RFC 5123 : Considerations in Validating the Path in BGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 avril 2008

Date de publication du RFC : Février 2008

https://www.bortzmeyer.org/5123.html

La sécurité du protocole BGP, par lequel les routeurs Internet échangent l'information sur les routes existantes, est depuis longtemps un sujet de préoccupation. Actuellement, BGP (RFC 4271 [1]) n'offre quasiment aucune sécurité contre les usurpations (un routeur annonce une route qu'il n'a pas « le droit » d'annoncer, comme lors de la récente usurpation perpétrée par Pakistan Telecom <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>). Pourquoi ne valide t-on pas les routes annoncées ? En partie parce que c'est plus compliqué que ça n'en a l'air, comme l'explique ce récent RFC.

Beaucoup de gens, étonnés qu'un technicien incompétent à Karachi puisse stopper l'activité d'un site Web stratégique et essentiel uniquement en détournant son trafic grâce à BGP, réclament des mesures drastiques et notamment la **validation** des routes annoncées par BGP. Certains opérateurs, rares, font une validation partielle, en général basée sur le contenu des IRR. Pourquoi cette pratique n'est-elle pas plus répandue ?

Les mécanismes existants de sécurité comme BGP-MD5 (RFC 2385) ou TCP-AO (RFC 5925) ne sécurisent que le **canal** de communication entre deux routeurs. Ils permettent d'être sûr de l'identité du pair BGP, mais pas de valider ce qu'il annonce. Le routeur de Pakistan Telecom était authentique, il était aussi menteur et BGP-MD5 ne protège pas le **message**, uniquement le canal.

Notre RFC fait donc la liste des points à vérifier lors d'une validation. Le premier (section 1.1) est évidemment de savoir si l'AS d'origine est autorisé à annoncer cette route. C'est un point crucial mais qui n'est pas le sujet de notre RFC, qui se consacre au devenir ultérieur de cette annonce. Plusieurs autres questions sont ensuite posées dans le RFC. Par exemple, la section 1.3 demande « Est-ce que l'annonce par un routeur qui n'est pas de l'AS d'origine est autorisée ? » et explique que la question est bien plus subtile qu'elle ne le semble puisqu'il y a en fait trois sous-questions derrière cette question apparemment simple :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4271.txt

— L'autorisation d'annoncer une route particulière, par exemple `192.0.2.128/25` ("*route authorization*").
— L'autorisation d'annoncer un préfixe qui inclus la route, par exemple `192.0.2.0/24` ("*reachability authorization*").
— L'autorisation de faire transiter les paquets par son réseau ("*transit authorization*").

Ces trrois autorisations, à première vue équivalentes, peuvent en fait donner des résultats différents, comme le montrent les exemples ultérieurs.

Citons uniquement un exemple, présenté en section 2.2, qui exploite le fait que la route réellement empruntée n'est pas contrôlée par la source mais par chaque AS intermédiaire. Un AS annonce à son voisin une route avec un chemin d'AS, mais, en interne, il a une route statique qui prend un autre chemin. L'annonce est-elle valide ? L'AS annonceur était autorisé à annoncer cette route ("*route authorization*" et "*reachability authorization*") mais il est impossible de déterminer s'il y avait "*transit authorization*" puisque le chemin réellement emprunté n'apparait pas dans l'annonce.

Globalement, ce RFC fait à mon avis œuvre utile en expliquant la complexité du routage Internet. Il donne parfois un peu trop dans le pinaillage en montant en épingle des cas intéressant mais très rares. Le vrai problème de la validation des routes en BGP est plutôt l'absence d'un système de « droit d'usage » permettant de savoir qui a le droit d'annoncer telle route. Sans un tel système, les protocoles sécurisés de diffusion de routes (qui existent, et reposent sur la cryptographie) n'ont rien sur lequel se baser. (Un groupe de travail de l'IETF, RPSEC `<http://tools.ietf.org/wg/rpsec>`, travaille actuellement à un cahier des charges pour un routage sécurisé. Un exemple de mécanisme permettant de valider les annonces de route a été publié début 2012 `<https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>`.)