New Ways to Find a DoH Resolver

Paul Hoffman

ICANN 63

11 March 2019

ICANN

Quick introduction to DNS over HTTPS (DoH)

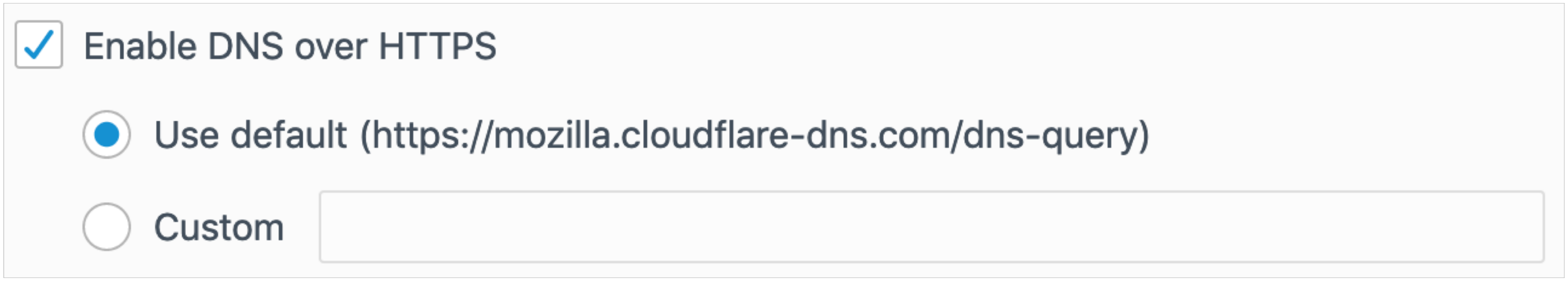
- Different than DNS-over-TLS (DoT) because the traffic under TLS is normal HTTP traffic that is specific to DNS requests and responses
- Mostly intended for browsers because they already know how to create HTTPS requests and process the results
- Could also be useful for web applications (JavaScript)
- Standardized last year as RFC 8484
- DoH raises some policy issues, but those are barely being mentioned here
  - Emerging Identifiers Technology tomorrow

Choosing a DoH server

- The standard does not mandate how to choose
- There were many assumptions made during the development of the standard, but we were wrong
- The expectation was that there would be many listed for the user to choose from
- Mozilla Firefox now has DoH visible to users in the normal UI, Google Chrome does not
- Web applications (JavaScript) have no user interface, so they just specify the DoH server they want
- After DoH was standardized, there was a desire to make it easy to find the DoH server associated with a user’s resolver

How Firefox chooses resolvers today

- Preferences → General → Network Settings → Settings



☑ Enable DNS over HTTPS

● Use default (https://mozilla.cloudflare-dns.com/dns-query)

○ Custom

- There is only one DoH server listed, but more might be added in the future

- Mozilla says that there is a program that allows other public DoH servers to get added to the list

- The user (or their admin) can add a custom DoH server in the dialog

Finding the DoH server associated with a resolver

- Users already have a resolver associated with the OS
- That resolver might also have a DoH server on it, or the resolver operator might have a chosen DoH server
- Proposals in the IETF's DOH Working Group
- Special-use domain name
  - `resolver-associated-doh.arpa`
- A well-known URI on a web server on the resolver:
  - `https://IPADDR/.well-known/doh-servers-associated/`

Next steps

- More discussion in the DOH Working Group
- Implementation by browser vendors
- Figuring out how to make this option available and understandable to users
- Dealing with the larger policy questions that DoH presents, and whether allowing a user to specify that the browser should use the DoH server associated with its resolver is sufficient to answer those questions
  - Don’t forget web applications...

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: paul.hoffman@icann.org

@icann	linkedin/company/icann
facebook.com/icannorg	slideshare/icannpresentations
youtube.com/icannnews	soundcloud/icann
flickr.com/icann	instagram.com/icannorg