Network Device Interpretation # 201721

Making password-based authentication optional in FCS_SSHS_EXT.1.2

Status: ☒ *Active* ☐ *Inactive*

Date: *20-Mar-2018*

End of proposed Transition Period (to be updated after TR2TD process): *11-May-2018*

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): *NDcPP V2.0, FWcPP V2.0, ND SD V2.0*

Affected Section(s): *FCS_SSHS_EXT.1.2*

Superseded Interpretation(s): *None*

Issue:

A vendor has a network device that is managed using a TL-1 (https://en.wikipedia.org/wiki/Transaction_Language_1) interface. While this interface can be invoked manually by an administrator to enter human-interpretable CLI commands, it is more common for it to be invoked by a remote machine using some sort of application as an intermediary. In this situation, a management workstation has a graphical application that accepts administrator inputs, converts them to the TL-1 commands that execute the desired functions, and transmit them to the network device over a trusted channel over SSH. Because the trusted channel is a machine-to-machine connection, the SSH protocol is authenticated using public key only. This does not technically conform to RFC 4252 because SSH password-based authentication is not supported by the protocol, but this is the industry standard application of TL-1 over SSH because it is primarily used for machine-to-machine communications. The device still requires username/password authentication for administrators but it is performed at the application layer after SSH communications are established. The logic for this is the same as TD200, except on the server side; i.e., it is acceptable for SSH connections to use public key authentication only if it is a machine-to-machine connection, regardless of whether the client side or the server side of the connection is being looked at.

This is considered to be consistent with "Case 2" in section 3.1 of the NDcPP - the management application is expected to be a non-TOE component that resides in the operational environment as a user-friendly method to perform configuration activities remotely, similar to how an administrator could use a web browser on their workstation to manage a network device over a remote HTTPS interface. The boundary of the certification would only include the device itself.

Based on the summary information below, is this an acceptable TOE boundary/operational environment under the NDcPP 2.0?

1. The TOE is still defined as a single hardware network appliance; no 'distributed TOE' use cases apply.

2. The administrative interface to the TSF is through a non-TOE application that resides on an administrator workstation (similar to a web browser).

3. The trusted path from a remote administrator to the TSF is an SSH connection that uses public-key authentication at the session layer since the client end of the connection is a software application and not an interactive SSH terminal (the TSF still provides username/password authentication but it is at the application layer and is performed only after the SSH channel is established).

Resolution:

The NIT acknowledges the issue described in the 'Issue' section. It shall be noted, that the NIT neither approves nor rejects specific TOE implementations or TOE Operational Environments. Therefore this resolution does not address the summary statements included in the Issue, which are considered to be matters specific to the context of an individual evaluation.

In NDcPP and FWcPP the following changes shall be applied

FCS_SSHS_EXT.1.2 shall be modified as follows:

*"***FCS_SSHS_EXT.1.2** The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: *password-based, no other method*]."

The following application note shall be added to FCS_SSHS_EXT.1.2:

"If the TOE supports password-based authentication, the option 'password-based' shall be selected. If the TOE supports only public key-based authentication, the option 'no other method' shall be chosen."

In ND SD the following changes to the evaluation activities for FCS_SSHS_EXT.1.2 shall be applied

The TSS section shall be replaced as follows:

<old>"The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and ensure that password-based authentication methods are also allowed."</old>

shall be replaced by

<new>"The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHS_EXT.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described."</new>

The Test section for FCS_SSHS_EXT.1.2 shall be replaced as follows:

<old>"Test 1: Using the guidance documentation, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.

Test 2: The evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.

Note: Public key authentication is tested as part of testing for FCS_SSHS_EXT.1.5"</old>

shall be replaced by

<new>"Test 1: If password-based authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that user authentication succeeds when the correct password is provided by the user.

Test 2: If password-based authentication methods have been selected in the ST then the evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.

Note: Public key authentication is tested as part of testing for FCS_SSHS_EXT.1.5"
</new>

Rationale:

From a security perspective, a TOE does not necessarily need to support password-based authentication.

It shall be noted, that the NIT does neither approve nor reject specific TOE implementations or TOE Operational Environments. It is expected, though, that all TSF (e.g. user authentication) are implemented by the TOE itself but not the TOE environment and that properly protected paths and channels are used where critical security parameters like user passwords are transmitted between the TOE and other endpoints.

Background: Public key-based authentication has been (originally) specified as mandatory requirement in FCS_SSHS_EXT.1.2 in compliance with RFC4252, chap.5.

Further Action:

None.

Action by Network iTC:

None.