Faut-il changer la clé DNSSEC de la racine ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 septembre 2014

https://www.bortzmeyer.org/root-key-rollover.html

Voici le genre de question qui ne va pas angoisser le célèbre M. Michu, mais que se posent sérieusement des tas de techniciens de l'Internet. Cette question a suscité la création récente d'une liste de diffusion très animée <https://mm.icann.org/mailman/listinfo/ksk-rollover>, et fera l'objet d'une réunion à la rencontre ICANN de Los Angeles en octobre prochain.

De quoi s'agit-il et de quoi discute-t-on sur cette liste ksk-rollover ? Les informations diffusées par le DNS sont sécurisées par des signatures cryptographiques, un système connu sous le nom de DNSSEC. Comme le DNS, DNSSEC est décentralisé mais arborescent. Le résolveur DNS qui veut valider (vérifier ces signatures) trouve la clé publique de la zone dans la zone parente, et ainsi de suite jusqu'à la racine, le sommet du DNS, qui est un cas particulier, le résolveur doit en connaître la clé. Typiquement, elle est incluse dans la distribution du logiciel et installée automatiquement. Aujourd'hui, cette clé de la racine, clé de voute de l'authentification des données DNS, est une RSA, a l'identificateur **19036**, et vaut :

```
. IN DNSKEY 257 3 8 (
   AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQ
   bSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh
   /RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWA
   JQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXp
           oY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3
           LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGO
           Yl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGc
           LmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
  ) ; KSK; alg = RSASHA256; key id = 19036
```

(Il y a en fait plusieurs sortes de clés, celle qui est importante, le point de départ de la confiance - "*trust anchor*" - est la KSK, "*Key Signing Key*".) Mais, si on la change, comment mettre à jour (en anglais "*to roll over*") les dizaines de milliers (et demain les centaines de milliers) de résolveurs qui l'utilisent ?

Avant cela, demandons-nous **pourquoi** la changer ? Il peut y avoir au moins deux cas où nous serions **obligés** de la changer : si elle est compromise (si la clé privée est copiée par un méchant) ou si les progrès de la cryptanalyse la rendent trop peu sûre. Aujourd'hui, aucun de ces deux cas ne se présente. Mais,

si cela arrivait (et, au moins pour le premier cas, cela peut arriver du jour au lendemain), nous serions bien embêtés car on n'a jamais essayé une opération aussi complexe.

C'est le principal argument des « changeurs », ceux qui veulent qu'on change de clé : cela n'est pas nécessaire maintenant mais cela permet de tester les procédures et de s'assurer qu'on sait faire, de manière à ne pas être pris au dépourvu en cas de problème. Ils ajoutent que, pour l'instant, seules 10 à 20 % des requêtes DNS passent par un résolveur validant mais que DNSSEC se répand et que donc, plus on attend, plus ce sera dur. Les « conserveurs », eux, disent que c'est déjà trop tard, et que c'est embêtant de changer une donnée aussi critique juste pour faire des tests. Le risque de tout casser (et de donner ainsi une mauvaise réputation à DNSSEC) est trop important.

Par exemple, sur la machine Ubuntu où je tape cet article, il faudrait, si la décision de changer de clé est prise, que je récupère la nouvelle clé (évidemment de manière sécurisée, pas en copiant/collant depuis Twitter) et que j'édite `/etc/unbound/root.key`. Pas évident d'obtenir cela de nombreux administrateurs système dispersés et qui ne lisent pas forcément tous les jours la liste dns-operations <https://lists.dns-oarc.net/mailman/listinfo/dns-operations>... Il existe en théorie des solutions qui éviteraient de mettre à jour manuellement. Certaines sont dépendantes du logiciel. Unbound a son programme `unbound-anchor` qui récupère la clé sur le serveur de l'IANA, en HTTPS, et en vérifiant le certificat. Il y a aussi les mises à jour automatiques ou semi-automatiques des logiciels : si on met à jour son résolveur ainsi, on aura la nouvelle clé. Si on n'est pas trop pressé, cela marchera. Et il y a la technique du RFC 5011 [1] qui permet d'indiquer dans le DNS que l'ancienne clé est révoquée et de publier la nouvelle, signée avec l'ancienne (cela ne marche pas si l'ancienne clé privée a été copiée par un attaquant ; comme le disait l'auteur du RFC dans la discussion sur la liste ksk-rollover « *"If you lose your last trust anchor, you're screwed."* »). Le gros problème du RFC 5011 est qu'il n'a jamais été testé au feu.

Et il y a aussi les questions bureaucratiques, qui prendront certainement dix fois plus de temps que les discussions techniques (pourtant déjà très bavardes), dans le marigot qu'est la gouvernance d'Internet. Pour l'instant, aucune décision n'a été prise. Les discussions se poursuivent...

Et mon opinion personnelle à moi ? Je crains qu'il ne soit effectivement trop tard pour changer la clé de manière propre. Elle est présente en trop d'endroits qu'on ne maitrise pas. Il faudrait mettre en place un vaste programme de mise à jour des logiciels, pour s'assurer que tous mettent en œuvre le RFC 5011 proprement. Quand ce sera fait, dans dix ou vingt ans, on pourra remettre sur le tapis la question du changement ("*rollover*") de clé.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5011.txt`