Network Device Interpretation # 202024

RFC 5077 question

Status: ☒ *Active* ☐ *Inactive*

Date: *29-Oct-2020*

End of proposed Transition Period (to be updated after TR2TD process): *29-Nov-2020*

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): *NDSDv2.2*

Affected Section(s): *FCS_TLSS_EXT.1.4, Test 3*

Superseded Interpretation(s): *None*

Issue:

Test FCS_TLSS_EXT.1.4 Test 3 inadequate/inaccurate

Summary:

The testing for part A of FCS_TLSS_EXT.1.4 Test3 can lead to a situation where the TOE correctly obeys RFC 5077 for Session Ticket Renegotiation but does not pass the tests as worded, leading to a situation similar to Schrodinger's cat.

Issue:

The test is intended to test that a TOE can correctly perform session renegotiation using Session tickets and then specifies the Record contents that are to be present for the renegotiation connection. In the test, the packets specified indicate that the TOE must issue a new session ticket during the renegotiation (not true renegotiation) or renew the current session ticket (not mandated by the RFC), due to the presence of the NewSessionTicket Record.

However, RFC 5077 also permits the Server to use an abbreviated exchange format for Renegotiation if it desires to not issue a new session ticket and continue using the presented session ticket, as described in the first paragraph after Figure 3 of 5077. The specific wording from RFC 5077 is "It is also permissible to have an exchange similar to Figure 3 using the abbreviated handshake defined in Figure 2 of RFC 4346, where the client uses the SessionTicket extension to resume the session, but the server does not wish to issue a new ticket, and therefore does not send a SessionTicket extension." [1] however this case is not covered by the test activity from ND_2.2E's supporting documents. The specific packet flow in this case would be: "

Client		***Server***
ClientHello	*-------->*	
		ServerHello
		[ChangeCipherSpec]
	<--------	*Finished*

[ChangeCipherSpec]
Finished -------->
Application Data <-------> Application Data
Fig. 2. Message flow for an abbreviated handshake " [2].

Thus we are asking if the flow described in Figure 2 of 4346, which 5077 indicates is a valid flow for session ticket renegotiation, is to be considered valid for the testing of FCS_TLSS_EXT.1.4 Test 3 or if the NIT is specifying their own obedience requirements that must be followed in order to be considered in compliance?

References:

[1] RFC 5077: Transport Layer Security (TLS) Session Resumption without Server-Side State, https://tools.ietf.org/html/rfc5077
[2] RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1, https://tools.ietf.org/html/rfc4346

Resolution:

The issue is acknowledged and FCS_TLSS_EXT.1.4 test case 3(a) shall be modified as follows:
<old>
The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with a ServerHello with an empty SessionTicket extension, NewSessionTicket, ChangeCipherSpec and Finished messages (as seen in figure 2 of RFC 5077).
</old>
shall be replaced by
<new>
The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with an abbreviated handshake described in section 3.1 of RFC 5077 and illustrated with an example in figure 2. Of particular note: if the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello in the abbreviated handshake (which is shown in figure 2). This is not required, however as further clarified in section 3.3 of RFC 5077.
</new>

Rationale:

As per section 3.3 of RFC 5077, it is not mandatory for a TLS Server to re-issue a session ticket and therefore the required message flow in the original test case was overly restrictive.

Further Action:

None

Action by Network iTC:

None