Quel nom vérifier dans un certificat X.509, si on a été redirigé ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 janvier 2012

https://www.bortzmeyer.org/redirection-certificat.html

Une discussion animée vient d'avoir lieu sur la liste du groupe de travail IETF DANE <http://tools.ietf.org/wg/dane>, qui travaille à permettre l'utilisation de certificats dans le DNS (en simplifiant, il s'agit de remplacer X.509 par DNSSEC, voir mon exposé aux JRES <https://www.bortzmeyer.org/jres-dane-2011.html>). La question était « Lorsqu'il y a eu des redirections vers un autre nom de domaine, quel nom chercher dans le certificat ? Celui de départ ? Celui d'arrivée ? »

Prenons un exemple concret pour voir. Supposons un protocole nommé PDP (pour "*Pur Distribution Protocol*") qui permet de récupérer des contenus (musique, films, etc) qui avaient été auparavant chargés sur un serveur. Pour trouver le serveur adéquat, mettons que cet hypothétique PDP utilise les enregistrements SRV du DNS (RFC 2782 [1]), afin d'assurer la répartition de charge, et la résistance aux pannes. Mettons que le domaine microupload.example ait deux serveurs, on aurait quelque chose comme :

```
_pdp._tcp.microupload.example.     SRV     0 0 6642  content.example.com.
                                   SRV     1 0 6642  content.backup.example.
```

Vu les priorités (le premier chiffre après SRV), le second serveur ne sera utilisé qu'en cas de panne du premier. Mais, et c'est là que ça devient intéressant, on va supposer que PDP, pour échapper à des gens malintentionnés qui voudraient savoir ce qu'on télécharge, chiffre toutes ses communications avec TLS et authentifie le serveur avec X.509. Imaginons que le premier serveur soit en panne à ce moment et que le client PDP se connecte donc à content.backup.example. À quel nom doit être le certificat de ce dernier ? microupload.example parce que c'est le point de départ de la transaction ? content.backup.example parce que c'est le nom du serveur ? Prenez le temps de réflechir à cette question cinq minutes, et essayez de faire une liste des raisons en faveur du premier choix et de celles en faveur du second. Il est probable que vous en oublierez, car le problème est compliqué.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2782.txt

Vous y êtes ? Vous avez vraiment cherché ? Bon, alors, maintenant, des éléments de réponse. Le problème du groupe DANE avait été enregistré comme ticket #28 <http://trac.tools.ietf.org/wg/dane/trac/ticket/28> mais, si vous n'avez pas lu le RFC 6394, ce n'est pas trop grave, la question n'est pas du tout spécifique à DANE. Elle a même fait l'objet d'un RFC entier, le RFC 6125, que je trouve personnellement peu lisible. Son principal mérite est de montrer que la question de l'**identité** n'est pas triviale du tout et qu'elle peut signifier des choses différentes selon la personne.

Et la question n'est pas non plus spécifique aux enregistrements SRV comme dans l'exemple ci-dessus. On aurait la même question, par exemple avec des MX.

Alors, une liste de raisons en faveur du premier choix, utiliser le nom de départ (ici, `microupload.example`) :

— Le nom de départ est celui que voit l'utilisateur. C'est celui en lequel il a confiance. C'est le nom du service, pas celui du serveur du moment.
— Si la résolution DNS n'est pas sécurisée (par exemple avec DNSSEC), rien ne prouve que le SRV obtenu est légitime. X.509 ne servirait à rien dans ce cas. (Notez que, dans le cas spécifique de DANE, DNSSEC est obligatoire donc, si on décide que le nom utilisé par DANE sera le premier, il sera sécurisé par DNSSEC de toute façon.)

Et les raisons d'utiliser au contraire le nom d'arrivée, ici `content.backup.example` ?

— Dans le cas d'un serveur qui héberge des services pour des milliers de domaines différents, il faudra gérer beaucoup de certificats.
— Il existe plusieurs méthodes pour avoir plusieurs certificats sur la même machine <https://www.bortzmeyer.org/auth-x509-plusieurs-noms.html>. Si la méthode choisie est de mettre tous les noms dans un même certificat <https://www.bortzmeyer.org/plusieurs-noms-dans-html>, celui qui se connecte peut apprendre la liste de tous les clients (au sens affaires, pas au sens protocole réseau) du serveur juste en regardant le certificat.
— Dans le cas où le serveur n'est pas géré par la même organisation que le domaine (ce qui est fréquent aujourd'hui), une stricte coordination sera nécessaire. Si le domaine acquiert un nouveau certificat, il leur faudra s'assurer qu'il est bien installé sur le serveur.

Bref, tester le domaine de départ est en général meilleur du point de vue sécurité, mais tester le domaine d'arrivée facilite en général le déploiement.

Mais, puisque le problème est connu depuis longtemps, que spécifient les différents RFC sur les protocoles qui utilisent TLS ? Eh bien, souvent, ce n'est pas clair. Essayez de lire le RFC 3207 pour voir ce que devrait faire un bon client SMTP, par exemple. Le vocabulaire peu stable du RFC ne permet guère de trancher. L'avis dominant est toutefois que SMTP doit utiliser le domaine d'arrivée. Donc, s'il y a un MX :

```
michu.example.     IN      MX      10 mail.provider.example
```

Alors, le MTA qui essaiera de transmettre du courrier en TLS à `monsieur@michu.example` cherchera sur l'autre MTA un certificat portant le nom de `mail.provider.example`.

Mais, et c'est là que cela devient amusant, d'autres protocoles ont pu faire des choix différents ! C'est ainsi que XMPP spécifie le contraire, on doit utiliser le domaine du début, avant toute redirection (RFC 6120, section 5.4.3.1). Et pour HTTP ? Ce dernier n'utilise pas d'enregistrement DNS de redirection (comme les MX ou les SRV). Il ne reste donc comme possibilité de piège, au niveau DNS, que les CNAME. Ceux-ci sont délicats car, contrairement aux SRV ou MX, la bibliothèque qui fait la résolution ne donne pas forcément à l'application (ici, le navigateur), une indication sur la présence ou non d'un alias (un enregistrement CNAME). Le RFC 2818 n'est pas parfaitement clair mais semble de toute façon avoir choisi aussi l'approche « domaine de départ » (ici, celui qui est dans l'URI).

Et que va faire le groupe DANE ? La question n'est pas encore définitivement tranchée mais ce sera probablement « chaque protocole se débrouille » car il est trop difficile de spécifier un choix qui convienne à tous.

`https://www.bortzmeyer.org/redirection-certificat.html`