Network Device Interpretation # 34

TLS Mutual authentication - inclusion of FCS_TLSC_EXT.2

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Sep-2016*

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

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

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FTP_ITC.1, FCS_TLSC_EXT.1*

Superseded Interpretation(s): *None*

Issue:

TLSC Mutual Authentication

FTP_ITC.1 includes an application note suggesting that if TLS is used to provide a trusted channel, then FCS_TLSC_EXT.2 must be used.

"If TLS is selected, the ST author will claim FCS_TLSC_EXT.2 instead of FCS_TLSC_EXT.1."

A similar note appears for FCS_TLSC_EXT.1:

"If TLS is selected as a means to provide a trusted communication channel for an external IT entity in FTP_ITC.1, then FCS_TLSC_EXT.2 is required."

There are several concerns about this SFR relationship defined in an application note.

1) This effectively demands the support for X509 mutual authentication for all of the TLS protected trusted channels. However, trusted channels based on SSH and IPsec (with Pre-shared keys) are not forced to provide X509 mutual authentication.

2) The TLS protocol requirements are only selected in FTP_ITC.1 and FTP_TRP.1. However, if TLS is selected for FTP_TRP.1, the TOE would be a TLS server, not a TLS client, so FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2 would not be included. If any inclusion of TLS in the FTP_ITC.1 requirement leads to the inclusion of FCS_TLSC_EXT.2, then when is it appropriate to use FCS_TLSC_EXT.1?

3) X509-based TLS mutual authentication is redundant to authentication built into some typical trusted services which are commonly protected as trusted channels (e.g., RADIUS, LDAP).

4) There are no tests in FCS_TLSC_EXT.2 that actually demonstrate support for mutual authentication (i.e., FCS_TLSC_EXT.2.5).

As a result, we believe that the application notes calling for the inclusion of FCS_TLSC_EXT.2 whenever TLS is selected by FTP_ITC.1 are inconsistent with the rest of the NDcPP requirements and requiring X509-based mutual authentication is not always appropriate.

We suggest the application notes NOT be enforced as a required relationship between SFRs.

Resolution:

The NIT supports the proposal. The sentence "If TLS is selected, the ST author will claim FCS_TLSC_EXT.2 instead of FCS_TLSC_EXT.1." shall be removed from the Application Note for FTP_ITC.1. The sentence "If TLS is selected as a means to provide a trusted communication channel for an external IT entity in FTP_ITC.1, then FCS_TLSC_EXT.2 is required." shall be removed from the Application Note for FCS_TLSC_EXT.1.

Rationale:

None

Further Action:

None

Action by Network iTC:

Revise Application Notes for FTP_ITC.1 and FCS_TLSC_EXT.1 accordingly.