Security

Eric Rescorla*

Document Status

- Fixed a bunch of issues
- Both documents in WGLC
- Some comments on list

Security

- Editorial comments from Magnus
- Added description of potential threat from WebAudio + SRTP (residual risk)

Security Arch

- Revise identity mechanism based on implmentatio experience
- Explicitly forbid NULL ciphers and SDES
- Clean up examples
- Reference RTCP-based DoS issue in RTP Usage
- Editorial cleanup

When is IFRAME ready? (Procter)

- IETF draft says “any message”
- W3C draft says “LOGINDONE”

Proposed resolution: LOGINDONE

RTP/RTCP Key Management (Aboba)

- Some lack of clarity about how many DTLS connections when no RTCP-mux
- The right answer is two per media stream

Proposed resolution: make this clear in doc.

DTLS versions

- DTLS 1.0 versus 1.2
- Everyone does 1.2 now
- Some people not eager to change

Proposed resolution: MUST 1.0, SHOULD 1.2.
Chairs to clear this with ADs.

MTI Cipher Suite

- Assuming we do TLS 1.0
- We require PFS
- TLS recently decided to adopt ECC on Standards Track

Proposed resolution:
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA