RFC 7824 : Privacy considerations for DHCPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 juin 2016

Date de publication du RFC : Mai 2016

https://www.bortzmeyer.org/7824.html

Le protocole DHCP sert à transmettre à une machine qui vient de se connecter au réseau, des informations utiles pour sa connexion. Il est surtout connu pour son utilisation avec IPv4 mais DHCP existe aussi pour IPv6 (il est normalisé dans le RFC 8415 [1]). Comme son équivalent IPv4, DHCP pour IPv6 pose un certain nombre de problèmes de vie privée, que ce RFC explore.

Il fait donc partie de la série de RFC développés après le RFC 6973 et, surtout, après les révélations de Snowden qui ont mené l'IETF à s'engager plus vigoureusement <https://www.bortzmeyer.org/ietf-securite-espionnage-bis.html> contre la surveillance massive. Ce RFC ne propose pas de solutions (elles sont décrites dans le RFC 7844), il décrit le problème.

Le problème fondamental est le même qu'en IPv4 (RFC 7819) : le client DHCP, lorsqu'il vient de se connecter à un réseau et émet des requêtes, publie des informations trop détaillées, dont certaines sont des véritables identificateurs stables (cf. section 2 de notre RFC), permettant au serveur DHCP, mais aussi à toute machine qui écoute le réseau, de suivre à la trace une machine donnée. Au contraire des solutions comme SLAAC, où le client est purement passif, DHCP impose au client d'annoncer son existence et de donner des informations. Bref, si vous avez déjà lu le RFC équivalent pour IPv4, le RFC 7819, vous n'apprendrez pas grand'chose de nouveau.

La section 3 du RFC donne une liste aussi complète que possible des options DHCPv6 qui peuvent servir à la surveillance. D'abord, l'adresse IP source. Bon, elle ne fait pas partie de DHCP à proprement parler et tout protocole va la publier, puisqu'elle apparait dans tous les paquets émis. (Dans le cas de DHCP, la requête du client est émise depuis une adresse locale au lien, "*link-local*", celles qui commencent par `fe80::`.) Néanmoins, l'adresse IP source mérite une mention car certains mécanismes de

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8415.txt`

génération d'une adresse IPv6 peuvent poser des problèmes de vie privée (cf. RFC 7721). Il faut donc utiliser des mécanismes comme ceux du RFC 8981 ou du RFC 7217.

L'exemple suivant est celui d'une option particulièrement dangereuse pour la vie privée, "*Client Identifier*", qui envoie au serveur le DUID ("*DHCPv6 Unique Identifier*", RFC 8415, section 11) du client. Comme son nom l'indique, il identifie chaque machine de manière unique et, par défaut, il est stable. La méthode la plus courante pour le générer est d'utiliser l'adresse MAC, elle-même un identificateur unique et stable. Même si on prend la précaution de changer l'adresse MAC, le DUID ne change pas. C'est donc un excellent moyen de suivre une machine, cassant complètement la sécurité de techniques comme celle du RFC 8981.

Également dangereuse, l'option "*Client FQDN*" (RFC 4704) qui envoie un FQDN.

Certaines options peuvent être moins clairement indiscrètes mais peuvent néanmoins révéler indirectement l'identité du client. C'est le cas de l'option "*Option Request*" qui dit au serveur quelles options on souhaiterait qu'il utilise. Cette liste de choix peut servir à distinguer entre plusieurs clients DHCP : toutes les fois où il y a un choix dans un protocole, il y a une possibilité de "*fingerprinting*".

Certaines options n'envoient pas directement un identificateur unique mais envoient de l'information sur une classe à laquelle appartient la machine. Par exemple, les options "*Vendor Class*" et "*Vendor-specific Information*" (sections 21.16 et 21.17 du RFC 8415), ou encore l'option "*Client System Architecture*" (RFC 5970), indiquent le matériel et le logiciel du client.

On n'a vu ici que des options allant du client vers le serveur mais l'inverse existe aussi, et certaines options qu'un serveur peut envoyer sont révélatrices (par exemple "*Civic Location*", RFC 4776). Mais les problèmes de vie privée du serveur sont moins graves que ceux du client et notre RFC passe donc rapidement (voir aussi la section 5.3).

En dehors des options DHCP, certains mécanismes utilisés dans le cadre de DHCP peuvent être bien indiscrets. C'est par exemple le cas de la demande d'adresses temporaires (RFC 8415, section 6.5), pourtant bien intentionnée. Le but était de pouvoir obtenir des adresses qui ne soient pas stables, pour minimiser justement les risques pour la vie privée. Le RFC détaille les nombreux problèmes et pièges que récèle ce mécanisme. Mais le principal problème est que la seule demande de ces adresses, visible par tout surveillant, est déjà très révélatrice ! Cela revient à sa promener avec une cagoule sur sa tête pour préserver sa vie privée.

Autre mécanisme qui peut être révélateur, la mise à jour du DNS que font certains serveurs DHCP. Si le nom utilisé est stable (cf. l'option "*Client FQDN*" mentionnée plus haut), tout surveillant ayant accès au DNS (c'est-à-dire tout le monde) pourra suivre les changements d'adresse IP de la machine, connaissant ainsi ses déplacements d'un réseau à l'autre.

Les stratégies d'allocation d'adresses du serveur DHCP peuvent également être dangereuses pour la vie privée. Le serveur DHCP dispose d'une certaine plage d'adresses. S'il alloue les adresses en commençant toujours par la plus basse adresse libre, les adresses attribuées vont être assez prévisibles, ce qui n'est en général pas bon pour la discrétion. (Et ce mécanisme, qui a certes l'avantage d'être simple et rapide, tend à concentrer les adresses allouées au début de la plage.) Autre possibilité, allouer des adresses fixes (le même client - identifié par une option comme "*Client Identifier*" - a toujours la même adresse IP). C'est évidemment très pratique pour l'administrateur du réseau local. Mais c'est la pire solution pour la vie privée, puisque cela oblige le client à divulguer son identité, et cela permet même aux serveurs extérieurs de le suivre à la trace lorsqu'il communique avec eux avec son adresse fixe. Pour la

vie privée, la meilleure stratégie d'allocation est sans doute le tirage au sort parmi les adresses libres de la plage.

Maintenant qu'on a vu les vulnérabilités de DHCPv6, voyons ce qu'un attaquant peut en faire (section 5 du RFC). D'abord, il peut découvrir le type de machine chez le client (matériel et/ou logiciel), ce qui peut être utile, par exemple pour sélectionner une attaque spécifique à un système d'exploitation, ou bien, si le matériel/logiciel utilisé est rare, pour identifier un client particulier. Cette information sur le type de machine peut être trouvé dans l'adresse MAC (les premiers octets identifient le vendeur), dans les identificateurs dérivés de l'adresse MAC, ou dans les options comme "*Vendor Class*".

L'espion peut également utiliser ces faiblesses de DHCPv6 pour identifier les réseaux visités précédemment (je n'en ai pas parlé plus haut, mais il existe une option qui indique la précédente adresse IP utilisée : elle est pratique pour obtenir une adresse stable, mais elle est indiscrète).

Plus généralement, le surveillant peut essayer de découvrir une identité stable, lui permettant de savoir combien de machines utilisent ce serveur DHCP, et lui permettant également de corréler deux machines sur deux réseaux, découvrant qu'il s'agit en fait de la même. Le DUID est particulièrement sensible ici.

Le surveillant peut ainsi suivre une machine, soit dans le temps (toutes ses activités en un réseau donné), soit dans l'espace (suivre à la trace un engin mobile).

Si le surveillant a les moyens d'une agence d'un État riche (par exemple si le surveillant est la NSA), il peut effectuer une surveillance massive très efficace (RFC 7258). Il est par exemple conceptuellement aisé de bâtir une liste de très nombreuses machines, en observant beaucoup de réseaux : les failles de sécurité de DHCPv6 citées dans ce RFC permettront de reconnaitre chaque machine individuelle. Ainsi, un organisme comme la NSA peut se faire une base de données permettant de répondre très vite à des questions du genre « où était `38:59:f9:7d:b6:47` la dernière fois qu'on l'a vu ? »

Enfin, la section 6 de notre RFC rappelle une triste réalité : en sécurité, il faut en général faire des compromis. Ici, le RFC note que toute authentification du client va à l'encontre du souhait de préserver la vie privée. Ce genre de choix (sécurité de son réseau, ou bien vie privée des utilisateurs) est bien embêtant pour l'administrateur système.