RFC 7710 : Captive-Portal Identification Using DHCP or Router Advertisements (RAs)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 décembre 2015

Date de publication du RFC : Décembre 2015

https://www.bortzmeyer.org/7710.html

Les portails captifs sont une des plaies de l'accès à l'Internet. À défaut de pouvoir les supprimer, ce nouveau RFC propose des options aux protocoles DHCP et RA pour permettre de signaler la présence d'un portail captif, au lieu que la malheureuse machine doive le détecter elle-même. depuis, il a été remplacé par le RFC 8910 [1].

On trouve de tels portails captifs en de nombreux endroits où de l'accès Internet est fourni, par exemple dans des hôtels ou des cafés. Tant que l'utilisateur ne s'est pas authentifié auprès du portail captif, ses capacités d'accès à l'Internet sont très limitées. Quels sont les problèmes que pose un portail captif ?

— Le plus important est qu'il détourne le trafic normal : en cela, le portail captif est une attaque de l'Homme du Milieu et a donc de graves conséquences en terme de sécurité. Il éduque les utilisateurs à trouver normal le fait de ne pas arriver sur l'objectif désiré, et facilite donc le hameçonnage.
— Le portail captif ne marche pas ou mal si la première connexion est en HTTPS, ce qui est de plus en plus fréquent. Là encore, il éduque les utilisateurs à trouver normaux les avertissements de sécurité (≪ mauvais certificat, voulez-vous continuer ? ≫).
— Le portail captif n'est pas authentifié, lui, et l'utilisateur est donc invité à donner ses informations de créance à un inconnu.
— En Wifi, comme l'accès n'est pas protégé par WPA, le trafic peut être espionné par les autres utilisateurs.
— Spécifique au Web, le portail captif ne marche pas avec les activités non-Web (comme XMPP). Même les clients HTTP non-interactifs (comme une mise à jour du logiciel via HTTP) sont affectés.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8910.txt

Pourquoi est-ce que ces hôtels et cafés s'obstinent à imposer le passage par un portail captif ? On lit parfois que c'est pour authentifier l'utilisateur mais c'est faux. D'abord, certains portails captifs ne demandent pas d'authentification, juste une acceptation des conditions d'utilisation. Ensuite, il existe une bien meilleure solution pour authentifier, qui n'a pas les défauts indiqués plus haut. C'est 802.1X, utilisé entre autres dans eduroam (voir RFC 7593). La vraie raison est plutôt une combinaison d'ignorance (les autres possibilités comme 802.1X ne sont pas connues) et de désir de contrôle (« je **veux** qu'ils voient mes publicités et mes CGU »).

L'IETF travaille à développer un jour un protocole complet d'interaction avec les portails captifs, pour limiter leurs conséquences. En attendant, ce RFC propose une option qui permet au moins au réseau local de signaler « attention, un portail captif est là, ne lance pas de tâches - comme Windows Update - avant l'authentification ». Cette option peut être annoncée par le serveur DHCP (RFC 2131 et RFC 8415) ou par le routeur qui envoie des RA (RFC 4861).

Cette option (section 2 du RFC) annonce au client qu'il est derrière un portail captif et lui fournit l'URI de la page d'authentification (ce qui évite d'être détourné, ce qui est grave quand on utilise HTTPS). Dans cet URI, le serveur HTTP doit être désigné par son adresse IP, pour éviter d'avoir à faire du mensonge DNS.

Les sections 2.1, 2.2 et 2.3 de notre RFC donnent le format de l'option en DHCP v4, DHCP v6 et en RA. Le code DHCP v4 est 160 <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml#options> (qui était malheureusement squatté, ce qui a nécessité son changement dans le RFC 8910), le DHCP v6 est 103 <https://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2> et le type RA est 37 <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-5>.

La section 4 de notre RFC étudie les conséquences de cette option pour la sécurité. Elle rappelle que DHCP et RA ne sont pas sécurisés, de toute façon. Donc, un méchant peut envoyer une fausse option « il y a un portail captif, allez à cet URI pour vous authentifier » mais le même méchant peut aussi bien annoncer un faux routeur...

Il est même possible que cette option nouvelle améliore la sécurité, en n'encourageant pas les utilisateurs à couper les mécanismes de validation comme la vérification des certificats, contrairement à ce que font les portails captifs actuels.

Pour DHCP, la plupart des serveurs permettent de servir une option quelconque, en mettant ses valeurs manuellement et une future mise à jour ne servira donc qu'à rendre l'usage de cette option plus simple. Autrement, il n'existe pas encore de mise en œuvre côté clients DHCP ou RA. (Pour des nouvelles plus récentes, voir le RFC 8910.)