RFC 4732 : Internet Denial-of-Service Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 janvier 2007

Date de publication du RFC : Décembre 2006

https://www.bortzmeyer.org/4732.html

Les attaques par déni de service ("*DoS*") étant le fléau de l'Internet depuis plusieurs années, et un fléau dont l'ampleur croît chaque jour, il n'est pas étonnant que l'IAB aie voulu consacrer un RFC à une vision générale du problème.

Contrairement à d'autres, les attaques DoS ne visent pas à prendre le contrôle d'un système informatique, mais à l'empêcher de fonctionner. Les motivations peuvent être de pur vandalisme ou bien relever de l'extorsion criminelle (à la veille du Super Bowl, beaucoup de sites Web de paris en ligne ont reçu des messages du genre « Payez ou bien on vous DoS demain, pendant la journée qui est normalement celle du plus gros chiffre d'affaires. ») Ces attaques sont d'autant plus difficiles à contrer qu'elles utilisent désormais en général un "*botnet*", un réseau de dizaines ou de centaines de milliers de machines Windows piratées et transformées en zombies, prêts à attaquer sur l'ordre de leur contrôleur.

La section 2 de notre commence par expliquer les différents types d'attaques DoS. Elles peuvent viser un logiciel mal programmé, tenter d'épuiser une ressource limitée (mémoire ou espace disque ou bien des structures de données de taille finie), elles peuvent viser les machines ou bien les liens qui les relient, elles peuvent viser un service essentiel comme le DNS dont l'arrêt bloquera presque tout le reste (songeons à la la grande attaque du 21 octobre 2002 <http://www.isc.org/f-root-denial-of-service-21-oct-200 contre les serveurs racine).

Les attaques DoS peuvent aussi être physiques, c'est-à-dire consister en atteintes matérielles contre le réseau. Elle peut aussi être légale, comme les courriers menaçants, misant sur l'ignorance en droit du destinataire, et qui commandent l'arrêt immédiat de tel ou tel service (lettres "*cease and desist*" en anglais).

Notre RFC rappelle à plusieurs reprises que les DoS utilisent souvent une solution anti-DoS. Par exemple, un serveur de courrier qui utilise une liste noire <http://www.halte-au-spam.com/ddm-blacklists.htm> pour tenter de limiter l'avalanche de spam peut être victime d'une DoS si les serveurs de la liste noire, piratés, se mettent à renvoyer, pour chaque adresse IP, « C'est un spammeur ».

Certaines attaques DoS se font par **force brute** : l'attaquant dispose de ressources supérieures à sa victime et peut, par exemple, se permettre d'envoyer des paquets IP en quantité, sans égard pour sa propre bande passante. C'est évidemment une tactique efficace si on contrôle un "*botnet*" puisque les plus grosses machines, reliées au mieux connecté des réseaux, ne peuvent jamais aligner autant de ressources que les centaines de milliers de zombies du "*botnet*".

Mais d'autres attaques DoS sont plus subtiles car elles exploitent l'**amplification** : c'est une propriété de certains protocoles que la réponse peut être bien plus grosse que la requête, permettant ainsi à l'attaquant d'économiser ses propres ressources. Ainsi, la réponse à une requête DNS peut être des dizaines de fois plus grosses que la requête, propriété exploitée dans les attaques via des récursifs ouverts <https://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html>.

La section 4 du RFC envisage les contre-mesures : elle se divise en conseils pour les auteurs de protocoles, pour les implémenteurs, et pour les opérateurs de réseau.

Les auteurs de protocole, et l'IESG y veille désormais, doivent veiller à ce que leur protocole ne permette pas l'amplification pour un client non authentifié et n'alloue pas de ressources pour de tels clients. Par exemple, les anciennes mises en œuvre de TCP allouaient une petite quantité de mémoire pour chaque demande de connexion, même non confirmée, ce qui permettait l'attaque dite "*SYN flooding*". Les implémentations récentes permettent d'utiliser des petits gâteaux à la place. L'invention de ce mécanisme de "*SYN cookies*" n'a été possible qu'en trichant légèrement avec la définition du protocole TCP.

Ce mécanisme, ainsi que les autres défenses spécifiques à TCP, sont exposées dans le RFC 4987[1].

De plus, les protocoles ne devraient plus permettre, comme le fait SIP, d'inclure dans les messages les adresses IP auxquelles il faut envoyer la réponse. Une telle possibilité fait que l'attaquant n'a même plus besoin d'usurper l'adresse IP de sa victime !

Mais, de toute façon, cela ne concerne que les nouveaux protocoles et on ne peut pas supprimer d'un coup les anciens. Et l'IAB note bien que les protocoles conçus pour faciliter la vie des utilisateurs et des administrateurs réseaux, comme DHCP ou LLMNR, sont particulièrement vulnérables et qu'on ne peut pas les renforcer sans perdre cette possibilité de « réseau sans configuration » qui est si pratique. La sécurité est clairement ici en opposition avec la facilité d'usage.

Les architectes et administrateurs de réseaux devraient veiller à ce que l'accès aux équipements soit toujours possible en cas d'attaque, par exemple via des connexions "*out-of-band*", c'est-à-dire n'utilisant pas le réseau principal.

Les implémenteurs devraient veiller à se méfier de l'usage de structures de données de taille finie. D'un autre côté, comme la mémoire de l'ordinateur est finie, fermer une possibilité d'attaque pourrait en ouvrir une autre. Le RFC recommande donc de bien veiller à une bonne gestion en cas d'épuisement des ressources : le programme peut ralentir mais il ne devrait pas crasher.

À nouveau, notre RFC insiste sur l'importance qu'il y a à ne pas réagir n'importe comment : l'histoire de la sécurité est pleine de mesures adoptées dans l'urgence et qui se révèlent pires que le mal. La sécurité n'aime pas les Yaka et les Fokon...

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4987.txt