SDP Security Descriptions for Media Streams

<draft-ietf-mmusic-sdescriptions-00.txt>

Mark Baugher
Dan Wing
- Cisco Systems -

Overview

- Brief overview of Session Description Protocol
- Rationale & Requirements
  - End-to-end vs Hop-by-hop uses
  - Comparison with existing and nascent standards
- Security descriptions
  - Session descriptors vs. media descriptors
  - Syntax
- Next steps

This is an mmusic work item that we want evaluated in both transport and security areas.

Session Description Protocol

```
v=0
o=mhandley 2890844526 2890842807
   IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session
   description protocol
u=http://www.cs.ucl.ac.uk/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

- Describes multimedia sessions
- Uses textual descriptions
- Two “parts”
  - Session-level description
  - Media-entry level description

SDP Session-level descriptions

```
v=0
o=mhandley 2890844526 2890842807
   IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session
   description protocol
u=http://www.cs.ucl.ac.uk/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

- Apply to all media entries
  - Version (v)
  - Origin (o)
  - Session name (s)
  - URI content (u)
  - Contact info (e) (p)
  - Session times (t)
- Apply to session or media levels
  - Connection (c)
  - Bandwidth (b)
  - Attribute (a)
  - Keys (k)
  - And others…

SDP Media Entries

```
v=0
o=mhandley 2890844526 2890842807
   IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session
   description protocol
u=http://www.cs.ucl.ac.uk/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

- Session level starts at v= and ends at m=
- Media level begins at first m=
- Each m= starts a new media entry

m=<media>
<port>
<transport>
<fmt list>

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
k=(base64)vg&T+)xG7@fb5j/,jaA}\|p0%*
m=audio 49170 RTP/SAVP 0
m=video 51372 RTP/SAVP 31
m=application 32416 udp/ipsec-esp wb
k=(base64)gAe>=?#fQzo4jeI.:](:-)97kV
a=orient:portrait
```

- At session or media level

k=<method>

k=<method><encryption key>

- Method can be
  - clear
  - base64
  - uri
  - Prompt
- Not suitable for SRTP
  - SRTP key is unique
- Probably for others, too

Rationale for this Work

1. Overcomes limitations of k=
   - Enables SRTP, TLS,… signaling in SDP
2. Leverages “existing” infrastructure
   - SDP used to signal media sessions
   - TLS or IPsec offers signaling protection
   - Absence of a global PKI

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

Comparison with SDP k= Line

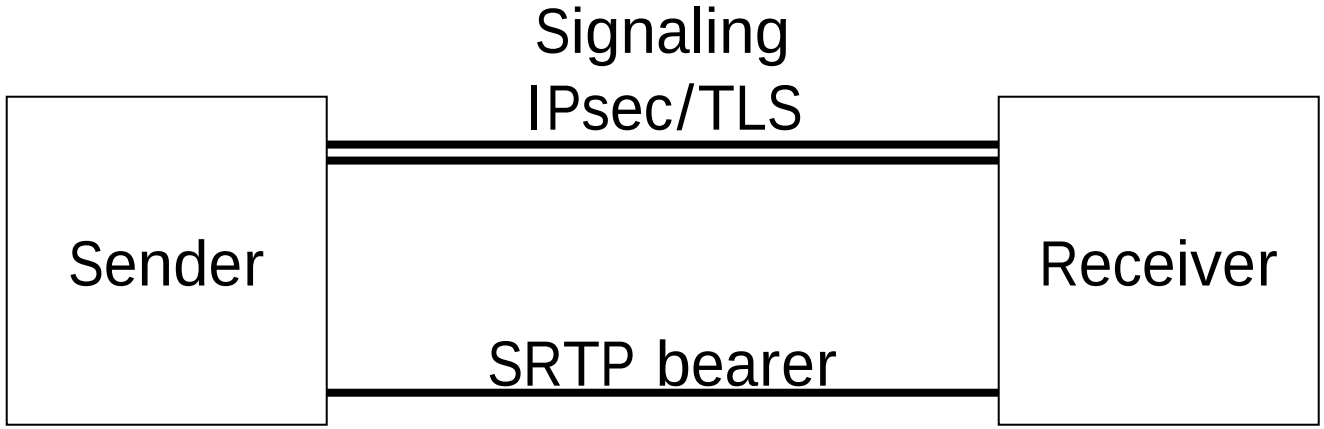
A cryptographic key

1. Has descriptors…
   - Parameters describing the key
   - Parameters describing the crypto session
2. And structure
   - SRTP master salt and master key
3. And session or media-level parameters

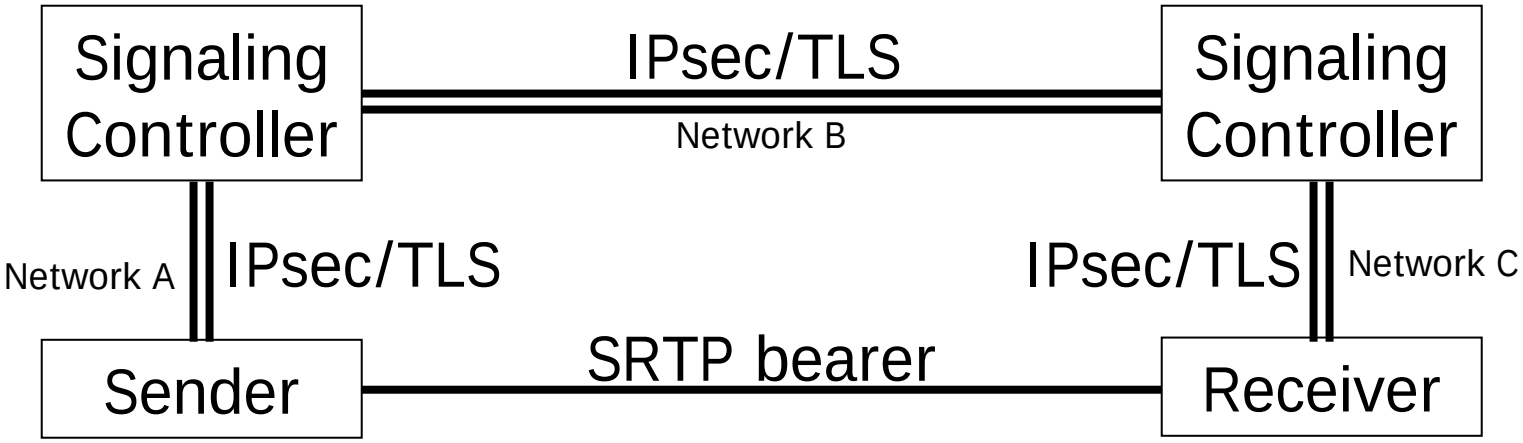
k= defines only structure, not parameters

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

SDP Signaling:
Secure End-End Channel



SDP Signaling: Hop-by-Hop Channels



SDP message (e.g. SIP/SDP) travels multiple hops
e.g. networks a, b, and c encrypted/authenticated
Not end-end, security as good as weakest link
MMUSIC key-mgt approach does not suffer from this

Comparison with key-mgt Line

- 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
  - Additional latency
- Security descriptions
  - No AKE
  - Textual SDP parms
    - Extends k= statement
    - SDP secured with TLS, IPsec, …
  - May not provide end-to-end security
  - As secure as hop-by-hop data security protocol
  - No additional latency

Transport-Specific vs. Generic

- K= & key-mgt are transport-generic
- Sdescriptions seeks to be as generic
  - A framework for security transports
  - Parameters are generic to the transports
  - Parameter values are transport specific
- But do not operate at SDP session level
  - Complicated interactions with transport-session parameters

SDP Security Descriptions

a=crypto:<crypto-suite> <application> <key> [<session>]

An SDP attribute with 4 parameters

- *Crypto-suite*=value (e.g. SRTP: AES-CTR-HMAC-SHA1-80)
- *application*=sub-protocol (e.g. SRTP or SRTCP)
- *Key* has two incarnations

  uri: absolute-uri

  inline: transport-specific-key-descriptor
- *Session* is transport-specific session parameters (e.g. SRTP: unencrypted srtp, FEC order, etc.)

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:AES_CM_128_HMAC_SHA1_80 both
    inline:16/14/d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj/2^20/1:32
m=audio 49170 RTP/SAVP 0
a=crypto:AES_CM_128_HMAC_SHA1_32 srtp
    inline:16/14/NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj/2^20/1:32
a=crypto:AES_CM_128_HMAC_SHA1_80 srtcp
    inline:16/14/eZkBkQythOTg3NjU0MSEzMDMyMT01NDg5N2RlRkF/2^20/1:32
m=application 32416 udp wb
a=orient:portrait
```

Next Steps

- Fix known errors
  - SDP direction attribute ambiguities
- Add missing pieces
  - Generalize Offer/Answer
  - Generalize to transports beyond RTP/SAVP
- Get implementation experience
- Report back to next mmusic meeting