Attaques par amplification : TCP aussi

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 octobre 2015

https://www.bortzmeyer.org/amplification-tcp.html

On a beaucoup parlé des attaques DoS par réflexion + amplification <https://www.bortzmeyer.org/attaques-reflexion.html> en les présentant souvent comme spécifiques à UDP. Mais un article récent (mais passé curieusement inaperçu) montre qu'on peut en faire également avec TCP.

Petit rappel du principe de cette attaque : il y a trois parties, l'attaquant A, la victime V et le réflecteur R. Ce dernier est innocent (il n'a rien contre la victime) mais souvent négligent (il a laissé un réflecteur ouvert alors qu'il n'aurait pas dû). A envoie un paquet IP dont l'adresse source est usurpée : il met l'adresse de V (cela implique que le FAI de A ait ignoré le RFC 2827 [1]). L'adresse de destination est celle de R. Celui-ci répond à celui qu'il croit être l'expéditeur, donc à V. Ainsi, R va bombarder V.

Sans amplification, les attaques par réflexion n'ont que peu d'intérêt. Mais ce qui est rigolo, c'est que certains protocoles envoient une réponse plus grande (en nombre de paquets ou bien en nombre d'octets) que la question. On a ainsi une amplification, A obtient plus de paquets ou d'octets qu'il n'en a envoyé. L'efficacité d'un réflecteur se mesure à son PAF ("*Packet Amplification Factor*") ou à son BAF ("*Bandwidth Amplification Fcator*").

Usurper une adresse IP en TCP est très difficile <https://www.bortzmeyer.org/usurpation-adresse-ip.html> et c'est pour cela que ces attaques, dans la nature, étaient typiquement faites en UDP (en utilisant par exemple NTP <https://www.bortzmeyer.org/ntp-reflexion.html>). Le seul cas que je connaissais personnellement où on pouvait avoir une amplification avec TCP était la suivante : A envoie un paquet `SYN`, R transmet le `SYN/ACK` à V, puis, n'ayant pas de nouvelles de V, réémet le `SYN/ACK`, typiquement cinq fois. Cela donne donc un PAF de 5 et un BAF ayant la même valeur (le `SYN/ACK` ayant la même taille que le `SYN`). Comme toutes les attaques, la pratique est plus compliquée que cela (si V émet un `RST` en recevant ce `SYN/ACK` inattendu, cela stoppe la réémission) mais l'attaquant astucieux peut s'en tirer quand même. Ceci dit, un PAF et un BAF de 5 ne font pas une attaque bien terrifiante.

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

C'est là qu'arrive l'article de Kührer, Hupperich, Rossow et Holz, « "*Hell of a handshake : Abusing TCP for reflective amplification DDoS attacks*" <http://www.christian-rossow.de/publications/tcpamplificat pdf> » publié à USENIX en août 2014 et apparemment passé relativement inaperçu (merci à Paul Vixie pour me l'avoir signalé).

Les auteurs ont montré qu'il existait d'autres voies d'amplification avec TCP que le `SYN/ACK` indiqué plus haut et, pire, qu'il existait des machines dans l'Internet qui répondaient et qui étaient disponibles comme réflecteurs. Par exemple, certains systèmes répondent au `SYN` initial par des paquets de données, souvent de très grande taille, avant même que la triple poignée de mains (l'établissement de la connexion TCP) soit terminée ! (Ce qui justifie ma loi « si une connerie d'implémentation de TCP/IP est possible, alors il existe au moins une machine dans l'Internet qui la fait ».)

Les mesures décrites dans l'article sur un échantillon de vingt millions de machines montrent ainsi plus de 600 000 machines qui répondent sur le port de MySQL dont 8 sont des amplificateurs, avec un BAF moyen de 84 000 (oui, une réponse 84 000 fois plus grosse que la requête). Extrapolé à tout l'Internet IPv4, cela ferait 1 700 amplificateurs MySQL.

Le BAF est plus faible sur les ports FTP ou telnet (de l'ordre de 50) mais il y a beaucoup plus d'amplificateurs (des millions, en extrapolant à tout l'Internet IPv4).

Les analyses des réflecteurs semblent indiquer qu'il s'agit de machines très variées et qu'il n'y a donc pas **un** vendeur dont l'implémentation particulièrement boguée serait responsable. Par exemple, les machines avec un port telnet ouvert semblent être surtout des routeurs, mais de marques très variées. Les fanas de sécurité noteront toutefois que de nombreuses caméras de vidéosurveillance IP semblent être des réflecteurs. Joie de l'Internet des objets.

Les auteurs discutent aussi des solutions, pour l'instant peu convaincantes. Le mieux, pour la victime, est d'envoyer des `RST` ou, surtout, des ICMP "*port unreachable*" aux réflecteurs : souvent, cela les calme. Mais le problème de fond, surgi de la combinaison entre la possibilité de tricher sur son adresse IP et la disponibilité de nombreux réflecteurs amplificateurs, reste.