Attaques par réflexion : DNS, SNMP mais aussi...

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 août 2013

http://www.bortzmeyer.org/attaques-reflexion.html

Lorsqu'on parle d'attaques par déni de service utilisant la **réflexion**, on pense souvent uniquement au DNS. Pourtant, d'autres protocoles permettent ces attaques. C'est ainsi qu'un récent message <http://mailman.nanog.org/pipermail/nanog/2013-July/060094.html> sur la liste NANOG vient de rappeler que le protocole SNMP est couramment employé pour ces attaques.

En quoi consiste une **attaque par réflexion** ? C'est une attaque où le méchant ment sur son adresse IP : il envoie des paquets avec une adresse IP source qui n'est pas la sienne. Si tout le monde mettait en œuvre la recommandation « BCP 38 <http://www.bortzmeyer.org/bcp38.html> » (les RFC 2827 [1] et RFC 3704), ce mensonge ne serait pas possible. Mais BCP 38 est très loin d'être déployé partout, pour de simples raisons économiques (déployer BCP 38, c'est dépenser de l'argent pour protéger ses concurrents...) Les paquets mensongers sont donc possibles et les réponses à ces paquets mensongers seront envoyés à l'adresse IP source indiquée, qui est celle de la victime.

Cela n'est possible que si le protocole de transport n'impose pas l'établissement d'une connexion. Ainsi, UDP est vulnérable mais pas TCP, du moins si on le met en œuvre correctement (RFC 6528).

Le trafic reçu par la victime peut être énorme en raison de l'**amplification**. Contrairement à certains protocoles comme ICMP "*echo*" (celui utilisé par ping), les protocoles comme le DNS ou comme SNMP amplifient l'attaque lors de la réflexion : la réponse est plus grosse que la question. Avec le DNS, on atteint des facteurs d'amplification de 40 ou 50 <http://www.bortzmeyer.org/amplification-dns-combien.html>. Avec SNMP, comme l'indique le message NANOG cité plus haut, on atteint plusieurs centaines... Un attaquant peut alors obtenir une attaque de 100 Gb/s en « dépensant » seulement quelques dizaines de Mb/s.

Le risque associé à SNMP est connu depuis un certain temps. Le BITAG <http://www.bitag.org/> a ainsi produit l'année dernière un excellent rapport sur la question <http://www.bitag.

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

org/report-snmp-ddos-attacks.php> (malgré des conclusions qui ne vont pas toujours dans le sens de la neutralité du réseau <http://www.bortzmeyer.org/neutralite.html>). Un membre de BITAG, Comcast a annoncé des mesures <http://corporate.comcast.com/comcast-voices/taking-steps-to-prevent-unintentional-network-abuse> comme « *"we will gradually change our default residential Internet device bootfile to restrict SNMP by default"* ».

Mais quelles sont les parts relatives de DNS ou de SNMP dans ces attaques ? Peut-on dire que l'un est bien plus dangereux, car plus souvent exploité que l'autre ? Et, d'ailleurs, s'agissant du DNS, les attaques par réflexion peuvent se faire avec des résolveurs ouverts <http://www.bortzmeyer.org/fermer-les-recursifs-ouverts.html> ou bien avec des serveurs faisant autorité ; en pratique, quels sont les plus utilisés ? Eh bien, c'est embêtant, mais **on ne le sait pas**. Il n'y a pas d'étude systématique et indépendante des attaques par déni de service. Lorsqu'une grosse attaque se produit (genre Spamhaus/Cloudflare <http://seenthis.net/messages/125474>), on ne sait que ce que contient le communiqué officiel, toujours très court en détails techniques. Et, souvent, il n'y a même pas de communiqué et on n'a que des supputations journalistiques à se mettre sous la dent. Donc, c'est un point important dont il faut se rappeler : on ne connait pas vraiment les attaques par déni de service. Chacun connait celles dont il est victime mais pas celles des autres. Certaines attaques font l'objet de rapports détaillés dans des réunions mais impossible de savoir si elles sont représentatives.

Et il n'y a pas que le DNS et SNMP. NTP a aussi servi à ces attaques <http://www.bortzmeyer.org/ntp-reflexion.html>. Et les protocoles utilisés par les jeux en réseau ont également été utilisés (un cas fameux <http://www.ar15.com/archive/topic.html?b=1&f=5&t=1131291> a touché Call of Duty - voir aussi cet article <http://www.lexsi-leblog.com/cert-en/new-dos-attack-amplified html>, une étude comparative <http://blog.cinu.pl/2013/03/amplifying-ddos-data-volume-by-usi html> a montré que Counter-Strike fournissait la meilleure amplification, etc). Comme les développeurs n'ont pas en général de culture historique, la vulnérabilité d'UDP aux attaques par réflexion est régulièrement oubliée et redécouverte <http://comments.gmane.org/gmane.network.peer-to-peer.p2p-hackers/3603>. Des protocoles en cours de développement (comme COAP) sont ainsi créés avec cette vulnérabilité.

Sinon, pour mes lecteurs juristes, une discussion intéressante : quelle est la responsabilité juridique du réflecteur, l'entité qui fait l'amplification mais ne participe pas volontairement à l'attaque ? L'article 1382 <http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438819&dateTexte=20140115> du Code Civil (qui fait obligation de réparer les dommages qu'on cause) peut-il s'appliquer ?