La sécurité de BIND, et le gonflationnage par le marketing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 mai 2014

https://www.bortzmeyer.org/bind-securite-marketing.html

Le 29 avril 2014, l'université Technion a publié un communiqué ridicule <http://www.technion.ac.il/en/2014/04/students-reveal-loophole-in-dns-security/> prétendant que leurs chercheurs avaient trouvé un moyen de subvertir les requêtes DNS. C'est apparemment sa reprise par The Hacker News <http://thehackernews.com/2014/05/critical-vulnerability-in-bind-software.html> le 5 mai qui a lancé le « "*buzz*" ». Comme le communiqué du service marketing de l'université, l'article de The Hacker News est fertile en superlatifs et, à le lire, on se dit qu'Heartbleed n'était que de la petite bière. Sauf que tout est tellement gonflé qu'il est très difficile d'apercevoir le vrai problème de sécurité derrière cette accumulation de sensationnalisme.

Revenons aux choses sérieuses. Lorsqu'un client veut utiliser le DNS pour résoudre un nom de domaine en données (par exemple l'adresse IP), il s'adresse à un **résolveur** DNS. Les logiciels les plus courants pour cette fonction sont BIND et Unbound. Le résolveur n'a pas d'informations propres, il doit les obtenir auprès des **serveurs faisant autorité** pour la zone considérée. Par exemple, `linuxfr.org` a deux serveurs faisant autorité :

```
% dig +short NS linuxfr.org
ns1.tuxfamily.net.
ns2.tuxfamily.net.
```

Lequel des deux sera interrogé par un résolveur dont le client veut visiter <http://linuxfr.org> ? Cela dépend d'un algorithme suivi par le résolveur, qui prend en compte le RTT des réponses lors des requêtes précédentes, mais aussi une certaine dose de hasard, à la fois pour voir si les temps de réponse ont changé, et aussi pour compliquer la tâche d'un attaquant. En effet, lors de certaines attaques, notamment l'attaque d'empoisonnement Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-fa
html>, l'attaquant a besoin de savoir quel serveur faisant autorité sera utilisé. En tirant partiellement au sort, on complique sa tâche.

Venons-en à l'attaque elle-même, documentée dans un article à Usenix <https://www.usenix.org/conference/woot13/workshop-program/presentation/hay> (et je ne sais pas pourquoi l'université de Technion a choisi de "*buzzer*" maintenant, sur une publication de l'année dernière). Son

titre résume bien le peu d'étendue de l'attaque : « "*Subverting BIND's SRTT Algorithm Derandomizing NS Selection*" ». Les auteurs ont trouvé une méthode (astucieuse, je ne dis pas le contraire) pour influencer l'algorithme par lequel un résolveur BIND choisit le serveur d'une zone à qui il va parler pour résoudre les noms dans cette zone. (Notez que ce n'est donc pas une vulnérabilité DNS mais une - faible - vulnérabilité BIND.)

Lorsque cette attaque est en cours, l'attaquant peut donc forcer l'usage d'un serveur faisant autorité, parmi tous ceux de la zone. Cela diminue un tout petit peu le nombre de paramètres qu'un attaquant qui tente un empoisonnement doit deviner. Pourquoi « un tout petit peu » ? Parce qu'un attaquant doit deviner bien d'autres paramètres (RFC 5452 [1] pour les détails). Et celui-ci, le serveur interrogé, est un des moins importants, la grande majorité des zones (comme `linuxfr.org` cité plus haut), n'ont que deux serveurs faisant autorité ! L'attaque, même quand elle réussit complètement, ne fait donc gagner qu'un seul bit d'entropie à l'attaquant... J'emprunte donc une conclusion à Dan Kaminsky « "*While a neat trick, the recent DNS security research by the Technion students is in no way a critical vulnerability in BIND.*" »

Un résumé de l'attaque et de ses conséquences pour BIND avait été fait par l'ISC <https://kb.isc.org/article/AA-01030> (et réitérée après la nouvelle vague de buzz <https://lists.isc.org/pipermail/bind-users/2014-May/093141.html>). Par contre, la correction promise n'a pas encore été apportée. Une bonne réfutation avait été écrite l'année dernière par Tony Finch <http://fanf.livejournal.com/127748.html> (et la relance marketing de cette année n'en a pas tenu compte.) Un des auteurs de l'article original a publiquement dénoncé le gonflage <http://roeehay.blogspot.co.il/2014/05/about-impact-of-bind-srtt-vulnerability.html>.

À noter que DNSSEC résout complètement ce problème : quel que soit le serveur interrogé, on peut vérifier la validité des données.

Merci à X_cli <https://twitter.com/X_Cli> pour les tweets stimulants.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5452.txt