Network Device Interpretation # 201644

Self-testing of integrity of firmware and software

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Feb-2017*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *NDcPP V1.0, FWcPP V1.0, ND SD V1.0*

Affected Section(s): *FPT_TST_EXT.1*

Superseded Interpretation(s): *None*

Issue:

Question about the FPT_TST_EXT.1 SFR which affect multiple vendors. The SFR states:

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]] to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF].

The SFR does not impose any specific self-tests in the last assignment. However the application note seems to contain a requirement within it:

Application Note 29

It is expected that self-tests are carried out during initial start-up (on power on). Other options should only be used if the developer can justify why they are not carried out during initial start-up. It is expected that at least self-tests for verification of the integrity of the firmware and software as well as for the correct operation of cryptographic functions necessary to fulfil the SFRs will be performed. If not all self-test are performed during startup multiple iterations of this SFR are used with the appropriate options selected. In future versions of this cPP the suite of self-tests will be required to contain at least mechanisms for measured boot including self-tests of the components which perform the measurement.

Other PPs such as the MDMPP contain a second element, FPT_TST_EXT.1.2, for integrity and this application note seems inconsistent with that approach. The originator of this RfI does not believe the application note should be creating a requirement.

Question: Must self-tests for verification of the integrity of the firmware and software be performed?

Resolution:

FPT_TST_EXT.1 has been defined in a generic way because implementations for self-tests are often implementation specific. Therefore the expectation on self-testing is described in the Application Note. This could be regarded as defining additional requirements in the Application Note which should be avoided in cPPs. This sort of change to the self-test requirement requires work by the full Network iTC to create an updated version of the SFR in a future version of the cPP, and is beyond the intended scope of an interpretation by the NIT. Self-testing needs therefore to be done according to the current definition of the SFR and Application Note.

Rationale:

None

Further Action:

None

Action by Network iTC:

None