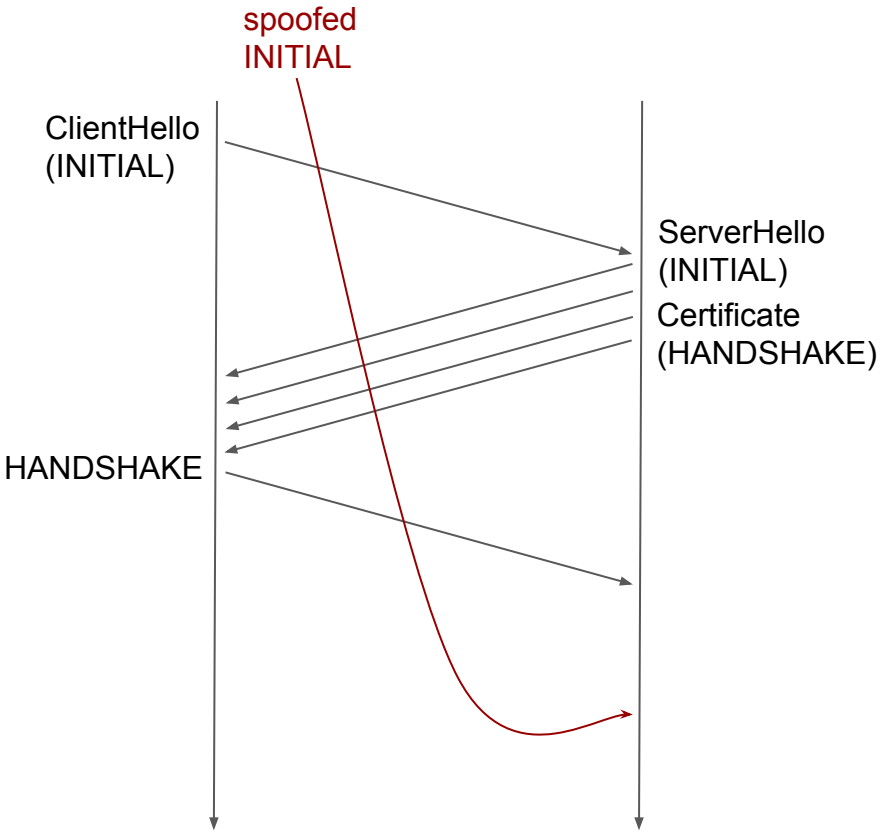
INITIAL
Injection Attack

IETF 103, Marten Seemann

INITIAL injection attack



- by injecting an INITIAL an attacker can blow up the connection
  - by sending a CONNECTION_CLOSE
  - by sending a malformed packet
  - ....
- endpoints accept INITIALS at least for 3 RTOs after all INITIAL data has been received & acked
  - which might be after the handshake completes

Proposal: treat INITIAL as the special snowflake it is

- it's the only packet an attacker can spoof
  - so we need to take extra steps to limit the attack surface
- stop accepting and retransmitting INITIALs as soon as possible:
  - for the client: stop accepting INITIAL packets after switching to handshake write keys
  - for the server: stop accepting INITIAL when receiving a HANDSHAKE packet
- congestion implications:
  - what to do with unacked INITIAL packets?
  - not unique to this proposal: peer might drop packets, we don't want to apply congestion penalty if we aren't sure that the network caused the loss (e.g. 0-RTT might be dropped by the server)