Des certificats pour prouver qu'on est titulaire d'une ressource Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 mars 2009

<https://www.bortzmeyer.org/certificats-ressources-internet.html>

On le sait bien, le système de routage de l'Internet est très peu fiable, comme l'a montré par exemple le détournement du trafic de YouTube par Pakistan Telecom <<https://www.bortzmeyer.org/pakistan-pirate-youtube.html>>. Pourquoi ne pas sécuriser les annonces BGP par des signatures cryptographiques, comme on authentifie le DNS avec DNSSEC? Il y a plusieurs raisons à cela, mais l'une est souvent oubliée : il n'y a pas de moyen facile de « prouver » qu'on est bien le titulaire d'une ressource Internet, par exemple une adresse IP.

Avant donc de vouloir transformer BGP en protocole utilisant la cryptographie, il faut donc d'abord distribuer aux titulaires de ressources numériques (adresses IP, numéros de systèmes autonomes, etc). Fin 2008, l'APNIC a été le premier RIR à avancer dans cette direction, en annonçant un logiciel de gestion de PKI de ressources, rпки-engine, et en prévoyant de commencer la distribution de certificats. Les extensions à X.509 pour ces ressources sont normalisées dans le RFC 3779¹.

Notons tout de suite que le déploiement ne survient pas maintenant par hasard : les adresses IPv4 s'épuisent <<https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>> et tout le monde s'attend à un développement du marché de ces adresses. Une pré-condition d'un tel marché étant l'équivalent des titres de propriété du monde physique, on voit que BGP ne sera pas le seul client de ces nouveaux certificats...

Un résumé du projet figure dans l'article "*Detecting Internet routing 'lies'*" <<http://www.networkworld.com/news/2009/012009-internet-routing.html>>. Un article très détaillé est "*Resource Certificates*" <<http://www.isoc.org/tools/blogs/ispcolumn/?p=138>>.

En février 2012, une nouvelle étape a été franchie, dans la voie de l'utilisation de ces certificats, avec la sortie des RFC spécifiant leur utilisation pour sécuriser le routage <<https://www.bortzmeyer.org/securite-routage-bgp-rпки-roa.html>>.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc3779.txt>