SDP Security Descriptions for Media Streams

Mark Baugher

Cisco Systems

Overview

- SDP key management approaches
  - Problems with k=
  - The keymgt-extensions approach
  - Textual SDP security descriptions approach
- Security descriptions
  - Key parameters & Session parameters
- Use with Offer/Answer
- Conclusion: Future MMUSIC work item?

Security descriptions complements the keymgt-extensions for environments where SDP message is secure (e.g. SSL, IPsec).

SDP Encryption Keys (k=)

```
v=0
o=mbaugher 12 12 IN IP4 12.224.88.17
s=SDP Descriptions for SRTP
i=Talk about using SDP for SRTP keys
u=http://people.cisco.com/mbaugher
e=mbaugher@cisco.com (Mark Baugher)
c=IN IP4 224.2.17.12/127/3
t=2873397496 2873404696
m=audio 49170 RTP/SAVP 0
m=video 51372 RTP/SAVP 31
k=(base64)NzB4d1BINUAvLEw6UzF3WSJ+P
m=application 32416 udp/ipsec-esp wb
k=h!)8gAe>=?#fQzo4jeI.:](:-)97kV
a=orient:portrait
```

- At session or media level

k=<method>

k=<method><encryption key>

- Method can be
  - clear
  - base64
  - uri
  - Prompt
- We can extend the method
- But this is not enough…

We would like to use a mechanism such as k= for establishing keys and sessions in cases where the SDP channel is secure.

Issues with SDP k=

- A cryptographic key has descriptors…
  - Parameters describing the key
  - Parameters describing the crypto session
- ..and structure
  - SRTP master salt and master key
- …session and media-level semantics

k= can be extended with a *method* but no provision is made for descriptors and complicated session and media-level semantics.

2 Approaches to SDP Keying

- Key mgt extensions
  - Supports AKE
  - Uses encrypted blob
    - New key-mgt stmt
    - Conveys a key mgt protocol message
  - Provides end-to-end security
  - As secure as the key management protocol
- Security descriptions
  - No AKE
  - Textual SRTP parms
    - Extends k= statement
    - SDP secured with SSL, IPsec, …
  - May not provide end-to-end security
  - As secure as the data security protocol

SDP Security Descriptions

a=crypto: key_parameters session_parameters

- 4 key_parameters
  - transport=SDP-transport (e.g. *RTP/SAVP*)
  - format=descriptor (e.g. dynamic payload type)
  - crypto_suite=value (e.g. SRTP crypto suites)
  - mkey=(method)value (much like k= description)
- session_parameters are specific to the security service (e.g. SRTP session parms)

An SRTP Example

```
v=0
o=jdoe 2890844526 2890842807 IN IP4 10.47.16.5
s=SDP Seminar i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 224.2.17.12/127 t=2873397496 2873404696
a=recvonly m=video 51372 RTP/SAVP 31
a=crypto: transport=RTP/SAVP
  crypto_suite=AES_CM_128_HMAC_SHA1_80
  mkey=(srtp)/16/14/d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj/20/1:32
m=audio 49170 RTP/SAVP 0
a=crypto: transport=RTP/SAVP
  mkey=(srtp)/16/14/NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj/20/1:32
m=application 32416 udp wb
a=orient:portrait
```

Generic and Specific Descriptions

Generic

- crypto attribute and its parameters
  - transport
  - format
  - crypto_suite
  - mkey(method)

Specific

- crypto_suite is specific to security protocol
- mkey & method are specific to security protocol

SRTP-Specific Descriptions

- crypto_suite values
  - AES_CM_128_HMAC_SHA1_32
  - F8_128_HMAC_SHA1_32
  - AES_CM_128_HMAC_SHA1_80
  - NULL
- mkey for SRTP
  - Method MAY be *URI* or *SRTP*

`key_length/salt_length/base64(key || salt)/lifetime/MKI:length`

- session parameters
  - ROC=n
  - ENCRYPTED_SRTCP
  - UNENCRYPTED_SRTP
  - FEC_ORDER=(FEC_SRTP, SRTP_FEC, SPLIT)

Why Use Crypto Suites?

- Functional dependencies among parameters, e.g.
  - Encryption algorithm and authentication algorithm
  - Authentication tag length and key size
- Too many parameters are overwhelming, hard to understand

Use With Offer/Answer

- We “get it for free”
  - By virtue of codec selection
  - But it is verbose and complex
- Can improve upon this at session level
  - Session-level *crypto*
  - Multiple are offered
  - Answerer selects one

```
v=0
o=carol 28908764872 28908764872
  IN IP4 100.3.6.6
s=-
t=0 0
c=IN IP4 192.0.2.4
a=crypto: transport=RTP/SAVP
  format=1 format=2 format=3
  mkey=(srtp)/16/14/d...m/20/1:32
a=crypto: transport=RTP/SAVP
  format=1format=2 format=3
  crypto_suite=
        aes_cm_128_hmac_sha1_80
  mkey=(srtp)/16/14...n/20/1:32
m=audio 0 RTP/SAVP 0 1 3
a=rtpmap:0 PCMU/8000
a=rtpmap:1 1016/8000
a=rtpmap:3 GSM/8000
```

Recommendation

- Make SDP Security Descriptions an MMUSIC work item
- Develop public-domain implementation
- Allow for technical community comment
- Allow Security Descriptions to proceed independently of keymgt draft