RFC 5635 : Remote Triggered Black Hole filtering with uRPF

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 août 2009

Date de publication du RFC : Août 2009

https://www.bortzmeyer.org/5635.html

Un des ennuis les plus fréquents sur l'Internet est l'attaque par déni de service. Répondre à ce genre d'attaques ne peut pas se faire par une mise à jour logicielle ou par un changement de configuration ; d'une manière ou d'une autre, il faut éliminer le trafic anormal qui constitue la DoS. Notre RFC 5635 [1] présente une technique permettant de déclencher le filtrage à distance, et en le faisant en fonction de l'adresse source des paquets IP de l'attaquant.

Plusieurs techniques ont déjà été développées pour faire face aux DoS, résumées dans la section 1 du RFC. Filtrer le trafic sur son propre routeur ou pare-feu est souvent inefficace : le trafic anormal a déjà transité sur votre liaison Internet et cela suffit souvent à la rendre inutilisable. Le mieux est en général de filtrer chez le FAI. Filtrer par le biais d'ACL marche bien mais les routeurs sont en général bien plus rapides à router qu'à filtrer à l'aide d'ACL. Il est donc préférable d'utiliser le routage en créant des routes « bidon », qui aboutissent dans le vide (`Null0` sur IOS, par exemple, ou bien `route ... discard` sur JunOS), et à qui on envoie le trafic indésirable. L'élimination des paquets sera ainsi faite à la vitesse maximale du routeur.

Autre problème avec le filtrage chez le FAI : le faire à la main, après échange de coups de téléphone, n'est pas très pratique, et impose des détails alors que l'attaque est déjà en cours. D'où l'utilité de pouvoir déclencher le filtrage à distance, selon la technique dite **RTBH** ("*Remote Triggered Black Hole*"), qui est décrite dans le RFC 3882. Dans ce RFC, on se sert de BGP pour annoncer le filtrage à un autre routeur, en marquant les annonces en question avec une **communauté** BGP particulière (une communauté est une sorte d'étiquette numérique attachée à l'annonce BGP).

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5635.txt`

C'était l'état de l'art documenté avant la sortie de ce RFC 5635. Le problème de cette méthode du RFC 3882 est que les routes, dans le protocole IP, sont en fonction de la **destination**. On va par exemple filtrer tout le trafic à destination du serveur victime d'une attaque. On empêche ainsi les dommages collatéraux sur les autres machines mais on rend le serveur attaqué complètement inaccessible (section 1 du RFC). Lors d'une attaque, on préférerait parfois filtrer selon la **source**.

Le principe est donc de combiner le RTBH ("*Remote Triggered Black Hole*") classique avec les techniques RPF du RFC 3704. C'est là l'apport de notre RFC, détaillé en section 4.

Avant cela, le RFC rappelle, dans sa section 3, le fonctionnement du RTBH par destination tel que décrit dans le RFC 3882, en fournissant des détails nouveaux. Le principe du RTBH est que l'annonce BGP indique comme routeur suivant ("*next hop*") une route vers un trou noir, où tous les paquets sont détruits. Les détails pratiques sont en section 3.2. Parmi eux, attention aux importants filtres de sortie, qui empêcheront les annonces BGP de destruction de fuir en dehors du réseau de l'opérateur.

Le déclenchement du filtrage par le client nécessite que celui-ci puisse communiquer ses desiderata. Il le fait en général en marquant ses annonces par une communauté BGP, choisie par l'opérateur. Celui-ci a même intérêt à prévoir plusieurs communautés, pour un filtrage plus fin.

La section 4 présente la nouvelle technique. Le principe est de réutiliser le mécanisme **uRPF** ("*unicast Reverse Path Forwarding*") du RFC 3704. uRPF vérifie qu'il existe une route légitime pour l'adresse **source** du paquet entrant, afin d'éliminer des paquets dont l'adresse source est fausse. Si le routeur sait qu'une route vers un trou noir n'est pas légitime, alors, il peut filtrer en fonction de la source, si des routes vers ces adresses sources ont été installées par RTBH. Pour l'instant, aucun routeur ne fournit apparemment la possibilité de refuser uniquement les adresses pour lesquelles la route va dans un trou noir, mais elle devrait apparaitre bientôt.

La section 4.1 fournit les étapes exactes à suivre lorsqu'on met en œuvre ce filtrage. Lorsqu'on veut bloquer les paquets venant de `192.0.2.66`, on doit :

— Activer RPF sur les routeurs du FAI,
— Annoncer, depuis le client, une route vers `192.0.2.66/32`, marquée avec la communauté BGP de filtrage indiquée par le FAI. (Attention, cela veut dire que le client va annoncer des réseaux qui ne lui appartiennent pas : le FAI devra accepter ces annonces mais faire très attention à ce qu'elles ne se propagent pas au delà de son réseau.)
— La route sera alors installée dans les routeurs du FAI, pointant vers un trou noir. Les tests RPF échoueront alors pour les paquets émis par l'attaquant et les paquets seront rejetés.

Permettre à n'importe quel client de vouer ainsi n'importe quelle adresse source au trou noir est évidemment dangereux et le RFC conseille de ne pas activer cette possibilité par défaut (contrairement à ce qu'on peut faire pour le filtrage selon la destination). Le RTBH reste utile même s'il n'est utilisé que dans le réseau de l'opérateur, car il évite de configurer manuellement tous les routeurs de ce dernier. La section 5 détaille les risques de cette technique et les précautions à prendre.

L'annexe A détaille la configuration des routeurs pour cette famille de techniques, avec des exemples concrets pour IOS et JunOS.

Un bon article sur RTBH est « "*Mitigating DoS/DDoS attacks with Real Time Black Hole (RTBH) filtering*" <http://blog.jason-rowley.com/2010/01/02/mitigating-dosddos-attacks-with-real-time-bla > », avec exemples pour Cisco IOS.