HTTPS : la sécurité pour tous, mais à quel prix ?

	**HTTPS : la sécurité pour tous, mais à quel prix ?**

Réseaux : Plusieurs chercheurs ont présenté lors des conférences ACM CoNext à Sidney le résultat de leurs recherches sur le coût et les implications du déploiement de HTTPS. Un gain de sécurité pour l'utilisateur mais un choix qui implique d'envisager les conséquences.

Face aux écoutes de la NSA, les principaux constructeurs et acteurs du numérique semblent au moins tous d'accord sur un point : il faut tout chiffrer. Non pas que cela vous sauvera immédiatement des grandes oreilles de la NSA, qui est peut être déjà arrivé à bout des algorithmes de chiffrement les plus pointus, mais cela aura au moins un mérite : celui d'augmenter le « coût de la surveillance » pour les importuns, compliquer la tache des Five Eyes afin de décourager l'espionnage à grande échelle de nos communication.

Quel est le prix du S dans HTTPS ?

Chacun y va donc de son petit chiffrement mais pour le web, en attendant un http/2 qui se fait désirer, la plupart des principaux sites web ont progressivement basculé au déploiement de HTTPS, une couche de chiffrement sécurisant les connexions web. Mais quel est le coût réel de cette sécurité ? C'est la question que se sont posée plusieurs chercheurs de l'université de Carnegie Mellon, de Telefonica ou de l'école polytechnique de Turin.

Déployer le HTTPS suppose tout d'abord des coûts financiers non négligeables à travers l'achat et le maintien de certificats : l'étude se base sur les tarifs de Symantec mais les offres dans le domaine sont extrêmement variables en fonction du prestataire et des services associés. Mais plus que la question financière, c'est celle des performances qui intéresse les chercheurs.

L'utilisation de HTTPS présente plusieurs désavantages : tout d'abord une augmentation, minime mais sensible, de la latence et du temps nécessaire au chargement d'une page. Si celle-ci varie beaucoup en fonction de nombreux facteurs, les chercheurs constatent néanmoins une augmentation du temps de réponse, parfois de plus de 300ms. Un cout de performance « pas si négligeable que cela », rappellent les auteurs de l'étude, qui rappellent que chaque seconde compte pour les internautes.

Un réseau opaque

Si l'impact sur la batterie est jugé mineur, le déploiement du HTTPS pourrait en revanche se retourner contre les opérateurs en compliquant l'utilisation de solutions reposant sur le Deep Packet Inspection. Certes, c'est plus ou moins le but initial puisque le Deep Packet Inspection est utilisée par des applications de surveillance, mais cette technologie permet également à un opérateur de lutter contre le spam ou les attaques ddos.

Le DPI a mauvaise presse et cela se comprend, mais si le déploiement du HTTPS se poursuit, comme le supposent les auteurs de l'étude, alors les opérateurs vont devoir envisager de nouvelles solutions pour lutter contre ces problèmes. Moins polémique mais peut être plus problématique encore : le HTTPS empêche par exemple les opérateurs et fournisseurs d'accès d'avoir recours à du caching pour épargner leur bande passante.

Pourtant, malgré les problèmes relevés par l'étude, les chercheurs restent confiant et s'attendent à voir HTTPS de plus en plus présent au cours des années à venir : « le S est là pour rester » concluent ils, et ce malgré les désavantages liés au chiffrement sur les connexions web. Reste donc à trouver un moyen de minimiser l'impact, peut être grâce à http/2, dont les premières spécifications sont attendues cette année.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/https-la-securite-pour-tous-mais-a-quel-prix-39810969.htm
Par Louis Adam