Devil's Advocacy for DoH

Aydın Mercan

OARC 44 — 2025-02-07

aydin@isc.org

About Myself

- BIND 9 SWE
- Cryptography at METU
- Located in Turkey
- DNS, censorship and privacy has daily relevance
- New to the industry/everything but with a different perspective on the problem

Figure 1: archive.is/5qjKY

But why defend DoH?

It’s no secret that DoH has a mixed reputation among the DNS community.

Common thoughts from network operators and server implementers:

- I need to block unwanted lookups but now I can’t see them!
- Where is the privacy? Everything is offloaded to `$BIGCORP`!
- Why does my DNS server needs to parse HTTP?

Thinking About Censorship

Censorship isn't homogeneous around the world.

- Generally motivated politically with a weaponized legal system
- Usually state mandated but offloaded to ISPs
- With exceptions, prevalent in not-so-well-off countries

Censorship itself is costly:

- **Can I afford the activity lost?** e.g. Week long ban on Instagram: 10% e-commerce by volume and 0.5B USD [1]
- **Do I have the muscle?** e.g. Forced MITM CAs pushed back by market force on multiple occasions [2], [3]
- **How much can I finance?** Cost of equipment, personnel and adapting to new bypasses
- **Do I want censor myself too?** Bureaucracy and technical staff also want to enjoy the banned content

Take it as an assumption, find me later if you disagree.

Should we care at all?

- Not every bypass includes DNS traffic. Solutions outside VPN-like tunneling exist.
- DNS is *very* sensitive to latency, modern sites keep inflating the lookup volume. Quality-of-life degradation is noticeable.
- Heterogeneous remedies, not every endpoint needs a bypass.

Why does DoH help?

DoT/DNSCrypt works on an explicit permission model. These encrypted DNS transports themselves can be censored by dropping their traffic.

Despite DoH looking like regular web traffic, it doesn't actually do much on top of DoT. However, these subtle changes are powerful:

- Port 443
- ALPN (Application-Layer Protocol Negotiation) values of `h2` or `http/1.1`
- Ideally hosted alongside big collateral damage

This is where Things Fall Apart

DoH is a target and generic censorship methods are effective:

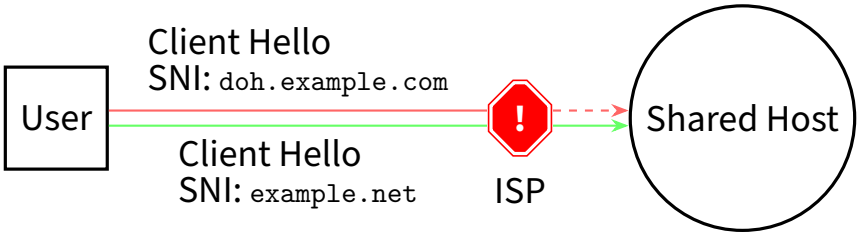
- IP Blocking
- SNI Based Filtering
- Traffic Analysis

Big Resolver is also a Big Target

- Catchy endpoints **beg** to be blocklisted by address.
- Already seen in reality: big resolvers are commonly blocked [4]
- Small DoH setups are likely to work for some time or scale threshold
- Scattering big resolvers doesn't have to mean more providing parties, just more resolvers (relax with the anycast?)

SNI Filtering

Integral part of TLS censorship, by shoehorning DNS we automatically get hit by the same method. [4]



Traffic Analysis

- Final frontier of censorship but a tale as old as myself. [5]
- DNS traffic will always be DNS traffic by itself, no matter the transport
- The mechanism must scale to every single user
- Companies, not too unreachable; countries, very hard to realize
- Painful bypasses to work around, generally includes huge volumes of empty traffic to fool analysis

~~An Escalated~~ Better Future

Existing development(s) that might help:

- ECH

What can be done:

- DoT ALPN Uplifting
- Obfuscation
- SNI Siblings

Common Theme

Don’t overfit, raise the bar or create powerful building blocks without overwhelming base traffic. (re: padding)

ECH

Encrypted Client Hello (née ESNI) hides the actual SNI alongside other information during Client Hello [6]

Not made with censorship in mind but removes the biggest vector.

All or Nothing

Allow ECH traffic de-facto fallback and all is for nothing. Standoff between different parties.

ALPN Uplifting

- If ECH is adopted, DoT can be uplifted to current status of DoH.
- `dot` in ALPN = throw away the HTTP parser.

Otherwise, a non-standard but similar solution: straight up lie.

Domain forwarding & ALPN forwarding: will upset everyone in the room but it will nullify most methods.

Obfuscation

Cryptographic indistinguishability possible with Elligator etc. Can be used to obfuscate DNS traffic in every point.

- No answer to post-bootstrap patterns
- Slowly becoming yet another encrypted DNS transport
- Maybe distinguishable resolver deployments?

SNI Siblings

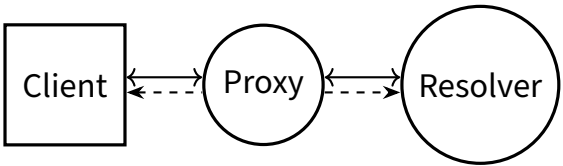


Figure 2: Simplified view of ODoH

Oblivious DoH:

- Privacy improvement through proxies and HPKE (Hybrid Public Key Encryption)
- Layers from resolver's perspective

SNI Siblings

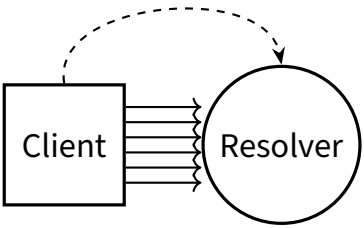


Figure 3: Simplified idea of SNI Siblings

- Stable address-SNI pairs are a liability
- Layers from inspectors' perspective
- Opt-in auto-discovery of new pairs
- Ideally, SNI's are fake without sticking out

SNI Siblings: How?

HTTP Header `SNI-Siblings`?

⇒ `SNI-Siblings: not-dns-news.com,dns-cooking.net,baldurs-dns-three.com:162.159.61.4`

\+ Easy to implement and ignore

\- DoH Specific

SNI Siblings: How?

New RR `SIBLINGRESOLVER`?

- ⇒ Return it as you do with `RRSIG`s
- \+ Pure DNS
- \- Size bloat for a lot of resolvers
- \- Potentially fake entries get involved with zones now
- \- Implementation involves everyone
- \- Might be painful to use with DNSSEC or effectively incompatible

SNI Siblings: How?

SVCB Parameter Key `sni-siblings`?

- ⇒ Fetch siblings from the resolver
- \+ Doesn’t pollute query sizes
- \+ Only interested parties need to implement it
- \- Also might be painful to use with DNSSEC if desired

Conclusion

- Censorship is a problem in DNS that shouldn't be ignored
- DoH is the best we have so far yet it still has blatant shortcomings
- Standards can help with building blocks to a censorship-resistant DNS infrastructure
- SNI Siblings to help bootstrapped resolvers navigate, how horrible is it?

Questions?

Thank you for listening!

Sources

[1] M. Gümüş, “Instagram’a erişim engeli: Platformdan gelir elde edenler ne kadar zarar etti?” (Sep. 2024), [Online]. Available: https://medyascope.tv/2024/08/02/instagrama-erisim-engeli-platformdan-gelir-elde-edenler-ne-kadar-zarar-etti/.

[2] A. Whalley, “Protecting Chrome users in Kazakhstan,” (Sep. 2019), [Online]. Available: https://security.googleblog.com/2019/08/protecting-chrome-users-in-kazakhstan.html.

Sources

[3] W. Thayer, “Protecting our Users in Kazakhstan,” (Sep. 2019), [Online]. Available: https://blog.mozilla.org/security/2019/08/21/protecting-our-users-in-kazakhstan/.

[4] S. Basso, “Measuring DoT/DoH Blocking Using OONI Probe: a Preliminary Study,”, Feb. 2021. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/dnspriv21-02-paper.pdf.

Sources

[5] A. Back, U. Möller, and A. Stiglic, “Traffic analysis attacks and trade-offs in anonymity providing systems,” in Information Hiding, I. S. Moskowitz, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 245–257, ISBN: 978-3-540-45496-0.

[6] E. Rescorla, K. Oku, N. Sullivan, and C. A. Wood, “TLS Encrypted Client Hello,” Internet Engineering Task Force, Internet-Draft draft-ietf-tls-esni-22, Sep. 2024, Work in Progress, 52 pp. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/22/.