RFC 6480 : An Infrastructure to Support Secure Internet Routing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 février 2012

Date de publication du RFC : Février 2012

https://www.bortzmeyer.org/6480.html

Les techniques de sécurisation de BGP du groupe de travail SIDR <http://tools.ietf.org/wg/sidr> viennent d'être publiées <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Elles reposent sur une infrastructure de clés publiques cryptographiques, la RPKI ("*Resource Public Key Infrastructure*"). Ce RFC décrit cette RPKI, fondation de tous les systèmes de sécurisation du routage dans l'Internet, ainsi que l'architecture générale du système.

Le principe est le suivant : le titulaire d'un préfixe IP a un certificat lui permettant de signer des objets, par lesquels il autorise tel ou tel AS à annoncer ce préfixe. Ces signatures peuvent être ensuite vérifiées par les routeurs, qui rejetteront les erreurs et les tentatives de piratage.

La section 1 résume les **trois** composants essentiels de la solution, qui permettra de protéger le routage BGP (RFC 4271 [1]) :

— La RPKI, l'infrastructure de gestion de clés, dont la hiérarchie est plaquée sur l'actuelle hiérarchie d'allocation des adresses (IANA -¿ RIR -¿ LIR, etc),
— Des objets numériques signés (par les clés contenues dans les certificats de la RPKI), les "*routing objects*", qui expriment les autorisations de routage,
— Le mécanisme de distribution de ces objets, pour que les routeurs y aient accès afin de valider les annonces BGP.

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

Dans un premier temps, cette solution permettra de valider l'**origine** des annonces BGP (le premier AS, cf. RFC 6483). Plus tard, elle pourra servir de base à des solutions plus globales, encore en cours de développement, comme soBGP <ftp://ftp-eng.cisco.com/sobgp/index.html> ou "*Secure Border Gateway Protocol (Secure-BGP)*" <http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/045.pdf>.

La correspondance entre le graphe des certificats et celui existant pour allouer des ressources comme les adresses IP évite de réinventer une nouvelle classe d'acteurs. Cela ne veut pas dire que les rapports de force ne vont pas être modifiés. Ainsi, à l'heure actuelle, un RIR peut toujours, techniquement, retirer un préfixe à un LIR, mais cela n'aura pas de conséquence pratique, le RIR n'ayant aucun rôle dans le routage. Demain, avec la RPKI, le RIR enverra une révocation et les routeurs considéreront la route comme invalide... Il y a donc bien renforcement des pouvoirs de la hiérarchie, comme l'analysait un article de l'IGP <http://blog.internetgovernance.org/blog/_archives/2010/9/7/4624281.html>.

Techniquement, peu de protocoles ou de formats nouveaux sont développés. Ainsi, les certificats de la RPKI sont du X.509, avec les extensions déjà existantes de l'IETF, RFC 5280, plus celles permettant de représenter des ressources (adresses IP et numéros d'AS), normalisées dans le RFC 3779 et suivant le profil du RFC 6487. Les objets signés (cf. RFC 6488) utilisent quant à eux le format CMS (RFC 5652).

Le premier des trois composants, la RPKI ("*Resource Public Key Infrastructure*"), est décrit en section 2. L'idée est que c'est le **titulaire** d'une plage d'adresses IP qui décide comment elle peut être routée et par qui. Les certificats permettent donc d'attester que telle entité est bien le titulaire (ce qui se fait actuellement en consultant la base du RIR, par exemple via whois). L'IANA va donc signer les plages qu'elle alloue aux RIR (cette étape est optionelle, voir plus loin), les RIR signent les plages qu'ils allouent aux LIR et ainsi de suite si nécessaire (il y a des cas plus complexes, pour les NIR, ou bien pour les adresses PI, ou encore lorsqu'un titulaire sous-alloue une partie de ses adresses). Lorsqu'un certificat affirmera « je suis titulaire du 192.0.2.0/24 », il sera ainsi possible de remonter la chaîne, jusqu'à une référence de confiance (l'IANA ou bien l'ensemble des RIR) pour vérifier cette assertion. Donc, bien que le routage dans l'Internet ne soit **pas** hiérarchique, l'allocation l'est, et la RPKI s'appuie là-dessus.

Les exemples ci-dessus portent sur des adresses IP mais le raisonnement est le même pour les numéros d'AS, d'où ce nom collectif de **ressources** (adresses IP et numéros d'AS).

Il faut bien noter que ces certificats, s'ils sont techniquement des certificats X.509 comme les autres, ont une sémantique différente ; Le fait qu'une CA signe un certificat ne dit pas qu'elle certifie l'identité contenu dans le certificat mais qu'elle certifie le lien entre une ressource et un titulaire. Ces certificats sont davantage d'autorisation que d'authentification. Le RFC recommande simplement de mettre comme nom (X.509 appelle cela le "*subject*") un identificateur spécifique à la CA, par exemple un numéro de client.

Comme cette sémantique est différente, et qu'il n'y a pas les risques juridiques associés aux certificats d'authentification classiques, il n'y a donc pas de nécessiter d'utiliser les CA existantes, ni de raison d'hésiter, pour un opérateur, à devenir CA. Les certificats fournis aux entités intermédiaires (typiquement les LIR) doivent être des certificats CA, autorisant le titulaire à émettre lui-même des certificats (la signature de chaque objet nécessite la création d'un certificat pour cet objet, cf. section 2.2). Les sites terminaux, en général, n'auront pas besoin de certificats du tout (sauf s'ils sont "*multi-homés*" avec des adresses PI, cf. section 7.3.2).

Les certificats finaux (section 2.3), ceux qui n'auront pas besoin d'avoir le bit CA à un, servent pour signer les objets (l'intérêt de créer un certificat juste pour signer un objet est de permettre une révocation, en réutilisant les mécanismes existants de X.509).

Pour vérifier, les validateurs (les routeurs BGP, ou bien les machines à qui ces routeurs sous-traiteront le travail), auront besoin de certificats « racine ». Comme en général pour X.509, le choix de ces certificats est une question politique locale et n'est pas spécifiée par la norme. Le RFC évite ainsi (section 2.4) l'épineuse question politique de savoir s'il faut configurer le validateur avec le certificat de l'IANA (donnant à celle-ci un grand pouvoir) ou bien avec les certificats des cinq RIR (court-circuitant ainsi l'IANA).

La section 3, elle, décrit les objets qu'on va signer, les **ROA** ("*Route Origination Authorization*"). La RPKI va dire « il est le titulaire de `192.0.2.0/24` » et le ROA va ajouter « l'AS 64641 est autorisé à annoncer `192.0.2.0/24` » (le ROA n'autorise que l'origine, pas les AS ultérieurs qui relaieront l'annonce). Le ROA est donc tout au bout du graphe des autorisations. On pourrait donc avoir une chaîne comme :

— IANA : « ARIN gère `192.0.0.0/8` »,
— ARIN : « le FAI Example est titulaire de `192.0.2.0/24` »,
— Example : « l'AS 64641 est autorisé à être l'origine d'une annonce de `192.0.2.0/24` » (cette dernière assertion étant un ROA).

Le format des ROA est décrit en RFC 6482 et leur utilisation dans la validation des annonces BGP en RFC 6483. Le format est une spécialisation du format générique des objets de la RPKI, décrit dans le RFC 6488, lui-même issu de CMS. Chaque ROA contient un numéro d'AS, un ou plusieurs préfixes que cet AS a l'autorisation d'« originer » et (facultativement) une longueur maximale des sous-préfixes. Notez bien qu'il n'y a qu'un AS. Si plusieurs AS ont le droit d'être à l'origine des annonces de ces préfixes, il faut créer plusieurs ROA. Il n'y a pas de durée de validité dans le ROA, la validité est celle du certificat.

La distribution des ROA se fait essentiellement par le système de dépôts décrit dans la section 4 mais pourrait se faire dans le futur par d'autres moyens, comme les messages BGP `UPDATE`. On l'a vu, la validation des routes suppose que les validateurs (les routeurs BGP eux-même, ou bien des machines spécialisées à qui les routeurs sous-traitent l'opération) aient accès à tous les ROA. (Ce n'est pas un nombre énorme, typiquement un seul par route visible mondialement.) Un mécanisme est proposé pour créer un dépôt distribué de ROA, accessible à la demande (les mécanismes où les ROA seraient poussés vers les validateurs, par exemple par BGP, ne sont pas encore définis). Le dépôt est décrit en détail dans le RFC 6481.

Le dépôt n'est pas spécialement « de confiance ». Ce sont les signatures sur les ROA qui comptent, pas l'endroit où ils ont été récupérés. C'est d'autant plus vrai que le RFC encourage à recopier le dépôt, pour faciliter l'accès.

Le dépôt pourra offrir un choix de protocoles d'accès (section 4.3). Notre RFC décrit juste les fonctions de ces protocoles :

— Téléchargement en bloc de toutes les données (rappelez-vous que le validateur est supposé avoir une vue complète). Les données sont donc réellement publiques.
— Ajout d'une donnée, ou modification d'une donnée existante.

Des tas de protocoles offrent ces fonctions (par exemple HTTP/REST, même s'il n'est pas cité). Pour éviter que chaque acteur du routage ne déploie un protocole d'accès différent, rendant la vie des clients infernale, notre RFC impose que chaque copie soit accessible en lecture avec rsync, garantissant ainsi un mécanisme toujours disponible. On désigne donc la copie avec un URI rsync (RFC 5781) et on y accède par :

```
% rsync -av rsync://rpki.ripe.net/repository /where/i/want/RPKI-repository
```

Les experts en sécurité ont peut-être noté un peu de "*hand waving*" dans les paragraphes précédents. J'ai dit que la sécurité du dépôt était peu importante puisque ce sont les signatures des ROA qui font foi et que l'endroit où on les a trouvé ne compte donc pas. Mais si un méchant arrive à modifier un dépôt et **supprime** un ROA ? La signature ne protège pas contre ce genre de problèmes. La RPKI a donc un système de manifestes, des listes d'objets signés, listes elle-même signées et mises dans le dépôt (section 5 et RFC 6486).

Le dépôt sera donc massivement distribué, et les validateurs encouragés à garder des copies locales. La section 6 décrit ce processus, où le validateur obtient la copie de tous les objets (ROA, certificats, manifestes, etc), valide la signature des manifestes, puis vérifie leur contenu, et vérifie la signature des objets indiqués dans le manifeste.

Comme avec tous les caches, cette copie pose le problème de la fraîcheur des informations. Le cache ne contient-il pas des informations dépassées ? La section 6 n'est pas très bavarde sur ce point. À l'heure actuelle, ces informations de routage sont assez stables (on ne change pas d'AS d'origine tous les mois) donc le problème n'est pas trop aigü.

La section 7 décrit la vie du dépôt, et les opérations courantes. Les acteurs du routage devront donc désormais penser à la mise à jour de ce dépôt. Dans le futur, l'émission de ces certificats se fera peut-être automatiquement, en même temps que l'allocation des ressources. Aujourd'hui, ce n'est pas encore le cas.

La section 7.3 décrit en détail les aspects pratiques de cette gestion des ROA. Il va falloir acquérrir de nouveaux réflexes, notamment celui de créer et signer des ROA lors de tout changement de la politique de routage. Comme l'absence d'un ROA pour une annonce donnée pourra être interprété comme un détournement, et mener à un refus de l'annonce BGP par les routeurs validants, il y aura plein de possibilité de « se tirer une balle dans le pied ». Les opérateurs devront donc appliquer le principe « "*make before break*" », c'est-à-dire créer le ROA signé bien avant d'annoncer la route (pour permettre à tous les dépôts et tous les caches d'être à jour) et, en sens inverse, arrêter l'annonce longtemps avant de signer la révocation du ROA correspondant (et s'assurer qu'il existe un autre ROA, pour la nouvelle annonce).

Cela ne s'applique qu'aux opérateurs, pas au client final. Le site qui a des adresses PA et est connecté à un seul opérateur, n'a rien à faire, les ROA seront émis par l'opérateur. Ce site ne participe donc pas à la RPKI. En revanche, un site "*multi-homé*" peut, dans certains cas, avoir à émettre des ROA. Par exemple, s'il a un préfixe PA qu'il fait relayer par deux opérateurs, il doit créer un ROA pour cela (et donc obtenir un certificat depuis l'opérateur qui lui a affecté le préfixe PA) ou demander à l'opérateur de le faire pour lui. Si les adresses sont PI, le site doit émettre un ROA avec son propre AS en origine, en utilisant le certificat reçu avec le préfixe PI.

Si vous souhaitez appronfondir la question, une liste d'articles à lire se trouve dans mon article général <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Si vous voulez pratiquer et voir la RPKI en action, regardez mon article sur les logiciels <https://www.bortzmeyer.org/rpki-tests.html>.