draft-ietf-sip-dtls-srtp-framework-00

IETF 70

Vancouver

Changes since draft-fischl-sipping-media-dtls-03.txt

- Added section on best effort encryption
- Added mmusic-sdp-capability-negotiation to example
- Added appendix with requirements analysis

Issue 1: Identity

- Issue: Use of RFC 4474 for phone numbers
  - Calls from sip:alice@example.com aren't a problem
  - Calls from sip:+14155551212@example.com present issues
- No single authoritative entity that can assert who is allowed to use a particular E.164 number
  - Who does the target trust to sign numbers?
  - This is an intrinsic problem with telephone numbers

Issue 1: Identity Cont.

- This is better than SDES + SRTP
  - Solves lots of other issues which were already discussed in the requirements document.
  - We don’t require TLS end to end and there is no way to ensure end to end TLS.

Issue 2: SRTP / TCP

- Issue: DTLS-SRTP over TCP vs RTP over TLS
- Resolution: Agreement in Chicago. Need to update the document

Issue 3: Anonymity

- Issue: Anonymity
- Resolution: Just need to update the text to say that DTLS isn't going to break existing anonymity

Issue 4: middle box issues

- Issue: SBC issues with blocking key exchange before a 200 OK
- Not specific to DTLS-SRTP
- discussed in draft-sipping-stucker-media-path-middleboxes-00

Next…

- Apply edits
- Ready for WGLC to meet the milestone?