RFC 5074 : DNSSEC Lookaside Validation (DLV)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 novembre 2007. Dernière mise à jour le 18 septembre 2008

Date de publication du RFC : Novembre 2007

https://www.bortzmeyer.org/5074.html

DLV ("*DNSSEC Lookaside Validation*") était une technique apparemment simple, qui résout élégamment un nœud gordien, mais qui a suscité de très chauds débats, pour des raisons politiques. DLV vise en effet à résoudre un problème de fond de DNSSEC, la signature de la racine. Elle est désormais abandonnée (cf. RFC 8749[1].)

En effet, avec DNSSEC tel qu'il est spécifié dans le RFC 4033, le résolveur qui tente de vérifier un domaine doit partir de la racine, si elle est signée, ou bien connaitre un ensemble de points de départ, les "*trust anchors*", qui sont les clés publiques des registres qui signent certaines zones. En l'absence d'une racine signée, c'est cette seconde solution que j'ai utilisée pour mes tests du résolveur Unbound <https://www.bortzmeyer.org/unbound-dnssec.html>.

Signer la racine est trivial techniquement (l'IANA l'a déjà fait <https://ns.iana.org/dnssec/status.html>) mais très compliqué politiquement. Il faut trouver un signataire légitime (et des sommets internationaux entiers ont été consacrés au problème d'une autorité légitime pour la racine) et il faut que ce signataire soit prêt à s'engager sérieusement puisque qu'une fois que les résolveurs testent la signature, on ne peut plus revenir en arrière.

DLV résout donc le problème en permettant aux racines de signature (comme celle de l'ISC <https://secure.isc.org/index.pl?/ops/dlv/index.php>) d'être distinctes de la racine du DNS. Ainsi, pour vérifier la signature de parano.example, un résolveur DNSSEC avec support DLV, pourra allez chercher les signatures dans, par exemple, parano.example.dlv.isc.org. DLV utilise les enregistrements DNS de type DLV, décrits dans le RFC 4431.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8749.txt

La section 7 du RFC est consacrée à un problème difficile. Avec DLV, contrairement au DNSSEC classique, plusieurs « racines » peuvent signer un même domaine. On peut avoir par exemple une racine DLV qui signe `.org` et une autre qui signe `example.org`. Laquelle utiliser dans le cas de tels recouvrements ? La solution choisie est de ne pas choisir : le résolveur DLV peut utiliser l'algorithme qu'il veut, le plus simple étant décrit comme « choisir la racine la plus spécifique » (celle de `example.org` dans notre exemple). La section 7 décrit d'autres algorithmes et recommande que le résolveur propose un choix à l'utilisateur.

DLV fournit donc désormais une alternative à la longue attente d'une signature officielle de la racine. Cette alternative a semblé trop simple à certains et beaucoup d'objections ont été levées contre DLV, accusé notamment de retarder la « vraie », la « bonne » solution de signer la racine. Pour citer Paul Vixie, un grand défenseur de DLV, on peut dire que ces objections reviennent à empêcher des adultes consentants <http://www1.ietf.org/mail-archive/web/ietf/current/msg47950.html> d'expérimenter une idée intéressante et qui ne fait de mal à personne. À noter que l'IAB a publié un communiqué <http://www1.ietf.org/mail-archive/web/ietf/current/msg47978.html> qui, après pas mal de détours, accepte l'idée de DLV.

L'ISC a une note technique, 2006-01 <http://www.isc.org/index.pl?/pubs/tn/index.pl?tn=isc-tn-2006-1.html> sur le sujet de DLV. DLV est implémenté dans le résolveur de BIND depuis plusieurs versions. Il se configure ainsi (une documentation détaillée est en <https://secure.isc.org/index.pl?/ops/dlv/>) :

```
// À l'intérieur du bloc "options"
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside . trust-anchor dlv.isc.org.;
```

À partir de là, on peut valider un domaine qui est enregistré dans le registre DLV de l'ISC, même si on n'a pas de "*trust anchor*". Prenons par exemple `sources.org` :

```
% dig +dnssec MX sources.org.

; <<>> DiG 9.5.0-P2 <<>> +dnssec MX sources.org.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15559
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
                  ^^
>>>>              Authentic Data, donc validées par DNSSEC

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;sources.org.                   IN      MX

;; ANSWER SECTION:
sources.org.            86400   IN      MX      10 uucp.bortzmeyer.org.
...
```

Autre solution pour tester si son résolveur utilise bien le registre DLV de l'ISC : <https://www.dns-oarc.net/oarc/services/dlvtest>. Par exemple :

```
% dig +dnssec a.nsec.dlvtest.dns-oarc.net txt


; <<>> DiG 9.5.1-P3 <<>> +dnssec a.nsec.dlvtest.dns-oarc.net txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56042
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
```

Cet essai a bien fonctionné, on a bien le 'ad'.

Le service DLV de l'ISC a été arrêté depuis et cette technique transitoire n'est désormais plus d'actualité.