Comment on dit « returnability » ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 mai 2012. Dernière mise à jour le 4 mai 2012

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

Un concept important est présent dans beaucoup de protocoles de la famille TCP/IP, mais pas toujours sous un nom explicite : le concept de « "*returnability*" » ou « existence d'une voie de retour » (je vais plutôt dire « réversibilité »).

Le protocole IP est unidirectionnel : si un paquet émis depuis une certaine adresse source vers une certaine destination arrive, rien ne prouve que la destination pourra répondre juste en inversant source et destination. Dans certains cas, cela marchera, mais pas dans d'autres :

- Adresse IP source usurpée, ce qui fait que le méchant ne recevra pas les réponses (technique utilisée dans des attaques en aveugle),
- Pare-feu qui laisse passer les paquets dans un seul sens,
- Routage incomplet : la transmission des paquets, dans IP, se fait uniquement sur la destination. Dans la plupart des cas, l'adresse source est ignorée, et il n'y aura pas forcément de route menant la réponse vers elle.

Certains protocoles aimeraient bien tester qu'il y a « réversibilité », autrement dit qu'on peut répondre à celui qui écrit. Par exemple, ce test permet de lutter contre les attaques effectuées en aveugle. C'est ainsi que TCP génère des numéros de séquence initiaux qui sont non prévisibles (et qui devront être utilisés par le pair), pour s'assurer que le pair reçoit bien les paquets (et n'est donc pas un attaquant aveugle). Le RFC 6528 [1] décrit le problème de TCP et sa solution.

À l'inverse, il n'existe pas de tel test dans le DNS (qui fonctionne presque toujours sur UDP), ce qui permet les attaques par réflexion <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>.

Aujourd'hui, ce terme de « "*returnability*" » figure dans les RFC du protocole LISP, protocole qui fait un gros usage du concept, en le nommant explicitement. LISP teste la réversibilité via des nonces, qui jouent le même rôle que les numéros de séquences initiaux de TCP. Lisez le RFC 6830, ou bien la bonne introduction de David Meyer <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_11-1/111_lisp.html>. Vu la montée des préoccupations de sécurité, notamment contre les DoS, il est probable que le terme sera de plus en plus employé. Le protocole QUIC <https://www.bortzmeyer.org/quic.html> intègre également des tests de réversibilité.

Merci à Gaëtan <https://twitter.com/Erebuss> pour avoir proposé « réversibilité ». On trouve aussi d'autres suggestions intéressantes lors de la discussion sur SeenThis <http://seenthis.net/messages/67667>.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6528.txt