Network Device Interpretation # RFI201823

Reliance on external servers to meet SFRs

Status: ☒ *Active* ☐ *Inactive*

Date: *5-Feb-2019*

End of proposed Transition Period (to be updated after TR2TD process): *5-Feb-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, ND cPP v2.1*

Affected Section(s): *FPT_ITC.1*

Superseded Interpretation(s): *None*

Issue:

Background

FTP_ITC.1 allows the selection of an authentication server which implies a TOE may use an authentication server to authenticate administrators; however, the PP does not specify which SFRs may be satisfied by the authentication server.

Question

Which SFRs can be satisfied by the authentication server? What restrictions are there when satisfying SFRs using an authentication server?

Proposed Resolution

The TOE must always retain a local capability to identify and authenticate users (the number of supported accounts may be limited). All SFRs must be met for all aspects of authentication for those (locally managed) accounts.

When an authentication server is used to authenticate accounts in a manner that is independent from locally managed accounts, the following SFRs may be satisfied by the authentication server for the accounts managed by the authentication server:

FIA_AFL.1

FIA_PMG_EXT.1.1 item b.

When an authentication server authentication and local authentication functions apply or potentially apply to the same user account, the following SFR may be satisfied by the authentication server when it applies to credentials managed by the authentication server:

FIA_PMG_EXT.1.1 item b.

Example of using an authentication server in conjunction with local authentication:

SSH pubkey auth is performed on the TOE for a user while password authentication is performed by the authentication server for the same user.

Note: If an authentication server is only used for logging or determination of privileges, all FIA requirements must be satisfied by the TOE.

If this is agreeable to the TRRT/NIT, then the following is a proposed method to reflect these interpretations:

The following paragraph shall be added to SD Section 2.3.1.1 for FIA_AFL.1 TSS requirements:

For TOEs that support use of an external authentication server, the evaluator shall verify the TSS describes if an external authentication server is used to satisfy FIA_AFL.1. The evaluator shall verify the description indicates the TOE does not perform any type of authentication for the accounts being handled by the authentication server.

The following paragraph shall be added to SD Section 2.3.1.1 for FIA_AFL.1 Guidance requirements:

For TOEs that support use of an external authentication server, the evaluator shall examine guidance documentation to determine that it describes when the authentication server is used to satisfy FIA_AFL.1. The description shall include recommendations to configure the authentication server account lockout policy to be equal or more robust than the lockout requirements enforced by the TOE.

The following paragraph shall be added to SD Section 2.3.2.1 for FIA_PMG_EXT.1 Guidance requirements:

For TOEs that support use of an external authentication server, the evaluator shall examine guidance documentation to determine that it identifies the logon methods provides recommendations to configure the authentication server password policy to equal or more robust than the password requirements enforced by the TOE.

The following shall be appended to Paragraph 136, SD Section 2.3.3.1 for FIA_UIA_EXT.1 TSS requirements:

For TOEs that support use of an external authentication server, the description shall identify the logon methods and credentials that may be used with the authentication server.

Rationale

While this appears to be adding requirements, FIA_AFL.1 and FIA_PMG_EXT.1 do not indicate that they only apply to locally checked authentication attempts and passwords, so this is actually loosening requirements.

FIA_PMG_EXT.1.1 item a: This SFR must still be satisfied by the TOE, because it specifies what characters will be accepted at a password prompt in addition to specifying what character can be configured in a password.

FIA_PMG_EXT.1.1 item b: When passwords are managed by an authentication server, the TOE would only be aware of the password during the authentication step. It does not make sense for a TOE to indicate a user's password does not meet minimum length requirements during the authentication step.

FIA_AFL.1 may be satisfied by the authentication server, because the authentication failures are aggregated so they should provide an administrator with a better opportunity to detect a brute force attempt. The scenario where the legitimate user logs in on a different system thereby resetting the authentication failure counter while an attacker is brute forcing the TOE has been considered.

The following documents the research performed by the CCTL and should not be published in if a TD is issued:

Section 3.2.7 of VID guidance document (aaa local authentication attempts max-fail <x>) appears to show the configuration of FIA_AFL.1 in a manner that does not apply to authentication server managed accounts due to the inclusions of the "local" keyword.

VID and VID support authentication servers; however, available documentation did not indicate if either requirement is enforced when an authentication server is used.

Answer provided by NIAP:

The NDcPP does not allow for an Authentication Server to satisfy any FIA requirements. If the PP author allowed this, there would be appropriate application notes describing how to do it.

The TRRT may only provide an interpretation to clarify cPP Security Functional Requirements (SFRs) and Evaluation Activities (EAs) in the context of a specific product evaluation and specifically its ability to meet the cPP requirements. We may not issue a decision that adds, modifies, or deletes SFRs or EAs. A Network Interpretations Team (NIT) has been established by the iTC to address issues which may result in modifications to the cPP. Your question will be forwarded to the NIT shortly and we highly recommend your participation in the iTC to bring this to closure.

Resolution:

The NIT agrees with NIAP's answer: "The NDcPP does not allow for an Authentication Server to satisfy any FIA requirements."

The TOE shall be capable of independently implementing all TSF, including FIA requirements, without relying on external IT entities. For example, the TOE is expected to be able to maintain the system clock without having to synchronize it with an external NTP server. This way, if the external NTP server becomes unavailable, the TOE can still maintain time. Another example: the TOE is expected to be able to maintain a local user database, allowing local administrators to log in without reliance on external authentication components. This way, if an external authentication server becomes unavailable, the TOE can still be accessed by local administrators.

This does not preclude secure integration with an external IT server to duplicate some of the existing TSF functionality. The TOE may optionally integrate with an external authentication server that in turn enforces its own distinct password complexity and authentication failure lockout policies. In such cases, there is no expectation that the TOE would impose or enforce its own policies on external IT entities.

Rationale:

A TOE must meet all the applicable SFRs in the cPP.

Further Action:

None

Action by Network iTC:

None