Certificate Compression

draft-ietf-tls-certificate-compression

Alessandro Ghedini, Cloudflare

Victor Vasiliev, Google

Draft status

- No major update, just small editorial changes.

Implementation / Deployment status

- Chrome (BoringSSL) support shipped in July 2018.
- Cloudflare (BoringSSL) deployed to all zones in September 2018.
- Implementations also from Apple (BoringSSL?) and Facebook.

Data

From Cloudflare's deployment:

- Average 1.5KB certificate size reduction for both RSA and ECDSA.
- ECDSA from 3.5KB to 2KB, RSA from 4.9KB to 3.5KB.
- QUIC allows for 3x amplification from server before address verification.
- Client must send at least 1200 bytes in first flight, so server is allowed ~3.6KB for its first flight.
- Compressing certificates is enough for ECDSA, but RSA certificates might not always fit (partially depends on CA, so YMMV).

Open issue

- Only one open issue: potential attack on decompression function.
- If the decompression function produces different output depending on timing of received data, attackers could modify the certificate processed by the receiver by delaying data on the wire.
- Same applies to ASN.1 parsing.

Potential solution

- Add decompressed certificate too to handshake transcript.
- Is it worth it? / Do we care enough?

Next steps:

- WGLC?