Latest Measurements on DNS Privacy

Sinodun

Sara Dickinson  sara@sinodun.com (Presenter)
John Dickinson  jad@sinodun.com
Jim Hague  jim@sinodun.com
Agenda

• Two topics
  • Summary of initial benchmarking work on TCP/TLS for recursive resolvers
  • (Time permitting) Brief look at level of implementation & deployment of both DNS over TLS & HTTP
Partly funded by a grant from the Open Technology Fund (and NLnet Foundation)

• GOALS of this initial work:
  • Understand characteristics of how existing recursive servers handle TCP and TLS loads
  • Looking at relative performance cf. UDP more than absolute at this stage
Partly funded by a grant from the Open Technology Fund (and NLnet Foundation)

• **GOALS of this initial work:**
  
  • **Understand characteristics** of how existing recursive servers handle TCP and TLS loads
  
  • **Looking at relative performance** cf. UDP more than absolute at this stage

Much more complex than UDP... Many more parameters...
Nameservers tested

- Bind 9.12.1 (No TLS)
- Unbound 1.7.0
- Knot Resolver 2.3.0
- dnsdist 1.3.0

Other nameservers are available....
Test setup - Hardware

- 2*8 core Intel Xenon @ 2.1Ghz, 32Gb RAM
- Ubuntu 18.04
- Only basic OS and NS tuning
- NS locked to 4 cores (threads)
- Hot cache

Hardware:
- 2*8 core Intel Xenon @ 2.1Ghz, 32Gb RAM
- Ubuntu 18.04
- Only basic OS and NS tuning
- NS locked to 4 cores (threads)
- Hot cache
Test setup - Software

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp**: fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but...
  - implementation issues due to threading

GitHub: sinodun/dnsperf-tcp
Test setup - Software

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp**: fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but...
  - implementation issues due to threading

GitHub: sinodun/dnsperf-tcp

TLS 1.2, No TFO, TLS SR,...
Test setup - Software

- **dnsperf**: from Nominum/Akamai (not resperf)
- **dnsperf-tcp**: fork of dnsperf with tcp support
- **dnsperf-tls**: branch with tls support but..
  - implementation issues due to threading

---

Focus on few clients, Varying q per conn

TLS 1.2, No TFO, TLS SR,...
UDP

- Increasing load by adding clients
- Unbound & dnsdist similar
- Bind very flat
• Increasing load by adding clients
• 20,000 q per conn

UDP vs TCP

- dnsdist TCP better than UPD (but threading is diff)!
- Others similar reduction
% of UDP

TCP and TLS (as percent of UDP)

- DNSWG @ RIPE76
- DNS Privacy Measurements

- 8 clients
- 20,000 q per conn

- dnsdist best
- Unbound does not do concurrent processing
Low q/conn

- Using 8 clients
- Solid line is TCP, dotted is TLS

- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat
Low q/conn

- Using 8 clients
- Solid line is TCP, dotted is TLS

- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat
Low q/conn

- Using 8 clients
- Solid line is TCP, dotted is TLS
- dnsdist fall-off ~2000
- U & B fall-off ~1000
- Knot TCP is very flat
Using 8 clients
Current test system hits issues...

Knot flat till ~100 q/conn
Others linear decline
(1 + N)/N dips ~ 100
Low q/conn

- Using 8 clients
- Current test system hits issues...
- Knot flat till ~100 q/conn
- Others linear decline
- \((1 + N)/N\) dips ~ 100
TODO list

• Understand implementations better
• OS + NS tuning
• Drill to lower q/conn for TCP and TLS
  • Add tricks: TFO, TLS Session Resumtion, TLS 1.3,…
• Scale to MANY clients
• Compare to TLS proxy e.g. nginx, haproxy
• Add concurrent processing to Unbound
• Use new/different test tool?

Full report on dnsprivacy.org
Deployment & Implementation

DOT: DNS-over-TLS
DOH: DNS-over-HTTPS (WIP)
# Implementation

<table>
<thead>
<tr>
<th></th>
<th><strong>Client</strong></th>
<th><strong>Recursive Resolver</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DOT</strong></td>
<td>• Stubby</td>
<td>• Unbound, Knot Resolver, dnsdist + CoreDNS, Tenta</td>
</tr>
<tr>
<td></td>
<td>• Unbound/Knot resolver (fwd)</td>
<td>• BIND on the way?</td>
</tr>
<tr>
<td></td>
<td>• Android system (dev)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• systemd (PR)</td>
<td></td>
</tr>
<tr>
<td><strong>DOH</strong></td>
<td>• Android Intra App</td>
<td>• Various experimental</td>
</tr>
<tr>
<td></td>
<td>• Firefox config option</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Stubby (next release)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Various experimental</td>
<td></td>
</tr>
</tbody>
</table>

* 10+ implementations (see DOH mailing list and IETF 101 Hackathon)
## Recursive Resolver Deployment

<table>
<thead>
<tr>
<th>DOT</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 19 test servers</td>
<td>• Quad9 (9.9.9.9)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cloudflare (1.1.1.1)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DOH*</th>
<th>Standalone</th>
<th>Large Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Few other test servers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Experimental, some support JSON as well as wireformat
Stub to recursive is changing

- DOH draft is in WGLC
- Expect browsers to adopt DOH (default?), other apps?
- System components to use either DOT or DOH…?
- What does this mean for users
  - Privacy (yeah!) but…
  - Multiple config points (transport & DNSSEC), multiple recursives, monitoring?
Stub to recursive is changing

- DOH draft is in WGLC
- Expect browsers to adopt DOH (default?), other apps?
- System components to use either DOT or DOH…?
- What does this mean for users
  - Privacy (yeah!) but…
  - Multiple config points (transport & DNSSEC), multiple recursives, monitoring?
Thank you!

More information at:

dnsprivacy.org