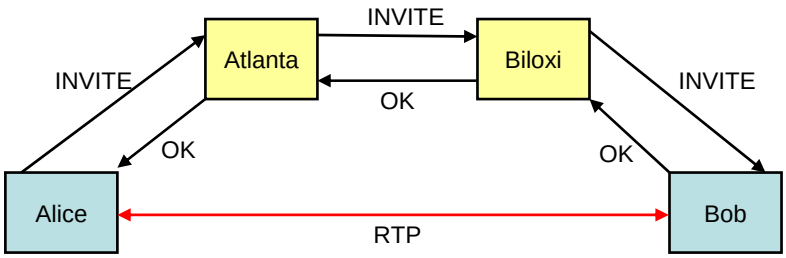
Overview of SIP Media Security Options

Dan Wing
dwing@cisco.com
March 21, 2006 -- IETF 65

1

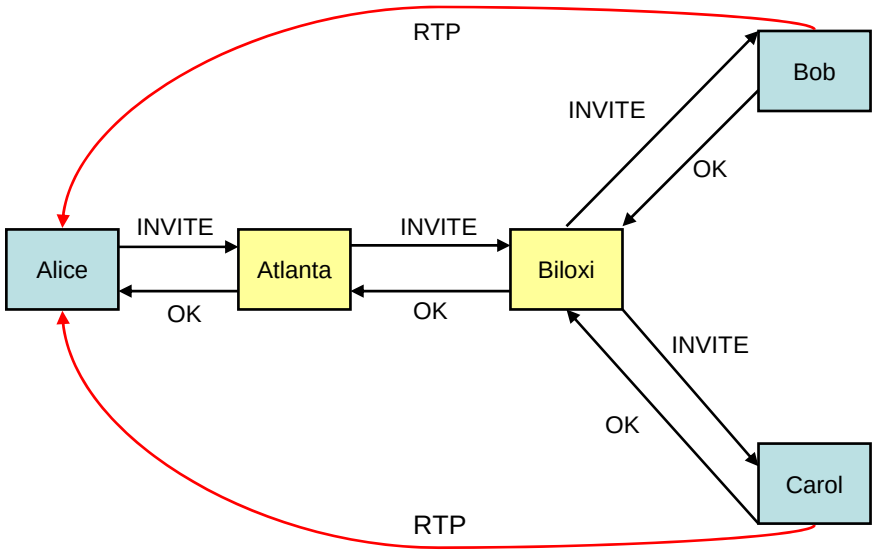
Reminder: Basic Topology



- SIP and RTP follow different paths
  - SIP: Signaling path
  - RTP: Media path
- Media path is often faster (fewer hops)

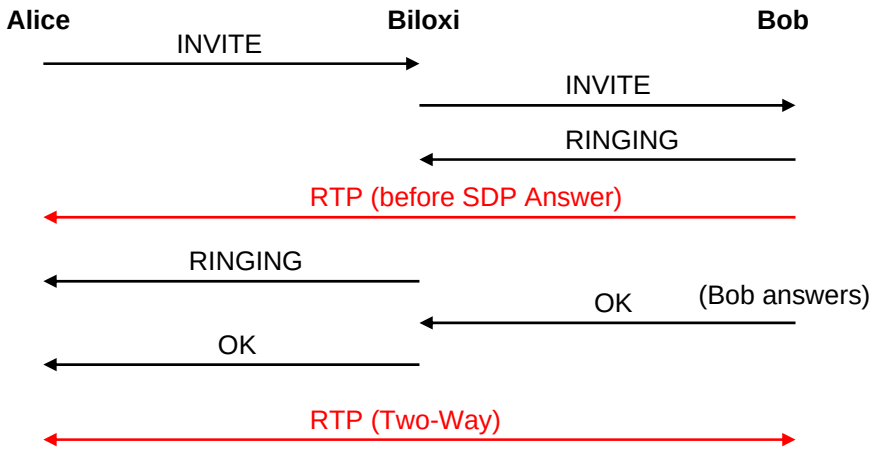
2

Forking



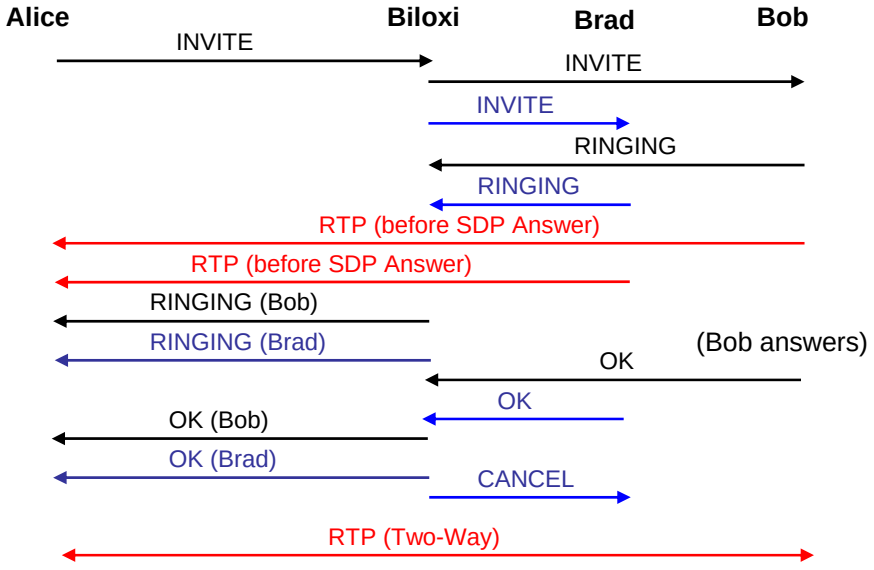
3

Media Before SDP Answer ("Clipping")



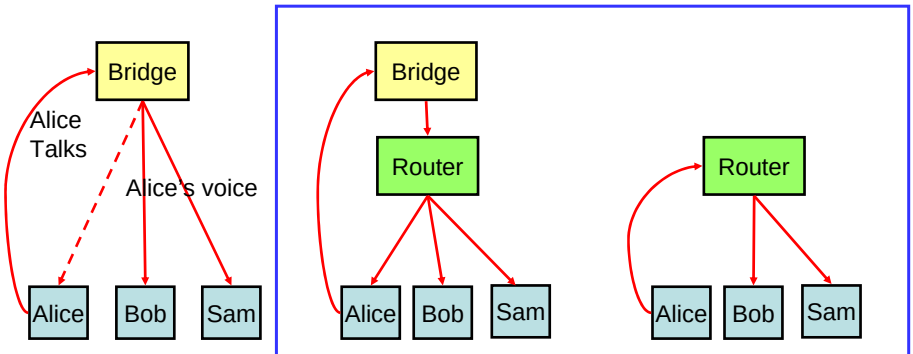
4

Forking with Media Before SDP Answer



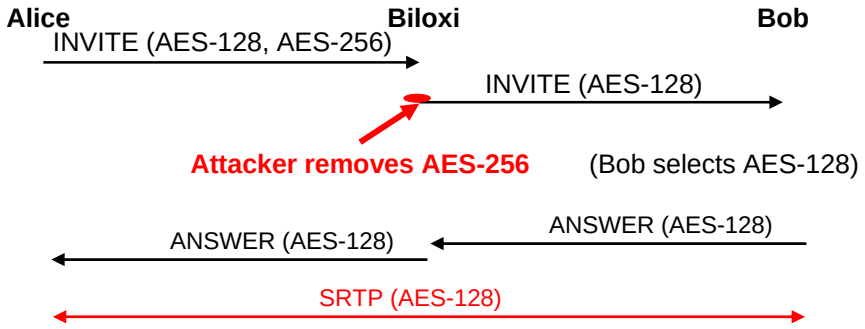
5

Conferencing Architectures



6

Bid-Down Attack



- Bid down SRTP encryption level
- Bid down to RTP (mult/alt, SDP grouping)

7

Secure RTP

- Channel security is well understood
  - Techniques documented in RFC3711
- Problem is association management
  - Key establishment
  - Peer authentication
  - Algorithm selection
- This means some kind of handshake

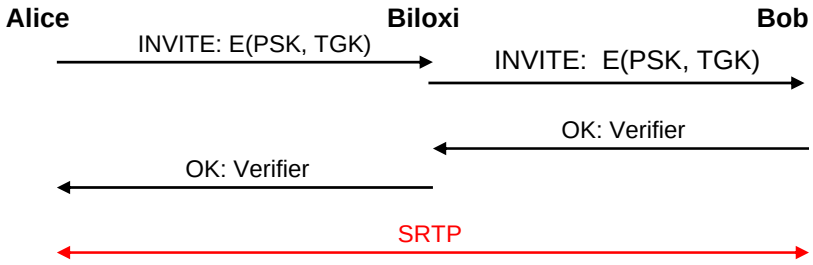
8

Overall design choices

- Handshake in signaling channel
  - MIKEY, Security Descriptions
  - Already written up and implemented
  - Problems with forking and media-before-SDP-answer
- Handshake in media channel
  - ZRTP, EKT, RTP/DTLS
  - Internet Drafts only
  - Work well with forking and media-before-SDP-answer

9

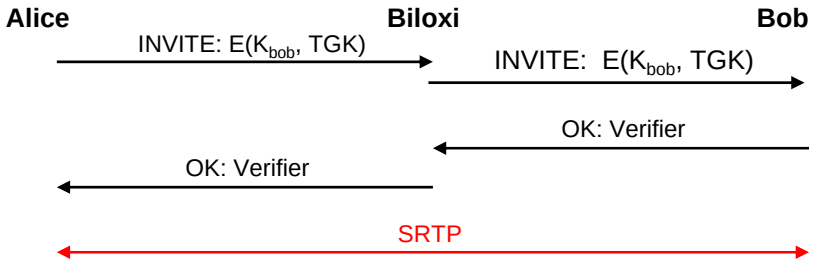
MIKEY Pre-Shared Key Mode (3830)



Requires signalling confidentiality	No
Forking	No
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	No (but pre shared key)
Rekeying	Yes
Downgrade attack protection	Yes

10

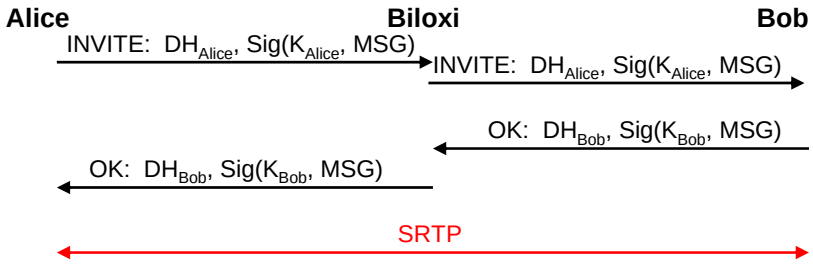
MIKEY Public Key Mode (3830)



Requires signalling confidentiality	No
Forking	No
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

11

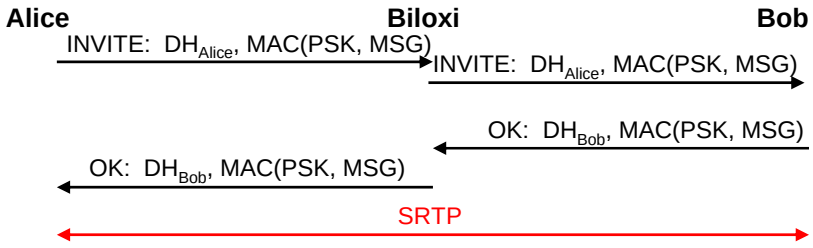
MIKEY Diffie-Hellman Mode (3830)



Requires signalling confidentiality	No
Forking	No
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

12

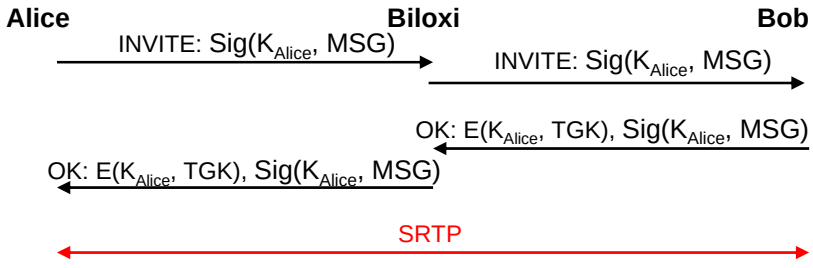
MIKEY Diffie-Hellman HMAC Mode (draft-ietf-msec-mikey-dhhmac-11)



Requires signalling confidentiality	No
Forking	No
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	No (pre-shared key)
Rekeying	Yes
Downgrade attack protection	Yes

13

MIKEY RSA-R Mode (draft-ietf-msec-mikey-rsa-r-02)

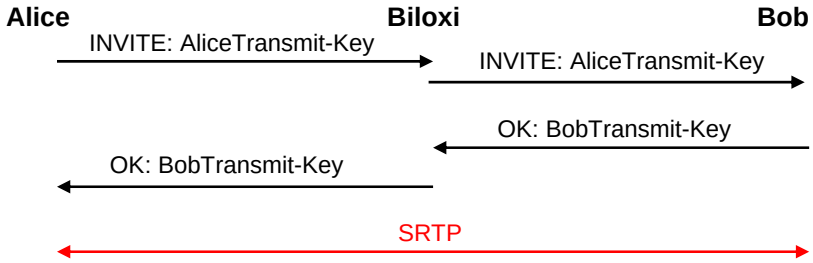


Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	No
Shared-key conferencing	Yes
Requires PKI	Yes
Rekeying	Yes
Downgrade attack protection	Yes

14

SDESCRIPTIONS (draft-ietf-mmusic-sdescriptions-12)

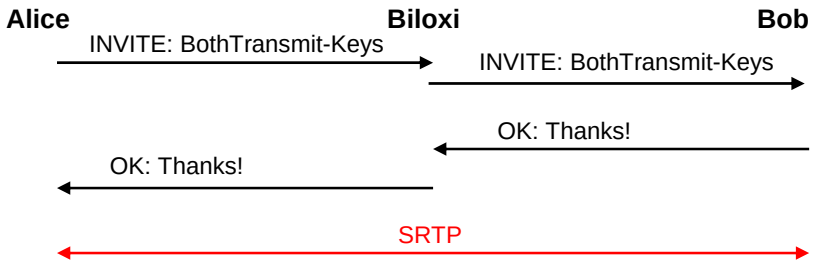
dwing5



Requires signalling confidentiality	Yes
Forking	Yes (insecure)
Media before SDP answer	No
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes (New Offer)
Downgrade attack protection	No

15

SDES Early Media Mode (draft-wing-mmusic-sdes-early-media-00)

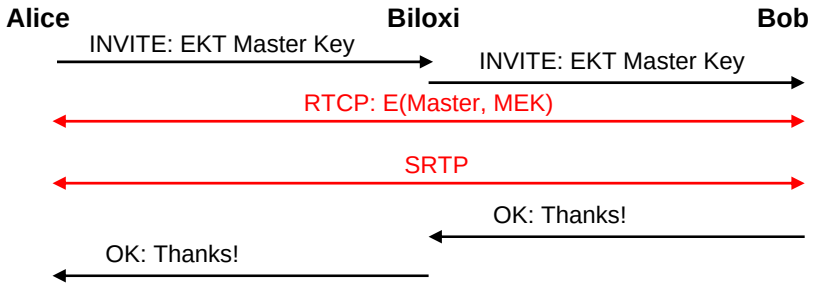


Requires signalling confidentiality	Yes
Forking	Yes (insecure)
Media before SDP answer	Yes
Shared-key conferencing	Yes
Requires PKI	No
Rekeying	Yes (New Offer)
Downgrade attack protection	No

16

dwing5 "SDES Mode" -> "sdescriptions"
Dan Wing; 08.03.2006

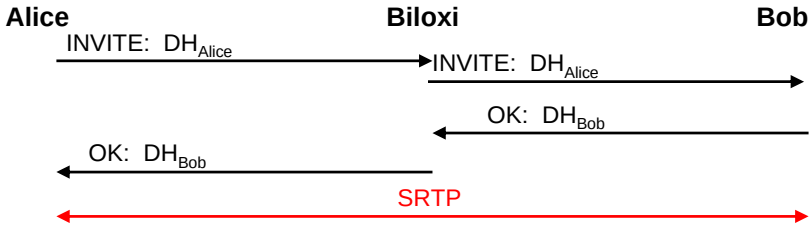
Encrypted Key Transport w/ SDES (draft-mcgrew-srtp-ekt-00)



	In SDES mode
Requires signalling confidentiality	Yes (insecure)
Forking	Yes
Media before SDP answer	Yes
Shared-key conferencing	No
Requires PKI	Yes
Rekeying	Depends on base handshake
Downgrade attack protection	

17

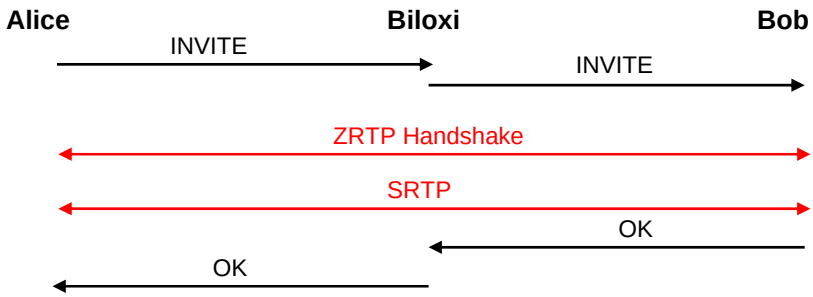
SDP DH Mode (draft-baugher-mmusic-sdp-00)



Requires signalling confidentiality	No
Forking	No
Media before SDP answer	No
Shared-key conferencing	No
Requires PKI	No
Rekeying	No
Downgrade attack protection	No

18

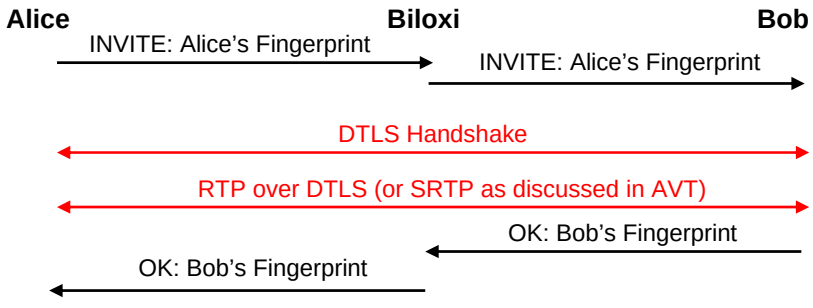
ZRTP (draft-zimmermann-avt-zrtp-01)



Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	Yes
Shared-key conferencing	No
Requires PKI	No
Rekeying	Yes
Downgrade attack protection	Yes

19

DTLS/RTP (draft-tschofenig-avt-rtp-dtls-00, etc.)



Requires signalling confidentiality	No
Forking	Yes
Media before SDP answer	Yes
Shared-key conferencing	No
Requires PKI	No
Rekeying	Yes
Downgrade attack protection	Yes

20

Summary Table

	Sig. Conf.	Forking	Media before Answer	Shared -key conf.	PKI?	Rekey	Bid-down protection
MIKEY-PSK	No	No	Yes	Yes	No*	Yes	Yes
MIKEY-RSA	No	No	Yes	Yes	Yes	Yes	Yes
MIKEY-DH	No	No	No	No	Yes	Yes	Yes
MIKEY-DHHMAC	No	No	No	No	No*	Yes	Yes
MIKEY-RSA-R	No	Yes	No	Yes	Yes	Yes	Yes
SDES	Yes	Yes*	No	Yes	No	Yes*	No
SDES-EM	Yes	Yes*	Yes	Yes	No	Yes	No
EKT	Yes*	Yes*	Yes	Yes	No	Yes	*
SDP-DH	No	No	No	No	No	No	No
ZRTP	No	Yes	Yes	No	No	Yes	Yes
DTLS	No	Yes	Yes	No	No	Yes	Yes

Architecture: Key Exchange: Signalling or Media Path?

- Signalling (SDP, SIP)
  - Already standardized
    - MIKEY/kmgmt-ext, Security Descriptions
  - Problems with
    - Media-before-SDP-Answer, forking
- Media path
  - Internet Drafts only
    - Pure inline
      - ZRTP
    - Hybrid
      - EKT (key exchange using security descriptions)
      - DTLS/RTP (fingerprints in SDP)
  - Better coordination with media protection
  - Changes RTP architecture

22

Architecture: Authenticating the Association

- Through external PKI
  - This seems problematic
- Through security of signalling channel
  - Confidentiality (TLS, S/MIME)
  - Integrity only
- Voice authentication
- Protocols more flexible than specified
  - Could use ZRTP with fingerprints, MIKEY-DH with voice authentication, MIKEY-DH w/o certificate validation, etc.
  - Not really a function of handshake but of design style
    - With some exceptions

23

Discussion Topics

- Importance of:
  - Media before SDP answer (“clipping”)
  - Secure Forking
  - Shared-Key Conferencing
- Interoperable SRTP Keying is Desirable ?
- Architecture Choices
  - Key Exchange: Signaling / Media Path
  - PKI

24

List of documents

RFC 3830 (MIKEY)
RFC 3711 (SRTP)
draft-ietf-mmusic-kmgmt-ext-15
draft-ietf-mmusic-sdescriptions-12

draft-ietf-msec-mikey-rsa-r-02
draft-ietf-msec-mikey-dhhmac-11
draft-ietf-msec-newtype-keyid-05
draft-mcgrew-srtp-ekt-00
draft-baugher-mmusic-sdp-dh-00
draft-zimmermann-avt-zrtp-01
DTLS:
- draft-tschofenig-avt-rtp-dtls-00
- draft-fischl-sipping-media-dtls-00
- draft-fischl-mmusic-sdp-dtls-00
- draft-rescorla-tls-partial-00
- draft-modadugu-dtls-short-00

draft-lehtovirtya-srtp-rcc-00
draft-fries-msec-applicability-00
draft-wing-mmusic-sdes-early-media-00 (expired)

25