Sécuriser son téléphone

Les informations à connaître et les bonnes pratiques à suivre pour sécuriser son téléphone.

Recommandations sur l’utilisation de Signal

Rappels avant toute action

1. Eviter au maximum de venir avec son téléphone à une action.
2. Supprimer un maximum de données (signal, mattermost, Email, photos & vidéo, données du presse papier, etc). Sur signal, supprimer les conversations et quitter les groupes non indispensables (actions passées, etc).
3. S’assurer que son téléphone est chiffré.
4. Eteindre son téléphone pour activer le chiffrement. En effet, le premier déverrouillage désactive le chiffrement, il faut donc l'éteindre pour le réactiver.

Pourquoi faut-il supprimer l’application Signal avant une action ou durant l’action avant une possible interpellation ?

Le principal intérêt de Signal est de protéger l'interception à distance des contenus des messages. En utilisant Signal, les messages sont chiffrés de bout en bout, c'est-à-dire que même si une personne 'voit' le message, elle ne pourra pas le lire. Cependant, la protection n'est pas garantie si l'attaquant à un accès physique à un téléphone dans un état non chiffré, soit car le chiffrement a été désactivé avec le premier déverrouillage, soit car le téléphone n'est de base pas chiffré.

Supprimer l’application Signal supprime toutes les données de l’application. Ainsi si les forces de l'ordre ont accès au téléphone dans un état non chiffré elles ne pourront pas obtenir les données.

En cas de suppression de l'application, je veux retrouver les données une fois le risque passé, que puis-je faire ?

Il est possible de créer une sauvegarde chiffrée des données sur le téléphone ou en dehors. Pour cela aller dans: (en passant par Settings > Chats > Chat backups > Turn on). Il faut bien noter dans un endroit sécurisé la passphrase (non accessible par les Forces de l'Ordre). Ainsi si l'application ou le compte signal a été supprimé, lors de la réinstallation on peut utiliser cette sauvegarde en la décryptant via la passphrase et ainsi retrouver ses données.

Les forces de l'ordre ne peuvent-elles pas me demander cette passphrase ?

Si elles le peuvent mais encore faudrait-il qu'elles identifient cette sauvegarde. Même si elle est stockée sur le téléphone, ce n'est pas si simple et on peut donc espérer qu'elles ne l'identifient pas. Il est aussi possible de stocker la sauvegarde en dehors du téléphone. De plus, si vous dites (devant un tribunal, en GAV on ne dit rien) ne plus avoir cette passphrase car vous ne l'aviez pas notée ou que vous l'avez perdu, ce sera une position plus crédible juridiquement car c'est plausible.

Faut-il mieux supprimer l'application ou supprimer son compte signal ?

Signal donne la possibilité de supprimer son compte: Settings > Accounts > Delete account. La différence par rapport à supprimer l'application est qu'en cas de suppression du compte le numéro de mobile n'est plus répertorié sur les serveurs de Signal. Ainsi, une personne extérieure ne peut pas soupçonner que tu utilises Signal habituellement (en entrant ton numéro dans Signal un.e utilisateur.rice le verra comme non sécurisé). De plus, supprimer son compte quitte automatiquement tous les groupes.

Les failles dans l'outil Cellebrite, outil utilisé par les FDO pour analyser les téléphones remettent-elles en question ces recommandations ?

Non.

Context sur Cellebrite

Cellebrite est un outil utilisé par les forces de l'ordre pour extraire et analyser automatiquement les données d'un téléphone. Pour ce faire, il faut avoir brancher physiquement à l'outil le téléphone allumé et dévérouillé. L'utilisation de Cellebrite est donc par exemple possible dans un cas où un.e militant.e serait amené.e en garde à vue et n'aurait pas son téléphone chiffré.

Notez que sur les versions récente d'Android, le téléphone est chiffré par défaut, jusqu'à ce que vous l'ayez déverouillé une première fois depuis son démarage, même si vous l'avez revérouillé ensuite, il est donc fortement conseillé de l'avoir éteint ou rédémarré avant que les FDOs le récupère, pour qu'il soit chiffré à ce moment là.

Lien avec Signal

Signal a publié cet article disant qu'iels avaient exploité.e.s des failles dans Cellebrite afin de corrompre la donnée collectée. Cette exploitation peut permettre de rendre la donnée collectée lors une analyse automatique du téléphone moins fiable et donc contestable devant un tribunal. Cependant, selon Signal, cette corruption est très loin d'être systématique et il est possible que Cellebrite a pu réparer la faille ou qu'un autre outil d'analyse soit utilisé par les Forces de l'Ordre. De plus, une analyse humaine (en lisant simplement les messages) peut-toujours être réalisée. Ainsi ces failles ne remettent pas en cause le besoin de supprimer Signal et d'avoir le moins de données possibles sur son téléphone.

Autres ressources

Tuto très détaillé sur les bonnes pratiques sur Signal: https://paris-luttes.info/IMG/pdf/zine_signal_ppp.pdf

Sécurité du téléphone: 1 - Comment chiffrer son téléphone ?

Contenu transféré depuis la base: Sécurité du téléphone: 1 - Saisie par la police

Le téléphone est un point critique de sécurité, car il contient de nombreuses informations et il est toujours saisi lors de perquisitions ou d'arrestations. Il est donc important de vous demander si votre téléphone est vraiment nécessaire avant d'aller sur une action.

D'une manière générale, plutôt que chacun·e ait des documents sensibles sur son téléphone, il vaut mieux désigner quelques personnes garantes de ces documents, qui sécurisent bien leurs téléphones et qui sont conscientes qu'elles pourraient le perdre au cours de l'action.

> **Modèle de menace :** lors d'une arrestation ou d'une perquisition, un téléphone qui contient des informations sur des actions futures ou passées et/ou sur l'identité de rebelles est saisi par la police.

Note : *en dessous de ce post vous trouverez un message d'Avocatvert donnant quelques indications précises dans le cas d'une demande de déchiffrement du téléphone par les forces de police.*

Chiffrer le contenu d'un téléphone

i Dans cette première étape, nous allons voir comment chiffrer les données de son téléphone. Le chiffrement (ou cryptage) est une technique qui vise à rendre impossible la compréhension d'un fichier par quelqu'un qui ne possède pas la clef de chiffrement (mot de passe). Les téléphones qui ne peuvent ni prendre de photos ni se connecter à internet ne peuvent pas être chiffrés. Ils stockent les contacts et des fichiers textes, rien de plus. □□ Attention : rien sur ces téléphones ne

peut être considéré comme sécurisé.

> ⚠ Si vous pensez qu'il y ai le moindre risque que votre téléphone ne tombe dans les mains de la police, assurez-vous de l'éteindre. C'est seulement lorsqu'un téléphone est chiffré **et** éteint qu'il est le plus sécurisé.

La plupart des téléphones fonctionnent avec deux systèmes d'exploitation (OS) : Apple (iOS) et Android. Ce sont les deux cas qui sont traités ici.

Téléphones Apple

Les téléphones Apple les plus récents intègrent déjà un chiffrement. Mais ça n'empêche pas d'accéder à vos données. Le chiffrement doit être protégé par un mot de passe, auquel "l'attaquant·e" n'a pas accès, c'est seulement dans ce cas que les données sont sécurisées.

*Pour connaitre quelle version fonctionne sur votre téléphone : Identification de la version du logiciel de votre iPhone, iPad ou iPod - Assistance Apple (FR)

Pour les appareils qui tournent sous iOS 4-iOS 7 :

1. Ouvrir le menu 'Général' dans l'application 'Réglages' et choisir 'Code' (ou iTouch et code)
2. Suivre les instructions pour créer un mot de passe.

Pour les appareils qui tournent sous iOS 8-iOS 11:

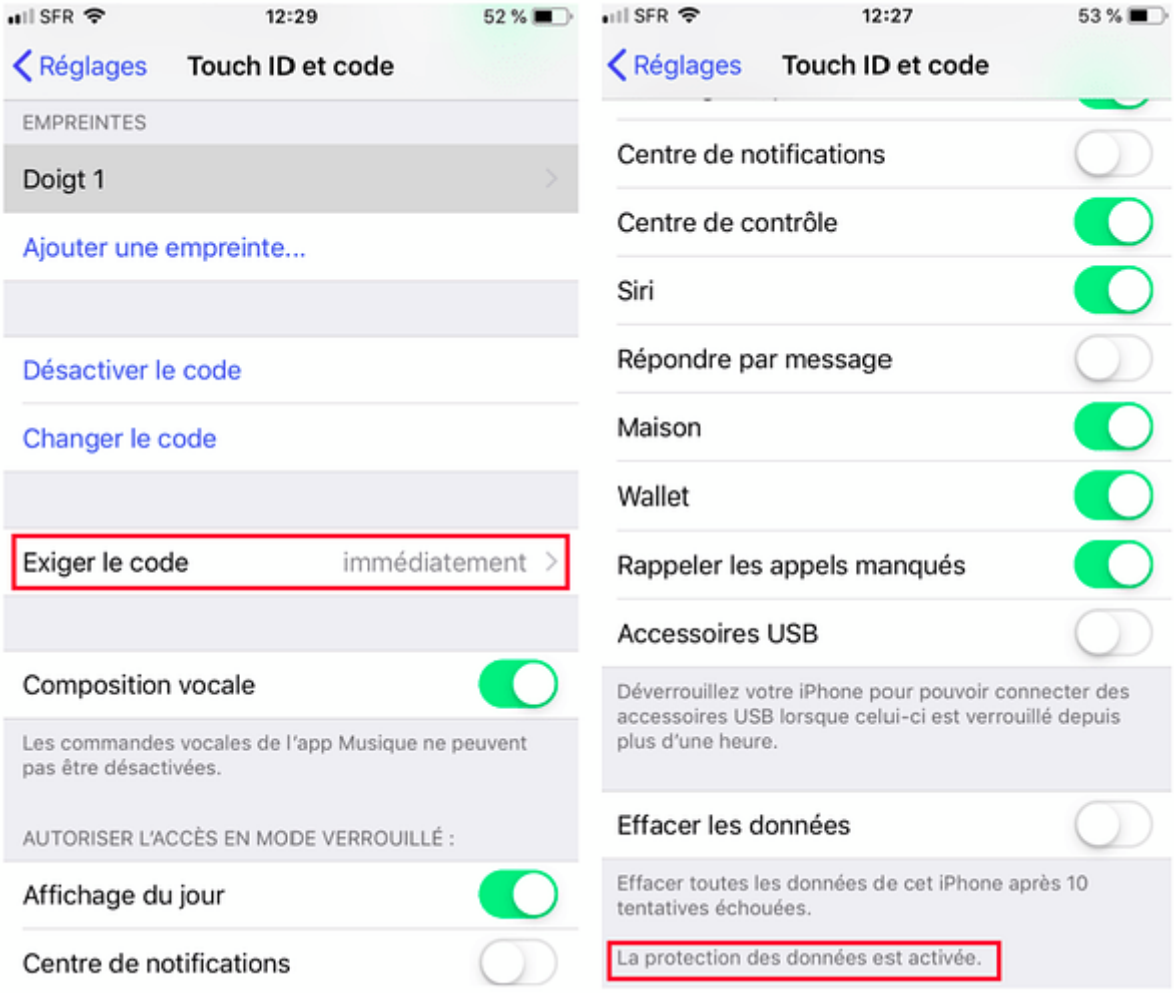
1. Ouvrir l'application 'Réglages'.
2. Appuyer sur 'Touch ID et code'.
3. Suivre les instructions pour créer un mot de passe.

Si votre appareil est sous iOS 8, désactiver l'option "mot de passe simple" pour créer un code de plus de quatre caractères. Avec la mise à jour sur iOS 9, Apple a mis par défaut un mot de passe à six caractères.

i Si vous choisissez un mot de passe avec seulement des chiffres, vous aurez un clavier numérique quand vous devrez déverrouiller votre téléphone, ce qui peut être plus simple que de taper une série de lettres et de symboles sur un tout petit clavier. Cependant, même si le logiciel Apple est conçu pour ralentir les outils de 'craquement' de mot de passe, nous vous suggérons de choisir un mot de passe de six caractères ou plus, qui contient des chiffres et des lettres. C'est tout simplement plus compliqué à 'craquer'.

Pour modifier votre mot de passe, allez dans Réglages > [votre nom] > Mot de passe et sécurité et sélectionnez 'Modifier le mot de passe'. Vous devrez aussi paramétrer l'option 'Exiger le code' sur 'immédiatement', afin que votre appareil ne soit pas déverrouillé lorsque vous ne l'utilisez pas.

Une fois que vous avez paramétré votre mot de passe, faites défiler vers le bas la page des paramètres du mot de passe. Vous devriez voir un message disant 'La protection de données est activée'. Cela signifie que le chiffrement de votre appareil est maintenant relié à votre mot de passe, et que le mot de passe est nécessaire pour accéder à la majeure partie des données de votre téléphone.



Un point sur les sauvegardes Apple

Les propriétaires d'appareils Apple effectuent généralement des sauvegardes sur iCloud ou iTunes.

⚠ Si vous effectuez des sauvegardes sur l'iCloud, vous devez être conscient·e que toutes ces données peuvent être accessibles à la police d'après la loi. Et quand bien même Apple vous assure que vos données sont cryptées, ils ont les clefs de chiffrement et sont obligés de les donner en cas d'enquête pénale. La police peut donc avoir accès aux données sauvegardées sur l'iCloud. Pour cette raison, nous vous recommandons de ne faire aucune sauvegarde sur ces clouds.

Si vous sauvegardez votre appareil Apple sur votre ordinateur en utilisant iTunes, il est important de savoir que, par défaut, le système de sauvegarde de iTunes ne chiffre pas les données. Vous devez donc choisir l'option 'Chiffrer la sauvegarde' afin que toutes les données soient bien stockées de façon chiffrée sur l'ordinateur. Assurez-vous de bien retenir le mot de passe et de sécuriser votre disque dur entier.

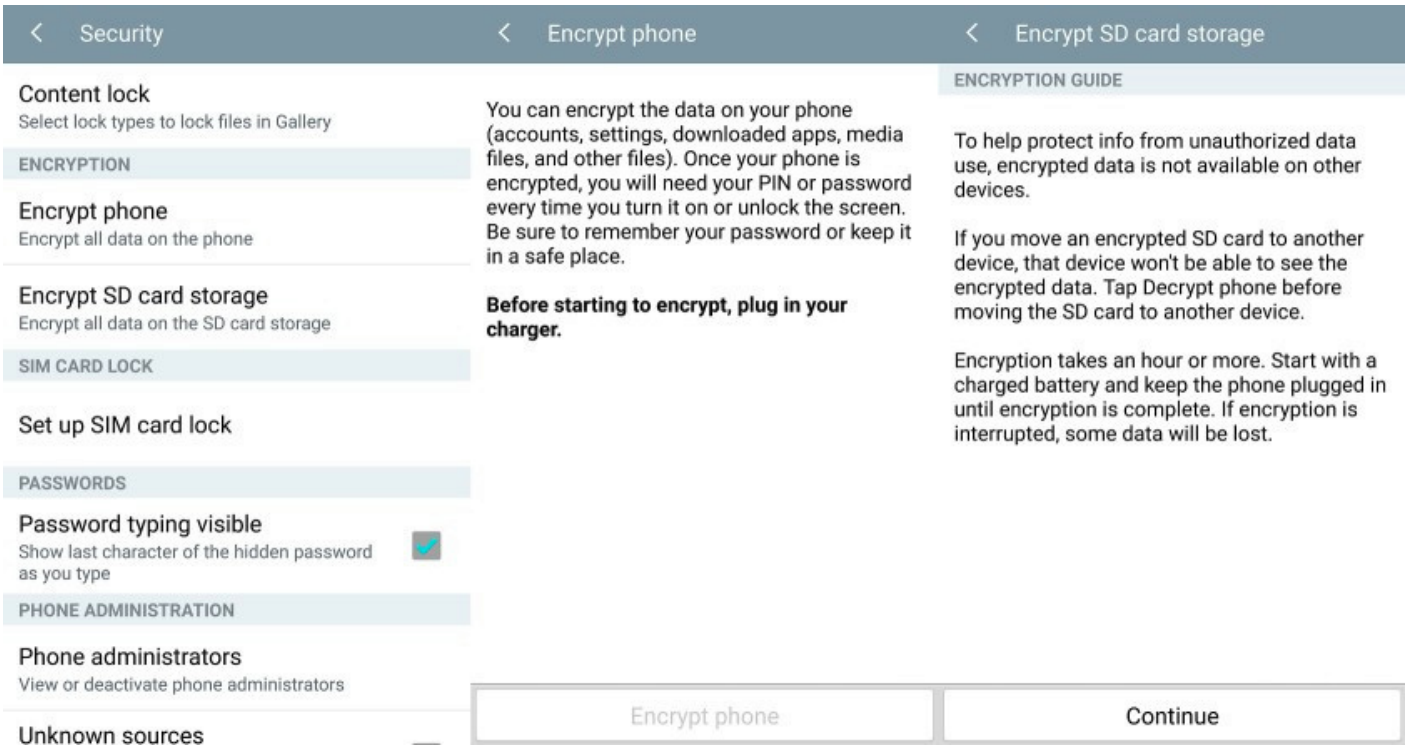
Téléphones Android

Aujourd'hui, par défaut, la plupart des appareils sont cryptés, en particulier les appareils qui fonctionnent sous les dernières versions d'Android. Si jamais ce n'était pas le cas sur votre appareil, il est possible et simple de l'activer.

Pour connaitre quelle version d'android fonctionne sur votre téléphone : https://www.astuces-aide-informatique.info/4826/identifier-version-android

Android 5.0 ou plus

Pour les téléphones et tablettes sous Android 5.0 Lollipop ou plus récent, vous pouvez aller directement dans l'onglet 'Sécurité'. Cela dépend un peu des appareils pour y accéder, mais généralement on y arrive via Paramètres > Personnel > Sécurité.



Vous trouverez ici une option pour chiffrer votre téléphone. Vous devrez brancher celui-ci sur secteur pour être sûr·e que le processus puisse se faire sans encombre. Si vous ne l'avez jamais fait, il vous sera demandé de choisir un code PIN ou mot de passe dont vous aurez besoin pour déverrouiller votre téléphone.

Android 4.4 ou moins

Si vous avez un téléphone avec Android 4.4 KitKat ou moins, vous devrez configurer un mot de passe ou PIN avant de commencer le processus de cryptage. Allez dans Paramètres > Sécurité > Verrouillage de l'écran. Vous pouvez choisir entre un schéma, des chiffres (PIN) ou un mélange de chiffres et lettres. Ce sera votre mot de passe après le chiffrement alors assurez-vous de le retenir.

Une fois que c'est fait, vous pouvez revenir au menu Sécurité et cocher 'Chiffrer le téléphone', ou 'Chiffrer la tablette'. Vous devrez brancher votre téléphone sur secteur et lire les messages d'avertissement, et sûrement confirmer votre mot de passe une dernière fois avant que commence le processus de cryptage.

Le cryptage du téléphone peut durer une heure ou plus, en fonction de la puissance de votre appareil et la quantité de données stockées. Une fois le processus terminé vous pouvez déverrouiller votre appareil et commencer à utiliser votre appareil fraîchement chiffré.

ℹ De retour dans le menu sécurité, vous pourrez aussi chiffrer votre carte microSD. C'est recommandé pour que toutes vos données soient sécurisées. Veuillez noter que dans ce cas, votre carte microSD ne pourra pas être utilisée sur un autre appareil (ordinateur, appareil photo, ...).

ℹ Il peut être assez difficile de se souvenir d'un mot de passe permettant un niveau de chiffrement élevé, c'est une raison pour laquelle les mots de passe choisis sont souvent moins sécurisés, plus courts. Sur tous les appareils Android, il y a une option schéma qui est excellente car des gestes complexes sont souvent plus faciles à retenir qu'un mot de passe complexe. Assurez-vous que le schéma contienne au moins six lignes, et une grille de 4x4 points ou plus.

Un point sur les sauvegardes Android

Les appareils Android sont synchronisés avec différents types de sauvegardes à distance. Toutes ces sauvegardes doivent être désactivées au profit d'une sauvegarde en local sur un appareil (comme un ordinateur par exemple), qui doit lui-même avoir un disque dur entièrement chiffré (cf. Sécurité de l'ordinateur: 1 - Saisie par la police). Avant de faire des sauvegardes, les fonctionnalités telles que 'SideSync' doivent être désactivées.

⚠ Les développeu·r·se·s et passioné·e·s ont souvent des fonctionnalités spéciales pour manipuler leur téléphone en bas niveau, cela peut présenter des risques. Par exemple, activer le 'USB Debugging' présente un risque réel qu'un "attaquant" ayant un accès physique à l'appareil puisse utiliser les outils `adb` d'Android pour accéder à l'appareil. Assurez-vous que le débogage par USB est désactivé avant d'aller sur une action.

Références

How to encrypt your iphone ?

How to encrypt android device ?

▶ Suivant : Sécurité du téléphone 2 - Tracage par gsm et wifi

Sécurité du téléphone: 1.1 - Bonnes pratiques et faiblesses du chiffrement d'un téléphone

Résumé du contenu de ce guide

- Chiffrer ton téléphone permet grandement d'améliorer la protection des données s'y trouvant.
- Cependant, pour que le chiffrement soit effectif le téléphone doit être éteint ou allumé sans jamais avoir été déverrouillé depuis le dernier allumage. En effet, les outils utilisés par les forces de l'ordre permettent d'accéder à la donnée d'un téléphone ayant déjà été déverrouillé depuis le dernier allumage.
- Un mot de passe fort (10 charactères composés de lettres, chiffres et charactères spéciaux peut-être considéré comme raisonnable) doit être utilisé pour éviter une attaque du chiffrement. Un téléphone protégé par un mot de passe de 6 chiffres ou par un pattern peut-être déchiffré en moins d'un jour par les outils utilisés par les forces de l'ordre.
- Un téléphone étant passé entre les mains des forces de l'ordre, par exemple lors d'une garde-à-vue, est à risque d'être infecté par un enregistreur de saisie (keylogger). La réinitialisation de l'appareil et le changement du mot de passe est alors vivement recommendée.
- Le téléphone doit être mis à jour régulièrement car Android et iOS font souvent des mises à jour pour résoudre des vulnérabilités pouvant être exploitées.
- La protection par chiffrement doit se combiner avec une bonne hygiène numérique dont la réduction des données sensibles (par exemple en utilisant les messages éphémères dans les messageries cryptés ou en supprimant les messages sur Mattermost).
- Ces conseils s'appliquent à tous les téléphones Android et iOS (iPhone).
- Toutes ces éléments se basent sur des sources ouvertes sur un domaine confidentiel qui évolue vite. Il est donc possible qu'ils ne soient plus pertinents pour le meilleur comme pour le pire.

Qu'est ce que le chiffrement d'un téléphone ?

Le chiffrement d'un téléphone est une couche de protection supplémentaire pour toutes les données stockées sur le téléphone. Il ne protège pas ledit appareil contre les menaces externes, ni ne rend les communications privées ou illisibles, etc. Ce que le chiffrement de l'appareil fait est de convertir toutes les données du téléphone sous une forme accessible uniquement en entrant d'abord un mot de passe. Ainsi les données du téléphone, telles que les images, les messages des applications Signal ou Mattermost, etc ne sont pas compréhensibles. Bien que cela puisse ressembler à un écran de verrouillage ou un mot de passe normal, la protection qu'il offre est beaucoup plus complète. Le chiffrement et déchiffrement des données se fait grâce à un algorithme de chiffrement et à une clé de chiffrement. La clé de chiffrement est composée de deux éléments: le mot de passe du téléphone (Pattern, PIN, Password) et une clé unique stockée de manière sécurisée directement sur le téléphone. Cette dernière est invisible pour l'utilisateur.ice.

Sur les téléphones mobiles récents, il est possible de chiffrer son téléphone qu'il soit un iPhone (tournant avec le système d'exploitation iOS) ou un téléphone tournant sous le système d'exploitation Android (Samsung, Google, Fairphone etc...). Ce reporter à la page du wiki "Comment chiffrer son téléphone" pour obtenir plus d'information.

Impact du chiffrement sur les données en fonction de l'état du téléphone

Un téléphone peut être dans 4 états:

- Déverrouillé. La donnée est alors accessible que l'option du chiffrement du téléphone soit activée ou non.
- Téléphone non-chiffré et éteint. La donnée est accessible. Un téléphone peut être non chiffré même si un code est nécéssaire pour y accéder. Voir le chapitre expliquant comment chiffrer son téléphone pour vous assurer que votre téléphone est chiffré. NB: Tous les nouveaux téléphones sont chiffrés par défaut.
- Allumé et vérrouillé en ayant été déverrouillé au moins une fois depuis le dernier allumage, acronyme **AFU** pour **After First Unlock**.
- Etéint ou allumé et vérrouillé sans avoir été déverrouillé depuis le dernier allumage, acryonyme **BFU** pour **Before First Unlock**. Dans les deux premiers cas, la donnée est accessible et donc non protégé pour quiconque, incluant les forces de l'ordre. La question que nous chercherons à répondre est: **dans le cas où le téléphone est dans un état AFU ou BFU, la donnée est-elle sécurisée ?**

Téléphone en état AFU

Pour un téléphone AFU, la donnée n'est pas accessible directement. Par exemple, si vous le brancher à un ordinateur, vous n'aurez pas accès à la donnée à moins de rentrer le code. Cependant, des outils tels que Cellibrite ou GrayKey (voir image ci-dessous) sont utilisés par les forces de l'ordre pour accéder à la donnée. **Ces cas sont documentés aux Etats-Unis mais pour l'instant pas en France** même si on sait que les forces de l'ordre française s'équipe de ce genre d'appareil.

L'appareil GrayKey

Connect the desired Apple mobile device to the cable on the left side (active LED) of the GrayKey unit. GrayKey will automatically detect the device and attempt to install a brute force agent.

The following conditions are allowed for a GrayKey connection:

- Device is powered off (known as BFU – Before First Unlock)
- Device is powered on (typically known as AFU – After First Unlock)
- Damaged display* (GrayKey extraction available but replacement screen required for additional tool extractions)
- Low battery device (GrayKey known to install agent with 2 to 3% battery life)

Condition pour l'utilisation de GrayKey - Image Motherboard

Comment ces outils peuvent accéder à la donnée ?

Lorsqu'un téléphone en état AFU est déverrouillé (pour la première fois), la clé de chiffrement est générée afin d'accéder à la donnée et de la déchiffrer. Quand le téléphone est verrouillé sans être éteint (et donc qu'il passe en état BFU), la donnée n'est alors pas rechiffrée. De plus, la clé de chiffrement reste accessible dans la mémoire vive du téléphone. Les outils utilisés par les forces de l'ordre arrivent à accéder à cette donnée non chiffrée et aussi à récupérer la clé de chiffrement afin de déchiffrer la donnée qui pourrait encore être dans un état chiffré. Android et iOS tente d'améliorer la sécurité du téléphone dans cet état mais ils restent des vulnérabilités exploitables

par les forces de l'ordre.

Comment s'en protéger ?

Il faut faire en sorte de rechiffrer la donnée et de faire disparaitre la clé de chiffrement. Pour cela, il existe une **méthode toute simple: éteindre son téléphone** ! En éteignant son téléphone, celui-ci passe d'un état AFU à BFU. Mais un téléphone en état BFU est-il protégé ?

Téléphone en état BFU

Lorsqu'un téléphone est en état BFU, la donnée est chiffrée. Les mêmes outils qui permettaient d'accéder à la donnée d'un téléphone en état AFU peuvent être utilisés mais les méthodes pour accéder à la donnée ne sont plus du tout les mêmes. Selon les sources sérieuses disponibles, ces méthodes peuvent être bloquées si on suit certaines règles.

En effet, alors que pour un téléphone en état AFU, les outils des forces de l'ordre permettre d'exploiter des vulnérabilités des téléphones pour accéder à la clé de chiffrement, pour un téléphone en état BFU, cette clé n'existe pas, les outils ne peuvent donc y accéder. Ils doivent à la place essayer de la recréer. Pour cela, ils vont essayer un maximum de combinaisons possibles de clé de chiffrement sur la donnée chiffrée. S'ils trouvent la bonne clé, la donnée est alors déchiffrée. C'est ce qu'on appelle une attaque par force brute. Deux types d'attaque par force brute existent.

Attaque par force brute hors-line

Cette technique consiste à copier toutes les données chiffrées de l'appareil, ici un téléphone, sur un support externe. Une fois la donnée copiée, l'attaque par brute force est lancée. L'avantage de cette méthode est qu'elle permet d'utiliser des ressources informatiques très grandes (des ordinateurs très puissants et très nombreux) si l'attaquant en a les moyens financiers et techniques. Le succès de l'attaque dépend de l'algorithme de chiffrement utilisé et de la complexité du mot de passe qui crée la clé de chiffrement. Si la donnée a été chiffré par une clé de chiffrement créée par le mot de passe "123", la donnée sera déchiffrée en moins d'une seconde. Cependant, cette méthode ne semble pas utilisée pour attaquer des téléphones chiffrés. En effet, d'une part les téléphones sont chiffrés avec des algorithmes de chiffrement robustes pour lesquels il n'existe pas de grandes vulnérabilités et de l'autre la clé de chiffrement ne dépend pas seulement du mot de passe renseigné par l'utilisateur mais aussi de la clé unique stockée de manière sécurisée directement sur le téléphone. En essayant d'accéder à la donnée sans passer directement par le téléphone, cette clé unique n'est plus accessible et doit être aussi trouvée. Cette clé étant très longue, c'est théoriquement impossible, rendant les attaques hors-line sur les téléphones caduques.

Attaque force brute directement sur le téléphone

Afin d'éviter de devoir trouver cette clé unique qui complexifie la clé de chiffrement, l'attaque peut se faire directement sur l'appareil contenant la clé unique. C'est la méthode d'attaque des outils utilisés par les forces de l'ordre.

Ces outils vont donc essayer une multitude de combinaisons possibles de mot de passe. Le succès de cette méthode va donc dépendre de la complexité du mot de passe. Les outils vont d'abord essayer les mots de passe les plus communs (exemple: "password") puis ils vont essayer un maximum de combinaisons possibles. La vitesse d'essai des mots de passe va dépendre des ressources de l'appareil. Contrairement à une attaque hors-line où des millions de combinaisons peuvent être testées par heure si l'attaquant en a les moyens, ici le nombre va être grandement réduit du fait des limites sur la vitesse d'essai du systèmes d'exploitation (Android ou Apple) et des ressources limitées du téléphone. Les estimations varient d'une centaine d'essais par jour à environ 2 millions par jour. Pour cette dernière estimation, il faudra 11 heures pour craquer un mot de passe de 6 nombres et 46 jours pour un mot de passe de 8 nombres. À titre de comparaison, sans ces limites liées à l'appareil, sur une attaque de force brute hors-line, il est très simplement possible de brute force à une vitesse de 2 millions de l'appareil PAR SECONDE. Un code a 6 nombres sera alors deviné en moins d'une seconde.

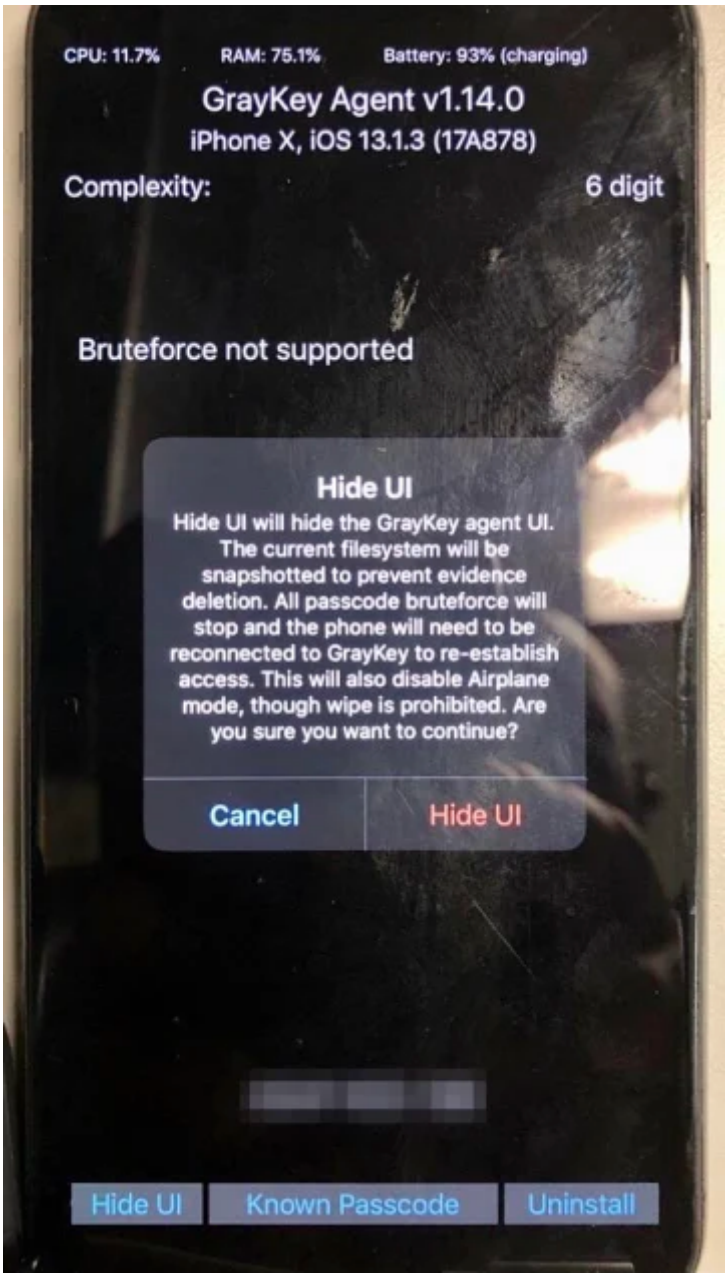
Comment s'en protéger ?

Le nombre de combinaisons dépendant de la taille et de la complexité du mot de passe, il faut définir un mot de passe fort c'est-à-dire long avec des chiffres, des lettres majuscules et miniscules et des caractères spéciaux. Un mot de passe de 10 charactères composés de lettres, chiffres et charactères spéciaux peut-être considéré comme raisonnablement fort. Au contraire, comme explicité plus haut, un mot de passe de 6 nombres est faible car il faudra que quelques heures pour accéder aux données. De manière général, les mots de passe pattern ou les codes numériques sont faibles. Vous pouvez calculer à quel point un mot de passe est fort sur omnicalculator.

Une fonctionnalité optionnelle disponible sur les versions récentes d'iOS ou Android permet d'effacer les données après un certain nombre d'essais de mots de passe en rétablissant la configuration usine de l'appareil. Android et iOS forcent aussi les utilisateurs à atteindre un certain temps après plusieurs mauvais mots de passe. Ces fonctionnalités protègent-t-elles des attaques par force brute ? Cela dépend. Certains outils, tel que GrayKey, semblent réussir à désactiver ces fonctionnalités en exploitant des vulnérabilités Android ou iOS. Il est cependant conseillé d'activer la fonctionnalité pour effacer les données. En effet, il est difficile de savoir les outils utilisés par les forces de l'ordre. Peut-être que dans certains cas, ces fonctionnalités renforcent la protection. De plus, une mise à jour Android ou iOS pourrait résoudre ces vulnérabilités. Enfin, c'est une fonctionnalité qui peut-être utilisée pour effacer les données d'un téléphone sans avoir à le déverrouillé. Il suffit en effet de rentrer des mauvais mot de passe jusqu'à la réinitialisation du téléphone.

Attaque par enregistreur de frappes (key-logger)

Une dernière méthode existe pour récupérer l'accès aux données, l'utilisation d'un logiciel enregisteur de frappes, pour enregistrer le mot de passe saisie par l'utilisateur. L'outil GrayKey a une telle fonctionnalité appelée "Hide UI". Cette fonctionnalité peut-être installée de manière invisible sur un téléphone. Il n'est pas documenté si c'est en état BFU ou AFU, mais il semble plus logique que ça soit possible dans l'état BFU car d'autres méthodes plus simples permettent d'accéder à la donnée en état AFU.



Fonctionnalité Hide UI sur IphoneX par GrayKey

La prochaine fois, que l'utilisateur saisira son mot de passe, celui-ci sera enregistré. Les forces de l'ordre en récupérant à nouveau le téléphone pourront alors accéder au mot de passe et déchiffrer la donnée. La méthode consiste donc à: 1 - Obtenir un accès physique au téléphone pour y installer le keylogger 2 - Faire en sorte que l'utilisateur saisisse son mot de passe 3 - Récupérer l'appareil afin de déchiffrer la donnée avec le mot de passe subtilisé.

On peut par exemple imaginer les forces de l'ordre proposer à la personne en garde-à-vue d'appeler son avocat. Si celle-ci entre son mot de passe puis éteint à nouveau son téléphone, le mot de passe sera enregistré sans qu'elle en ait connaissance. Les forces de l'ordre pourront alors y accéder. On peut aussi imaginer les forces de l'ordre installer ce logiciel durant une garde-à-vue, rendre le téléphone à la sortie de la garde-à-vue puis réinterpeller quelques temps plus tard la personne afin de récupérer le téléphone avec le mot de passe enregistré.

Comment s'en protéger ?

Il est très difficile de savoir si son téléphone contient un keylogger. Si le téléphone est passé entre les mains des forces de l'ordre par exemple lors d'une garde-à-vue, il faut considérer comme possible qu'un keylogger y soit installé. Dans ce cas, il faut réinitialiser son téléphone afin d'effacer le keylogger et changer son mot de passe.

Sources:

Wired - How Law Enforcement Gets Around Your Smartphone's Encryption - January 2021

Motherboard - Instructions Show How Cops Use GrayKey to Brute Force iPhones - Juin 2021

9to5mac - Cellebrite iPhone cracking: Here’s which models the kit can unlock and access, and how to protect your data - Avril 2022

Vice - Stop Using 6-Digit iPhone Passcodes - 2018

Page de présentation de GrayKey sur le site de GrayShift, entreprise commercialisant GrayKey

Everything you need to know about Android encryption - Mai 2021

Android - documentation sur le chiffrement

Reddit - Discussion on Cellebrite

GrayKey Hide UI, enregisteur de frappe:

NBC News - iPhone spyware lets police log suspects' passcodes when cracking doesn't work 2020

AppleInsider - New Grayshift spyware lets police surreptitiously snatch iPhone passcodes - Mai 2020

Sécurité du téléphone: 2 - Traçage par GSM et Wifi

Contenu transféré depuis la base: Sécurité du téléphone: 2 - Traçage par GSM et Wifi

Sécurité du téléphone. Fiche 2

Dans cette fiche, nous allons voir les risques peu connus liés au traçage d'un téléphone mobile.

> **Modèle de menace** : la police présente sur une action utilise un **IMSI-catcher** pour repérer tous les téléphones présents dans une zone, enregistrant les numéros IMSI et les numéros de téléphone. Ces numéros permettent d'identifier les propriétaires de téléphones anonymes en analysant leur déplacement sur le réseau de téléphonie mobile.

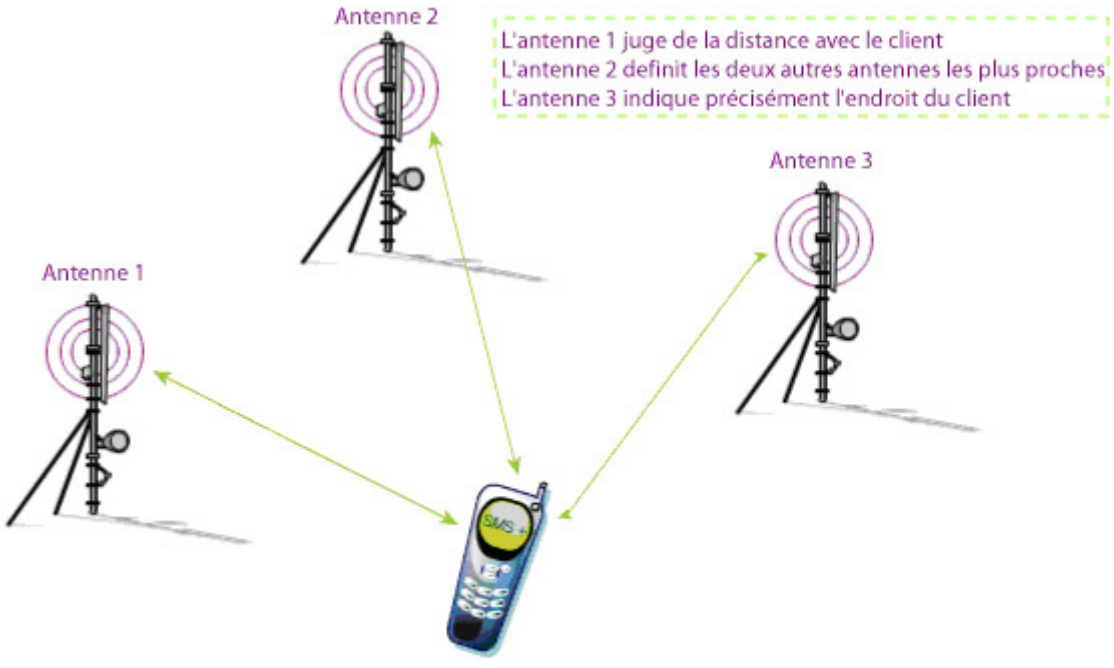
Menace type 1 : la carte SIM est tracée et le ou la propriétaire est identifiée

Le suivi par GPS

Contrairement à une idée repandue, nous sommes rarement traqués par le GPS de nos mobiles. Les capteurs GPS sur les téléphones sont des **récepteurs**. Des satellites géostationnaires envoient constamment des données qui permettent aux téléphones de déterminer leur position sur le globe. Cette position est calculée **dans le téléphone** en fonction de la distance connue d'au moins 4 satellites. Les satellites n'ont même pas connaissance des récepteurs GPS utilisant leurs données.

Le traçage GPS peut se produire via des logiciels malveillants présent sur des téléphones, qui transmettent la position calculée par le téléphone à un serveur via internet. Pour introduire un logiciel malveillant sur le téléphone, l'attaquant doit généralement avoir un **accès physique au téléphone (déverrouillé)**, ou que le/la propriétaire ait été victime d'une attaque de *fishing* pour qu'iel installe lui/elle-même l'application malveillante. Une fois le logiciel malveillant installé, il faut quand même que le GPS et que les données mobiles soient activés pour qu'il puisse vous suivre et transmettre les données.

Pour repérer un téléphone géographiquement le plus pratique est d'utiliser le réseau téléphonique. Nos téléphones sont toujours connectés à une ou plusieurs bornes/antennes plus ou moins éloignées (les fameuses buchettes qui représentent la qualité de la connexion au réseau). Cela permet de communiquer sans être coupé à chaque changement d'antenne. C'est également très pratique pour suivre un téléphone car l'on peut voir nos appareils sautiller d'antenne en antenne. Les antennes qui sont généralement arrangées en réseaux le long des routes et au sommet des bâtiments, et que l'on appelle souvent des tours ou antennes relais, sont des points de repères connus. Il suffit alors de faire une "triangulation" pour obtenir le point d’émission de votre téléphone avec une bonne précisions. C'est la méthode employée, par exemple, par les nazis pour repérer les radio clandestines pendant la Seconde Guerre mondiale.



La combinaison des 3 antennes permettent d'obtenir les coordonnées XY du client

Identifier le propriétaire d'un téléphone

A chaque carte SIM correspond un numéro de téléphone mais également un numéro unique lui servant à s'identifier avec les antennes relais : le IMSI (International Mobile Subscriber Identity). Puisqu'il sert d'identifiant, il est constamment diffusé lors des échanges avec les antennes. Or il est très simple de capter les numéros IMSI des téléphones avoisinants quelques centaines de mètres autour de soi en utilisant un récepteur SDR à 15€.

Cela à des conséquences importantes :

1. Les carte SIM sont souvent achetées via des cartes de crédit (votre abonnement mensuel ou l'achat au tabac du coin). Donc l'association utilisateur = SIM est facile à connaître.
2. Même si vous achetez en liquide une carte pré-payée, utiliser ce téléphone à coté de votre téléphone officiel ou celui d'un copain vous identifie. Par exemple : je suis dans un bar, j'allume mon téléphone pré-payé et je suis avec mon téléphone officiel dans la poche. Les deux téléphones sont 'vus' ensemble donc il y a un lien. De même, si vous éteignez votre téléphone officiel mais allumez votre téléphone pré-payé au domicile, l'adresse est connue.
3. Insérer une sim dans un téléphone utilisé officiellement permet à l'opérateur d'associer l'identification de votre terminal (téléphone) avec la nouvelle sim. (l'IMEI est utilisé avec la SIM X appartenant à Harry mais aussi avec la SIM Y.... donc Y = Harry). Ayez un téléphone dédié et si possible jamais utilisé ou acheté d'occasion.

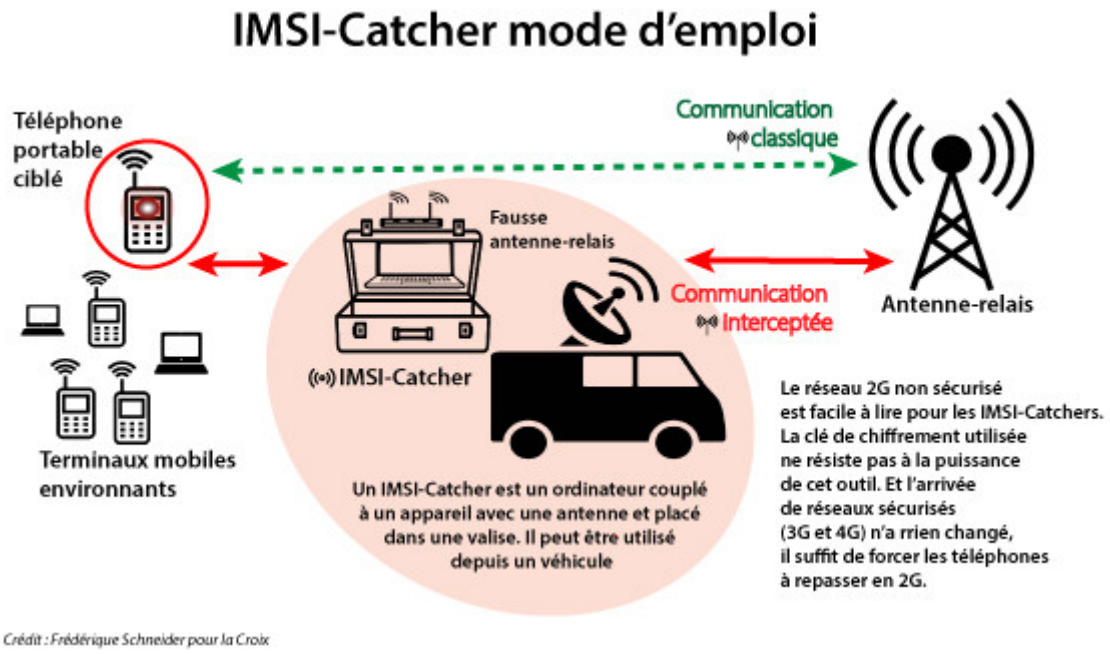
Conséquence : vous êtes localisable avec votre téléphone, prépayé ou non. Si quelqu'un a accès à la fois à votre numéro IMSI et l'accès à la base de donnée du fournisseur (ce que les autorité obtiennent facilement), il est possible de remonter à l'identités des individus présent dans le rayon d'une antenne, dont la vôtre.

Cela peut être utilisé pour déterminer les identités des individus présents à une manifestation, et peut être utilisé plus tard pour trouver des groupes d'activistes pendant une réunion. Il se pourrait que cette technique ait été utilisée pour découvrir et mettre fin aux *Black Lives Matter* aux USA.

Une **autre conséquence** est l'identité du téléphone : le IMEI (*International Mobile Equipment Identity*). C'est comme la plaque d'immatriculation de votre téléphone. L'IMEI est également diffusé par le téléphone à chaque interaction avec une antenne de téléphonie mobile (BTS). L'IMEI couplé à l'IMSI peut ajouter une couche supplémentaire de preuves d'identification en cas de saisie, car même si la carte SIM est retirée, l'appareil est identifié.

La surveillance des appels

Une autre menace existe. Au lieu de récolter seulement le numéro IMSI, les téléphones peuvent être facilement trompés en leur faisant croire qu'ils communiquent avec une vraie antenne téléphonique alors qu'en réalité ils sont traqués. Les appels et SMS envoyés peuvent être surveillés (même si cryptage du téléphone) à l'insu du propriétaire du téléphone. Cela a été largement utilisé par les services de polices aux Etats-Unis et ailleurs grâce au déploiement d'un *IMSI Catcheur*.



Crédit : Frédérique Schneider pour la Croix

Les systèmes Stingray sont utilisés à la fois pour traquer les téléphones et surveiller leur transmissions. Ces systèmes sont connus pour avoir été largement utilisés contre les activistes. Les services de police des Etats Unis, du Canada, de l'Irlande, du Royaume-Uni Uni, Arabie Saoudite, UAE et Turquie ont reconnu les avoir utilisé.

Ces systèmes appelés IMSI Catcher peuvent aussi être fait maison, avec un budget de 1000€.

Se défendre contre les IMSI Catchers

Utiliser des cartes SIM prépayées

Pour éviter l'identification via l'IMEI, l'identité du téléphone, vous devez utiliser des téléphones achetés uniquement avec du liquide. De plus, même si ça peut paraitre irréaliste la plupart du temps, mais pour des action à haut risques, vous devriez acheter un téléphone portable sans abonnement avec une carte SIM prépayée.

> ℹ On recommande que tous les coordinateur·rice·s, surtout ceux·elles engagé·e·s dans la planification d'actions et la logistique, utilisent des carte SIM prépayées, et idéalement des téléphone sans abonnements. Le groupe infrastructure devrait considérer avoir un stock de cartes SIM prépayées. Ces dépenses de 7-10€ peuvent être faites avant une action puis les cartes SIM recyclées pour les actions suivantes. Dans le pire des cas, cela peut permettre une confusion dans l'effort de la police utilisant un système de capture de IMSI.

Les téléphones sans abonnement (prépayés) sont des investissements qui peuvent être considérés pour des actions à hauts risques.

⚠ Attention à bien prendre en compte la partie sur l'identification au dessus. Avoir une carte pré-payée permet de freiner l'identification mais de nombreuses erreurs telles que la présence de téléphones "fantômes" à côté de téléphones officiels rends caduques l'anonymisation. Pensez à distribuer les téléphones pré-payés uniquement après avoir éteint tout téléphone officiel.

Installer un détecteur de IMSI Catcher

Des applications ont été développées pour détecter et avertir de la présence de catcher IMSI. Elles utilisent une carte des antennes de téléphonie mobile pour détecter la présence d'antennes inconnues qu'elles considèrent alors comme suspectes. Sans être entièrement fiables, certaines applications sont plus complexes que d'autres et détectent les "SMS silencieux" souvent utilisés par les IMSI catchers. Une de ces applications est Android IMSI catcher detector pour les services Android. En voici une autre SnoopSnitch (**Avertissement :** lien Google Play).

Est-ce qu'on est detectable quand on est en mode avion ?

Pour simplifier un peu grossièrement : Il n'est pas totalement exclu que bluetooth, wifi et réseau mobile fonctionnent et dialoguent avec les différents hubs qu'il y a autour MALGRÉ le mode avion : c'est selon les OS et l'honnêteté des marques qui les développent.

Néanmoins :

1. Sans carte SIM, l'opérateur ne peut pas faire le lien avec nos noms. L'antenne va avoir une adresse IP, mais pas de numéro client, et l'adresse IP change ofc d'une antenne à l'autre, donc pas possible de faire le lien avec une identité.
2. La seule vraie faille est au niveau de l'adresse MAC de nos smartphones (qui est une adresse statique, sauf sur le réseau mobile). Il est théoriquement possible de la retracer via les boxs wifi de particuliers à côté desquelles on passe : Même si on ne s'y connecte pas, nos smartphones crient en permanence leurs adresses MAC à toutes les boxs wifi qu'ils rencontrent.

Mais (1) c'est très difficile à faire et ça demande des efforts et un temps considérables pour identifier ne serait-ce qu'un appareil, et (2) si les flics peuvent demander à SFR d'accéder aux données de leurs antennes (ce que suggérais l'article), ils ne peuvent pas demander les données des boxs de tous les particuliers d'une rue (juridiquement et logistiquement : un enfer. Les opérateurs n'ont pas intérêt à leur filer les données de boxs de particuliers) En bref : clairement pas intéressant pour eux de s'attaquer à un si gros défi pour des délits aussi mineurs.

3. Le GPS est hors de propos, nos smartphones ne lui parlent pas.

NB : Concernant la prise de photo en revanche, elle peut poser problème, et ce même à postériori parce qu'elles sont souvent liées par défaut à une localisation (ou autres exifs, vous en parliez) et à des comptes personnels sur différents services. Charge à chacun d'aller checker ses réglages si iel veut prendre le risque de photographier des trucs. Sur ce sujet ça dépend des googles & co, pas du fonctionnement des réseaux, du coup ça reste une zone d'ombre.

Menace type 2 : traçage et identification via WiFi

Comme sur le réseau de téléphonie mobile, un téléphone diffuse des informations d'identification au réseaux WiFi. La partie WiFi d'un téléphone peut également être utilisée pour suivre un appareil lorsqu'il se déplace en ville. L'équivalent du IMSI ou IMEI est une adresse MAC (Media Access Controller) comme par exemple `62:7d:34:c1:04:2b`.

Même si l'on est connecté à aucun réseaux, le téléphone diffuse quand même des demandes de sonde aux points d'accès WiFi qui constituent une cartographie excellente en ville et donc une traçabilité du téléphone.

Les téléphone Apple récents "anonymisent" de telle requête jusqu'à ce que le téléphone soit connecté au réseaux WiFi. Les Androids ne le font pas. Dans tous les cas, il est important de savoir que cela se produit, tout comme le fait que les points d'accès gardent en mémoire une trace du passage de votre téléphone. De telles traces ont été utilisées comme preuve à plusieurs reprises dans les tribunaux.

⚠ Si vous effectuez des recherches sur le terrain et/ou ailleurs pour aider à une action, réfléchissez à deux fois avant de rejoindre un réseaux public non-fiable et n'activez votre WiFi que lorsque vous en avez besoin.

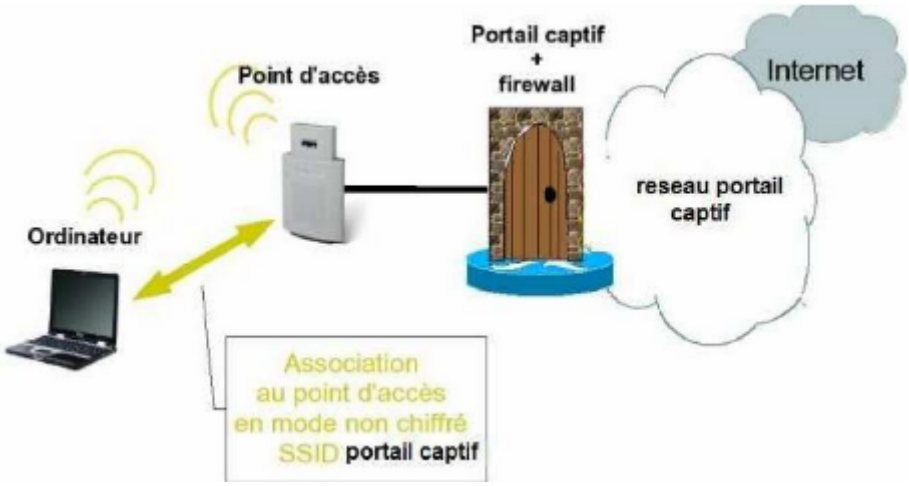
Utiliser un réseau WIFI inconnu

Lorsque vous utilisez un réseau WiFi inconnu vous ne pouvez garantir la confidentialité des données échangées. De nombreux réseaux ouverts officiels (les hôtels par exemple) utilisent des outils de type portail captif. Ces composants servent à garantir la traçabilité des usages des réseaux. En France, un fournisseur d'accès internet (un hôtel devient fournisseur en proposant son wifi) se doit de garder des traces des accès Internet en cas de demande des services d’état dans le cadre d’enquêtes (cf.

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164 Article 6). Tout accès vers internet est enregistré dans des journaux (logs) et souvent les flux chiffrés sont

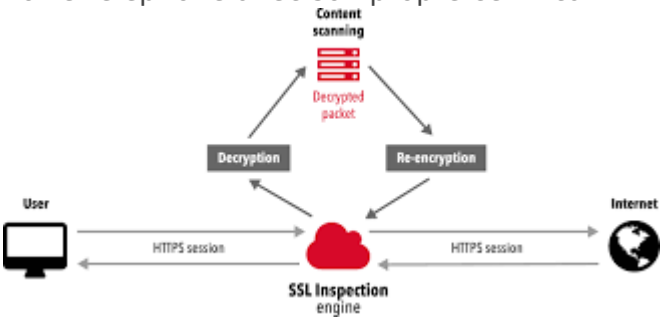
décryptés. C'est facilement repérable sur un pc, un peu moins sur un téléphone. Dans ce cas, lors de l'utilisation du WiFi, vous êtes redirigés vers une page d'authentification qui demande à connaître :

- N° de chambre,
- Numéro de téléphone pour recevoir un code par SMS. Le pire. Vous êtes automatiquement relié a votre identifiant téléphonique, voir ci-dessus les impacts.
- Votre nom
- Votre email
- Tout autre type d'information.

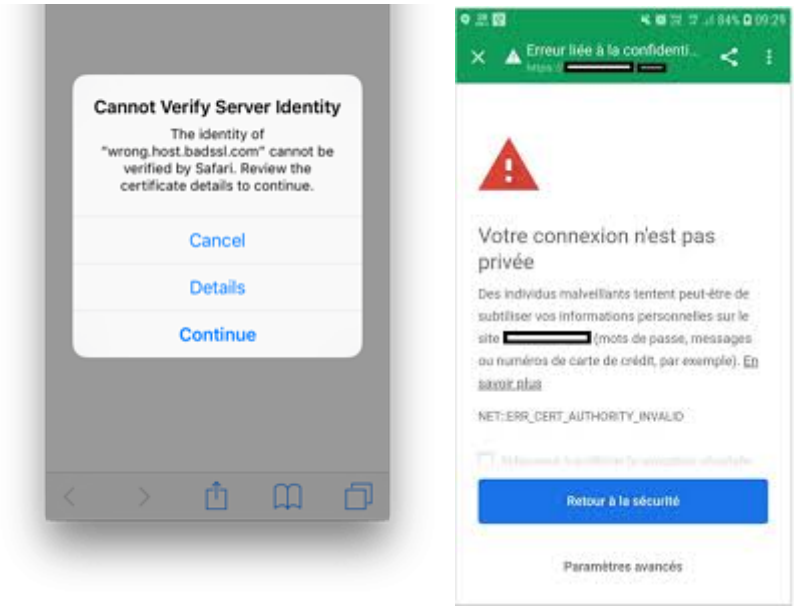


Dès que vous avez ce type de page vous pouvez être certain que vous n'aurez pas un accès direct à Internet comme avec votre box, mais que tout va être enregistré dans un journal (log).

De plus, même si vous naviguez en chiffrant vos communications, cela est très souvent insuffisant. Les Portails ou les routeurs du restaurant, hôtel... peuvent faire de l'inspection SSL. Ils déchiffrent vos communications pour voir l'intérieur des messages. C'est également repérable car vous devez avoir une alerte de sécurité sur votre client de mail, navigateur web etc... Le routeur va se substituer à vous lors de la connexion avec le site internet et vous renvoyer les informations sur votre téléphone avec son propre certificat.



Votre téléphone ne reconnaissant pas le certificat d'origine doit vous alerter.



Dans tous les cas, vous devez vous déconnecter et supprimer le réseau de vos paramètres WiFi de votre téléphone sinon il essayera de nouveau de s'y connecter.

Références :

- (fr) Wikipedia sur le système IMSI-catcher
- (en) Wikipedia page on the Stingray system.
- (en) Article in The Intercept on Stingray systems

▶ Suivant : Sécurité du téléphone, fiche 3

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