Peut-on usurper une adresse IP ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 novembre 2013. Dernière mise à jour le 15 novembre 2013

https://www.bortzmeyer.org/usurpation-adresse-ip.html

Question technique du jour : peut-on usurper une adresse IP source sur l'Internet, c'est-à-dire peut-on envoyer un paquet IP en utilisant une adresse IP source qui n'est pas la sienne et qu'on n'a normalement pas « le droit » d'utiliser ? Tous les gens qui connaissent un peu l'Internet vont répondre « oui, on peut, c'est même une faiblesse de sécurité connue ». Mais la réalité est plus complexe.

La possibilité d'envoyer un paquet IP avec une adresse source usurpée découle du mode « datagramme » de fonctionnement d'IP. Chaque paquet est indépendant, porte des adresses source et destination que l'émetteur met à la valeur qui lui chante et, le paquet n'étant routé que sur la destination, il devrait arriver sans problème. Un certain nombre d'attaques, comme les attaques par réflexion <https://www.bortzmeyer.org/attaques-reflexion.html>, fonctionnent sur cette base.

Sur une machine Unix, par exemple, l'envoi d'un tel paquet se fait facilement avec hping :

```
% sudo hping --syn --spoof 192.0.2.42 -p 80 www.example.com
```

Notez que cela nécessite d'être root. À l'époque des gros "*mainframes*" très chers sur lesquels on n'avait qu'un compte utilisateur, c'était une limite. Aujourd'hui que chacun est root sur son PC ou sur son Pi <https://www.bortzmeyer.org/raspberry-pi.html>, cela n'est plus un obstacle.

En raison des possibilités d'attaque, cet envoi avec une fausse adresse est très mal vue. La position officielle de l'IETF est que les FAI et autres acteurs des réseaux doivent interdire cet envoi, et c'est documenté dans deux RFC connus collectivement sous le nom de « BCP 38 <https://www.bortzmeyer.org/bcp38.html> » (BCP pour "*Best Current Practices*"), les RFC 2827[1] et RFC 3704.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt

BCP 38 est loin d'être déployé par tous les opérateurs, comme le montrent les statistiques du Spoofer Project <http://spoofer.cmand.org/> et cela explique pourquoi les attaques par réflexion continuent, et ne semblent pas devoir disparaître de si tôt. Néanmoins, certains opérateurs bloquent les paquets usurpés. (Un projet plus récent, visant à aller plus loin que BCP 38, est SAVI, RFC 6959.)

J'ai fait quelques tests avec hping et avec un logiciel écrit spécialement, afin de tester aussi en IPv6 (hping ne parle toujours pas IPv6 et son concurrent nping très mal et j'avais la flemme d'installer hping6 <http://hping6.sourceforge.net/>). Sur trois fournisseurs différents de VPS, trois échecs. Chez un FAI grand public, idem (la "*box*" de ce FAI peut être configurée de deux façons différentes et je n'en ai testé qu'une, l'autre est peut-être plus favorable à l'usurpation). En IPv4, le NAT gêne probablement beaucoup toute tentative de triche. (Mais il y a une astuce, chez ce FAI, pour réussir à faire sortir les paquets usurpés malgré le NAT.)

Donc, si vous voulez vous lancer dans l'usurpation d'adresses IP, attention, ne vous attendez pas à ce que cela marche partout (mes tests ont été faits à partir d'accès accessibles au grand public ; cela peut être différent si l'usurpateur contrôle un réseau entier, avec un fournisseur de transit qui ne vérifie rien). Mais il y a d'autres obstacles que ceux de la couche 3. En effet, bien des protocoles utilisés au dessus d'IP nécessitent une réponse or l'usurpateur ne recevra pas forcément les réponses à ses paquets, puisqu'il a mis une autre adresse que la sienne. Distinguons deux cas : dans le premier, l'usurpateur peut voir les réponses (par exemple parce qu'il est sur le même réseau local que la victime dont il a usurpé l'adresse, et que ce réseau local n'a pas de protection contre le "*sniffing*" ; ou bien parce qu'il pratique le détournement de préfixes entiers par une attaque contre les protocoles de routage, ce qui est possible mais bien plus sophistiqué). Alors, l'usurpateur, s'il n'est pas bloqué par BCP 38 <https://www.bortzmeyer.org/bcp38.html>, pourra envoyer des paquets avec une adresse mensongère et, voyant les réponses, pourra entretenir le dialogue.

Mais le second cas est plus fréquent : l'usurpateur ne voit pas du tout les paquets de retour, il doit travailler en aveugle. C'est beaucoup plus embêtant pour lui, car les protocoles sont en général conçus pour rendre la vie difficile pour un attaquant aveugle. Ainsi, TCP a un numéro de séquence dans les paquets et ce numéro part d'un numéro initial, l'ISN ("*Initial Sequence Number*") qui est désormais choisi de manière imprévisible (si tout le monde suit bien les RFC 6528 et RFC 5961). Ne sachant pas quel est l'ISN, l'usurpateur ne pourra pas tenir un dialogue avec son correspondant. C'est pour la même raison que l'IETF recommande des ports source imprévisibles dans le RFC 6056. Et c'est aussi pour cela que le DNS a ses "*Query ID*", un nombre imprévisible mis dans la requête et qui doit être renvoyé dans la réponse, pour que celle-ci soit acceptée. Malheureusement, dans le cas du DNS, ce "*Query ID*", avec ses 16 bits, est trop petit et un usurpateur a donc toujours une chance. Et la technique de TCP n'est pas imparable non plus.

En résumé, oui, IP permet de tricher sur l'adresse source mais si vous voulez utiliser cette possibilité pour l'amusement, la gloire ou le fric, étudiez bien la question : cela peut être plus difficile à exploiter que cela n'en a l'air.