Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH

draft-mcgrew-ipsec-me-esp-ah-reqts-00

mcgrew@cisco.com
wajdi.k.feghali@intel.com

Motivations

- ESP & AH algorithms last updated 1/07
  - If updated in 2013, should last until 2019
  - Should give best current recommendation for efficient, secure, and supported algorithms
- Usage guidance lacking
  - Should discourage ESP without authentication
  - Should discourage AH wrapped in ESP

Description of Problems with RFC4835

- No AES-GCM and AES-GMAC
  - Efficient
    - Kounavis, Kang, Grewal, Eszenyi, Gueron, Durham, *Encrypting the Internet*, SIGCOMM 2010
    - Optimized Galois Counter Mode, Intel, 2011
  - Support
    - Law, Solinas, *Suite B Cryptographic Suites for IPsec* [RFC6379]

Description of Problems with RFC4835

- Does not discourage use of Triple DES
  - 64-bit block ciphers inappropriate for protecting large amounts of data
  - Collision attacks leak data
    - ~ 1 bit after 8 Gigabytes have been encrypted
    - ~ 1.8 x 10^6 bits after 10,800 Gigabytes encrypted (1 Gigabit/second for one day)
- AES is more efficient, more secure

Description of Problems with RFC4835

- AES-XCBC-MAC-96 is a SHOULD+
  - But it is not widely implemented or used
  - Incompatible with AES-CMAC [RFC4493][800-38B]

Description of Problems with RFC4835

- AES-CTR is a SHOULD
  - Not as good as AES-GCM
    - Inadvertent lack of authentication with AES-CTR problematic
  - Not widely used

Description of Problems with RFC4835

- HMAC-MD5 not deprecated
  - MD5 discouraged [RFC6151]
  - HMAC-SHA1 better, and widely supported
  - AES-GMAC better

Summary - Requirements

	Old Requirement	**New Requirement**
AES-GCM [RFC4106]	MAY	SHOULD+
AES-GMAC [RFC4543]	MAY	SHOULD+
Triple DES-CBC [RFC2451]	MUST-	SHOULD NOT
AES-XCBC-MAC-96 [RFC3566]	SHOULD+	SHOULD
AES-CTR [RFC3686]	SHOULD	MAY
HMAC-MD5-96 [RFC2403]	MAY	SHOULD NOT

Summary – Usage Guidance

- Both confidentiality and authentication SHOULD be provided. If confidentiality is not needed, then authentication MAY be provided. Confidentiality without authentication is not effective [DP07] and SHOULD NOT be used. We describe each of these cases in more detail below.

- To provide confidentiality and authentication, an authenticated encryption transform SHOULD be used in ESP, in conjunction with NULL authentication. Alternatively, an ESP encryption transform and ESP authentication transform MAY be used together (provided that neither transform is NULL). If authentication on the IP header is needed in conjunction with confidentiality of higher-layer data, then AH SHOULD be used in addition to the transforms recommended above. It is NOT RECOMMENDED to use ESP with NULL authentication in conjunction with AH; some configurations of this combination of services have been shown to be insecure [PD10].

- To provide authentication without confidentiality, an authentication transform MUST be used in either ESP or AH. It is not possible to provide effective confidentiality without authentication, because the lack of authentication undermines the efficacy of encryption [B96][V02]. An encryption transform MUST NOT be used with a NULL authentication transform (unless the encryption transform is a authenticated encryption transform).