Exposé sur DoH (DNS sur HTTPS) aux JDLL

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 avril 2019. Dernière mise à jour le 9 avril 2019

https://www.bortzmeyer.org/doh-jdll.html

Comme chaque année, les Journées du Logiciel Libre <https://jdll.org/> à Lyon ont été passionnantes et très bien organisées. J'y ai fait un petit exposé sur une technique qui a fait un peu de bruit récemment, DoH (DNS sur HTTPS).

DoH a été normalisé dans le RFC 8484[1]. Cette technique permet de chiffrer le trafic DNS, afin d'échapper à la surveillance et à la modification du trafic. (DNSSEC permet de détecter ces modifications mais pas d'y échapper.) Elle suscite donc les réactions de ceux qui avaient pris l'habitude de regarder le trafic DNS, voire de changer les réponses.

Mais le déploiement de DoH soulève une autre question. Un acteur important, Mozilla, a choisi de configurer DoH par défaut dans son navigateur Firefox (ce qui se défend) mais également de désigner comme résolveur par défaut celui d'un GAFA, Cloudflare. Question vie privée, passer d'une surveillance et d'une censure par le FAI à une surveillance et peut-être demain une censure, par une entreprise capitaliste états-unienne n'est pas forcément un progrès...Il est donc important et urgent que des résolveurs DoH vraiment libres soient déployés par des acteurs non-GAFA, par exemple des chatons <https://chatons.org/>.

Les supports de mon exposé sont disponibles ici (en ligne sur https://www.bortzmeyer.org/files/doh-jdll.pdf) (ainsi que leur source (en ligne sur https://www.bortzmeyer.org/files/doh-jdll.tex)). La conférence a été filmée et la vidéo est sur PeerTube chez Benzo <https://tube.benzo.online/videos/watch/756a8447-5a27-408d-a513-611f0288e1dd> (cf. son article <https://tutox.fr/2019/04/20/doh-dns-over-tls-video/>) et chez GoogleTube <https://www.youtube.com/watch?v=Fp_0xT2oEbM&feature=youtu.be&t=9878>.

La démonstration de DoH a été faite avec un serveur DoH écrit en Python lors d'un hackathon à l'IETF <https://www.bortzmeyer.org/hackathon-ietf-101.html>, tournant sur https://doh.bortzmeyer.
Attention : non seulement ce serveur DoH est purement expérimental, et toujours en panne, mais en outre il n'offre aucune vie privée, je regarde tout le trafic. Voici par exemple ce qui s'affiche lorsqu'un client DoH a fait une requête pour jdll.org :

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

```
INFO: id 0
opcode QUERY
rcode NOERROR
flags RD
;QUESTION
jdll.org. IN A
;ANSWER
;AUTHORITY
;ADDITIONAL
[2019-04-09 18:55:36,513] 10.251.62.29:35552 GET / 2 200 42 870793
```

Le client DoH de test utilisé (développé au même hackathon <https://www.bortzmeyer.org/hackathon-ietf-101.html>, utilisait la méthode HTTP `GET`. curl, lui, utilise `POST`. La requête `curl --doh-url https://doh.bortzmeyer.fr/ https://jdll.org/` provoque :

```
INFO: id 0
opcode QUERY
rcode NOERROR
flags RD
;QUESTION
jdll.org. IN AAAA
;ANSWER
;AUTHORITY
;ADDITIONAL
INFO: id 0
opcode QUERY
rcode NOERROR
flags RD
;QUESTION
jdll.org. IN A
;ANSWER
;AUTHORITY
;ADDITIONAL
[2019-04-09 19:01:51,750] 82.251.62.29:35610 POST / 2 200 91 8403
[2019-04-09 19:01:51,750] 82.251.62.29:35608 POST / 2 200 42 6703
```

Notez également que curl a fait deux requêtes, A et AAAA. Voici ce qu'affiche curl de son activité :

```
% curl --doh-url https://doh.bortzmeyer.fr/ https://jdll.org/
* Hostname 'doh.bortzmeyer.fr' was found in DNS cache
* Connected to doh.bortzmeyer.fr (193.70.85.11) port 443 (#1)
* ALPN, offering h2
* ALPN, offering http/1.1
* ALPN, server accepted to use h2
* Server certificate:
*  subject: CN=doh.bortzmeyer.fr
*  start date: Apr  5 12:54:32 2019 GMT
*  expire date: Jul  4 12:54:32 2019 GMT
*  subjectAltName: host "doh.bortzmeyer.fr" matched cert's "doh.bortzmeyer.fr"
*  issuer: C=US; O=Let's Encrypt; CN=Let's Encrypt Authority X3
*  SSL certificate verify ok.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x56448a35af30)
> POST / HTTP/2
Host: doh.bortzmeyer.fr
Accept: */*
Content-Type: application/dns-message
```

```
Content-Length: 26

* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
< HTTP/2 200
< content-type: application/dns-message
< content-length: 42
< cache-control: no-cache
< date: Tue, 09 Apr 2019 17:03:48 GMT
< server: hypercorn-h2

...

<!DOCTYPE html>
<html lang="">
<head>
    <meta charset="utf-8" />
    <title>Accueil | JdLL</title>

    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta property="og:image" content="/user/themes/jd-ll/images/favicon.ico"/>
    <meta name="generator" property="og:description" content="GravCMS" />
```

Sur Firefox, il faut configurer DoH dans un onglet `about:config`. Le mot-clé est TRR pour "*Trusted Recursive Resolver*". On voit ici les réglages disponibles (2 veut dire « utiliser DoH mais se rabattre sur le DNS normal en cas de problème », 3 serait « uniquement DoH » et 0 « pas de DoH du tout ») :

Merci aux organisat·eur·rice·s. On peut trouver de jolies photos des JDLL <https://epn.salledesrancy.com/photos-jdll-de-la-20eme-edition-samedi-6-7avril-2019/>. Merci à Syst et Marne pour leur excellent exposé sur « Le vrai coût écologique de la publicité en ligne ». J'ai modestement contribué à la lutte contre les panneaux de surveillance publicitaire <https://antipub.org/> en installant une copie de la page de désinscription (en ligne sur `https://www.bortzmeyer.org/files/retency.html`). Autre exposé très utile, celui d'Oriane <https://epn.salledesrancy.com/wp-content/uploads/2019/04/IMG_1526-1024x626.jpg> sur « La Fédération FDN et la fibre optique. Enjeux et perspectives de l'Internet associatif en haut débit. » analysant les chances pour un opérateur Internet « alternatif » de pouvoir utiliser la fibre optique des RIP (Réseaux d'initiative publique). L'énorme travail de récolte d'informations fait par la FFDN montre que ce n'est pas gagné <https://fibre.ffdn.org/>...