RFC 8205 : BGPsec Protocol Specification

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/8205.html

Ce RFC s'inscrit dans la longue liste des efforts de normalisation d'une solution de sécurité pour BGP. Actuellement, il est trop facile de détourner le routage Internet via BGP (cf. mon article « La longue marche de la sécurité du routage Internet <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html> »). Le RFC 6482[1] introduisait une solution partielle, les ROA ("*Route Origin Authorizations*"). S'appuyant sur une infrastructure de clés publiques et de certificats prouvant que vous êtes détenteur légitime d'une **ressource Internet** (comme un numéro d'AS ou bien un préfixe IP), infrastructure nommée la RPKI ("*Resource Public Key Infrastructure*"), ces ROA permettent de valider l'**origine** d'une annonce BGP, c'est-à-dire le premier AS du chemin. C'est insuffisant pour régler tous les cas. Ainsi, lors de la fuite de Telekom Malaysia <https://www.bortzmeyer.org/bgp-malaisie.html> en juin 2015, les annonces avaient une origine normale. Avec les ROA, on ne détectait donc pas le problème. D'où cette nouvelle étape, **BGPsec**. Il s'agit cette fois de valider le **chemin d'AS complet** de l'annonce BGP, chaque routeur intermédiaire signant cryptographiquement l'annonce avant de la transmettre. BGPsec permet donc de détecter bien plus d'attaques, mais il est aussi bien plus lourd à déployer.

Donc, pour résumer BGPsec en une phrase : un nouvel attribut BGP est créé, `BGPsec_Path`, il est transporté dans les annonces de route BGP, il offre la possibilité de vérifier, via les signatures, que chaque AS listé dans ce chemin a bien autorisé l'annonce. BGPsec ne remplace pas les ROA, il les complète (et, comme elles, il s'appuie sur la RPKI). Deux bonnes lectures : le modèle de menace de BGPsec, dans le RFC 7132, et le cahier des charges de BGPsec, dans le RFC 7353.

Le reste, ce n'est que du détail technique. Contrairement aux ROA, qui sont transportés en dehors de BGP, BGPsec est une modification du protocole BGP. Deux routeurs qui font du BGPsec doivent donc le négocier lors de l'établissement de la session (section 2 de notre RFC). Cela se fait par le mécanisme des capacités du RFC 5492. La capacité annonçant qu'on sait faire du BGPsec est BGPsec Capability, code

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6482.txt

n° 7 <https://www.iana.org/assignments/capability-codes/capability-codes.xml>. Notez que cette capacité dépend de celle de gérer des AS de quatre octets (normalisée dans le RFC 6793).

Le nouvel attribut est décrit en section 3. (Le concept d'attributs BGP est dans la section 5 du RFC 4271.) Les annonces BGP avaient traditionnellement un attribut nommé `AS_PATH`, qui indiquait le chemin d'AS suivi par l'annonce. (Deux choses importantes à se rappeler : lorsqu'on écrit un chemin d'AS, il se lit de droite à gauche, et vous n'avez aucune garantie que les paquets IP suivront effectivement ce chemin « "*the data plane does not always follow the control plane*" ».)

Le nouvel attribut **remplace** `AS_PATH`. Il se nomme BGPsec_path (code 33) <https://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml#bgp-parameters-2> et est optionnel et non-transitif, ce qui veut dire qu'il ne sera pas passé tel quel aux pairs. Au contraire, le routeur est supposé créer un nouvel attribut `BGPsec_path` , ajoutant son AS (signé) et celui de l'AS à qui il transmet l'annonce. On n'envoie une annonce portant cet attribut à un pair que si celui-ci a signalé sa capacité à gérer BGPsec. (Sinon, on lui envoie un `AS_PATH` ordinaire, non sécurisé, formé en extrayant les AS du `BGPsec_path`, cf. section 4.4.)

La signature contient entre autres un identifiant de l'algorithme utilisé. La liste des algorithmes possibles est dans un registre IANA <https://www.iana.org/assignments/rpki/rpki.xml#bgpsec-algorithm-suite> (RFC 8208).

Pour pouvoir mettre sa signature dans le `BGPsec_path`, le routeur doit évidemment disposer d'une clé privée. La clé publique correspondante doit être dans un certificat de la RPKI, certificat valable pour l'AS qui signe.

Un routeur qui transmet une annonce à un pair BGPsec ne garantit pas forcément qu'il a validé le chemin sécurisé. (Même s'il le garantissait, pourquoi lui faire confiance ?) C'est à chaque routeur de vérifier l'intégrité et l'authenticité du chemin d'AS (section 5 du RFC).

C'est dans cette section 5 qu'est le cœur du RFC, les détails de la validation d'un chemin d'AS. Cette validation peut être faite par le routeur, ou bien par une machine spécialisée dans la validation, avec laquelle le routeur communique via le protocole RTR ("*RPKI To Router protocol*", cf. RFC 8210). Bien sûr, si on valide, c'est sans doute pour que la validation ait des conséquences sur la sélection de routes, mais notre RFC n'impose pas de politique particulière : ce que l'on fait avec les annonces BGPsec mal signées est une décision locale, par chaque routeur (et peut-être, sur un routeur donné, différente pour chaque pair BGP).

L'algorithme de validation est simple :

— Contrôles syntaxiques de l'annonce,
— Vérification que l'AS le plus récemment ajouté est bien celui du pair qui nous l'a envoyé (à part le cas particulier des serveurs de route, traités en section 4.2),
— Test de la présence d'une signature pour chaque AS listé dans `BGPsec_path`.

À ce stade, on peut déjà rejeter les annonces qui ont échoué à l'un de ces tests, et les traiter comme signifiant un retrait de la route citée (RFC 7606). Ensuite, on passe aux vérifications cryptographiques :

— Vérification que toutes les signatures sont faites avec un algorithme cryptographique qu'on accepte (voir la section 6 et aussi le RFC 8208),
— Pour chaque AS listé dans le chemin, recherche d'un certificat correspondant à cet AS, et ayant la clé publique avec laquelle l'AS dans le chemin a été signé,
— Test de la signature.

Notez qu'on ne négocie pas les algorithmes cryptographiques au moment de l'établissement de la session BGP, comme cela se fait, par exemple, en TLS. En effet, il ne suffit pas de connaitre l'algorithme de ses pairs, il faut valider tout le chemin, y compris des AS lointains. C'est pour cela que le RFC 8208 liste des algorithmes obligatoires, que tout le monde est censé connaître (actuellement ECDSA avec la courbe P-256 et SHA-256).

On note que l'attribut `BGPsec_path` avec ses signatures n'est « transmis » qu'aux routeurs qui comprennent BGPsec (pour les autres, on envoie un `AS_PATH` classique). Au début du déploiement, ces attributs ne survivront donc pas longtemps, et les îlots BGPsec seront donc rares (section 7 du RFC).

Notez que ce protocole est en développement depuis plus de six ans, et qu'il s'est parfois nommé PathSec dans le passé.

BGPsec est apparemment mis en œuvre au moins dans BIRD et dans Quagga (mais pas dans les versions officielles).

Quelques bonnes lectures sur BGPsec :

— Les transparents de mon exposé (en ligne sur `https://www.bortzmeyer.org/files/bortzmeyer-bgpsec.pdf`) à FRnog 29 <`http://www.frnog.org/?page=frnog29`>.
— Le RFC 8374 explique et justifie les différents choix effectués lors de la conception de BGPsec.
— La série qui commence ici <`http://packetpushers.net/bgpsec-basic-operation/`> et les suivants <`http://packetpushers.net/bgpsec-leaks-leaks/`>. Très critique de BGPsec mais attention, certains reproches ne sont plus d'actualité (les **timers** sur les mises à jour, qui devaient limiter le risque d'attaque par rejeu ont été retirés depuis).

Et merci à Guillaume Lucas pour m'avoir rappelé que BGPsec est compliqué et que je suis loin de le maitriser.