RFC 2827 : Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 mars 2006. Dernière mise à jour le 14 novembre 2006

Date de publication du RFC : Mai 2000

https://www.bortzmeyer.org/2827.html

Une faille sérieuse de la sécurité dans l'Internet, identifiée depuis de nombreuses années, est la trop grande facilité avec laquelle une machine peut usurper ("*spoofer*") son adresse IP source. Un attaquant peut ainsi déguiser son identité et court-circuiter les filtres. Ce RFC propose une solution, que les FAI devraient déployer, si on veut améliorer sérieusement la sécurité de l'Internet.

Mettons que ma machine soit connectée à l'Internet, via un FAI, avec l'adresse IP `172.20.34.125`. Je pingue une machine distante, par exemple `www.elysee.fr`. C'est ma machine qui fabrique les paquets IP et qui met dans le champ "adresse IP source" le `172.20.34.125`. Mais si je suis un méchant, qu'est-ce qui m'empêche de mettre une autre adresse en source ? Rien. (Si vous ne savez pas programmer, ne vous inquiétez pas, des outils comme hping <http://www.hping.org/> sont là pour cela, avec l'option bien nommé `--spoof`.)

L'adresse source étant usurpée, l'attaquant ne recevra en général pas la réponse mais, pour certains protocoles, comme UDP, ce n'est pas un problème.

Et cela permet des attaques intéressantes, comme les DoS. La victime ne pourra pas savoir d'où le paquet vient réellement. Il y a aussi les attaques par **réflexion** où l'attaquant écrit à une machine tiers, en usurpant l'adresse de sa victime. Le tiers va alors répondre à la victime, qui se croira attaquée par le tiers, pourtant innocent. Une telle attaque est décrite en <http://www.grc.com/dos/drdos.htm>.

Encore pire, les attaques par réflexion avec amplification, qui permettent à l'attaquant d'obtenir un débit sur sa victime supérieur à celui que l'attaquant doit lui-même fournir. Les récentes attaques DNS, utilisant comme tiers des relais DNS récursifs <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html> ouverts, appartiennent à cette catégorie. Ces attaques sont décrites en <http://weblog.barnet.

com.au/edwin/cat_networking.html> et une approche du problème est en <http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>.

Notre RFC propose donc de tenter de mettre fin à ces usurpations. Cela peut se faire chez les FAI, en s'assurant que ne peuvent sortir du réseau du FAI que les paquets IP dont l'adresse est une des adresses allouées par ledit FAI.

Le principe est simple (notre RFC est d'ailleurs très court car, techniquement, il n'y a pas grand'chose à dire) : sur les routeurs du FAI, soit sur ceux faisant face aux clients, soit sur ceux de sortie, mettre en place une règles de filtrage interdisant tout trafic venant d'une adresse non allouée. Par exemple, si le routeur est une machine Linux, et que le réseau du FAI est le 172.20.128.0/22, il suffit de :

```
iptables --insert FORWARD --out-interface eth1 --source \! 172.20.128.0/22  --jump LOG --log-prefix "IP spoo
iptables --insert FORWARD --out-interface eth1 --source \! 172.20.128.0/22  --jump DROP
```

Naturellement, il faut bien vérifier qu'on couvre tous les cas : beaucoup d'opérateurs ont du mal à compiler une liste exacte de tous leurs préfixes, ce qui explique en partie le peu de déploiement de ce RFC.

Notons que, comme toute mesure de sécurité, celle-ci a des faux positifs (le RFC cite le cas des mobiles) et qu'elle peut bloquer ou bien rendre très difficiles des usages parfaitement légitimes (le RFC cite le cas du "*multihoming*", traité dans un autre document, le RFC 3704 [1]). Elle a aussi des faux négatifs : certaines usurpations ne seront pas forcément détectées, par exemple lorsqu'un client du FAI usurpe l'adresse d'un autre client du même FAI.

Notre RFC date de presque six ans et ne semble toujours pas largement déployé : cela donne une idée de la difficulté du problème. En effet, déployer ce RFC (aussi connu sous son numéro de bonne pratique, BCP38 <https://www.bortzmeyer.org/bcp38.html>), coûte de l'argent au FAI et en fait économiser aux autres opérateurs de l'Internet, par les attaques que cela leur épargne. On conçoit que le simple bon sens économique et l'absence de régulation autre que celle du marché limitent la mise en œuvre de ce RFC.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3704.txt