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 dévérouillé 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 dévérouillé 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 explotées.
- La protection par chiffrement doit se combiner avec une bonne hygiène numérique dont la réduction des données sensibles (par exemple en utilisant les messages éphèmères 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:

- Dévérouillé. La donnée est alors accessible que l'option du chiffrement du téléphone soit activée ou non.
- Téléphone non-chiffré et étéint. La donnée est accessible. Un téléphone peut être non chiffré même 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 vérouillé en ayant été dévérouillé au moins une fois depuis le dernier allumage, acronyme **AFU** pour **After First Unlock**.
- Etéint ou allumé et vérouillé sans avoir été dévérouillé 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 dévérouillé (pour la première fois), la clé de chiffrement est générée afin d'accéder à la donnée et de la déchiffrée. 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: éteintre son téléphone** ! En éteignant son téléphone, celui 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. A 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.

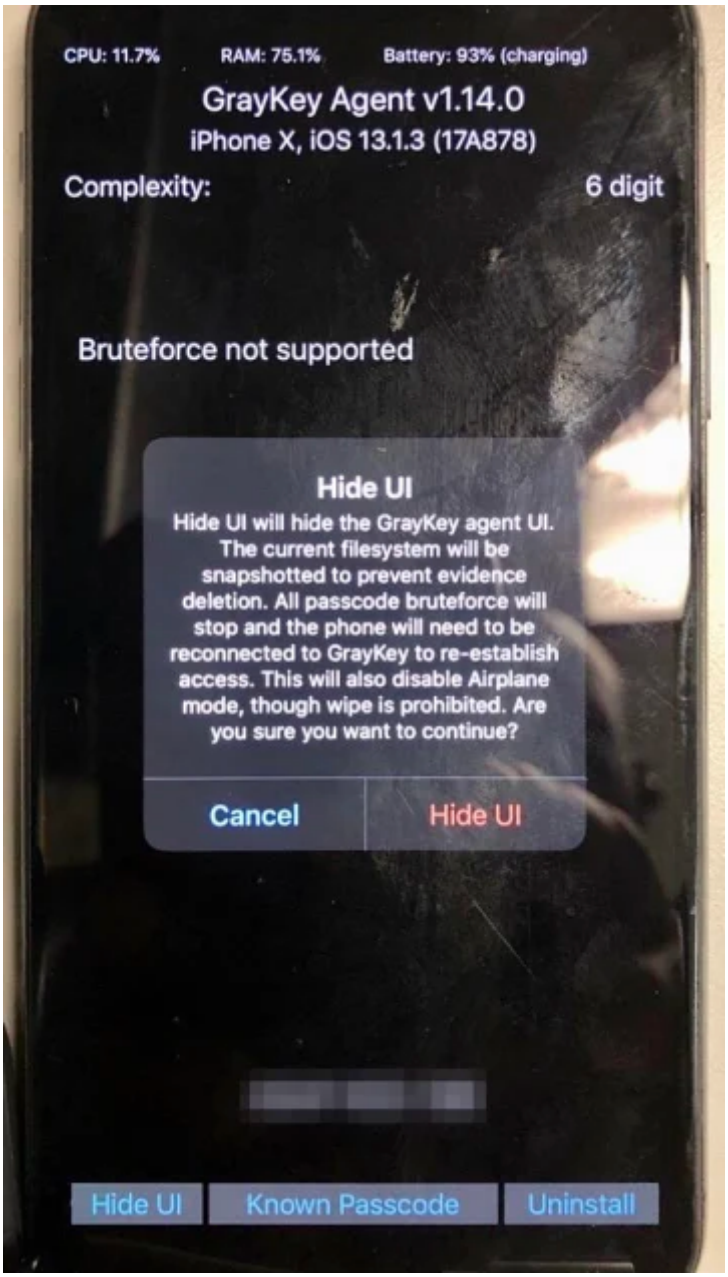
Comment s'en protéger ?

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 dévérouillé. 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, la 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

Redit - 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

Révision #1
Créé 8 September 2023 18:16:26 par mollusque
Mis à jour 8 September 2023 18:16:29 par mollusque