SSLKEYLOGFILE
Extension for ECH

Yaroslav Rosomakho  Hannes Tschofenig
SSLKEYLOG is a useful troubleshooting tool
Challenges of TLS troubleshooting with ECH

• Inspecting ECH
• Troubleshooting TLS handshake with ECH
• Decrypting TLS session when ECH is negotiated
The proposed solution

• ECH_SECRET label to log HPKE shared_secret
• ECH_CONFIG label to log ECHConfig
• Outer ClientHello Random as keys for ECH_SECRET and ECH_CONFIG
• Inner ClientHello Random for the rest of the session as long as ECH was accepted
Prototype implementations

- **NSS**: [https://github.com/yaroslavros/nss-echkeylog](https://github.com/yaroslavros/nss-echkeylog)
  - Very straightforward as shared secret is a part of HPKE context

- **BoringSSL**: [https://github.com/yaroslavros/boringssl-echkeylog](https://github.com/yaroslavros/boringssl-echkeylog)
  - Required additional callback in HPKE key schedule process

- **Wireshark**: [https://github.com/yaroslavros/wireshark-echkeylog](https://github.com/yaroslavros/wireshark-echkeylog)
Visibility into ECH
Confirming server acceptance

- **TLSv1.3 Record Layer: Handshake Protocol: Server Hello**
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 155
- **Handshake Protocol: Server Hello**
  - Handshake Type: Server Hello (2)
  - Length: 151
  - **Version: TLS 1.2 (0x0303)**
  - **Random: 6aef33f6f07cc80db36ce1300dc13a76ff340388e5e9759ea06f7f30fd8b8cc**
    - ECH Confirmation Bytes: ea06f7f30fd8b8cc
  - [Computed ECH Confirmation Bytes: ea06f7f30fd8b8cc]
    - [Expert Info (Note/Protocol): Calculated ECH Confirmation matches Server Random bytes, ECH was accepted]
Visibility into the rest of the session

<table>
<thead>
<tr>
<th>4</th>
<th>0.817821</th>
<th>192.168.1.90</th>
<th>213.108.108.101</th>
<th>TLSv1.3</th>
<th>583</th>
<th>Client Hello (SNI=cover.defo.ie) (SNI=defo.ie)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.833520</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TCP</td>
<td>66</td>
<td>443 → 49837 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TLSv1.3</td>
</tr>
<tr>
<td>6</td>
<td>0.833522</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>177</td>
<td>Hello Retry Request, Change Cipher Spec</td>
</tr>
<tr>
<td>7</td>
<td>0.833738</td>
<td>192.168.1.90</td>
<td>213.108.108.101</td>
<td>TCP</td>
<td>66</td>
<td>49837 → 443 [ACK] Seq=518 Ack=112 Win=131648 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>0.834369</td>
<td>192.168.1.90</td>
<td>213.108.108.101</td>
<td>TLSv1.3</td>
<td>561</td>
<td>Change Cipher Spec, Client Hello (SNI=cover.defo.ie)</td>
</tr>
<tr>
<td>9</td>
<td>0.858603</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TCP</td>
<td>66</td>
<td>443 → 49837 [ACK] Seq=112 Ack=953 Win=64384 Len=0</td>
</tr>
<tr>
<td>10</td>
<td>0.82960</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>1514</td>
<td>Server Hello, Encrypted Extensions</td>
</tr>
<tr>
<td>11</td>
<td>0.82962</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>1514</td>
<td>Certificate</td>
</tr>
<tr>
<td>12</td>
<td>0.82963</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>353</td>
<td>Certificate Verify, Finished</td>
</tr>
<tr>
<td>13</td>
<td>0.853158</td>
<td>192.168.1.90</td>
<td>213.108.108.101</td>
<td>TCP</td>
<td>66</td>
<td>49837 → 443 [ACK] Seq=953 Ack=3295 Win=128448 Len=0</td>
</tr>
<tr>
<td>14</td>
<td>0.854652</td>
<td>192.168.1.90</td>
<td>213.108.108.101</td>
<td>TLSv1.3</td>
<td>124</td>
<td>Finished</td>
</tr>
<tr>
<td>15</td>
<td>0.869765</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TCP</td>
<td>66</td>
<td>443 → 49837 [ACK] Seq=3295 Ack=1011 Win=64384 Len=0</td>
</tr>
<tr>
<td>16</td>
<td>0.869766</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>337</td>
<td>New Session Ticket</td>
</tr>
<tr>
<td>17</td>
<td>0.869767</td>
<td>213.108.108.101</td>
<td>192.168.1.90</td>
<td>TLSv1.3</td>
<td>337</td>
<td>New Session Ticket</td>
</tr>
<tr>
<td>18</td>
<td>0.869971</td>
<td>192.168.1.90</td>
<td>213.108.108.101</td>
<td>HTTP</td>
<td>121</td>
<td>GET / HTTP/1.1</td>
</tr>
</tbody>
</table>
Thank you!

• What do you think about the problem?
• What do you think about proposed solution?
• Should this work be adopted by the Working Group?