Network Device Interpretation # 201717

Testing both thresholds for SSH rekey

Status: ☒ *Active* ☐ *Inactive*

Date: *13-Nov-2017*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *ND SD V.1.0, ND SD V2.0*

Affected Section(s): *FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8*

Superseded Interpretation(s): *Partially supersedes RfI#201624rev2 (ND SD, TSS and Tests sections)*

Issue:

Background

FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.8 *The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.*

Application Note 168

This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold, the total incoming and outgoing data needs to be counted. The rekey applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic.

It is acceptable for a TOE to implement lower thresholds than the maximum values defined in the SFR.

For any configurable threshold related to this requirement the guidance documentation needs to specify how the threshold can be configured. The allowed values must either be specified in the guidance documentation and must be lower or equal to the thresholds specified in this SFR or the TOE must not accept values beyond the thresholds specified in this SFR.

Issue

Some network devices have limited data transfer speeds over SSH imposed by hardware limitations, (such as for example CPU clock speed) and may not be capable to transmit one gigabyte of data over SSH in less than one hour. If both thresholds are not configurable (meaning that for those devices the time threshold cannot be set to more than 1 hour, and the transmitted data threshold cannot be set to less than 1 gigabyte), then for those devices the transmitted data threshold will never be able to initiate rekeying because time threshold will always be reached first.

It is possible for such a device to implement the required rekey thresholds of one hour for time and one gigabyte of transmitted data and meet the requirement. However, testing the traffic-based threshold as specified in paragraph #451 of the ND Supporting Document v2 ("The evaluator shall test both, the time-based threshold and the traffic-based threshold") would be impossible on such devices since the time threshold will be crossed and trigger a rekey before the data threshold can be crossed.

Proposed Resolution

Provide clarification in the "Tests" section of FCS_SSHS_EXT.1.8 in the SD stating that when both thresholds are not configurable, and the device cannot transmit one gigabyte of data in less than one hour, testing the traffic threshold is not applicable.

Resolutions:

The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).

The NIT acknowledges the issue described in the 'Issue' section above but confirms that the intention of FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 SFRs is to ensure that the TOE implements both thresholds. The NIT also acknowledges that it is possible that hardware limitation may prevent reaching data transfer threshold in less than one hour. In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:

a. *An argument is present in the TSS section describing this hardware-based limitation and*
b. *All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.*

The iTC recommends to place an additional limitation on the validity of certification, where any hardware change of the components identified in the argument will invalidate certification. This limitation should be clearly identified as part of certified product listing.

Rationale:

As stated in the 'Resolution' section above, the NIT confirms that the intention of FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 is that both thresholds are implemented and tested. But in particular case when the threshold cannot be met due to hardware limitations, it is reasonable that testing could be omitted for

this threshold. It is not expected that a check is implemented for a threshold that cannot be reached by the TOE.

Further Action:

None

Action by Network iTC:

None