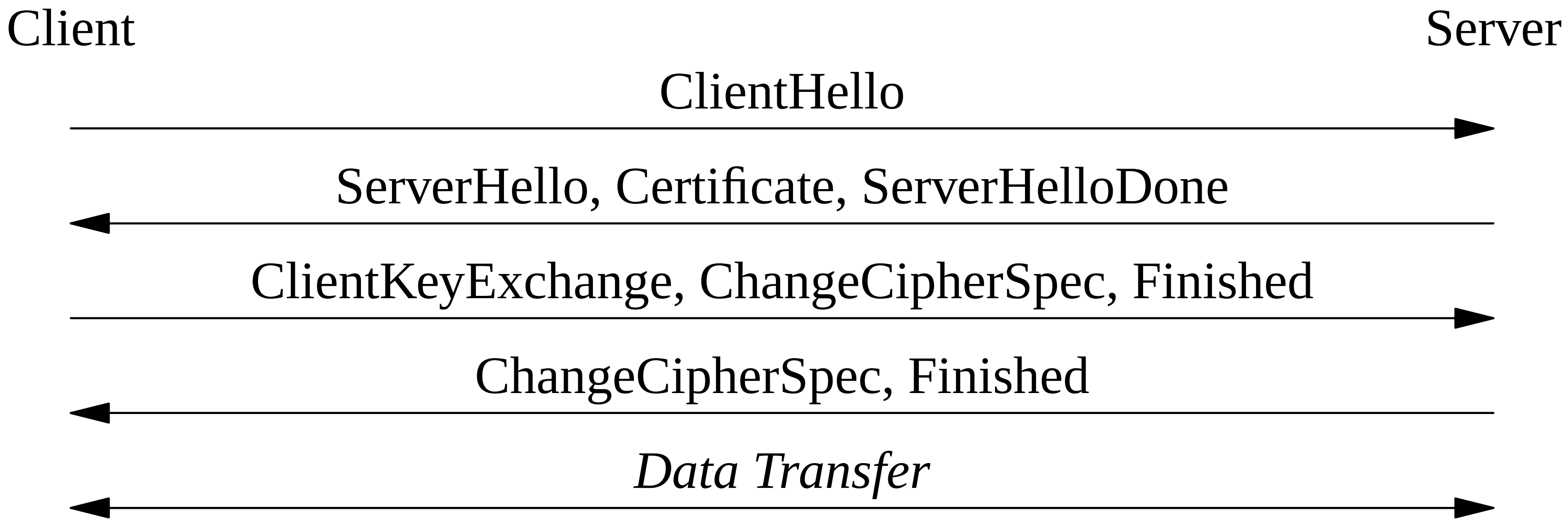
Thoughts on DTLS over DCCP

Eric Rescorla

Rationale for DTLS

- TLS doesn't work over datagram transport
  - Assumes reliability for handshake messages
  - Record $n + 1$ can only be interpreted in the context of record n
- DTLS fixes this problem
  - Timeout and retransmission for handshake messages
  - Record independence (stolen from TLS 1.1)
- As close as possible to TLS

Background: TLS Overview



Client

Server

ClientHello

ServerHello, Certificate, ServerHelloDone

ClientKeyExchange, ChangeCipherSpec, Finished

ChangeCipherSpec, Finished

Data Transfer

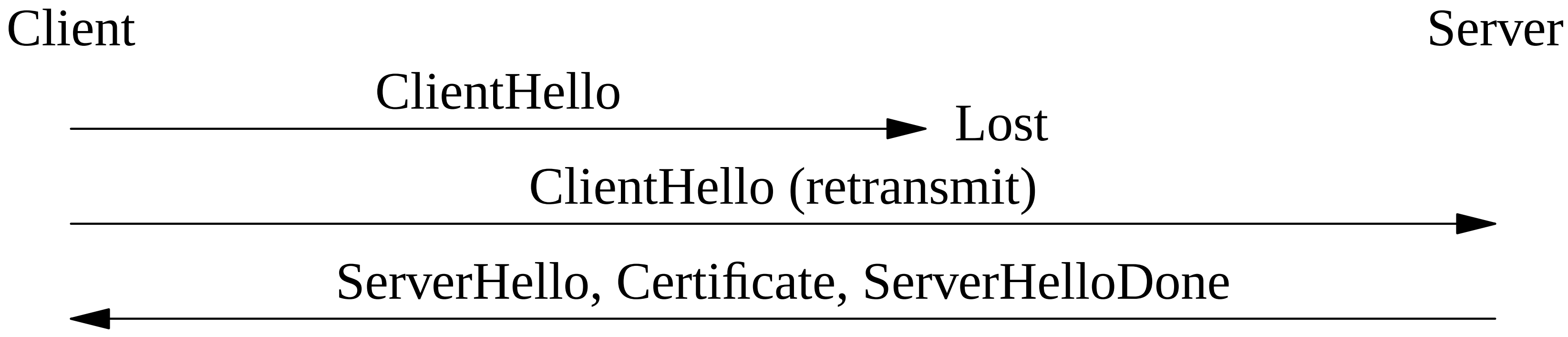
- All these steps are assumed to happen in order
- Doesn't apply in datagram contexts
  - Packets get lost
  - ... or re-ordered

Basic Principles for DTLS

- Start with TLS
- Make minimal changes to allow operation over datagram
- Don't make any "improvements"

DTLS Handshake Message Retransmission

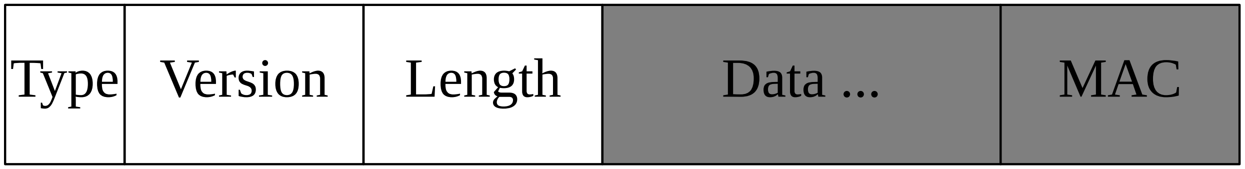
- What happens if handshake packets get lost?
  - Timeout and retransmit
  - Next message saves as ACK
  - Currently use a simple exponential backoff scheme



Record Independence

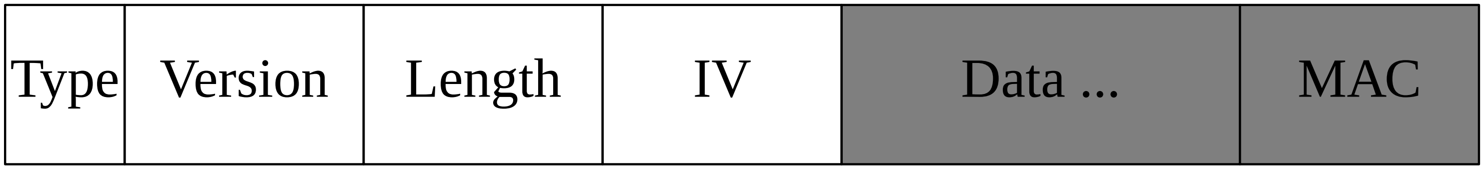
- TLS 1.0 records are not independent
  - Need sequence number to check message integrity
  - Stream ciphers (RC4) pretend to be one long stream
  - Block ciphers In CBC mode (AES, DES) record $n + 1$ depends on record n CBC residue
  - None of this works with loss
- DTLS Response
  - Explicit sequence number
    - With optional replay checking
  - Don't use stream ciphers
  - Explicit CBC initialization vector (from TLS 1.1)

Record Format Comparison (not to scale)



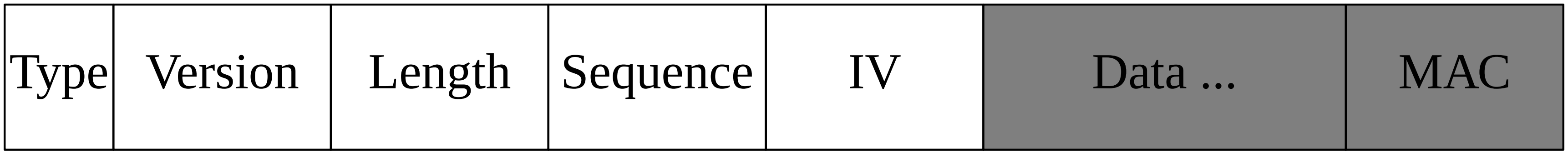
Type	Version	Length	Data ...	MAC

TLS 1.0



Type	Version	Length	IV	Data ...	MAC

TLS 1.1



Type	Version	Length	Sequence	IV	Data ...	MAC

DTLS

Status

- DTLS RFC-Ed queue (draft-rescorla-dtls-05.txt)
- In OpenSSL 0.9.8
- This implies a binding for UDP
  - Or something like it

Interactions with DCCP: Handshake Latency

- DCCP has its own handshake
- Natural procedure is to do DCCP handshake first then DTLS handshake
- This introduces latency
- Question: is there some way to merge these handshakes?

Interactions with DCCP: Retransmission and Congestion Control

- DCCP has built-in congestion control (duh!)
- This interacts with the DTLS retransmit algorithm
- But how?

What else?

- Probably lots of other stuff I don't know about
- Interest in working on a draft?