RFC 8027 : DNSSEC Roadblock Avoidance

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 décembre 2016

Date de publication du RFC : Novembre 2016

https://www.bortzmeyer.org/8027.html

Normalement, en 2016, tous les résolveurs DNS sérieux devraient valider avec DNSSEC. Mais ce n'est pas le cas. Il y a plusieurs raisons à cela, mais ce nouveau RFC se focalise sur un problème précis : le cas d'un résolveur connecté via un réseau pourri, non-neutre, et qui se permet d'interférer avec le transport des paquets IP, menant le résolveur à de sérieuses difficultés. Comment détecter ces réseaux pourris ? Et que faire pour valider quand même ?

Si le résolveur est une grosse machine dans un centre de données, connectée directement à des opérateurs neutres, il n'y a pas trop de problème. C'est le cas des résolveurs des FAI, par exemple. Mais la situation est bien moins favorable à M. Michu. Si celui-ci veut, à juste titre <https://www.bortzmeyer.org/son-propre-resolveur-dns.html>, avoir son propre résolveur DNS sur sa machine, il dépend des réseaux où on laisse M. Michu se connecter, et ceux-ci sont rarement neutres. (Le RFC couvre le cas où ce résolveur local fait suivre - "*forwarde*" - les requêtes à un autre résolveur, et celui où il parle directement aux serveurs faisant autorité.)

La section 1.2 du RFC décrit les cas où la validation DNSSEC va être difficile ou impossible :

— Résolveur qui ne connait pas DNSSEC (évidemment),
— Intermédiaires (relais DNS dans la "*box*", par exemmple), qui viole le protocole DNS au point de gêner le fonctionnement de DNSSEC (ce cas est décrit en détail dans le RFC 5625 [1]),
— Équipements réseau actifs qui modifient ou bloquent les messages DNS, par exemple en supprimant les signatures DNSSEC (beaucoup de « "*firewalls*" » sont dans ce cas),
— Réseau qui ne gère pas correctement les fragments, ce qui est plus fréquent avec DNSSEC.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5625.txt

Bien des outils ont été développés pour contourner ces problèmes, comme dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html>.

Pour faire des tests des résolveurs et de tous les équipements intermédiaires qui peuvent poser des problèmes de validation DNSSEC dans certains cas, le RFC parle d'une zone de test nommée `test.example.com`. Elle n'existe pas en vrai mais, aujourd'hui, la zone `test.dnssec-tools.org` fait la même chose (elle est par exemple utilisée pour les travaux pratiques lors de la formation DNSSEC chez HSC <http://www.hsc-formation.fr/formations/dnssec.html.fr>). Cette zone est délibérement peuplée avec des noms mal signés. Ainsi, le nom `badsign-aaaa.test.dnssec-tools.org` a un enregistrement AAAA dont la signature a été modifiée, la rendant invalide. Testons (pour tous les tests, comme le but était de voir le comportement DNSSEC, j'ai utilisé un fichier de configuration `/.digrc` contenant `+dnssec +multiline`, merci à Landry Minoza de l'avoir remarqué) :

```
% dig AAAA badsign-aaaa.test.dnssec-tools.org
; <<>> DiG 9.9.5-9+deb8u8-Debian <<>> AAAA badsign-aaaa.test.dnssec-tools.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 60910
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;badsign-aaaa.test.dnssec-tools.org. IN AAAA

;; Query time: 3759 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Dec 04 17:12:28 CET 2016
;; MSG SIZE  rcvd: 63


% dig +cd AAAA badsign-aaaa.test.dnssec-tools.org
; <<>> DiG 9.9.5-9+deb8u8-Debian <<>> +cd AAAA badsign-aaaa.test.dnssec-tools.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29404
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;badsign-aaaa.test.dnssec-tools.org. IN AAAA

;; ANSWER SECTION:
badsign-aaaa.test.dnssec-tools.org. 86400 IN AAAA 2001:470:1f00:ffff::1
badsign-aaaa.test.dnssec-tools.org. 86400 IN RRSIG AAAA 5 4 86400 (
20170101064820 20161202054820 19442 test.dnssec-tools.org.
nZ8bPLBleW/sW6x135+Iz4IhO6Lr04V8C9fC1bMVfCVY
3rKqbOoBk1i+wnnGDCTWQ5iCicWTKLIpbDmCSW9C33pj
P2j7C/ensspbdwpD/7Ia8zN+XUSN+ThLU6lgYGKFuoVL
QmIG/vr1lOn6xdjXY2E4mStAjaGuertvKKDYy/I= )

;; AUTHORITY SECTION:
test.dnssec-tools.org. 280 IN NS dns1.test.dnssec-tools.org.
test.dnssec-tools.org. 280 IN NS dns2.test.dnssec-tools.org.
test.dnssec-tools.org. 280 IN RRSIG NS 5 3 86400 (
20170101064820 20161202054820 19442 test.dnssec-tools.org.
AK95JOAuvfZ1ZwEsrKiR8DP1zluoBvBkXHRXa78rrK5U
UuZdLnZwnYlnNplrZZOrQNuUaPyb4zI0TGfw/+aa/ZTU
qyx8uQODSHuBTPQTlcmCFAfTIyd1Q+tSTEs2TuGUhjKe
H9Hk+w6yOjI/o52c2OcTMTJ4Jmt2GlIssrrDlxY= )

;; ADDITIONAL SECTION:
dns1.test.dnssec-tools.org. 280 IN A 168.150.236.43
```

```
dns2.test.dnssec-tools.org. 280 IN A 75.101.48.145
dns1.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 (
20170101064820 20161202054820 19442 test.dnssec-tools.org.
zoa0V/Hwa4QM0spG6RlhGM6hK3rQVALpDve1rtF6NvUS
Sb6/HBzQOP6YXTFQMzPEFUza8/tchYp5eQaPBf2AqsBl
i4TqSjkIEklHohUmdhK7xcfFjHILUMcT/5AXkEStJg7I
6AqZE1ibcOh7Mfmt/2f0vj2opIkz6uK740W7qjg= )
dns2.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 (
20170101064820 20161202054820 19442 test.dnssec-tools.org.
hGq7iAtbHrtjCYJGMPQ3fxijhu4Izk8Ly+xZOa0Ag24R
lqpFgdd2amDstFVLTRs3x15UqQIO+hmFdlbSOterDkbg
/o2/FhtZOJr7c75Pu3EWi/DDbT9pULk4Uwjlie1QBopv
LLZ94SlqKO7eQ02NRyy5EL4gD2G5rSffsUqEkj8= )

;; Query time: 206 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Dec 04 17:12:44 CET 2016
;; MSG SIZE  rcvd: 885
```

Le second test, celui fait avec le bit CD ("*Checking Disabled*"), montre que le problème vient bien de DNSSEC. Autre test, avec une signature expirée :

```
% dig A pastdate-a.test.dnssec-tools.org
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 46319
...


% dig +cd A pastdate-a.test.dnssec-tools.org
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49547
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5
...
;; ANSWER SECTION:
pastdate-a.test.dnssec-tools.org. 86400 IN A 64.90.35.104
pastdate-a.test.dnssec-tools.org. 86400 IN RRSIG A 5 4 86400 (
20161201224321 20161101234821 19442 test.dnssec-tools.org.
lIL0zcEZpG/4uG5hImvpivH1C/D3PFI3RNYHlPbZ [...]
```

La liste de tous les noms à tester est en ligne <https://www.dnssec-tools.org/testzone/index.html>.

Le but de ce RFC est de lister tous les tests que peut et devrait faire un validateur local, pour arriver à valider malgré des résolveurs amont, ou bien un réseau, hostile. Ces stratégies sont mises en œuvre, par exemple, dans dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html>.

En détectant la non-conformité ("*compliance*", un terme à la mode dans les organisations), le validateur situé sur la machine terminale, ou bien dans le réseau local, peut alors adopter la meilleure stratégie de contournement (ou, dans le pire des cas, prévenir loyalement l'utilisateur qu'on ne pourra pas faire de validation DNSSEC). Les tests doivent être faits au début d'une nouvelle connexion réseau, ou bien lorsque celle-ci change.

La section 3 du RFC est consacrée à ces tests de non-conformité. Je ne vais pas décrire la totalité de ces tests, un sous-ensemble suffira. Ainsi, le premier test, le plus trivial, est que la machine puisse parler en

UDP à son résolveur attitré (celui typiquement reçu en DHCP). On lui demande `good-a.test.dnssec-tools.org` et on doit avoir une réponse sous forme d'une adresse IP (comme son nom l'indique, ce nom est correctement signé). Si un test aussi trivial ne marche pas, ce n'est sans doute pas la peine d'aller plus loin. Un peu plus subtil, on teste le même résolveur en TCP.

Après, on passe à EDNS (RFC 6891), qui est indispensable pour DNSSEC. Une requête pour ce même nom, mais avec une option EDNS, doit passer. Si EDNS ne marche pas, on peut arrêter, DNSSEC ne marchera pas non plus. Mais s'il marche ? On teste alors avec le bit DO ("*DNSSEC OK*") qui indique au serveur qu'il doit envoyer les données DNSSEC, notamment les signatures. La réponse doit inclure ce même bit DO. (C'est plus tard qu'on teste qu'on a bien reçu des signatures. Rappelez-vous que la plupart des "*middleboxes*" sont horriblement boguées. Certaines acceptent le bit DO et le renvoient, sans pour autant transmettre les signatures.)

On teste alors des zones qu'on sait signées et on regarde si le résolveur met le bit AD ("*Authentic Data*"), au moins pour les algoritmes RSA + SHA-1 et RSA + SHA-256. Si cela ne marche pas, ce n'est pas forcément une erreur fatale, puisque, de toute façon, on voulait faire la validation nous-même. Il faut aussi penser à faire le test inverse : un résolveur validant doit mettre le bit AD pour une réponse signée correctement, et doit répondre avec le code de retour SERVFAIL ("*Server Failure*") si la réponse devrait être signée mais ne l'est pas, ou bien l'est mal. Cela se fait en testant `badsign-a.test.dnssec-tools.org`.

Dans les enregistrements DNSSEC, il n'y a pas que les signatures (RRSIG), il y a aussi les enregistrements servant à prouver la non-existence, NSEC et NSEC3. Il faut donc également tester qu'ils sont reçus car, en pratique, on voit en effet des "*middleboxes*" qui laissent passer les RRSIG mais bloquent stupidement les NSEC et les NSEC3. On demande donc `non-existent.test.dnsssec-tools.org`, et on doit récupérer non seulement une réponse avec le code NXDOMAIN ("*No Such Domain*") mais également les NSEC ou NSEC3 permettant de valider cette réponse :

```
% dig AAAA non-existent.test.dnsssec-tools.org
[...]
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 40218
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1
[...]
;; AUTHORITY SECTION:
h9p7u7tr2u91d0v0ljs9l1gidnp90u3h.org. 900 IN NSEC3 1 1 1 D399EAAB (
H9PARR669T6U8O1GSG9E1LMITK4DEM0T
NS SOA RRSIG DNSKEY NSEC3PARAM )
iruevfos0vs8jssfj22me5p458p0qj1e.org. 900 IN RRSIG NSEC3 7 2 86400 (
20161222153046 20161201143046 3947 org.
kgCZC/gE4ySP7eZUb1+2ORYRhTrvL5YBIHLCBK5F8pqK
MXGJXJ/hX+8LLrg4jHJaER2AelUgUGywRn4uY80ajYpg
eTuSGzRX1aVCKAR8UB80bX/YLUPUPKWOdfgxTekD4nZk
eoi/9JNmIMZRc0cmMGp8LSVMqX98F2bVJnZro8U= )
iruevfos0vs8jssfj22me5p458p0qj1e.org. 900 IN NSEC3 1 1 1 D399EAAB (
IRVVBMC65HCBCFQNQS8NQFTAB943LCFU
NS DS RRSIG )
vaittv1g2ies9s3920soaumh73klnhs5.org. 900 IN RRSIG NSEC3 7 2 86400 (
20161222153046 20161201143046 3947 org.
Nj/zvU0GB8vQ7bFfpSSWW+inE7RiOFjOpNc1K/TMnQqG
QsKTLD9gBM8vgh3K1WdPXOCzthf/isDJAy2xLA/oRFFq
KZ+Coo+33FManVmuyndGJ5bdgQqnpa0xGP7yOgjTfUsh
Ff9HkX0mkzqYtWYzw0J7WnMPcOjmrlg26WsfwlU= )
vaittv1g2ies9s3920soaumh73klnhs5.org. 900 IN NSEC3 1 1 1 D399EAAB (
VAJB898DELVT5UJ4I9D1BRD2FRTBSCM1
NS DS RRSIG )
```

Certains serveurs DNS (ou, plus exactement, certains ensembles serveur+réseau+"*middlebox*") n'acceptent que certains types d'enregistrement DNS (les plus connus, comme A, AAAA, MX, parfois SRV, etc). Il faut donc tester que le serveur accepte bien tous les types d'enregistrement,

Jusqu'à présent, on n'a testé que le résolveur « normal ». Même s'il ne valide pas, tant qu'il transmet fidèlement toutes les données DNS, on pourra au moins l'utiliser comme relais et cache. Par contre, dans certains cas, si on veut valider avec DNSSEC, il faudra complètement le court-circuiter. Ainsi, s'il ne transmet pas les signatures, on n'a pas d'autre choix que d'aller les demander à un autre résolveur, ou bien directement aux serveurs faisant autorité. Il faut donc tester qu'on puisse interroger ces serveurs, avec UDP et avec TCP. (Ce n'est pas toujours possible, certains réseaux violent tellement la neutralité de l'Internet <https://www.bortzmeyer.org/neutralite.html> qu'ils bloquent le port 53 <https://www.bortzmeyer.org/port53-filtre.html>, celui du DNS.)

Avec DNSSEC, les réponses sont souvent de grande taille, et parfois fragmentées. Il faut donc tester que les fragments passent (ils sont souvent bloqués par des administrateurs réseau incompétents).

Une fois ces tests faits, il reste à synthétiser les résultats (section 4). L'idée est de pouvoir dire si le résolveur « normal » est :

— Un validateur (on peut alors tout lui déléguer, en tout cas si on a confiance en lui),
— Un résolveur DNSSEC (même s'il ne valide pas, il passe bien tous les enregistrements DNSSEC),
— Une horreur à fuir.

En pratique, tous les résolveurs (ou plutôt l'ensemble du résolveur et du réseau situé devant, avec ses "*middleboxes*" qui cassent tout) ne rentrent pas parfaitement dans une de ces trois catégories. Ainsi, certains vont bloquer les fragments mais accepter TCP (ce qui permettra de quand même faire passer les données de grande taille), tandis que d'autres n'auront pas TCP mais qu'UDP fonctionnera bien, même en cas de fragmentation.

Une fois ces données collectées, et le résolveur correctement classé, on pourra alors déterminer comment contourner les éventuels problèmes (section 5 du RFC). Par exemple :

— Si le résolveur officiel est un validateur ou bien un résolveur DNSSEC, on l'utilise comme "*forwarder*" pour transmettre les requêtes, profitant ainsi de son cache et réduisant la charge sur les serveurs faisant autorité.
— Si le résolveur officiel est une horreur, mais que les requêtes DNS vers l'extérieur marchent, alors, ne pas faire appel au résolveur officiel et parler directement aux serveurs faisant autorité.
— Si le résolveur officiel est une horreur, et que les requêtes DNS vers l'extérieur sont bloquées, tenter de joindre un résolveur extérieur de confiance, en utilisant DNS sur TLS (RFC 7858), ce que fait dnssec-trigger <https://www.bortzmeyer.org/dnssec-trigger.html> (dans son fichier de configuration, des lignes comme `tcp80: 185.49.140.67` ou `ssl443: 185.49.140.67` ...).
— Sinon, si rien ne marche, laisser tomber, prévenir l'utilisateur et pleurer.

La section 6 du RFC sert de voiture-balai, en mentionnant les cas spéciaux qui peuvent être embêtants. Par exemple, DNSSEC dépend de l'horloge, puisqu'il faut vérifier que les signatures n'ont pas expiré. Mais la synchronisation de l'horloge dépend de NTP donc parfois du DNS si on a mis des noms de domaine dans son `ntp.conf`. Si la machine a une horloge assez stable pour garder l'heure entre un arrêt et un démarrage, ce n'est pas trop grave. Mais si la machine est un engin bon marché avec une horloge qui dévie beaucoup (genre le Raspberry Pi), que faire ?

Autre problème, les affreux portails captifs. Tant qu'on n'a pas cliqué sur « j'accepte cinquante pages de conditions d'utilisation que je n'ai pas lues, je veux recevoir du spam, et je promets de ne pas partager de la culture », on n'a pas un vrai accès Internet et le port 53 est sans doute bloqué. Il faudrait donc refaire les tests après le passage par le portail captif.

Face à ce genre de problèmes, une première solution est de ne pas tenter de faire du DNSSEC tant qu'on n'a pas synchronisé l'horloge, passé le portail captif (c'est ce que fait dnssec-trigger), au détriment de la sécurité. Au moins, on peut prévenir l'utilisateur et lui proposer de réessayer plus tard.