

Enrichir la communication ou les publicitaires ?

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 octobre 2015

<https://www.bortzmeyer.org/enrichir-qui.html>

Les FAI ne manquent pas d'imagination lorsqu'il s'agit de violer la neutralité du réseau <<https://www.bortzmeyer.org/neutralite.html>>. Un exemple récent est décrit dans l'article de Narseo Vallina-Rodriguez, Srikanth Sundaresan, Christian Kreibich et Vern Paxson, « *Header Enrichment or ISP Enrichment? Emerging Privacy Threats in Mobile Networks* » <<http://www.icir.org/vern/papers/header-enrichment-hotmiddle15.pdf>> », qui consiste à modifier les flux HTTP automatiquement pour ajouter, à l'insu de l'utilisateur, des informations personnelles qui seront utiles aux publicitaires qui gèrent les sites Web. Et cela se nomme cyniquement l'« enrichissement des en-têtes ».

Un exemple de fournisseur de matériel et logiciel qui propose cette technique est Juniper <http://www.juniper.net/techpubs/en_US/junos-mobility11.4/topics/concept/httphe-mobility-overview.html> mais il y en a plein d'autres qui fournissent aux FAI sans scrupules des moyens de modifier les flux HTTP (HTTPS, pour l'instant, protège contre ces manipulations).

Est-ce que cette pratique est répandue? On sait que, dans le monde de l'accès Internet par mobile, la neutralité du réseau est violée bien plus souvent (ce qui explique les campagnes marketing répétant en boucle que bientôt, X % des accès Internet seront par un mobile : il est important de convaincre les utilisateurs de passer à des technologies où la triche est plus fréquente). Avec quelle ampleur? Les auteurs de l'article ont utilisé l'application Netalyzer <<http://netalyzer.icsi.berkeley.edu/>> pour récolter des données à ce sujet. Sur les 300 opérateurs mobile identifiés, 5 ajoutent des en-têtes qui compromettent la vie privée de l'utilisateur, 6 ajoutent des en-têtes qui permettent de suivre un utilisateur à la trace (remplaçant les "cookies" désormais trop bien connus des utilisateurs), 24 mettent des informations techniques dans ces en-têtes, informations qui peuvent mener également à des problèmes de vie privée (cf. RFC 7239¹).

Inutile de dire que la majorité des opérateurs en question sont situés dans les pays du Sud, où la vigilance des citoyens et leurs connaissances techniques sont plus faibles : nettement moins de chances de se

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc7239.txt>

faire prendre en Jordanie qu'en Californie! Orange Jordanie fait partie des « enrichisseurs d'en-têtes » et ajoute le numéro de téléphone du client aux en-têtes HTTP qui seront récupérables par les publicitaires sur le site Web visité! L'en-tête utilisé est `msisdn:`. (Notez que la documentation de Juniper citée plus haut utilisait exactement cela comme exemple, avec juste le préfixe `x-` qui indique traditionnellement qu'il s'agit d'un en-tête non standard.)

Le record appartient apparemment à Vodafone Afrique du Sud pour publier dans les en-têtes ajoutés le numéro de téléphone et l'IMEI (depuis la parution de l'article, ils semblent avoir arrêté).

Si la signification de l'en-tête ajouté subrepticement est parfois évidente (comme `msisdn:`, "*Mobile Subscriber ISDN*", cité plus haut), ce n'est pas toujours le cas. Par exemple, Verizon met un en-tête `x-uidh:` qui semble dédié au traçage : il est unique par abonné.

Enfin, il y a les en-têtes techniques, indiquant les logiciels utilisés pour cette opération. En France, SFR ajoute ainsi des `x-bluecoat-via:` (cf. la page Wikipédia sur cette sympathique entreprise), et des `x-nokia-gateway-id:`. Très souvent, l'opérateur (par exemple Bouygues et SFR en France) ajoute un `x-forwarded-for:` (en-tête depuis remplacé par un en-tête standard, cf. RFC 7239) qui indique l'adresse IP privée et peut aider au traçage d'un utilisateur. Sans compter les en-têtes mystérieux comme le `x-vfstatus:` chez SFR.

Bref, cet excellent travail de recherche montre que la neutralité de l'Internet <<https://www.bortzmeyer.org/neutralite.html>> n'est pas un problème abstrait : elle est violée tous les jours, et il est donc crucial qu'elle soit défendue.