RFC 7353 : Security Requirements for BGP Path Validation

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 septembre 2014

Date de publication du RFC : Août 2014

https://www.bortzmeyer.org/7353.html

La sécurité du routage BGP est un sujet de préoccupation sur l'Internet depuis de nombreuses années. Ce protocole ne dispose en effet par défaut d'aucune sécurité, n'importe quel opérateur (ou personne extérieure ayant piraté les routeurs d'un opérateur) pouvant annoncer une route vers n'importe quel préfixe, détournant, par exemple le trafic d'un service vital <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>. Ce manque de sécurité ne vient pas d'une confiance naïve dans la nature humaine, mais plutôt de la nature même de l'Internet : il n'y a pas (heureusement !) de Haute Autorité Supérieure de l'Internet qui connaitrait tous les opérateurs et pourrait les autoriser et les surveiller. Un opérateur ne connait (et encore, pas toujours très bien) que ses voisins immédiats, et ne sait pas quelle confiance accorder aux autres. Dans ces conditions, la sécurisation de BGP est forcément un projet à long terme. La première grande étape avait été la normalisation et le déploiement de RPKI et ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. L'étape suivante est la sécurisation du chemin entier (et pas uniquement de l'origine), dont ce nouveau RFC est le cahier des charges. En route donc vers **BGPsec** ! (Le nom PATHsec ne semble plus utilisé.)

Rappelons en effet qu'une annonce BGP (RFC 4271 [1]) comprend un **chemin**, la liste des AS par lesquels l'annonce est passée (et, dans la plupart des cas, celle, en sens inverse, dans lequel un paquet IP émis par le récepteur de l'annonce voyagera s'il veut atteindre l'AS d'origine). Voici un telle annonce, extraite du service de "*looking glass*" d'Hurricane Electric :

```
Prefix: 2001:678:c::/48,  Status: E,  Age: 31d9h14m31s
         NEXT_HOP: 2001:7fa:0:1::ca28:a116, Metric: 0,  Learned from Peer: 2001:7fa:0:1::ca28:a116 (1273)
          LOCAL_PREF: 100,  MED: 1,  ORIGIN: igp,  Weight: 0
         AS_PATH: 1273 2200 2484
```

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

Le chemin comprend trois AS, et l'**origine**, l'AS émetteur de l'annonce, est 2484 (oui, tout à droite : un chemin d'AS se lit de droite à gauche).

Avec les certificats de la RPKI (RFC 6480) et avec le système des ROA ("*Route Origin Authorization*", RFC 6482), on peut désormais (RFC 6811) valider l'origine d'une annonce. Cela protège contre les détournements accidentels (comme celui de YouTube par Pakistan Telecom cité plus tôt), où l'AS d'origine est en général celle du détourneur. Mais lors d'une attaque délibérée, l'attaquant peut tricher sur le chemin et envoyer une annonce avec un chemin d'AS qui semble correct, avec la bonne origine. RPKI+ROA ne protègent pas contre cet attaquant compétent. (Les RFC 4593 et RFC 7132 décrivent en détail les vulnérabilités de BGP.)

Maintenant, place aux exigences que devra satisfaire la nouvelle solution de sécurisation. La section 3 du RFC liste les exigences générales et la section 4 celles spécifiques au traitement effectué lors de la réception d'une annonce BGP. Les exigences générales d'abord, numérotées de 3.1 à... 3.23 (oui, une longue liste). D'abord, 3.1 et 3.2, qui résument le projet complet : le routeur BGP qui reçoit une annonce doit pouvoir déterminer, avec un bon niveau de confiance, que l'origine dans l'annonce (exigence 3.1), et le chemin des AS ("*AS Path*") dans l'annonce (exigence 3.2) sont authentiques. On veut être sûr que l'AS d'origine avait bien le droit d'annoncer ce préfixe, et que le chemin d'AS dans l'annonce reflète bien le chemin suivi par l'annonce (dans l'exemple ci-dessus, que 2484 avait bien le droit d'annoncer le préfixe `2001:678:c::/48`, et qu'il a bien transmis l'annonce à 2200, qui l'a lui-même bien transmis à 1273). Attention, il ne s'agit pas uniquement de montrer que le chemin d'AS est possible (ces AS sont bien des pairs...) mais que c'est bien celui qui a effectivement été utilisé. Les autres attributs de l'annonce (comme le MED dans l'exemple ci-dessus) ne sont **pas** protégés (exigence 3.3) car ils ne sont utilisés que dans un AS ou ses voisins immédiats. (Voir aussi l'exigence 3.10.)

Comme toute technologie nouvelle, BGPsec aura des difficultés de déploiement, dans un Internet très ossifié, et la nouvelle solution devra donc être déployable de manière incrémentale (exigences 3.4 et 3.5) : les routeurs BGPsec devront pouvoir travailler avec les routeurs actuels (exigence 3.13 ; la section 5 reconnait que cette exigence ouvre la voie aux attaques par repli, où un attaquant réussit à faire croire qu'un pair ne gère pas BGPsec et qu'il faut donc se replier sur un protocole non sécurisé). Au début, les routeurs BGPsec auront sans doute des pairs BGPsec et d'autres en BGP non sécurisé et BGPsec doit donc pouvoir être configuré pair par pair (exigence 3.12). La cryptographie peut coûter cher en ressources matérielles et un routeur BGP typique a un CPU moins puissant que celui d'une console de jeu de salon. L'exigence 3.6 autorise donc BGPsec à réclamer du matériel nouveau (par exemple des processeurs cryptographiques spécialisés). La compatibilité avec le matériel existant n'est donc pas exigée.

L'attaquant n'est pas forcément situé dans un garage à des milliers de kilomètres, comme dans le cas des détournements BGP spectaculaires connus. Il peut aussi être mieux placé, par exemple sur le lien entre deux routeurs (l'attaquant peut être sur le même point d'échange que ses victimes...) L'exigence 3.8 impose donc une solution qui marche même en cas d'ennemi sur le lien Ethernet (le RFC note que AO - RFC 5925 - ou TLS - RFC 5246 suffisent).

La cryptographie ne sert pas à grand'chose si on n'a pas de moyen de vérifier l'authenticité des clés utilisés. C'est bien joli de tester l'intégrité d'une signature mais il faut aussi que la clé de signature soit reliée aux ressources qu'on veut protéger (ici, les préfixes d'adresses IP et les numéros d'AS). L'exigence 3.9 dit donc que la solution technique a le droit de s'appuyer sur une infrastructure existante établissant ce lien, comme la RPKI (et qu'évidemment cette infrastructure doit être fiable, cf. section 5). 3.17 ajoute que cette infrastructure doit permettre le choix, par l'opérateur, des entités à qui faire confiance (toutes les mises en œuvre actuelles de la RPKI permettent cela, en éditant la liste des "*trust anchors*").

L'exigence 3.14 concerne une question de gouvernance. Il a souvent été reproché aux projets de sécurisation de BGP de faire un déplacement de pouvoir, des opérateurs BGP aux RIR qui gèrent les

points de départ de la RPKI. Avec le BGP traditionnel, le RIR a un pur rôle de registre, il ne prend aucune décision opérationnelle concernant le routage. Avec un BGP sécurisé, ce n'est plus le cas. Pour rassurer les opérateurs, 3.14 rappelle que, signature correcte ou pas, la décision d'accepter, de refuser, de prioriser ou de déprioriser une annonce doit rester locale au routeur et à son opérateur. La question « que doit faire un routeur BGPsec en recevant une annonce invalide ? » n'a donc pas de sens et les futurs RFC n'y répondront pas. BGPsec permettra de dire « cette annonce est invalide », il ne dira pas quelle politique adopter vis-à-vis de ces annonces.

Pas question de sacrifier le secret des affaires à la sécurité BGP : l'exigence 3.18 dit que BGPsec ne doit pas révéler au monde plus que ce que BGP diffuse déjà. On ne pourra donc pas exiger, par exemple, qu'un opérateur publie la liste de ses pairs privés ou de ses clients.

Bien sûr, la solution adoptée devra permettre (exigence 3.19) la journalisation des événements pertinents, notamment en matière de sécurité (c'est plus une exigence pour les mises en œuvre que pour les futurs RFC).

Rien n'étant éternel dans l'Internet, le BGP sécurisé devra ré-authentifier les informations de temps en temps, par exemple suite aux mises à jour de la RPKI (exigence 3.20), même s'il n'y a pas eu de changement BGP (ce protocole n'annonce en effet que les changements : une route qui n'a pas changé ne sera pas ré-annoncée périodiquement, et les sessions BGP peuvent durer des mois, l'annonce montrée au début de cet article était vieille de 31 jours).

Enfin, pour en finir avec les exigences générales, la 3.21 impose que la solution BGPsec permette de changer les algorithmes cryptographiques utilisés, pour faire face aux progrès de la cryptanalyse.

La section 4 décrit les exigences spécifiques au traitement des messages BGP `UPDATE` qui annoncent une nouvelle route ou bien en retirent une ancienne. C'est le moment où il faut valider (exigences 4.1 et 4.2). L'exigence 4.3 dispense BGPsec d'une protection générale contre les attaques par rejeu, qui resteront donc possibles (retransmission d'une annonce BGP qui était valide mais ne l'est plus, vu les changements dans le graphe BGP). Plus difficile, 4.4 demande qu'on puisse se protéger, au moins partiellement, contre le retrait par l'attaquant d'un message BGP.

Pour terminer, la section 5, sur les problèmes généraux de sécurité, rappelle plusieurs choses importantes notamment le fait que la sécurité du routage ne garantit pas celle des paquets IP (« *"The data plane may not follow the control plane"* ») et le fait qu'une sécurité de bout en bout, assurée par les deux machines qui communiquent, reste nécessaire. (Il existe d'autres moyens de détourner le trafic que les attaques BGP.)

Le protocole n'est pas encore terminé (ce RFC n'est qu'un cahier des charges) et il n'existe donc pas encore de mise en œuvre de BGPsec dans du code livré aux opérateurs.

Merci à Bruno Decraene pour les corrections.