Diffie-Hellman Exchanges for Multimedia Sessions

Mark Baugher

David McGrew

Overview

- draft-baugher-mmusic-sdp-dh-00
- Improves SDP Security Descriptions
  - Adds perfect forward secrecy to keys
  - Describes keys with public information
  - Establish keys without encryption
- Defines SDP use of NIST 800-56
- Should we do this work in MMUSIC?

SDP Security Descriptions

- An SDP media-level attribute
  - Organized into Offers and Answers
- Describes SRTP parameters and keys
  - Relies on signaling-channel authorizations
  - Uses signaling-channel protections
- Carries a media-session key inline
  - NOT a key management protocol
  - Uses a secured channel and its key management

a=crypto Media Attribute

```
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 161.44.17.12/127
t=2873397496 2873404696
m=video 51372 RTP/SAVP 31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
   inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
m=audio 49170 RTP/SAVP 0
a=crypto:1 AES_CM_128_HMAC_SHA1_32
   inline:NzB4d1BINUAvLEw6UzF3WSJ+PSdFcGdUJShpX1Zj|2^20|1:32
m=application 32416 udp wb
a=orient:portrait
```

Sdesc Rationale and Issues

- Fixes two problems with SDP k=
  - Describing the attrributes of the key
  - Describes attributes of the secure media session
- Easy to parameterize a data security protocol when the signaling is protected
- Problematic when signaling is not well protected or the protection level is not known
- Lacks an important option of perfect forward secrecy for cryptographic keys

The Diffie-Hellman Attribute

- A session-level SDP attribute
- Separate from but usable by media-level security signaling such as sdesc, ISMAcryp
- Adds perfect forward secrecy for media keys
- Replaces secret keying information with public information for DH-capable devices

a=DH Session Attribute

```
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 161.44.17.12/127
t=2873397496 2873404696
a=DH: STAT_ECDH_GROUP_19
 dhkey: 2tC2U5QiHPmwUeH+yleH0Jjf5jf8kLnvlF0MN3JYEYA=
        UnGgRhzbglLWHxxFb6PlmrH0WzOsz19YOJ4Fd7iZC7M=
m=video 51372 RTP/SAVP 31
a=crypto:1 AES_CM_128_HMAC_SHA1_80
 nonce:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAwJSoj|2^20|1:32
```

Specification

- Based entirely on NIST 800-56

  Recommendation for Pair-Wise Key Establishment using Discrete Logarithm Cryptography
- Supports static and ephemeral keys
- Supports ECC and FFC
  - IKE Group 2, IKE Group 19, IKE Group 14
- Enables fingerprint authentication or can use SIP Identity authorization

Conclusion

No panacea for SIP key establishment

- Doesn’t solve the “early media” problem
- Usefulness to any future solution is TBD

- Applicable to other SDP applications
  - Brings PFS to sdesc keys
  - Useful for pre-encryption applications
- Reduces potential vulnerabilities of sending plaintext keys