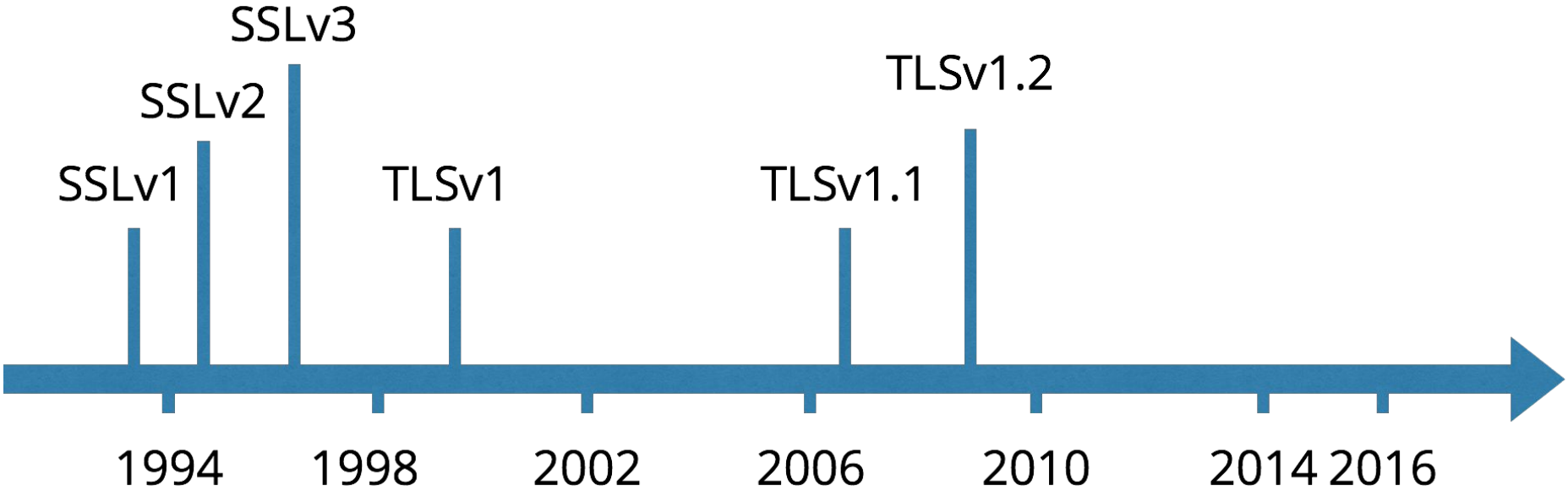
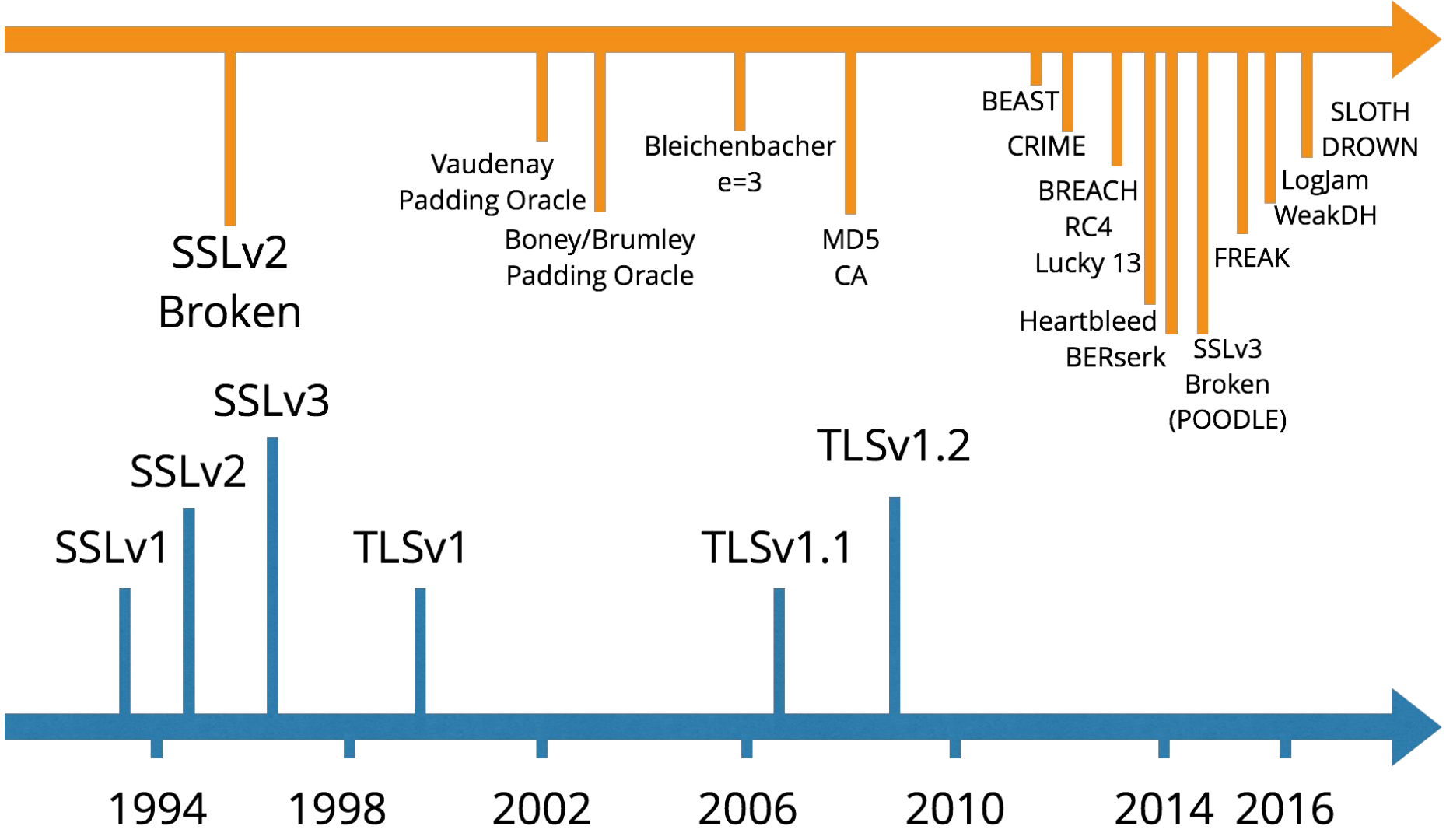
TLS 1.3 Hackathon

Nick Sullivan, CloudFlare Inc.

What is TLS?

A protocol that encrypts and authenticates transport for HTTPS, WebRTC, others.


SSLv3
SSLv2
SSLv1
TLSv1
TLSv1.1
TLSv1.2
1994
1998
2002
2006
2010
2014
2016


SSLv2
Broken
Vaudenay
Padding Oracle
Boney/Brumley
Padding Oracle
Bleichenbacher
e=3
MD5
CA
BEAST
CRIME
BREACH
RC4
Lucky 13
Heartbleed
BERserk
SSLv3
Broken
(POODLE)
FREAK
LogJam
WeakDH
SLOTH
DROWN
SSLv1
SSLv2
SSLv3
TLSv1
TLSv1.1
TLSv1.2
1994
1998
2002
2006
2010
2014
2016

Top HTTPS Adoption Issues

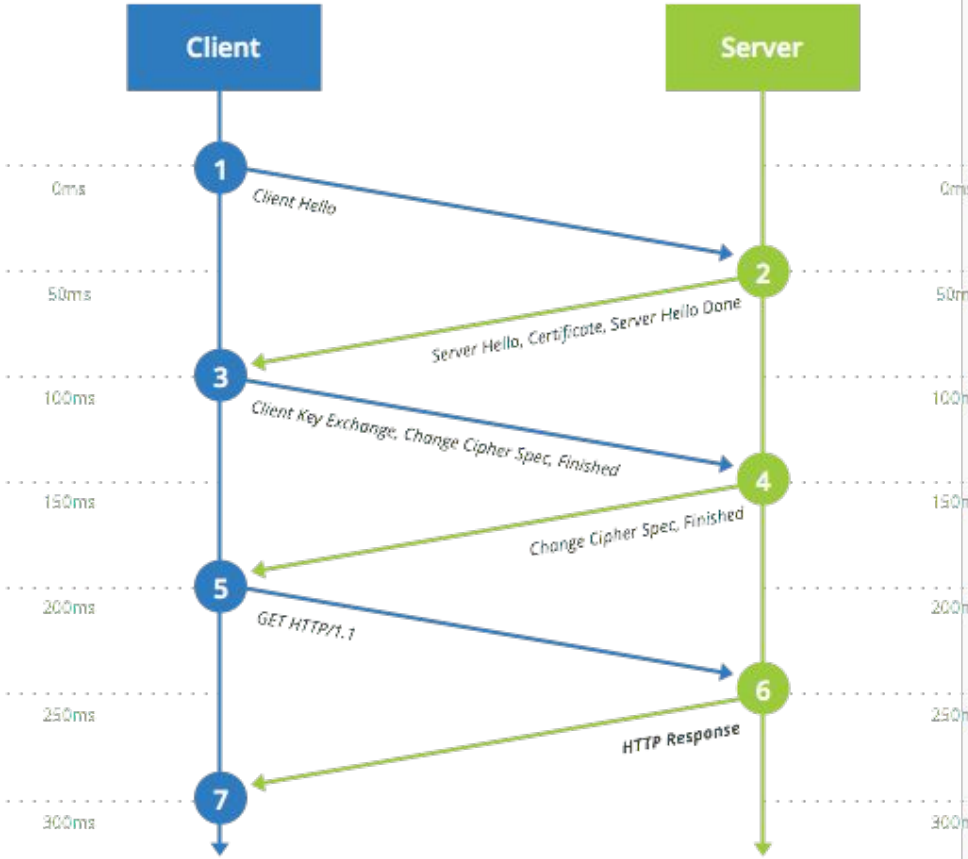
2016

Certificate Management

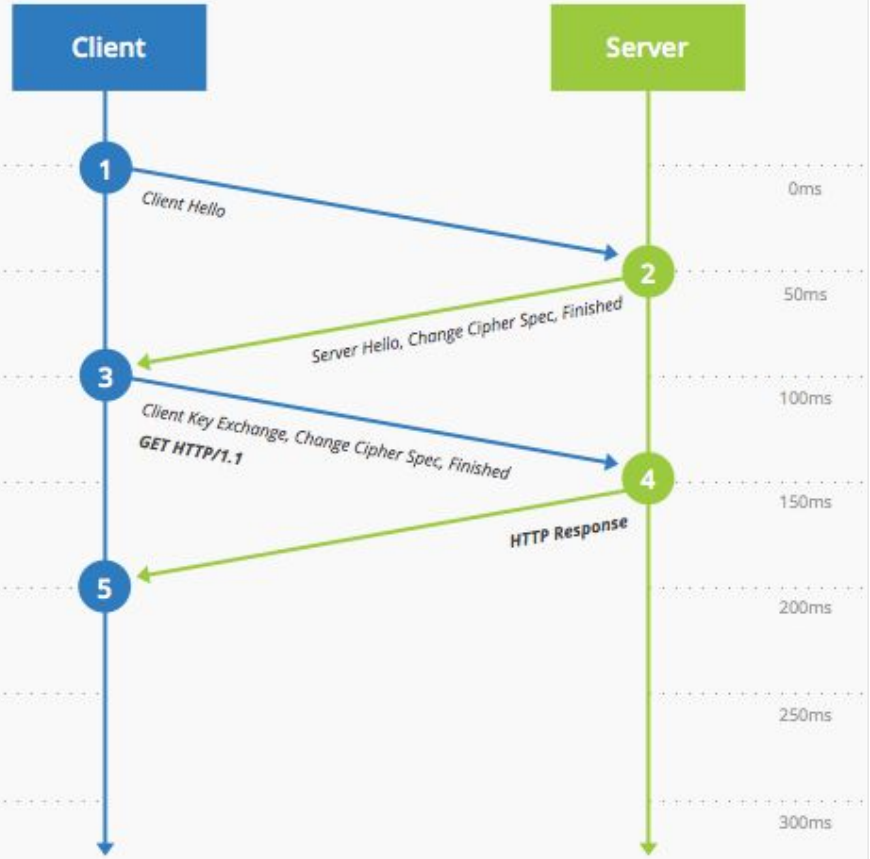
Mixed Content

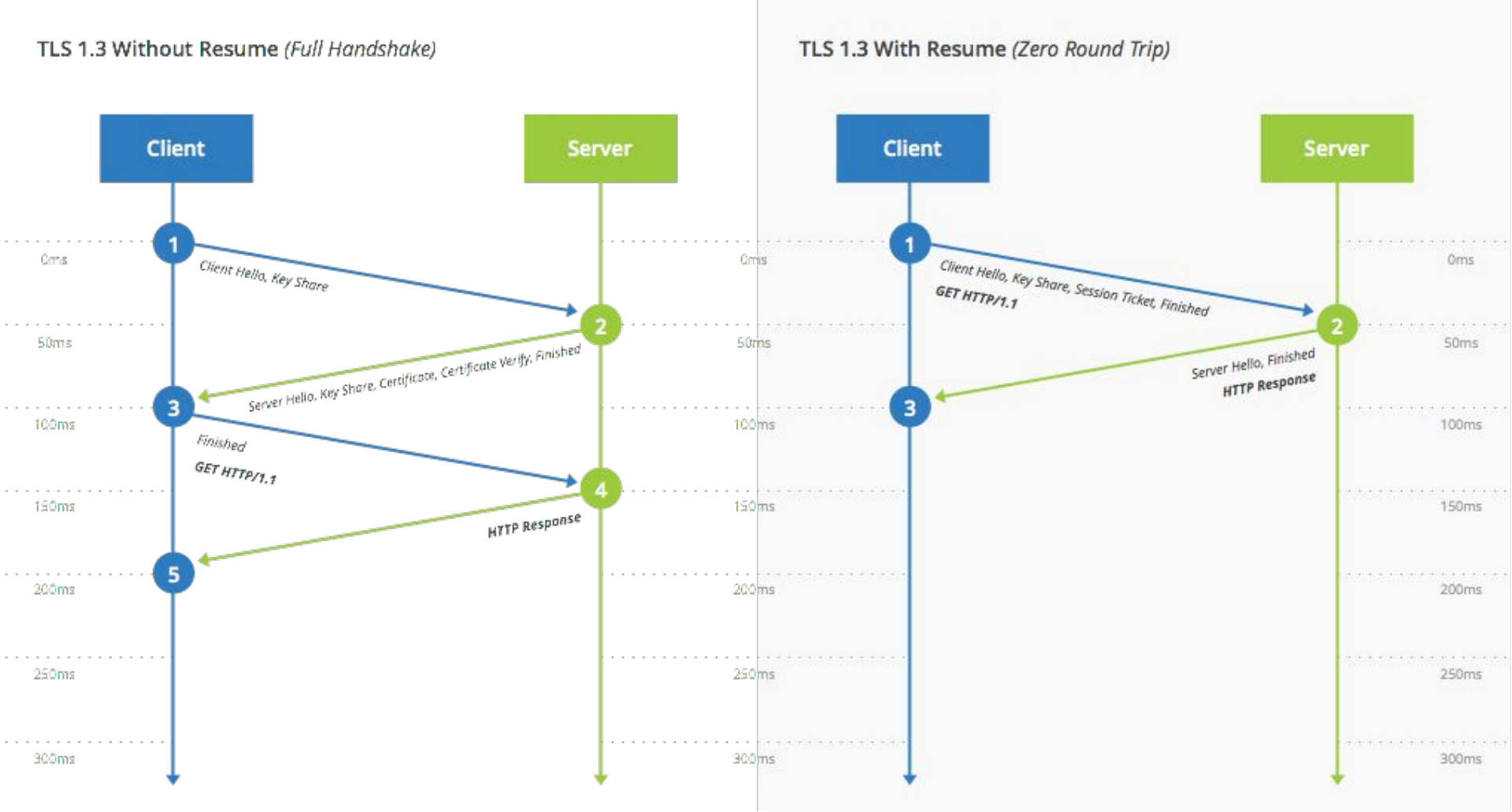
Added Latency

TLS 1.2 Without Resume *(Full Handshake)*



TLS 1.2 With Resume *(Abbreviated Handshake)*




TLS 1.3 Without Resume (Full Handshake)
Client
Server
1
Client Hello, Key Share
2
Server Hello, Key Share, Certificate, Certificate Verify, Finished
3
Finished
GET HTTP/1.1
4
HTTP Response
5
0ms
50ms
100ms
150ms
200ms
250ms
300ms
TLS 1.3 With Resume (Zero Round Trip)
Client
Server
1
Client Hello, Key Share, Session Ticket, Finished
GET HTTP/1.1
2
Server Hello, Finished
HTTP Response
3
0ms
50ms
100ms
150ms
200ms
250ms
300ms

Current Status

Draft 12: Near final draft

Implementations:

- F#
- OCaml
- C (NSS)
- Go (Under construction)

OpenSSL: “We’re not starting until the final draft”

Hackathon Goals

1. Finish integration with Firefox so we can do an HTTP request.

2. Actually demonstrate Firefox->CloudFlare interop (tls13.cloudflare.com)

3. Resumption-PSK between NSS and Mint

4. 0-RTT between NSS and Mint

5. 0-RTT in Firefox

6. (Stretch goal) 0-RTT between Firefox and CloudFlare