No Port 53, Who Dis?
A Year of DNS over HTTPS over Tor

@alecmuffett, February 2021 — v2.0 final
Conclusion
My partner and I have exclusively used **DNS over HTTPS over Tor (DoHoT)** at home for 1 year.
It worked fine
It worked so well that I set it up and forgot about it from February to July, because suddenly lockdown
Everything I'd read about this, told me to **expect disaster**
Everything I'd read about this, was and is **wrong**
It turns out that it's not bad to live with a median DNS latency of 250 to 500ms.
<table>
<thead>
<tr>
<th>server</th>
<th>count</th>
<th>min</th>
<th>p25</th>
<th>p50</th>
<th>mean</th>
<th>p75</th>
<th>p90</th>
<th>p95</th>
<th>p99</th>
<th>max</th>
<th>mean</th>
<th>mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>overall</td>
<td>2406088</td>
<td>0</td>
<td>0</td>
<td>262</td>
<td>592</td>
<td>1238</td>
<td>1873</td>
<td>5555</td>
<td>10726</td>
<td>536</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>only DoH</td>
<td>1633002</td>
<td>30</td>
<td>251</td>
<td>464</td>
<td>838</td>
<td>1558</td>
<td>2492</td>
<td>6483</td>
<td>10726</td>
<td>789</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>only cache</td>
<td>773086</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2176</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>google</td>
<td>321821</td>
<td>37</td>
<td>213</td>
<td>403</td>
<td>644</td>
<td>1174</td>
<td>1716</td>
<td>5544</td>
<td>10007</td>
<td>632</td>
<td>164</td>
<td></td>
</tr>
<tr>
<td>cloudflare</td>
<td>317427</td>
<td>42</td>
<td>221</td>
<td>417</td>
<td>669</td>
<td>1207</td>
<td>1775</td>
<td>5595</td>
<td>10726</td>
<td>649</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>nextdns</td>
<td>278311</td>
<td>30</td>
<td>234</td>
<td>423</td>
<td>669</td>
<td>1227</td>
<td>1731</td>
<td>4379</td>
<td>10003</td>
<td>631</td>
<td>170</td>
<td></td>
</tr>
<tr>
<td>a-and-a</td>
<td>270325</td>
<td>45</td>
<td>242</td>
<td>446</td>
<td>708</td>
<td>1317</td>
<td>1905</td>
<td>5568</td>
<td>10216</td>
<td>691</td>
<td>171</td>
<td></td>
</tr>
<tr>
<td>powerdns</td>
<td>180415</td>
<td>37</td>
<td>238</td>
<td>455</td>
<td>745</td>
<td>1467</td>
<td>2330</td>
<td>6249</td>
<td>10001</td>
<td>748</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>iij</td>
<td>106336</td>
<td>50</td>
<td>494</td>
<td>825</td>
<td>1356</td>
<td>2290</td>
<td>3619</td>
<td>7438</td>
<td>10021</td>
<td>1204</td>
<td>428</td>
<td></td>
</tr>
<tr>
<td>t53</td>
<td>105285</td>
<td>57</td>
<td>404</td>
<td>844</td>
<td>1508</td>
<td>2917</td>
<td>4352</td>
<td>7785</td>
<td>10037</td>
<td>1291</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>onion-cf</td>
<td>53082</td>
<td>194</td>
<td>876</td>
<td>1563</td>
<td>2534</td>
<td>5535</td>
<td>6988</td>
<td>9102</td>
<td>10218</td>
<td>2224</td>
<td>1484</td>
<td></td>
</tr>
</tbody>
</table>
It turns out that some people live with worse performance, day-in, day-out
100 lookups of random IPv4s; DoHoT in red

mean (n=5) time to perform 100 separate *dig -x* of random IPv4 addresses
It turns out that some people choose latency to obtain value
Some people filter their DNS, who knew?

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>dr1a</td>
<td>30</td>
<td>myself</td>
<td>125</td>
<td>104</td>
<td>51</td>
<td>84</td>
<td>82</td>
<td>51</td>
<td>125</td>
<td>89.2</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>am1a</td>
<td>20</td>
<td>70</td>
<td>dohoh</td>
<td>122</td>
<td>88</td>
<td>103</td>
<td>106</td>
<td>66</td>
<td>66</td>
<td>122</td>
</tr>
<tr>
<td>28</td>
<td>db1a</td>
<td>20</td>
<td>200</td>
<td>pihole-cloudflare</td>
<td>89</td>
<td>84</td>
<td>108</td>
<td>80</td>
<td>125</td>
<td>80</td>
<td>125</td>
</tr>
<tr>
<td>29</td>
<td>jr1d</td>
<td>100</td>
<td>1000</td>
<td>cloudflare</td>
<td>115</td>
<td>94</td>
<td>101</td>
<td>82</td>
<td>111</td>
<td>82</td>
<td>115</td>
</tr>
<tr>
<td>30</td>
<td>le1h</td>
<td>100</td>
<td>1000</td>
<td>cloudflare</td>
<td>102</td>
<td>158</td>
<td>109</td>
<td>110</td>
<td>57</td>
<td>57</td>
<td>158</td>
</tr>
<tr>
<td>31</td>
<td>jr1f</td>
<td>100</td>
<td>1000</td>
<td>cloudflare</td>
<td>92</td>
<td>91</td>
<td>125</td>
<td>113</td>
<td>123</td>
<td>91</td>
<td>125</td>
</tr>
<tr>
<td>32</td>
<td>jr1b</td>
<td>100</td>
<td>1000</td>
<td>quad9_unfiltered</td>
<td>117</td>
<td>155</td>
<td>137</td>
<td>125</td>
<td>71</td>
<td>71</td>
<td>155</td>
</tr>
<tr>
<td>33</td>
<td>db1b</td>
<td>20</td>
<td>200</td>
<td>pihole-quad9</td>
<td>212</td>
<td>87</td>
<td>101</td>
<td>178</td>
<td>52</td>
<td>52</td>
<td>212</td>
</tr>
<tr>
<td>34</td>
<td>ya1a</td>
<td>10</td>
<td>100</td>
<td>cloudflare</td>
<td>132</td>
<td>133</td>
<td>151</td>
<td>129</td>
<td>135</td>
<td>129</td>
<td>151</td>
</tr>
</tbody>
</table>
It turns out that presuming to argue 5ms vs 50ms vs: 500ms DNS latency, is a presumptuous act of tech privilege
minimum latency isn't everything

latency is only a fraction of the user experience and value proposition

... albeit one that's easy to measure and compare

... which probably explains why we are so hung up about it
If you accept this perspective, why not invest the latency budget in order to pursue better privacy value?
DoHoT Rationale
Assume for simplicity that ...

In a domestic context, or similar ...

- ISP blocks/allows are by port, or by tuples of \{ip, net\} address & port
- HTTPS is not "wildcard" blockable (cf: "port 53 and not host A.B.C.D")
  - ... as it is the "raison d'être" of modern communication ...
- Tor is "hard" to globally surveil, and resistant to block, collusion or subpoena
  - ... Tor's relay cloud & "triple-hop" system greatly complicates correlation ...
  - ... bad actors can run bad relays, but Tor actively hunts / resists them ...
- HTTPS adequately assures identity via certificates
DoHoT was designed to address ...

a privacy-invasive threat model based around actors who ...

1. may surveil my network links
2. block my queries to my chosen proxies or resolvers
3. tamper with those queries
4. block responses from my chosen proxies or resolvers
5. tamper with those responses
6. pretend to be my chosen proxies or resolvers
7. may learn that my identity is/was associated with particular queries or responses
8. may surveil the path to and beyond my chosen proxy and resolver, pursuing 7. (e.g. correlation attack)
9. may collude with, or FISA / subpoena logs from, my proxies or resolvers, pursuing 7.
Comparative Analysis
According to the DoHoT threat model ...

• **Do53** risks all of these;
  egregiously insecure yet somehow ubiquitous

• **DoT** risks 2, 4, 7, 7+8, 7+9;
  port blocks, second-party surveillance, third-party surveillance or collusion

• **DoH** risks 7, 7+8, 7+9;
  second-party surveillance, third-party surveillance or collusion

• **ODNS** risks *2, *4, 7+8, 7+9
  *maybe* port blocks, third-party surveillance or collusion

• **ODoH** risks 7+8, 7+9
  third-party surveillance or collusion; proper use requires an informed user

• **DoHoT** risks ... arguably **none of the above**, unless Tor relays become severely compromised
ODxx (ODNS and ODoH) are interesting but suffer from issues that Tor actively works to address

- Designers appear to have made choices primarily to minimise latency impact
- Choices include: tiers of single-layer proxies that may be open to:
  - selective ip-blocks (cf: Russia/AWS, Iran/Signal, vs: Tor bridges, obs4proxy, ...)
  - "both sides" surveillance with timing & metadata, to synthesise collusion
- (ODoH) user may accidentally choose proxy that is run by the same organisation which runs their resolver, yielding unintentional self-collusion:
  - "Choose a different proxy orgo from your resolver orgo, or bad things may happen"
- User education is hard and expensive and easy to miss or mess up
Consequently ...
If you need strong DNS privacy, then deploy DoHoT

- It's free, it exists, it requires no new tooling, and it's easy
  - You are in control, you can roll your own
- It's an operational practise rather than a protocol
  - downside: less opportunity for publication in research journals
    - maybe some research on cache-tuning, but maybe "why bother?"
    - some "standardisation" would be good to increase uniformity of queries
- If performance is on par with Pi-hole, there are already privacy-centric communities who would value the latency-privacy tradeoff
Architecture
I set up a copy of `dnscrypt-proxy` configured as a stub resolver.

- presented to the LAN as a DHCP Do53 DNS Service, enforced by firewall
- configured to make all resolution requests over Tor (via SOCKS5)
- attempting to minimise fingerprintable metadata (e.g. session tix, ciphers)
- into a load-balanced pool of public DoH servers
- which are chosen to offer both DNSSEC and a promise of "no filters"

... and that's all.
Terrible Network Diagram

- Client
- Stub
- Tor
- DoH

The diagram shows a client connected to a stub, which in turn connects to a Tor node. The Tor node then connects to five DoH nodes, indicating a possible misdirection or security issue.
Rhetorical Question
If we can address the entire threat model within a reasonable latency budget, why address a mere subset of it?
Utter Strawman Answers ...
We should solve privacy centrally, not on the client-side ...

Every solution suggests at least client code-changes, if not use of proxy or stub resolvers. Also: isn't DNS meant to be a "distributed" protocol? Doesn't that also involve the clients?
We need to solve this for everyone, so we need a privacy solution that scales ...

That's admirable, but what's your baseline threat model and value proposition? Latency?
If DNS "goes dark" then "the authorities" will be forced to regulate it more tightly ...
(e.g. TLS1.3 vs: ETS/eTLS)

The capabilities of democratic states today will be those of totalitarian despots tomorrow. Personally, I feel that we should plan for, and proactively mitigate the latter.
We reject this "NSA-inspired" threat model as being {unrealistic, impolitic, illegal, ...}

Fine, it'll be incumbent upon you to explain to people what you're NOT defending against, and why.
Your stats are inadequate / don't stack up!

Awesome, go measure and publish. We need diverse, holistic, value-centric user experience data.
Other?

I'd love to see fresh consideration.
If you only remember 1 slide ...
Please stop thinking of latency as cost
Please consider it a budget to offer value

github.com/alecmuffett/dohot