# RFC 4471 : Derivation of DNS Name Predecessor and Successor

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2006. Dernière mise à jour le 27 septembre 2006

Date de publication du RFC : Septembre 2006

https://www.bortzmeyer.org/4471.html

---

Le protocole DNSSEC, censé sécuriser le DNS a, tel qu'il est normalisé dans le RFC 4033 [1] un gros défaut : il permet d'énumerer tous les domaines d'une zone signée. C'est cette faille que tente de résoudre notre RFC.

Pour permettre à un serveur DNSSEC de signer la non-existence d'un domaine, le RFC 4033 a normalisé l'enregistrement NSEC. Celui-ci dit "il n'y a aucun domaine avant `XYZ.example`" où XYZ est le label suivant celui demandé. "Suivant" est défini comme "suivant dans l'ordre alphabétique". Le gros problème de cette approche est qu'elle permet ainsi à un attaquant d'obtenir tous les domaines de la zone, par chaînage. C'est ainsi que Simon Josefsson a développé un programme <http://josefsson.org/walker/> de "*zone walking*" qui montre bien la vulnérabilité des zones DNSSEC. Muni du contenu de la zone, un attaquant peut ensuite utiliser whois ou un système équivalent pour obtenir des renseignements à des fins de "*spamming*" ou bien de harcèlement juridique. Le registre britannique, Nominet, avait ainsi refusé de déployer DNSSEC.

Certains, sans avoir suffisamment réfléchi au problème, disent "mais les données de la zone sont publiques, de toute façon", oubliant ainsi que l'obtention de la zone entière (ce que permet le "*zone walking*") est autrement plus dangereux que la posisbilité d'interroger la zone sur quelques noms choisis : c'est bien pour cela que les registres ne distribuent par leur zone (cas de `.fr` ou en tout cas pas gratuitement (cas de Verisign).

Notre RFC s'attaque à ce problème en redéfinissant le mot "suivant". Il spécifie un algorithme qui permet d'obtenir un nom suivant ou précédant celui demandé, sans permettre d'utiliser ce nom suivant ou précédant pour obtenir d'autres noms. Le nom "suivant" ou "précédant" n'est pas vraiment lisible (de nombreux exemples figurent dans le RFC) mais est suffisant pour les besoins de DNSSEC.

Kim Minh Kaplan <http://www.kim-minh.com/> a mis en œuvre notre RFC, en Common Lisp. Son code peut être récupéré avec darcs :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4033.txt`

```
darcs get http://www.kim-minh.com/src/cl-dnssec
cd cl-dnssec
make
```

et ensuite exécuté ainsi :

```
%  ./rfc4471 -- P foobar.example.org. example.org.
P(foobar.example.org., example.org.) = \255{49}.\255{63}.\255{63}.foobaq\255{57}.example.org.
```