Conséquences politiques du déploiement des RPKI

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 septembre 2010

https://www.bortzmeyer.org/rpki-et-igp.html

Il est curieux de constater que la gouvernance des noms de domaine déplace autant de vent et suscite autant de réunions internationales (voir par exemple le FGI qui se tient en ce moment à Vilnius) alors que celle du routage, plus cruciale pour l'Internet, se fait essentiellement derrière des portes closes, dans des petits cercles fermés. Ainsi, le déploiement, déjà en cours <https://www.bortzmeyer.org/certificats-ressources-internet.html>, d'une **RPKI** ("*Resource Public Key Infrastructure*", IGC de routage) se fait dans la plus grande discrétion. Il est temps de discuter des implications politiques de ce déploiement, ce que fait l'excellent papier de l'IGP <http://www.internetgovernance.org/>, « "*Building a new governance hierarchy : RPKI and the future of Internet routing and addressing*" <http://blog.internetgovernance.org/blog/_archives/2010/9/7/4624281.html> ».

C'est un très bon document qui sera lu avec intérêt par le petit nombre de gens qui s'intéressent à la fois à l'aspect technique (ici, il s'agit de protéger le protocole de routage BGP contre des attaques ou des problèmes comme les fantaisies de Pakistan Telecom <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>) et à l'aspect politique (le rôle des RIR, la distribution de pouvoir entre eux et l'ICANN et les opérateurs). Mais un petit avertissement tout de même : l'article commence par annoncer qu'il va être consacré à l'information du lecteur, sans prendre position, mais ce n'est pas tout à fait exact : l'article penche plutôt du côté de l'inquiétude, mettant en avant le fait que la RPKI va augmenter le pouvoir des RIR, au détriment des FAI (et sans doute de l'ICANN). En effet, à l'heure actuelle, le pire que puisse faire un RIR est de retirer une plage d'adresses de sa base de données (celle qu'on peut consulter avec whois). Cela ne change rien au routage, sauf pour la minorité d'opérateurs qui filtre les annonces BGP en se fiant aux bases des RIR. Le RIR ne pourra même pas réaffecter d'autorité cette plage à un autre utilisateur car, si l'ancien continue à l'annoncer, la réaffectation punira davantage le nouveau client innocent que le titulaire historique.

En effet, le principe des RPKI est d'attribuer des certificats aux titulaires de ressources comme les plages d'adresses IP. Les routeurs BGP acceptent ensuite (ou pas) les annonces selon qu'elles sont signées (ou pas) avec la clé indiquée dans le certificat. Le rôle essentiellement administratif des RIR devient donc un rôle opérationnel, avec possibilité d'influer directement sur les politiques de routage.

C'est une importante différence avec le déploiement de DNSSEC, où le même IGP <http://www.internetgovernance.org/> a exprimé des craintes que cela ne mène à une plus grande centralisation du DNS. Mais le DNS a a toujours été hiérarchique, le gouvernement états-unien, via son sous-traitant VeriSign, a toujours eu la possibilité de supprimer ou d'ajouter un TLD comme il le voulait <https://www.bortzmeyer.org/fin-de-yu.html>. DNSSEC ne change donc pas grand'chose à l'équilibre existant. Au contraire, aujourd'hui, les RIR n'ont pas la possibilité d'agir sur le routage (et ils le répètent à l'envi, « nous allouons des ressources virtuelles, c'est tout »). Avec la RPKI et un BGP sécurisé, on a donc un vrai changement de pouvoir.

Pourtant, cet important changement de politique de l'Internet a été très peu discuté et notamment pas dans les cercles habituels comme l'ICANN ou le FGI. Il est vrai que ceux-ci sont plus remplis d'avocats ou de politiciens que de gens qui comprennent le routage Internet, son importance et ses conséquences. Le papier de l'IGP explique bien qu'il n'y a nul complot pour dissimuler la vérité aux masses : il suffit de ne pas trop en parler, de présenter le sujet comme essentiellement technique, et le tour est joué, personne ne s'y intéresse.

Le déploiement en cours de RPKI est d'autant plus important qu'il n'a, pour l'instant, n'avait fait l'objet d'aucune décision formelle (depuis, l'IETF a publié une série de RFC <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> sur un routage sécurisé, cf. aussi les RFC 4272 [1], RFC 4593 et RFC 5123). Et, du côté des RIR, il semble qu'aucun d'eux n'avait développé à l'époque une politique concernant la RPKI (fouillez vous-même les politiques du RIPE <http://www.ripe.net/ripe/docs/>, vous n'y trouverez que des propositions, comme la 2008-04 <http://www.ripe.net/ripe/policies/proposals/2008-04.html>), celle-ci étant simplement présentée comme un service optionnel. Il est vrai que l'aspect « sécurisation de BGP », quoique plus vendeur, est peut-être moins motivant pour le déploiement des RPKI que l'arrivée prochaine du marché des adresses IPv4, après l'épuisement proche de celles-ci <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> (ce point est à peine mentionné dans l'article de l'IGP).

On ne peut donc que recommander la lecture de cet article pour encourager le débat. Une version plus longue a été produite par la suite, « "*Negotiating a New Governance Hierarchy : An Analysis of the Conflicting Incentives to Secure Internet Routing*" <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2021835> ».

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4272.txt