RFC 9156 : DNS Query Name Minimisation to Improve Privacy

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 novembre 2021

Date de publication du RFC : Novembre 2021

https://www.bortzmeyer.org/9156.html

Protéger la vie privée sur l'Internet nécessite au moins deux techniques : chiffrer les données en transit pour éviter leur lecture par des tiers **et minimiser** les données qu'on envoie, pour éviter les abus par les récepteurs des données. Ce deuxième point, pourtant bien mis en avant dans la loi Informatique & Libertés ou dans le RGPD est souvent oublié. Ce RFC applique ce principe au DNS : il ne faut pas envoyer aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> le nom de domaine complet mais seulement la partie du nom de domaine qui lui est strictement nécessaire pour répondre, le **minimum**. Cette norme succède au RFC 7816 [1], qui était purement expérimental alors que cette minimisation de la requête ("*QNAME minimisation*") est désormais une norme. Le principal changement est la recommandation d'utiliser le type de données A (adresse IPv4) et plus NS (serveurs de noms).

Ce principe de minimisation, qui devrait être central dans toute approche de la protection de la vie privée est également exposé dans le RFC 6973, section 6.1. Le DNS violait ce principe puisque, traditionnellement, un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> qui recevait une demande d'information sur `www.foobar.example` transmettait aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html> la question complète, alors que, par exemple, les serveurs faisant autorité pour la racine ne connaissent que les TLD et que leur demander simplement des informations sur le TLD `.example` aurait suffi. (Voir le RFC 7626 pour une analyse complète des relations entre le DNS et la vie privée.) Cette tradition (qui ne s'appuyait sur aucune norme technique) est remise en cause par la "*QNAME minimisation*" qui demande au contraire qu'on n'envoie aux serveurs faisant autorité que le nom minimal (`example` à la racine, `foobar.example` aux serveurs du TLD `.example`, etc).

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7816.txt`

Cette minimisation est unilatérale, elle ne nécessite qu'un changement des résolveurs, sans toucher aux serveurs faisant autorité puisqu'elle ne change pas le protocole DNS. Depuis la sortie du RFC 7816, en 2016, elle a été largement déployée (si le résolveur que vous utilisez ne le fait pas, réclamez-le à votre service informatique !).

Le précédent RFC sur cette technique, le RFC 7816 avait le statut d'expérimentation alors que notre RFC 9156 est désormais une norme. En effet, une expérience considérable a été accumulée depuis le RFC 7816, qui a été mis en œuvre dans pratiquement tous les résolveurs, et souvent activé. Le FUD souvent entendu comme quoi la "*QNAME minimisation*" allait tuer Internet et des chatons a été largement réfuté. Les leçons tirées sont documentées dans « "*DNSThought QNAME minimisation results. Using Atlas probes*" <https://dnsthought.nlnetlabs.nl/#qnamemin> », « "*Maximizing Qname Minimization : A New Chapter in DNS Protocol Evolution*" <https://blog.verisign.com/security/maximizing-qname-minimization-a-new-chapter-in-dns-protocol-evolution/> », « "*Measuring Query Name Minimization*" <https://indico.dns-oarc.net/event/34/contributions/787/attachments/777/1326/2020-09-28-oarc33-qname-minimisation.pdf> » et « "*A First Look at QNAME Minimization in the Domain Name System*" <https://nlnetlabs.nl/downloads/publications/devries2019.pdf> ».

Maintenant, la pratique, comment fait-on de la "*QNAME minimisation*" ? La question envoyée par le résolveur au serveur faisant autorité comprend un QNAME ("*Query Name*", le nom demandé) et un QTYPE ("*Query Type*", le type de données, par exemple serveur de courrier, adresse IP, texte libre, etc). Avec la "*QNAME minimisation*", le nom doit être le nom le plus court possible. Quand le résolveur interroge un serveur racine, il n'envoie comme QNAME que le TLD, par exemple. Trouver « le plus court possible » n'est pas forcément trivial en raison des coupures de zone. Dans un nom comme `miaou.foo.bar.example`, `foo.bar.example` et `bar.example` font peut-être partie de la même zone (et ont donc les mêmes serveurs faisant autorité) et peut-être pas. Rien dans la syntaxe du nom ne l'indique. Contrairement à une idée fausse et répandue, il n'y a pas forcément une coupure de zone pour chaque point dans le nom. Trouver les coupures de zone est expliqué dans le RFC 2181, section 6. Un résolveur qui valide avec DNSSEC doit savoir trouver ces coupures, pour savoir à qui demander les enregistrements de type DS. Les autres (mais quelle idée, en 2021, d'avoir un résolveur qui ne valide pas) doivent s'y mettre. Si, par exemple, `foo.bar.example` et `bar.example` sont dans la même zone, le résolveur qui veut trouver des données associées à `miaou.foo.bar.example` va envoyer le QNAME `example` à la racine, puis `bar.example` au serveur du TLD, puis `miaou.foo.bar.example` au serveur de `bar.example`. (Avant la "*QNAME minimisation*", il aurait envoyé le QNAME `miaou.foo.bar.example` à tout le monde.)

Cela, c'était pour le QNAME. Et le QTYPE ? On peut choisir celui qu'on veut (à l'exception de ceux qui ne sont pas dans la zone, comme le DS), puisque les délégations de zones ne dépendent pas du type. Mais, et c'est un sérieux changement depuis le RFC 7816, notre RFC recommande le type A (ou AAAA), celui des adresses IP, et plus le type NS (les serveurs de noms), que recommandait le RFC 7816. Deux raisons à ce changement :

— Certaines "*middleboxes*" boguées jettent les questions DNS portant sur des types qu'elles ne connaissent pas. Le type A passe à coup sûr.
— Le but de la "*QNAME minimisation*" étant la protection de la vie privée, il vaut mieux ne pas se distinguer et, notamment, ne pas dire franchement qu'on fait de la "*QNAME minimisation*" (les requêtes explicites pour le type NS étaient rares). Un serveur faisant autorité, ou un surveillant qui espionne le trafic, ne peut donc pas déterminer facilement si un client fait de la "*QNAME minimisation*".

Vous voyez ici le schéma de la résolution DNS sans la "*QNAME minimisation*" puis avec :

Dans certains cas, la "*QNAME minimisation*" peut augmenter le nombre de requêtes DNS envoyées par le résolveur. Si un nom comporte dix composants (ce qui arrive dans des domaines `ip6.arpa`), il faudra dans certains cas dix requêtes au lieu de deux ou trois. Les RFC 8020 et RFC 8198 peuvent aider

à diminuer ce nombre, en permettant la synthèse de réponses par le résolveur. Une autre solution est de ne pas ajouter un composant après l'autre en cherchant le serveur faisant autorité mais d'en mettre plusieurs d'un coup, surtout après les quatre premiers composants.

Un algorithme complet pour gérer la `QNAME minimisation` figure dans la section 3 du RFC.

Notez que, si vous voulez voir si votre résolveur fait de la "*QNAME minimisation*", vous pouvez utiliser tcpdump pour voir les questions qu'il pose mais il y a une solution plus simple, la page Web de l'OARC <https://cmdns.dev.dns-oarc.net/> (dans les "*DNS features*").

Un test avec les sondes RIPE Atlas semble indiquer que la "*QNAME minimisation*" est aujourd'hui largement répandue (les deux tiers des résolveurs utilisés par ces sondes) :

```
% blaeu-resolve --requested 1000 --type TXT   qnamemintest.internet.nl
["hooray - qname minimisation is enabled on your resolver :)!"] : 651 occurrences
["no - qname minimisation is not enabled on your resolver :("] : 343 occurrences
Test #33178767 done at 2021-11-05T14:41:02Z
```

Il existe aussi une étude récente sur la QNAME minimization <https://adam.pages.nic.cz/reports/adam/qname-minimisation-en/> en République Tchèque.

Comme son prédécesseur, ce RFC utilise (prétend Verisign) un brevet <https://datatracker.ietf.org/ipr/5197/>. Comme la plupart des brevets logiciels, il n'est pas fondé sur une réelle invention (la "*QNAME minimisation*" était connue bien avant le brevet).

Ah, et vous noterez que le développement de ce RFC, par trois auteurs, a été fait sur FramaGit <https://framagit.org/bortzmeyer/rfc7816-bis>.

””