La longue marche de la sécurité du routage Internet : une étape importante, RPKI+ROA

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 février 2012

https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html

---

On le sait, le protocole BGP (normalisé dans le RFC 4271 [1]), sur lequel repose tout l'Internet, car c'est lui qui permet à l'information de routage de circuler entre les opérateurs, ce protocole, donc, est peu sûr. N'importe qui peut annoncer n'importe quelle route, dire « Je suis Google, envoyez-moi toutes les requêtes Google » et les autres le croient. Résoudre cette vulnérabilité n'est pas trivial, pour des raisons essentiellement non techniques. Néanmoins, le manque d'un mécanisme standard pour valider les routes était une des faiblesses du routage Internet. Une série de RFC vient de partiellement combler ce déficit.

Écrits par le groupe de travail IETF SIDR <http://tools.ietf.org/wg/sidr> ("*Secure Inter-Domain Routing*"), ces RFC décrivent une série de protocoles, règles et formats qui permettent de sécuriser une partie de BGP. À eux seuls, ils sont loin de résoudre le problème, qui est très complexe. Mais ils fournissent des briques sur lesquelles seront bâties les solutions ultérieures.

Ces annonces de route anormales sont relativement banales sur l'Internet. Pour ne citer que trois exemples relativement récents :

— Le 24 février 2008, Pakistan Telecom annonce les adresses de YouTube et prive le monde de ce service pendant plusieurs heures <https://www.bortzmeyer.org/pakistan-pirate-youtube.html>,
— Le 8 avril 2010, China Telecom annonce les adresses d'une bonne partie de l'Internet et attire ainsi leur trafic <http://bgpmon.net/blog/?p=323>,
— Le 23 juin 2011, OpenTransit fait la même erreur et détourne également une partie du trafic <http://www.mail-archive.com/frnog@frnog.org/msg15150.html>. Les abonnés au service d'alarme BGPmon <https://www.bortzmeyer.org/alarmes-as.html> reçoivent des avis de détournement (en ligne sur https://www.bortzmeyer.org/files/bgpmon-as5511-june-2011.txt).

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

Toutes étaient des erreurs et pas des attaques. Néanmoins, le risque que cette même faiblesse soit exploitée pour des attaques est réel. Celles-ci seront sans doute plus subtiles que les trois grosses bavures citées plus haut, et utiliseront sans doute des techniques de furtivité comme celle de Kapela & Pilosov <https://www.bortzmeyer.org/faille-bgp-2008.html>.

Mais alors, pourquoi malgré autant d'attaques (n'exagérons rien : il n'y en a pas tous les mois), n'a-t-on pas encore déployé une solution de sécurité ? Parce que le problème est compliqué. Le routage sur l'Internet n'est pas hiérarchique. Les relations entre opérateurs sont un graphe plutôt complexe, et un opérateur qui est situé loin ne sait pas ce qui est normal : après tout, qui me dit que YouTube n'a pas subitement changé de fournisseur pour s'installer au Pakistan ? Même si un être humain peut trouver cela bizarre, le pauvre routeur BGP n'a pas de moyen de décider si une annonce est normale ou pas.

Il y a en fait deux choses qu'on peut vouloir authentifier dans une annonce BGP. Imaginons qu'un routeur reçoive une annonce pour le préfixe `2001:db8:666::/48` et que le chemin des AS traversés soit `64496 65550 65543` (rappelez-vous que le chemin se lit de droite à gauche, l'annonce initiale a donc été faite par l'AS 65543). Le routeur peut se demander « Est-ce que 65543 était bien autorisé à annoncer ce préfixe ? », ce qu'on appelle la **validation de l'origine**. Et il peut aussi s'interroger « Est-ce que 65550 avait le droit de relayer cette annonce ? Et 64496 ? ». C'est la **validation du chemin**. La première est relativement simple (il n'y a pas tant de préfixes IP que cela et ils sont normalement tous enregistrés dans les bases des RIR, et les origines changent rarement). La seconde est bien plus complexe (explosion combinatoire du nombre de possibilités, relations entre opérateurs qui ne sont pas dans les bases des RIR, changements fréquents) et ne sera traitée que dans un deuxième temps.

Il y a donc eu de nombreuses tentatives de résoudre ce problème de sécurité (une liste partielle figure à la fin de cet article). Attention d'ailleurs en lisant ce qu'on trouve sur l'Internet : vous extrayerez des tas de propositions dépassées ou abandonnées.

L'approche choisie par le groupe SIDR est modulaire : il n'y a pas une technique unique qui résout tout mais un ensemble d'outils, à combiner selon les cas. À la base, se trouve la RPKI, une IGC hiérarchique, partant de l'IANA et des RIR, permettant de produire des certificats attestant de la « possession » d'une ressource (un préfixe IP, un numéro d'AS, etc). L'émission de ces certificats a été un des premiers pas concrets <https://www.bortzmeyer.org/certificats-ressources-internet.html>.

Une fois les certificats émis, les titulaires des ressources (typiquement, des adresses IP) créent des objets signés, les ROA ("*Route Origin Authorizations*"). Ces ROA et les certificats sont distribués sur l'Internet (pas en temps réel) et tout routeur peut les consulter pour savoir si une annonce est légitime. Pour éviter de charger le routeur avec des calculs cryptographiques, la validation sera typiquement faite par une machine spécialisée, le validateur, que le routeur interrogera avec un protocole simple.

Voici la longue liste des 14 (!) RFC qui viennent de paraître sur ce sujet. L'ordre ci-dessous est leur ordre d'importance décroissante (selon moi) :

— RFC 6480, "*An Infrastructure to Support Secure Internet Routing*", le plus important, décrit l'architecture générale du système et notamment l'infrastructure de clés publiques, la RPKI ("*Resource Public Key Infrastructure*").
— RFC 6483, "*Validation of Route Origination using the Resource Certificate PKI and ROAs*", décrit le mécanisme de validation de l'**origine** (le premier AS) d'une route, en utilisant les techniques ci-dessus.
— RFC 6481, "*A Profile for Resource Certificate Repository Structure*", décrit la structure du dépôt des objets de la RPKI (certificats et ROA).
— RFC 6488, "*Signed Object Template for the Resource Public Key Infrastructure*", spécifie le profil CMS des objets signés,

— RFC 6482, "*A Profile for Route Origin Authorizations (ROAs)*", décrit le format concret des **ROA** ("*Route Origin Authorization*"), les objets signés cryptographiquement qui permettent d'autoriser un AS à annoncer l'origine d'une route.
— RFC 6486, "*Manifests for the Resource Public Key Infrastructure*", sur les manifestes, ces listes d'objets signés, elles-mêmes signées, et qui seront distribuées dans les dépôts de la RPKI,
— RFC 6487 "*A Profile for X.509 PKIX Resource Certificates*", spécifie le profil (la restriction) pour les certificats numériques utilisés dans la RPKI,
— RFC 6493, "*The RPKI Ghostbusters Record*", indique comment préciser dans le certificat les informations permettant de contacter le titulaire de la ressource.
— RFC 6490, "*Resource Certificate PKI (RPKI) Trust Anchor Locator*", indique comment trouver les certificats racine (il a depuis été remplacé par le RFC 7730),
— RFC 6492, "*A Protocol for Provisioning Resource Certificates*", le protocole d'avitaillement des certificats entre l'AC et ses clients,
— RFC 6484, "*Certificate Policy (CP) for the Resource PKI (RPKI)*", où sont exposés les principes de la politique que devraient suivre les AC de la RPKI,
— RFC 6491, "*RPKI Objects issued by IANA*", décrit les objets que va devoir signer l'IANA pour amorcer le processus (typiquement, les réseaux « spéciaux », normalement non annoncés en BGP),
— RFC 6489, "*CA Key Rollover in the RPKI*",
— Et enfin RFC 6485, "*The Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure*", qui spécifie les algorithmes de cryptographie utilisés par la RPKI.

En outre, quelques mois après, est sorti le RFC 6810, sur RTR ("*RPKI/Router Protocol*") le protocole de communication entre le routeur BGP et son validateur, typiquement un serveur Unix spécialisé. Et le RFC 6811, décrivant plus précisement la validation de préfixes.

Quelles sont les chances d'adoption de RPKI+ROA, sachant que d'innombrables protocoles de sécurité de l'IETF ont été peu ou pas déployés (IPsec, PGP, etc) ? Tout le monde dit en effet vouloir davantage de sécurité mais, en pratique, personne ne veut en payer le prix. Les systèmes de sécurité sont lourds, contraignants, et ne semblent pas en valoir la peine. Il est possible que des des mesures a posteriori <https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html> (via des systèmes d'alerte <https://www.bortzmeyer.org/alarmes-as.html>) suffisent à gérer le problème de la sécurité de BGP.

Sinon, ce système soulève des tas de questions liées à la gouvernance, comme c'est souvent le cas des mécanismes de sécurité. Quelques exemples :

— Faut-il une racine unique de certification ? Sur le papier, tout le monde dit oui (par exemple le NRO <http://www.nro.net/news/nro-declaration-on-rpki> ou bien l'IAB <http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html> ; notez que les conflits dont parle l'IAB se sont déjà produits <https://www.bortzmeyer.org/conflit-numeros-as.html>) mais, en pratique, les membres du NRO n'en veulent pas et le candidat évident pour cette racine unique, l'IANA, n'a donc qu'un rôle minime. Pour l'instant, chaque RIR est racine de certification et il faut donc avoir cinq certificats racine. L'IGP <http://www.internetgovernance.org/> a produit une critique de la déclaration de l'IAB <http://blog.internetgovernance.org/blog/_archives/2010/3/13/4479658.html>.
— RPKI+ROA augmente le pouvoir des RIR, via les révocations, ce qui est une nouveauté. Avant, les RIR n'intervenaient pas dans le routage, uniquement dans l'allocation des adresses. Un RIR pouvait en théorie révoquer une allocation, mais cela n'avait aucune conséquence pratique. Avec la RPKI, le RIR émettra une révocation X.509 et les routeurs ROA arrêteront automatiquement d'accepter la route... Le RIR aura donc désormais un rôle opérationnel. Comme l'explique très bien l'excellent article de l'IGP "*Building a new governance hierarchy : RPKI and the future of Internet routing and addressing*" <http://internetgovernance.org/pdf/RPKI-VilniusIGPfinal.pdf>, cela peut changer les rôles des acteurs de la gouvernance de l'Internet et la RPKI devrait donc être discutée politiquement, pas uniquement techniquement (une version plus longue de cet article est « "*Negotiating a New Governance Hierarchy : An Analysis of the Conflicting Incentives*

---

https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html

to Secure Internet Routing" <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2021835> » par Brenden Kuerbis et Milton Mueller). Pour l'instant, les partisans de la RPKI considèrent que le problème doit être relativisé car le contrôle final est entre les mains du cache validateur qui croit qui il veut. S'il ne veut pas utiliser les "*trust anchors*" des RIR, il le peut. (Il peut aussi ne pas valider du tout, ou bien accepter les routes invalides, surtout s'il n'y a pas de routes alternatives.) Concernant spécifiquement le RIPE-NCC, leur politique quant à une éventuelle révocation de routes est que ce n'est pas possible <http://www.ripe.net/ripe/mail/archives/address-policy-wg/2011-May/005858.html>.

— Discussions animées au sein de la communauté quant à l'intérêt pour le RIR de travailler dans cette direction. En novembre 2011, celle du RIPE a voté pour la poursuite du projet (voir les articles de Malcolm <https://publicaffairs.linx.net/news/?p=6118> et de Michele Neylon <http://www.circleid.com/posts/20111103_ripe_members_vote_to_continue_rpki_work/>).

Pour le fonctionnement concret du système RPKI+ROA, et des exemples, voir mon autre article <https://www.bortzmeyer.org/rpki-tests.html>.

Dans le futur, des travaux auront lieu pour valider le **chemin** et non plus seulement l'**origine** comme le fait notre nouveau système (le cahier des charges de ce projet a été publié dans le RFC 7353). Après des propositions comme Secure BGP <http://blog.ioshints.info/2010/03/secure-bgp.html>, le futur protocole se nommera probablement BGPSEC <http://tools.ietf.org/html/draft-ietf-sidr-bg car, contrairement au système qui vient d'être normalisé, il sera une modification de BGP. Humour par Hugo Salgado <https://twitter.com/huguei> : si l'actuel BGP, sans sécurité, est **BGPbrut**, RPKI+ROA est un **BGPdemisec** - à moitié sécurisé - et le futur protocole sera, logiquement, **BGPsec**...

Quelques articles intéressants :

— Une introduction pour grands débutants <http://www.apnic.net/services/services-apnic-provi resource-certification/RPKI> par l'APNIC.
— Un court résumé technique <http://www.ietf.org/proceedings/75/slides/sidr-7.pdf> qui avait été fait à l'IETF.
— Un tutoriel RIPE <http://ripe63.ripe.net/presentations/32-RIPE63-RPKI-Session.pdf>, rappelant l'effort du RIPE-NCC.
— Une proposition alternative, où on ne valide pas les routes mais où on ne les adopte que prudemment, Pretty Good BGP <http://www.cs.unm.edu/~karlinjf/pgbgp/>.
— Mes transparents à FRnog19 sur la RPKI <https://www.bortzmeyer.org/rpki-frnog.html>,
— Une autre alternative à RPKI+ROA, plus simple, ROVER <https://www.bortzmeyer.org/rover-bgp.html>,
— Un très bon article général <http://www.potaroo.net/ispcol/2011-07/bgpsec.pdf>, très détaillé, sur RPKI+ROA puis le passage à BGPsec.