Cloudflare comments on Mozilla DNS-over-HTTPS Implementation

Cloudflare welcomes the opportunity to provide input to Mozilla's call for comments on DNS over HTTPS (DoH) and its Trusted Recursive Resolver (TRR). Cloudflare is proud to work alongside Mozilla to help develop, test, and deploy next-generation Internet standards. We are very excited about our collaborations to improve the protocols that help secure connections between browsers and websites, such as our partnership with regard to the TRR program.

We also applaud Mozilla's efforts to draw attention to the important role that data collection and retention, transparency, and blocking policies have on user privacy. Cloudflare shares Mozilla's commitment to strong data policies that limit the unnecessary collection of user data and provide transparency about a company's data practices. The technical nature of DNS services has too often made it difficult for users to understand the impact of data collection policies and practices. By requiring a set of minimum privacy standards, Mozilla has put a spotlight on how data is used, and how those practices can be improved.

Cloudflare believes it is possible both to provide additional privacy and security through the use of protocols such as DoH and to give users choices about how to control the information they see. We would encourage Mozilla to consider providing users with additional mechanisms for filtering content for those users who want to opt-in to those services.

Supporting ODoH

While Cloudflare made major steps towards supporting DoH at scale, we are aware of concerns over the centralization of DoH infrastructure. This issue was initially addressed through policy means; Mozilla's Trusted Recursive Resolver (TRR) agreement requires that DoH resolvers supported in Firefox agree to adhere to strict privacy guidelines. Additionally, more DoH partners have signed on, such as Comcast joining Mozilla's TRR in June 2020, a deployment advance that also serves to reduce DNS data centralization and gives users more choice about which resolvers to trust.

However, there are more ways in which DNS privacy can be enhanced, and Cloudflare took another incremental step in December 2020 by announcing support for Oblivious DoH (ODoH). ODoH is a proposed DNS standard — co-authored by engineers from Cloudflare, Apple, and Fastly — that separates IP addresses from queries, so that no single entity can see both at the same time. ODoH requires a **proxy** as a key part of the communication path between client and resolver, with encryption ensuring that the proxy does not know the contents of the DNS query (only where to send it), and the resolver knowing what the query is but not who originally requested it (only the *proxy*'s IP address). Barring collusion between the proxy and the resolver, the identity of the requester and the content of the request are unlinkable.

As with DoH, successful deployment requires partners. A key component of ODoH is a proxy that is disjoint from the target resolver. Cloudflare is working with several leading proxy

partners -- currently PCCW, SURF, and Equinix -- who are equally committed to privacy, and hopes to see this list grow.

Similar to DoH, real user privacy impacts with ODoH can only be achieved with significant adoption of the protocol. There are a number of steps required to facilitate widespread adoption, some of which can be assisted through browser changes. For example, there is the issue of how to discover proxies and targets that support ODoH; it is possible for an interested party to host a centralized list, which could be bootstrapped in a browser such as Firefox. In addition, browser changes in Firefox could include support for ODoH from the browser itself (similar to DoH). This would prevent users from having to run a system resolver that supports the ODoH protocol. Such changes would support a more seamless ODoH rollout.

****

Cloudflare looks forward to continuing to work with Mozilla on the TRR, and on developing and deploying new privacy-enhancing protocols.