Network Device Interpretation # 28

Applicability of X.509 certificate testing to IPsec

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Jun-2016*

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

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

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FIA_X509_EXT.1.1*

Superseded Interpretation(s): *None*

Issue:

The FIA_X509_EXT.1.1 tests e, f, and g require modification of certificates presented to the TOE, and demonstration that the certificates fail to validate. While these tests are possible for TLS, HTTPS, and code signing, in IPsec/IKE, the certificates are exchanged within the encrypted IKE_SA/Phase1_SA. Thus, it's not possible for a MITM to change/corrupt the certificates presented to the TOE, and the lab thinks that these tests do not apply to IPsec/IKE.

Rationale regarding trying to smash IKEv1 certificates on the wire: IKEv1 Main Mode completes the Phase 1 key exchange before authentication occurs (and thus the peer certificates exchanged are encrypted by the Phase 1 SA). See RFC 2409 section 5.1 (shows the shows the Key Exchange completing before the first certificate is sent) and 7.1 (https://tools.ietf.org/html/rfc2409#section-7.1, which states that after the second exchange that "the shared keys, SKEYID_e and SKEYID_a, are now used to protect and authenticate all further communication). The PP explicitly prohibits aggressive mode, so we weren't considering it.

The lab thinks that these tests do not apply to IPsec/IKE, do you agree?

Resolution:

The X.509 certificate testing should be performed for all functionality using X.509 certificates, including IPsec. MITM is not practical for modification of the certificates used in IPsec/IKE, instead the X.509 tests should use instrumented clients or servers, presenting modified certificates, to perform the tests.

Rationale:

The X.509 requirements are about ensuring the behavior of the TOE when encountering malformed or invalid X.509 certificates regardless of protocol.

Further Action:

None

Action by Network iTC:

None