DNS over HTTPS

Internet Service Providers and Connectivity Providers Constituency (ISPCP) statement

(2020-05-29)

Introduction

DNS over HTTPS (**DoH**) is a protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol. A goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks by using the HTTPS protocol to encrypt the data between the DoH client and the DoH-based DNS resolver. In addition to improving security, another goal of DNS over HTTPS is to improve performance.
[https://en.wikipedia.org/wiki/DNS_over_HTTPS].

In 2019 and at several ICANN meetings, the question of DNS over HTTPS (DoH) deployment was brought to the attention of the ICANN community. Given the potential impacts this deployment has for Internet Service Providers and Connectivity Providers, the ISPCP would like to offer the following as the view of the constituency on this topic. The ISPCP appreciates that several DoH-related initiatives have been launched to address some of the issues that DoH raises, and in this respect, a number of unknowns remains as to what such initiatives can achieve, what the deployment models/policy, and the timeline or conditions of this deployment may be. The following statement is therefore offered in this context with the hope that it helps progress this work and eventually deploy the protocol for the benefit of Internet users in general and ISP customers in particular.

Guiding principles for the ISPCP:

- The protocol may provide benefits to the security and privacy of DNS data on the interface
- The models of deployments for the protocol have generated concerns notably on the impact for DNS resolvers provided by ISPs [ETNO, Open-xchange, CENTR, Centralized DNS over HTTPS (DoH) Implementation Issues and Risks, DoH Considerations for Operator Networks]. Concerns are mostly related to
    - the consequences of the joint use of DoH and public resolvers
    - and in particular the fact that the some deployments of DoH may be used to enforce a change in browser's settings to use an alternative resolver to the currently defined (unencrypted) DNS resolver

Impact on ISPs

In particular, the following consequences have been documented by ISPs and are largely described in the papers referenced above:

- technical impacts: CDN selection, DNS query logging, load balancing, DNS-based address mapping for IPv4/IPv6 coexistence, joint use of NAT and stub resolvers, malware detection, enterprise/split DNS
- Regulatory and Policy Considerations: administrative block-lists of domain names associated with hate speech or child pornography, parental control, data privacy

The ISPCP shares these concerns and considers that the deployment of DoH must not have a detrimental impact in these areas.

Regarding the work in progress, the ISPCP commends the on-going technical work in the including EDDI and IETF ADD work in progress, but notes the limited scope in terms of policy work. For example, the draft charter states that:

- "*the working group will focus on discovery and selection of DNS resolvers by DNS clients […] supporting both encrypted and unencrypted resolvers* "
- "*Recommendations about specific policies for clients or servers is out of scope [of the work of the proposed working group]*"

The ISPCP is also aware that the "same provider DoH auto upgrade" approach suggested by some application / OS provider based on the look up of current DNS resolver public IP addresses will not work for large volumes of broadband ISP customers served by stub resolvers in customer premise equipment that only provide clients with a private IP address for the stub resolver. The ISPCP would welcome the development of a context aware DoH discovery standard that will work across all customer scenarios.
The ISPCP considers however that the deployment of DoH raises a number of policy issues, and notably those listed above.

Regarding the policy that determines the choice of the DNS resolver, the ISPCP supports the approach that the upgrade to DoH should not change the user's DNS resolver choice, i.e.:

- selection policy
    - use DoH when it is available on the DNS resolver configured in the browser/Operating System
    - remain unencrypted if DoH is not available on this resolver – unless the user has explicitly chosen to do otherwise
        - in particular not redirect user DNS traffic to a DoH compliant resolver owned by/partnered with the browser/OS maker by changing the user's DNS resolver provider
- maintain/define a long term mechanism to opt-out of DoH deployment (e.g., "canary domain name")

The rationale is the following:

- A well-functioning DNS resolver is a condition for Internet connectivity:

- ISPs have direct relationship with their customers who would turn to the ISP support if Internet access – the above maintain some control from the ISP
- IPSs are evaluated (or have regulatory constraints) on access to content conditioned by the performance of their DNS resolvers

Regarding the role of ICANN and the potential impact of DoH, the ISPCP notes that ISPs provide a uniform access to all the DNS Top Level Domain names and their DNS cache servers rely on IANA as the provider of the Root Zone Database; the legitimacy of ICANN is ultimately ensured by the endorsement of the ecosystem of DNS resolvers.
Although the impacts of DoH will depend on the policy applied to select the DoH provider, some models of deployment whereby the DNS/DoH resolver function is concentrated on a very limited number of public resolvers may affect ICANN in various ways, for example:

- the ability to change this and offer them a potential opportunity for defining a parallel “public” namespace/TLDs.
- the centralisation of the client-to-resolver DNS queries on a limited number of players, which may ultimately affect the stability and security of the DNS, and ICANN's key security, stability, and resiliency activities in particular.

References

ETNO, ETNO position on DNS over https (DoH),
https://etno.eu/library/positionpapers/401-etno-position-on-dns-over-https-doh.html

Open-xchange https://www.open-xchange.com, white paper DNS-over-HTTPS and the Rise of OTT DNS
http://open-xchange.com/fileadmin/user_upload/Blog/DoH_Public_Policy_Briefing.pdf

CENTR Issue Paper on DNS over HTTPs, June 2019,
https://centr.org/library/library/policy-document/centr-issue-paper-on-dns-over-https.html

Security & Stability Advisory Committee (SSAC) SAC-109 "The Implications of DNS over HTTPS and DNS over TLS"
https://www.icann.org/en/system/files/files/sac-109-en.pdf