Utilité de DNSSEC contre un attaquant qui contrôle la clé privée de la racine

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 décembre 2013

https://www.bortzmeyer.org/dnssec-racine-nsa.html

Aujourd'hui, petit exercice intellectuel avec du DNS, de la cryptographie et de la sécurité. Si un attaquant peut injecter des fausses réponses DNS et le faire accepter par un résolveur, il peut **empoisonner** ce résolveur. DNSSEC protège contre cette attaque. Mais DNSSEC, comme le DNS, est arborescent. Si l'attaquant contrôle d'une façon ou d'une autre la racine, tout DNSSEC s'écroule-t-il ?

Cet exercice provident d'un article de Bruce Schneier <https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html> où il décrit un des programmes d'espionnage de la NSA, QUANTUM. L'attention du public, suite aux révélations d'Edward Snowden, s'est surtout focalisée sur les attaques **passives** de la NSA, comme la copie des données stockées dans les grands silos états-uniens (programme PRISM). Mais QUANTUM est, lui, un programme d'attaque **active**. La NSA peut aussi injecter des paquets dans le réseau, afin de faciliter un espionnage passif ultérieur. Schneier ne parle pas du tout du DNS dans son article. Mais on peut néanmoins supposer que, parmi ces attaques actives de la NSA (ou d'autres attaquants), certaines vont consister à utiliser le DNS pour empoisonner les résolveurs, détournant les utilisateurs vers des copies des sites à visiter. Ce mécanisme (sur lequel, rappelez-vous, nous n'avons pas de preuve dans les documents Snowden), a été décrit dans un excellent article <http://www.wired.com/opinion/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-> d'un expert DNS, Nicholas Weaver. Weaver dit « "*Since every communication starts with a DNS request, and it is only a rare DNS resolver that cryptographically validates the reply with DNSSEC, a packet injector can simply see the DNS request and inject its own reply. This represents a capability upgrade, turning a man-on-the-side into a man-in-the-middle.*" ».

Weaver mentionne DNSSEC comme une solution possible contre cette attaque. (Si vous ne connaissez pas DNSSEC, vous pouvez commencer par mon article à JRES <https://www.bortzmeyer.org/jres-dnssec-2009.html>.) Seulement, si l'attaquant est la NSA, il faut supposer qu'il peut signer des données quelconques avec la clé privée de la racine, cette racine étant sous le contrôle exclusif des États-Unis. Notez que je dis « l'attaquant peut signer des données », pas « l'attaquant peut mettre la main sur la clé privée ». En effet, cette clé est dans un HSM dont elle ne peut jamais, sauf bogue ou porte dérobée dans le HSM, sortir. Mais peu importe : la NSA peut certainement accéder au système

de signature et faire signer ce qu'elle veut, pour injection ultérieure. La question est « est-ce réaliste techniquement ? » Accrochez-vous, la réponse peut être compliquée.

En théorie, oui, cette attaque va marcher et DNSSEC ne serait donc pas utile contre la NSA. En pratique, Nicholas Weaver est sceptique. Il fait remarquer qu'il faudrait que l'attaquant fabrique une chaîne complète. S'il veut faire une fausse signature pour `www.slate.com` (en supposant que ce domaine soit signé avec DNSSEC, ce qui n'est pas le cas aujourd'hui), il doit fabriquer un faux ensemble d'enregistrements NS pour `.com`, et que les machines ainsi désignées répondent aux autres requêtes pour `.com`, sinon l'attaque sera vite détectée. Ou alors faire un faux enregistrement NSEC pour convaincre le résolveur que `.com` n'est pas signé. Car le vrai `.com` l'est et cette information se retrouve très vite dans les caches de n'importe quel résolveur de la planète, rendant difficile l'empoisonnement. Pour empoisonner, il faut être rapide, avant que le résolveur ait pu apprendre qu'il y a un "*zone cut*" entre la racine et `.com`, et qu'il y a un DS pour `.com`.

Bien sûr, pour `.com`, il y a une autre solution, signer des données avec la clé privée de `.com` puisque son registre est également situé aux États-Unis et donc vulnérable aux demandes officielles. Mais si la NSA veut détourner `www.petrobras.com.br`, là, l'attaquant n'a pas cette possibilité et il doit donc bien fabriquer une chaîne entière, ou alors un faux NSEC.

Bref, on se retrouve dans un cas classique en sécurité : il y a bien une faiblesse, mais son exploitation effective n'est pas forcément de la tarte. Bien sûr, ce qui précède n'est qu'un raisonnement théorique. Si vous êtes un programmeur courageux, il serait intéressant d'essayer de réaliser cette attaque en laboratoire et de documenter le résultat.

D'autres points à garder en tête :

— En pratique, il y a aujourd'hui trop peu de résolveurs validant avec DNSSEC. Donc, si j'étais la NSA, je ne m'embêterais pas immédiatement.
— Les empoisonnements de résolveurs peuvent se détecter. Certes, les gérants des résolveurs sont parfois incompétents, négligents ou débordés de travail. Mais il suffirait d'**un** gérant de résolveur qui, au bout moment, fasse un dig pour examiner son propre cache, découvre les données mensongères mais signées et les publie. N'importe qui pourrait vérifier que la clé privée de la racine n'est plus digne de confiance et tout DNSSEC, pour lequel le gouvernement des États-Unis a beaucoup investi, s'écroulerait.
— Si on n'a pas confiance dans la racine, une possibilité est de configurer son résolveur DNSSEC avec d'autres clés de confiance pour les zones situées plus bas. Par exemple, celles de `.fr` sont publiées `<https://www.afnic.fr/fr/certificats/>`. Mais **attention** : les conséquences en terme d'administration du résolveur sont sérieuses car il faut modifier ces clés de confiance lorsque le gérant de la zone ainsi protégée les change.
— Si on a confiance dans les clés de zones gérées en dehors des États-Unis, il faut aussi se demander si ces clés sont correctement protégées contre des attaques techniques ou légales.

`https://www.bortzmeyer.org/dnssec-racine-nsa.html`