RFC 4882 : IP Address Location Privacy and Mobile IPv6: Problem Statement

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 juin 2007

Date de publication du RFC : Mai 2007

https://www.bortzmeyer.org/4882.html

La protection de la vie privée sur Internet suscite de plus en plus d'intérêt à l'IETF, d'autant plus que certaines techniques comme la **mobilité** peuvent aggraver la diffusion d'informations confidentielles. Notre RFC explique le problème.

Lorsqu'une machine A correspond avec une machine B, celle-ci apprend l'adresse IP de A, c'est inévitable. B apprend aussi beaucoup d'autres choses (par exemple via les "*cookies*" Web) qui, mises ensemble, peuvent représenter une sérieuse menace pour la vie privée. Dès qu'on cherche un peu, on est étonné du nombre de moyens qu'il existe pour détecter des choses que le correspondant voulait cacher. Par exemple, l'analyse du temps de réponse du correspondant peut donner une idée de la distance, et donc permettre de savoir quand un portable a quitté son « port d'attache ».

En effet, dans le cas de la mobilité IP, de nouvelles vulnérabilités apparaissent. La mobilité « traditionnelle » où la machine en déplacement (on parle de MN pour "*Mobile Node*") acquiert une nouvelle adresse IP à chaque réseau visité, typiquement par DHCP, avait déjà ses propres dangers. Si le correspondant du MN, le CN ("*Corresponding Node*"), peut découvrir un invariant du MN (par exemple un "*cookie*" Web envoyé ou, de manière plus sophistiquée, une signature du comportement de l'horloge <http://www.cl.cam.ac.uk/~sjm217/#talk-ccc06hotornot> de la machine, le CN peut littéralement suivre à la trace le MN et déterminer sa position approximative, comme si votre téléphone GSM révélait à vos correspondants votre position !

La mobilité IPv6, décrite dans le RFC 3775[1], a deux modes de fonctionnement, le mode « normal » ("*reverse tunneling*") où tout le trafic passe par un routeur sur le réseau principal du MN (et où le CN ne voit donc pas l'actuelle adresse IP du MN, la « care-of address ») et un mode « optimisé » où le passage par le routeur « de la maison » ("*Home Agent*") n'est plus obligatoire et qui retrouve donc le même inconvénient qu'avec DHCP pur. Chacun de ses deux modes a ses propres défauts pour la protection de la vie privée et notre RFC les détaille. La section 4 est particulièrement vivante dans son exposé des risques qui guettent le malheureux utilisateur d'un PC portable.

Notre RFC ne propose pas de solution, il explique les problèmes à résoudre et donne une idée des compromis qu'il faudra sans doute faire.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3775.txt