La sécurité de BGP et l'importance des réactions rapides

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 septembre 2008

https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html

---

Des problèmes récents comme l'attaque involontaire de Pakistan Telecom contre Youtube <https://www.bortzmeyer.org/pakistan-pirate-youtube.html> ou comme la polémique autour des annonces de l'ancienne adresse d'un serveur racine du DNS <https://www.bortzmeyer.org/qui-controle-les-s html> ont ravivé l'intérêt pour les problèmes de sécurité de BGP. L'annonce en août 2008 d'un nouveau moyen pour limiter le risque d'être détecté lorsqu'on fait des fausses annonces BGP <https://www.bortzmeyer.org/faille-bgp-2008.html> a encore renforcé l'inquiétude. Certains se posent donc la question : pourquoi ne « sécurise » t-on pas BGP ? Pourquoi n'importe quel incompétent à Pakistan Telecom peut-il détourner l'accès à un service vital et stratégique comme Youtube ?

La réponse à cette question est parfois « parce que l'Internet a été conçu par des étudiants hippies et irresponsables qui ne pensaient pas à la sécurité ; aujourd'hui que l'Internet est une ressource critique, il faudrait prendre la sécurité de BGP plus au sérieux ». Cette position laisse entendre qu'on pourrait sécuriser BGP pour peu qu'on le veuille vraiment. Mais c'est trop simpliste. Voyons pourquoi.

BGP, normalisé dans le RFC 4271 [1], fonctionne entre **pairs**, des routeurs qui ont été configurés pour échanger de l'information sur les routes disponibles. Chaque routeur peut accepter et refuser les routes annoncées par son pair, selon des critères choisis unilatéralement, et ils ne s'en privent pas (le RFC 5291 fournit un mécanisme - facultatif - pour informer son pair). Les deux pairs étant en général proches physiquement, souvent sur un câble dédié, la sécurité du canal BGP n'est guère en cause (on peut l'améliorer avec IPsec mais la plupart des opérateurs préfèrent la solution du RFC 2385, qui sera peut-être remplacée dans le futur par celle du RFC 5925). Le problème n'est pas d'authentifier le pair voisin, le problème est d'authentifier ce qu'il raconte ! Sachant que les annonces BGP sont transmises de routeur en routeur, comment garantir une chaîne de confiance depuis le premier ? En d'autres termes, si mon voisin m'annonce qu'il a entendu qu'il y avait une route vers 192.0.2.0/24, et qu'il le sait parce que lui-même l'a entendu d'un de ses voisins, comment savoir si cette route est authentique, d'autant que ce terme même n'est pas clairement défini (cf. RFC 5123) ?

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

Alors, comment authentifier des annonces BGP ? Les propositions actuelles, comme "*Secure BGP*" <http://www.ir.bbn.com/sbgp/> ou soBGP <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html>, actuellement discutées au sein du groupe de travail SIDR de l'IETF <http://www.ietf.org/html.charters/sidr-charter.html> ne sont pas nouvelles. Elles visent à mettre au point un mécanisme de signature cryptographique des annnonces BGP. Le RIR qui attribue un préfixe IP signera cette attribution, permettant à l'opérateur qui a reçu le préfixe de signer ses annonces. Les RFC normalisant cette technique ont été publiés début 2012 <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.

La principale difficulté commune à tous ces mécanismes est que la hiérarchie d'attribution des adresses IP (de l'IANA vers les RIR puis vers les LIR) ne correspond pas très bien au maillage BGP, qui, lui, n'est pas hiérarchique. Le client final annonce sa route (s'il fait du BGP lui-même) ou bien la fait annoncer par qui il veut, sans que le LIR par qui il a obtenu l'adresse n'approuve ou même soit au courant. Et c'est sans même parler des adresses PI, qui ne sont pas liées à un LIR. Changer ce mécanisme est certainement possible, mais cela change le modèle de fonctionnement de l'Internet. Et cela donnerait un plus grand pouvoir aux opérateurs puisque seules les annonces approuvées par eux pourront être faites.

Bien sûr, les annonces qui sont faites sont normalement annoncées dans les IRR. Mais les IRR publics sont souvent de piètre qualité. Certains sont assez à jour, par exemple celui du RIPE-NCC mais ce n'est pas le cas de tous (parfois tout simplement parce que les procédures de mise à jour sont trop strictes). Certaines entreprises ont leur propre IRR, tâche assez lourde. Il n'est donc pas étonnant que le filtrage des annonces BGP sur la base des IRR (n'accepter que les routes qui sont publiées dans un IRR) aie eu assez peu de succès : comme l'ont montré beaucoup d'études et d'expériences douloureuses, ce filtrage rencontre beaucoup de faux positifs (des routes légitimes refusées) et également des faux négatifs (routes illégitimes acceptées quand même). Il faut aussi se rappeler que, dans le cas du « détournement » du serveur racine L <https://www.bortzmeyer.org/qui-controle-les-serveurs-racine.html>, l'annonce « anormale » était bien faite par le titulaire du préfixe...

Alors, n'y a t-il pas d'espoir pour la sécurité et la stabilité de l'Internet ? Notons d'abord que, bien que triviales en pratique et très connues, les vulnérabilités de BGP n'ont pas eu pour conséquence des attaques nombreuses. Une des raisons est que tout le monde voit l'attaque et peut réagir et tomber sur le dos du responsable. Jusqu'à l'annonce de Kapela & Pilosov <https://www.bortzmeyer.org/faille-bgp-2008.html>, ces « attaques » (souvent en fait, des erreurs) étaient détectées et corrigées très vite. C'est un point important de la sécurité de l'Internet : celui-ci n'a pas la sécurité d'un bloc de béton, passif et n'étant protégé que par sa résistance aveugle. L'Internet est plutôt un organisme vivant : très vulnérable, mais aussi très réactif, doté d'un système immunitaire particulièrement efficace, puisque ses leucocytes sont intelligents...

L'Internet peut ainsi réagir à une large gamme d'attaques, y compris des attaques pas encore inventées. Lors de l'attaque contre Youtube, la détection, l'identification du responsable et la correction avaient été faites en quelques heures.

C'est pour cela que, jusqu'à présent, les armes les plus efficaces contre les détournements BGP ont été des systèmes d'alerte <https://www.bortzmeyer.org/alarmes-as.html> comme MyASN <http://www.ris.ripe.net/myasn.html> ou bien IAR <http://cs.unm.edu/~karlinjf/IAR/index.php>. Ces systèmes fonctionnent aussi lors d'attaques du style Kapela & Pilosov. En effet, le détournement de Youtube avait été noté car plus personne ne pouvait travailler, sans ce service indispensable. Si l'attaquant avait utilisé les techniques mises au point par Kapela et Pilosov, il aurait pu échapper à la détection, mais pas si Youtube avait utilisé MyASN (ils utilisent probablement un tel service).

Un peu plus lointain, d'autres systèmes sont actuellement mis au point pour donner du temps aux administrateurs réseaux en cas de détournement, évitant ainsi d'avoir une perturbation, même de

durée limitée. C'est ainsi que "*Pretty Good BGP*" <http://cs.unm.edu/~karlinjf/pgbgp/> ralentit délibérement la propagation de nouvelles routes (considérées suspectes par défaut) pendant 24 heures. Ainsi, une équipe réactive pourra arrêter le détournement avant qu'il ne soit accepté par les routeurs. (Une mise en œuvre de "*Pretty Good BGP*" est disponible <http://cs.unm.edu/~karlinjf/pgbgp/#[[PGBGP%2BQuagga]]> pour Quagga.)

---

https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html