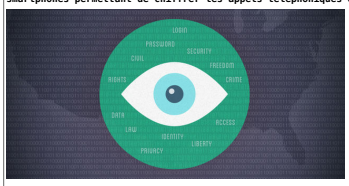
Des communications téléphoniques sécurisées avec Signal

Des communications téléphoniques sécurisées avec Signal

A 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.



À 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.

Les communications entre deux appareils équipés de Signal passent par l'Internet ouvert, mais restent indéchiffrables pour tout observateur extérieur. N'importe quel possesseur de smartphone peut ainsi disposer, sans formalités ni inscription, d'un service naguère réservé aux chefs d'Etat, aux PDG de multinationales et aux agents secrets.

La nouveauté de Signal est que l'on n'a pas besoin d'être un « geek » pour s'en servir : une fois l'application chargée, tout se fait automatiquement. « Les systèmes précédents en demandaient trop aux utilisateurs, relève Frédéric Jacobs. C'est pour ça que jusqu'à présent, le grand public a très peu utilisé le chiffrement. » Il fait allusion à PGP (Pretty Good Privacy), inventé il y a 25 ans par l'Américain Philip Zimmermann, pionner mondial du chiffrement sur Internet.

PALLIER LA DIFFICULTÉ DU CHIFFREMENT

Outre la facilité d'utilisation, l'autre objectif prioritaire de Signal était de proposer un chiffrement intégral, de bout en bout. « Le cryptage et le décryptage se font à l'intérieur de votre téléphone, explique Frederic Jacobs. Quand vous chargez l'application, elle crée automatiquement une centaine de clés de chiffrement, qui restent stockées dans l'appareil. »

Le système permet une rotation systématique : « Chaque clé servira une seule fois. Quand vous recevez un message, vous utilisez une clé qui se détruira aussitôt, et quand vous envoyez un message, l'application crée une nouvelle clé. De cette façon, si un attaquant voulait casser le chiffrement de vos communications, il serait obligé de recommencer le travail pour chaque message. Et s'il s'emparait d'une clé, il ne pourrait pas lire vos vieux messages. »

Frédéric Jacobs travaille avec deux développeurs américains installés à San Francisco : Moxie Marlinspike, un vétéran du chiffrement sur mobile qui a vendu sa première startup à Twitter, et Lilia Kai, ex-militante de l'Electronic Frontier Foundation, association de défense des libertés numériques. Au total, l'équipe permanente de Signal se compose de cinq personnes. Elle est financée par des fondations américaines engagées dans la défense des libertés sur Internet, notamment la Freedom of the Press Foundation et l'Open Technology Fund.

Le budget reste serré, et les salaires modestes. Pour gagner correctement sa vie, Frederic Jacobs travaille comme consultant informatique pour des entreprises. A court terme, cet arrangement le satisfait : « A aucun moment je n'ai pensé à m'enrichir grâce à Signal. Auparavant, j'ai travaillé dans des startups, mais j'ai vite été dégoûté par l'ambiance. Aujourd'hui, je fais partie d'une organisation libérée de l'influence perverse de l'argent. Et rassurez-vous, nous n'allons pas nous vendre à Google. »

UN LARGE PUBLIC EN ALLEMAGNE ET AUX ÉTATS-UNIS

En ces temps d'état d'urgence et de guerre contre le terrorisme, les créateurs de logiciels de chiffrement se sont fait des ennemis puissants, depuis le directeur du FBI jusqu'au premier ministre britannique. De plus en plus, les responsables politiques et policiers exigent que les développeurs créent des backdoors (portes de derrière), par exemple des systèmes permettant de récupérer les clés de chiffrement d'utilisateurs visés par des enquêtes.

Frederic Jacobs assure que Signal ne possède aucune backdoor, et qu'il peut le prouver : « Notre code est en open source, disponible librement sur Internet. Tous les experts peuvent l'analyser et le décortiquer à loisir. » Il affirme aussi qu'à ce jour, Signal n'a subi aucune pression, officielle ou autre : « Personne n'est venu nous voir, peut-être parce que nous sommes encore peu connus. »

Signal ne donne pas de chiffre précis sur son nombre d'utilisateurs, mais l'application a été chargée plusieurs millions de fois. Les plus gros contingents sont aux Etats-Unis et en Allemagne : « Signal a été adopté par des hauts fonctionnaires, y compris à Washington, mais aussi par des familles ordinaires qui veulent protéger les communications de leurs enfants, ou des jeunes couples qui s'échangent des photos intimes… »

Signal dispose de dizaines de relais sur tous les continents. Fin décembre, les principaux se trouvaient aux Etats-Unis (côte est et côte ouest), en Allemagne, en Irlande, au Brésil, en Australie et à Singapour : « Leur nombre exact varie en fonction des besoins, explique Frederic Jacobs, ce sont des serveurs ordinaires, qui se louent à la minute. Si par exemple, le trafic est important en Allemagne vers 17 heures, nous ajoutons des relais locaux, et s'il baisse à 18 heures, nous en retirons. »

Signal possède aussi un serveur central, installé aux Etats-Unis, qui envoie les notifications aux appareils avant un appel. De ce fait, le système n'est pas complètement invulnérable. Si un attaquant réussit à avoir accès à un serveur, par effraction ou lors d'une perquisition, il ne pourra pas déchiffrer le contenu des messages, mais pourra s'emparer des informations techniques dont le réseau a besoin – origine et destination des messages, date et durée des appels… En ce sens, Signal n'a pas été pensé pour les lanceurs d'alerte qui doivent rester totalement inconnus des autorités.

Pour le reste, les cryptologues célèbres qui ont audité le code de Signal se sont dit impressionnés par sa qualité. La consécration la plus éclatante vient de Philip Zimmermann qui travaille aujourd'hui pour Silent Circle, société américaine offrant un service payant de chiffrement des communications, dont le siège social est en Suisse depuis 2014. Créée par des anciens membres des commandos d'élite de l'US Navy et visant une clientèle haut de gamme, ainsi que les militaires et les humanitaires en mission, Silent Circle, pour les messages-texte, a abandonné son ancien protocole de chiffrement, et a adopté celui de Signal.

Réagissez à cet article

Source : *Signal, une application pour téléphoner de manière sécurisée*