Repenser la sécurité du routage Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 février 2017

https://www.bortzmeyer.org/rethinking-routing-security.html

Ah, voilà une question qu'elle est bonne : comment améliorer la sécurité du routage Internet ? On sait qu'elle n'est pas bonne, on sait que n'importe qui <https://www.bortzmeyer.org/bgp-malaisie.html> ayant accès à un routeur de la DFZ peut annoncer les routes qu'il veut et ainsi détourner du trafic. On sait aussi qu'il existe plusieurs techniques pour limiter les dégâts. La question est : sont-elles bonnes, et ne perd-on pas du temps avec des techniques compliquées lorsque de plus simples marcheraient presque aussi bien ? C'est, en gros, l'argument des auteurs de cet excellent article de Robert Lychev, Michael Schapira et Sharon Goldberg, « "*Rethinking Security for Internet Routing*" <http://cacm.acm.org/magazines/2016/10/207763-rethinking-security-for-internet-routing/> ».

(Au passage, je n'ai pas trouvé cet article en ligne - le dinosaure ACM, pourtant censé être une association d'**informaticiens**, ne le permet pas - mais on peut le télécharger via l'excellent Sci-Hub. Encore merci à son auteure, pour cet indispensable apport à la science.)

Pour empêcher quelqu'un d'annoncer une route illégitime dans l'Internet, on a plusieurs solutions (qui ne sont pas incompatibles : on peut en déployer plusieurs, voir RFC 7454 [1]). On peut valider les annonces reçues de ses pairs BGP contre un IRR ("*prefix filtering*", dans l'article ; sur les IRR, voir le RFC 7682). On peut utiliser les techniques qui reposent sur la RPKI comme les ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> ("*origin validation*" dans l'article) ou comme le futur BGPsec ("*path validation*", dans l'article, les RFC sur BGPsec ne sont pas encore sortis). On peut même ne rien faire et corriger après coup <https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html> quand une annonce anormale apparait. Ces techniques ont en commun de nécessiter qu'on connaisse bien ses adresses IP et sa connectivité (ne riez pas, certains opérateurs ont du mal ici !) La RPKI stocke à peu près 5 % des routes de l'Internet aujourd'hui.

Les auteurs de « "*Rethinking Security for Internet Routing*" <http://cacm.acm.org/magazines/2016/10/207763-rethinking-security-for-internet-routing/> » ont testé (enfin, simulé).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7454.txt

Sur un banc de test représentant une partie de l'Internet, ils ont essayé plusieurs stratégies et les résultats ne sont pas ceux qu'on attendait. Si le filtrage des annonces des clients était complètement déployé, il bloquerait presque autant d'attaques que les techniques plus sophistiquées de ROA ou de BGPsec. Cela montre que les techniques simples et anciennes sont souvent très efficaces.

Évidemment, c'est irréaliste : on n'a jamais une technique de sécurité qui soit complètement déployée partout. Toute analyse doit tenir compte des « maillons faibles », qui ne vérifient rien. Mais, même dans ce cas, leur simulation montre que le filtrage à la source est efficace. Pensez à cela la prochaine fois que votre transitaire vous embêtera à exiger que vos routes apparaissent dans la base d'un RIR : c'est pénible, mais c'est efficace contre les détournements.