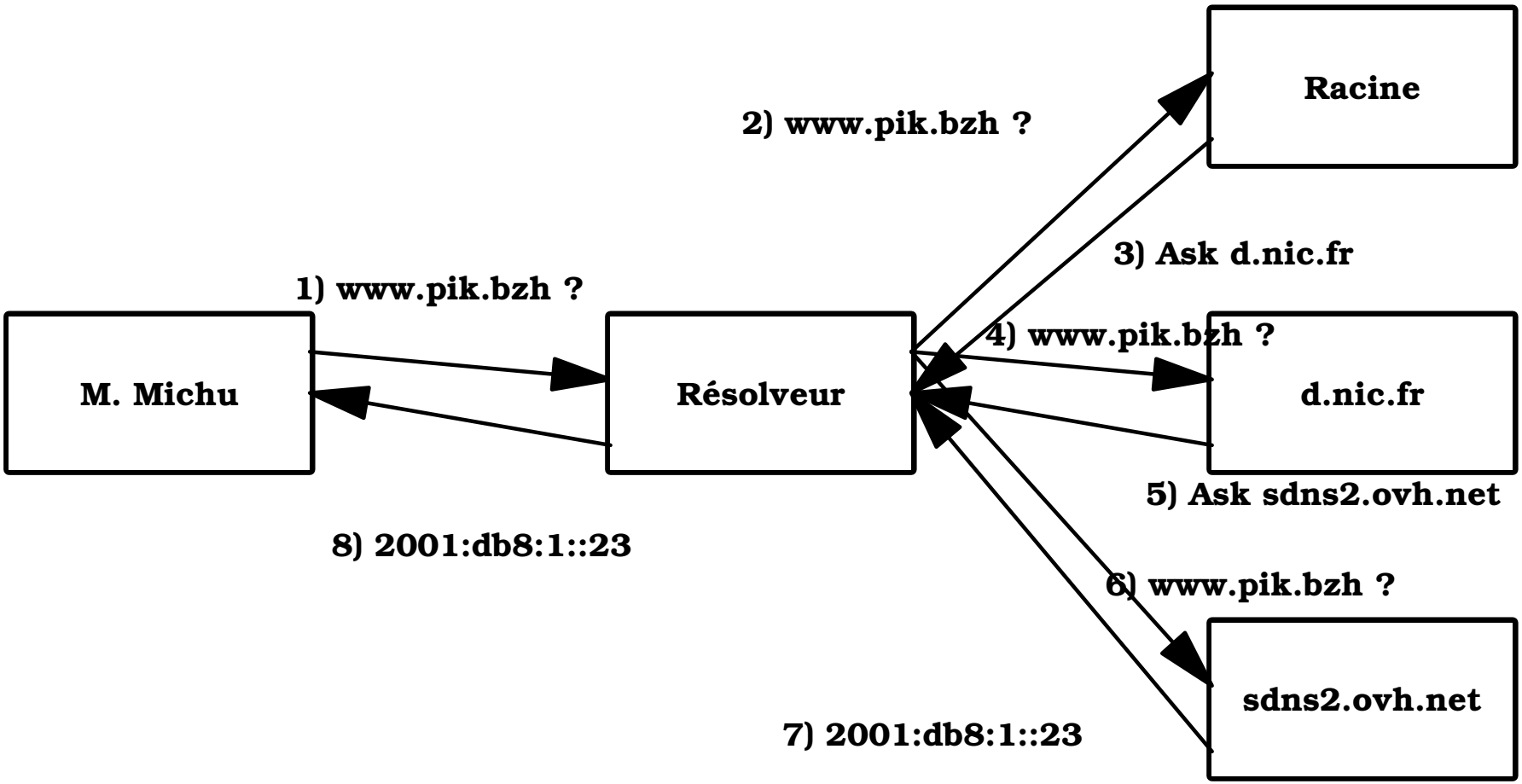
Qui va contrôler les noms de domaine ?

Stéphane Bortzmeyer stephane+jdll@bortzmeyer.org

JDLL, 7 avril 2019

Le DNS


Racine
2) www.pik.bzh ?
3) Ask d.nic.fr
1) www.pik.bzh ?
M. Michu
Résolveur
4) www.pik.bzh ?
d.nic.fr
5) Ask sdns2.ovh.net
8) 2001:db8:1::23
6) www.pik.bzh ?
sdns2.ovh.net
7) 2001:db8:1::23

Le problème

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 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
[] : 12 occurrences
[127.0.0.1] : 110 occurrences
[ERROR: SERVFAIL] : 4 occurrences
[186.2.163.90] : 237 occurrences
[ERROR: NXDOMAIN] : 2 occurrences
Test #20567707 done at 2019-04-05T14:54:55Z
```

Les solutions

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

Les solutions

- Les solutions 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,

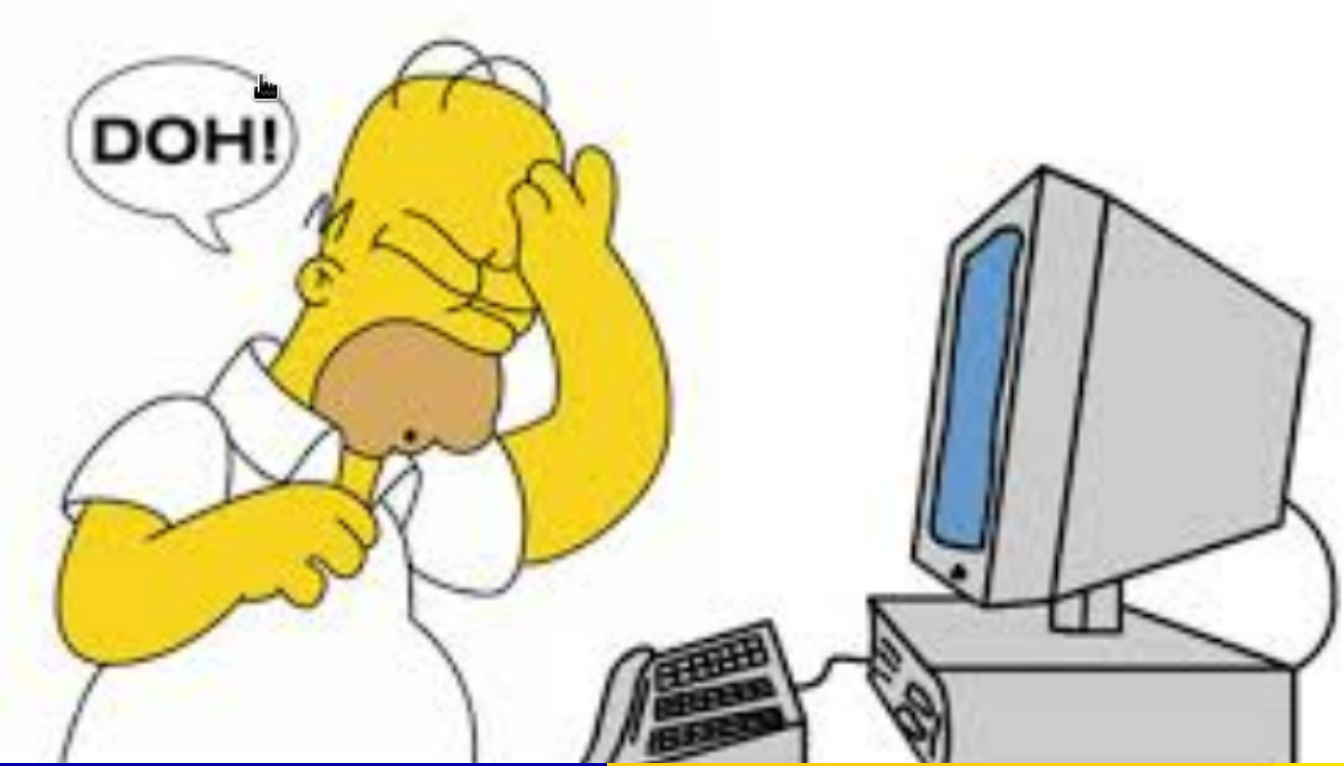
Les solutions

- Les solutions 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

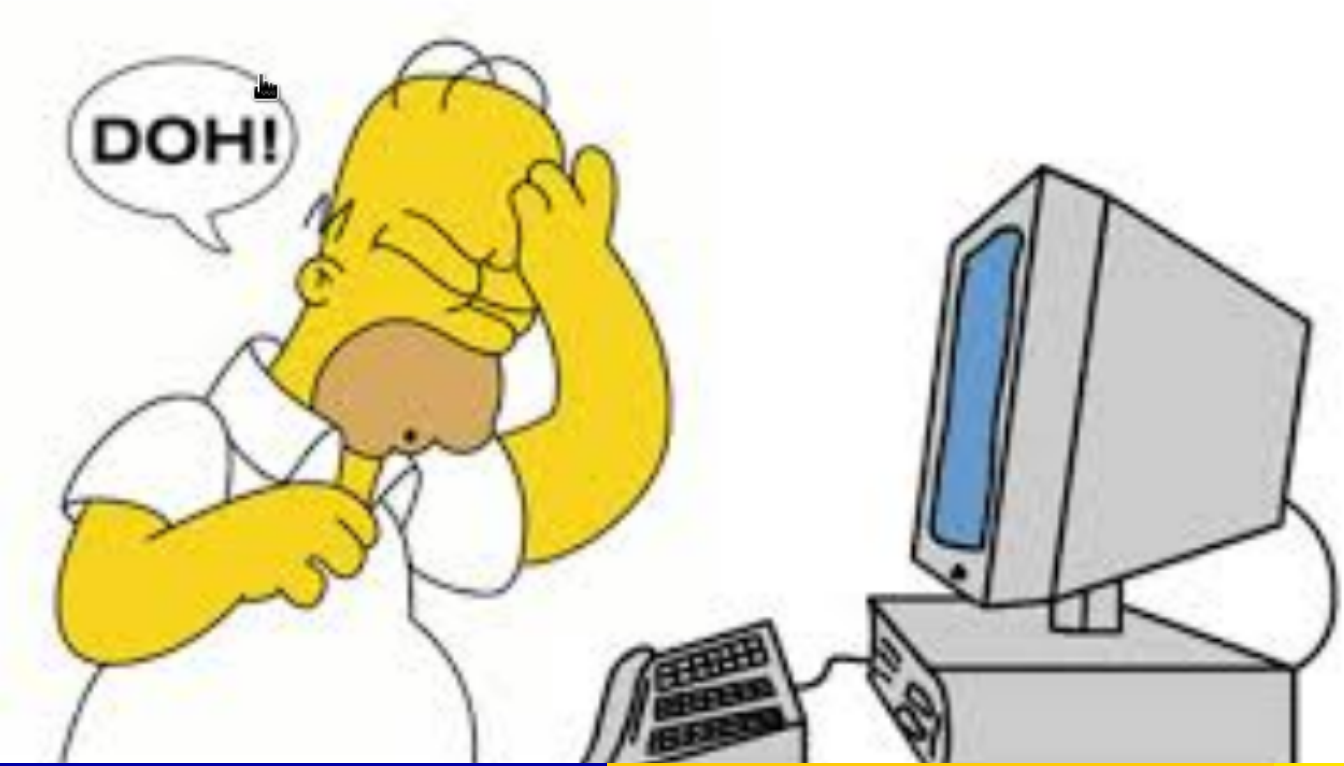
- Les solutions présentées ici sont uniquement pour le lien entre machine terminale et résolveur.
- DoT : DNS-over-TLS (RFC 7858), port dédié (853), donc susceptible de blocage,
- DoH : DNS-over-HTTPS (RFC 8484), le HTTPS normal sur le port 443, plus lent mais plus difficile à bloquer.
- Dans les deux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

Autres choses sur DoH



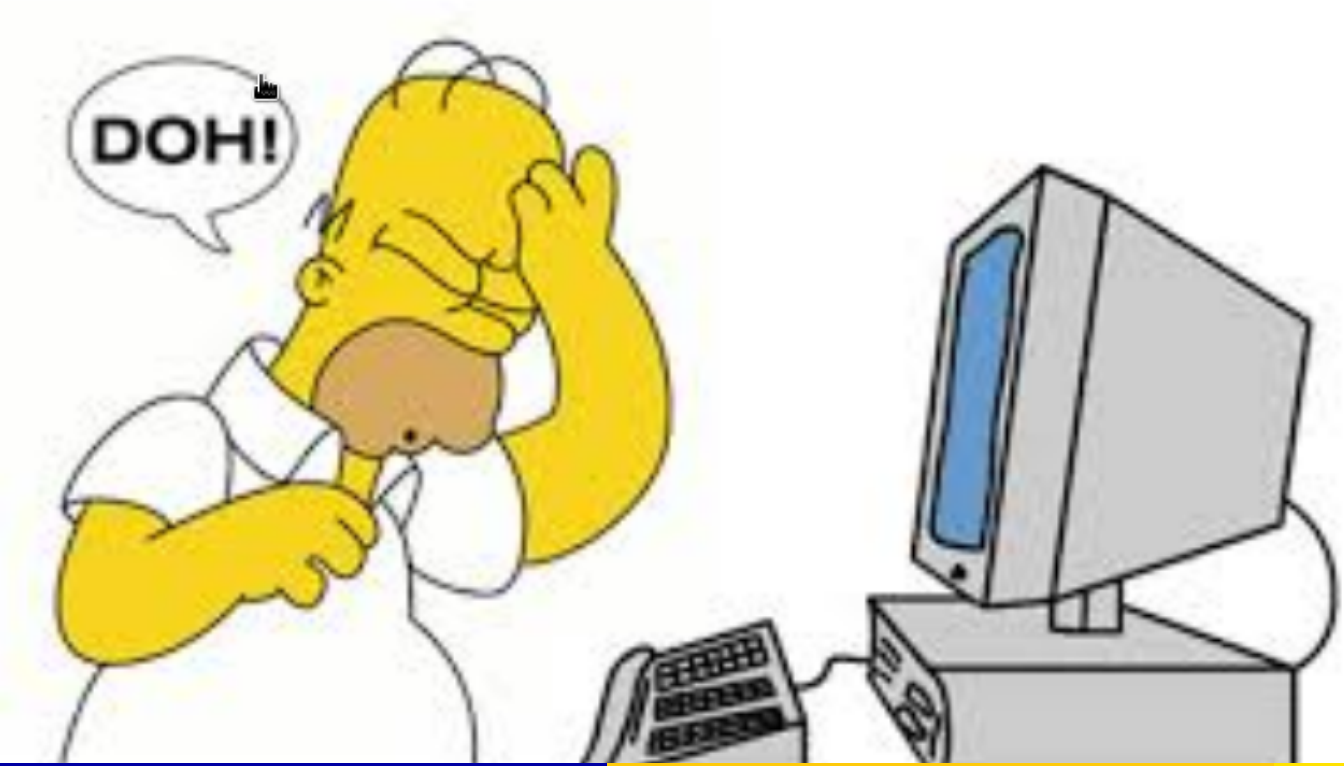
Autres choses sur DoH

- 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 semaines, grosse offensive idéologique contre DoH, cf. débat au FOSDEM en février 2019,

On ne peut pas plaire à tout le monde

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

On ne peut pas plaire à tout le monde

- Depuis quelques semaines, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certains* 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 semaines, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certains* 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 semaines, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certains* 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 semaines, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certains* 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 semaines, grosse offensive idéologique contre DoH,
- Le protocole DoH ?
- Risque de centralisation avec *certains* 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.

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

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

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.