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**

<table>
<thead>
<tr>
<th>Network latency</th>
<th>Full</th>
<th>1-RTT resumed</th>
<th>0-RTT resumed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3 ms</td>
<td>29.2 ms</td>
<td>6.3 ms</td>
<td>6.6 ms</td>
</tr>
<tr>
<td>50 ms</td>
<td>190.1 ms</td>
<td>160.1 ms</td>
<td>109.6 ms</td>
</tr>
<tr>
<td>100 ms</td>
<td>340.8 ms</td>
<td>310.3 ms</td>
<td>209.7 ms</td>
</tr>
</tbody>
</table>

- **CPU time**

<table>
<thead>
<tr>
<th>Peer</th>
<th>Full</th>
<th>1-RTT resumed</th>
<th>0-RTT resumed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>7.8 ms</td>
<td>2.3 ms</td>
<td>2.6 ms</td>
</tr>
<tr>
<td>Client</td>
<td>9.2 ms</td>
<td>2.4 ms</td>
<td>2.5 ms</td>
</tr>
</tbody>
</table>
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
Questions and Answers

E-mail: tls@erik-sy.de
Preprint: https://erik-sy.de/Paper104.pdf
Slides: https://erik-sy.de/104.pdf