End to End Data Protection with Encryption - Negotiation

David Kwak; dkwak@marvell.com
Ali Khwaja; akhwaja@marvell.com
Craig W. Carlson; cwcarlson@marvell.com

T11-2021-00087-v002

Intro

- Previous presentation (T11-2021-00021-v000) introduced proposed feature of End-to-end data protection for Encryption
- For that proposal, no feature negotiation proposal was given
- The goal of this proposal is to define negotiation of the End-to-end data protection for Encryption feature based on exisiting methods used in FC-P-2
- During June T11 meeting we decided use some of the Vendor Unique space

Encryption negotiation background

- Any encryption used is negotiated by the IKE_SA_INIT message defined in clause 6 of FC-SP-2
  - This allows the message initiator to propose a set of transforms (e.g., encryption algorithms)
  - The message responder can then respond with what is acceptable
- This process allows multiple transforms, with possible varying attributes, to be proposed

Negotiation

- Negotiation for End-to-end Encryption CRC
  - Should NOT require a bit in the FLOGI
    - These bits are becoming scarce
  - Should be tied to security negotiation via the IKE_SA

- Proposal
  - Define an FC range out of the Transform_ID’s

Proposal – Transform_ID range

- Define a range out of the Vendor Specific values for FC unique items
  - Pick range of 1024 to 2048
  - Pick value of 1046 ENCR_AES_GCM with End-to-end encryption protection
  - Pick value of 1047 ENCR_AES_AUTH_AES_GMAC with End-to-end encryption protection

Table 75 – Encryption Algorithms Transform_IDs (Transform Type 1)

Transform_ID[a]	Encryption Algorithm	Reference
3	ENCR_3DES	RFC 2451
11	ENCR_NULL	RFC 2410
12	ENCR_AES_CBC	RFC 3602
13	ENCR_AES_CTR	RFC 3686
20[b]	ENCR_AES_GCM[c] (with a 16 bytes ICV)	RFC 4106[d]
21[e]	ENCR_NULL_AUTH_AES_GMAC[c]	RFC 4543[d]
1 024 .. 65 535	Vendor Specific	
all others	Reserved to IANA	

[a] These values are a subset of those specified by IANA in the "IKEv2 Parameters" registry (see http://www.iana.org/assignments/ikev2-parameters).

[b] ENCR_AES_GCM with a 8 or 12 bytes ICV shall not be used.

[c] ENCR_AES_GCM and ENCR_NULL_AUTH_AES_GMAC may be used with a 128 bit key, a 192 bit key or a 256 bit key. If ENCR_AES_GCM or ENCR_NULL_AUTH_AES_GMAC is implemented, support for the 128 bit key is mandatory, support for the 192 bit and 256 bit key is optional. The key size is specified by using the Key Length Transform Attribute (see 6.3.2.5).

[d] This standard requires a variation in the content of the Additional Authentication Data (AAD) field from that specified in the RFC. The AAD field specified by the RFC shall be prefixed by the modified Fibre Channel Frame_Header (see FC-FS-3) to construct the AAD field required by this standard.

[e] ENCR_NULL_AUTH_AES_GMAC is used only for authentication, but is documented as an encryption algorithm so that it can use an initialization value.

Proposal - Continued

- ”Vendor Specific” field to be changed as shown

Transform_ID	Encryption Algorithm	Reference
…		
1024 .. 2047	FC Specific	
1046	ENCR_AES_GCM with End-to-end encryption protection	
1047	ENCR_AES_AUTH_AES_GMAC with End-to-end encryption protection	
2048 .. 65535	Vendor Specific	
…		

MARVELL

Thank You

Essential technology, done right™