TCP-AO Crypto Goo

IETF74

Monday, March 23, 2009

Gregory M. Lebovitz
Juniper
gregory.ietf@gmail.com

Intellectual Property

- No IPR on this document about which I’m aware.

Current Requirements

Requirement	Authentication Algorithm
MUST -	HMAC-SHA-1-96 [RFC2404]
SHOULD +	AES-128-CMAC-96 [RFC4493]
Requirement	Key Derivation Function (KDF)
MUST -	KDF_HMAC_SHA1
SHOULD +	KDF_AES_128_CMAC

Key Derivation Function

Derived_Key =

KDF(Master_Key, Input, Output_Length)

Master_Key -	PSK in manual key mode
Input	See next slide

KDF’s “Input”

(i || Label || 0x00 || Context || Output_Length)

- i: A counter,
- Label: ASCII string "TCP-AO“ (FIPS140 conformance)
-
- 0x00: Eight zero bits, or 0 represented in byte form
- Context : Conn_Block
- Output_Length: in bits, of the key that the KDF will produce.

KDF_HMAC_SHA1

- PRF: HMAC-SHA1 [RFC2404]
- Input:
  - i: "0“ [ASCII “0” (0x30) or a NUL (0x00)?]
  - Label: "TCP-AO“
  - Context: Conn_Block
  - Output_Length 160
  - Result: Conn_Key

KDF_AES_128_CMAC

- PRF: AES-CMAC-PRF-128 [RFC4615]
- Input:
  - i: "0“ [ASCII “0” (0x30) or a NUL (0x00)?]
  - Label: "TCP-AO“
  - Context: Conn_Block
  - Output_Length 128

- And … (see next slide)

Make sure you get a 128bit input to AES-128

- Input: MK (variable len Master_Key)
- Output: TK (128 bit output of the KDF, Traffic_Key)

- Step 1: K:=AES-CMAC(0^128, MK, MKlen);
- Step 2: TK := AES-CMAC(K, I, len);

  - Done only once at very beginning of connection, then used for all keys gen'd for that connection.

Issues
ID#1 – Reqs

- SHOULD +, MUST – bad idea. Use:
  - HMAC-SHA1 in both MUST
  - AES-128-CMAC in both cases SHOULD
- WG: Decide and move on.

Issues
ID#2 – Labels, Ditch them?

- Pro:
  - Be forward looking. Will be needed once we get to using a KMP (down the road) and PSK, vs PKI and new KDF’s get defined as time goes on.
- Con:
  - We only have manual keying and 2 KDF’s now. Don’t introduce complexity until it’s absolutely needed.

Others

- 3.1 Clarify Output length stuff with text provide.
- Clean up text explaining KDF_AES_128_CMAC
- Change Conn_key to Traffic_Key throughout

Wrap Up

- Accept as WG document?
- More review from crypto community

GOAL

Get reviews	May 1
WG Rev-00	May 15
Go to WG LC	June 1

Advertisement: KMART Roadmap

draft-lebovitz-kmart-roadmap-01

(http://tools.ietf.org/html/draft-lebovitz-kmart-roadmap-01)

- Goal: Improve security of routing protocol transports by beefing up authentication/integrity
- How:
  - Step 1 - Improve existing manual key mechanisms for “modern” practice
  - Step 2 – Add automatic key management protocol to make operations easier
- Where: kmart@ietf.org

Feedback?