T-DNS: Connection-Oriented DNS to Improve Privacy and Security

IETF 89 DNSE BOF

USC/ISI
John Heideman
Zi Hu
Liang Zhu

Verisign Labs
Allison Mankin
Duane Wessels
Why Consider T-DNS

• Privacy – Lacking encryption, vanilla DNS is susceptible to eavesdropping; especially so given widespread use of WiFi and third-party recursive DNS services.

• Spoofing – UDP’s connectionless nature makes it ideal for use in reflection/amplification attacks.

• Fragmentation – Large DNS responses are increasingly common, leading to IP fragmentation and a new set of security concerns.
Downsides

• TCP setup adds 1 RTT.
  – Amortized with reuse and pipelining.
  – Reduced with TCP Fast Open.
• Have to worry about middleboxes that interfere with TCP/53.
• TLS setup adds another 2 RTTs.
  – Reduced with Session Resumption.
• Have to think about certificate validation.
• Have to think about failover.
Proposed: New EDNS0 bit “TO”
a.k.a. STARTTLS for DNS

1. Establish TCP connection.
2. Client sends (dummy) query with TO bit set.
   “Hey, let’s upgrade this connection to TLS!”
3. Server responds with TO bit set.
   “Yeah, I’m down with that!”
4. TLS session negotiation commences.
## Performance Improvements

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP setup</td>
<td>Connection reuse</td>
<td>stub—recursive: good recursive—auth: poor</td>
</tr>
<tr>
<td>TCP setup</td>
<td>TCP fast open [draft-ietf-tcpm-fastopen-07]</td>
<td>In Linux Requires application change</td>
</tr>
<tr>
<td>TLS setup</td>
<td>Session Resumption [RFC 5077]</td>
<td>In GnuTLS</td>
</tr>
<tr>
<td>Stop-and-Wait</td>
<td>Pipelining</td>
<td>poor</td>
</tr>
</tbody>
</table>
Implementation Status

• TO bit server-side in Unbound.
  – partial support for OOOP
• TO bit client-side in custom client.
  – supports pipelining and OOOP
• A DNS proxy
  – Accepts UDP/TCP/TLS on server side
  – Outbound UDP to upstream server
Further Information

- draft-hzhwm-start-tls-for-dns-00
- T-DNS: Connection-Oriented DNS to Improve Privacy and Security
  - ftp://ftp.isi.edu/isipubs/tr-688abs.htm
- http://www.isi.edu/ant/tdns/index.html
Appendix
Simulated Connection Reuse
stub-to-recursive

number of concurrent connections vs. time-out window (seconds)
estimated memory consumption (GB)
Simulated Connection Reuse recursive-to-authoritative

- Number of concurrent connections vs. time-out window (seconds)
- Memory consumption (GB)
Latency Measurements

The graph shows the latency measurements for different network protocols and configurations over time. The y-axis represents the elapsed time in seconds, while the x-axis indicates the number of queries after a certain point in time. Various protocols and configurations are compared, including UDP stop-and-wait, UDP pipelined, TCP no-reuse, TCP reuse stop-and-wait, TCP pipelined, TCP pipelined+ooop, SSL no-reuse, SSL reuse stop-and-wait, and SSL pipelined+ooop. The graph demonstrates how each configuration affects latency under different conditions.