Network Device Interpretation # 201911

Clarify authentication methods SSH clients can use to authenticate SSH servers

Status: ☒ *Active* ☐ *Inactive*

Date: *20-Aug-2019*

End of proposed Transition Period (to be updated after TR2TD process): *20-Sep-2019*

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): *ND cPP v2.1, ND SD v2.1*

Affected Section(s): *FCS_SSHC_EXT.1.9*

Superseded Interpretation(s): *None*

Issue:

Issue(#778):

In NDcPPv2.1, it appears that the intention is that server identity authentication against a local database is required, and a list of trusted certification authorities is optional. However, by using "or" before the selection, the following completion is allowed:

The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [no other methods] as described in RFC 4251 section 4.1.

Usage of "or" appears to allow no authentication (no other methods) to be implemented by TOEs. If that is not the intended requirement, should "and" be used rather than "or"?

Resolution:

The following text shall be modified in the cPP:

<old>
FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [selection: a list of trusted certification authorities, no other methods] as described in RFC 4251 section 4.1.
</old>
Replaced with:

<new>
FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [selection: a list of trusted certification authorities, no other methods] as described in RFC 4251 section 4.1.
</new>

Rationale:

See Issue section.

Further Action:

It may make sense to look at making both the local database and CA list optional. The tests should also be reviewed to ensure they are testing what we are expecting and that the "list of CA's" option is adequately tested.

Action by Network iTC:

None