IETF 100
HACKATHON
TLS 1.3
THE FINAL LAP
Deploying TLS 1.3
GOALS

• Interoperability

• TLS 1.3 Draft 21 plus middlebox compatibility patch (#1091 on Github)

• Application integration

• Proxies, debugging tools, development tools
TEAM

- 16 in Singapore
- 8 remote participants
  - Japan, London, Mauritius (hackers.mu)
APPLICATIONS

- Wireshark, stunnel, wget, curl (w/ WolfSSL D18)
- Monit, Stunnel, Hitch, Aria2c, Nagios-plugins, Ftimes (D21)
- Envoy (D21+)
**TLS INTEROP**

F = Full Handshake, R = Resumption, H = HRR, Z = 0RTT, "-" = 21 only

<table>
<thead>
<tr>
<th>Client/Server</th>
<th>NSS</th>
<th>BoringSSL</th>
<th>OpenSSL</th>
<th>TLS-tris</th>
<th>Envoy</th>
<th>Fizz</th>
<th>Haskell 1.3</th>
<th>picotls</th>
<th>mint</th>
<th>mbedTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS</td>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>BoringSSL</td>
<td>FRHZ</td>
<td>FRHZ</td>
<td></td>
<td>FRHZ</td>
<td>FRHZ</td>
<td>FRZ</td>
<td>FRHZ</td>
<td></td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>FRHZ</td>
<td></td>
<td>FRH(Z)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>TLS-tris</td>
<td>F-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>Fizz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Haskell 1.3</td>
<td>FRZ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FRHZ</td>
</tr>
<tr>
<td>picotls</td>
<td>FRHZ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>mint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F-</td>
<td></td>
<td>FH-</td>
</tr>
<tr>
<td>mbedTLS</td>
<td>F-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>F-</td>
<td>F-</td>
<td></td>
</tr>
</tbody>
</table>
TAKEAWAYS

• TLS 1.3 is closer than ever to releasing

• Ready for more experiments with middleboxes

• Integration into a wider variety of applications

• A strong network of implementers
IETF 100

HACKATHON

TLS 1.3