TCP-AO Crypto Goo

draft-lebovitz-ietf-tcpm-tcp-ao-crypto-02

IETF75

Monday, July 27, 2009

Gregory M. Lebovitz
Juniper
gregory.iertf@gmail.com
No IPR on this document about which I’m aware.
# Current Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Authentication Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUST</td>
<td>HMAC-SHA-1-96 [RFC2404]</td>
</tr>
<tr>
<td>MUST</td>
<td>AES-128-CMAC-96 [RFC4493]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Key Derivation Function (KDF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MUST</td>
<td>KDF_HMAC_SHA1</td>
</tr>
<tr>
<td>MUST</td>
<td>KDF_AES_128_CMAC</td>
</tr>
</tbody>
</table>
Key Derivation Function

\[
\text{Derived\_Key} = \text{KDF(Master\_Key, Input, Output\_Length)}
\]

- Master\_Key - PSK in manual key mode
- Input - See next slide
KDF’s “Input”

( i || Label || Context || Output_Length)

- i: A counter,
- Label: ASCII string "TCP-AO" (FIPS140 conformance)
- DROPPED – “0x00” – it’s a field maker; not needed here since Label is fixed length. So dropped it.
- Context: Data_Block
- Output_Length: in bits, of the key that the KDF will produce.
KDF_HMAC_SHA1

- PRF: HMAC-SHA1 [RFC2404]
- Input:
  - i: "0"
  - Label: "TCP-AO"
  - Context: Data_Block
  - Output_Length 160
- Result: Traffic_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: Data_Block
  - Output_Length 128

- And … (see next slide)
Make sure you get a 128bit key to use in AES-128

- **Given:** MK (variable len shared secret string)
  - **Output:** K (128 bit output of the KDF, the Key, then used as key in Step 2)

- **Step 1:** $K := \text{AES-CMAC}(0^{128}, \text{MK}, \text{MKlen})$;
- **Step 2:** $TK := \text{AES-CMAC}(K, \text{Input}, \text{len})$;

- Step 1 is done only once at very beginning of connection, then used for all TK’s gen’d for that connection.
What’s new in -02 (from -00)

- 3.1 Clarified Output length stuff
- Cleaned up text explaining KDF_AES_128_CMAC
- On Key Extractor for AES-128-CMAC, changed from 0^128 as key to a fixed constant string
- Removed the “labels section”. Replaced with “tips for UI’s” 3.1.3
- In the input block, dropped “0x00” and explained why it’s not needed, per NIST 800…
- Cleaned up wording to match auth-opt-05, i.e. TSAD -> MKT, Conn_Block -> Data_Block, conn_key -> traffic_key, etc.
- added the text on how to deal with future KDF to end of s3.1 (EKR)
- Editorial stuff
Changes For -03

- Change to -00 as a wg document
- Ensure w/ Joe Touch that text from crypto-03 sect xx aligns with auth-opt-05 sec 7.
Wrap Up

GOALS

- Get 4 reviews        Aug 5
- WG Rev-00            Aug 7
- Go to WG LC          Aug 10
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

See proceedings from Rtg Area Open Mtg today
Feedback?