Cafouillage entre .PR et le registre DLV de l'ISC

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 septembre 2009

https://www.bortzmeyer.org/dlv-pointpr.html

DNSSEC, technologie chargée d'améliorer la sécurité du DNS, est une source de distractions sans fin pour l'administrateur système. Depuis que j'ai activé la validation DNSSEC sur le résolveur de ma machine au bureau, je vois des problèmes qui sont évidemment complètement invisibles si on ne vérifie pas les signatures DNSSEC. Ce fut le cas cette semaine avec la panne de .pr.

Comme toute technique cryptographique, DNSSEC (normalisé dans le RFC 4033 [1] et suivants), produit des **faux positifs**, des cas où la vérification échoue, sans qu'il y aie eu de tentative de fraude, simplement parce que la cryptographie est compliquée et que les erreurs opérationnelles sont fréquentes. Avant d'améliorer la sécurité, la cryptographie sert donc souvent à casser des choses qui marchaient très bien avant qu'on ne l'utilise.

Le registre DNS de .pr a tenu à être un des premiers domaines de tête à signer avec DNSSEC. Mais leurs moyens humains ne semblent pas à la hauteur de leurs ambitions et il y a déjà eu plusieurs cafouillages, par exemple des signatures expirées ou, en dehors de DNSSEC, des attaques par injection SQL <https://www.bortzmeyer.org/attaques-registres-noms.html>. Ce mois-ci, .pr a procédé à un changement de sa clé, certainement l'opération la plus dangereuse de DNSSEC. Cette opération a été assez mal faite, notamment parce que les administrateurs du domaine continuent à laisser l'ancienne clé sur leur site Web <http://dnssec.nic.pr/serverconf.php> mais aussi parce qu'ils n'ont attendu que deux jours entre l'ajout de leur clé dans ITAR <https://www.bortzmeyer.org/itar-dnssec.html> et le retrait de l'ancienne. Or, la racine du DNS n'étant pas signée, et le suivi à la main de toutes les clés de tous ceux qui signent n'étant pas réaliste, les très rares personnes qui, comme moi, utilisent un résolveur DNSSEC validant, se servent en général du registre DLV de l'ISC. DLV ("*DNSSEC Lookaside Validation*"), normalisé dans le RFC 5074, permet de ne gérer qu'une seule clé, celle du registre DLV, qui contient les autres clés. Heureusement que, grâce à l'ISC, ce registre DLV existe. Mais, problème, dlv.isc.org, ne se mettait apparemment à jour à partir d'ITAR que toutes les semaines. Résultat, l'ancienne clé de .pr a été retirée de la zone alors qu'elle était encore dans DLV (et, on l'a vu, sur le site Web du registre de .pr, donc le problème ne concerne pas que DLV).

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

Résultat, un beau SERVFAIL ("*Server Failure*") à chaque tentative de résolution d'un nom en .pr. Gageons que cela n'encouragera pas les administrateurs de serveurs DNS récursifs à activer la validation DNSSEC.

L'incident a également réanimé tous ceux qui n'avaient pas apprécié le travail de l'ISC pour la mise en place du registre DLV. Pas mal de noms d'oiseaux ont été échangé sur des listes de diffusion comme celle du groupe de travail dnsop de l'IETF <http://tools.ietf.org/wg/dnsop>. Après tout, ce sont toujours ceux qui font le travail concret qui attirent les reproches...