delv, le futur outil principal de débogage de DNSSEC ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 juillet 2014

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

La version 9.10 de BIND vient avec un nouvel outil de débogage en ligne de commande, **delv**. Qu'apporte-t-il par rapport à dig ? C'est surtout pour ce qui concerne DNSSEC qu'il est utile.

L'outil de base de celui qui débogue un problème DNS, l'équivalent de ce que sont ping et traceroute pour l'ingénieur réseaux, c'est dig. Cet outil permet de récupérer des données DNS et de les afficher. Avec le DNS traditionnel, on n'avait pas besoin de plus. Mais avec DNSSEC, un problème supplémentaire survient : les données obtenues sont-elles vérifiées cryptographiquement ? dig avait bien une option `+sigchase` pour tester cela mais, très boguée, elle est restée peu connue. On n'avait donc pas d'outil simple, en ligne de commande, pour valider du DNSSEC. On a bien sûr `drill` (livré avec ldns <http://www.nlnetlabs.nl/projects/ldns/>) mais son option `-S` est très bavarde.

Depuis la version 9.10 de BIND, est apparue avec ce logiciel un nouvel outil, nommé **delv**. delv permet de faire la même chose que dig (en moins bavard par défaut) :

```
% delv  www.ssi.gouv.fr
; unsigned answer
www.ssi.gouv.fr. 21600 IN A 86.65.182.120

% delv -t mx  laposte.net
; unsigned answer
laposte.net. 600 IN MX 10 smtp4.laposte.net.
```

Mais c'est surtout lorsque le domaine est signé que delv est utile. (Autrement, comme vous l'avez vu plus haut, il affiche un triste "*unsigned answer*".) Testons avec un nom correctement signé :

```
% delv www.bortzmeyer.org
; fully validated
www.bortzmeyer.org. 52712 IN A 204.62.14.153
www.bortzmeyer.org. 52712 IN RRSIG A 8 3 86400 20140813162126 20140724102037 37573 bortzmeyer.org. ZU9fgjc34O2xf
```

Cette fois, il a procédé à une validation DNSSEC de la réponse (correcte, dans ce cas, "*fully validated*").

Vous allez le dire « mais il suffit d'utiliser un résolveur DNS validant et on sait, via le bit AD ("*Authentic Data*") que les données sont correctement signées ». Mais delv donne des informations supplémentaires. Par exemple, si le domaine est signé mais pointe vers un domaine non-signé :

```
% delv www.paypal.co.uk
; fully validated
www.paypal.co.uk. 3600 IN CNAME www.intl-paypal.com.edgekey.net.
www.paypal.co.uk. 3600 IN RRSIG CNAME 5 4 3600 20140816050243 20140717044122 22776 paypal.co.uk. TU8EubeTmR0

; unsigned answer
www.intl-paypal.com.edgekey.net. 120 IN CNAME e493.a.akamaiedge.net.
e493.a.akamaiedge.net. 20 IN A 23.58.178.37
```

Dans ce cas (aucun CDN ne gère aujourd'hui DNSSEC, hélas), delv indique bien quelle partie de la réponse est signée et laquelle ne l'est pas.

Et en cas de problème ? Si on teste avec des domaines délibérement cassés :

```
% delv -t mx servfail.nl
;; resolution failed: failure
```

Eh oui, on utilise un résolveur validant, il ne nous donne donc pas les données liées à ce domaine. Il faut donc (paradoxalement !) utiliser un résolveur non-validant ou bien, tout simplement, ajouter l'option `+cd`, "*Checking Disabled*", à delv :

```
% delv +cd -t mx servfail.nl
;; validating servfail.nl/DNSKEY: verify failed due to bad signature (keyid=25594): RRSIG has expired
;; validating servfail.nl/DNSKEY: no valid signature found (DS)
;; no valid RRSIG resolving 'servfail.nl/DNSKEY/IN': 127.0.0.1#53
;;   validating R6K26LDO0GS7N66JPQALLM0JIDU6PHML.servfail.nl/NSEC3: bad cache hit (servfail.nl/DNSKEY)
;; broken trust chain resolving 'servfail.nl/MX/IN': 127.0.0.1#53
;; resolution failed: broken trust chain
```

Voilà, on connait désormais la raison du problème, l'enregistrement `DNSKEY` de `servfail.nl` a une signature expirée. Avec un autre domaine, comportant une autre erreur (une signature délibérement modifiée) :

```
% delv +cd -t mx dnssec-failed.org
;; validating dnssec-failed.org/DNSKEY: no valid signature found (DS)
;; no valid RRSIG resolving 'dnssec-failed.org/DNSKEY/IN': 127.0.0.1#53
;;   validating dnssec-failed.org/NSEC: bad cache hit (dnssec-failed.org/DNSKEY)
;; broken trust chain resolving 'dnssec-failed.org/MX/IN': 127.0.0.1#53
;; resolution failed: broken trust chain
```

Et, ici, avec une date de signature dans le futur :

```
% delv +cd -t aaaa futuredate-aaaa.test.dnssec-tools.org
;; validating futuredate-aaaa.test.dnssec-tools.org/AAAA: verify failed due to bad signature (keyid=19442):
;; validating futuredate-aaaa.test.dnssec-tools.org/AAAA: no valid signature found
;; RRSIG validity period has not begun resolving 'futuredate-aaaa.test.dnssec-tools.org/AAAA/IN': 127.0.0.1#
;; resolution failed: RRSIG validity period has not begun
```

Comme vous avez vu, delv est parfait pour du premier débogage, donc, quitte à utiliser des outils plus complexes par la suite. Au fur et à mesure que les versions récentes de BIND se diffuseront, et que DNSSEC sera plus courant, dig sera sans doute souvent remplacé par delv.

Voir aussi l'article « "*Debugging dnssec with delv*" <http://bkraft.fr/blog/Debugging_dnssec_with_delv/> ».