DTLS 1.3

Eric Rescorla
ekr@rtfm.com

November 8, 2021

Current Status

- In AUTH48
- Two substantive issues raised

Issue #249: Sequence numbers and epochs

- DTLS has tighter record limits than TLS w/ AES-GCM
  - See Appendix B
- The guidance is to rekey
  - But epochs are only 16 bits
  - This means that the total number of records is $2^{40.5}$
- This is a prohibitively small number

Two designs

- PR#255: Expands epoch to 64 bits but just encodes the lower 16 bits
  - Expands ACK to 112 bits
  - This is the more minimal change
  - Not clear that the epoch in the nonce helps; each epoch has separate keys
- PR#257: As with 255, but with 64-bit sequence numbers
  - More consistent with TLS
  - We need to be confident that key separation is enough anyway
  - Allows more record number space for ciphers which can use it
- Proposed resolution: PR#257 after quick consultation

Issue 247: handshake transcript

- DTLS `Handshake` is different from TLS

```
struct {
    HandshakeType msg_type;     /* handshake type */
    uint24 length;              /* bytes in message */
    uint16 message_seq;         /* DTLS-required field */
    uint24 fragment_offset;     /* DTLS-required field */
    uint24 fragment_length;     /* DTLS-required field */
```

- What do we do with `message_hash`
- TLS 1.3 and DTLS 1.3 transcripts are no longer clearly separable
- Is it time to bite the bullet and make DTLS 1.3 like TLS 1.3?
  - Pain for DTLS 1.2 impls