Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

25th March 2019
IETF 104 Prague

Enhanced Performance through TLS Resumptions across SNI values

Erik Sy

Problem statement

- TLS resumption across Server Name Indication (SNI) values is a legitimate performance-optimization but TLS 1.3 recommends against it

- Currently, it lacks a mechanism to announce, that TLS resumption across specific SNI values are supported

Loading behavior of the Alexa Top 1K Sites

- Facts on the average website
  - requires 20.24 TLS connections to different SNI values
  - these SNI values form 9.49 TLS trust groups
    - results based upon x 509 certificate and feasible TLS resumptions
  - requires 4.04 sequential full TLS handshakes
    - Page loading time is affected several times by the delay overhead of the TLS connection establishment

Performance gain of resumed TLS 1.3 connection establishment

- Elapsed time

Network latency	Full	1-RTT resumed	0-RTT resumed
0.3 ms	29.2 ms	6.3 ms	6.6 ms
50 ms	190.1 ms	160.1 ms	109.6 ms
100 ms	340.8 ms	310.3 ms	209.7 ms

- CPU time

Peer	Full	1-RTT resumed	0-RTT resumed
Server	7.8 ms	2.3 ms	2.6 ms
Client	9.2 ms	2.4 ms	2.5 ms

Performance benefits of TLS resumption across SNI values

- Benefits for the first visit of an average website
  - converts about 58.7% of the required full TLS handshakes to resumed connection establishments
  - reduces the required CPU time for the TLS connection establishments by about 44%
  - reduces the elapsed time to establish all required TLS connections by up to 30.6%

Design of a TLS extension for resumptions across SNI values

- Server requires a flag to signal support for this feature
- Flag declares the subject alternative name (SAN) list of the x509 certificate as a trust group
- Members of a trust group support the resumption of sessions with any other member of the same group

Privacy considerations

- The proposal enables tracking across hostnames that share the same private key of their x 509 certificate
  - similar linking of user visits is feasible via redirects, hyperlinks, and connection reuse of HTTP/2
- Defense should focus on avoiding long-term tracking via session resumption

Thank you

Questions and Answers

E-mail: tls@erik-sy.de

Preprint: https://erik-sy.de/Paper104.pdf

Slides: https://erik-sy.de/104.pdf