Un problème DNSSEC : pas assez de NSEC3

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2013

https://www.bortzmeyer.org/nsec3-insuffisant.html

C'est une banalité que de noter que DNSSEC est complexe. Heureusement, cette complexité est souvent cachée par les outils utilisés. Mais, parfois, elle resurgit lorsque quelque chose ne marche pas. C'est le cas à l'instant du tout nouveau TLD .[Caractère Unicode non montré [1]][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré], dont les enregistrements NSEC3 sont insuffisants.

.[Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré][Caractère Unicode non montré] s'écrit en Punycode xn--80asehdb. Comme tous les nouveaux TLD, il est signé avec DNSSEC. Interrogeons un résolveur DNS qui valide avec DNSSEC, un du ODVR <https://www.dns-oarc.net/oarc/services/odvr> :

```
% dig @149.20.64.20   SOA xn--80asehdb

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @149.20.64.20 SOA xn--80asehdb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44970
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;xn--80asehdb. IN SOA

;; ANSWER SECTION:
xn--80asehdb. 84319 IN SOA anycast10.irondns.net. secretariat.corenic.org. (
1310231925 ; serial
21600      ; refresh (6 hours)
```

1. Car trop difficile à faire afficher par LaTeX

```
3600       ; retry (1 hour)
604800     ; expire (1 week)
86400      ; minimum (1 day)
)
xn--80asehdb. 84319 IN RRSIG SOA 10 1 86400 20131106172547 (
20131023172547 38327 xn--80asehdb.
ZUg0BUeRcEyTuyUmhcUC95U/iSd8/6GQS1D7k8YnADJa
QV1nBPJ+9EOW7ycMKtg0XokKl+i8SqlCLqOs2mUs6nFg
p9jB/T1sUar/w1QAjtClM9JcIliXC7AdDi4bmg5G15yX
rgkrdgXrm/8kyUEbMUlto6LNdBz/IYP5fS4hlvo= )
...
;; Query time: 215 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Thu Oct 24 16:20:02 2013
;; MSG SIZE  rcvd: 726
```

Bon, tout va bien, on obtient bien l'enregistrement SOA demandé, et la réponse inclut le bit `AD` (”*Authentic Data*”) montrant que la validation s'est bien faite. Des outils de tests plus sophistiqués comme Zonecheck <`http://www.zonecheck.fr/`> ne montrent pas non plus de problèmes. Mais ils ne testent pas assez. Cherchons cette fois un nom qui n'existe pas, `www.xn--80asehdb` :

```
% dig @149.20.64.20   SOA www.xn--80asehdb

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @149.20.64.20 SOA www.xn--80asehdb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 38016
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.xn--80asehdb. IN SOA

;; Query time: 744 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Thu Oct 24 16:20:20 2013
;; MSG SIZE  rcvd: 45
```

Aïe ! On n'a pas le `NXDOMAIN` qu'on attendait mais un `SERVFAIL` qui semble indiquer un problème DNSSEC. Pour être sûr, demandons au résolveur de tester sans validation, avec l'option `CD` (”*Checking Disabled*”) :

```
% dig +cd @149.20.64.20   SOA www.xn--80asehdb

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> +cd @149.20.64.20 SOA www.xn--80asehdb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 28571
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.xn--80asehdb. IN SOA
```

```
;; AUTHORITY SECTION:
xn--80asehdb. 0 IN SOA anycast10.irondns.net. secretariat.corenic.org. (
1310231925 ; serial
21600      ; refresh (6 hours)
3600       ; retry (1 hour)
604800     ; expire (1 week)
86400      ; minimum (1 day)
)
xn--80asehdb. 0 IN RRSIG SOA 10 1 86400 20131106172547 (
20131023172547 38327 xn--80asehdb.
ZUg0BUeRcEyTuyUmhcUC95U/iSd8/6GQS1D7k8YnADJa
QV1nBPJ+9EOW7ycMKtg0XokKl+i8SqlCLqOs2mUs6nFg
p9jB/T1sUar/w1QAjtClM9JcIliXC7AdDi4bmg5G15yX
rgkrdgXrm/8kyUEbMUlto6LNdBz/IYP5fS4hlvo= )
1kj9h96b2lh023ss088d4sv4fldblii8.xn--80asehdb. 0 IN RRSIG NSEC3 10 2 43200 20131106172200 (
20131023172200 38327 xn--80asehdb.
ConuMwi7xtPhtcwzZxH9+hrjE1yGVwYp7ql8nWbiUDqh
AjUyzisxCjGUwSjiFTESUFMVnVuhd38Ns89pWxOfevPo
jFVCo9kyNhZJ/OlIFTPto/Fi2gTsWiug/RDOD4rQ+66T
Jr0GNZQFQHN/TEb7OywBKXWw9DegLyFRdbBdlaA= )
1kj9h96b2lh023ss088d4sv4fldblii8.xn--80asehdb. 0 IN NSEC3 1 0 12 7740536091A63907 HFVHO12QAPRRRKQ16K4R241K2OE81B

;; Query time: 280 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Thu Oct 24 16:20:31 2013
;; MSG SIZE  rcvd: 557
```

Là, tout a marché. Aucun doute, c'est un problème DNSSEC. Mais lequel ? (Je triche, Mark Andrews a donné l'explication sur la liste dns-operations, je n'ai pas trouvé tout seul.) C'est parce que l'enregistrement NSEC3 ci-dessus, `1kj9h96b2lh023ss088d4sv4fldblii8.xn--80asehdb`, ne couvre pas tout, seulement l'apex. Il faut plusieurs enregistrements NSEC3 pour prouver une non-existence. Les enregistrements NSEC3, normalisés dans le RFC 5155 [2] sont considérés, à juste titre, comme une des parties les plus terribles de DNSSEC, et ce RFC comme un des plus difficiles à lire. Essayons quand même de comprendre. D'abord, récupérons les paramètres réglables de NSEC3 pour ce TLD :

```
% dig +short NSEC3PARAM xn--80asehdb
1 0 12 7740536091A63907
...
```

Donc, le sel est `7740536091A63907`, l'algorithme de condensation 1 et il faut faire 12 itérations. Calculons ce que ça donne pour l'apex de la zone :

```
% nsec3hash 7740536091A63907 1 12 xn--80asehdb
1KJ9H96B2LH023SS088D4SV4FLDBLII8 (salt=7740536091A63907, hash=1, iterations=12)
```

(Cet outil est livré avec BIND.) Bon, c'est bien la partie gauche de l'enregistrement NSEC3. Sa partie droite était `HFVHO12QAPRRRKQ16K4R241K2OE81BLP`. Et quel était le NSEC3 du nom qu'on demandait ?

```
% nsec3hash 7740536091A63907 1 12 www.xn--80asehdb
VFAQP7GOV8SECOUA5KL7QMUPU09ABPF3 (salt=7740536091A63907, hash=1, iterations=12)
```

2. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5155.txt`

Et voilà l'explication du problème. Le condensé `VFAQP7GOV8SECOUA5KL7QMUPU09ABPF3` n'est **pas** entre `1KJ9H96B2LH023SS088D4SV4FLDBLII8` et `HFVHO12QAPRRRKQ16K4R241K2OE81BLP`, le résolveur validant ne peut donc pas valider. Il faudrait en fait plusieurs enregistrements NSEC3, pas seulement celui qui couvre l'apex. Regardez avec un autre TLD signé comme `.fr` :

```
% dig SOA nexistepasdutout.fr

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> SOA nexistepasdutout.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 16892
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nexistepasdutout.fr. IN SOA

;; AUTHORITY SECTION:
fr. 5400 IN SOA nsmaster.nic.fr. hostmaster.nic.fr. (
2222302497 ; serial
3600       ; refresh (1 hour)
1800       ; retry (30 minutes)
3600000    ; expire (5 weeks 6 days 16 hours)
5400       ; minimum (1 hour 30 minutes)
)
fr. 5400 IN RRSIG SOA 8 1 172800 20131223203009 (
20131024193009 62646 fr.
DaGlS0gg6ZdrpPAlrGgTLnX7YIpuNy+drz9PXug4OQop
DFDNbn5RGCyHaAwGI2C97F/unRNfJWxfJbvahKXjSxUk
h1TV/HuJNR7NQ7B7ZbQhrXM+WJJOG2HMfM0ZjbuV7EDj
i65zhfM4y+a9gxEofMtFpxvG/GLtmkToq0XYT5s= )
gbncp12fmut57r0t7oncls9uqlmlodmk.fr. 5400 IN RRSIG NSEC3 8 2 5400 20131222134010 (
20131023124010 62646 fr.
YMskIKa5wXIfNeM7nFuS+t7CrkIBj8yDbViY/UFaJHyY
Fi6DluzDmzMro1P9JGtjMfOyCoHzELF/ypyP1AbD6gl6
Q+8M+pWFaVcAqw2YM8gj5tTs/EaeBHkRt5LN+ieP46em
24eW00n3hYVbbPzH16675tHQc6AQhKHV8XPilrE= )
gbncp12fmut57r0t7oncls9uqlmlodmk.fr. 5400 IN NSEC3 1 1 1 BADFE11A GBO5LRV9JCF6S1Q2IULLHM3S2E0HFNKT NS DS RRS
meqimi6fje5ni47pjahv5qigu1lv3jlj.fr. 5400 IN RRSIG NSEC3 8 2 5400 20131217141424 (
20131018141424 62646 fr.
HSlFBLGerg9v8cVNw/QtYfw9gtCxqsx4EI9GcL9loqUg
FzYrpbEp/1Du6h3me1zmxY1QvywljEUqnYBVFN9S3JC2
jDqxY+/xoHauiiz7ZCIWKaMT7UIo5o4Q/i+II1QfGRj1
YoSZfH/qjASnitYaRse2rDa8R2MmZ9Hn56nO9j0= )
meqimi6fje5ni47pjahv5qigu1lv3jlj.fr. 5400 IN NSEC3 1 1 1 BADFE11A MER9S1NKQCO41NBRBJLTPKQ93HEONLR8 NS SOA TX
s450cin37ia3u7s37vsnc0po8vj2igth.fr. 5400 IN RRSIG NSEC3 8 2 5400 20131217141424 (
20131018141424 62646 fr.
bU6ZhqlPC0h6hf8xLqAtzpgkqyrHL/OZNJOlzUutjreL
mL34i00G9eWIUAsjvKC2PZviFkvwhAuapD7OAGcAJvMS
o3R+KYqTSQ39AmYTX80uVSupkRHw5CGIX3g87LY7CbQ+
TRZ+LUUoYQ8vng3Ogi2IKEJwr9FAB9SCjHNeVSk= )
s450cin37ia3u7s37vsnc0po8vj2igth.fr. 5400 IN NSEC3 1 1 1 BADFE11A S45UOSDK5KJKQABLBLSBP7B5UK3R1MSV NS DS RRS

;; Query time: 37 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct 24 22:40:14 2013
;; MSG SIZE  rcvd: 1006
```

On peut voir graphiquement ce problème avec DNSviz `<http://dnsviz.net/d/xn--80asehdb/UmkY3A/dnssec/?rr=all&a=all&ds=all&doe=on&ta=.&tk=>`. Il faut activer l'option *"Denial of existence"* qui ne l'est pas par défaut (et peut donc rassurer à tort).

Pourquoi cette erreur ? NSEC3, on l'a dit, est très complexe. Mais on ne fabrique pas ses NSEC3 à la main ! La très grande majorité des administrateurs DNS qui utilisent DNSSEC n'auront jamais à analyser des problèmes comme celui-ci. On utilise un outil pour générer signatures et NSEC3, et aucun outil n'oublierait une partie de l'espace à protéger. Soit le registre a développé un outil à lui, ce qui serait une opération délicate et dangereuse, et c'est donc peu vraisemblable, soit quelque chose a cafouillé au moment de la publication des données.

Merci à Marco Davids pour le diagnostic initial.