TSIG si on n'utilise pas BIND ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 mars 2014

http://www.bortzmeyer.org/tsig-sans-bind.html

Il existe des zillions (voire des zilliards) de HOWTO et d'articles de blog sur la configuration d'un serveur DNS BIND pour une authentification avec TSIG, par exemple entre serveur maître et serveurs esclaves. Et si on n'utilise pas les outils BIND ? Là, il y a nettement moins de documents. Voici donc un exemple.

Un petit rappel sur TSIG d'abord. Normalisée dans le RFC 2845 [1], cette technique permet à deux serveurs DNS de s'authentifier mutuellement, en utilisant un secret partagé (une sorte de mot de passe, quoi). Comme les secrets partagés ne sont pas pratiques du tout à distribuer et à garder confidentiels, TSIG ne peut pas réalistement s'envisager comme solution générale de sécurisation du DNS. Mais, pour un petit groupe de serveurs qui se connaissent (typiquement les serveurs faisant autorité pour une zone donnée), c'est utile. Cela évite notamment qu'un serveur esclave, croyant parler au maître, parle en fait (par exemple par suite d'un détournement BGP) à un serveur pirate qui lui enverra des fausses données. Bien sûr, si tout le monde faisait du DNSSEC, le problème n'existerait pas, les fausses données seraient détectées par la validation DNSSEC. Mais tant que DNSSEC n'est pas largement répandu, TSIG est un moyen simple et pas cher de sécuriser les communications entre serveurs faisant autorité pour une zone (et qui transfèrent le contenu de la zone avec le mécanisme du RFC 5936).

Supposons maintenant qu'on gère une zone `example.com` et qu'on ait comme maître un serveur de noms n'utilisant pas du tout BIND ou les outils qui viennent avec. On va alors se servir des outils de la bibliothèque ldns <http://www.nlnetlabs.nl/projects/ldns/> pour générer les clés (les secrets partagés) et NSD <http://www.bortzmeyer.org/nsd.html> comme serveur de noms.

D'abord, on va décider d'avoir une clé (un secret) différente par couple esclave/zone. Mettons que `ns1.example.net` soit esclave pour la zone `example.com`, on va nommer la clé `ns1.example.net@example.com` et on va générer la clé ainsi :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2845.txt`

```
% ldns-keygen -a hmac-sha256  ns1.example.net@example.com
Kns1.example.net@example.com.+159+63629
```

(L'algorithme HMAC-SHA256 est considéré comme sûr aujourd'hui, TSIG utilisait traditionnellement MD5 qui est fortement déconseillé aujourd'hui.) On obtient alors deux fichiers mais qui ont le même contenu, seul le format est différent. Prenons `Kns1.example.net@example.com.+159+63629.private` :

```
% cat Kns1.example.net@example.com.+159+63629.private
Private-key-format: v1.2
Algorithm: 159 (HMAC_SHA256)
Key: E8mRpGdzXXiT5UZaeUvcecKEjLOu95PJJSN6e4aFnD+cnn4BqkyYgbK2HNyA1m/aSpJIIm9jxS8QnCqvQU2685zO71ozLU02Erhoio1
```

Le secret partagé est le champ `Key:` (évidemment, ce secret particulier ne doit plus être utilisé, depuis qu'il a été publié sur ce blog...) Mettons-le dans la configuration du maître NSD :

```
key:
      name: ns1.example.net@example.com
      algorithm: hmac-sha256
      secret: "E8mRpGdzXXiT5UZaeUvcecKEjLOu95PJJSN6e4aFnD+cnn4BqkyYgbK2HNyA1m/aSpJIIm9jxS8QnCqvQU2685zO71ozL

...

zone:
        name: "example.com"
        ...
        notify: 2001:db8:1::3:83  ns1.example.net@example.com
        provide-xfr: 2001:db8:1::3:83 ns1.example.net@example.com
```

La ligne `notify:` indique que les notifications de mise à jour (RFC 1996) doivent être signées avec TSIG et notre nouvelle clé. La ligne `provide-xfr:` indique qu'on n'accepte de transférer la zone qu'à la machine authentifiée avec cette clé. Si vous avez dans le journal :

```
Mar 23 16:49:05 foobar nsd[23773]: axfr for zone example.com. \
          from client 2001:db8:2::3:83 refused, no acl matches
```

C'est qu'il y a une erreur (ici, adresse IP inconnue) dans la configuration.

Il ne vous reste plus qu'à envoyer le secret au gérant du serveur esclave, qu'il fasse la configuration de son côté. Naturellement, cela doit se faire de manière confidentielle, par exemple par un message chiffré avec PGP.