Network Device Interpretation # RFI201914

Applicability of FPT_APW_EXT.1

Status: ☒ *Active* ☐ *Inactive*

Date: *14-Oct-2019*

End of proposed Transition Period (to be updated after TR2TD process): *14-Nov-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 v2.0e, FW cPP v2.0e, ND cPP v2.1*

Affected Section(s): *FPT_APW_EXT.1*

Superseded Interpretation(s): *None*

Issue:

FPT_APW_EXT.1 is titled "Protection of Administrator Passwords", but the actual requirement never limits the scope to administrative passwords. The wording of the requirement, technically, applies to all passwords (admin and non-admin alike). Similarly, Application Note 27 only talks about passwords, not administrative passwords. (The threat that this SFR is mapped to, T.PASSWORD_CRACKING, is about weak administrative passwords.)

Is the intent of FPT_APW_EXT.1 to apply to only administrative passwords? Or does it apply to all passwords?

<u>Proposal:</u>

If it only applies to administrative passwords, then maybe the SFR wording should be changed to:

FPT_APW_EXT.1.1 The TSF shall store <u>administrative</u> passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext <u>administrative</u> passwords.

If it applies to all passwords (both admin and non-admin), then maybe change the SFR title to "Protection of Passwords" and mention in the App Note that the SFR covers both admin and non-admin passwords even though the threat is regarding administrative passwords.

Resolution:

Since the Security Administrator as defined in FMT_SMR.2 is the only authorized user covered by NDcPP, the protection of passwords formally also only applies to administrative passwords.

Therefore FPT_APW_EXT.1.1 and FPT_APW_EXT.1.2 shall be modified as follows:

<old>

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

</old>

shall be replaced by

<new>

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

</new>

The Application Note for FPT_APW_EXT.1 shall be updated as follows:

<old>

The intent of the requirement is that raw password authentication data is not stored in the clear, and that no user or Administrator is able to read the plaintext password through "normal" interfaces. An all-powerful Administrator could directly read memory to capture a password but is trusted not to do so. Passwords should be obscured during entry on the local console in accordance with FIA_UAU.7.

</old>

shall be replaced by

<new>

The intent of the requirement is that raw password authentication data of Security Administrators is not stored in the clear, and that no user or Administrator is able to read the plaintext password of a Security Administrator through "normal" interfaces. An all-powerful Administrator could directly read memory to capture a password but is trusted not to do so. Passwords should be obscured during entry on the local console in accordance with FIA_UAU.7.

Although this is out-of-scope of this cPP, it is strongly advised to protect all authentication data of the device the same way and/or with similar strength as administrative passwords to reduce the risk of attacks like privilege escalation, etc.

</new>

The extended component definition for FPT_APW_EXT.1 shall be updated accordingly.

To further clarify the role of the Security Administrator the following paragraphs shall be added to the Application Note for FMT_SMR.2:

<new>

A single user associated with the Security Administrator role does not necessarily have to be able to perform all security management functions defined in FMT_SMF.1 and does not necessarily have to able to perform local and remote administration. All users associated with the Security Administrator role together need to be able to perform all security management functions defined in FMT_SMF.1 (mandatory and selected ones) and need to be able to perform local and remote administration.

This implies that a user that can perform only a single security management function defined in FMT_SMF.1 needs to be regarded as Security Administrator of the TOE.

</new>

Rationale:

See Resolution.

Further Action:

None

Action by Network iTC:

None