RFC 6811 : BGP Prefix Origin Validation

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 janvier 2013

Date de publication du RFC : Janvier 2013

https://www.bortzmeyer.org/6811.html

Il manquait un élément dans les normes de la sécurisation du routage avec RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>, une description de la façon exacte dont on valide une annonce BGP lorsqu'on a des ROA ("*Route Origin Authorizations*") pour ce préfixe. Ce RFC comble ce manque. Jusqu'à présent, en suivant les RFC, on pouvait distribuer des certificats authentifiant le titulaire d'un préfixe IP (la RPKI) et on pouvait émettre des autorisations, pour un AS, d'annoncer un préfixe (les ROA). Désormais, on peut utiliser RPKI et ROA pour avoir une solution de sécurité complète.

Cette solution traite le cas des détournements BGP dont le plus célèbre est celui de YouTube par Pakistan Telecom <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>. Elle permet de s'assurer de la validité de l'**origine** d'une annonce de route. Dans un routeur BGP, les annonces reçues des autres routeur, dans un message BGP `UPDATE`, ressemblent à `192.0.2.0/24 : 64497 64499 65550`, ce qui indique que ce préfixe `192.0.2.0/24` a pour **origine** l'AS 65550 (on lit de droite à gauche) qui l'a ensuite transmis à l'AS 64499, qui l'a ensuite envoyé à 64497. Cette liste d'AS est transmise d'un routeur BGP à l'autre dans les attributs `AS_PATH` et `AS4_PATH`. La technique décrite dans ce RFC permet d'authentifier l'origine (et elle seule), ce qui traite le cas de la plupart des accidents (comme la bavure de Pakistan Telecom) mais pas forcément celui des attaques délibérées.

Depuis plus d'un an, une RPKI réelle est en cours de déploiement <https://www.bortzmeyer.org/rpki-tests.html>. Elle contient des certificats permettant de prouver la titularité d'adresses IP et de numéros d'AS (RFC 3779 [1]). Ces certificats servent ensuite à la signature des ROA. Dans le modèle actuellement privilégié, RPKI et ROA sont distribués à des machines validantes chez les opérateurs et les routeurs BGP récupèrent une liste des ROA validés auprès de ces machines, avec le protocole RTR du RFC 6810 (cette séparation permet de réduire le travail, notamment cryptographique, des routeurs). Notre RFC appelle cette liste la liste des **VRP** ("*Validated ROA Payload*").

Armé de ces VRP, un routeur peut, pour chaque annonce BGP, la classer en :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3779.txt

— Pas trouvée : aucun VRP ne couvre cette route (fin 2012, c'est le cas de la très grande majorité des routes, puisque le déploiement de la RPKI est encore récent),
— Valide : au moins un VRP couvre cette route, et indique l'AS effectivement reçu,
— Invalide : au moins un VRP couvre cette route mais l'AS ne correspond à aucun d'entre eux (oui, il peut y avoir plusieurs ROA pour un préfixe).

À noter que certains VRP ne peuvent jamais correspondre à une annonce légale, par exemple, si l'AS d'origine est zéro (RFC 7607). Cette propriété est utilisée pour indiquer que certains préfixes ne doivent jamais être annoncés (RFC 6491).

Tirés d'une documentation du RIPE-NCC <http://www.ripe.net/lir-services/resource-management/certification/router-configuration/#Cisco>, voici un exemple avec un routeur Cisco, montrant ces trois états :

```
isco-rpki-rtr>sh ip bgp 93.175.146.0/24
BGP routing table entry for 93.175.146.0/24, version 8995350
Paths: (1 available, best #1, table default)
...
  64510 3333 12654, (received & used)
...
      path 51012284 RPKI State valid

cisco-rpki-rtr>sh ip bgp 93.175.147.0/24
BGP routing table entry for 93.175.147.0/24, version 8995351
Paths: (1 available, no best path)
...
  64510 3333 12654, (received & used)
...
      path 510122C8 RPKI State invalid

cisco-rpki-rtr>sh ip bgp 84.205.83.0/24
BGP routing table entry for 84.205.83.0/24, version 5427340
Paths: (1 available, best #1, table default)
...
  64510 3333 12654, (received & used)
...
      path 2609454C RPKI State not found
```

Le RFC parle de « couvrir » un préfixe, pas d'être égal à un préfixe car le calcul est fait en tenant compte du caractère hiérarchique des adresses. Ainsi, un ROA pour `192.0.2.0/24` couvre une annonce pour `192.0.2.128/26`. L'algorithme en pseudo-code figure en section 2.1.

Et une fois qu'on a déterminé l'état Non trouvé ou Valide ou Invalide, qu'en fait-on ? Un point important de notre RFC (section 3) est que la décision est **locale**. Chaque routeur décide de ce qu'il fait du résultat de la validation (c'est analogue à la façon dont fonctionnent d'autres techniques de sécurité comme DNSSEC ou X.509 : la norme précise la technique, pas la décision). Le routeur peut se contenter d'envoyer une "*trap*" SNMP pour les routes invalides, il peut changer la préférence locale selon le résultat de la validation, ou bien il peut carrément rejeter les routes invalides (section 5).

Naturellement, avant de configurer son routeur pour prendre des décisions radicales, l'administrateur réseaux s'assurera que la validation se passe bien, que la machine validante se met bien à jour, n'a pas de faux positifs, est bien sécurisée, etc (section 8).

Insistons : cette technique ne valide que l'origine de l'annonce, pas le chemin d'AS complet (en anglais, c'est une "*Origin validation*", pas une "*Path validation*"). Un attaquant malin qui veut fabriquer des

fausses annonces BGP va donc s'assurer de mettre l'origine correcte, avant d'injecter l'annonce. Le RFC note donc que cette technique est plutôt une sauvegarde contre les « attaques du singe du milieu » (le singe étant supposé moins intelligent que l'homme du milieu) plutôt qu'une technique de sécurité au sens classique. D'autres techniques sont en cours de développement pour assurer la validation du chemin, mais c'est un problème bien plus complexe.

Fin 2012, les routeurs de Cisco et de Juniper (et sans doute d'autres) mettent déjà en œuvre ce RFC et permettent de configurer le sort des routes en fonction de leur validité.

On notera que Cisco prétend avoir un brevet sur cette technique : IPR #1569 <http://datatracker.ietf.org/ipr/1569/>, où Cisco ne s'engage **pas** à permettre des licences gratuites.