RTP over DTLS

Jason Fischl (CounterPath)*
Nagendra Modadugu (Stanford)
Eric Rescorla (Network Resonance)
Hannes Tschofenig (Siemens)

* speaking
Basic problem: Key Mgmt

• Currently SRTP uses external key mgmt.
  – Existing proposals all use SIP for key exchange
  – Several proposals at IETF 65 with alternatives
• Current solutions have a number of problems:
  – Early media
  – Forking
  – Rollover counter management
  – Rekeying
  – Dependence on PKI
  – Capabilities discover problems
  – Drafts available to fix some but not all of these
• These problems are architectural
  – Correlation issues between signalling and media channels
  – Can’t be cleanly fixed at signalling level
Target applications

- Anything point-to-point
  - VoIP
    - Solution completely described
  - Streaming
    - Would need some more elaboration
- Not multicast/broadcast
  - This is a fundamentally different problem
    - Less well understood
    - Group keying has very different requirements
Existing approaches

• MIKEY
  – Shared key mode doesn’t scale
  – RSA mode requires global PKI
    • And directory
  – DH mode requires PKI
  – Problems with early media
  – Basic problem: not enough round trips

• SDESCRIPTIONS
  – Unrealistic security assumption: full channel confidentiality
  – Problems with early media
  – Forking has security issues
Fixes being discussed

- Modifications to MIKEY handshake
- Rollover counter management
- Public key support for SDESCRIPTIONS
- In-channel key updates
- Key management on media channel
RTP Over DTLS Overview

• Move key management to media channel
  – Carry media over Datagram TLS
  – Well understood technology

• Authenticate with certificate fingerprints
  – Same technique as comedia TLS
  – Could also use Short Authentication String a la ZRTP
  – Integrity protect the fingerprint using sip-identity

• Same packet format as SRTP
Message Flow

M1: INVITE: Fingerprint

M2: INVITE: Fingerprint

M3: INVITE: Fingerprint

M4: DTLS handshake

M5: RTP over DTLS

M6: OK: Fingerprint

M7: OK: Fingerprint

M8: OK: Fingerprint
Performance Issues

• SRTP is highly tuned for RTP
  – Low overhead
  – Headers in clear

• DTLS is generic
  – Higher overhead

• Meeting in the middle: “SRTP compatibility mode” looks like SRTP
  – New CTR mode cipher suite
  – Partial encryption
  – Implicit headers
    • But can interleave with explicit headers for easy resynchronization
  – On-the-wire only changes retain DTLS security arguments
Internet Drafts

- draft-tschofenig-avt-rtp-dtls-00
- draft-fischl-sipping-media-dtls-00
- draft-fischl-mmusic-sdp-dtls-00
- draft-ietf-tls-ctr-00
- draft-rescorla-tls-partial-00
- draft-modadugu-dtls-short-00