RFC 7646 : Definition and Use of DNSSEC Negative Trust Anchors

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2015

Date de publication du RFC : Septembre 2015

https://www.bortzmeyer.org/7646.html

Comme toutes les techniques de sécurité, DNSSEC, qui vise à assurer l'authenticité des réponses DNS, a ses inconvénients. De même qu'une serrure fermée à clé peut avoir pour conséquence de vous empêcher de rentrer chez vous, si vous avez oublié la clé, de même DNSSEC peut empêcher d'accéder à un domaine si le gérant de la zone a commis une erreur technique. Autant le DNS d'avant était très tolérant (il fallait vraiment insister pour « planter » une zone), autant DNSSEC est délicat : les erreurs ne pardonnent pas, puisque le but de DNSSEC est justement d'empêcher l'accès aux données si elles sont suspectes. Mais les outils et les compétences pour gérer DNSSEC ne sont pas encore parfaitement au point et ne sont pas utilisés partout. Il y a donc de temps en temps des plantages, qui ont pour conséquence la panne d'une zone DNS entière. Face à ce problème, les gérants des résolveurs DNS validants aimeraient bien temporairement suspendre les vérifications, après avoir vérifié qu'il s'agissait bien d'un problème et pas d'une attaque. Cette suspension temporaire et limitée se nomme NTA pour "*Negative Trust Anchor*" et est décrite dans ce RFC.

DNSSEC est normalisé dans les RFC 4033 [1], RFC 4034 et RFC 4035. Il permet de valider des enregistrements DNS en les signant. Plusieurs points peuvent invalider accidentellement la signature. Par exemple, les signatures ont une durée de validité limitée (pour éviter les attaques par rejeu) : si le dispositif de re-signature périodique a une panne, les signatures expirent et la zone devient invalide. Ce genre de problèmes a été très fréquent au début du déploiement de DNSSEC <http://ianix.com/pub/dnssec-outages.html> et n'a pas complètement disparu. Lorsque cela frappe un domaine important, cela se remarque <http://www.darkreading.com/risk/dnssec-error-caused-nasa-website-to-be-bd/d-id/1136990>. (Rappel : toutes les techniques de sécurité ont ce genre de problème. Qu'on pense par exemple aux innombrables expirations de certificats X.509 <https://www.bortzmeyer.org/tester-expiration-certifs.html>.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4033.txt

Mettez-vous deux secondes à la place du responsable des serveurs DNS récursifs (les **résolveurs**) d'un gros FAI, ayant beaucoup de clients. Comcast, par exemple, puisque cette entreprise a beaucoup plaidé en faveur de ce nouveau RFC. L'administrateur d'un domaine important, mettons `nasa.gov`, a cafouillé, la zone est invalide. Mais seuls les résolveurs validants (ceux qui protègent leurs utilisateurs avec DNSSEC) voient cela. Les autres, les anciens résolveurs non sécurisés, ne testent pas DNSSEC et la zone, pour eux, marche normalement. Les utilisateurs des FAI qui n'ont pas déployé DNSSEC pourront donc accéder aux ressources de la zone en panne, mais pas les vôtres. Ils téléphonent au support en masse, et, sur les réseaux sociaux, disent « Comcast a bloqué l'accès à `nasa.gov` » (oui, c'est un cas réel <`http://www.internetsociety.org/deploy360/blog/2012/01/comcast-releases-detailed-analy`> et qui a été souvent mal présenté dans les forums publics <`https://disqus.com/home/discussion/nasawatch/comcast_blocks_customer_access_to_nasagov/`>). Le résultat de cette mauvaise interprétation par les utilisateurs risque d'être un recul de DNSSEC : les gérants de résolveurs DNS pourraient se dire « si les mesures de sécurité embêtent les utilisateurs, coupons les mesures de sécurité ».

La « solution » proposée dans ce RFC, la NTA ("*Negative Trust Anchor*", ou « débrayage explicite de la validation ») est une option de configuration du résolveur qui dit « ne valide pas ces domaines, je sais qu'ils sont cassés, ce n'est pas une attaque ». Chaque gérant de résolveur devra donc prendre la décision unilatérale de configurer ou pas ces NTA. Il n'est pas prévu de protocole pour les distribuer. Les NTA sont un comportement, pas un objet sur le réseau. Il n'y a pas, par exemple, d'enregistrement DNS `NTA`.

Au passage, s'il y a des "*negative trust anchor*", c'est qu'il en existe des "*positive*", non ? Le concept de « point de départ de la confiance » ("*trust anchor*") est décrit dans le RFC 5914. Le résolveur validant vérifie une zone à partir de sa parente, la parente à partir de la grand-parente et... Il faut bien un endroit où ancrer la vérification : c'est la "*trust anchor*", en général la clé de la racine du DNS, qui sert récursivement à valider toutes les autres. Au contraire, la NTA arrête la validation et dit « tout ce qui est en dessous n'est pas vérifié ».

La section 1.2 de notre RFC décrit plus en détail les motivations pour le concept de NTA. En effet, l'idée de base est surprenante : on dépense beaucoup d'efforts et d'argent pour déployer DNSSEC, afin de vérifier les données DNS, puis on fournit un mécanisme qui permet de débrayer la validation. L'idée a en effet suscité beaucoup de remous à l'IETF et de longues discussions. Comme souvent, le débat opposait, non pas tant les pro contre les anti, que ceux qui disaient « cela existe dans la nature, il vaut mieux le documenter » à ceux qui affirmaient « en le documentant, on le légitimise ». Les premiers l'ont finalement emporté, d'où ce RFC 7646. Les raisons sont documentées dans cette section 1.2.

Aujourd'hui, où bien des administrateurs système sont encore débutants en DNSSEC, la majorité des problèmes de validation sont dus à des erreurs de l'administrateur, pas à une vraie attaque (notez que c'est sans doute également le cas en HTTPS...) Bien sûr, les administrateurs en question devraient lire le RFC 6781, et notamment sa section 4.2. Ils éviteraient ainsi bien des malheurs. Mais, en attendant, il est pratique d'avoir un moyen pour ignorer leurs erreurs. C'est l'un des buts des NTA.

Deuxième motivation, le problème de l'utilisateur. Le DNS est une technologie d'infrastructure. Il n'est pas visible à l'utilisateur final et les problèmes au niveau DNS ne peuvent donc pas être analysés par M. Toutlemonde. C'est délibéré : tout le rôle du DNS est justement d'isoler ce M. Toutlemonde de détails pratiques, comme le fait que `seenthis.net` a changé d'adresse IP. Il est donc cohérent avec ce rôle que l'utilisateur final ne soit pas informé qu'il y a un problème DNSSEC. Il ne peut donc pas savoir ce qui l'empêche d'aller sur son site Web favori et, dans son ignorance, il risque de ne pas attribuer les responsabilités correctement. Comme dans l'exemple plus haut, il pourrait dire « c'est la faute de mon FAI » au lieu de pointer du doigt, à juste titre, l'administrateur de la zone mal signée. Comme dans l'exemple Comcast/NASA cité plus haut, si un domaine important est signé, et fait une erreur déclenchant un problème DNSSEC, on risque de voir vite apparaitre des gazouillis désobligeants contre

le FAI, qui n'y est pourtant pour rien. Cela risque de mener la direction du FAI à ordonner qu'on arrête de valider avec DNSSEC. « Le bruit de l'alarme dérange les utilisateurs : coupez l'alarme. » Mettre une NTA pour le domaine critique en question serait certes un recul de la sécurité, mais qui pourrait éviter des reculs encore pires. (C'est compliqué, la politique de sécurité.)

Cette décision stupide pourrait aussi être prise par l'utilisateur, qui passerait d'un résolveur validant à un résolveur non validant. Sur les réseaux sociaux, les conseils idiots se propagent plus vite que les bons, surtout en matière de sécurité « zyva, mets `192.0.2.1` comme résolveur et ça va marcher ». La NTA vise à ralentir cette fuite.

La section 2 de notre RFC décrit la bonne façon d'utiliser les NTA. D'abord, avant d'installer une "*Negative Trust Anchor*", il faut une vérification **manuelle**, faite par un technicien compétent, de la situation (cf. section 7 sur les tests techniques). Est-ce bien une erreur de la part du gestionnaire de la zone ? On peut s'en assurer en testant la zone depuis différents points (en comptant qu'ils n'ont probablement pas tous été victimes d'une attaque par empoisonnement en même temps) ou tout simplement en prenant connaissance d'une annonce officielle du gestionnaire de la zone, s'il y en a une. Prendre contact avec le gestionnaire de la zone permettra aussi de s'assurer que le problème est bien involontaire (cf. section 6). En tout cas, il ne faut **pas** installer aveuglément une NTA à chaque fois qu'une validation DNSSEC échoue : cela annulerait complètement l'intérêt de DNSSEC. D'accord, une telle vérification par un humain coûte cher mais il n'y a pas non plus de problème de ce genre tous les mois, ou même tous les trimestres.

Lors de la discussion avec le gérant de la zone, l'administrateur du résolveur qui hésite à installer une NTA peut communiquer à son interlocuteur les enregistrements DNS qu'il voit (obtenus avec `dig +cd`, pour ignorer la validation), afin de pouvoir s'assurer que ces enregistrements sont bons, qu'il ne s'agit pas d'une attaque. Bien sûr, il faut être pragmatique : si un gros TLD a planté son DNSSEC, rendant ainsi de nombreuses zones invalides, et que ses employés ne répondent pas, il peut être raisonnable de placer unilatéralement la NTA, compte-tenu de l'urgence.

Les NTA sont censées être une mesure sale et temporaire. Il est donc important de faire en sorte qu'elles ne restent pas éternellement, par exemple en indiquant clairement la date <`https://www.bortzmeyer.org/mettre-date-fichiers-config.html`> dans le fichier de configuration ou dans le journal.

Comme la NTA est une action « anormale » (on ignore une alerte de sécurité), le RFC recommande d'informer clairement les utilisateurs du résolveur comme l'a fait Comcast <`http://dns.comcast.net/index.php/entry/faa-gov-failing-dnssec-validation-fixed`>. C'est d'autant plus important que les utilisateurs n'ont pas d'autre moyen de savoir qu'une NTA est en place (le protocole DNS ne fournit pas de mécanisme pour cela).

Mettre une NTA, c'est facile. Mais il ne faut pas la laisser éternellement, sinon cette zone n'est plus protégée par DNSSEC ! Le RFC demande donc (section 4) que les NTA soient, par défaut, supprimées automatiquement, par exemple au bout d'une semaine (si c'est vraiment une panne, elle ne dure jamais plus longtemps que quelques jours). Idéalement, il faudrait tester régulièrement la validité du domaine, et retirer la NTA s'il redevient valide. À cause de ces recommandations, une gestion entièrement manuelle des NTA, comme dans l'exemple ci-dessous avec la directive `domain-insecure:` d'Unbound, n'est pas forcément à recommander.

Et, évidemment, une fois la NTA retirée, il faut vider les caches DNS <`https://www.bortzmeyer.org/vider-cache-resolveur.html`> pour la zone.

La NTA revient à prendre une décision sur la gestion d'une zone alors qu'on n'est pas le gérant de la zone. Cela doit donc rester exceptionnel. Le problème, et la solution décrite dans ce RFC, sont très spécifiques à DNSSEC, ou plus exactement à son état actuel. La section 5 de notre RFC dit clairement qu'il ne **faut pas** envisager de telles solutions pour d'autres problèmes. Si un gérant de zone maladroit a mis le mauvais MX dans la zone, il ne faut pas « corriger » dans les résolveurs. Le principe du DNS doit rester que le gérant de la zone fait autorité sur le contenu de la zone.

Certaines zones, comme `servfail.nl` cité plus loin dans un exemple, ou comme `dnssec-failed.org` sont cassées exprès. Leur but est de permettre de tester les outils de diagnostic ou de mesurer le nombre de validateurs <http://jpmens.net/2012/07/30/is-my-web-site-being-used-via-dnssec-validato>. Cette mesure se fait typiquement en incluant dans une page Web un objet (une image, par exemple) accessible via un nom de domaine ainsi invalide. Si le chargement de l'objet se fait, c'est que le navigateur Web n'utilisait pas de résolveur validant.

Il ne faut évidemment pas mettre de NTA sur ces domaines volontairement invalides (section 6 de notre RFC). J'utilise `servfail.nl` ci-dessous mais c'est juste un exemple.

On a dit plus haut qu'une NTA ne devait être ajouté qu'après qu'un technicien DNS ait évalué l'état de la zone et déterminé que c'était bien un accident. Pour l'aider à faire cette évaluation, il existe plusieurs outils. Par exemple, l'histoire compte : si l'enregistrement de type AAAA de `example.net` est invalide, mais qu'il vaut `2001:db8:67::ab` et qu'il a cette valeur depuis deux ans, on peut être raisonnablement sûr que c'était une erreur DNSSEC et pas une attaque. Comment sait-on que la valeur n'a pas changé depuis deux ans ? On peut utiliser une base de *"passive DNS"* comme DNSDB <https://www.bortzmeyer.org/dnsdb.html>. Un autre outil historique important est DNSviz <http://dnsviz.net/>, qui stocke le résultat des tests DNSSEC précédents (un domaine populaire a forcément été testé plusieurs fois).

Notre RFC liste plusieurs outils de débogage qui permettent d'analyser l'état actuel de la zone :

— DNSviz <http://dnsviz.net/>, déjà mentionné, qui a l'avantage de produire une jolie représentation graphique des relations entre clés et signatures.
— ZoneMaster <https://www.zonemaster.fr/> (« *"Who you gonna call ? ZoneMaster !"* ») de l'AFNIC et d'IIS.
— DNSSEC debugger <http://dnssec-debugger.verisignlabs.com/> de Verisign.

Les deux premiers sont des logiciels libres et peuvent être installés localement sur votre machine. (Une analyse du cas de `nasa.gov` a été faite avec ces outils <http://ianix.com/pub/dnssec-outages/20150814-nasa.gov/>.)

En effet, dans certains cas, le résultat peut dépendre de l'endroit où vous vous trouvez. Par exemple, certaines instances d'un nuage anycast peuvent servir des signatures expirées et d'autres pas. Il est donc utile d'avoir accès à des résolveurs DNSSEC distants. On peut utiliser les sondes Atlas <https://atlas.ripe.net>, ou se connecter à des serveurs distants pour y lancer dig. Si tous les résolveurs validants de la planète voient `SERVFAIL`, il est beaucoup plus probable qu'on soit confronté à une erreur dans la gestion de la zone qu'à une attaque par empoisonnement.

Le RFC liste aussi, dans cette section 7, les causes les plus fréquentes de problème DNSSEC aujourd'hui :

— Signatures expirées. Les clés DNSSEC n'ont pas de durée de validité mais les signatures, si (elle vaut en général de deux à huit semaines). Avant DNSSEC, une fois qu'une zone DNS était configurée et testée, elle restait correcte plus ou moins éternellement. Depuis DNSSEC, il faut re-signer la zone régulièrement puisque les signatures expirent, **même si on n'a pas changé le contenu de la zone**. Cette tâche doit évidemment être automatisée (par exemple, OpenDNSSEC ou BIND peuvent le faire sans intervention humaine) mais les logiciels ont des bogues. Si le programme de re-signature ne marche plus, les signatures vont expirer. Au début, c'était quasiment la seule cause de problème DNSSEC, menant au dicton « on peut déboguer DNSSEC avec deux commandes Unix, `dig` et `date` ». Aujourd'hui que les outils automatiques sont bien plus fréquents, cette erreur est plus rare.

— Les autres causes de problème sont toutes liées à la chaîne de confiance, qui part en général de la racine et qui, via des signatures de zone parente en zone fille, permet de valider toute information stockée dans le DNS. Si cette chaîne casse (par exemple un enregistrement DS qui pointe vers une clé inexistante), la zone est invalide. Ici, DNSviz est vraiment l'outil idéal, grâce à la représentation graphique qu'il fait de cette chaîne de confiance. La chaîne de confiance peut être cassée à la suite d'une erreur en transmettant la clé à la zone parente, ou par suite d'un changement ultérieur de clés ("*key rollover*") en oubliant de prévenir la parente.

Enfin, la section 8 de notre RFC couvre plusieurs points de sécurité qui n'étaient pas évidents. Politiquement, la NTA est une prise du pouvoir par le résolveur, qui se permet de contrarier les résultats. C'est un mal nécessaire mais, quand même, il faut être conscient de ce décalage des responsabilités. D'où l'importance d'informer le gérant de la zone signée et de discuter avec lui/elle.

Autre problème, la NTA transforme une zone signée en zone non signée. Cela évite les erreurs de validation mais cela pose un problème pour toutes les applications qui vérifient que le contenu des données est valide (par exemple lorsqu'on lit des clés cryptographiques dans le DNS). Cette vérification se fait typiquement en regardant le bit AD ("*Authentic Data*") dans la réponse DNS. S'il est absent, c'est que la zone n'est pas signée, et les applications risquent alors d'ignorer les informations qu'elles ont trouvées dans le DNS, faute de validation positive. C'est par exemple un problème pour DANE (RFC 6698) : si une NTA est placée, les certificats mis par DANE seront tout à coup ignorés, ce qui pourra couper l'accès à certains serveurs TLS. Le RFC estime que les applications feront de plus en plus leur propre validation, ce qui diminuera le problème, mais ce pronostic me parait très contestable.

L'annexe A du RFC contient plein d'exemples de gestion des NTA sur différents logiciels. Je vais commencer par une méthode non décrite dans le RFC, avec Unbound. Voyons d'abord un domaine invalide avec une requête normale :

```
% dig A www.servfail.nl

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> A www.servfail.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 26269
...
```

On récupère un `SERVFAIL` ("*Server Failure*") ce qui est normal puisque ce domaine est (délibérement) invalide. Essayons avec l'option `+cd` ("*Checking Disabled*") qui indique au résolveur de ne **pas** valider :

```
% dig +cd A www.servfail.nl

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> +cd A www.servfail.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53947
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.servfail.nl.       IN A

;; ANSWER SECTION:
www.servfail.nl.        60 IN CNAME www.forfun.net.
...
```

Maintenant, modifions la configuration d'Unbound en ajoutant dans le `unbound.conf` la "*Negative Trust Anchor*" :

```
# Added on 2015-09-22, after confirmation from <foobar@forfun.net>
domain-insecure: "servfail.nl"
```

Notez l'importance de mettre la date dans le fichier de configuration : les NTA ne doivent **pas** être permanentes. On recharge la configuration :

```
% sudo unbound-control reload
ok
```

Et on réessaie :

```
% dig A www.servfail.nl

; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> A www.servfail.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62157
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 4, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.servfail.nl.       IN A

;; ANSWER SECTION:
www.servfail.nl.        60 IN CNAME www.forfun.net.
```

Notez qu'on a eu la réponse mais que le bit AD ("*Authentic Data*") n'est évidemment pas mis, comme discuté en section 8 du RFC.

Cette méthode a l'inconvénient d'être un peu trop manuelle et de ne pas être automatiquement réversible. À noter que l'annexe A du RFC cite également une méthode qui ne nécessite pas de changer le fichier de configuration, mais utilise l'outil de contrôle à distance d'Unbound (qu'il faut configurer préalablement) :

```
[Quels NTA sont installées ? ]
% sudo unbound-control list_insecure
%
[Aucun]

[On installe une NTA]
% sudo unbound-control insecure_add servfail.nl
ok
% sudo unbound-control list_insecure
servfail.nl.

% dig A www.servfail.nl
...
www.servfail.nl.        60 IN CNAME www.forfun.net.
...

[On retire la NTA]
% sudo unbound-control insecure_remove servfail.nl
ok
% sudo unbound-control list_insecure
%
```

BIND n'a pas d'équivalent de la directive `domain-insecure:`. C'est une de ses faiblesses. Mais il permet, à partir des récentes versions (non encore publiques, apparemment réservées aux clients payants), d'avoir des NTA plus conformes à ce que demande le RFC, notamment avec retrait automatique au bout d'un temps donné. Je n'ai pas testé donc voici les commandes que donne le RFC :

```
[Quels NTA sont installées ? ]
% sudo rndc nta -dump

[On installe une NTA pour une heure - la valeur par défaut]
% sudo rndc nta servfail.nl

[On retire explicitement la NTA (sinon, il est retiré automatiquement)]
% sudo rndc nta -remove servfail.nl
```