Faut-il remplacer régulièrement les clés DNSSEC ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 avril 2011

http://www.bortzmeyer.org/remplacement-cles.html

Je ne l'ai pas fait exprès mais une bonne partie des discussions qui ont suivi mon exposé à la conférence SATIN <http://www.bortzmeyer.org/satin.html> le 4 avril, ont porté sur la question qui figure en titre, le remplacement des clés ("*key rollover*").

En effet, DNSSEC repose sur des clés cryptographiques qui vont par paire, une privée et une publique. Le conseil souvent donné dans les cours et formations DNSSEC est de changer ces clés régulièrement. Pourquoi ? Et est-ce vraiment une bonne idée ?

Il y a plusieurs raisons possibles pour changer les clés assez souvent (du genre, tous les deux mois pour une clé de 1024 bits) :

- Pour des raisons cryptographiques : le plus longtemps la clé reste en service, le plus de temps les cryptanalystes auront à leur disposition pour la casser (d'où le lien entre la taille de la clé et l'intervalle de remplacement).
- Pour des raisons opérationnelles : on aura toujours besoin de changer des clés dans certains cas (par exemple parce qu'on découvre soudainement qu'une clé privée a été copiée par un méchant ou simplement par précaution parce qu'un membre important de l'équipe est parti, et qu'on préfère changer le matériel cryptographique auquel il avait accès ; n'oubliez pas que les clés DNSSEC n'expirent pas toutes seules). L'idée est que, si on ne fait des remplacements que contraints et forcés, les procédures ne seront pas réellement testées, et les employés ne sauront pas vraiment quoi faire. Au contraire, si le remplacement est de la routine, les remplacements forcés passeront comme une lettre à la Poste.

Il y a aussi des raisons de ne **pas** changer les clés systématiquement et souvent :

- Chaque changement est une modification d'une donnée importante, et peut déclencher des bogues dans les logiciels. Ce n'est pas juste de la paranoïa, c'est ce qui est arrivé à .FR <https://www.dns-oarc.net/files/workshop-201103/DNSSEC_Key_Deletion_Issue-Vincent_Levigneron-afnic.pdf> (voir aussi la discussion sur la liste dns-operations <https://lists.isc.org/pipermail/bind-users/2011-February/082743.html>).
- Faire des remplacements de clés complique l'ensemble du système et peut décourager les administrateurs réseau de mettre en place DNSSEC.

Alors, quel est le consensus sur ce point ? Eh bien justement, il n'y a pas eu de consensus, si la majorité des participants à la conférence SATIN semblait pencher pour le remplacement fréquent et « gratuit », une minorité n'était pas d'accord. Le premier point de discussion portait sur la validité de l'argument cryptographique : compte-tenu de l'état de la sécurité du DNS aujourd'hui (très bas), se préoccuper d'un éventuel cassage d'une clé RSA de 1024 bits est-il vraiment pertinent ? De fait, l'argument cryptographique n'a été défendu par personne.

L'autre argument, l'opérationnel, est plus sérieux : il est clair qu'une procédure qui n'existe que sur papier, qui n'a jamais été testée, ne vaut rien. La crainte des « remplaceurs » (qui plaident pour des remplacements fréquents, afin que l'équipe d'exploitation ne perde pas la main) est que, en l'absence de ces remplacements fréquents, le jour où il y aura un problème nécessitant un remplacement d'urgence, personne ne sache réellement faire.

L'argument était contesté sur deux bases :

— Les remplacements d'urgence (face à une compromission d'une clé privée, par exemple, ou suite à une panne physique d'un HSM) ne sont pas comparables aux changements réguliers, qui peuvent être automatisés. Ces changements réguliers ne garantissent donc pas que tout se passera bien lors d'un remplacement d'urgence.
— Le DNS est un système vital, avec lequel on ne peut pas jouer juste pour s'entraîner. Pour habituer le pilote de ligne à voler avec un moteur en panne, on ne coupe pas un réacteur de l'avion à chaque vol !

Dans le cas de l'avion, la solution est la multiplication d'exercices sur simulateur. Transposé à l'informatique, cela veut dire des exercices réguliers sur un banc de test. Ce banc de test se comportera-t-il toujours comme la réalité ? C'est le reproche que font les remplaceurs.

Bref, pas d'accord encore. Au minimum, si on remplace souvent les clés, il faut le faire avec un logiciel qui marche (je suggère OpenDNSSEC <http://www.bortzmeyer.org/opendnssec-debut.html>). Mon étude présentée à SATIN <http://www.bortzmeyer.org/satin.html> montrait que les problèmes liés aux remplacements de clés sont toujours fréquents en pratique.