RFC 9147-bis

Eric Rescorla
ekr@rtfm.com

Current State

- Published -01 WG draft
- Uncontroversial changes, mostly from errata
    - Key updates (8047)
    - 128-bit record sequence number (8131)
    - Legacy session id (8066, 8067)
    - Initial handshake (8051)
    - Message seq wrapping (8048)
    - Clarify not ACKing epoch 1 (8107)
    - Code point no longer proposed (8100–oops)

Current State

- Published -01 WG draft
- Uncontroversial changes, mostly from errata
  - Key updates (8047)
  - 128-bit record sequence number (8131)
  - Legacy session id (8066, 8067)
  - Initial handshake (8051)
  - Message seq wrapping (8048)
  - Clarify not ACKing epoch 1 (8107)
  - Code point no longer proposed (8100–oops)

Replay Detection (PR #317, Issue #312)

- RFC 9147 makes replay detection optional
- John Mattson argues that it would be stronger to have it mandatory
  - But DTLS-over-SCTP has its own replay so doesn’t want duplicated drops
- Option 1: leave as-is
- Option 2: “must perform replay detection when run over a transport which does not provide anti-replay”

Acks in epoch 0 (issue #291)

- RFC 9147 specifies how to use ACKs in epoch 0 (unencrypted)
- You can’t send ACKs to DTLS 1.2 clients
  - So you can’t send an ACK until you know the version is DTLS 1.3+
  - But people typically parse ClientHello in one chunk
  - Client could maybe ACK partial ServerHellos
  - You can ACK after HRR
- DavidBen proposes just banning ACKs in epoch 0
  - Consequence: if CH is really big (e.g., Classic McEliece), then you get full retransmit
  - Does this really matter?
- Proposal: forbid sending ACKs in epoch 0, but don’t treat as an error

Plaintext Sequence Numbers

- DTLS 1.3 sequence numbers are encrypted
- nVidia has proposed an extension to allow for unencrypted sequence numbers https://datatracker.ietf.org/doc/html/draft-pismenny-tls-dtls-plaintext-sequence-number-02

- Should we make this change?
- My preference: not to DTLS core.

Next Steps

- Still issues around ACKs on epoch boundaries
- Hannes prepared some PRs based on DavidBen’s errata
    - I dropped the ball on really understanding all of these
    - Self-assignment: read through all these and propose a resolution (which may be “do what DavidBen says”)
- A few other small issues that I’ve got outstanding questions on