TextSecure

Genma

13 octobre 2014

À quoi sert TextSecure ?

C'est un logiciel de messagerie instantanée, conçu pour être très simple d'usage, pour servir de remplaçant « tel quel » aux logiciels SMS actuels, tout en offrant une meilleure protection de la vie privée, dans certains cas.

- TextSecure remplace l'application SMS par défaut.
- TextSecure offre un bon compromis entre facilité d'usage et sécurité.

TextSecure du point de vue utilisateur

L'utilisateur s'en sert comme de l'outil SMS par défaut.

Le principal changement est que certains messages vont être marqués d'un cadenas :

- si le correspondant utilise également TextSecure, les messages sont chiffrés automatiquement avec sa clé.

Si on est simple utilisateur, on a donc un peu plus de vie privée, et on en aura de plus en plus au fur et à mesure que TextSecure se répand.

Comment fonctionne TextSecure ?

TextSecure peut utiliser deux transports différents le SMS et la liaison « données » du smartphone (ce second transport se nomme PUSH dans la terminologie TextSecure, et est utilisé par défaut pour les correspondants qui ont également TextSecure).

Le mode PUSH peut être intéressant si on a un quota SMS limité mais pas en Internet, et le mode SMS dans le cas contraire.

Les messages apparaissent en vert traditionnel quand ils ont été transportés en SMS et en bleu autrement.

Chiffrement de tous les SMS

TextSecure peut aussi chiffrer toute la base des SMS reçus et stockés. Ainsi, même si on vole votre téléphone, vos communications resteront sûres.

Attention : si vous oubliez la phrase de passe, tout est fichu. Pensez à sauvegarder.

Les limites de TextSecure

Lles métadonnées de la communication sont en clair. Des tiers peuvent donc savoir qui écrit à qui et quand, même si le contenu des messages est chiffré.

Les metadata sont connues d'OpenWhispe, si on utilise PUSH

ou de l'opérateur mobile, si on utilise le SMS traditionnel.

Peut-on faire confiance à TextSecure ?

TextSecure est un logiciel libre : le code est disponible, et des experts en sécurité l'ont déjà lu et personne n'a encore trouvé de défaut significatif.

Le code du serveur utilisé par OpenWhisper est également disponible en ligne.

Mais cela s'avère moins utile car on ne peut pas vérifier que le serveur effectif exécute bien ce code.

Comment valider sa correspondance ?

À la première communication, TextSecure fait confiance, c'est un système, dit TOFU (Trust On First Use), qui a l'avantage d'être trivial d'utilisation.

Si le correspondant réinitialise sa clé mais, d'après la documentation, TextSecure vous prévient.

Si on veut, on peut toujours vérifier, lors d'une rencontre AFK, la clé de son correspondant, soit en la lisant à l'écran, soit via des codes QR.

Les limites de TextSecure

Aucun moyen d'enregistrer le fait qu'on a vérifié, afin, par exemple, d'afficher les messages ultérieurs d'une couleur différente si le correspondant a ainsi été solidement authentifié.

On ne peut pas envoyer un message à plusieurs personnes simplement (il faut d'abord créer un groupe statique).

En savoir plus ?

Pour aller plus loin, la société qui développe TextSecure, OpenWhisper, a une bonne FAQ.