RFC 7673 : Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 octobre 2015

Date de publication du RFC : Octobre 2015

https://www.bortzmeyer.org/7673.html

Le protocole DANE, normalisé dans le RFC 6698 [1], permet d'associer au nom d'un serveur un certificat qu'on peut comparer avec celui qui est présenté par le serveur lors d'une session TLS, authentifiant ainsi directement ou indirectement le serveur. Cela permet de boucher certaines failles de X.509. Mais DANE ne marche qu'avec un nom de serveur, tel que l'utilise HTTP. La quasi-totalité des protocoles ont, au contraire, une indirection supplémentaire entre nom de service et nom de serveur, typiquement via un enregistrement SRV (RFC 2782). Dans un tel cas, où trouver les enregistrements TLSA, ceux utilisés par DANE ? Le choix est de vérifier le domaine pointé (nom du serveur, celui du prestataire) et pas le pointeur (nom de service, celui de l'utilisateur).

Voici un exemple d'un enregistrement TLSA (au passage, ne cherchez pas à quels mots correspondent les lettres de TLSA : ce n'est officiellement pas un acronyme) classique, pour un serveur HTTP, en l'occurrence pour <https://www.freebsd.org> :

```
% dig TLSA _443._tcp.www.freebsd.org
...
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 13
...
;; ANSWER SECTION:
_443._tcp.www.freebsd.org. 600 IN TLSA 3 0 1 (
A9F16D689F5AEE122E86A8468A8586DDA4440A7298C6
4AD4EED1AAE8BEB2A892 )
...
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6698.txt

Mais, à part HTTP (dont c'est l'une des principales faiblesses, menant à un mélange entre nom de service et nom de serveur), les protocoles utilisent en général un **nom de service** (vu par l'utilisateur) et un **nom de serveur** (récupéré automatiquement dans le DNS via les enregistrements SRV ou, dans le cas du courrier, des enregistrements MX). Il fallait donc étendre la définition originelle de DANE, celle du RFC 6698, pour ces protocoles. Pour SMTP et ses MX, c'est le RFC 7672. Pour les protocoles à SRV, comme XMPP, c'est ce RFC 7673.

Le choix principal qui se posait lors de la rédaction de ce RFC était « l'enregistrement TLSA doit-il être associé au service (l'origine, en partie gauche de l'enregistrement SRV) ou bien au serveur (la cible, en partie droite) ? » Le choix a été fait d'accrocher le TLSA, l'enregistrement DNS contenant le certificat au **serveur**. Ainsi, si on a cet enregistrement SRV pour XMPP à `example.com` :

```
_xmpp-client._tcp.example.com. SRV     1 0 5222 im.example.net.
```

L'enregistrement TLSA sera en `im.example.net`, pas en `example.com`. Les raisons de ce choix sont expliquées dans l'annexe B du RFC et résumées plus loin.

Pour la sécurité du lien entre service et serveur, on compte sur DNSSEC, qui signera l'enregistrement SRV (ainsi que, bien sûr, le TLSA). Maintenant, place aux détails concrets.

La section 3 du RFC commence par les tests DNS. Si l'utilisateur veut se connecter à un service `foobar` dans `example.com`, il va demander le SRV de `_foobar._tcp.example.com`. Supposons qu'il existe un alias (enregistrement CNAME) vers `foobar.example.net` et qu'ensuite on trouve le SRV qui liste un seul serveur, `foobar1.example.org`. Pour pouvoir utiliser DANE, il faut que toute la chaîne DNS soit sécurisée par DNSSEC. Dans cet exemple, les deux enregistrements qui forment la chaîne (le CNAME puis le SRV) doivent donc tous les deux être signés et validés. Sinon, si l'un de ces enregistrements n'est pas signé, pas question de lancer DANE puisqu'on ne peut pas avoir confiance dans leur contenu.

On n'en a pas fini avec le DNS : il faut maintenant trouver l'adresse IP des serveurs (ici, un seul), ce qui doit être également validé avec DNSSEC. Enfin, on fait les requêtes pour les enregistrements TLSA, en utilisant comme nom (le QNAME ou "*Query Name*") le nom du serveur, préfixé du numéro de port. Si l'application `foobar` fonctionne sur le port 5634 (il est indiqué dans l'enregistrement SRV), on demandera ici le ou les TLSA de `_5634._tcp.foobar1.example.org` (et non pas d'`example.com`). Autre exemple, emprunté au RFC, avec IMAP, le SRV pour `example.com` valait :

```
_imap._tcp.example.com. 86400 IN SRV 10 0 9143 imap.example.net.
```

On demandera donc un enregistrement TLSA pour `_9143._tcp.imap.example.net`. Évidemment, on vérifie la validité de cet enregistrement avec DNSSEC (ignorer les enregistrements non signés et donc non validés est un principe de base de DANE, cf. RFC 6698, section 4.1).

Le client se connecte en TLS au serveur. Quelles vérifications doit-il faire (section 4) ? S'il n'a trouvé aucun enregistrement TLSA utilisable (par exemple parce qu'il n'y en avait pas, ou bien parce qu'ils n'étaient pas signés avec DNSSEC), il doit faire la validation habituelle d'un certificat X.509 (à partir des AC que le client a dans son magasin), décrite dans le RFC 5280. Il peut être nécessaire d'utiliser quelques règles spécifiques à l'application, cf. RFC 6125. Au passage, notons que la terminologie est

variable : ce que notre RFC 7673 nomme service et serveur est appelé dans la RFC 6125 « domaine source » et « domaine dérivé ».

Par contre, s'il y a des enregistrements TLSA et qu'ils sont utilisables (ce qui implique notamment qu'ils soient signés et validés), alors le client doit valider le certificat obtenu dans le dialogue TLS avec DANE (RFC 6698, section 2.1). Notamment, si l'enregistrement TLSA indique un usage « DANE-EE » ("*DANE End Entity*"), alors le client ne doit pas faire de vérification X.509 du tout et donc ignorer les RFC 5280 et RFC 6125.

Si vous êtes l'auteur d'un protocole qui utilise des enregistrements SRV, lisez la section 5 de notre RFC : elle écrit les détails auxquels vous devez penser pour votre protocole. Ce sont notamment :

— Les éventuels mécanismes de repli si le client n'arrive pas à se connecter de manière sûre,
— Comment les clients doivent-il faire s'ils ne trouvent pas d'enregistrement SRV ou s'ils ne savent pas faire de requêtes SRV (ce qui est un problème fréquent avec le JavaScript exécuté dans un navigateur Web).
— La méthode générique en TLS pour indiquer le nom de domaine auquel on veut se connecter est l'extension SNI du RFC 6066. Certains protocoles ont une méthode à eux et il faut donc la documenter (par exemple, XMPP utilise l'élément `<to>` de son flux XML).
— Utilisation d'éventuels autres mécanismes de découverte, en sus des SRV, comme les NAPTR (RFC 3403) utilisés par SIP.

Si vous êtes opérateur d'un service sécurisé avec TLS, voyez la section 6. Elle rappelle la nécessité de signer les enregistrements DNS SRV et TLSA avec DNSSEC. D'autre part, en créant le certificat qui sera servi en TLS, il faut suivre certaines règles :

— Si l'enregistrement TLSA prévoit un usage DANE-EE, le ou les noms indiqué(s) dans le certificat n'ont pas d'importance pour DANE (cf. la section 9.2). D'un autre côté, les clients non-DANE ne pourront pas se connecter en TLS si les noms ne correspondent pas à ce qu'ils attendent.
— Avec d'autres usages que DANE-EE, ou bien si on veut que le certificat marche même avec les clients non-DANE, il faut que le nom dans le certificat soit le nom de serveur et de préférence qu'il y ait aussi le nom de service (les règles exactes, compliquées, sont dans le RFC 6125). Dans un environnement où un fournisseur sert un grand nombre de domaines hébergés (environnement "*multi-tenant*"), mettre le nom du service va souvent être difficile.

L'extension SNI du RFC 6066, déjà citée, permet d'envoyer au client le bon certificat, si le serveur en a plusieurs. Un exemple d'un usage de TLSA où il faut vérifier le nom est l'usage DANE-TA où le certificat dans l'enregistrement TLSA autorise l'AC, pas le certificat du serveur. Cet usage empêche les attaques par une autre AC mais pas celles par un autre utilisateur de la même AC. Il faut donc vérifier que le(s) nom(s) dans le certificat est(sont) bien celui attendu (cf. section 9.2).

Après les auteurs de protocoles et les administrateurs système, place aux développeurs (section 7). Pour limiter le temps d'attente pour les utilisateurs, le RFC leur recommande de faire les différentes résolutions aussi en parallèle que possible. Par exemple, une fois obtenu un SRV, on peut faire les résolutions d'adresse (enregistrements A et AAAA) en même temps que le TLSA.

La section 9 du RFC revient sur quelques pièges de sécurité. D'abord, un ensemble d'enregistrements SRV pouvant contenir plusieurs noms de serveurs, il ne faut pas croire que tous auront le même niveau de sécurité, surtout si l'un d'eux est sous-traité à un opérateur ne servant qu'en cas de problème avec les serveurs « principaux ». Par exemple, certains peuvent accepter TLS et d'autres pas. Il sera donc inutile de chercher des enregistrements TLSA pour les seconds. Ce point est d'autant plus important que le traitement des enregistrements SRV ne donne aucune priorité aux serveurs ayant TLS.

L'annexe B de notre RFC est cruciale et doit absolument être lue. Elle revient sur un choix qui a été délicat et très discuté à l'IETF : l'enregistrement TLSA doit-il se situer sur le nom de service (domaine originellement indiqué par l'utilisateur et donc a priori le domaine important qu'on veut vérifier) ou bien sur le nom de serveur (obtenu après une requête SRV et information normalement purement technique) ?

Le choix de notre RFC 7673 est clair : le TLSA pertinent est situé sur le nom du serveur, essentiellement parce que c'est la seule méthode réaliste pour les services hébergés chez un gros opérateur qui a des milliers, voire des millions, de client hébergés.

Des raisons diverses viennent à l'appui de ce choix :

— Le certificat fait partie de la configuration du serveur. Il est donc logique de mettre le TLSA au nom du serveur.
— Pensez à un changement de certificat : si le TLSA est lié au serveur, il n'y a qu'un seul changement dans le DNS. S'il est lié au client, il y en aura autant que de domaines hébergés (et certains l'oublieront probablement).
— Si le client n'utilise pas SNI, le certificat servi devra lister tous les domaines de tous les hébergés (comme on le voit sur des gros hébergeurs comme CloudFlare, où `https://www.republique-numerique.` partage son certificat avec un site porno chinois, `https://renxxx.com/`).
— Avec la méthode choisie, le même certificat marchera pour une connexion via un SRV et aussi pour une connexion directe quand on connait le nom du serveur, ce qui peut être pratique pour le déboguage.
— Certains protocoles applicatifs permettent d'envoyer des messages pour plusieurs domaines en une seule transaction. Cela ne serait plus possible si l'enregistrement TLSA était lié au service. Un exemple d'un tel protocole est SMTP (qui n'utilise pas SRV mais c'est juste un exemple) lors de plusieurs `RCPT TO` vers des domaines différents.
— Pour certains protocoles (là encore, c'est le cas de SMTP), un serveur peut jouer plusieurs rôles (par exemple, pour SMTP, cible des enregistrements MX, en réception, mais aussi envoyeur). Il est plus simple de n'avoir qu'un certificat pour tous les cas.

Bien sûr, il y a des cas où le TLSA sur le nom du service (du domaine source) serait préférable. L'IETF avait envisagé de permettre cette possibilité, en plus de la « normale » mais y a renoncé pour garder le protocole simple. Dans certains cas (clients non-DNSSEC, par exemple, qui ne peuvent donc pas valider le SRV et doivent donc vérifier le domaine d'origine), cela compliquera les choses (SNI aidera parfois).

Allez, un exemple réel d'un enregistrement SRV avec DANE au bout :

```
% dig +nodnssec +short SRV _xmpp-server._tcp.mailbox.org
0 5 5269 xmpp.mailbox.org.

%  dig +nodnssec +short TLSA _5269._tcp.xmpp.mailbox.org
3 1 1 4758AF6F02DFB5DC8795FA402E77A8A0486AF5E85D2CA60C294476AA DC40B220
```

Et je vous recommande de lire cet excellent article sur la sécurisation de XMPP avec DNSSEC et DANE <http://op-co.de/blog/posts/yax_im_dnssec/>.