Verisign Comments on Mozilla's DNS-over-HTTPS Implementation

Verisign Technical Note
January 20, 2021

This note is in response to Mozilla's request for public comment on areas related to security, privacy, and operational concerns of the DNS ecosystem as a result of Mozilla's implementation of DNS-over-HTTPS.

Recursive resolvers play a pivotal role in the DNS ecosystem as the primary interface between operating systems, browsers (such as Firefox), and other applications, and the authoritative name servers in the global DNS. While recursive resolvers, like all components of the DNS ecosystem, follow the various DNS protocol standards, these components generally have not been subject to specific policies on their operations. This flexibility in implementation reflects the "permissionless" innovation that has made the internet successful, but it also contrasts with the well-defined policies that are in place for other components, namely the root servers and the top-level domain (TLD) servers.

While the role of similarly defined policies for recursive resolvers is not yet clear, what is becoming clear is that it's important for users and organizations to have a better understanding of the attributes of the recursive resolvers they interact with. This is especially important as users are offered more choices of recursive resolvers, as browsers and other clients make it easier for users to make these choices, and new DNS capabilities emerge that can make it possible for such choices to be made automatically by clients in support of user and organizational objectives.

For all these reasons, it's encouraging to see Mozilla taking a leadership role in defining workable expectations for the recursive resolvers that interact with the Firefox browser via DNS-over-HTTPS. Mozilla's publication of requirements for Trusted Recursive Resolver (TRR) partners is an important step in the direction of greater transparency and accountability for these components, providing a helpful reference for improving resolver practices across the industry.

The IETF has been working on consensus-driven standards, recommendations, and best practices, such as those for recursive resolvers and other DNS ecosystem components for many years. To maximize the impact of the TRR program and the interoperability of participating resolvers, Verisign strongly encourages Mozilla to align with the guidance put forward by the IETF. If this is not possible, then Mozilla's policies ought to clearly state agreements and disagreements with those documents.

For example, the IETF recently published RFC 8932, "Recommendations for DNS Privacy Service Operators" (BCP 232, October 2020)[1]. Mozilla's requirements for Trusted Recursive Resolver (TRR) partners should be brought into conformance with the technical recommendations and operational guidelines set out in sections 5 and 6 of that document.

[1] https://tools.ietf.org/html/rfc8932

A recent study published in the Journal of Cyber Policy[2] highlights the risks and concerns that recursive resolver market consolidation places on whole of the DNS ecosystem – an outcome that resolver partnership programs including initiatives such as Mozilla's TRR may well facilitate.

Verisign encourages Mozilla to engage with the DNS community to better understand and assess the operational and systemic implications of DNS consolidation and other DNS ecosystem changes, which can thereby improve the TRR program and policy requirements. In particular, we encourage Mozilla to consider the impact that DNS encryption on the client-to-resolver exchange can have on traditional network monitoring capabilities, as well as the consequences of the bifurcation of DNS resolution between the traditional operating system stack and the application layer.

"Trusted" is a designation that carries significant weight. We appreciate Mozilla's stated commitment to policy enforcement, including the intent "to publicly document violations of this Policy and take additional actions if necessary."[3]

One of the most important, and often unstated, expectations of a recursive resolver is that, unless otherwise stated, the resolver is a *DNS* resolver — that is, by default, the resolver performs DNS resolution on behalf of its clients with respect to the global DNS root. This assumption becomes especially prominent with the "trusted" designation. As a leading specification of such expectations, it's important that the TRR policy state this assumption explicitly. TRR partners should be required to adhere to ICANN's ICP-3 document[4] in respecting a single, authoritative root for the DNS, i.e., no alternative roots or new distributed naming systems that have not gone through an ICANN multistakeholder process. Proposals to expand the DNS represent likely sources of confusion and potential security threats.[5] Mozilla has already followed ICANN's ICP-3 approach with respect to its management of the Public Suffix List.[6]

Mozilla should detail additional commitments, technologies, and techniques that the TRR policy requires to improve the trustworthiness and integrity of the DNS. For instance, TRR partners should be required to implement DNSSEC validation for their clients, in order to ensure the integrity of responses. The TRR policy should also consider requiring providers to assure regular DNS-related security audits, e.g., mitigating recent cache poisoning[7] vulnerabilities.

Verisign applauds the existing technical requirements for TRRs[8] to reduce the disclosure of sensitive information by implementing query name minimization[9] [10]and also not forwarding EDNS(0) Client

---

[2] Roxana Radu & Michael Hausing, "Consolidation in the DNS resolver market – how much, how fast, how dangerous?" in Journal of Cyber Policy, Volume 5, 2020, https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1722191

[3] https://wiki.mozilla.org/Security/DOH-resolver-policy#Enforcement

[4] https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en

[5] C. Patsakis, et al., "Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS," in *IEEE Access*, vol. 8, pp. 118559-118571, 2020, doi: 10.1109/ACCESS.2020.3004727 https://ieeexplore.ieee.org/document/9123760

[6] https://github.com/publicsuffix/list/wiki/Guidelines

[7] Keyu Man et al. "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels" (2020-10) CCS '20, https://dl.acm.org/doi/10.1145/3372297.3417280

[8] https://wiki.mozilla.org/Security/DOH-resolver-policy

[9] RFC 7816, "DNS Query Name Minimisation to Improve Privacy" https://tools.ietf.org/html/rfc7816

[10] M. Thomas, "Maximizing Qname Minimization: A New Chapter in DNS Protocol Evolution," Verisign Blog, September 16, 2020, https://blog.verisign.com/security/maximizing-qname-minimization-a-new-chapter-in-dns-protocol-evolution/

Subnet (ECS) information[11] without appropriate protections[12]. A TRR partner should also consider policies detailed in "Aggressive Use of DNSSEC-Validated Cache" (RFC 8198)[13] and "NXDOMAIN: There Really Is Nothing Underneath" (RFC 8020)[14] as a way of further reducing the sensitivity of information on the resolver-to-root and resolver-to-TLD exchanges. The TRR policy should also consider requiring additional client query obfuscation techniques as specified by RFC 8932 section 5.3.2[15], as well as techniques to mitigate cache snooping[16]. "Minimization" techniques of these various kinds can be particularly attractive at the root and TLD authoritative levels because of their low operational impact, compared to encryption on the resolver-to-authoritative exchange[17].

Finally, we encourage Mozilla to consider the concerns mentioned in RFC 7754 "Technical Considerations for Internet Service Blocking and Filtering,"[18] which state, among other things, that blocking and filtering of DNS queries should be implemented narrowly. As such, we also recommend consideration of the relevant concerns and commitments identified by ICANN committees' work on DNS blocking and filtering[19] in the context of requirements for the TRR program.

As stewards of the Internet infrastructure, we appreciate Mozilla's efforts to strengthen the DNS ecosystem. This ecosystem is critical to the secure and reliable operation of the global Internet upon which billions of people worldwide depend, every second of every day. We look forward to working with Mozilla and the DNS community to ensure the deployment of DNS capabilities including encryption continue to enhance this fundamental objective.

[11] See RFC 7871, "Client Subnet in DNS Queries" https://tools.ietf.org/html/rfc7871
[12] https://wiki.mozilla.org/Security/DOH-resolver-policy#Privacy_Requirements
[13] https://tools.ietf.org/html/rfc8198
[14] https://tools.ietf.org/html/rfc8020
[15] https://www.rfc-editor.org/rfc/rfc8932.html#name-client-query-obfuscation
[16] For a recent research example of the feasibility of cache snooping, see Randall, Audrey, et al., "Trufflehunter: Cache Snooping Rare Domains at Large Public DNS Resolvers" (IMC 2020), https://www.sysnet.ucsd.edu/~voelker/pubs/truffle-imc20.pdf
[17] B. Kaliski. "A Balanced DNS Information Protection Strategy: Minimize at Root and TLD, Encrypt When Needed Elsewhere," Verisign Blog, December 7, 2020, https://blog.verisign.com/security/a-balanced-dns-information-protection-strategy-minimize-at-root-and-tld-encrypt-when-needed-elsewhere/
[18] https://tools.ietf.org/html/rfc7754
[19] ICANN Security and Stability Advisory Committee, "SAC050: DNS Blocking: Benefits Versus Harm" (2011-06-14), https://www.icann.org/en/system/files/files/sac-050-en.pdf; "SAC056: SSAC Advisory on Impacts of Content Blocking via the Domain Name System" (2012-10-09) https://www.icann.org/en/system/files/files/sac-056-en.pdf; ICANN Root Server System Advisory Committee, "RSSAC037: A Proposed Governance Model for the DNS Root Server System" (2018-06-12) §3.7, https://www.icann.org/en/system/files/files/rssac-037-15jun18-en.pdf; "Proposed Memorandum of Understanding (MOU) / Letter of Intent (LOI)" (2020-10-06) §5.2.1.2 https://www.icann.org/en/system/files/files/letter-of-intent-06oct20-en.pdf

