Synthèse Bibliographique: Où en est le déploiement du DNS encrypté à grande échelle ?

Auteure : Agnès Thouvenin

SOMMAIRE :

1- INTRODUCTION

Le DNS (Domaine Name System) est aujourd'hui indispensable et omniprésent dans l'utilisation d'internet. En effet, une requête DNS se résoud en traduisant une url lisible pour l'utilisateur en adresse IP permettant de localiser le serveur hébergent la page web ou le service en quelques milisecondes à peine. Cependant, par son implémentation traditionnelle, les paquets DNS sont envoyés sans aucune encryption, rendant ces paquets vulnérables (à de la surveillance du traffic DNS, de la censure, de la manipulation des réponses DNS, de la redirection de traffic), nuisant à la sécurité et la vie privée des utilisateurs d'Internet.

C'est pourquoi, pour pallier à ce problème, des solutions ont été déployées depuis quelques années et plusieurs protocoles ont été proposés pour encrypter les requêtes DNS entre les clients et les serveurs, que nous généralisont par l'appellation DNS encrypté. Parmis eux nous retrouveront notamment DoT (DNS-over-TLS), encryptant les requêtes DNS au niveau de la couche de transport (protocols TCP/UDP) et DoH (DNS-over-HTTPS), encryptant cette fois-ci les requêtes au niveau de la couche application (protocole HTTPS).

L'objectif de cette synthèse est d'avoir une vue d'ensemble sur le déploiement à grande échelle de cette nouvelle solution. À l'heure actuelle, quelle est l'utilisation du DNS encrypté ? Est-ce globalement utilisé ?

2- ETAT DE L'ART DU DOMAINE

Cet état de l'art consiste en une vue générale sur le marché du DNS et du DNS encrypté depuis sa création et quels sont ses enjeux.

L'apparition du terme DNS a lieu au début des années 1980, avec Paul Mockapetrisand Jon Postel. Ce dernier présente le system DNS en 1983, avec le même principe de requête qu'expliqué dans l'introduction.

A l'origine, le marché est plûtot compétitif, car le service de protocol DNS est standardisé et c'est relativement accessible de faire tourner des résolutions de DNS. Il y a principalement deux façons de résoudre un DNS : la première façon est de passer par le FAI (Fournisseur d'Accès à Internet, ISP en anglais) ; et la deuxième, qui est d'utiliser un resolveur de DNS (publique). Cette deuxième alternative s'est développée à partir de la fin des années 2000, et a été initialisée par Google. En plus d'offrir plusieurs options avantageuses (notamment des options de regroupement dont nous parleront ci-après), c'est cette alternative de resolveur DNS publique qui a aussi permis la mise en place l'encryption du DNS, apportant ainsi plus de sécurité aux utilisateurs penchant pour cette option. En fait, la plupart des résolveurs de DNS publiques (comme Cloudflare, Quad9, Google, c'est à dire des organismes qui ont des serveurs internet à leur disposition) peuvent lire et traiter des requêtes de DNS encrypté, ce qui n'est souvent pas le cas des FAI.

D'autre part, les clients (c'est à dire les utilisateurs d'internet), sont souvent intéressés pour que leurs services soient regroupés et fournis par un seul organisme afin de leur simplifier la vie et limiter les coûts. C'est ainsi que les résolveurs de DNS, (et surtout les plus gros d'entre eux, parce qu'ils peuvent souvent proposer un plus grand nombre de services)

viennent prendre le contrôle du marché et écraser toute concurence. On notera que les leaders de ces résolvers de DNS sont aussi peu nombreux dû au nombre relativement restreint de navigateurs internet.

Cependant, la concurrence n'est pas forcément un atout dans ce type de marché. Effectivement, d'après l'étude de l'article « How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem » (référence [2]) l'interconnexion du réseau, c'est à dire s'associer à des concurrents afin de pouvoir proposer et couvrir davantage de services est très intéressant car il permet donc un regroupement des services, ce que nous avons vu comme solution à privilégier plus haut. On pourra donner comme exemple d'alliance celle du navigateur Mozilla Firefox avec le résolveur de Cloudflare, ce qui permet aux consommateurs de bénéfier des avantages des deux services à la fois , et aux entreprises de récupérer plus de clients (pour Cloudflare parce qu'il gagne des parts de marché, et pour Firefox parce qu'il peut proposer une expérience de navigateur plus sécurisé en terme de vie privée), donc c'est gagnant de tous les cotés.

3- OÙ EN EST LE DEPLOIMENT DU DNS ENCRYPTÉ À GRANDE ÉCHELLE : ÉTUDE, COMPARAISON, SYNTHÈSE

Avant Propos. Cette synthèse va venir répondre à la problématique posée, à savoir où en est le DNS encrypté à grande échelle à l'heure actuelle, en s'appuyant sur **2** articles traitant de cette problématique parus tout deux en 2019. Ces articles sont d'une part l'article de référence, « An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? », (référence [1]), et d'autre part d'un deuxième article légèrement plus récent que [1] : "DNS Privacy in Practice and Preparation," (référence [4]). Le premier article répond à la problématique en apportant un regard sur le traffic DNS plus spécifiquement, tandis que le deuxième s'attarde plus sur une vision de compatibilité du DNS encrypté.

Remarque : il n'y a pas d'article de référence de l'article de référence [1] pour composer cette synthèse car mon article de référence est le premier à réaliser une évaluation sur l'utilisation du DNS encrypté à grande échelle. Je cite cet article : « This paper performs by far the first end-to-end and large-scale analysis on DNS-over-Encryption ». Cet article de référence est d'ailleurs parmis les références de l'article [4] présenté dans l'Avant propos. Afin de confirmer ces dires, voici un extrait de ce dernier , parlant de l'article [1]: « Other studies have been conducted to identify and characterize open DNS resolvers and to measure the availability of DNS authoritative servers. However, the first study that we know of related to the deployment of DNS privacy was released more recently ».
Par ailleurs, les articles traitant de cette problématique plutôt précise se font très rares, et il est vrai que je manque un peu d'éléments de comparaison pour réaliser cette synthèse, mais ce n'est vraiment pas faute d'avoir cherché.

Pour commencer, le traffic de DNS encrypté reste aujourd'hui très minoritaire : en effet, et les deux articles sont d'accord là dessus, moins de 1 % des résolveurs de DNS proposent de résoudre des requêtes de DNS encrypté. Plus en détail, il a été étudié dans l'article [4] qui pour 1,197,794 résolveurs publiques, seuls 1747 arrivaient à résoudre du DNS encrypté, ce qui donne comme pourcentage 0,15 %. On remarquera que dans les études réalisées dans les deux papiers, il a été mise en place une vérification qui s'assurait que ce traffic ne soit pas faussement gonflé par des scanners automatiques. Cela n'est en conclusion pas le cas, mais c'est vrai que cette part de DNS encrypté pourtant plus sécurisée reste extremement faible. Etant donné que le développement du DNS encrypté a débuté il y a une dizaine d'année, cela soulève la question de pourquoi un tel écart entre son développement et son utilisation. Pourquoi le DNS encrypté prend-t-il autant de temps à être adopté à grande échelle ?

Cependant, et ce d'après les résultats présentés dans l'article [1], l'utilisation des protocoles

DoT et DoH (voir signification dans l'introduction) sont en hausse cette dernière année (2018) : à titre d'exemple, le traffic DoT de Cloudflare aurait augmenté de 56 % entre juillet et décembre 2018 tandis que pour Quad9, un autre résolveur de DNS, son traffic de DoT aurait fluctué au cours de la période. Concernant le protocole DoH, le volume des requêtes est également en hausse, comme l'illustre ce graphique ci-dessous, issue de l'article [1].

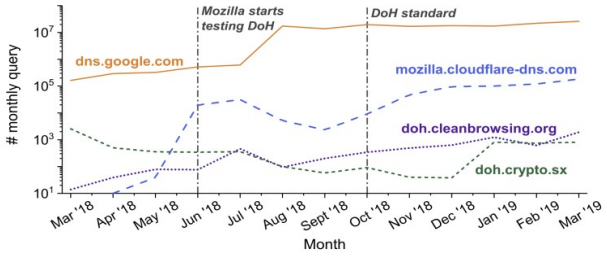

Figure 1 : évolution du volume des requetes DoH pour les domaines les plus populaires.
(source : Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In IMC '19: Proceedings of the Internet Measurement Conference 2019. ACM, New York, NY, USA, 14)

Regardons à présent quelle version de TLS est supportée par les résolveurs de DNS capables de résoudre du DoT. D'après le tableau intitulé « Table 1: Summary of DoT, DoH, and TFO measurements against open DNS resolvers. » dans l'article 4, sur les 1747 résolveurs de DNS supportant le DoT encrypté, seulement 4,5 % d'entre eux supportent la dernière version de TLS, c'est à dire la 1.3. En revanche, toujours d'après ce même tableau, 97 % supportent la version antérieure 1.2. Cette version 1.2 n'est pas encore obsolette à l'heure actuelle, donc le résultat est plutôt bon. À noter cependant que ce n'est pas le cas des versions 1 et 1.1 de TLS, qui elles ne sont plus sécurisées, et donc pour le coup, totalement obsolettes.

Enfin, d'après l'article 1, nous totalisons à l'heure de publication de celui-ci 150 fournisseurs qui offrent un service de DoT et 17 fournisseurs pour DoH. Concernant les fournisseurs de DoH, l'article [4] reporte que seulement 9 adresses IP différentes ont pu répondre à une requete DoH suite à une expérimentation réalisée par leur soin. Ce nombre est d'ailleurs confirmé par l'article [5] également, qui liste les résolveurs de DoH et en comptabilise également 9. La différence entre le résultat de l'article [1] et des autres peut venir du fait que des fournisseurs comptabilisés comme différents sont en fait localisés sur la même adresse IP, ce qui pourrait expliquer l'écart entre les deux nombres.
On remarquera par ailleurs que ce nombre de résolveurs DoH reste très petit, même comparé au nombre de résolveurs DoT (cité au début du paragraphe, et on rappelle au nombre de 150). Cela peut s'expliquer par le fait que pour DoH, contrairement à DoT, le protocole n'est pas standardisé, ce qui « sépare » les résultats. Ici par exemple, nous avons seulement les résultats du standard d'IETF (Internet Engineering Task Force), mais il existe d'autre organisation avec leur propre standard de DoH, comme DNS script par exemple.

4- CONCLUSION

En conclusion, le DNS encrypté reste aujourd'hui très peu (trop peu) utilisé à grande échelle malgré son développement depuis pas mal d'années. Cela peut s'expliquer par des soucis de configuration et une implémentation pas toujours très bonne de ses protocoles générant alors des erreurs. Malgré tout, le traffic de DoT et DoH a pas mal augmenté ces derniers temps, ce qui est un peu encourageant. Des efforts doivent cependant être faits de la part des résolveurs de DNS sur l'encrypté pour que son déploiement puisse davantage se démocratiser.

5- RÉFÉRENCES

- article de référence :

[1] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang,

Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In IMC '19: Proceedings of the Internet Measurement Conference 2019. ACM, New York, NY, USA, 14

- références pour l'état de l'art :

[2] Kevin Borgolte, Tithi Chattopadhyay, Nick Feamster, Mihir Kshirsagar,

Jordan Holland, Austin Hounsel, Paul Schmitt, How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem, Princeton University and The University of Chicago, 2019

[3] Roxana Radu & Michael Hausding (2020) Consolidation in the DNS resolvermarket – how much, how fast, how dangerous?, Journal of Cyber Policy, 5:1, 46-64, DOI:10.1080/23738871.2020.1722191

- article de la bibliographie (de l'article de référence) :

Pas d'article de référence, et ce car cet article est le premier à réaliser ce genre d'évaluation. Pour plus de détail, consulter la remarque suivant Avant-propos au début de la section 3 (synthèse).

- article ne figurant pas dans la bibliographie (de l'article de référence) :

[4] C. Deccio and J. Davis, "DNS Privacy in Practice and Preparation," inACM CoNEXT '19, 2019

[5] Timm Boettger, Felix Cuadrado, Gianni Antichi, Eder Leao Fernandes, Gareth Tyson, Ignacio Castro and Steve Uhlig, An Empirical Study of the Cost of DNS-over-HTTPS, Queen Mary University of London, septembre 2019