Network Device Interpretation # RFI201829

Applicability of FIA_AFL.1 to key-based SSH authentication

Status: ☒ *Active* □ *Inactive*

Date: *6-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *6-Mar-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, ND SD v2.0e, ND SD v2.1*

Affected Section(s): *FIA_AFL.1 (NDcPP), section 2.3.1.3 (ND SD)*

Superseded Interpretation(s): *None*

Issue:

The testing assurance activity for FIA_AFL.1 in the CPP_ND_V2.0E SD (SD section 2.3.1.3, paragraph 133, pg. 32) requires: "The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application)."

The TOE provides HTTPS/SSH password-based authentications and SSH Key-based authentication. The CCTL has verified that TOE HTTPS/SSH password-based authentications are blocked after a defined number of unsuccessful attempts (for a defined period of time or until the device is rebooted as required by the FIA_AFL.1.2), but the SSH key-based authentication will always be available and it is not blocked by unsuccessful attempts.

The TSS and AGD states that: "SSH key-based authentication is a more secure authentication mechanism and it will not be disabled/blocked by unsuccessful authentication attempts."

Discussion:

The CCTL believes the public key-based authentication mechanism does not have to be disabled/blocked by unsuccessful authentication attempts and the TOE meets FIA_AFL.1.2 due to the following considerations:

- *Section 6.5 Identification and Authentication (FIA), of the CPP_ND_V2.0E clearly and unambiguously limited the scope of the SRFs to password-based authentication mechanism only.*

- *Section 4.1.4.2 of the CPP_ND_V2.0E maps FIA_AFL.1 to only the T.PASSWORD_CRACKING threat, which addresses the threat from an agent that may be able "… to take advantage of weak administrative passwords to gain privileged access to the device …" and all SFR rationale mentions the password (no other mechanisms are discussed). Specifically, for FIA_AFL.1, the PP states that: "Actions on reaching a threshold number of consecutive password failures are specified in FIA_AFL.1".*
- *Public keys are much safer than password authentication, as keys are much longer than a password (a typical key is 4096 bits, or 512 bytes/characters) and almost impossible to guess. It can take millions of years for a supercomputer to brute force the key-based authentication (https://withblue.ink/2016/07/15/stop-ssh-brute-force-attempts.html).*
- *The TSS and AGD clearly state that "SSH key-based authentication is a more secure authentication mechanism and cannot be disabled/blocked by unsuccessful authentication attempts".*

The CCTL is asking for guidance on whether the TOE should be tested for blocking the key-based authentication after a defined number of unsuccessful authentication attempts, or if the current statement in the ST and AGD is acceptable given the requirement as it is outlined in the CPP_ND_V2.0E

Resolution:

The NIT agrees that blocking due to authentication failures is intended to be applied to password-based authentication rather than key-based authentication.

Note that the TD for RfI#201818, related to how FIA_AFL.1 applies to local vs. remote administrator accounts, adds text to FIA_AFL.1.1 (and to the Application Note below FIA_AFL.1 – Application Note 16 in NDcPPv2.0e/17 in NDcPPv2.1) that clarifies that the element applies to password-based authentication.

This TD therefore confirms the interpretation that application of FIA_AFL.1 is only mandatory for password-based authentication, but no additional change is needed beyond that applied by RfI#201818.

Rationale:

As noted in the introductory text in section 6.5 of v2.1 of the cPP, the FIA SFRs in that section (including FIA_AFL.1) are aimed at protecting password-based logon mechanisms (the selection in FIA_UAU_EXT.2 acknowledges the potential existence of other authentication mechanisms). In particular FIA_AFL.1 helps protect where brute-forcing is considered a feasible attack: subject to appropriate key sizes, this is not the case for key-authentication based on asymmetric keys and therefore is not necessary to support key-based SSH authentication.

Further Action:

None

Action by Network iTC:

None