RFC 4272 : BGP Security Vulnerabilities Analysis

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 21 janvier 2006

Date de publication du RFC : Janvier 2006

https://www.bortzmeyer.org/4272.html

BGP est un protocole absolument vital au bon fonctionnement de l'Internet et il est toujours amusant et parfois un peu inquiétant de s'apercveoir qu'il est très peu sécurisé. Ce RFC fait le point sur les vulnérabilités de BGP, notamment sur celles qui affectent la communication directe entre deux pairs, deux routeurs BGP.

BGP, décrit dans le RFC 4271 [1], est le protocole d'échange de routes dans l'Internet. Si on peut compromettre des routeurs grâce à une faiblesse de BGP, on peut, comme l'explique bien l'introduction de notre RFC, couper une partie de l'Internet mais aussi détourner tout le trafic à son profit (par exemple pour l'espionner) ou bien tricher sur son adresse IP (une bonne part de la sécurité de l'Internet repose sur le fait qu'avec des protocoles comme TCP, correctement implémentés, tricher sur son adresse IP est difficile ; ce n'est plus vrai si BGP est activement compromis).

Il existe deux façons de s'attaquer à BGP : en attaquant la communication entre deux pairs, deux routeurs BGP qui échangent des routes, ou bien en injectant de fausses informations que les routeurs vont relayer. Notre RFC parle surtout de la première attaque, la seconde, sur laquelle je reviendrai à la fin de cet article, est bien plus difficile à contrer.

Notre RFC décrit de manière très détaillée les failles possibles du protocole, et comment un attaquant peut les utiliser pour s'immiscer dans le bon fonctionnement de BGP.

Il ne fournit pas beaucoup de solutions clé en main : à part une mise en œuvre soignée du protocole, la difficulté de sécuriser BGP ne vient pas tellement du canal de communication entre deux pairs (qui peut être relativement protégé par la signature MD5, RFC 2385, par la plus récente TCP-AO, RFC 5925,

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

ou bien par IPsec) mais du fait que le message lui-même, l'annonce de routes, n'est pas protégé. Autrement dit, un pair BGP peut être authentifié, sans que l'on sache pour autant s'il n'injecte pas de routes invalides, que ce soit délibérement ou parce qu'il relaie ces routes qu'il a lui même reçu d'un pair.

Notre RFC cite quelques protections contre ces routes invalides comme le protocole Secure-BGP qui permet de signer les annonces de route. Comme avec beaucoup de protocoles utilisant des signatures cryptographiques, le problème n'est pas tant le protocole (même si la cryptographie est souvent délicate) que l'infrastructure sociale : qui va signer, qui a l'autorité pour dire que tel opérateur est autorisé ou non à annoncer tel réseau ? Il n'existe aucune autorité suprême coiffant tous les opérateurs Internet et pouvant amorcer le processus de signature. (Le RFC 3779 propose une technique pour encoder ces certificats.) Cette approche a depuis été normalisée, sous le nom de RPKI+ROA, dans une série de RFC <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.

Le RFC 4272 cite également une autre possibilité : le filtrage de routes, basée sur le contenu des registres de route (IRR pour "*Internet routing registry*"), exprimé en langage RPSL ("*Routing Policy Specification Language*", RFC 2622). Ces registres, comme celui du RIPE-NCC, sont notoirement mal tenus et rarement à jour et il est peu réaliste de compter dessus. BGP reste donc assez vulnérable à des injections de routes invalides, injections qui en pratique se produisent assez souvent, en général par accident.

Ces attaques BGP ne sont pas que théorie. Une étude de Georgia Tech <http://sigcomm06.stanford.edu/discussion-beta/getpaper.php?paper_id=28> montre qu'elles sont réellement utilisées par les spammeurs.