Network Device Interpretation # 201713

TLS and DTLS Server Tests - Applying RfI#201643 to NDcPPv2

Status: ☒ *Active* ☐ *Inactive*

Date: *25-Jul-2017*

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

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

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

Affected Section(s): *FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2*

Superseded Interpretation(s): *None*

Issue:

RfI#201643b, Issue2 and RfI#201643c, Issue3 were related to ND SD V1.0. A resolution needs to be defined to apply the results also for ND SD V2.0. Note that for ND SD V2.0 the issue applies not only to TLSS, but also to DTLSS.

RfI#201643b, Issue2: TD0040 identified changes in [MDM] FCS_TLSS_EXT.1.1 Test 3. It appears that the test requirements for [ND] FCS_TLSS_EXT.1.1 Test 3 and [ND] FCS_TLSS_EXT.2.1 Test 3 should be replaced with the text from TD0040 for the reasons provided in TD0040.

„Test 3: The evaluator shall use a client to send a key exchange message in the TLS connection that the does not match the server-selected ciphersuite (for example, send an ECDHE key exchange while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite or send a RSA key exchange while using one of the ECDSA ciphersuites.) The evaluator shall verify that the TOE disconnects after the receiving the key exchange message."

RfI#201643c, Issue3: TD0040 also identifies changes for [MDM] FCS_TLSS_EXT.1.1 Test 4 bullet 5. This corresponds to [ND] FCS_TLSS_EXT.1.1 Test 4e and [ND] FCS_TLSS_EXT.2.1 Test 4e. This change should not be carried forward, since bullet 5/test 4e does not duplicate bullet 4/test 4d. Bullet 4/Test 4d requires specifies sending a Finished message before the ChangeCipherSpec (and not sending a ChangeCipherSpec message. Bullet 5/Test 4e specifies sending a ChangeCipherSpec message, but sending a garbled message instead of a finished message.

„Test 4: The evaluator shall perform the following modifications to the traffic:

...
e) Send a garbled message from the client after the client has issued the ChangeCipherSpec message and verify that the Server denies the connection."

Resolutions:

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).

The NIT acknowledges the issue described in the 'Issue' section above for Issue2. After careful consideration, the NIT came to the conclusion that Test 3 as defined in the Issue section is not suitable to detect the intended flaw. Even a flawed TOE that would not detect the mismatch in ciphersuites would disconnect due to a decryption error and therefore would pass the test. Since the NIT could not identify additional value of this test regarding security the NIT decided that FCS_DTLSS_EXT.1.1 Test 3, FCS_DTLSS_EXT.2.1 Test 3, FCS_TLSS_EXT.1.1 Test 3 and FCS_TLSS_EXT.2.1 Test 3 shall be dropped.

The NIT acknowledges also the issue described in the 'Issue' section above for Issue 3. FCS_DTLSS_EXT.1.1 Test 4e, FCS_DTLSS_EXT.2.1 Test 4e, FCS_TLSS_EXT.1.1 Test 4e and FCS_TLSS_EXT.2.1 Test 4e shall therefore be modified as follows:

"Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to:

a) Correctly encrypt (D)TLS Finished message

b) Encrypt every (D)TLS message after session keys are negotiated

Test 4 e): The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent.

The evaluator shall verify that the Finished message (handshake type hexadecimal 16) is sent immediately after the server's ChangeCipherSpec (handshake type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal, 16 03 03 00 40 14 00 00 0c...), where '14' is the hexidecimal message type code in the verify_data header and '00 00 0c' is the verify_data field length. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'."

This resolution has been developed with support of the Network iTC's TLS Working Group.

Rationale:

As stated in the 'Resolution' section.

Further Action:

None

Action by Network iTC:

None