Network Device Interpretation # 202018rev3

Session ID Usage Conflict in FCS_DTLSS_EXT.1.7

Status: ☒ *Active* ☐ *Inactive*

Date: *26-Jan-2021*

End of proposed Transition Period (to be updated after TR2TD process): *26-Feb-2021*

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 v2.2e, ND SD v2.2*

Affected Section(s): *FCS_DTLSS_EXT.1.7, Test 1*

Superseded Interpretation(s): *None*

Issue:

Test 1 of FCS_DTLSS_EXT.1.7 conflicts with IETF approved standards. For a TOE that does not support session resumption, Test 1 does not account for other uses of a SessionID that a TOE must comply with.

Specifically, step f) does not allow a client to verify the TOE implicitly rejects a SessionID by performing a full handshake independent of the SessionID contents in the ServerHello message.

SessionIDs may be used for other purposes, specifically those described in Section 11, 2nd paragraph of RFC 5415.

Proposal:

See strikethrough text below:
Test 1

f) The client verifies the TOE (1) implicitly rejects the SessionID ~~by sending a ServerHello containing a different SessionID and~~ by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.

Rationale:

If the TOE does not support session resumption and SessionIDs are used to meet IETF approved standards that include "MUST" statements, the client should not verify the SessionID content is different in step f) of Test 1.

Resolution:

The NIT does not support the proposed change to Test 1. To clarify the cPP, the following changes shall be performed.

To Application Note 73 related to FCS_DTLSS_EXT.1.7 and Application Note 111 related to FCS_TLSS_EXT.1.4 the following paragraph shall be added:

<new>
In case session establishment (i.e. generating a new session ID) and session resumption are always using a separate context (e.g. a control channel that always requires a full TLS handshake, and a data channel that supports session resumption), then it is acceptable for the ST author to claim 'no session resumption or session tickets' for the context that only establishes and never resumes. If one or more claimed contexts allow session resumption, the ST author selects 'session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)', or 'session resumption based on session tickets according to RFC 5077' (or both), depending on which methods are supported.
</new>

To the TSS requirements in ND SD v2.2 for FCS_DTLSS_EXT.1.7 and FCS_TLSS_EXT.1.4 the following paragraph shall be added:

<new>

If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.
</new>

Guidance documentation requirements shall be added to ND SD v2.2 for FCS_DTLSS_EXT.1.7 and FCS_TLSS_EXT.1.4 as follows:

<new>

FCS_DTLSS_EXT.1.7/FCS_TLSS_EXT.1.4

The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
</new>

The following paragraph shall be added to the definition of Test 1 for FCS_DTLSS_EXT.1.7 and FCS_TLSS_EXT.1.4 in ND SD v2.2:

<new>

Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may *only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.*

</new>

The following paragraph shall be added to the definition of Test 2 for FCS_DTLSS_EXT.1.7 and FCS_TLSS_EXT.1.4 in ND SD v2.2:

<new>

Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ID may be obtained in one context for resumption in another context. There is no requirement that the session ID be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ID constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.

</new>

The following paragraph shall be added to the definition of Test 3 for FCS_DTLSS_EXT.1.7 and FCS_TLSS_EXT.1.4 in ND SD v2.2:

<new>

Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ticket may be obtained in one context for resumption in another context. There is no requirement that the session ticket be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ticket constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.

</new>

Rationale:

The current definitions in NDcPP v2.2e and ND SD v2.2 imply that for session resumption there is only a single context. The paragraphs above have been added to support TOEs which are allowing multiple contexts for session resumption.

Further Action:

None

Action by Network iTC:

None