RFC 9724 : Randomized and Changing MAC Address State of Affairs

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 mars 2025

Date de publication du RFC : Mars 2025

https://www.bortzmeyer.org/9724.html

Dans le contexte de la surveillance massive qui s'exerce contre les utilisateurices de l'Internet, tout identifiant un peu stable peut être utilisé pour pister quelqu'un. On en laisse, des traces ! C'est par exemple le cas avec l'adresse MAC. Ce nouveau RFC décrit les mécanismes existants pour diminuer le risque de pistage par l'adresse MAC. Il ne spécifie pas un protocole, il liste les solutions.

Ne croyez donc pas les médias et les politiciens qui vous diraient que le problème de l'Internet, c'est l'anonymat. C'est tout le contraire : il est extrêmement difficile d'utiliser l'Internet sans laisser de traces partout, traces qui peuvent être corrélées si on réutilise un identifiant, comme l'adresse MAC (dite également adresse Ethernet ou bien adresse physique).

(Au passage, le RFC contient une remarque très désagréable comme quoi l'une des causes des problèmes de vie privée serait « le manque d'éducation [des utilisateurices ?] ». S'il est vrai que la littératie numérique en matière de sécurité est très perfectible, il ne faudrait pas pour autant tout rapporter à l'ignorance. Les utilisateurices ne sont pas responsables de la surveillance massive, dont l'ubiquité et la sophistication font qu'il est difficile de se défendre, même pour un·e expert·e. Et les innombrables entreprises et États qui pistent les utilisateurices ne le font pas par ignorance mais cherchent en toute conscience à récolter le maximum de données.)

Le problème du pistage se place à tous les niveaux du modèle en couches ; les adresses MAC en couche 2, les adresses IP en couche 3, les "*cookies*" pour le Web en couche 7, etc. Pour la couche 2, sujet de notre RFC, voyez par exemple l'analyse « "*Wi-Fi internet connectivity and privacy : Hiding your tracks on the wireless Internet*" <https://ieeexplore.ieee.org/document/7390443> » (comme l'IEEE fait partie de ces organisations de normalisation réactionnaires qui ne permettent pas l'accès libre à leurs documents, prenez une copie <https://www.it.uc3m.es/cjbc/papers/pdf/2015_bernardos_cscn_privacy.pdf>), ou bien cet article <https://www.independent.co.uk/life-style/gadgets-and-tech

news/updated-london-s-bins-are-tracking-your-smartphone-8754924.html> décrivant comment les poubelles vous pistent.

Le problème est d'autant plus sérieux qu'aujourd'hui, plein d'équipements électroniques ont la WiFi (en termes plus techniques, IEEE 802.11) et donc une adresse MAC unique, qui peut servir au pistage. On ne pense pas forcément à ces équipements comme étant des ordinateurs, susceptibles d'émettre et donc de révéler leur présence. Quiconque écoute le réseau va voir ces adresses, il n'y a pas besoin d'être actif, une écoute passive suffit. Même sans association avec la base, la machine se signale par les "*Probe Request*" qu'elle envoie. Dans le cas typique, l'adresse 802.11 est composée de deux parties, l'OUI ("*Organizationally Unique Identifier*"), qui identifie le fournisseur, et le "*Network Interface Controller Specific*", qui identifie une des machines (en toute rigueur, plutôt une des interfaces réseau) dudit fournisseur. La combinaison des deux fait une adresse unique (au moins en théorie), traditionnellement attribuée à la fabrication et pas changée ensuite. Cette adresse unique est donc, malheureusement pour la vie privée, un bon identificateur stable. Mais une adresse MAC peut aussi être localement gérée (elle n'est alors plus forcément unique), et, contrairement à ce que croient certaines personnes, l'adresse globale par défaut n'est pas obligatoire. (Un bit dans l'adresse indique si elle est globale ou locale. Le RFC 8948[1] définit même un plan d'adressage pour ces adresses locales.) On peut donc échapper au pistage en changeant d'adresse de temps en temps (cf. l'article de Gruteser et D. Grunwald, « "*Enhancing location privacy in wireless LAN through disposable interface identifiers : a quantitative analysis*" <https://dl.acm.org/doi/10.1145/941326.941334> »). Ces questions de vie privée liées à l'adresse MAC sont décrites plus en détail dans l'article « "*Privacy at the Link Layer*" <https://www.w3.org/2014/strint/papers/35.pdf> », de Piers O'Hanlon, Joss Wright et Ian Brown, présenté à l'atelier STRINT, dont le compte-rendu a été le RFC 7687. Notre RFC rappelle aussi que, bien sûr, la protection de la vie privée ne dépend pas uniquement de cette histoire d'adresse MAC et que les surveillants ont d'autres moyens de pistage, qu'il faut combattre également, cf. section 9.

Un peu d'histoire : l'IEEE, qui normalise 802.11 et donc les adresses MAC, avait pour la première fois traité le problème lors d'un tutoriel <https://mentor.ieee.org/802-ec/dcn/14/ec-14-0043-01-00EC-in pdf> en 2014, qui avait suivi l'atelier STRINT (celui dont le compte-rendu est dans le RFC 7687). Suite à ce tutoriel, l'IEEE avait créé l'"*IEEE 802 EC Privacy Recommendation Study Group*" <http://www.ieee802.org/PrivRecsg/>, ce qui avait finalement donné naissance à des documents IEEE comme "*IEEE 802E-2020 - IEEE Recommended Practice for Privacy Considerations for IEEE 802 Technologies*" <https://1.ieee802.org/security/802e/> et "*802c-2017 - IEEE Standard for Local and Metropolitan Area Networks :Overview and Architecture–Amendment 2 : Local Medium Access Control (MAC) Address Usage*" <https://ieeexplore.ieee.org/document/8016709>. Les idées documentées avaient été testées lors de réunions plénières de l'IEEE et de l'IETF. Ces tests ont montré que les collisions (deux adresses MAC identiques) étaient extrêmement rares. Elles ont aussi permis de constater que certains identificateurs visibles (comme celui envoyé en DHCP, cf. RFC 7819) restent stables et qu'il ne suffit donc pas de changer l'adresse MAC. Je recommande la lecture du rapport « "*IEEE 802E Privacy Recommendations & Wi-Fi Privacy Experiment @ IEEE 802 & IETF Networks¿*" <https://www.ietf.org/proceedings/96/slides/slides-96-edu-ieee802work-3.pdf> », présenté à l'IETF 96 à Berlin <https://www.ietf.org/proceedings/96/> en 2016.

Depuis, l'aléatoirisation des adresses MAC a été largement déployée, sur iOS <https://support.apple.com/en-us/HT211227>, sur Android <https://source.android.com/devices/tech/connect/wifi-mac-randomization-behavior>, sur Microsoft Windows <https://support.microsoft.com/en-us/windows/how-to-use-random-hardware-addresses-in-windows-ac58de34- sur Fedora <https://fedoramagazine.org/randomize-mac-address-nm/>, etc. Il n'y a évidemment pas de solution parfaite et des chercheurs ont déjà trouvé comment contourner l'aléatoirisation <https:

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8948.txt

//arxiv.org/abs/1703.02874>. Cela a mené à une nouvelle norme IEEE, 802.11aq <https://ieeexplore.ieee.org/document/8457463>.

Ce changement de l'adresse MAC a ensuite posé problème à certains opérateurs <https://mentor.ieee.org/802.11/dcn/20/11-20-1117-03-0rcm-rcm-sg-proposed-rcm-csd-draft.docx> de réseaux mobiles. (Voir aussi « *"IEEE 802.11 Randomized And Changing MAC Addresses Topic Interest Group Report"* <https://mentor.ieee.org/802.11/dcn/19/11-19-1442-09-0rcm-rcm-tig-draft-report-odt> » et « *"RCM A PAR Proposal"* <https://mentor.ieee.org/802.11/dcn/20/11-20-0854-07-0rcm-par-p docx> ».)

La question de la vie privée s'est beaucoup posée à l'IETF dans le contexte de l'auto-affectation des adresses IPv6 (SLAAC : *"Stateless Address Autoconfiguration"*). Le RFC 1971 et ses successeurs (le dernier en date est le RFC 4862) prévoyaient que la partie spécifique à la machine de l'adresse IPv6 soit fondée sur l'adresse MAC, ce qui permettait le pistage. Cette méthode, qui a fait couler beaucoup d'encre, est désormais déconseillée (RFC 8064). La méthode recommandée maintenant est celle du RFC 8981, avec ses adresses aléatoires et temporaires. (Elles ont d'autres avantages, comme de limiter la durée pendant laquelle on peut se connecter à une machine depuis l'extérieur.) Évidemment, ces adresses temporaires ne conviennent pas aux serveurs (qui doivent être joignables) ni aux cas où l'administrateur réseau veut pouvoir garder trace des adresses IP des machines (dans ce dernier cas, le RFC 7217, avec ses adresses stables tant qu'on reste dans le même réseau, est la solution recommandée).

On l'a dit, l'adresse MAC n'est pas le seul moyen qu'on a de suivre une machine à la trace. Les identifiants qui figurent dans la requête DHCP en sont un autre. Le RFC 7844 rassemble les recommandations faites aux auteur·es de logiciels DHCP pour limiter ce pistage.

On a donc vu qu'on pouvait changer son adresse MAC et que c'était une bonne chose pour la protection de sa vie privée. Mais la changer pour quoi ? La section 6 de notre RFC résume toutes les politiques possibles :

— Adresse MAC fixe déterminée par le fournisseur (c'est la politique ancienne et traditionnelle) et enregistrée en dur dans l'interface réseau.
— Adresse permanente mais générée localement, sur la machine, typiquement au premier démarrage. On parle de PDGM (*"Per-Device Generated MAC"*).
— Adresse temporaire générée localement, au démarrage de la machine. On parle de PBGM (*"Per-Boot Generated MAC"*). Plus besoin de mémoire stable.
— Adresse fixe générée localement, pour chaque réseau. L'adresse est stockée dans une mémoire stable, indexée par un identificateur du réseau (le SSID pour le Wifi, et diverses heuristiques utilisant par exemple STP pour les réseaux fixes). Cette politique empêche le pistage trans-réseau mais permet une stabilité utile pour l'administrateur du réseau. On parle de PNGM (*"Per-Network Generated MAC"*).
— Adresse temporaire renouvelée régulièrement, par exemple toutes les douze heures. On parle de PPGM (*"Per-Period Generated MAC"*).
— Adresse temporaire par « session ». La session étant par exemple une connexion via le portail captif. On parle de PSGM (*"Per-Session Generated MAC"*).

Que font les systèmes d'exploitation d'aujourd'hui ? La section 7 détaille les pratiques actuelles. Un point important est que, depuis longtemps, tous ces systèmes mettent en œuvre une forme ou l'autre d'aléatoirisation, pour les questions de vie privée citées ici. Comme la situation évolue, plutôt que de lire cette section du RFC, vous avez peut-être intérêt à suivre en ligne <https://github.com/ietf-wg-madinas/draft-ietf-madinas-mac-address-randomization/blob/main/OS-current-practic md>. Au moment de la rédaction de cet article, les versions actuelles d'Android et d'iOS étaient en PNGM (adresse choisie aléatoirement mais liée au SSID). Idem pour Debian et Windows. Mais lisez les détails, qui peuvent dépendre de points subtils.