DTLS 1.2 Status

Eric Rescorla
RTFM, Inc.
ekr@networkresonance.com

Current State

- New draft: `draft-ietf-tls-rfc4347-bis-01.txt`

- Defined handling of invalid cookies
- Fixed state machine for lost last flight
- Clarified buffering of out of order packets
- Editorial

Handling of Invalid Cookies

- Issue raised by Pasi Eronen
- Just dropping the HelloRequest creates deadlocks
  - For instance, what happens is server changes keys
- Resolution: treat as missing cookie

Lost Last Flight

- Issue raised by Robin Seggelman
- What happens if the last flight is lost
  - Other side retransmits
  - Does the sender retransmit?
- Fixed state machine
  - Required to hold last flight for 2MSL
  - Immediate retransmit in response to receive retransmit

```
 +-----------+
 |           |
 | FINISHED  |
 |           |
 +-----------+
      |  /|\
      |   |
      |   |
      +----+

   Read retransmit
Retransmit last flight
```

Buffering of Out of Order Packets (I)

- Issue raised by Michael Tuexen
- What happens about packets received before Finished
  - Packet drops
  - Reordering
- Clarified text to encourage buffering for reliable transports

> Implementations MAY either buffer or discard such packets, though when DTLS is used over reliable transports (e.g., SCTP), they SHOULD be buffered and processed once the handshake completes. Note that TLS's restrictions on when packets may be sent still apply, and the receiver treats the packets as if they were sent in the right order. In particular, it is still impermissible to send data prior to completion of the first handshake.

Buffering of Out of Order Packets (II)

- Issue raised by Michael Tuexesn
- What about reordering in rehandshakes?
- There is potential for glitches in dataflow
  - Data sent with new epoch
  - But not ready until CSS, Finished received
- Proposal: implementations MAY accept packets before receiving CSS, Finished
  - Major vulnerability here is downgrade attack
    - ∗ Epoch mostly replaces ChangeCipherSpec
  - SHOULD only do this during rehandshake?

Trajectory

- New version shortly
- Hopefully get more input
- Last call before PHL?