Network Device Interpretation # RFI201839

Granularity of audit events

Status: ☒ *Active* ☐ *Inactive*

Date: *8-May-2019*

End of proposed Transition Period (to be updated after TR2TD process): *8-Jun-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): *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Superseded Interpretation(s): *None*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:

When auditing "reason for failure" in cryptographic protocols and X.509 validation, how granular must the reason be? Can generic messages be used as long as suitable guidance is given in the AGD to help administrators trouble-shoot the connection?

When auditing "reason for failure" in X.509 validation, are the only specific reasons that need to be logged the 3 listed under application note 49? Can the remainder of reasons (eg. Expiry, revocation) continue to be generic?

When attempting to validate the product is actually failing on the appropriate error condition for ATE_IND, is it permissible to rely on (non-public) debugging logs or similar?

Resolution:

The NIT agrees that the current text shall be updated to enhance clarity about the described issue. Therefore the following paragraphs shall be added as a general description to the evaluation activities for FAU_GEN.1 in ND SD.

<new> The main reasons for collecting audit information are to detect and identify error conditions, security violations, etc. on the one hand and to provide sufficient information to the Security Administrator to resolve the issue on the other hand. The audit information to be collected according to FAU_GEN.1 and the failure conditions identified in tables 2, 4 and 5 need to enable the Security Administrator at least to detect and identify the problem and provide at least basic information to

resolve the issue. And for this level of detail also the other FAU requirements apply – in particular the need for local and remote storage of audit information according to FAU_STG_EXT.1.

The level of detail that needs to be provided to the Security Administrator to actually resolve an issue usually depends on the complexity of the underlying use case. It is expected that a product provides additional levels of auditing to support resolution of error conditions, security violations, etc. beyond the level required by FAU_GEN.1 but it should also be clear that a high level of granularity cannot be maintained on most systems by default due to the high number of audit events that would be generated in such a configuration. It is expected that the TOE will be capable of auditing sufficient information to meet the requirements of FAU_GEN.1. This may include audits that are generated only when configured if the TOE configuration can be modified without taking the TOE out of production.

The issue described above explicitly refers to the use of X.509 certificates. In case a certificate-based authentication fails, an error message telling the Security Administrator that 'something is wrong with the certificate' shall not be considered as sufficient information about the 'reason for failure' as a basic information to resolve the issue. The log message shall inform the Security Administrator at least about the type of error (Example types of error would be: 'Trust issue' with the certificate, e.g. due to failed path validation; use of an 'expired certificate'; absence of basicConstraints extension; CA flag not set for a certificate presented as a CA; signature validation failure for any certificate in the certificate path; failure to establish revocation status; revoked certificate). The NIT recommends for audit information related to the use of X.509 certificates that it uniquely identifies the certificate that couldn't be successfully verified. For example, identification of a certificate could include Key Subject and Key ID, where key subject is an identifier contained in the CN or SAN and where Key ID is a certificate's serial number and issuer name or subject key identifier (SKI) and authority key identifier (AKI).

In general when using open source libraries like OpenSSL, passing on error messages from such libraries to the user is regarded as good practice.</new>

Rationale:

See issue section. The level of detail that needs to be provided to enable the Security Administrator to fix issues based on the information in audit events usually depends on the complexity of the underlying use case. In simple scenarios with only one underlying root cause a single error message might be sufficient whereas in more complex scenarios the granularity of error messages should be higher. The NIT is of the opinion, though, that specifying dedicated levels of granularity for every audit event specified for FAU_GEN.1 would become overly complex and bears a high risk of specifying requirements which are not implementation independent. Therefore the NIT only specified a general guidance on the subject.

To validate the product is actually failing on the appropriate error condition for ATE_IND it is acceptable to use audit information that requires additional configuration if the TOE configuration can be modified for this without taking the TOE out of production.

Further Action:

For future versions of NDcPP and ND SD it should be considered to mandate that for audit events related to the verification of X.509 certificates for building a trusted path or trusted channel it must be clear

(either from the log message or from deduction using the information in that message) what connection and what certificate were involved in the failed verification (unique identification).

Action by Network iTC:

None