Network Device Interpretation # 201613

Negative testing for additional ciphers for SSH

Status: ☒ *Active* □ *Inactive*

Date: *8-Aug-2016*

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

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

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

Affected Section(s): FCS_SSHC_EXT.1.4, FCS_SSHS_EXT.1.4

Superseded Interpretation(s): *None*

Issue:

Most FCS_SSH of the protocol testing is positive testing, with the exception of 3des and diffie-hellman-group1. For symmetric ciphers, the tester verifies that the claimed ciphers can be negotiated and that 3des cannot; however, there are many other ciphers (e.g. RC4, blowfish) that could be supported. Should any other negative testing be performed? Since supporting other algorithms, does not violate any testing requirements, how should a lab handle knowledge or discovery of other algorithms?

Resolution:

The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish a SSH connection. To verify this, the evaluator shall start session establishment for a SSH connection with a remote server (for FCS_SSHC_EXT.1.4) or from remote client (for FCS_SSHS_EXT.1.4), respectively (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.

Rationale:

None

Further Action:

None

Action by Network iTC:

Update test definition in ND SD for FCS_SSHC_EXT.1.4 and FCS_SSHS_EXT.1.4 accordingly.