Sécurité du téléphone: 3 - Communication sécurisée

Contenu transféré depuis la base: Sécurité du téléphone: 3 - Communication sécurisée

Préambule

Ce guide est le dernier d'une série de trois. Avant de le lire, assurez-vous d'avoir :

- lu le 1 : protéger son téléphone face aux services de police et de justice
- lu le 2 : protéger son téléphone du traçage

> **Menace type :** en amont d'une action, la police, les entreprises adverses... travaillent avec les opérateurs mobiles et les compagnies d'internet pour rassembler des preuves sur les membres de l'équipe et/ou saboter et/ou surveiller l'action.

Même si on a chiffré le contenu de nos téléphones, et que l'on s'assure de ne copier aucune donnée vers un cloud comme iCloud ou Dropbox, nous diffusons des informations chaque fois que nous communiquons via notre appareil. Lorsque que nous sommes sur WiFi, nous utilisons un routeur local et les infrastructures du fournisseur d'accès internet (FAI) auxquelles le routeur est connecté. Lorsque nous utilisons le réseau mobile, nous communiquons via une antenne à une tour relais, qui est reliée à un opérateur mobile.

Si nous passons un appel, les données transitent sur le réseau vers l'opérateur du destinataire. Sans un chiffrement suffisant, sur les dizaines d'appareils qui composent l'itinéraire, le contenu peut être enregistré à chaque étape. L'appel relie deux cartes SIM qui sont deux points identifiables. Si nous échangeons via un chat, les données vont du réseaux à une plateforme comme Facebook Messenger, Twitter ou Mattermost, sur laquelle les données sont sauvegardées et ensuite téléchargées par le(s) destinataire(s). Dans le cas du chat, les données vont d'un compte à un autre avec des données d'identification pour chaque compte.

> :information_source: Les téléphones ont fait leurs preuves sur les actions et sont extrêmement avantageux pour la coordination, la photographie, le témoignage en direct des violences policières... C'est parfaitement normal de vouloir en prendre un. Mais attention : un téléphone non chiffré est extrêmement critique. Les données, facilement accessibles, peuvent être utilisées pour incriminer les personnes de l'équipe présentes dans vos contacts. Assurez-vous d'avoir suivi la procédure pour protéger son téléphone face au service de police et la justice si vous voulez bénéficiez des avantages du téléphone en action. On rappelle qu'il n'est pas important que tout le monde ait son téléphone et il est plus sûr de ne désigner que quelques personnes qui en aient. Sur le terrain, il est alors préférable de favoriser la communication via des messagers et des signes. Il faut toujours considérer que le téléphone peut être saisi et que vous pourriez ne pas le revoir.

Sécurisé ou non-sécurisé : savoir où se trouve la frontière

La séparation entre vie personnelle et vie militante est souvent floue et elle l'est aussi dans l'utilisation de nos plates-formes, ce qui représente un risque. Pour cette raison, il est bon de développer le réflexe de partitionner complètement les deux.

La situation :

1. Votre opérateur mobile est légalement obligé de collaborer avec les services de maintien de l'ordre.
2. Votre fournisseur internet est légalement obligé de collaborer avec les services de maintien de l'ordre.
3. Les réseaux sociaux et Google sont obligés de collaborer avec les services de maintien de l'ordre.
4. Le data center qui héberge Organise.Earth est légalement obligé de collaborer avec les services de maintien de l'ordre.

Dans les trois premiers cas, les fournisseurs sont contraints de transmettre les données et/ou autoriser leur accès dans le cadre d'une enquête. Dans le quatrième cas, le fournisseur est également obligé, à la différence que le disque dur sur lequel se trouvent les données est fortement chiffré. Des chiffrements de premier ordre, réputés pour ne pas être cassables, sont utilisés à la fois dans les couches de bases et les couches systèmes. On fournit donc une grosse brique hermétique aux autorités. Mais contrairement aux trois autres cas, si Organise.Earth est saisi, les communications s'arrêtent pendant le temps nécessaire à la restauration de sauvegardes antérieures. Cela peut prendre des jours voire une semaine, en fonction des circonstances.

Règles empirique (qui s'appuie sur l'expérience) :

:arrow_right: Utiliser des messages chiffrés de bout en bout pour quoi que ce soit de potentiellement sensible aujourd'hui ou dans le futur (des exemples sont proposés à la fin). Les preuves incluent les noms, les plans, les déclarations d'intentions. :arrow_right: Toujours respecter la vie privée et l'anonymat des personnes avec lesquelles vous êtes engagé·e·s. *Ne pas utiliser les vrais noms, les numéros de téléphones et adresses lorsque vous y faites référence.* Aider les autres rebelles à faire de même. N'envoyez à personne des preuves qu'un·e rebelle est impliqué·e dans une action. :arrow_right: Toujours éviter de donner les informations personnelles de membres de votre équipe ou de vous-mêmes à des entreprises comme Google ou Facebook, des entreprises qui ont une longue histoire de collaboration avec la police. :arrow_right: Créer un email et une identité pseudonyme pour des évènements XR lorsque c'est possible. Aller changer les comptes existants si besoin et changer l'adresse mail et l'identité associées. :arrow_right: Si vous risquez de vous faire arrêter, assurez-vous que les données de vos appareils sont inaccessibles aux mains des enquêteurs. Ayez connaissance de vos droits au moment de l'arrestation. Et supposez que vous risquez de ne jamais revoir vos appareils et que s'ils vous sont rendus, ils doivent être considérés comme compromis.

Messages et appel chiffré de bout-en-bout

Depuis 2013, il existe différentes solutions de chiffrement de bout-en-bout (*end-to-end : E2E*) pour les smartphones. Le chiffrement de bout-en-bout est une méthode *zero-knowledge* qui assure le chiffrement tout le long de la transmission, du transport au stockage, de l'origine à la destination.

Ces solutions présentent des niveaux de fonctionnalité et sécurité variés. On présente ici trois applications E2E. WhatsApp, Threema et Telegram ne seront pas présentées car elles présentent toutes des problèmes de sécurité et/ou ont des mauvaises pratiques d'implémentation.

Signal, de Open Whisper Systems

Signal est probablement la plus populaire, en partie parce que le Signal Protocol est largement estimé par les ingénieurs en sécurité informatique et les cryptographes, et parce que Open Whisper System avait six mois d'avance sur la plupart de ses concurrents et a distribué un service avec des fonctionnalités de bases correctes. Sa popularité lui permet de s'étendre encore davantage.

Signal est basé aux Etats-Unis, où elle doit composer avec le FBI. Elle ne conserve aucune metadonnée des utilisateurs. Néanmoins, il s'agit toujours d'un service centralisé et donc toujours d'un point de défaillance unique.

Bien que le chiffrement de bout en bout soit efficace, vous devez néanmoins donner votre numéro de téléphone mobile comme identifiant pour faciliter l'invitation d'une nouvelle personne sur le réseau. Les numéros de téléphones (comme expliqué précédemment) sont les plaques d'immatriculation de vos téléphones. Gardez cela en tête en utilisant Signal.

> :warning: Par précaution, surtout pour vos contacts, assurez-vous que votre téléphone a un mot de passe ou schéma complexe comme vu précédemment. Assurez-vous également de mettre un code spécifique à Signal comme c'est possible via les paramètres.

> :information_source: Signal ne fonctionne qu'avec le WiFi ou la 2/3/4/5G. Il ne fonctionnera pas sur le réseau mobile, vous devez donc être connecté·e·s à de la data pour l'utiliser.

Signal professionnel :

- appel, vidéo, chat chiffré e2e (one-to-one)
- facilitation de l'accès au dispositif via l'envoi de sms
- estimé très robuste
- transfert de fichier
- présent sur beaucoup de supports

Signal classique :

- pas d'appel ou vidéo de groupe
- besoin d'un appareil avec une carte SIM pour créer un compte
- Les numéros de téléphones sont les identifiants, à gardez en tête en cas de saisie
- interface simplifiée et peut être même trop minimaliste
- transfert de fichier limité à seulement certains types de fichiers

Wire

Wire s'est lancé environ 6 mois après Signal, il présente aujourd'hui quelques avantages par rapport à Signal. Contrairement à Signal, Wire ne dépend pas d'une carte SIM pour être activé et donc s'il n'est pas plus privé que Signal, il a certainement plus de potentiel pour l'anonymat. Wire utilise une cryptographie très puissante, pour les connaisseur·se·s :

- ChaCha20 (stream cipher)
- HMAC-SHA256 as MAC
- Elliptic curve Difffier Hellman key exchnage (Curve25519)

Wire est basé en Suisse et bénéficie des lois suisses très strictes sur la protection des données, avec aussi des serveurs localisés en Allemagne et Irlande. Ils ont même publié un rapport de tranparence des requêtes sur leur utilisation des données (une liste bien vide jusqu'à aujourd'hui). Wire est open source et offre des fonctionnalités de chat, voix, appel vidéo, et partage de fichier. Une fonctionnalité spéciale lui permet de supporter plusieurs comptes.

Wire professionnel :

- pas de dépendance avec aucun identifiant autre qu'un compte mail
- appel de groupe possible
- multiples comptes possible
- cryptographie élevée
- chat de groupe
- code ouvert pour les audits de sécurité
- transfert de fichier
- présent sur beaucoup de supports

Wire classique :

- maximum de 4 personnes pour un appel vidéo
- besoin d'un réseau WiFi ou mobile pour communiquer
- pas vraiment populaire

Briar

Briar est le dernier sorti mais présente une offre unique. A l'instar de ses deux concurrents, il ne dépend pas spécifiquement d'une infrastructure réseau traditionnelle. Conçu pour des activistes, il suppose de pouvoir être utilisé dans le cas où l'État a désactivé ou brouillé les réseaux cellulaires ou WiFi à proximité d'un lieu comme cela a été fait entre autres en Turquie, Chine, États-Unis, Ukraine.

Pour y parvenir, il exploite la fonctionnalité BlueTooth sur presque tous les smartphones pour envoyer des messages d'un appareil à l'autre, de manière maillée : un avantage significatif dans un effort coordonné pour désactiver l'infrastructure de communication lors d'une action, en supposant que la police n'a pas un accès physique à tous les participants et ne peut pas simplement saisir tous les appareils.

Lorsque l'accès à internet est possible, Briar utilise le réseau anonyme Tor avec une couche supplémentaire afin qu'il ne puisse pas être prouvé que l'appareil était la source d'une transmission avec quelqu'un d'autre.

Avantages de Briar :

- chiffrement e2e
- ne dépend pas des infrastructure pour transmettre les données
- résistant à la censure, pas de recherche de mots clés et de blocage le long du parcours
- message stockés sur l'appareil et non sur un serveur externe
- offre la possibilité de partager sur des forums
- gratuit et totalement open source
- un tuto existe sur la Base, en français.

Inconvénients de Briar :

- relativement non mis à jour, peu de versions et de mises à jour
- ne fonctionne que sur Android
- l'utilisation de Tor consomme beaucoup de batterie

Cet article est encore en cours de rédaction, des captures d'écran apparaitront bientôt. Merci de votre lecture

---

Créé 2023-09-08 20:16:25 CEST par mollusque
Mis à jour 2025-07-29 21:50:58 CEST par Guest