RFC 8207 : BGPsec Operational Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 septembre 2017

Date de publication du RFC : Septembre 2017

https://www.bortzmeyer.org/8207.html

Le mécanisme de sécurisation de BGP nommé **BGPsec**, normalisé dans le RFC 8205[1] n'a pas encore de déploiement important. Mais le bon sens, l'expérience d'autres mécanismes de sécurité, et les expérimentations déjà faites avec BGPsec permettent de dégager quelques bonnes pratiques opérationnelles, que ce RFC décrit. Le RFC est court : on manque encore de pratique pour être sûr de toutes les bonnes pratiques.

Bien sûr, ces pratiques évolueront. À l'heure de la publication de ce RFC, il y a encore très peu d'expérience concrète avec BGPsec. Au fait, c'est quoi, BGPsec ? Le protocole BGP, la norme pour les annonces de routes sur l'Internet, souffre d'une faiblesse de sécurité : par défaut, n'importe qui peut annoncer n'importe quelle route, même vers un préfixe IP qu'il ne contrôle pas. Il existe plusieurs systèmes pour limiter les dégâts : les IRR, les systèmes d'alarme <https://www.bortzmeyer.org/alarmes-as.html>, et, plus récemment, les ROA ("*Route Origin Authorizations*", cf. RFC 6482). BGPsec est la technique la plus efficace, mais aussi la plus difficile à déployer. Comme les ROA, il repose sur la RPKI <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Contrairement aux ROA, il ne valide pas que l'AS d'origine mais tout le chemin d'AS, par une signature de chaque AS. Il introduit donc la cryptographie dans le routage, ce qui causera sans doute quelques perturbations.

Donc, avant de lire ce RFC 8207, c'est sans doute une bonne idée de lire au moins les RFC 4271 sur BGP et RFC 6480 sur la RPKI. Comme BGPsec dépend de la RPKI, il est également bon de lire le RFC 7115, qui parle des questions opérationnelles des ROA (qui reposent également sur la RPKI). Et enfin il faut lire le RFC sur le protocole BGPsec, le RFC 8205.

Avec BGPsec, chaque routeur de bordure de l'AS va avoir une paire {clé privée, clé publique}. On peut avoir une seule paire pour tous ses routeurs (et donc publier un seul certificat dans la RPKI) ou

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8205.txt

bien une paire par routeur (section 4 du RFC). La première solution est plus simple mais, si un routeur est piraté, il faudra changer la configuration de tous les autres routeurs. Le RFC suggère aussi de pré-publier des clés de secours dans la RPKI, pour qu'elles soient bien distribuées partout le jour où on en aura besoin.

Tous vos routeurs ne sont pas censés parler BGPsec, seulement ceux au bord de l'AS, face au grand monde inconnu du méchant Internet (section 5). Si vous n'avez pas le temps ou l'envie d'activer BGPsec sur tous vos routeurs, commencez par ceux qui font face aux « maillons faibles », les pairs ou les transitaires que vous suspectez d'être le plus capable d'envoyer ou de relayer des annonces erronées ou mensongères. Évidemment, ce sont aussi ceux qui ont le moins de chance de déployer BGPsec…

Si vous ne vous contentez pas de vérifier les signatures BGPsec, mais que vous agissez sur la base de cette vérification (en ignorant les annonces invalides), attendez-vous, comme avec toute technique de sécurité BGP, à ce que le trafic se déplace, par exemple vers d'autres pairs. Un pré-requis au déploiement de BGPsec est donc sans doute un bon système de métrologie.

Attention aux limites de BGPsec : la signature couvre le chemin d'AS, pas les communautés (RFC 1997). Ne vous fiez donc pas à elles.

Si BGPsec vous semble bien compliqué à déployer, et que vous hésitez devant le travail que cela représente, la section 6 vous rassurera : la majorité des AS sont des "*stubs*", ils ne fournissent de connectivité à personne et n'ont donc pas forcément besoin de valider les annonces. Par contre, vous pouvez demander à vos transitaires s'ils utilisent BGPsec (début 2017, la réponse était forcément non).

Les lect·eur·rice·s subtil·e·s ont peut-être noté une différence avec les ROA. Alors que l'état de la validation ROA (RFC 6811) donne un résultat ternaire (pas de ROA, un ROA et valide, un ROA et invalide), BGPsec est binaire (annonce valide, ou invalide). C'est parce que les chemins d'AS sécurisés `BGPsec_path` ne sont propagés qu'entre routeurs BGPsec, qui signent et, a priori, valident. Si on reçoit une annonce BGPsec, c'est forcément que tout le chemin d'AS gérait BGPsec. L'équivalent du « pas de ROA » est donc une annonce BGP traditionnelle, avec `AS_PATH` mais sans `BGPsec_path`.

Quant à la décision qu'on prend lorsqu'une annonce est invalide, c'est une décision locale. Ni l'IETF, ni l'ICANN, ni le CSA ne peuvent prendre cette décision à votre place. Notre RFC recommande (mais c'est juste une recommandation) de jeter les annonces BGPsec invalides. Certains opérateurs peuvent se dire « je vais accepter les annonces invalides, juste leur mettre une préférence plus basse » mais cela peut ne pas suffire à empêcher leur usage même lorsqu'il existe des alternatives. Imaginons un routeur qui reçoive une annonce valide pour `10.0.0.0/16` et une invalide pour `10.0.666.0/24` (oui, je sais que ce n'est pas une adresse IPv4 correcte, mais c'est le RFC qui a commencé, ce n'est pas moi). Le routeur installe les deux routes, avec une préférence basse pour `10.0.666.0/24`. Mais les préférences ne jouent que s'il s'agit de préfixes identiques. Ici, lorsqu'il faudra transmettre un paquet, c'est la route la plus spécifique qui gagnera, donc la mauvaise (666 = chiffre de la Bête). Notez que l'article « "*Are We There Yet ? On RPKI[Caractère Unicode non montré [2]]s Deployment and Security*" `<https://eprint.iacr.org/2016/1010.pdf>` » contient plusieurs autres exemples où le rejet d'une annonce invalide a des conséquences surprenantes.

La même section 7 couvre aussi le cas des serveurs de routes, qui est un peu particulier car ces routeurs n'insèrent pas leur propre AS dans le chemin, ils sont censés être transparents.

Enfin, la section 8 traite de quelques points divers, comme le rappel que la RPKI (comme d'ailleurs le DNS) n'est pas cohérente en permanence, car pas transmise de manière synchrone partout. Par exemple, si vous venez d'obtenir un certificat pour un AS, ne l'utilisez pas tout de suite : les annonces BGP se propagent plus vite que les changements dans la RPKI et vos annonces signées risquent donc d'être considérées comme invalides par certains routeurs.

2. Car trop difficile à faire afficher par LaTeX