RFC 3779 : X.509 Extensions for IP Addresses and AS Identifiers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 octobre 2006

Date de publication du RFC : Juin 2004

https://www.bortzmeyer.org/3779.html

Le protocole BGP, qui distribue les routes à travers tout l'Internet, est peu sûr car il ne vérifie absolument pas la validité des routes qu'il transmet. Ce RFC propose d'étendre les certificats cryptographiques X.509 pour y stocker les routes et les numéros de systèmes autonomes autorisés à un émetteur. Les routeurs pourraient alors utiliser ces certificats pour s'assurer de la validité d'une annonce.

BGP est spécifié dans le RFC 4271 [1]. Le RFC 4272 détaille quant à lui ses problèmes de sécurité. L'un des principaux est le fait qu'authentifier un routeur ne sert pas à grand'chose, il faut pouvoir authentifier les routes qui peuvent être annoncées. Ainsi, même si je suis sûr de l'identité du routeur pair (celui avec qui je suis connecté en BGP), comment savoir s'il dit la vérité en annonçant une route pour tel ou tel réseau ? C'est d'autant plus difficile à déterminer que le pair a en fait souvent relayé cette annonce et qu'on ne peut pas être sûr que tous les routeurs le long de l'"*AS path*" ont bien vérifié.

Voici par exemple une mise à jour (message BGP `UPDATE`) envoyée par un pair :

```
2003/02/21 06:28:32 BGP: 213.248.70.225 rcvd 193.9.124.0/22
2003/02/21 06:28:32 BGP: 213.248.70.225 rcvd UPDATE w/ attr: nexthop 213.248.70.225, origin i, path 1299 3356 13
```

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 pair 213.248.70.225 nous dit qu'il a une route pour le préfixe 193.9.124.0/22 et que cette route a été émise par l'AS 12842. Elle a ensuite été relayée par trois autres AS différents avant de nous arriver. Quelle confiance faire à cette annonce, qui est passée par tant d'acteurs différents et arfois inconnus de nous ?

Il existe des projets de protocole effectuant des vérifications (comme S-BGP <http://www.ir.bbn.com/sbgp/>) mais tous achoppent sur le problème principal de toute vérification : examiner les papiers d'identité, OK, mais qui va les émettre ? À qui faire confiance ?

Notre RFC propose donc une technique qui a fait se preuves dans d'autres domaines : la signature numérique. Il reprend les certificats de X.509 qui permettent à une autorité de certification de dire que, par exemple, telle entité est autorisée à exploiter www.example.com. Et il les étend avec de nouveaux types de données :

— Adresses IP ou préfixes,
— Numéros de système autonome.

Ainsi, le routeur méfiant pourra vérifier la signature (en remontant la chaine des autorités de certification jusqu'aux RIR) et s'assurer qu'une route est valide.

OpenSSL sait afficher ces extensions. Mais attention, il doit avoir été compilé avec l'option enable-rfc3779, ce qui n'est pas le cas chez Debian <http://bugs.debian.org/630790>. Avec un bon OpenSSL, on obtient :

```
% openssl x509 -inform DER -text -in ./rpki.afrinic.net/repository/89208CE4119211E0B3FFDB1BAE001804/zYtk-DB4
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 6824 (0x1aa8)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=1320AEA9/serialNumber=374E802284C331BCF6A6282BFDDDB798F2B37479
        Validity
            Not Before: Apr 30 09:47:38 2012 GMT
            Not After : Mar 31 00:00:00 2013 GMT
        Subject: CN=F36432B6/serialNumber=CD8B64F83078516999993A1B67DC1F5A4A4FFC48
...
            sbgp-autonomousSysNum: critical
                Autonomous System Numbers:
                  36992

            sbgp-ipAddrBlock: critical
                IPv4:
                  41.152.0.0/15
                  41.222.128.0/21
                  197.120.0.0/13
                  197.192.0.0/13
                IPv6:
                  2c0f:fc88::/32
```

Aujourd'hui, de tels certificats sont surtout émis par les RIR et les opérateurs réseau, dans le cadre de la RPKI <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.