

afnic

DNS over HTTPS (DoH), présentation générale et enjeux autour de l'adoption

Stéphane Bortzmeyer

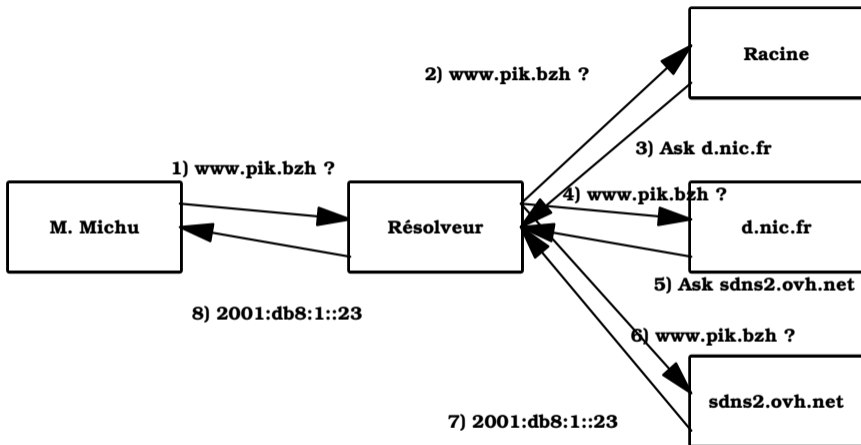
bortzmeyer@nic.fr

afnic

afnic



Le DNS



Le problème

afnic



Le problème

- Le DNS est l'étape obligée,



Le problème

- Le DNS est l'étape obligée,
- Mais il est très indiscret (RFC 7626), plein de gens peuvent savoir que vous demandez `pornhub.com`,



Le problème

- Le DNS est l'étape obligée,
- Mais il est très indiscret (RFC 7626),
- Et susceptible de modifications en route, (largement utilisé à des fins de censure comme Sci-Hub en mars 2019 en France),



Le problème

- Le DNS est l'étape obligée,
- Mais il est très indiscret (RFC 7626),
- Et susceptible de modifications en route,
- Comment garantir confidentialité et intégrité ?



Censure en action

Vue par les sondes RIPE Atlas

```
% blaeu-resolve --requested 1000 --country FR --type A sci-hub.tw  
[186.2.163.90] : 183 occurrences  
[] : 9 occurrences  
[127.0.0.1] : 212 occurrences  
[ERROR: SERVFAIL] : 1 occurrences  
[ERROR: NXDOMAIN] : 2 occurrences  
Test #22099888 done at 2019-06-25T13:25:37Z
```



Les solutions

- Les solutions de chiffrement présentées ici sont (pour l'instant), uniquement pour le lien entre machine terminale et résolveur.



Les solutions

- Les solutions de chiffrement présentées ici sont uniquement pour le lien entre machine terminale et résolveur.
- DoT : DNS-over-TLS (RFC 7858), port dédié (853), donc susceptible de blocage,



Les solutions

- Les solutions de chiffrement présentées ici sont uniquement pour le lien entre machine terminale et résolveur.
- DoT : DNS-over-TLS (RFC 7858), port dédié (853), donc susceptible de blocage,
- DoH : DNS-over-HTTPS (RFC 8484), le HTTPS normal sur le port 443, plus lent mais plus difficile à bloquer. Réutilise toute l'infrastructure de HTTP.

Les solutions

- Les solutions de chiffrement présentées ici sont uniquement pour le lien entre machine terminale et résolveur.
- DoT : DNS-over-TLS (RFC 7858), port dédié (853), donc susceptible de blocage,
- DoH : DNS-over-HTTPS (RFC 8484), le HTTPS normal sur le port 443, plus lent mais plus difficile à bloquer.
- Dans les deux cas, authentification habituelle TLS.

Autres choses sur DoH



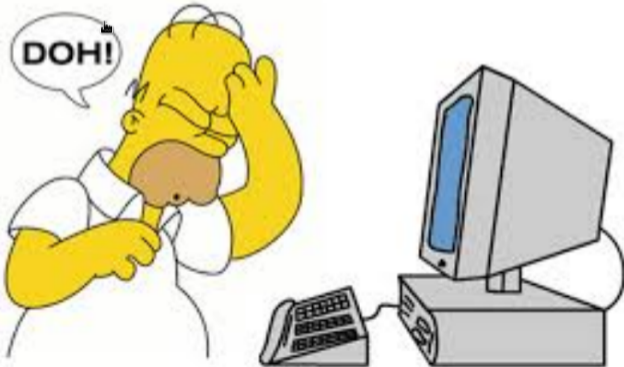
Autres choses sur DoH

- HTTP/2 seulement,



Autres choses sur DoH

- HTTP/2 seulement,
- Format « DNS binaire », pas évident à analyser en JavaScript.



On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH, cf. débat au FOSDEM en février 2019,



On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ? HTTP est trop bavard.



On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certaines* déploiements. Deux ou trois résolveurs DNS pour tout le monde ? **Problème non spécifique à DoH.**



On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certain*s déploiements.
- Résolution prise en main par les applications et pas par le système d'exploitation ?
Problème non spécifique à DoH, tous les logiciels malveillants font déjà cela.

On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certain*s déploiements.
- Résolution prise en main par les applications et pas par le système d'exploitation ?
- Perte de contrôle par les intermédiaires : ils ne peuvent plus surveiller et censurer. C'est un peu fait exprès. . . Et **ce n'est pas spécifique à DoH**. Cf. RFC 8404 qui regrettait déjà cette perte.

On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certain*s déploiements.
- Résolution prise en main par les applications et pas par le système d'exploitation ?
- Perte de contrôle par les intermédiaires : ils ne peuvent plus surveiller et censurer.
- Résolution dépendant du lieu problématique (CDN, noms privés, DNS64...)
Problème commun à tous les résolveurs publics.

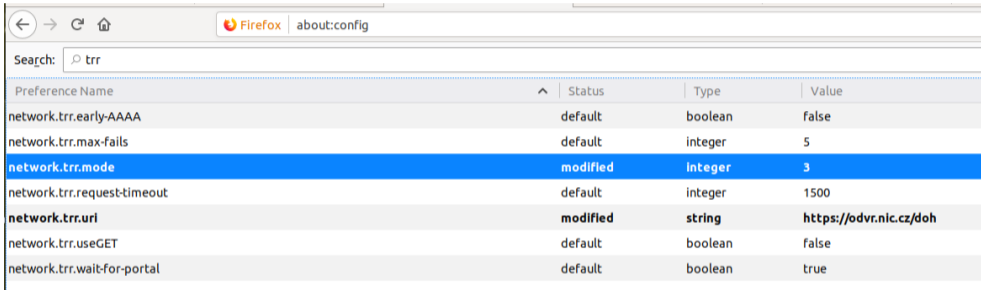
On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certain*s déploiements.
- Résolution prise en main par les applications et pas par le système d'exploitation ?
- Perte de contrôle par les intermédiaires : ils ne peuvent plus surveiller et censurer.
- Résolution dépendant du lieu problématique
- Tout sur le port 443.

On ne peut pas plaire à tout le monde

- Depuis quelques mois, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certain*s déploiements.
- Résolution prise en main par les applications et pas par le système d'exploitation ?
- Perte de contrôle par les intermédiaires : ils ne peuvent plus surveiller et censurer.
- Résolution dépendant du lieu problématique
- Tout sur le port 443.
- Confiance dans le résolveur ? (Comme avec tous les résolveurs.)

Firefox TRR (Trusted Recursive Resolver)



The screenshot shows the Firefox 'about:config' page with a search filter for 'trr'. A table lists several preferences, with 'network.trr.mode' highlighted in blue. The table has columns for Preference Name, Status, Type, and Value.

Preference Name	Status	Type	Value
network.trr.early-AAAA	default	boolean	false
network.trr.max-fails	default	integer	5
network.trr.mode	modified	integer	3
network.trr.request-timeout	default	integer	1500
network.trr.uri	modified	string	https://odvr.nic.cz/doh
network.trr.useGET	default	boolean	false
network.trr.wait-for-portal	default	boolean	true

Chiffré

```
10.101.0.51 → 185.43.135.1 TCP 74 45046 → https(443) [SYN] Seq=0 Win=26200 Len=0 MSS=1310
185.43.135.1 → 10.101.0.51 TCP 74 https(443) → 45046 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
10.101.0.51 → 185.43.135.1 TCP 66 45046 → https(443) [ACK] Seq=1 Ack=1 Win=26240 Len=0 TS=
10.101.0.51 → 185.43.135.1 TLSv1 608 Client Hello
185.43.135.1 → 10.101.0.51 TLSv1.2 1364 Server Hello
185.43.135.1 → 10.101.0.51 TLSv1.2 655 Certificate, Server Key Exchange, Server Hello Done
10.101.0.51 → 185.43.135.1 TLSv1.2 192 Client Key Exchange, Change Cipher Spec, Encrypted
10.101.0.51 → 185.43.135.1 TLSv1.2 546 Application Data, Application Data, Application Data
185.43.135.1 → 10.101.0.51 TLSv1.2 104 Application Data
```

dnsdist, pour faire votre résolveur DoH

dnsdist est un relais DNS, avec répartition de charge. Il permet de faire facilement DoT, DoH et DNS classique.

```
addDOHLocal("0.0.0.0:443", "/etc/dnsdist/server.pem",  
            "/etc/dnsdist/server.key")
```



Firefox

- Mozilla a annoncé DoH pour Firefox en juin 2018



Firefox

- Mozilla a annoncé DoH pour Firefox en juin 2018
- Par défaut, vers le résolveur public de Cloudflare



Firefox

- Mozilla a annoncé DoH pour Firefox en juin 2018
- Par défaut, vers le résolveur public de Cloudflare
- Pour se protéger des FAI, on va vers un GAFA ?



HTTP est indiscret

afnic



HTTP est indiscret

- Trop de détails dans la requête (User-Agent :, par exemple), comparé au DNS,



HTTP est indiscret

- Trop de détails dans la requête, comparé au DNS,
- Projet de profil pour réduire le bavardage HTTP.



Conclusion

afnic



Conclusion

- DoH est nécessaire, puisque les FAI ne veulent pas comprendre ce qu'est la neutralité du réseau,



Conclusion

- DoH est nécessaire, puisque les FAI ne veulent pas comprendre ce qu'est la neutralité du réseau,
- DoH est indispensable puisque souvent seul le port 443 est libre.



Conclusion

- DoH est nécessaire, puisque les FAI ne veulent pas comprendre ce qu'est la neutralité du réseau,
- DoH est indispensable puisque souvent seul le port 443 est libre.
- Il faut davantage de résolveurs DoH publics. Prenons exemple sur les tchèques <https://odvr.nic.cz/doh>. Logiciels existants : Knot, dnsmasq.

Merci !

afnic

www.afnic.fr
contact@afnic.fr

afnic