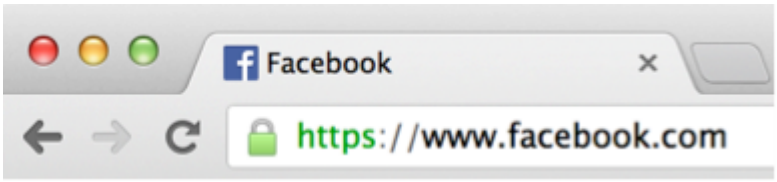
Facebook : tout le monde sous https !

« *Nous utilisons désormais https par défaut pour tous les utilisateurs de Facebook* ». C'est en ces termes que **Scott Renfro**, ingénieur infrastructure, a annoncé sur le blog de Facebook que le réseau social et donc ses utilisateurs ne communiqueraient plus sur les navigateurs que sous protocole https.



Le protocole – qui exploite la technologie TLS (*Transport Layer Security*), aussi appelée SSL (*Secure Sockets Layer*) – est disponible en option sur Facebok depuis deux ans, et utilisé par environ 35 % des membres du réseau. Il s'impose désormais à tous.

https obligatoire pour 'presque' tous

Rendu obligatoire, le protocole concerne désormais tout le trafic sur www.facebook.com… pardon, https://www.facebook.com, et 80 % du trafic m.facebok.com. Les utilisateurs des applications Facebook natives sur Android et iOS (iPhone et iPad) se connectent déjà sous ce protocole, les autres OS mobiles reconnus par Facebook sont à la traine !

En procédant ainsi, Facebook impose à ses membres une nouvelle couche de sécurité reconnue, tant pour leur connexion via un navigateur qu'avec la majorité des mobiles. De quoi assurer une meilleure isolation des membres vis-à-vis de pratiques provenant de pages douteuses. Evoluant vers des services de plus en plus personnalisés, voire intrusifs, Facebook s'offre une marge de sécurité pour l'avenir.

Facebook et la sécurité de demain

Facebook travaille également sur l'implémentation d'autres protocoles ou modules de sécurité :

- Les **clés RSA 2048-bit** associé aux sessions TLS, planifiées pour la fin 2013;
- **Elliptic Curve Cryptography**, de nouvelles clés cryptographiques asymétriques et de petite taille qui sont supportées par les dernières versions de navigateurs;
- Les clés d'échange **ECDHE** (Elliptic Curve Ephemeral Diffie-Hellman), qui exploitent une clé éphémère à chaque session TLS dans une approche nommée Perfect Forward Secrecy;
- L'identification du certificat du serveur **Certificate Pinning**, un mécanisme introduit à l'origine sur Chrome 13, et que Facebook va étendre à ses applications mobiles, et probablement sur les navigateurs.
- **HSTS** (*HTTP Strict TransportSecurit*y), un jeu d'instruction qui permet au navigateur de n'interagir qu'avec des sites exploitant des connexions https, ce qui devrait permettre de supprimer le https opt-out, c'est à dire les connexions https imposées contre la volonté de l'abonné, par opposition à l'opt-in qui demande préalablement l'autorisation de l'utilisateur.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes