Nouvelles attaques facilitant l'empoisonnement DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 août 2013

https://www.bortzmeyer.org/dns-attaques-shulman.html

À la réunion de l'IETF à Berlin le premier août, Haya Shulman a présenté le résultat de ses recherches sur des techniques permettant d'améliorer (en parlant avec le point de vue de l'attaquant) les attaques par empoisonnement DNS. Cela illustre un vieil adage de la sécurité : « les attaques ne régressent jamais, au contraire elles deviennent plus efficaces avec le temps ». Concrètement, cela veut dire que des attaques qui semblaient théoriques deviennent pratiques.

Il s'agit de plusieurs attaques différentes, permettant d'empoisonner un cache plus facilement. Ces attaques n'ont pas forcément de rapport entre elles mais, dans certains cas, une des attaques décrites peut faciliter les autres. La principale, de loin, est un mécanisme astucieux pour exploiter la fragmentation. On suscite la création d'une réponse qui sera fragmentée (`dig -4 +dnssec @$NAMESERVER ANY $DOMAIN`, où `$DOMAIN` est un domaine contenant suffisamment de données pour dépasser la MTU), et on obtient un paquet normal et un fragment (ici, vus avec tcpdump) :

```
09:05:06.032332 IP (tos 0x0, ttl 64, id 30286, offset 0, flags [none], proto UDP (17), length 59)
    192.0.2.69.47170 > 198.51.100.1.53: 53344+ [1au] ANY? example. (31)
09:05:06.034638 IP (tos 0x0, ttl 60, id 27730, offset 0, flags [+], proto UDP (17), length 1388)
    198.51.100.1.53 > 192.0.2.69.47170: 53344*- 22/0/1 example. SOA master.nic.example. ... |domain]
09:05:06.034662 IP (tos 0x0, ttl 60, id 27730, offset 1368, flags [none], proto UDP (17), length 1495)
    198.51.100.1 > 192.0.2.69: ip-proto-17
```

Toutes les techniques "*anti-spoofing*" (le "*Query ID*" du DNS, le port source `UDP`, même la casse du nom demandé) sont dans le **premier** paquet. Le second, le fragment final, peut donc être remplacé par le méchant et il contient un bout de la section réponse plus la section additionnelle, où le méchant peut glisser des fausses informations. L'attaque remplace donc le problème difficile de trouver {"*Query ID*", port} par le problème facile de trouver l'identificateur de fragment (ici 27730), bien plus prévisible (cf. RFC 7739 [1]), et sur seulement deux octets en IPv4 (d'où le -4 dans ma requête dig : l'attaque ne marche pas en IPv6, où l'identificateur de fragment fait quatre octets). Il reste comme seule protection la somme

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7739.txt`

de contrôle UDP : comme elle n'est pas cryptographiquement forte, il est trivial de la maintenir intacte tout en mettant ses fausses informations.

La seconde attaque détaillée dans cet exposé est la « dé-aléatoirisation » du port source. La technique dite SPR ("*Source Port Randomization*") est la principale technique qui avait été déployée à partir de 2008 contre la faille Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html>. Elle consiste à utiliser des ports sources aléatoires par requête DNS. L'étude des auteurs montre que trop de résolveurs font certes de la SPR mais sont trahis par la suite, notamment par un routeur NAT qui dé-aléatoirise (d'autant plus qu'il existe encore des gens qui croient que le NAT améliore la sécurité <https://www.bortzmeyer.org/nat-et-securite.html>).

Le risque est réel, l'attaque bien expliquée. DNSSEC est la seule solution. Il ne faut donc pas se rassurer en se disant que les empoisonnements sont trop durs à réaliser, les attaques s'améliorent. D'autant plus que tous les travaux de ces auteurs ne sont pas encore publics et que d'autres améliorations de l'attaque sont en cours.

Les bonnes lectures :

— Les diapos de Shulman <http://www.ietf.org/proceedings/87/slides/slides-87-saag-3.pdf> et l'article complet <http://arxiv.org/pdf/1205.4011v1.pdf>,
— Un précédent article des mêmes auteurs <http://arxiv.org/abs/1205.4011>, se focalisant sur l'attaque par fragmentation,
— Et encore un article des mêmes <http://seenthis.net/messages/100568>, consacré aux contre-mesures contre ces attaques.
— L'exposé d'Ond[Caractère Unicode non montré [2]]ej Sur[Caractère Unicode non montré] à la réunion OARC <https://www.dns-oarc.net/> de Phoenix en octobre 2013, où il annonçait la première mise en œuvre réussie <https://indico.dns-oarc.net/indico/materialDisplay.py?contribId=18&materialId=slides&confId=1> de cette attaque (voir aussi sa vidéo <https://indico.dns-oarc.net//getFile.py/access?resId=10&materialId=0&confId=1>).

2. Car trop difficile à faire afficher par LaTeX