Séminaire Crans

DNS

Neven Villani

2022-01-28

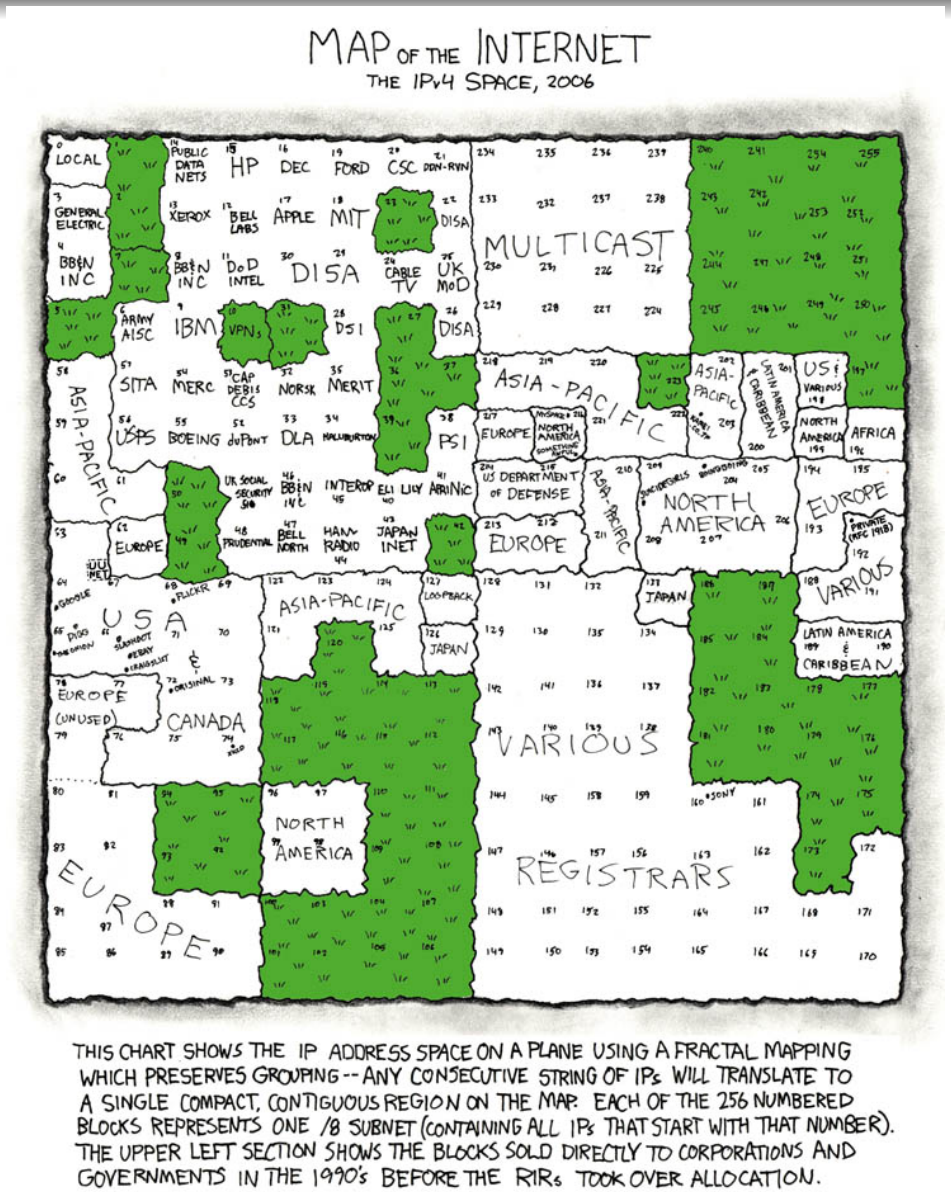
addresse IP vs *nom de domaine*

- les deux sont uniques [citation needed]
- *addresse IP* donne le chemin d'accès
- *nom de domaine* est humainement lisible

→ *addresse IP* plus pratique pour serveurs
→ *nom de domaine* plus pratique pour humains

addresse IP → *nom de domaine*: facile
Il faut donc un traducteur *nom de domaine* → *addresse IP*

addresse IP



XKCD

Map of the Internet

https://xkcd.com/195

Illustration du lien entre *addresse IP* et position géographique/affiliation

Plan

Objectif

Entrée: `hodaur.crans.org`
Sortie: `2a0c:700:2::ff:fe01:4502` ou `185.230.79.10`

Anatomie d'un *nom de domaine*

$$\underbrace{\texttt{hodaur}}_{3^{\text{rd}}\text{ level}} . \underbrace{\texttt{crans}}_{2^{\text{nd}}\text{ level}} . \underbrace{\texttt{org}}_{\text{toplevel}}$$

- toplevel
  - generique: `com`, `net`, `org`
  - pays: `fr`, `de`, `uk`, `eu`
- 2^{nd} level et 3^{rd} level
  unique pour le niveau supérieur et enregisté à la discrétion du responsable du niveau

Limites

- $\leqslant 63$ octets par niveau
- $\leqslant 255$ octets au total
- En revanche on peut trouver $\geqslant 4$ niveaux

Résolution

De droite à gauche: trouver le responsable du niveau ou quelqu'un qui a plus de chances de le connaître.

Initialisation: codé en dur

Caches pour accélerer la procédure

Détail: . → org.

```
$ dig +trace hodaur.crans.org

.               472363    IN    NS    k.root-servers.net.
.               472363    IN    NS    b.root-servers.net.
.               472363    IN    NS    e.root-servers.net.
.               472363    IN    NS    m.root-servers.net.
.               472363    IN    NS    a.root-servers.net.
.               472363    IN    NS    l.root-servers.net.
.               472363    IN    NS    i.root-servers.net.
.               516618    IN    RRSIG    NS 8 0 518400 2022011005
0000 20211228040000 14748 . NhT6Cm+50fsJ1eELfgG54zrMuxhQU2nVQP
N1jSVxs sjO6YvjXCbAAsB8vTo22RNraam7vRlxn4asVzHJn6ymLIWePXUn2za
2a yf4w0s5i9ZWCcTbURx2ESM18uUVoOowCWAhWpRME0M6 yu9PdQ==
;; Received 1125 bytes from 192.168.1.1#53
(192.168.1.1) in 13 ms
```

Détail: org. → crans.org.

```
org.                172800    IN    NS    d0.org.afilias-nst.org.
org.                172800    IN    NS    a0.org.afilias-nst.info.
org.                172800    IN    NS    c0.org.afilias-nst.info.
org.                172800    IN    NS    a2.org.afilias-nst.info.
org.                172800    IN    NS    b0.org.afilias-nst.org.
org.                172800    IN    NS    b2.org.afilias-nst.org.
org.                86400     IN    DS    26974 8 2 4FEDE294C53F438
A158C41D39489CD78A86BEB0D8A0AEAFF14745C0D 16E1DE32
org.                86400     IN    RRSIG    DS 8 1 86400 20220110C
50000 20211228040000 14748 . V0v8w8TZL8dwKRwGEvtO0fsWXCzqSPdHO
ZfQ/gHf3jriz5WrrVjptgEf rwAYtKAI2msNNayiE86IjFG1L6Kg5vKkBqbfNe
hKe cvEaO2vb+gMNdAi4j4CtPZoWONmDfo9AZsw2EdZhg2P8Z2JrRDg5X9zo G
cFHaQ==
;; Received 782 bytes from 2001:503:ba3e::2:30#53
(a.root-servers.net) in 20 ms
```

Détail: crans.org. → hodaur.crans.org.

```
crans.org.      86400   IN   NS   silice.crans.org.
crans.org.      86400   IN   NS   freebox.crans.org.
crans.org.      86400   IN   NS   sputnik.crans.org.
crans.org.      86400   IN   DS   54129 14 2 474221FF95
15C2A0D5106DD172A62783100CA05AE749B16572348148 B53E62C3
crans.org.      86400   IN   RRSIG   DS 8 2 86400 20220
115152429 20211225142429 63858 org. VGxV613Dbbcqms0lBvyUsK
Num/d8Zy8L4CJ5SS8TDPjZgs8nYj0g5RIy xx8X0HhcUWaDZDxvtf93kWZ
MGiJjIURhRMQpxKrrtVezzRO33V1bXXkf NDmPKNLFS2zrlZ+GxzyVjYai
Ccc5o+2JWfl8inzq8Mh/SnJ3ZN/TNpwO HcU=
;; Received 425 bytes from 2001:500:e::1#53
(a0.org.afilias-nst.info) in 166 ms
```

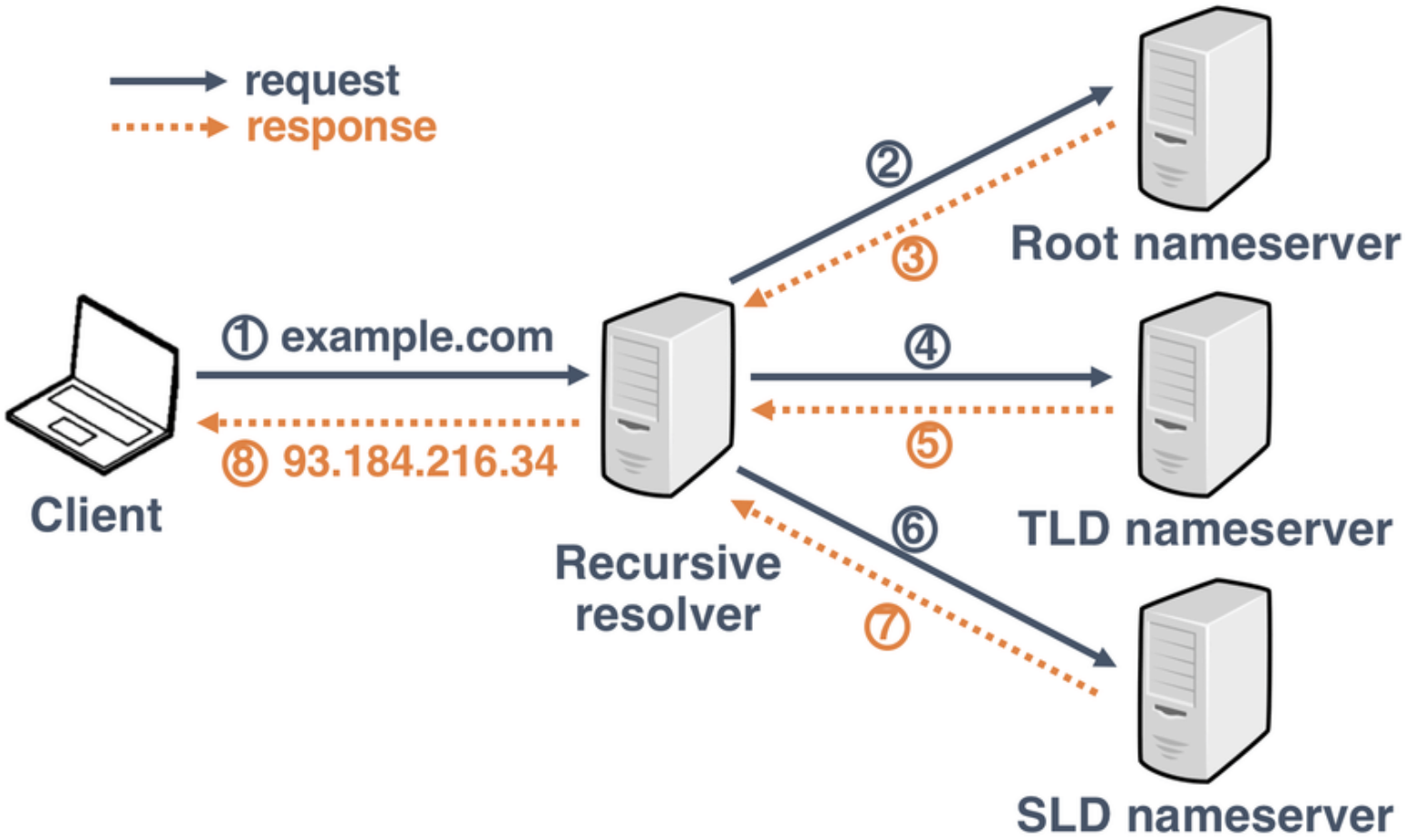
Détail: hodaur.crans.org.

```
hodaur.crans.org.    3600    IN    A    185.230.79.10
hodaur.crans.org.    3600    IN    RRSIG    A 14 3 3600
20220112075124 20211213065803 40871 crans.org. aqZnxxJk
6+LPPclLPxut87hzUcZZYwGsRfAgZKoNOkvuyPLYAW3CcpGs db5NN3
wZZZeJqz80fwbNiElBXaGYtW2l7JL1p2EN6OKjwwwanqkiyCVb 6gYk
v+sBm6Yhqv4+
```

Exceptions

```
dig +trace idp.impots.gouv.fr
→ .
→ fr.
→ impots.gouv.fr
→ idp.impots.gouv.fr
```

Résumé


request
response
②
③
Root nameserver
① example.com
④
⑤
⑧ 93.184.216.34
Client
Recursive resolver
⑥
⑦
TLD nameserver
SLD nameserver

Généralités

> DNS spoofing is a cyberattack that redirects traffic away from legitimate servers to fraudulent sites.

Cache poisoning

- nombreux serveurs enregistrent un cache
  - ⊕ raccourcis
  - ⊕ moins de charge
  - ⊖ mises à jour
  - ⊖ confiance
- si ce cache est modifié malicieusement, le traffic sera redirigé

Autres formes

- Man in the Middle
- Se faire passer pour un serveur de base

DNSSEC

DNS Security Extensions

- garantie d'origine
- intégrité des données
- certification de non-existence

Structure

- optionnel
- se greffe sur la structure arborescente de DNS
- chaque responsable de zone signe les fils et fournit une clé publique pour vérifier la signature
- la racine est codée en dur avec sa clé publique

Champs

- RRSIG: Ressource Record Signature
  Signature du nom de domaine par le parent
- NSEC: Next Secure
  Preuve de non-existence
- DNSKEY
  Clé publique
- DS: Delegation Signer
  Signature des fils

Aparté: NSEC

Preuve de non-existence:

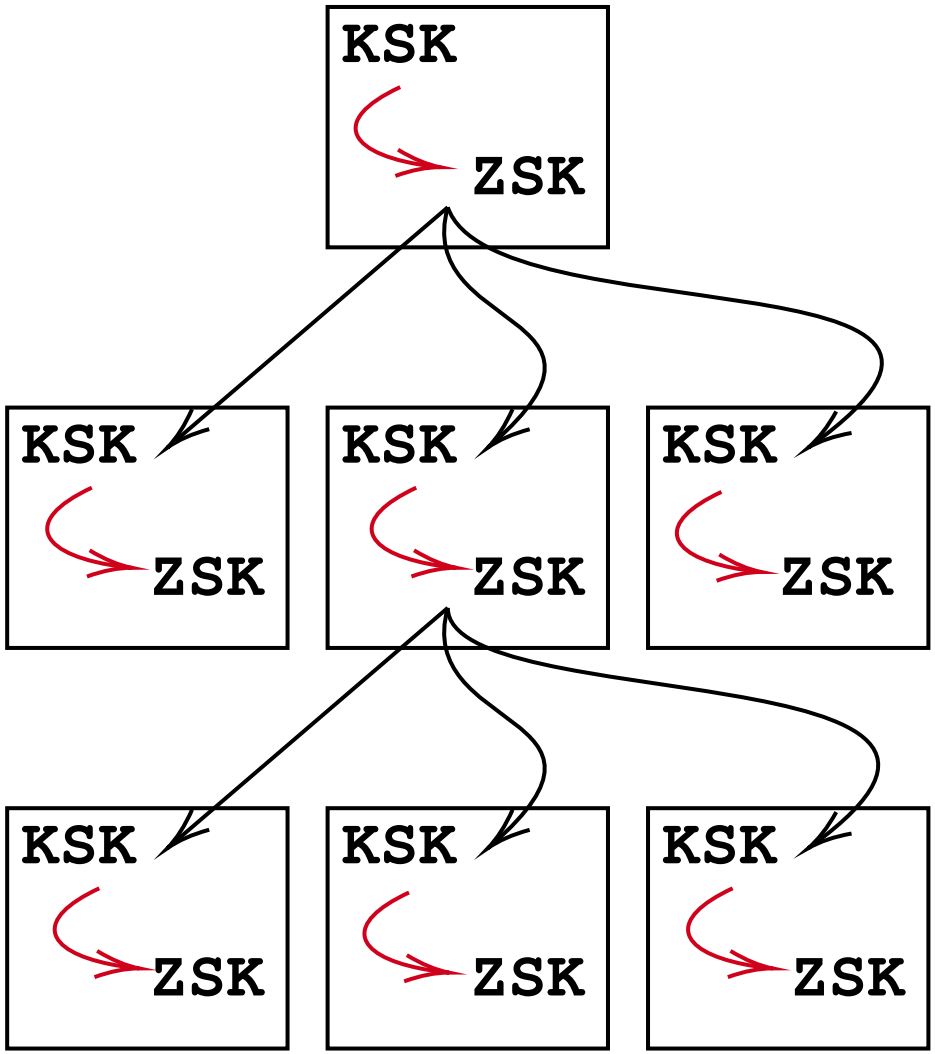
- trier les fils
- si le fils demandé n'existe pas, renvoyer un message signé contenant le suivant et le précédent

`bar`
`baz`
`foo`
`quux`

`eggs`?
→ N'existe pas, suivant `foo`, précédent `baz`

Problème: on peut extraire tous les noms
Solution: NSEC3 avec une couche de hachage en plus

Aparté: ZSK vs KSK



Records

- A (address): 185.230.79.10
- AAAA (address IPv6): 2a0c:700:2::ff:fe01:4502
- DNSKEY (clé publique DNSSEC)
- DS (DNSKEY des sous-domaines)
- MX (mail)
- TXT (fourre-tout): "v=DMARC1;p=none"

`dig +short <TYPE> <SERVEUR>`

e.g. `dig +short TXT _dmarc.crans.org`

Bind

`silice.crans.org`
→ `/var/local/dns/generated/*`

e.g. `grep -r TXT /var/local/dns/generated`

DnsViz

`wiki:CransTechnique/Services/DnS`
`dnsviz.net`

Examples:
`zamok.crans.org`
`truc.crans.org`