Le protocole DoH et pourquoi il y a tant de discussions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 septembre 2019

https://www.bortzmeyer.org/doh-et-ses-adversaires.html

Le 6 septembre dernier, Mozilla a annoncé <https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/> l'activation du protocole DoH par défaut dans leur navigateur Firefox. (Et, même si ce n'est pas explicite, il est prévu que ce soit par défaut avec le résolveur de Cloudflare.) Cette annonce a suscité beaucoup de discussions, souvent confuses et mal informées. Cet article a pour but d'expliquer la question de DoH, et de clarifier le débat.

DoH veut dire « DNS sur HTTPS ». Ce protocole, normalisé dans le RFC 8484 [1], permet l'encapsulation de requêtes et de réponses DNS dans un canal cryptographique HTTPS menant au résolveur. Le but est double : empêcher un tiers de lire les requêtes DNS, qui sont souvent révélatrices (cf. RFC 7626), et protéger les réponses DNS contre des modifications, faites par exemple à des fins de censure <https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes>. Le statu quo (laisser le DNS être le seul protocole important qui ne soit pas protégé par la cryptographie) n'est pas tolérable, et il faut donc féliciter Mozilla d'avoir agi. Mais cela ne veut pas dire que tout soit parfait dans leur décision. Notamment, DoH, comme toutes les solutions reposant sur TLS, ne fait que sécuriser le canal de communication contre la surveillance et la manipulation par un tiers. Il ne garantit pas que le partenaire à l'autre bout du canal est gentil. Faire du DoH vers un méchant résolveur ne serait donc pas très utile, et le choix du résolveur est donc crucial.

Voyons maintenant les principales critiques qui ont été faites contre DoH et/ou contre la décision de Mozilla (si j'en ai oublié, écrivez-moi). Rappelez-vous bien que le débat est très confus, en partie par mauvaise foi de certains, en partie par ignorance (du DNS ou de la sécurité). Notamment, certaines des critiques formulées contre DoH n'ont rien à voir avec DoH mais, par exemple, avec un aspect spécifique de la décision de Mozilla. Et, parfois, d'autres protocoles, comme DoT (DNS sur TLS, RFC 7858), présentent exactement les mêmes propriétés.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8484.txt

— DoH empêche (en réalité : rend plus difficile) d'appliquer une politique, par exemple de censurer Sci-Hub. Aucun doute à ce sujet, c'est même le but explicite. Ceux qui le présentent comme un inconvénient avouent franchement que leur but est le contrôle des utilisateurs. L'IETF, qui a normalisé le protocole, travaille pour un Internet ouvert. Si vous voulez utiliser les technologies TCP/IP dans un réseau fermé, vous avez le droit, mais c'est à vous de trouver des solutions. Cette critique n'est pas spécifique à DoH, DoT offre exactement le même avantage (ou le même inconvénient, si on est du côté des censeurs).
— DoH empêche (en réalité : rend plus difficile) la surveillance des utilisateurs. L'examen des requêtes DNS peut être très révélateur (cf. RFC 7626) et être utilisé pour le bien (détection de l'activité de logiciels malveillants) ou pour le mal (repérer qui visite tel ou tel site Web). Là encore, c'est le but explicite de DoH (comme de TLS en général) de rendre plus difficile la surveillance (cf. RFC 7258). Cette critique n'est pas spécifique à DoH, DoT offre exactement le même avantage (ou le même inconvénient, si on est du côté des surveillants).
— On a souvent lu que DoH aggravait la centralisation (déjà bien trop importante) de l'Internet et notamment du Web. C'est une drôle de façon de poser le problème que de l'attribuer à DoH. Lorsque Gmail rassemble la majorité du courrier électronique (oui, même si vous n'êtes pas client de Gmail, et n'avez pas accepté leurs conditions d'utilisation, une bonne partie de votre courrier est chez Gmail), est-ce qu'on décrit ce problème comme étant de la faute de SMTP ? (Notez que la relation entre les protocoles et les résultats de leurs déploiements est une question complexe, cf. RFC 8280.) Je suis personnellement d'accord que ce n'est pas une bonne idée d'envoyer tout le trafic DNS à Cloudflare, mais la solution n'est pas de supprimer DoH, ou de le limiter à parler aux résolveurs des FAI, précisément ceux auxquels on ne fait pas forcément confiance <https://framablog.org/2018/11/29/ce-que-peut-faire-votre-fournisseur-dacces-a-linternet/>. La solution est au contraire de multiplier les serveurs DoH, de même que la solution aux réseaux sociaux centralisés est d'avoir plein d'instances décentralisées. C'est ce que je fais avec mon résolveur DoH personnel <https://www.bortzmeyer.org/doh-bortzmeyer-fr-policy.html>, c'est ce que font, en plus sérieux, les CHATONS <https://chatons.org/>. Bref, la centralisation du Web autour d'une poignée de GAFA est un vrai problème, mais pas lié à DoH. Les résolveurs DNS publics, comme Google Public DNS <https://www.bortzmeyer.org/google-dns.html> posent le même problème.
— On a lu parfois que DoH diminuait la vie privée car HTTP est bavard, très bavard. Ainsi, une requête DNS contient très peu d'informations sur le client, alors que HTTP transmet plein d'informations inutiles et dangereuses comme `Accept-Language:` ou `User-Agent:`, qui peuvent servir à identifier un utilisateur <https://panopticlick.eff.org/>. Sans compter bien sûr les très dangereux biscuits (RFC 6265). Il s'agit là d'un vrai problème. Des solutions ont été proposées (cf. l'"*Internet-Draft*" `draft-dickinson-doh-dohpe`) mais n'ont guère suscité d'intérêt. C'est probablement l'une des deux seules critiques de DoH qui soit réellement spécifique à DoH (DoT n'a pas ce problème), le reste étant confusion et mauvaise foi.
— Un reproche plus conceptuel et abstrait qui a été fait à DoH (par exemple par Paul Vixie) est d'ordre architectural : selon cette vision, le DNS fait partie du plan de contrôle et pas du plan de données, ce qui fait qu'il doit être contrôlé par l'opérateur réseau, pas par l'utilisateur. Le positionnement du DNS ne fait pas l'objet d'un consensus : protocole situé dans la couche Application, il fait pourtant partie de l'infrastructure de l'Internet. Disons que cette ambiguïté est consubstantielle à l'Internet : plusieurs protocoles d'infrastructure (c'est aussi le cas de BGP) tournent dans la couche 7. Dans tous les cas, le DNS ne peut pas être vu comme purement technique (comme, par exemple, ARP), son utilisation massive pour la censure montre bien qu'il est aussi un protocole de contenu, et devrait donc être protégé contre la censure. Si les gens qui clament que le DNS fait partie de l'infrastructure et que l'utilisateur ne devrait pas pouvoir bricoler sa résolution DNS étaient cohérents, ils réclameraient également que les FAI s'engagent à ne jamais interférer (ce que suggérait l'IAB dans une récente déclaration <https://www.iab.org/documents/correspondence-reports-documents/2019-2/avoiding-unintended-harm-to-internet-infr>). Mais cela semble peu réaliste à court terme.
— Un autre reproche de nature architecturale a été fait à DoH : tout faire passer sur HTTPS n'est pas « propre ». Ce reproche est justifié du point de vue technique (l'Internet n'a pas été conçu pour fonctionner comme cela, normalement, les applications doivent tourner sur SCTP, TCP, UDP, pas

sur HTTPS). Mais, en pratique, « le bateau a déjà quitté le port », comme disent les anglophones. De plus en plus de réseaux bloquent tous les ports sauf 80 et 443 et, si on veut faire un protocole qui passe partout, il doit utiliser HTTPS. Si cela vous déplait, plaignez-vous aux gérants des points d'accès WiFi, pas à DoH. Notez que cette remarque est une des rares à être effectivement spécifique à DoH.

— Tel qu'il est mis en œuvre dans Firefox, DoH est fait par l'application, pas par le système d'exploitation (ce qu'on nomme parfois ADD, pour "*Applications Doing DNS*"). Ce n'est pas du tout une propriété de DoH, juste un choix de Firefox. Les nombreux schémas où on voit « avec DoH, c'est l'application qui fait les requêtes DNS » révèlent qu'ils ont été faits par des gens qui ne comprennent pas ce qu'est un protocole. DoH peut parfaitement être utilisé par les couches basses du système d'exploitation (par exemple, sur les systèmes qui ont le malheur d'utiliser systemd, par `systemd-resolve` ou, plus sérieusement, par un démon comme Stubby <`https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby`>). Le choix de Mozilla est à mon avis erroné, mais n'a rien à voir avec DoH. Là encore, rien de spécifique à DoH, une application a toujours pu faire des requêtes DNS directement avec UDP, ou utiliser DoT, ou avoir son propre protocole privé de résolution de noms (ce que font souvent les logiciels malveillants).
— Enfin, on lit parfois que DoH poserait des problèmes lorsque la réponse DNS dépend de la localisation du client (ce qui est courant avec les CDN). C'est un effet déplorable de la centralisation du Web : comme l'essentiel du trafic est concentré sur un petit nombre de sites, ces sites doivent se disperser sur la planète et utiliser des bricolages dans le DNS pour diriger le client vers « le plus proche », estimé en fonction de l'adresse IP du client. Si le résolveur est loin de l'utilisateur, on sera renvoyé vers un endroit sous-optimal. Il existe une solution technique (RFC 7871) mais elle est très dangereuse pour la vie privée, et c'est pour cela que Cloudflare, contrairement à Google, ne l'utilise actuellement pas. Ceci dit, cela n'a rien de spécifique à DoH, tout résolveur DNS public (notez que ce terme est défini dans le RFC 9499) soulève les mêmes questions (c'est également le cas si vous avez des noms de domaine privés, spécifiques à une organisation).

Articles intéressants sur le sujet :

— Wired a fait un article correct et exposant bien les différents points de vue <`https://www.wired.com/story/dns-over-https-encrypted-web/`>.

Et pour finir, une petite image (prise sur Wikimedia Commons <`https://commons.wikimedia.org/wiki/File:Scylla_and_Charybdis.jpg`>) du détroit de Messine où, selon les légendes, les marins qui tentaient d'éviter Scylla tombaient sur Charybde. Bref, ce n'est pas parce qu'on n'aime pas Cloudflare qu'il faut maintenir le statu-quo et continuer à envoyer ses requêtes DNS au résolveur fourni par le réseau d'accès