RFC 7132 : Threat Model for BGP Path Security

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 février 2014

Date de publication du RFC : Février 2014

https://www.bortzmeyer.org/7132.html

Tout le monde le sait, le système de routage de l'Internet, fondé sur le protocole BGP, n'est pas sûr. Il est trop facile d'y injecter des annonces de routes mensongères. Le premier pas vers une sécurité plus forte était de sécuriser la communication entre routeurs (RFC 5925 [1]). Un second pas a été réalisé avec le déploiement de la RPKI. Un troisième pas avec la normalisation de la solution RPKI+ROA <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>. Cette dernière protège uniquement l'**origine** d'une annonce BGP. Cela suffit à arrêter pas mal d'erreurs mais une attaque délibérée gardera probablement l'origine authentique et trichera sur le **chemin** d'AS présent dans l'annonce BGP. D'où la nécessité de continuer le travail. C'est le projet **PATHSEC** ("*Path Security*") pour lequel ce nouveau RFC énumère les motivations. (Le terme de BGPSEC avait été utilisé dans le passé mais PATHSEC semble plus fréquent aujourd'hui.)

Le but de PATHSEC est simple : garantir que le chemin d'AS dans une annonce BGP est authentique, et que les NLRI ("*Network Layer Reachability Information*") soient celles originellement annoncées. (Rappelez-vous que les ROA du RFC 6482 ne protègent que le début du chemin, l'origine.) Le chemin d'AS est transporté dans l'annonce BGP par l'attribut `AS_PATH` (RFC 4271, sections 4.3 et 5.1.2). La stratégie de PATHSEC est de s'appuyer sur la RPKI (RFC 6487), une infrastructure de distribution de certificats et d'objets signés. PATHSEC ne comptera pas sur une instance centrale qui connaitrait toutes les annonces BGP et pourrait tout vérifier. Au contraire, comme BGP lui-même, PATHSEC s'appuiera sur une vue locale, celle des routeurs d'un AS.

Pour concevoir proprement PATHSEC, il faut analyser les menaces, faire une **analyse de risque**. Que peut faire un méchant, même si tout le monde a déployé la RPKI et émet des ROA ? Il existe déjà des documents d'analyse des faiblesses de la sécurité du routage comme le RFC 4272 ou comme l'article de Kent, Lynn et Seo, « "*Design and Analysis of the Secure Border Gateway Protocol (S-BGP)*" » à la conférence

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5925.txt

IEEE DISCEX en 2000. Ce RFC détaille les faiblesses, notamment en indiquant celles qui resteront même dans un monde futur où tout les acteurs auront déployé PATHSEC. Le cahier des charges formel, lui, a été publié plus tard, dans le RFC 7353.

La section 3 résume les concepts. Une **menace** est un adversaire motivé et compétent. Il existe plusieurs catégories de menaces. Les opérateurs du réseau en sont une. L'opérateur peut demander à ses routeurs BGP d'émettre des messages visant à perturber le réseau ou à dérouter du trafic, par exemple pour le faire passer par des liens financièrement avantageux pour lui. Le contrôle légitime de routeurs BGP de la DFZ fait de cette catégorie d'attaquants potentiels une menace sérieuse. Si cet opérateur participe à la RPKI, il peut aussi émettre des vrais/faux certificats et ROA. Avec PATHSEC, il pourra donc signer de faux chemins d'AS.

Autre catégorie d'attaquants, les pirates informatiques qui prendraient le contrôle d'un ou plusieurs routeurs. Leurs capacités de nuisance seraient donc à peu près les mêmes que celles d'un opérateur, mais avec des limites (monter une attaque de l'Homme du Milieu serait plus difficile pour eux, le contrôle des routeurs ne donne pas forcément le contrôle de l'AC RPKI, etc). Le pirate est distinct du délinquant, étudié dans le paragraphe suivant, non par ses motivations (elles n'ont pas d'importance pour cette analyse technique du routage et de sa sécurité), mais par le fait que cette catégorie opère en général purement à distance, sans accès physique aux équipements. Le délinquant, lui, a d'autres possibilités. Par menace, chantage ou corruption, il peut même enrôler dans ses activités des employés de l'opérateur réseau. Contrairement au pirate, qui a parfois des motivations politiques, le délinquant est typiquement motivé par l'argent. Par exemple, il peut être payé pour réaliser une attaque par déni de service.

Les RIR sont aussi une menace pour le routage. Attribuant les ressources Internet (notamment les adresses IP), et étant à la racine de la RPKI, ils ont la possibilité de casser le routage. Pour prendre un exemple souvent cité, « l'attaque de la police néerlandaise <http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/summons-of-the-ripe-ncc-against-the-state-of-the-netherl une action en justice aux Pays-Bas contre le RIPE-NCC pourrait mener à une perturbation du routage de l'opérateur dont les ressources auraient été reprises par le RIR.

Enfin, les États sont eux-même souvent la principale menace. L'État contrôle, directement ou indirectement, les opérateurs sur son territoire, il a parfois des capacités de surveillance massive, il peut monter des attaques de l'Homme du Milieu (l'Iran l'a fait plusieurs fois et les mollahs ne sont certainement pas les seuls à le faire). Comme expliqué plus haut, l'État peut aussi avoir barre sur le RIR situé sur son territoire. Certaines de ces attaques peuvent se commettre en dehors du territoire de l'État (la NSA ou la DGSE espionnent à l'extérieur).

Après ce tour des (méchants) acteurs, la section 4 de notre RFC décrit les catégories d'attaques. D'abord, les attaques contre la session BGP établie entre deux routeurs. Un attaquant peut perturber une telle session (envoyer des paquets TCP `RST`) et ainsi fait du déni de service. Il peut aussi faire l'Homme du Milieu : le routeur d'Alice croit qu'il parle au routeur de Bob alors qu'en fait il parle au routeur pirate. Dans tous les cas, si la session BGP n'est pas protégée, l'attaquant peut faire des choses comme modifier les annonces BGP. Le problème est connu depuis longtemps, le RFC 4272 en parle en détail, et décrit les solutions. En gros, on peut considérer ce problème particulier comme étant résolu depuis des années.

Mais l'attaquant peut aussi viser directement le routeur. Que ce soit par piratage ou bien parce que l'attaquant est le gérant légitime du routeur, le résultat est le même. Une fois qu'on contrôle un routeur, on peut effectuer plein d'attaques. Attention, BGP permettant un contrôle détaillé de la politique de routage, toute manipulation BGP n'est pas forcément une attaque. Le RFC cite l'exemple d'une fuite où certaines routes sont propagées au-delà de ce que d'autres opérateurs considèrent comme légitime ; cela peut être une mauvaise idée égoïste, sans être forcément une attaque. (Un autre exemple pourrait être les annonces ultra-larges <https://www.bortzmeyer.org/annonces-bgp-larges.html>.) Par contre, ces manipulations seront unanimement considérées commes des attaques :

— Insérer d'autres numéros d'AS que les siens dans le chemin,
— Être à l'origine d'une route sans autorisation (les ROA - RFC 6482 - sont justement là pour bloquer cela),
— Voler (par copie) les clés privées utilisées par le routeur, soit pour l'authentification avec les routeurs voisins (s'ils utilisent l'AO du RFC 5925) soit pour signer les annonces de route avec PATHSEC,
— Et plusieurs autres (voir le RFC pour les détails).

Autres attaques possibles, moins directes : viser non pas les routeurs mais les machines de gestion du réseau. Si les routeurs sont gérés par un système central, avec Ansible ou Chef ou un logiciel équivalent, prendre le contrôle du système central permet de contrôler tous les routeurs.

La RPKI a ses propres vulnérabilités. L'attaquant peut viser un dépôt d'objets de la RPKI. S'il détruit les objets du dépôt ou bien rend celui-ci inutilisable, il a réalisé une attaque par déni de service contre la RPKI (voir aussi la section 5, sur ce risque). Notons quand même que la RPKI n'a jamais été prévu pour être synchrone. Les validateurs sont censés garder des copies locales et peuvent donc survivre un certain temps à une panne d'un dépôt en utilisant ces copies locales (et les durées typiques de synchronisation sont bien plus longues qu'avec le DNS, donc la mise en cache isolera de l'attaque pendant plus longtemps). Et, les objets étant signés, l'attaquant qui contrôle un dépôt ne peut pas changer les objets. Les manifestes du RFC 6486 protègent également contre certaines manipulations. Par contre, la RPKI reste vulnérable à certaines attaques par rejeu. Les opérateurs de la RPKI doivent donc choisir des dates de validité de leurs objets assez courtes pour les protéger du rejeu mais assez longues pour ne pas entraîner des problèmes opérationnels si, par exemple, le système de signature a un problème. (On note que c'est un problème très proche de celui de la sélection des durées de vie de signatures DNSSEC.)

Bien plus grave serait l'attaque réussie contre l'autorité de certification, et plus seulement contre le dépôt de publication. Parce que, cette fois, l'attaquant serait en mesure de créer des objets signés à sa guise. Il n'y a même pas besoin que l'attaquant réussisse à copier la clé privée de l'AC : il suffit qu'il prenne le contrôle du dispositif de gestion des données, avant la signature (c'est pour cela que les HSM ne protègent pas autant qu'on le croit, même s'ils ont le gros avantage de faciliter la réparation, une fois le problème détecté).

L'expérience de DNSSEC permet de prédire que les problèmes provoqués par la négligence, les bogues ou l'incompétence seront sans doute au moins aussi fréquents que les attaques. Pour reprendre une citation dans Pogo, rappelée par notre RFC, « "*We Have Met the Enemy, and He is Us*" ».

Enfin, la section 5 liste les vulnérabilités résiduelles, celles que même un déploiement massif de PATHSEC ne limiterait pas. Par exemple, une AC peut mal se comporter avec ses propres ressources (émettre un ROA pour un de ses préfixes mais avec le mauvais numéro d'AS, suite à une faute de frappe, par exemple). Même avec PATHSEC, quelques risques resteront. On a déjà parlé des fuites (route réannoncée alors qu'elle ne le devrait pas, mais avec un chemin d'AS correct), qu'on peut d'autant moins empêcher qu'il n'existe pas de définition consensuelle de ce qu'est une fuite. Il y a aussi le fait que PATHSEC ne protège pas **tous** les attributs d'une annonce BGP, alors même que certains sont utilisés pour prendre des décisions de routage. Et puis PATHSEC permet de vérifier une annonce mais pas de vérifier que l'annonce n'a pas été retirée entre temps. Si un lien est coupé, que des routeurs BGP retirent la route, mais qu'un méchant intercepte et détruit ces retraits de route, les anciennes annonces resteront valables un certain temps.