Analyse technique de l’infrastructure de clé publique de ressource (RPKI)

Bureau du directeur de la technologie de l’ICANN

Alain Durand
OCTO-014
2 septembre 2020

ICANN

TABLE DES MATIERES

Ce document fait partie de la série de documents publiés par le bureau du directeur de la technologie de l'ICANN (OCTO). Veuillez consulter la page de publications de l'OCTO pour accéder à la liste complète des documents compris dans la série. Si vous avez des questions ou des suggestions par rapport à ces documents, veuillez les envoyer à octo@icann.org.

Résumé analytique

Le protocole de passerelle frontière (BGP, pour ses sigles en anglais) est le protocole de routage utilisé par les fournisseurs d'accès à Internet (FAI). Ses origines remontent au début des années 1990. Les incidents de routage BGP, dont fait partie le célèbre détournement de YouTube par Pakistan Télécom en 2008, sont connus sous le nom de « fuites de route » et peuvent être à l'origine d'importantes déviations du trafic Internet. Ils se produisent désormais au quotidien, avec des conséquences opérationnelles considérables pour les FAI. Ces détournements peuvent être attribués à des erreurs de configuration, à des bogues logiciels ou à des attaques actives. La cause profonde de ces problèmes reste néanmoins l'absence de sécurité intégrée dans le protocole BGP.

La sécurisation du protocole BGP constitue un effort difficile et de longue haleine, qui reste encore inachevé. L'initiative la plus avancée, disponible actuellement pour être déployée, est dénommée « validation d'origine RPKI ». La validation d'origine RPKI s'appuie sur l'infrastructure de clé publique de ressource (dite aussi PKI de ressource ou bien RPKI), une structure hiérarchique composée d'un maillage de certificats de clé publique X.509 dont l'ancre de confiance se trouve au niveau des Registres Internet régionaux (RIR). Son objectif est de vérifier que les FAI qui génèrent des routes Internet sont autorisés à le faire par le détenteur des blocs d'adresses IP (Protocole Internet) correspondants. La validation d'origine RPKI existe depuis 2011. Le regain d'intérêt qu'elle connaît actuellement est le fruit d'un ensemble de facteurs : les initiatives mises en place par les RIR pendant de nombreuses années pour promouvoir sa pratique et former des ingénieurs à son utilisation, les efforts de l'Internet Society pour établir les Normes d'accord mutuel sur la sécurité du routage (MANRS) et le développement de logiciels RPKI financés par le département de la sécurité intérieure des États-Unis. Cet état de fait, combiné à des appels à l'action de plus en plus pressants pour mettre fin aux fuites de routes et à l'exemple donné par certains grands fournisseurs (tels que Cloudflare et NTT), ont contribué à placer la validation d'origine RPKI au cœur des sujets brûlants de l'année 2020.

Néanmoins, la technologie n'est pas encore tout à fait au point. De graves problèmes d'échelle persistent et entraînent des retards de propagation qui à leur tour réduisent la réactivité des FAI face à des urgences et fragilisent le système. Le système PKI de ressource lui-même peut faire l'objet d'attaques. Un scénario catastrophe de panne pourrait être difficile à détecter et encore plus difficile à résoudre. Ces risques sont d'autant plus graves que le modèle de déploiement, avec cinq ancres de confiance, peut donner lieu à d'éventuelles incohérences dans les données et ouvrir la voie à un nombre encore plus important d'ancres de confiance. Les parties qui n'utilisent pas la RPKI peuvent également devenir des victimes collatérales de toute compromission des ancres de confiance. Les risques de responsabilité associés à ces scénarios sont considérés si élevés par le Registre américain des numéros d'Internet (ARIN) qu'il exige aux consommateurs d'assertions une indemnisation pour l'usage de ses données RPKI. Le système accorde aux RIR un rôle opérationnel actif dans la gestion quotidienne de l'Internet, pour lequel ils risquent parfois de ne pas être les mieux adaptés, comme en témoignent certains incidents récents.

Qui plus est, avec une portée qui se limite à l'origine des annonces de routage, la validation d'origine RPKI protège uniquement contre les attaques les plus naïves du système de routage. Un système robuste de sécurisation du routage nécessite la validation de tout le chemin, une

démarche qui s'avère bien plus complexe.

Un certain nombre de FAI, de points d'échange Internet (IXP) et de fournisseurs de services d'informatique en nuage considèrent que l'utilisation de la validation d'origine RPKI pour mettre fin aux fuites de route liées à des configurations erronées et à des bogues logiciels constitue une amélioration opérationnelle suffisante pour justifier le coût de déploiement de ce système assez complexe. Or, tout projet de déploiement de la validation d'origine RPKI doit tenir compte des problèmes actuels de maturité technologique ainsi que des risques opérationnels associés. La sécurisation de l'infrastructure de routage ne se limite pas (encore) au seul déploiement d'un logiciel. Le compromis entre la sécurité du protocole et la complexité opérationnelle doit être soigneusement évalué.

Veuillez accéder à la publication OCTO 014 pour lire l'intégralité du document (en anglais).

Conclusion

La RPKI suscite un grand intérêt, en particulier chez les RIR et les opérateurs de réseau de toute taille. De nombreuses parties croient que les bénéfices à court terme que procure la RPKI sont suffisants pour garantir un retour sur investissement positif. La signature d'autorisations d'origine de route (ROA) est désormais assez simple pour que pratiquement tous les titulaires d'adresses IP puissent la mettre en place, et la validation d'origine RPKI offre une protection contre les erreurs de frappe, les erreurs de configuration et les bogues logiciels. De même, bien que la validation d'origine RPKI ne protège pas contre des attaques intentionnelles visant le système de routage, autant les attaques contre le système de routage que les fuites de route liées à des erreurs de frappe sont aux yeux des opérateurs des problèmes qui doivent être résolus. C'est pourquoi de nombreux FAI voient d'un bon œil l'aide que la validation d'origine RPKI peut leur apporter dans ce domaine.

Cependant, l'ensemble du système, fondé sur des certificats X.509, reste complexe. Cette complexité comporte le risque que de nouvelles erreurs ou fautes de frappe se glissent dans la PKI de ressource elle-même. Ainsi, une expertise solide dans la gestion des systèmes cryptographiques restera probablement une condition préalable à l'activation de la ROV. La RPKI elle-même comporte aussi des inconvénients. Le délai de propagation, qui peut aller jusqu'à 24 heures, combiné à l'absence de surveillance systématique généralisée, peuvent constituer un problème opérationnel majeur. Il convient également de noter que la validation d'origine RPKI offre non seulement une réponse partielle au problème de la sécurisation du routage mais peut aussi constituer un vecteur de nouvelles menaces pour le système de routage, sous forme d'attaques visant les répertoires de ressources PKI, les différents certificats ou les systèmes de distribution des ROA. À ce jour, la validation d'origine de route (ROV) à l'aide de la RPKI n'a été déployée qu'à une échelle limitée. Des questions sans réponse subsistent encore par rapport à la montée en charge de l'ensemble du système.

Finalement, il appartiendra aux opérateurs de réseau de déterminer si les bénéfices qu'apporte la validation d'origine RPKI en termes d'intégrité du routage valent bien le coût associé à son infrastructure et à sa complexité opérationnelle. Certains opérateurs de réseau, inquiets des conséquences opérationnelles des fuites de route résultant de mauvaises configurations, semblent croire que c'est le cas, alors que d'autres, préoccupés par la sécurisation du routage, n'en sont pas encore convaincus. Un autre élément à signaler, peut-être plus important encore,

concerne le fait que la RPKI suppose des changements dans la structure opérationnelle critique de l'Internet global. Reste à savoir si les communautés concernées et affectées par ces changements en sont pleinement conscientes. L'enjeu justifie clairement que des efforts importants soient consentis pour communiquer les implications de la RPKI.

Remerciements

Bien que toutes les opinions exprimées dans ce rapport soient celles de l'auteur, nous tenons à remercier les personnes ci-dessous, qui ont contribué avec des retours, des commentaires ou des avis à l'élaboration du présent rapport :

- Alain Aina, WACREN
- Rob Austein, Hacntr
- John Curran, ARIN
- Kim Davies, ICANN (IANA)
- Geoff Huston, APNIC
- Fredrik Korsback, Amazon
- Nathalie Künnake-Trenaman, RIPE NCC
- Martin Levy, Cloudflare
- Di Ma, ZDNS
- Terry Manderson, ICANN (DNS et ingénierie réseau)
- Carlos Martinez, LACNIC
- Christopher Morrow, Google
- Ricardo Patara, NIC Brésil
- Amreesh Phokeer, AFRINIC
- Andrei Robachevsky, ISOC
- Job Snijders, NTT
- Bill Woodcock, PCH

Nous remercions tout particulièrement David Huberman, de l'ICANN, pour son soutien permanent et ses conseils avisés pendant la rédaction du présent document.