Network Device Interpretation # 201902

Clarifying FPT_TUD_EXT.1 Trusted Update

Status: ☐ *Active* ☒ *Inactive*

Date: *30-Apr-2019*

End of proposed Transition Period (to be updated after TR2TD process): *30-May-2019*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

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

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

Affected Document(s): *ND SD V2.0e, ND SD V2.1*

Affected Section(s): *FPT_TUD_EXT.1, Tests section*

Superseded Interpretation(s): *None*

Issue:

FPT_TUD_EXT.1 Trusted Update Test 3:

"2) The evaluator uses a legitimate update and tries to perform verification of the hash value without storing the published hash value on the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE.

…

If the verification of the hash value over the update file(s) against the published hash is not performed by the TOE, Test 3 shall be skipped."

If the TOE implements a way to calculate a hash of provided update file, but relies on the administrator to decide if update is legitimate (i.e. SF will not prevent installation of any update file provided by the administrator but is capable of assisting in running hash comparison) can "If the verification of the hash value over the update file(s) against the published hash is not performed by the TOE” be claimed and Test 3 skipped?

Additionally, Test 3 part 2 is unclear and/or presumes specific implementation. Please clarify what does it mean “without storing” in “perform verification of the hash value without storing the published hash value on the TOE” and why should it result in update failing?

Resolution:

The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).

For FPT_TUD_EXT.1 Test 2 the test shall be marked conditional and the condition shall be clarified.
Therefore
<old> “Test 2 (if digital signatures are used)”</old>
Shall be replaced by
<new>”Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).”</new>

For FPT_TUD_EXT.1 Test 3 the test shall be marked conditional and the condition shall be clarified.
Therefore
<old> “Test 3 (if published hash is verified on the TOE):”</old>
Shall be replaced by
<new>”Test 3 [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outsidesuch that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted).”</new>

Note, that the scenario described in the issue section where the TOE provides capabilities to calculate the hash over an image but the decision about the authorization for the installation of the update is dependent on the authorization by the administrator is not regarded as a scenario where the TOE itself verifies the hash value.

For FPT_TUD_EXT.1 Test 3 part 2 the first sentence should be modified to enhance clarity.
Therefore
<old>“*The evaluator uses a legitimate update and tries to perform verification of the hash value without storing the published hash value on the TOE.*”</old>
Shall be replaced by
<new>”*The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE.” </new>*

The change of wording in Test 3 part 2 has been made to remove the confusion over “storing” the hash. The objective of Test 3 part 2 is to cover the scenario where the TOE is expected to perform the hash comparison by itself but the reference value is missing.

Rationale:

See Resolution section.

Further Action:

None

Action by Network iTC:

None