draft-ietf-mmusic-kmgmt-ext-07.txt

Elisabetta.Carrara@era.ericsson.se

Changes

- From .05 to .07
- prtcl-id name is case-sensitive attribute (recommended: lower case)
- More detailed description of interaction SDP - key mngmt module
- Re-keying
  - Same protocol as in the original INVITE
  - Specified behavior if re-INVITE fails ("606 Not Acceptable“ with Warning headers, and abort the security setup).
- IANA Considerations updated

Bidding-down attack (1)

- Opened by the possibility of offering multiple key management protocols
- In .05, was left to policy (*use protocols of similar strength*)
- Solution in .07
  - The list of identifiers of ALL the proposed key management protocols MUST be authenticated (from offerer to responder).
  - Such authentication is done by each key management.
- Requirement: each key management protocol MUST specify how the protocol identifier list is authenticated

Bidding-down attack (2) Example

v=0
o=alice 2891092738 2891092738 IN IP4 lost.downunder.dom
s=Secret discussion
t=0 0
c=IN IP4 lost.downunder.dom
a=key-mgmt:mikey <data1>
a=key-mgmt:keyp1 <data2>
a=key-mgmt:keyp2 <data3>
m=audio 39000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 42000 RTP/SAVP 31
a=rtpmap:31 H261/90000

The protocol list, "mikey;keyp1;keyp2", is generated from the SDP description and input to each key management protocol (together with the data for that protocol).

Bidding-down attack (3)
How it is solved in MIKEY

- [MIKEY: <draft-ietf-msec-mikey-06.txt>, MSEC WG]
- protocol id: “mikey”
- the list of the key management protocols is placed in a *General Extension Payload* (of type "SDP IDs")
- Such payload will be automatically integrity protected/signed by MIKEY.