Security Descriptions Extension for Media Streams

(draft-zhou-mmusic-sdes-keymod-00)

S. Zhou， T. Tian， Z. Xie

IETF 83-mmusic ， 2012-3

- Content of draft
  - An extension to cryptographic attribute included in SDP Security Description (RFC 4568)

- Motivation:
  - In forking and re-targeting scenarios, offerer sends outgoing keying material to the ultimate answerer, as well as intermediate users/devices
  - An UPDATE/Re-INVITE can send a new keying material to the ultimate answerer → an extra round trip messages

- Defined in 3GPP TR 33.829 V0.0.9 (2011-12)
  - 9.3.1.3 SDES solution 2

- a new session parameter extension "keymod"

  srtp-session-extension = keymod

  keymod = "keymod:" <keymod-info>

  keymod-info = <keymod-type> "|"<kdf-func>"|"<keymod- val>

  keymod-type = "rand"/"rand-salt"/keymod-type-ext

  keymod-type-ext = 1*(VCHAR)

  kdf-func = 1*(ALPHA / DIGIT / "_")

  keymod-val =*(base64);base64 encoded binary string

- Keymod→contained in answer, indicate the answerer is asking for the offerer to refresh its keying material using the information following it.
- rand→ only master key is requested to refresh according to kdf-func and keymod-val.
- Rand-salt→ master key is required to refresh according to kdf-func and part of keymod-val, and master salt is required to be replaced by part of keymod-val .
- kdf-func
  - “is”→ replacement
  - "xor“→XOR between older master key and keymod-val

- Examples
- Empty keymod in offer message

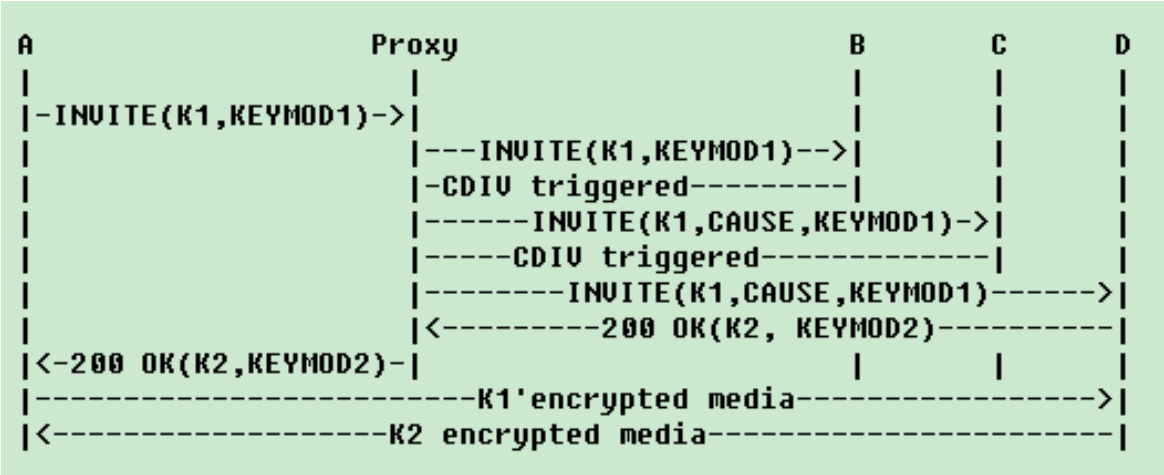
  a=crypto:1 AES_CM_128_HMAC_SHA1_80
  inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
  keymod:rand|xor|

- master key of offered required change(XORed), master salt unchanged

  a=crypto:1 AES_CM_128_HMAC_SHA1_32
  inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32;
  keymod:rand|xor|WVNfX19zZW1jdGwgKCkgew==

- Master key and master salt both required to change(replacement)

  a=crypto:1 AES_CM_128_HMAC_SHA1_32
  inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32;
  keymod:rand-salt|WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz



←Re-targeting scenario

Forking scenario →