Network Device Interpretation # 201836

FCS_SSHS_EXT.1.5 SFR and AA discrepancy

Status: ☒ *Active* □ *Inactive*

Date: *18-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *18-Apr-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): *NDcPP V2.0e, NDcPP V2.1, FWcPP V2.0e, ND SD V2.0e, ND SD V2.1*

Affected Section(s): *FCS_SSHS_EXT.1.5, Test 2*

Superseded Interpretation(s): *None*

Issue:

The SFR is written as:

"The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256] and [selection: ecdsa-sha2- nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, no other public key algorithms] as its public key algorithm(s) and rejects all other public key algorithms."

And Test 2 is written as:

"Test 2: The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize the public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails."

The SFR puts its focus on the SSH server public key algorithms (the host key) however Test 2 puts its focus on using an invalid key pair from the SSH client that the TOE will reject. The CCTL believes that in the context of the SFR, this test is miswritten and should be rewritten to confirm that the TOE (SSH server) only supports the public key algorithms listed in the SFR as its host key algorithm.

Also, the note in FCS_SSHS_EXT.1.2 states 'Public key authentication is tested as part of testing for FCS_SSHS_EXT.1.5'. However this does not appear to be true as FCS_SSHS_EXT.1.5 Test 1 is written in the context of the SSH server. The CCTL believe that the SSHS SFRs should be rewritten to separate requirements specifying which public key algorithms are accepted as SSH server host key algorithms and which are accepted SSH client public key algorithms accepted by the server (TOE). Further, the assurance activities should be updated to reflect this.

Resolution:

The NIT partially disagrees with the issue described in the Issue section. The test should be kept as-is. The following test objective definition shall be added to the definition of Test 2 for FCS_SSHS_EXT.1.5 to enhance clarity:

<new> *Test objective: The purpose of this negative test is to verify that the server rejects authentication attempts of clients that present a public key that does not match public key(s) associated by the TOE with the identity of the client (i.e. the public keys are unknown to the server). To demonstrate correct functionality it is sufficient to determine that an SSH connection was not established after using a valid username and an unknown key of supported type.* </new>

Rationale:

The added sentence clarifies the intention of the test.

Further Action:

FCS_SSHS_EXT.1.5 Test 2 should be considered to be moved to tests for FCS_SSHS_EXT.1.2 in future versions of the SD.

Action by Network iTC:

None.