RFC 7286 : ALTO Server Discovery

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 novembre 2014

Date de publication du RFC : Novembre 2014

https://www.bortzmeyer.org/7286.html

Le protocole ALTO ("*Application-Layer Traffic Optimization*"), normalisé dans le RFC 7285 [1], permet à une machine qui communique avec des pairs, de déterminer quel pair utiliser lorsqu'ils fournissent le même service (par exemple, dans un système de partage de fichiers pair-à-pair, lorsque les membres d'un même essaim ont le fichier convoité). La machine, un client ALTO, demande à un serveur ALTO quel est le « meilleur » pair, optimisant ainsi son utilisation du réseau. Oui, mais comment est-ce que le client trouve le serveur à utiliser ?

Le RFC 6708, le cahier des charges d'ALTO, disait dans son exigence AR-32 qu'il fallait un mécanisme pour trouver le serveur. ALTO reposant sur HTTP, trouver un serveur, c'est trouver l'URI qui le désigne. Le protocole de découverte va partir d'un nom de domaine (obtenu, par exemple, via DHCP, ou bien via une configuration manuelle), faire une requête DNS sur ce nom, en demandant le type U-NAPTR (RFC 4848, mais ne paniquez pas, j'explique le U-NAPTR plus loin). La réponse sera l'URI désiré.

Donc, première étape (section 3.1), récupérer le nom de domaine. Pour la machine typique de M. Michu, cela se fait en DHCP, le serveur DHCP donnant, parmi d'autres informations, le nom de domaine de référence du réseau local (options DHCP 213 - `OPTION_V4_ACCESS_DOMAIN` - et 57 - `OPTION_V6_ACCESS_DOMAIN` - de la section 3 du RFC 5986, ou bien, si elle n'est pas présente, et en IPv4 seulement, l'option 15 de la section 3.17 du RFC 2132). Le nom sera alors celui du FAI ou celui de l'organisation où M. Michu se connecte. Mais le RFC demande aussi que les mises en œuvre de la découverte de serveurs ALTO puisse aussi se faire à partir d'un nom de domaine rentré manuellement par l'utilisateur. Cela permet, par exemple, de traiter le cas où un utilisateur n'a pas confiance dans le serveur ALTO de son FAI et souhaite utiliser le serveur ALTO d'une organisation tierce. (Tiens, peut-être verrons-nous apparaître un Google Alto ?)

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7285.txt`

Une fois qu'on a le nom de domaine, on passe à la deuxième étape de la procédure de découverte du serveur (section 3.2). Pour cela, on va demander un enregistrement de type U-NAPTR. Ce type de données, normalisé dans le RFC 4848, est très complexe. Disons simplement qu'il permet de découvrir des services en utilisant un enregistrement DNS qui comprend une étiquette de service, et une expression rationnelle de remplacement dont le résultat sera l'URI recherché (la procédure de découverte de serveur d'ALTO simplifie les choses en n'utilisant pas la partie gauche de l'expression, seulement le résultat). Les U-NAPTR sont plus riches que les S-NAPTR du RFC 3958 mais moins que les NAPTR originels (RFC 3403). À noter que la différence entre NAPTR, S-NAPTR et U-NAPTR ne se voit pas dans le DNS : tous utilisent le même type, NAPTR. Voici un exemple d'un enregistrement DNS pour la découverte du serveur ALTO de `example.net` :

```
example.net. IN NAPTR 100 10 "u" "ALTO:https" "!.*!https://alto1.example.net/ird!"  ""
```

L'étiquette de service est `ALTO:https` (désormais enregistrée à l'IANA <https://www.iana.org/assignments/s-naptr-parameters/s-naptr-parameters.xml#s-naptr-parameters-1>). En filtrant sur cette étiquette, on pourra récupérer uniquement les enregistrements ALTO. Ici, l'URI de résultat sera `https://alto1.example.net/ird`.

Il peut y avoir plusieurs NAPTR, pour fournir des serveurs alternatifs, et on pourrait donc avoir :

```
example.net. IN NAPTR 100 10 "u" "ALTO:https" "!.*!https://alto1.example.net/ird!"  ""
             IN NAPTR 100 20 "u" "ALTO:https" "!.*!https://alto2.example.net/ird!"  ""
```

Dans ce cas, le champ « Préférence » du second serveur (le second URI, plutôt) étant plus élevé, il ne sera choisi que si le premier ne répond pas (oui, une préférence plus élevée veut dire qu'on sera moins considéré, comme pour les enregistrements MX).

Au fait, pourquoi un U-NAPTR et pas un simple S-NAPTR (puisqu'on ne se sert pas de la partie gauche de l'expression rationnelle) ? Parce que les S-NAPTR ne fournissent comme résultat qu'un couple {serveur, port}, pas un URI comme le protocole ALTO en a besoin.

En pratique, quelles questions posera le déploiement de cette procédure (section 4) ? Elle dépend d'une bonne réception du nom de domaine. Les options du RFC 5986 ne sont pas forcément gérées par tous les serveurs DHCP. Ensuite, dans le cas d'une connexion typique à la maison via un petit routeur CPE, il faudra que le routeur passe fidèlement en DHCP les noms de domaine qu'il a lui-même obtenu. Si, à la place du `example.net`, il transmet aux clients un nom comme, mettons, `.local`, la recherche de serveur ALTO échouera.

Cette procédure de découverte du serveur, comme le note la section 6 de notre RFC, n'est pas très sécurisée. Si un méchant arrive à diriger les clients vers un mauvais serveur ALTO, celui-ci pourra donner de l'information fausse, menant les clients à choisir un pair particulièrement lent. Pour cela, le méchant peut s'attaquer à l'échange DHCP. DHCP n'est pas sécurisé du tout mais, bon, si le méchant peut envoyer des fausses réponses DHCP, il pourra faire des choses bien pires que de donner un mauvais serveur ALTO. Donc, cette méthode d'attaque n'est pas très inquiétante. Une autre méthode pour l'attaquant serait de convaincre l'utilisateur de rentrer manuellement un nom de domaine menant au serveur ALTO malveillant, un problème qui ressemble à celui du hameçonnage (et qui, comme lui, n'a pas de solution technique).

Une dernière attaque possible serait de compromettre la résolution DNS. La procédure de découverte du serveur ALTO n'impose pas l'usage de DNSSEC et, sans lui, le DNS n'est pas vraiment sûr. Enfin, l'attaque pourrait porter, après la découverte du serveur correct, sur la communication HTTP avec le serveur (surtout si on n'utilise pas HTTPS). Personnellement, je ne suis pas trop inquiet : on a des problèmes de sécurité bien plus sérieux sur l'Internet.

À noter que d'autres mécanismes de découverte du serveur ALTO ont été proposés à l'IETF et qu'ils feront peut-être l'objet d'une spécification officielle plus tard.