能

**Initial ACK sequence number generation**

TCP的基本操作測試階段包括基於對“新”（例如，欺騙）TCP連接的初始序列號的預測來評估DUT對攻擊的抵抗力

**Requirement TCP.R5 – Unpredictability of DUT’s initial sequence numbers(DUT初始序列號的不可預測性)**

RFC793（TCP的初始規範）規定，初始TCP序列號應該從偽(虛擬)時鐘生成,通過RFC4987, TCP的現今實作不應該產生看起來是相關的初始序列號的值

為了通過不同的穩健性測試套件提供隨機性評估的一致性, 應該應用來自GPL'd dieharder隨機性測試套件的三個NIST發起的STS測試 - Monobit，Runs和Serial，並記錄他們的結果 在TCP穩健性測試報告中

**Presence of proprietary protocol extensions**

供應商通常以專有方式擴展標準協議以提供標準協議未涵蓋的功能，這些擴展可以採用額外消息類型，標準消息中的額外字段或標準消息中標準字段的額外功能的形式

**Requirement TCP.R6 – Equipment vendor disclosure of proprietary protocol extensions(設備供應商披露專有協議擴展)**

當提供用於測試的協議已經通過商討過的專有擴展實現時，供應商應該以類似於第4章的方式記錄擴展，這樣穩健性測試可以探索這些協議擴展的預期和非預期後果。 可以接受的是，設備供應商與提供ISCI穩健性測試服務的組織之間的保密協議（NDA）涵蓋對此專有信息的訪問權限

**Phase 2: Basic robustness testing**

概述:

通過分析控制協議標準來識別特定穩健性測試的區域,包括所有字段值範圍(field value range)和表示基本訊息的邊界值。基本穩健性測試包括測試每個這些邊界值的可接受性，以及當這些相鄰值可以在消息編碼中表示時，接受或拒絕相鄰值到那些邊界值,此外還包括測試是否正確區分和處理指定用於傳遞signed或unsigned的字段

此測試中還包括協議消息的無序接收(即訊息分開傳送後並非依序接收到)，以及相關協議消息的接收(多個IP片段的payload),其中的不一致的選項或是重疊到的部份必需要在處理過程中進行重組。此測試中還包括數據元素的各種替代表示(例如，UTF 8和各種字符轉義和重新編碼序列，例如URL中空格字符的％20的常見替換)

#!!

從概念上講，基本穩健性測試包括以下內容，其中消息流量的數量或速率不是一個因素：

a）有效消息流量的測試

1) in expected sequences, sent at a low rate(預期序列，以低速率發送)

注意TCP流量是有狀態的，因為可以傳達用於測試的更高層協議流量

2）以低速率發送的意外但有效的序列（即，在某些條件下消息被認為對協議有效，但對特定協議狀態，消息序列或相對時間不是預期的）

b）低速率錯誤消息流量的測試（例如，設備在接收到錯誤消息後的功能）包含

1）單個錯誤消息，包括具有不一致字段值(field value)的消息;

2）錯誤序列中正確形成的消息

3）錯誤消息的序列

[EDSA-310]描述了在這些網絡流量條件下充分發揮設備基本功能的標準。 這些標準取決於具體功能以及該功能是否在用於測試流量的同一網絡接口上運行

**Basis for TCP robustness testing**

從TD發送到DUT的正確和錯誤形成的TCP TPDU，其中一些請求來自DUT的預期回應，構成TCP穩健性測試的基礎 (Transport-layer Protocol Data Unit)

**Requirement TCP.R7 – Testing of each message field for sensitivity to invalid content(測試每個消息字段對無效內容的敏感性)**

對於需要錯誤消息或消息序列的基本穩健性測試，應改變從TD到DUT的有效TCP TPDU或TPDU序列,使得其中一個組成(component)是錯誤的或是讓它違反4.2.4,4.2.5,4.2.6或4.3所述內容。在基本穩健性測試期間，用於傳送被測試協議的低級PDU應該是有效的

注2：正在測試的是TCP協議本身，而不是任何傳送的更高級應用協議

建議基本穩健性測試分階段進行，從簡單到復雜，如6.6.1中所列舉，並由以下列表表示, 通常，這種排序簡化了定位軟件源或硬件問題的任務，如果它們被測試發現的話。 但是，這種排序不是必需的

**Requirement TCP.R8 – Constituent elements in basic robustness tests(基本穩健性測試中的組成元素)**基本的TCP穩健性測試應包括以下元素，可以是在不同的測試階段，也可以是測試供應商選擇的形式混合：

a）有效的消息流量

b）錯誤的消息

**Phase 3: Load stress testing**

**概述:**

注1：該測試階段用於探索對繁忙的工廠狀況以及故意的攻擊的抵抗。

從概念上講，負載壓力測試包括在兩個不同階段發送的有效消息流量測試

階段1 - 以低於DUT供應商指定的飽和率閾值的高速率發送有效消息流量（例如，模擬正常但繁忙的工廠條件）;

階段2 - 有效的消息流量以高達自動協商的鏈路速率發送（例如，模擬某種攻擊或故障）

針對協議實施的攻擊採取的形式是通過格式錯誤的消息重複探測，或者通過正確形成的消息，其到達順序和相對時間由攻擊者控制，或（更常見地）通過其組合控制，所有這些都旨在利用某些疏忽或 特定協議實現中的錯誤，或者激活實施組織未考慮的多層協議堆疊的某些交織方面

注2：由於設計人員或操作員的疏忽，也可能發生自身意外攻擊, 常見例子是故意的緩衝區溢出，其中實現者忽略了檢測過多的消息或字段大小

**Basis for load stress testing**

針對高流量速率的設備防禦會影響負載壓力測試，並由設備供應商根據以下要求進行記錄:

**Requirement TCP.R9 – Documentation of self-protective rate limiting behavior(自我保護速率限制行為的文檔)**

在DUT供應商對測試過程中的一個或多個協議施加速率限制（例如，“以太網”，IP或TCP）的情況下，DUT供應商應該記錄當消息速率超過未特定過的速率時, 對於所識別的協議產生速率限制。未指定的費率，按[CRT.Rate\_limiting]的要求

**Requirement TCP.R10 – Constituent elements in load stress tests(負載壓力測試中的組成元素)**

負載壓力測試應包括以下元素，可以是不同的測試階段，也可以是測試供應商選擇的形式混合

a）高速有效的消息流量

b）a）的過飽和率版本，以TD可以支持的最大自動協商鏈路速率

**Requirement TCP.R11 – Testing of saturation rate-limiting mechanism(s)(飽和速率限制機制的測試)**

飽和率測試應該持續兩分鐘，足以讓任何飽和效應顯現出來。本質上涉及大量TPDU（例如端口掃描）的測試可能需要運行更長的持續時間

**Requirement TCP.R12 – Reproducibility of robustness testing(穩健性測試的再現性)**

基本穩健性測試應使用確定性選擇過程，以測試有效和錯誤消息的組合。具體要求的測試用例參考ch7。負載壓力測試應使用確定性選擇過程，用於測試一系列有效消息。後者包括格式錯誤的消息

**Specific load stress testing**

概述:

由於其複雜的有狀態性和成功的TCP網絡攻擊的數十年歷史，有許多特定的TCP協議功能及其組合需要特別注意

a）初始ACK序列號生成

b）優先權流量交織和去交織

c）正確處理外部port號0和65535

d）DUT回應關閉並打開其對等方的TCP接收窗口

e）DUT回應其對等方的TCP接收窗口邊緣的不一致前進

f）DUT的TCP接收窗口邊緣的對等拒絕

g）拒絕欺騙性來源，試圖使DUT連接到自身

h）承受SYN洪水攻擊的機制

i）承受SYN / ACK泛洪攻擊的機制

j）承受RST和類似洪水襲擊的機制

k）承受DUT通信員的FIN，RST和類似TCP標誌的欺騙的機制

l）當DUT使用TS選項時，DUT響應對TS選項中的回顯時間戳值的操縱以破壞DUT的往返傳輸延遲估計過程

m）當DUT協商使用SACK選項時，DUT響應不一致和無效的選擇性確認

!! 許多TCP選項對其實用程序有限制, 在https://www.ietf.org/mail-archive/web/tcpm/current/msg03199.html中進行了總結。穩健性測試應包括在DUT無用時向DUT發送此類選項，因此可能不會出現這種情況。它還應包括發送違反選項值或編碼的任何指定約束的選項

**Priority traffic interleaving and de-interleaving**

**Requirement TCP.R13 – Ability to accept priority traffic(能夠接受優先流量的能力)**

TCP連接可以傳送正常和緊急字節流，它們在發送之前被交錯並且在接收之後被分離。因此，TCP穩健性測試應包括測試DUT在收到包含的TPDU時是否失敗

一個八位字節的優先級數據，以及非優先級數據的八位字節

僅優先級數據

注：允許並鼓勵測試優先級和非優先級數據的其他組合（或比率）

**Handling of extremal port numbers 0 and 65535**

**Requirement TCP.R14 – Handling of extermal port numbers 0 and 65535(處理外部port號0和65535=2^16-1)**

TCP端口號是無符號的16位數字，沒有範圍限制。當指定端口32768或更高時，預計未將端口號聲明為無符號數的實作會出現故障。同理port 0時也有一樣的情況

**DUT response to closing and opening its peer’s TCP receive window**

TCP連接的每一側通過發送方指定的接收窗口向其TCP對等方指定該方准備接受的附加TCP有效負載數據量。 每一方都可以完全控制自己的接收窗口，並可以隨意關閉，打開和重新關閉該窗口。當TD關閉其接收窗口時，DUT應在檢測到後關閉該閉包，並且在TD的接收窗口再次打開之前不發送TCP有效載荷的其他八位字節。 但是，由於並發和傳輸延遲，遠程TCP對等體檢測到接收窗口關閉可能需要一些時間; 在此期間，即使TD認為其接收窗口關閉，也可以由TD接收附加八位字節。當TD打開一個關閉的接收窗口時，DUT應該在檢測到該開放後尊重該開放，並發送TCP有效載荷的其他八位字節，直到但不大於為打開的接收窗口指定的八位字節數。

**DUT response to inconsistent advance of its peer’s TCP receive window edges**

**Requirement TCP.R15 – Defense against inconsistent peer receive window edges(防止不一致的對等接收窗口)**

在其TCP接收窗口前進不一致的攻擊者可能能夠利用DUT的TCP實作中的故障，特別是當與TCP連接的重置相結合時。 TD應該探測DUT對接收序列號和窗口變化的組合以及RST標誌的使用的回應

**Peer dishonoring of the DUT’s TCP receive window edges**

**Requirement TCP.R16 – Defense against peer dishonoring of the DUT’s TCP receive window edges(防禦DUT的TCP接收窗口邊緣的對等拒付)**

**Rejection of spoofed source addresses that attempt to cause the DUT to connect to itself**

**Requirement TCP.R17 – Rejection of TCP connection attempts where the source IP address is an IP address of the DUT)(拒絕TCP連接嘗試，其中源IP地址是DUT的IP地址)**

通過欺騙source IP地址，攻擊者可以請求DUT與其自身建立TCP連接，可以在單個DUT TCP端口（即目標端口和欺騙源端口相同）上，也可以在一對不同的DUT TCP端口之間建立TCP連接, 這種類型的攻擊被稱為“陸地”或“LaTierra”攻擊

在DUT能夠建立這種連接的情況下，對於嵌入式設備，它通常必然是兩個DUT端口之間的連接，它們都充當服務器。DUT保護自己免受此攻擊的最簡單方法是拒絕建立或維護遠程通信者分配給DUT的IP地址的任何連接。

TD應嘗試通過使用DUT自己的IP地址作為TD連接嘗試的欺騙源IP地址來與DUT建立TCP連接。可以指定任何欺騙的源端口，包括與TCP連接請求的目標端口相同的端口。 TD應通過竊聽觀察DUT的IP傳輸來報告這種連接請求是否成功

**Mechanisms to withstand a SYN flood attack**

**Requirement TCP.R18 – Resistance to SYN flood attacks(抵抗SYN泛洪攻擊)**

RFC4987和後續分析已經確定TCP服務器實現可以推遲為所請求的TCP連接分配狀態，直到啟動TCP連接的3次握手的第3階段之後，這對應於從第2個TPDU（ACK）的接收。所有TCP服務器實現應該實現這樣的延遲狀態分配，以最小化TCP SYN泛洪攻擊的影響，其中攻擊者只是發送無數的TCP連接建立請求而不完成任何一個的3次握手

**Mechanisms to withstand a SYN/ACK flood attack**

**Requirement TCP.R19 – Resistance to attacks that leave connections open but unused(抵抗使連接保持打開但未使用的攻擊)**

最近的分析已經確定TCP攻擊者可以採用類似的技術來推遲為所請求的TCP連接分配狀態，直到連接建立完成為止。

注1：這種攻擊技術的開發是為了使攻擊者能夠延遲自己的資源分配，直到它們從偵聽TCP服務器中引出響應，從而促進對大量可能響應的目標IP地址的“霰彈槍”攻擊。

注2：上述攻擊者技術可以通過使用少於32位的序列號來擴展，以確定48位的欺騙地址。這允許攻擊者將TCP連接保持活動一段時間，即使受攻擊的服務器安裝了導致非活動TCP連接終止的防禦措施

由於太多成功的TCP連接嘗試而導致TCP狀態記錄的內存資源運行不足的強大TCP服務器實現可以終止非活動TCP連接作為響應以緩解此潛在攻擊。

**Mechanisms to withstand RST and similar flood attacks**

**Requirement TCP.R20 – Resistance to attacks that spoof TCP flags(抵制惡意TCP標記的攻擊)**

可以竊聽與DUT的現有不安全TCP連接的攻擊者可以欺騙DUT的通信對象並使DUT接受攻擊者的TCP TPDU (->MITM?)

建立並維持與DUT的TCP連接的攻擊者可以引起DUT上由連接傳達的特定應用協議允許的任何負載，包括使DUT回應接收到的重置連接的TCP TPDU，或者打開和關閉攻擊者的接收窗口。一般而言，TCP內部無法抵禦此類攻擊

**Mechanisms to withstand spoofing of FIN, RST and similar TCP flags of a DUT correspondent**

在現有TCP連接中欺騙DUT的通信者的攻擊者可能導致DUT進行與DUT通信者所期望的狀態轉換不一致的狀態轉換。 特別是，顯然來自包含RST或FIN標誌的通信者的欺騙TCP TPDU將導致DUT呈現與其通信者不一致的狀態。

TD應該通過充當DUT通信者和欺騙攻擊者來測試DUT對這種欺騙性TCP TPDU的響應，觀察DUT對從“通信者”和“攻擊者”接收到交織TCP TPDU的響應。 TD應測試設置和重置TCP標誌的各種組合，包括FIN標誌置位和ACK和/或PSH標誌復位的情況。

**DUT response to receipt of inconsistent or contextually-inappropriate selective acknowledgment block edges**

**Requirement TCP.R21 – Defense against deliberately inconsistent and/or contextually-inappropriate selective acknowledgment block edges when the DUT has negotiated the use of the SACK option(當DUT協商使用SACK選項時，防止故意不一致和/或上下文不合適的選擇性確認區塊邊界)**

當DUT似乎支持選擇性確認時，通過有效地確認提供的SACKN選項，允許在TCP連接上使用選擇性確認，TD應測試DUT對SACK選項中不合邏輯和不一致的字段值的防禦, 此類測試還應包括由SACK選項傳達的選擇性確認之間的故意不一致的交互，以及由TPDU ACK標誌發信號通知的完全確認。TD應該探測DUT對接收TCP選擇性確認選項中傳達的不一致和/或錯誤塊子段的組合的回應，特別是當使用RST標誌時

**DUT response to manipulation of timestamp values in a TS option**

**Requirement TCP.R22 – Resistance to manipulation of timestamp values in a TS option(抵抗在TS選項中操縱時間戳值)**

許多TCP實現採用non-trivial算法來過濾使用TS選項產生的往返傳輸延遲測量序列中的延遲。

TD應測試DUT對故意操縱的反應

TS選項字段中的時間值(和/或)

是否存在TS選項字段

其中該操作旨在破壞DUT的往返傳輸延遲估計過程和/或破壞DUT對不屬於當前TCP連接的序列號空間的當前半週期的TPDU的拒絕。預期中斷中的第一個需要操縱回顯的時間戳,稱之為TS Echo應答（TSecr）, 第二個需要錯誤陳述始發時間戳稱之為TS值（TSval）

**Reproducibility**

**Requirement TCP.R23 – Overall reproducibility**

基本操作，基本穩健性測試和負載壓力測試應根據[CRT.Reproducibility]的要求重現。這些要求認識到DUT本身的確定性行為不受測試者的控制，必須假設。

**!#!Specific test cases**

**Requirement TCP.R24 – Specific test cases**

測試的協議套件至少應記錄在表5中指定的詳細信息中。

<see Table5> | protocol layer, 允許替代方案,受測protocol,max網路溝通載入時間

**Requirement TCP.R25 – Testing SHALL include at least that specified by Table 6 through Table 30(至少要測表6~表30)**

結果顯示為通過或失敗的測試，如果觀察到指示的預期響應，則應通過。如果表中的“結果”行未指示“通過/失敗”，則表示測試結果提供有關要包含在測試報告中的DUT的安全相關信息，但不會導致設備無法通過認證

Pass/Fail : 24

Response need: 1

Table items all the same:

Test ID, Test name, Test description, Reference requirements, Test type, Test status, Expected DUT behavior, Test object, Test configuration, Test procedure, Expected DUT response, Ultimate results, Remarks

Table 6: TCP.T00: Baseline operation

Reference requirements: Requirement TCP.R4

Test type: Baseline operation

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 7: TCP.T01: Statistical analysis of initial sequence number values

Reference requirements: Requirement TCP.R7, violating 4.3, M11; Requirement TCP.R5

Test type: Baseline operation

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Quality measure for the sequence of generated random numbers

Table 8: TCP.T02: Truncated TPDU: truncated fixed header

Reference requirements: Requirement TCP.R7, violating 4.3, M1 and M3

Test type: Basic robustness: PDU structural violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 9: TCP.T03: Truncated TPDU: truncated header options

Reference requirements: Requirement TCP.R7, violating 4.3, M2

Test type: Basic robustness: PDU structural or content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 10: TCP.T04: Truncated TPDU: truncated priority data

Reference requirements: Requirement TCP.R7, violating 4.3, M2

Test type: Basic robustness: PDU content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 11: TCP.T05: Invalid TPDU checksum

Reference requirements: Requirement TCP.R7, violating 4.3, M4 and M5

Test type: Basic robustness: PDU content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 12: TCP.T06: Malformed or undefined TCP TPDU options

Reference requirements: Requirement TCP.R7, violating 4.3, M10

Test type: Basic robustness: PDU content syntactic or semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 13: TCP.T07: Unrestricted interpretation of select TCP TPDU options

Reference requirements: Requirement TCP.R7, violating 4.3, M12

Test type: Basic robustness: PDU content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 14: TCP.T08: “Land” and “LaTierra” attacks

Reference requirements: Requirement TCP.R7, violating 4.3, M9 Requirement TCP.R17

Test type: Basic robustness: self-referent NPDU addressing

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 15: TCP.T09: Spoofed TCP flags

Reference requirements: Requirement TCP.R20

Test type: Basic robustness: PDU content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 16: TCP.T10: Inconsistent peer receive window edges

Reference requirements: Requirement TCP.R15

Test type: Basic robustness

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 17: TCP.T11: Defense against peer dishonoring of the DUT’s TCP receive window edges

Reference requirements: Requirement TCP.R16

Test type: Basic robustness

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 18: TCP.T12: Inconsistent and/or contextually-inappropriate selective acknowledgment block edges

Reference requirements: Requirement TCP.R21

Test type: Basic robustness

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 19: TCP.T13: Manipulation of DUT timestamps echoed to the DUT

Reference requirements: Requirement TCP.R21

Test type: Basic robustness

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 20: TCP.T14: Priority traffic interleaving

Reference requirements: Requirement TCP.R13

Test type: Basic robustness: PDU parsing and semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 21: TCP.T15: Use of extremal TCP port numbers

Reference requirements: Requirement TCP.R14

Test type: Basic robustness: PDU parsing and semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 22: TCP.T16: TCP conveyed-application robustness

Reference requirements: (none)

Test type: Basic robustness: APDU content semantic violations

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 23: TCP.T17: Maintenance of service under high load: Raw TPDU flood of urgent data

Reference requirements: Requirement TCP.R10

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 24: TCP.T18: Maintenance of service under high load: Initial SYN flood

Reference requirements: Requirement TCP.R18

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 25: TCP.T19: Maintenance of service under high load: Unused open connection flood

Reference requirements: Requirement TCP.R19

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 26: TCP.T20: Maintenance of service under high load: Segment reassembly flood

Reference requirements: Requirement TCP.R19

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 27: TCP.T21: Maintenance of service under high load: Closed receive window flood

Reference requirements: Requirement TCP.R19

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 28: TCP.T22: Maintenance of service under high load: RST flood

Reference requirements: Requirement TCP.R20

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 29: TCP.T23: Maintenance of service under high load: FIN flood

Reference requirements: Requirement TCP.R19, 6.7.3.11

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail

Table 30: TCP.T24: Maintenance of service under high load, including network saturation: Raw TPDU flood

Reference requirements: Requirement TCP.R10

Test type: Load stress

Test status: Mandatory

Test configuration: need ref [CRT.Test\_configuration\_1]

Ultimate results: Pass or fail