cTLS

Eric Rescorla
ekr@rtfm.com

2022-03-23

Recent changes

- Optional elements in the profile (PR#45)
- Move `profile_id` to `ClientHello` (PR#47)
- Make sequence number conditional on stream vs. datagram (PR#51)
- Clarify that alerts are the same as (D)TLS (PR#50)
- Clarify DTLS encryption computation (PR#52)

Issue#42: Self-Delimiting Handshake Messages (TCP)

- We removed `Handshake.length` to save space
- But this means you need to parse message internals in order to identify the end of handshake message.
- Should we reintroduce it? Ben Schwartz suggests a flag on the record, but this won't work for UDP

Issue#41: Fragmentation for Handshake Messages (UDP)

- cTLS was originally based on TLS
- Assumption was that the underlying transport would take care of in-order and reassembly
  - And maybe framing
- But then we extended it to DTLS

Proposed Solution: More Profiling

- Example: `handshakeFraming (none | length | full)`

Other Issues

- Already known: omit randoms and Finished
    - These need analysis. Can we do them later?
- Remove transcript reconstruction?
- Anything else?