Migration massive de compte vers l'application Signal.

ATTENTION LIRE TOUT l'ARTICLE AVANT d'INSTALLER SIGNAL

Qu'est ce que Signal ?

Signal c'est une application de messagerie soit en paire soit en groupe. Egalement elle permet de remplacer l'application de messagerie SMS et MMS.

La confidentialité en point fort.

Signal est considéré par de nombreux experts en sécurité informatique comme une excellente, pour ne pas dire la meilleure application gratuite en matière de confidentialité : chiffrement très robuste et PAR DEFAUT de tous les contenus échangés quand d'autres l'ont en OPTION. Ce chiffrement ou encodage masque tout accès extérieur au contenu des échanges.

De ce fait le contenu d'une discussion devient indéchiffrable sur les serveurs qui hébergent l'application et même par les développeurs qui la gère. Aucune réquisition gouvernementale ne peut faire que vos données deviennent accessibles.

> Si nous comparons avec Telegram, présentée aussi comme sécurisée, nous voyons que par défaut le chiffrement des discussions des utilisateurs n'est pas fait discussion par discussion (aux deux extrémités) idem pour Facebook Messenger.

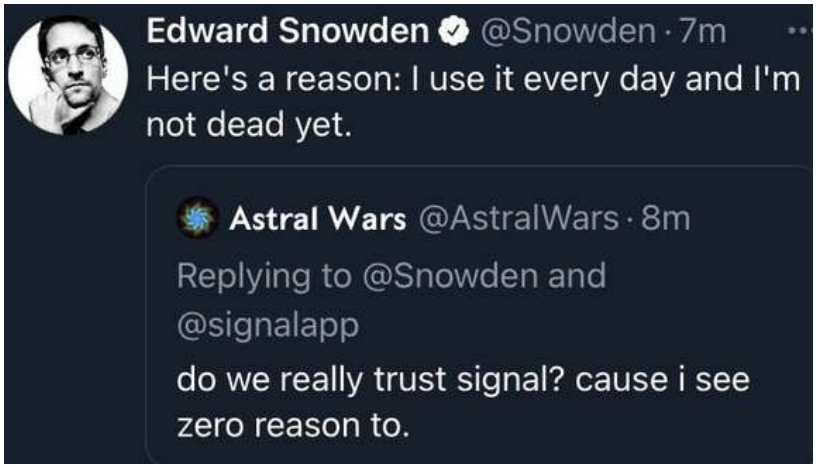
Autres avantages

Outre de remplacer les SMS et MMS en les sécurisant un autre plus de Signal l'autodestruction des messages échangés après un temps à choisir de quelques minutes ou quelques secondes.

Est-ce bien exact ?

La théorie c'est bien et constatons en pratique (une référence !) le lanceur d'alerte Edward Snowden, qui a dénoncé l'espionnage systématique des conversations faite par les services secrets américains déclarait *utiliser depuis 2015 ce qui l'a bien protégé*.

Des ONG et collectifs de journalistes (comme l' ICIJ qui enquête sur des sujets sensibles) recommandent aussi SIGNAL pour le respect de la vie privée et le secret des sources.



Des améliorations en vue

Même améliorable à date (01/2020) Signal mérite d'être adoptée.

Les idées pour améliorer serait une alternative à l'architecture *« centralisée » et qu'en bout elle* utilise le numéro de téléphone de l'utilisateur en identifiant unique. Sur ce point une alternative serait – une solution alternative pour ce dernier point est en cours de développement. Ceux sont des choix initiaux explique le créateur de Signal, Moxie Marlinspike, c'était le prix à payer pour créer cette solution assez pour qu'elle puisse être utilisée par plus de monde.

Autre point à améliorer c'est où stocker les contacts des utilisateurs qui sont chiffrés sur les serveurs de l'organisation. C'est en effet une (très modeste) vulnérabilité supplémentaire **si à l'installation de signal en place de code à 4 numériques vous utilisez un vrai mot de passe codé… ce que je vous recommande vivement.**