TLS Ticket Requests

draft-wood-tls-ticket-requests

Tommy Pauly (tpauly@apple.com)
David Schinazi (dschinazi.ietf@gmail.com)
Christopher A. Wood (cawood@apple.com)

TLS
IETF 103, November 2018, Bangkok

Problem

Servers vend a fixed number of tickets to clients upon connection establishment

Some clients may want or need more tickets to avoid reuse

- Parallel connections, Happy Eyeballs V2-style TLS racing, connection priming

Today, some tickets simply go to waste

Initial Design

Clients send post-handshake ticket request messages to receive individual NSTs on demand

Issues:

- Client-initiated post handshake message
- Non-trivial protocol change
- Complicated story around request reading and writing buffering

Simplified Approach

Clients send an extension that signals the number of tickets desired in the CH

- Clients must know the amount of tickets desired upon connection initiation

- Does not allow for dynamic vending of tickets

Post-Handshake Buffering

Implementations may require post-handshake message buffering

- More NSTs means more post-handshake data
- NSTs can arrive out-of-order in QUIC and require buffering and reassembly

TLS has no way to restrict handshake message size

- This should probably be addressed separately

Questions?
WG Adoption?