ROVER, un système alternatif pour sécuriser BGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 mars 2012

https://www.bortzmeyer.org/rover-bgp.html

Le protocole de routage BGP, sur lequel repose tout l'Internet, est connu pour son absence de sécurité. N'importe quel maladroit <https://www.bortzmeyer.org/pakistan-pirate-youtube.html> peut annoncer les routes d'un autre opérateur et détourner ou couper le trafic. Il existe une solution de sécurisation, normalisée et activement déployée, RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Mais cette solution, plutôt complexe, ne fait pas que des heureux. Une alternative vient d'être annoncée, ROVER <http://rover.secure64.com/> ("*ROute Origin VERification*").

ROVER a été présenté par Joe Gersch à l'atelier OARC <https://www.dns-oarc.net/oarc/workshop-201203> à Teddington. Le principe est le suivant : si on est le titulaire du préfixe IP 2001:db8:179::/48, on a a priori la délégation DNS pour l'arbre dit « inverse », 9.7.1.0.8.b.d.0.1.0.0.2.ip6.arpa. On peut alors publier dans cet arbre des enregistrements DNS spéciaux qui indiqueront l'AS d'origine autorisé. Un validateur situé près du routeur testera si les préfixes reçus ont un enregistrement ROVER correspondant. Le routeur n'aura qu'à lui demander ce résultat (le système RPKI+ROA a un fonctionnement analogue, le routeur ne valide pas lui-même). On a alors les mêmes possibilités qu'avec les ROA du RFC 6482[1]. Et la sécurité ? Pour que ROVER ait un sens, il faut évidemment signer les enregistrements avec DNSSEC.

Par rapport à la solution RPKI+ROA, on a donc :

— Pas de X.509 (les certificats du RFC 6487),
— Pas de rsync pour distribuer les données signées,
— Utilisation d'une infrastructure existante, le DNS et DNSSEC, ainsi que de son domaine existant. Le déploiement pourrait donc être plus facile.

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

Voyons un exemple concret avec le banc de test <http://rover.secure64.com/>. Je me crée un compte et je demande l'état du préfixe 2001:67c:217c::/48 (le site Web du banc de test offre plusieurs moyens de remplir l'information, à partir d'un numéro d'AS, d'un nom, etc). J'obtiens le résultat suivant :

J'accepte le choix proposé (autoriser les fournisseurs de transit mais pas les "*peerings*") et je demande le fichier de zone, qui est produit automatiquement, avec les AS actuels :

```
;    This is a reverse-DNS zone containing Secure Routing Records
;    for the CIDR address block 2001:67c:217c::/48 owned by  (RIPE Network Coordination Centre)
;
;    Created by bortzmeyer(bortzmeyer+rover@nic.fr) on 2012-03-22
;
;    This zone is for test purposes only and is hosted at the shadow zone located on
;    the public internet at 'in-addr.arpa.secure64.com'.  It is signed with DNSSEC.
;

$TTL 3600
$ORIGIN c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa.secure64.com.

@       IN      SOA     ns1.secure64.com.  hostmaster.secure64.com.  (
                         2012032200      ; serial number in date format
                         14400           ; refresh, 4 hours
                         3600            ; update retry, 1 hour
                         604800          ; expiry, 7 days
                         600             ; minimum, 10 minutes
                        )

        IN      NS      ns1.secure64.com.
        IN      NS      ns2.secure64.com.

$ORIGIN c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa.secure64.com.

@                               IN   TYPE65400 \# 0
;                                    RLOCK    deny all route announcements except those authorized

@                               IN   TYPE65401 \# 8 000009b600000898
; 2001:67c:217c::/48                 SRO AS2486 (NIC-FR-DNS-UNICAST-PARIS2) with transit AS2200 (FR-RENATER)

@                               IN   TYPE65401 \# 8 000009b60000201a
; 2001:67c:217c::/48                 SRO AS2486 (NIC-FR-DNS-UNICAST-PARIS2) with transit AS8218 (NEO-ASN)
```

Quelques points d'explication : ROVER est loin d'être normalisé donc les enregistrements DNS utilisés n'ont pas de nom mais utilisent les numéros réservés pour l'expérimentation (TYPE65400 et TYPE65401). Pour la même raison, ils apparaissent en hexadécimal. Les commentaires à la ligne suivante donnent l'enregistrement en clair, tel qu'il apparaîtra lorsqu'il sera normalisé. Un RLOCK impose que les routes sous ce préfixe soient sécurisées par ROVER. Un SRO ("*Secure Route Origin*") indique un AS d'origine autorisé (ici, 2486, avec deux transitaires, Renater et Neo).

Joe Gersch a annoncé avoir testé les performances : pour un routeur qui démarre à froid, et doit donc vérifier les 400 000 routes de l'Internet d'aujourd'hui, les requêtes DNS prennent moins de quatre minutes.

ROVER est actuellement décrit dans deux "*Internet-Drafts*", « "*DNS Resource Records for BGP Routing Data*" <http://tools.ietf.org/id/draft-gersch-grow-revdns-bgp> » et « "*Reverse DNS Naming Convention for CIDR Address Blocks*" <http://tools.ietf.org/id/draft-gersch-dnsop-revdns-ci
Il sera officiellement présenté à la réunion IETF à Paris la semaine prochaine.

Au fait, c'est très bien pour IPv6 mais pour IPv4, où les frontières des organisations tombent rarement sur une frontière d'octet ? Les auteurs proposent un nouveau schéma de nommage pour l'arbre « inverse » `in-addr.arpa`. L'idée est que, si le préfixe ne s'arrête pas sur une frontière d'octet, on ajoute un `m` suivi des bits restants. Ainsi, `129.82.64.0/18` devient `1.0.m.82.129.in-addr.arpa` (le 01 au début étant le 64 du préfixe, deux bits car le reste de la division de 18 par 8 est 2). C'est dans ce `1.0.m.82.129.in-addr.arpa` qu'on mettra les enregistrements SRO (ici, pour l'AS 65536) :

```
1.0.m.82.129.in-addr.arpa. IN SRO 65536
```

Un autre article sur Rover, en anglais, pas trop mal mais inutilement sensationnaliste a été publié par The Register <`http://www.theregister.co.uk/2012/04/23/ip_hijack_prevention/print.html`>.