Network Device Interpretation # 202402b

Separation of test definitions for TLSv1.2 and v1.3 (renegotiation) (Server)

Status: ☒ *Active* ☐ *Inactive*

Date: *5-Aug-2024*

End of proposed Transition Period (to be updated after TR2TD process): *5-Sep-2024*

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): *NDSD v3.0e*

Affected Section(s): *FCS_TLSS_EXT.1.8, Test 4*

Superseded Interpretation(s): *None*

Issue:

Issue:

The test activity for TLS Servers, that reject renegotiation, are not accurate for TLS 1.2. Below are the associated SFR (FCS_TLSS_EXT.1.8) and Test (FCS_TLSS_EXT.1.8, Test 4):

The test activity for FCS_TLSS_EXT.1.8, Test 4 requires the TSF to terminate the TLS session after receiving a TLS 1.2 Client Hello renegotiation request. For TLS 1.2, the TLS Server is required only to reject the request to renegotiate the TLS 1.2 session.

Specifically, a TOE with a TLS 1.2 Server does not take an action to terminate the TLS session when the TLS 1.2 Server receives a Client Hello renegotiation request sent from the Client. The TLS 1.2 Server is expected only to ignore the request to perform renegotiation. No further action is required by the TLS 1.2 Server.

This behavior is different from TLS 1.3. When a TLS 1.3 Server receives a Client Hello renegotiation request, the TLS 1.3 Server is expected to issue a fatal alert (Unexpected Message) and terminate the TLS session. This is because in TLS 1.3 there is no support for renegotiation. Attempts to perform TLS 1.2 renegotiation within a TLS 1.3 session are forbidden. For TOEs with a TLS 1.3 Server, the test activity for FCS_TLSS_EXT.1.8 Test 4 is accurate.

Proposed resolution:

FCS_TLSS_EXT.1.8, Test 4:

Test 4a [conditional, for TLS 1.3 only]: If "reject…renegotiation attempts" is selected, the evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate the version and reject renegotiation. The evaluator shall initiate a valid initial session, send a valid ClientHello on the non-renegotiable TLS channel, and observe that the TSF terminates the session. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, for TLS 1.2 only]: If "reject…renegotiation attempts" is selected, the evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate the version and reject renegotiation. The evaluator shall initiate a valid initial session, send a valid ClientHello on the non-renegotiable TLS channel, and observe that the TSF does not perform renegotiation of the TLS channel.

Resolution:

The NIT acknowledges the issue. The following change shall be applied to the Supporting Document, Test Section for FCS_TLSS_EXT.1.8, Test 4:

{old}

Test 4 [conditional]: If "reject…renegotiation attempts" is selected, then for each selected TLS version, the evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate the version and reject renegotiation. The evaluator shall initiate a valid initial session for the specified version, send a valid ClientHello on the non-renegotiable TLS channel, and observe that the TSF terminates the session. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

{/old}

shall be replaced by

{new}

Test 4a [conditional, if the TOE supports TLS 1.3]: The evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate TLS 1.3. The evaluator shall initiate a valid initial TLS 1.3 session, send a valid client hello on the non-renegotiable TLS channel, and observe that the TSF terminates the session.

Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, if the TOE supports TLS 1.2 and rejects TLS 1.2 renegotiation attempts]: The evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate TLS 1.2 and reject renegotiation. The evaluator shall initiate a valid initial TLS 1.2 session, send a valid ClientHello on the non-renegotiable TLS channel, and observe that the TSF does not perform renegotiation of the TLS channel.

{/new}

Rationale:

see Issue section

Further Action:

None

Action by Network iTC:

None