Network Device Interpretation # 202409

Correction of FCS_TLSS_EXT.1.4, Test 4

Status: ☒ *Active* □ *Inactive*

Date: *9-Sep-2024*

End of proposed Transition Period (to be updated after TR2TD process): *9-Oct-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): *cPP_ND_v3.0e-SD*

Affected Section(s): *FCS_TLSS_EXT.1.4, Test 4, FCS_DTLSS_EXT.1.7, Test 4*

Superseded Interpretation(s): *None*

Issue:

Issue:

The Test activity for NDcPP 3.0 Test Activity FCS_TLSS_EXT.1.4 Test 4 part ii cannot be completed as written. The Test activity specifies that the modified pre-shared key is to be sent as part of the ClientHello record. However, the TLS 1.3 protocol, as defined by RFC 8446, does not send the pre-shared key between the client and the server at any point in the resumption. The RFC defines two methods to perform the resumption: PSK_KE and PSK_DHE_KE. The difference boils down to using a pre-shared key with or without an ephemeral key exchange. As the NDcPP 3.0 only permits the use of a PSK in the context of an ephemeral key exchange (PSK_DHE_KE), that is what will be focused on here.

The RFC specifies that the pre-shared key is initially computed from the TLS1.3_KDF.ResumptionMasterSecret of the initial TLS sessions state. This value is then used as the input shared key for the initialization of the TLS1.3_KDF for the resumed session, and if SessionTickets are in use, this value is mixed with the nonce of the SessionTicket that was provided to the client. The client then computes a binder HMAC using the TLS1.3_KDF.Resumption_Binder as the key over a truncation of the new ClientHello for the resumed session, which is transferred in the PreSharedKey Extension binders field. The PreSharedKey Extension also contains an Identity field to specify the identity of the ticket that is being used so that the Server can use the correct nonce to initialize the TLS 1.3 KDF and correlate to the correct session.

This leads to the problem with the verbatim wording of the Test Activity, which is to "modify the pre-shared key and send it as part of a new Client Hello message." Since the pre-shared key itself is never sent from the client to the server, the CCTL cannot execute the test as written. The pre-shared key association is accomplished through the PreSharedKey extension which only contains a list of pre-shared key identities and their associated binder values. The pre-shared key identity only contains the a SessionTicket and the SessionTicketAgeAdd values from a NewSessionTicket record and omits the Nonce which is used as the input to the PreSharedKey. Given the contents of the PreSharedKey Extension, the CCTL can modify the values in three different locations;

Proposed resolutions:

1. The CCTL could modify the computed pre-shared key after correctly deriving the value but before initializing the TLS 1.3 KDF for the resuming session.
   This would cause all computations to be wrong as the TLS 1.3 KDF states would not agree on both the client and server and the binder value would be 'incorrect' as well, however the binder value would be computed in a correct manner given the inputs provided to the function.
2. The CCTL could modify the identity value of the PreSharedKey Extension Identity field.
   This would cause the TLS 1.3 KDF to be initialized correctly and the binder value to be computed 'correctly' (correct given the inputs) but the Server would not have a record of issuing a ticket by this identity and as such should reject the ticket.
3. The CCTL could modify the binder value. Option 1 would not be visible on the wire as this would only modify the local state of the TLS 1.3 KDF of the client. Options 2 and 3 would be visible on the wire as the modification would be made to a field which is transmitted between the client and the server. A server which is compliant to RFC 8446 should reject the resumption in all three change scenarios.

This would cause the TLS 1.3 KDF to be initialized correctly and the binder value computed correctly. The binder would then be modified prior to sending to the TLS Server and the binder would then fail to verify on the server.

The CCTL proposes that one or more of the above scenarios be used to demonstrate the required functionality is demonstrated rather than what is currently defined in the test. Note however that if Option 2 is chosen, there is a small chance that a session could be resumed unexpectedly because the input data to the identity value is not assured to be unique by the tests that are presently defined.

Resolution:

The NIT acknowledges the issue. The following change shall be applied to Sections 4.2.2.3 and 4.2.7.3 of the SD.

Section 4.2.2.3 FCS_DTLSS_EXT.1.7, Test 4, item ii:

{old}

The evaluator shall permit a successful DTLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then modify the pre-shared key and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake, or (2) terminates the connection in some way that prevents the flow of application data.

{/old}

{new}

The evaluator shall permit a successful DTLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then modify the session ticket (identity sent in the PreSharedKeyExtension) and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake, or (2) terminates the connection in some way that prevents the flow of application data.

{/new}

Section 4.2.7.3 FCS_TLSS_EXT.1.4, Test 4, item ii:

{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 modify the pre-shared key and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake, or (2) terminates the connection in some way that prevents the flow of application data.

{/old}

{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 modify the session ticket (identity sent in the PreSharedKeyExtension) and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake, or (2) terminates the connection in some way that prevents the flow of application data.

{/new}

Rationale:

see Issue section

Further Action:

None

Action by Network iTC:

None