Faut-il vraiment pouvoir rebouter l'Internet ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 juillet 2010

https://www.bortzmeyer.org/rebouter-internet.html

On le sait, la grande majorité des articles concernant l'Internet sont faux et, en prime, souvent ridiculement faux. Cela concerne évidemment les médias traditionnels (presse, télévision, etc) mais aussi les forums en ligne où les deux cents commentaires à un article sont écrits par des gens dont la seule compétence technique est l'installation de WordPress (et, parfois, ne soyons pas trop méchants, l'écriture de dix lignes de PHP). Mais des records ont été récemment battus à propos de la légende comme quoi « Sept personnes ont les clés pour rebouter l'Internet ».

Le point de départ de la légende semble avoir été un communiqué publicitaire de l'Université de Bath, « "*Bath entrepreneur holds key to internet security*" <http://www.bath.ac.uk/news/2010/07/26/internet-security/> ». Ce communiqué outrageusement cireur de pompes contenait beaucoup d'erreurs et a été repris, aussi bien dans la presse bas de gamme comme Metro (« "*Brit given a key to 'unlock' the internet*" <http://www.metro.co.uk/news/836210-brit-given-a-key-to-unlock-the-internet
que dans des médias prétendument sérieux comme la BBC (« "*Bath entrepreneur 'holds the key' to internet security*" <http://news.bbc.co.uk/local/bristol/hi/people_and_places/newsid_8855000/8855460.stm> », notez la reprise quasi-littérale du titre du communiqué de presse) ou comme le Guardian (« "*Is there really a key to reboot the internet ?*" <http://www.guardian.co.uk/technology/2010/jul/27/internet-key> », l'article le moins mauvais du lot).

La légende a ensuite franchi la Manche et, dans la traduction, le côté chauvin et la publicité pour une personne particulière ont disparu. Cela a donné « Sept personnes ont les clés d'Internet ! <http://www.gizmodo.fr/2010/07/29/sept-personnes-ont-les-cles-d%e2%80%99internet.html> », « Les sept clés de l'Internet sécurisé <http://www.20minutes.fr/article/586733/Web-Les-sept-cles-de-l-php> » ou « Rebooter internet - Comment ça marche ? <http://www.korben.info/rebooter-internet-comment-html> » (de moins mauvaise qualité).

Bon, qu'il y a t-il de vrai dans cette légende ? Sur quoi cela s'appuie t-il ? Depuis le 15 juillet dernier, le processus de signature de la racine du DNS par le système DNSSEC est complet : les serveurs de noms de la racine diffusent désormais des informations signées, ce qui permet de détecter des tentatives de modification des données, comme celles utilisant la faille Kaminsky <https://www.bortzmeyer.

org/comment-fonctionne-la-faille-kaminsky.html>. Tout ce processus est largement documenté sur le site officiel <http://www.root-dnssec.org/> et il est symptomatique qu'aucune des personnes qui ait écrit à ce sujet ne l'ait consulté. À l'ère d'Internet, toute l'information est gratuitement et librement disponible, encore faut-il la lire !

Notons d'abord que ce processus ne concerne que le DNS. Certes, ce protocole d'infrastructure est indispensable au bon fonctionnement de la quasi-totalité de l'Internet. Sans lui, on serait limité à des ping (en indiquant l'adresse IP) et à des traceroute (avec l'option `-n`). Certains services, comme le Web, dépendent encore plus du DNS. Néanmoins, on voit que parler d'un « redémarrage de l'Internet » est ridicule, que DNSSEC fonctionne ou pas n'empêchera pas le réseau de faire passer des paquets.

Ensuite, dans ce processus, quel est le rôle des fameux sept gusses ? Leur nom est disponible sur le site officiel <http://www.root-dnssec.org/tcr/selection-2010/> (alors que certains articles disaient « on ne connait que certains d'entre eux » et autres phrases censées faire croire qu'on révélait au lecteur des secrets stratégiques). Leur rôle est décrit dans le document « "*Trusted Community Representatives [Caractère Unicode non montré* [1] *] Proposed Approach to Root Key Management*" <http://www.root-dnssec.org/wp-content/uploads/2010/04/ICANN-TCR-Proposal-20100408.pdf> », document qui a été publié il y a des mois. Le processus complet figure dans « "*DNSSEC Practice Statement for the Root Zone KSK Operator*" <https://www.iana.org/dnssec/icann-dps.txt> ». DNSSEC fonctionne en signant cryptographiquement les enregistrements distribués. Il dépend donc d'une clé privée qui doit à la fois être disponible (pour signer) et être protégée pour éviter que les méchants ne mettent la main dessus. (À propos de méchant, tout article qui parle d'« attaque terroriste » est grotesque. Comme si Al-Qaida, spécialiste des bombes et des égorgements, avait tout à coup envie d'empêcher les riches pays du Nord de regarder YouTube.) Un des risques possibles est la perte complète de la clé privée (suite à un incendie ou à un tremblement de terre, risques autrement plus importants que la mythique attaque terroriste). Il y a donc des sauvegardes mais celles-ci sont protégées par chiffrement. Et c'est là qu'interviennent les TCR.

Il y a deux sortes de TCR (« "*Trusted Community Representatives*" »), choisis pour assurer des rôles de gestions des clés cryptographiques de DNSSEC. Il y a les « "*Crypto Officers*" » qui vont s'occuper de la génération des clés (au cours de solennelles cérémonies <http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-ceremonies-01.txt>) et les « "*Recovery Key Share Holders*" » (les fameux sept). Ces derniers sont simplement chargés de garder une partie de la clé qui permettra le déchiffrement des sauvegardes. C'est tout. Ils ne peuvent pas « redémarrer l'Internet », ce qui ne veut rien dire. Mais, si les articles sensationnalistes avaient commencé par « Sept personnes peuvent restaurer les sauvegardes des clés DNSSEC », gageons qu'ils auraient eu moins de succès...

Enfin, il faut relativiser : à l'heure actuelle, si un certain nombre de domaines sont signés par DNSSEC (par exemple, hier, `.dk` et `.edu` ont rejoint la liste des TLD dont la racine authentifie la signature), pratiquement aucun **résolveur** DNS (les serveurs directement interrogés par les utilisateurs) ne valide avec DNSSEC. Que la clé privée soit compromise ou pas ne changera rien, puisque les signatures sont ignorées. Il faudra sans doute des années avant que les résolveurs de M. Tout-le-Monde dépendent d'une signature DNSSEC. La remarque de Bruno <http://blog.spyou.org/wordpress-mu/2010/07/29/ils-vont-nous-redemarrer-internet/>, « les 7 gugusses et leurs cartes à puce ont autant de pouvoir sur le bon fonctionnement d'Internet que mon chat sur le problème des embouteillages sur le periph parisien » est donc à 100 % justifiée.

1. Car trop difficile à faire afficher par LaTeX