QUIC Resource Exhaustion Attacks

Marten Seemann, IETF 119
QUIC Connection ID Flow Control

active_connection_id_limit: 3

NEW_CONNECTION_ID (0)

NEW_CONNECTION_ID (1)

NEW_CONNECTION_ID (2)

NEW_CONNECTION_ID (3, Retire Before: 2)

RETIRE_CONNECTION_ID (0)

RETIRE_CONNECTION_ID (1)
Congestion Control

- on packet loss: reduce the congestion window
- on repeated packet loss: minimum congestion window is 2 (full-size) packets
- RTT measurement can be inflated by the peer
Compare to:

QUIC Stream Flow Control

- initial_max_stream_data: 100
- STREAM data (up to 50)
- STREAM data (up to 100)
- STREAM_DATA_BLOCKED (at 100)
- MAX_STREAM_DATA: 150
Similar to HTTP/2's Rapid Reset Attack
Better Flow Control for Connection IDs?

Should we have introduced a MAX_CONNECTION_ID frame?

For now, limiting the number of RETIRE_CONNECTION_ID frames mitigates the attack.

Path Validation is vulnerable, too

https://seemann.io/posts/2023-12-18-exploiting-quics-path-validation/