Protocoles et droits humains

Francesca Musiani
CNRS
francesca.musiani@cnrs.fr
Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Protocoles et droits humains

Francesca Musiani
CNRS
francesca.musiani@cnrs.fr
Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

Plan du tutoriel

Le modèle en couches

Utilisateur

Couche #3
Applications : ce que voient les utilisateurs

Couche #2
Protocoles : les règles des logiciels

Couche #1
Matériel : ce qu'on touche

La notion de protocole

La notion de protocole

- Les règles que doivent suivre les logiciels

La notion de protocole

- Les règles que doivent suivre les logiciels
- Ont des conséquences en terme de ce qu'on peut faire, ce qu'on ne peut pas faire.

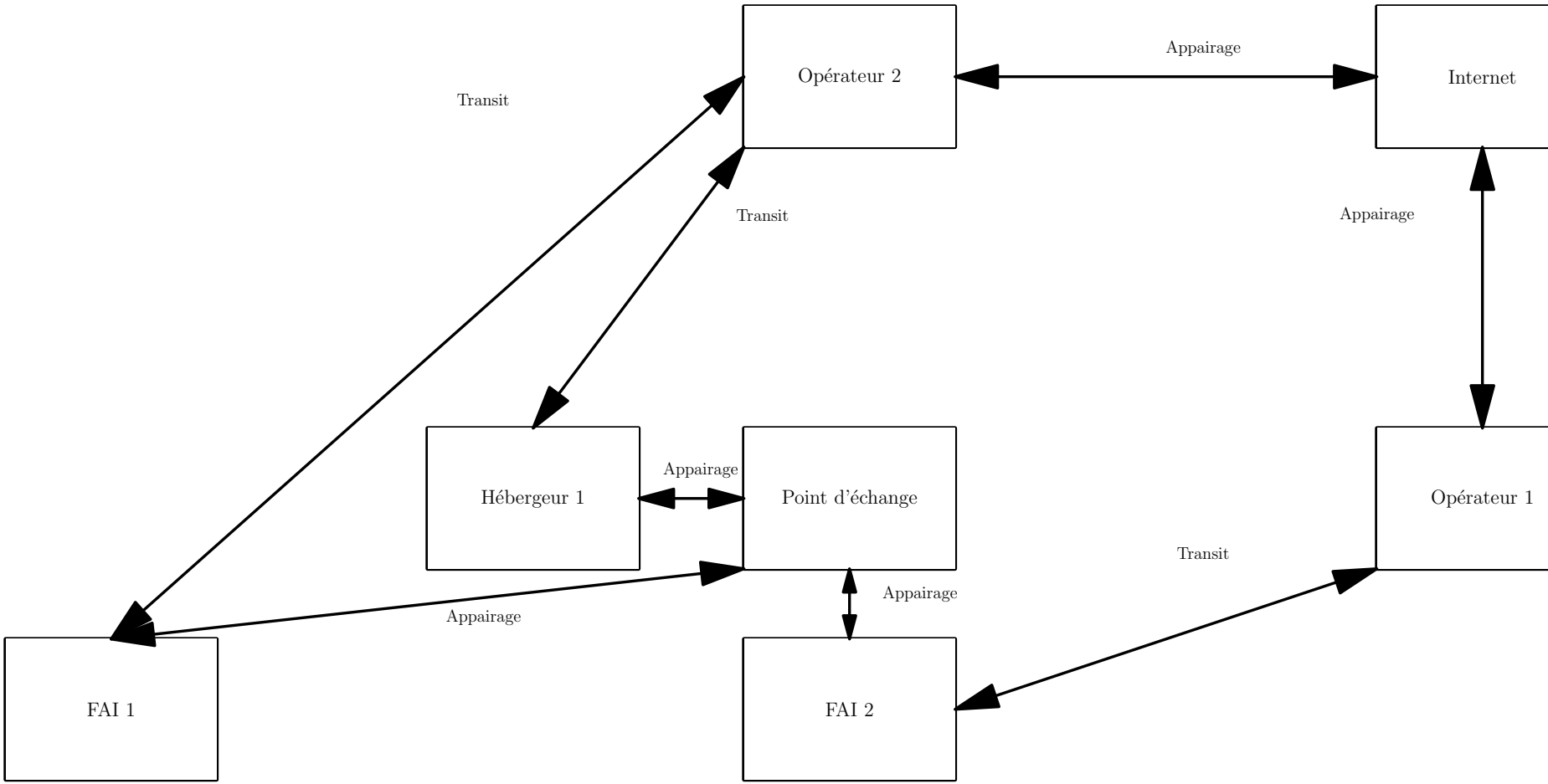
afnic

Infrastructure

« L'infrastructure, c'est ce que M. Michu ne voit pas. »

Exemples, le DNS, DHCP et BGP.

Exemple avec BGP



Plan du tutoriel

Définition

Définition

- Un concept ‘pluridisciplinaire’ (philosophique, juridique, politique)

Définition

- Un concept ‘pluridisciplinaire’
- Idée de base : tout être humain, en tant que tel, possède des droits ‘inhérents à sa personne, inaliénables et sacrés’, qui peuvent être opposés au pouvoir dans sa variété de formes. . .

afnic

Définition

- Un concept ‘pluridisciplinaire’
- Idée de base : tout être humain, en tant que tel, possède des droits ‘inhérents à sa personne, inaliénables et sacrés’
- . . .en tant que principes : donc, universalisme, égalitarianisme

afnic

Définition

- Un concept ‘pluridisciplinaire’
- Idée de base : tout être humain, en tant que tel, possède des droits ‘inhérents à sa personne, inaliénables et sacrés’
- . . .en tant que principes : donc, universalisme, égalitarianisme
- Reconnus par sources de droit nationales et internationales. . . mais sujet de controverse permanent !

Définition

- Un concept ‘pluridisciplinaire’
- Idée de base : tout être humain, en tant que tel, possède des droits ‘inhérents à sa personne, inaliénables et sacrés’
- . . .en tant que principes : donc, universalisme, égalitarianisme
- Reconnus par sources de droit nationales et internationales. . . mais sujet de controverse permanent !
- Exemples : liberté d’association, d’expression, droit à la vie privée. . .

afnic

Définition

- Un concept ‘pluridisciplinaire’
- Idée de base : tout être humain, en tant que tel, possède des droits ‘inhérents à sa personne, inaliénables et sacrés’
- . . .en tant que principes : donc, universalisme, égalitarianisme
- Reconnus par sources de droit nationales et internationales. . . mais sujet de controverse permanent !
- Exemples : liberté d’association, d’expression, droit à la vie privée. . .
- Quels rapports entre les droits humains et le numérique/les réseaux ?

afnic

La DUDH

La DUDH

- Adoptée en 1948 par l'Assemblée générale des Nations Unies

La DUDH

- Adoptée en 1948 par l'Assemblée générale des Nations Unies
- Valeur de 'proclamation de droits', sans portée juridique contraignante

La DUDH

- Adoptée en 1948 par l'Assemblée générale des Nations Unies
- Valeur de 'proclamation de droits', sans portée juridique contraignante
- Énonce les droits fondamentaux de l'individu, leur reconnaissance, et leur respect par la loi.

La DUDH

- Adoptée en 1948 par l'Assemblée générale des Nations Unies
- Valeur de 'proclamation de droits', sans portée juridique contraignante
- Énonce les droits fondamentaux de l'individu, leur reconnaissance, et leur respect par la loi.
- Préambule avec huit considérations reconnaissant la nécessité du respect inaliénable de droits fondamentaux de l'homme par tous les pays, nations et régimes politiques

La DUDH

- Adoptée en 1948 par l'Assemblée générale des Nations Unies
- Valeur de 'proclamation de droits', sans portée juridique contraignante
- Énonce les droits fondamentaux de l'individu, leur reconnaissance, et leur respect par la loi.
- Préambule avec huit considérations reconnaissant la nécessité du respect inaliénable de droits fondamentaux de l'homme par tous les pays, nations et régimes politiques
- Critiques d'effectivité/universalité supposée des droits humains.

Plan du tutoriel

Le coutellier est-il responsable du meurtre ?

Le coutellier est-il responsable du meurtre ?

- Une question philosophique, avec implications très concrètes

Le coutellier est-il responsable du meurtre ?

- Une question philosophique, avec implications très concrètes
- Neutralité = ne pas prendre parti dans les choix des valeurs et la détermination des objectifs

afnic

Le coutellier est-il responsable du meurtre ?

- Une question philosophique, avec implications très concrètes
- Neutralité = ne pas prendre parti dans les choix des valeurs et la détermination des objectifs
- La technique peut-elle se prévaloir du statut de ‘simple moyen’ ? Problèmes :
  - La technique a une fin propre : l’efficacité — une rationalité qui est déjà une position de valeur
  - Il n’y a pas de ’simple’ moyen — tout moyen sert implicitement une fin et il n’y a presque jamais de fin sans une (re-)distribution du pouvoir
  - Il ne peut pas y avoir une autonomie de l’autorité politique et morale

afnic

Le coutellier est-il responsable du meurtre ?

- Une question philosophique, avec implications très concrètes
- Neutralité = ne pas prendre parti dans les choix des valeurs et la détermination des objectifs
- La technique peut-elle se prévaloir du statut de ‘simple moyen’ ?
- Il ne s’agit pas de ‘condamner’ la technique, mais de comprendre que la détermination de ses fins ne se résume pas à la compétence technicienne

afnic

Pouvoir et limites

Pouvoir et limites

- Séparation des pouvoirs dans les démocraties libérales est une façon de les limiter

Pouvoir et limites

- Séparation des pouvoirs dans les démocraties libérales est une façon de les limiter
- Montesquieu : « pour qu'on ne puisse pas abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir »

afnic

Pouvoir et limites

- Séparation des pouvoirs dans les démocraties libérales est une façon de les limiter
- Montesquieu : « pour qu'on ne puisse pas abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir »
- Cela se passe-t-il de façon satisfaisante dans l'écosystème numérique ?

afnic

Pouvoir et limites

- Séparation des pouvoirs dans les démocraties libérales est une façon de les limiter
- Montesquieu : « pour qu'on ne puisse pas abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir »
- Cela se passe-t-il de façon satisfaisante dans l'écosystème numérique ?
- Nécessité de quelques 'garde-fous' pour éviter les abus et préserver les droits humains — par exemple pour éviter une 'délégation de confiance' excessive (ne pas se fier qu'à la vertu des fondateurs. . .)

afnic

Plan du tutoriel

Les traces qu'on laisse

Les traces qu'on laisse

- Avec le numérique, c'est trivial d'enregistrer et de chercher,

Les traces qu'on laisse

- Avec le numérique, c'est trivial d'enregistrer et de chercher,
- L'aiguille dans la botte de foin n'est plus cachée,

Les traces qu'on laisse

- Avec le numérique, c'est trivial d'enregistrer et de chercher,
- L'aiguille dans la botte de foin n'est plus cachée,
- Les moyens de la surveillance sont dans tout système numérique.

afnic

Les traces qu'on laisse

- Avec le numérique, c'est trivial d'enregistrer et de chercher,
- L'aiguille dans la botte de foin n'est plus cachée,
- Les moyens de la surveillance sont dans tout système numérique.
- DHCP est un exemple d'un protocole trop bavard :
  - Tout est diffusé,
  - Plein d'informations sont données (adresse IP précédente, p. ex.)

afnic

Exemple DHCP

```
19:26:30.174556 IP (tos 0x10, ttl 64, id 0, offset 0, flags [DF], proto
    0.0.0.0.68 > 255.255.255.255.67: [udp sum ok] BOOTP/DHCP, Request f
  Client-Ethernet-Address 84:cf:bf:8b:55:bc (oui Unknown)
  Vendor-rfc1048 Extensions
    Magic Cookie 0x63825363
    DHCP-Message Option 53, length 1: Request
    Client-ID Option 61, length 7: ether 84:cf:bf:8b:55:bc
    Requested-IP Option 50, length 4: 192.168.2.36
    Server-ID Option 54, length 4: turris
    MSZ Option 57, length 2: 1500
    Vendor-Class Option 60, length 18: "android-dhcp-6.0.1"
    Hostname Option 12, length 24: "android-526d34c04bb833b7"
    Parameter-Request Option 55, length 9:
      Subnet-Mask, Default-Gateway, Domain-Name-Server, Domain-Name
      MTU, BR, Lease-Time, RN
      RB
    END Option 255, length 0
```

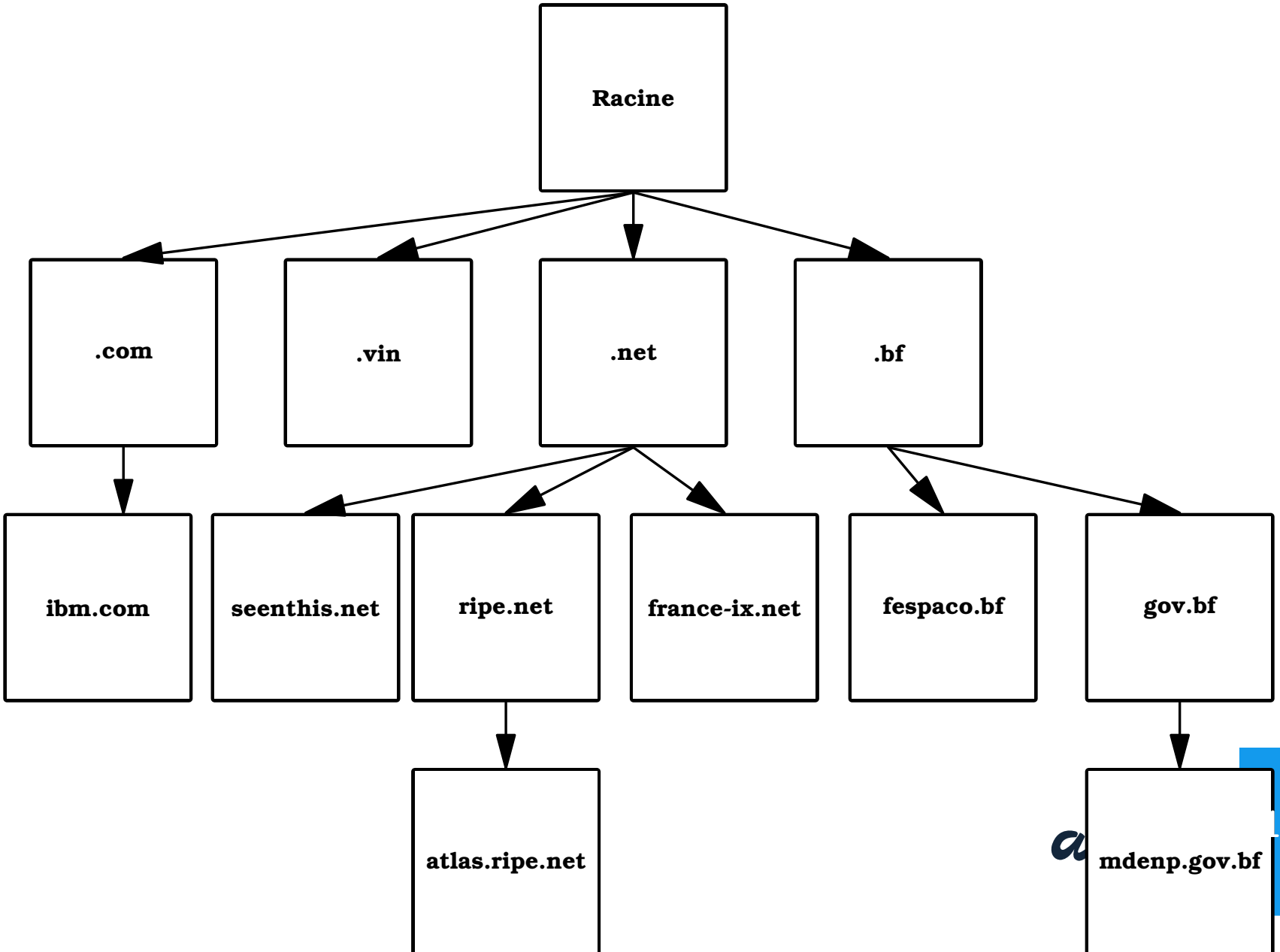
Sujet de réflexion

Pourquoi mettre l'adresse IP source dans chaque paquet ?

Aurait-on pu faire autrement ?

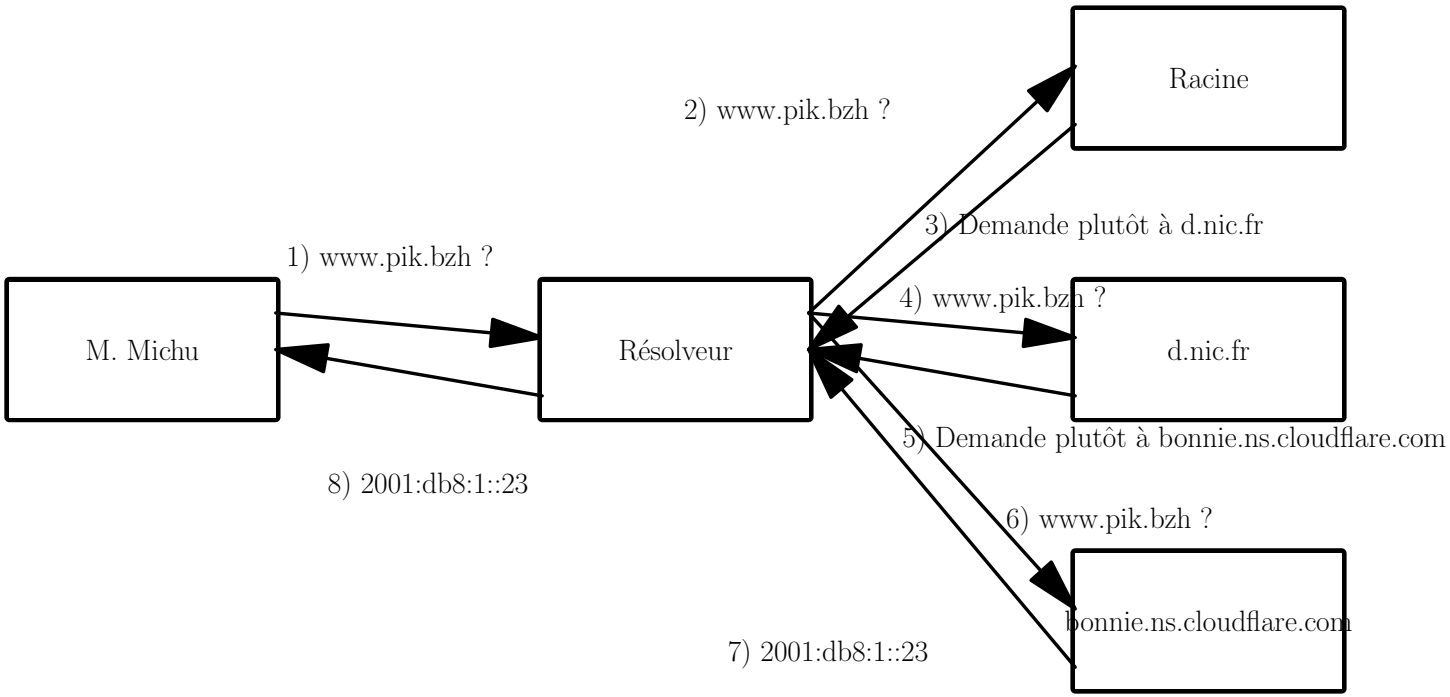
Censure via le DNS

1) Cible : l'enregistrement (cas de SciHub)



Censure via le DNS

2) Cible : la résolution (cas des sites de jeu en ligne)



Résolveurs DNS publics

Résolveurs DNS publics

- Google Public DNS, Quad9, Cloudflare...

Résolveurs DNS publics

- Google Public DNS, Quad9, Cloudflare...
- Pour fuir la censure, ou simplement les pannes

afnic

Résolveurs DNS publics

- Google Public DNS, Quad9, Cloudflare...
- Pour fuir la censure, ou simplement les pannes
- Peuvent être également menteurs

afnic

Résolveurs DNS publics

- Google Public DNS, Quad9, Cloudflare...
- Pour fuir la censure, ou simplement les pannes
- Peuvent être également menteurs
- Données personnelles ?

afnic

Centralisé et décentralisé

Centralisé et décentralisé

- Termes flous et utilisés à tort et à travers

Centralisé et décentralisé

- Termes flous et utilisés à tort et à travers
- Mais un vrai problème : si un acteur central a du pouvoir, il va en abuser (Montesquieu)

Centralisé et décentralisé

- Termes flous et utilisés à tort et à travers
- Mais un vrai problème : si un acteur central a du pouvoir, il va en abuser
- Attention, le pair-à-pair a ses faiblesses (vie privée)

Centralisé et décentralisé

- Termes flous et utilisés à tort et à travers
- Mais un vrai problème : si un acteur central a du pouvoir, il va en abuser
- Attention, le pair-à-pair a ses faiblesses
- La technique peut freiner la décentralisation (cf. Bitcoin et ses algorithmes qui ne sont pas ASIC-resistant)

afnic

Centralisé et décentralisé

- Termes flous et utilisés à tort et à travers
- Mais un vrai problème : si un acteur central a du pouvoir, il va en abuser
- Attention, le pair-à-pair a ses faiblesses
- La technique peut freiner la décentralisation
- ActivityPub et ses copains vont tout sauver ?

afnic

Arrêter l'Internet

Arrêter l'Internet

- *kill switch* pour les dictateurs

Arrêter l'Internet

- *kill switch* pour les dictateurs
- Lié à l'infrastructure : si elle est centralisée, c'est plus facile

afnic

Arrêter l'Internet

- *kill switch* pour les dictateurs
- Lié à l'infrastructure : si elle est centralisée, c'est plus facile
- Le *mesh networking* comme solution ?

Droit à l'accès

Houda Faraoun : Les citoyens ne seront pas remboursés pour les coupures d'Internet durant le BAC

Par **Baha eddine A.S** - 3 juillet 2018

La ministre de la poste, des technologies de l'information et de la communication, Imane Houda Fraoun a nié toute intention de la part du ministère ou d'Algérie télécom à rembourser les citoyens suite aux coupures d'Internet durant les examens nationaux du baccalauréat.

Droit à l'accès

- Fracture numérique, quelles conséquences ?

Droit à l'accès

- Fracture numérique, quelles conséquences ?
- La coupure par la HADOPI, une punition disproportionnée ?

Code 451

Code 451

- Code retour HTTP indiquant qu'une ressource est bloquée pour des raisons légales

Code 451

- Code retour HTTP indiquant qu'une ressource est bloquée pour des raisons légales
- Peu utilisée par les censeurs

Code 451

- Code retour HTTP indiquant qu'une ressource est bloquée pour des raisons légales
- Peu utilisée par les censeurs
- Un cas réel : les journaux étatsuniens qui croient punir les lecteurs européens (RGPD)

Élaboration des normes

Élaboration des normes

- Groupe de recherche IRTF HRPC *Human Rights and Protocol Considerations*

Élaboration des normes

- Groupe de recherche IRTF HRPC
- Idée de base : les protocoles développés par l'IETF ont des conséquences sur les droits humains

Élaboration des normes

- Groupe de recherche IRTF HRPC
- Idée de base : les protocoles développés par l'IETF ont des conséquences sur les droits humains
- RFC 1984 (refus d'affaiblir la cryptographie), RFC 7258 (post-Snowden, RFC affirmant que la surveillance de masse est une attaque contre l'Internet, et qu'il faut déployer des mesures techniques la rendant plus difficile), et bien sûr l'excellent RFC 6973 (sur la vie privée).

afnic

Élaboration des normes

- Groupe de recherche IRTF HRPC
- Idée de base : les protocoles développés par l'IETF ont des conséquences sur les droits humains
- RFC 1984, RFC 7258, et bien sûr l'excellent RFC 6973.
- Résultat : RFC 8280

afnic

Élaboration des normes

- Groupe de recherche IRTF HRPC
- Idée de base : les protocoles développés par l'IETF ont des conséquences sur les droits humains
- RFC 1984, RFC 7258, et bien sûr l'excellent RFC 6973.
- Résultat : RFC 8280
- Notamment la section 6 *check list* « Est-ce que votre protocole nécessite des machines intermédiaires ? Est-ce que ça ne pourrait pas être fait de bout en bout, plutôt ? Est-ce que votre protocole marchera également sur des liens à faible capacité et forte latence ? Est-ce que votre protocole est à état (alors que les protocoles sans état sont souvent plus robustes) ? »

afnic

La loi et la technique

La loi et la technique

- DNS-sur-HTTPS sert à contourner le blocage/modification du trafic DNS,

La loi et la technique

- DNS-sur-HTTPS sert à contourner le blocage/modification du trafic DNS,
- Est-ce une bonne ou une mauvaise idée que de faire une technique pour contourner ces règles ?

Financement du contenu

Financement du contenu

- Pas de mécanisme dans l'infrastructure Internet pour les paiements,

Financement du contenu

- Pas de mécanisme dans l'infrastructure Internet pour les paiements,
- Solutions bâties au dessus (Carte Visa, Paypal, Bitcoin, Flattr)

afnic

Financement du contenu

- Pas de mécanisme dans l'infrastructure Internet pour les paiements,
- Solutions bâties au dessus (Carte Visa, Paypal, Bitcoin, Flattr)
- Il n'y a pas que ce que la technique fait, il y a aussi ce qu'elle ne fait pas.

afnic

Merci !

www.afnic.fr
contact@afnic.fr