Sécurité et vie privée sur iOS

Par **Tom-Eliott Herfray** et **Natacha Padova**

1. Introduction

Installé par plus de 52% des utilisateurs américains de smartphones, iOS est aujourd'hui le second système d'exploitation le plus utilisé dans le monde après Android. De cela émane des préoccupations concernant la gestion des données et la sécurité générale de ce système qui regroupe aujourd'hui plus d'un milliard d'appareils dans le monde.

Source : *Statista*

Depuis plusieurs années, Apple s'efforce de communiquer sur le maintien total de la vie privée de ses utilisateurs et du respect stricto sensu de la confidentialité et de la sécurité de ses appareils. Entre des technologies anti-traçages de données, une architecture logicielle fermée et un cahier des charges rigoureux pour les développeurs tiers, retour dans cette fiche sur les principaux axes de respect de la vie privée et les fondations spécifiques de la sécurité sur la plateforme iOS.

2. Les arguments d'Apple pour un maintien de la vie privée

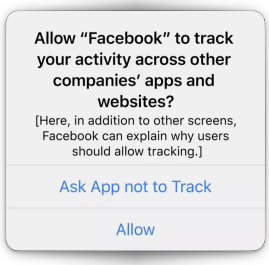
RGPD « Apple »

La vie privée sur les plateformes d'Apple est un argument marketing utilisé par la firme américaine depuis plusieurs années. Le PDG d'Apple, Tim Cook, a toujours soutenu la **RGPD** avant même son adoption par le Parlement européen en 2016, appelant même en 2019 dans une interview au Time à instaurer une RGPD aux États-Unis, expliquant que *« la technologie a le potentiel d'améliorer le monde, mais ne pourra pas le faire sans la confiance et la foi des personnes qui l'utilisent »*.

Apple a construit son propre RGPD au sein de son éco-système, en publiant chaque année un rapport de transparence sur la gestion des données des utilisateurs, mais également en incluant au sein même d'iOS des verrous numériques qui bloquent par exemple les traceurs de publicités personnalisées, l'*App Tracking Transparency*.

App Tracking Transparency

Présenté en 2021 lors de la conférence annuelle des développeurs (WWDC) et appliqué avec la dernière mise à jour d'iOS 14.5 en avril 2021, l'*App Tracking Transparency* a été une brique lancée dans l'océan des nombreux traceurs qui, à partir de vos données, personnalisent les publicités en ligne.



Exemple d'affichage du message d'avertissement de l'*ATT* sur Facebook.

L'instauration de ce nouvel outil, qui propose au lancement de l'application un message demandant à l'utilisateur s'il veut *« partager ses données personnelles avec des éditeurs de publicités tiers »* a fait couler énormément d'encres, notamment pour des acteurs comme Facebook dont les revenus proviennent majoritairement de la publicité.

Craig Federighi, VP de l'ingénierie logicielle d'Apple, rappelle que *« Les abus [sur l'utilisation des données] vont de l'effrayant au dangereux »* et qu'il est primordial de *« donner le choix aux utilisateurs »*. Avec cet outil, les utilisateurs peuvent ou non partager leurs données (localisation, données d'identité, ...) avec les applications tierces.

Relations avec les autorités : le cas Cellebrite

Apple applique une règle de déontologie souvent décriée dans le milieu des nouvelles technologies : le non-partage des données des utilisateurs avec les autorités compétences. L'exemple qui illustre cela est l'attentat terroriste de San Bernardino aux États-Unis en 2015. En effet, l'un des terroristes abattus durant la fusillade était en possession d'un iPhone verrouillé. Durant l'enquête officielle menée par le FBI, Apple refusa catégoriquement de déverrouiller l'appareil pour *« respecter la vie privée des utilisateurs »*. Elle invoqua des raisons technologiques selon lesquelles *« les outils d'Apple sont conçus inviolables y compris en interne par nos propres équipes »*.

C'est ainsi qu'une entreprise israélienne, *Cellebrite*, spécialisée dans le décodage et le déverrouillage d'appareils mobiles, prêta main forte aux autorités américaines pour forcer le déverrouillage de l'iPhone.

L'outil utilisé par Cellebrite pour déverrouiller les téléphones iOS et Android.

La solution de Cellebrite est basée sur la technologie du *jailbreak* (abordée dans la troisième section de cette fiche). Cette affaire a permis à *Cellebrite* de vendre des kits de déverrouillage de smartphones à plusieurs milliers de dollars à des entreprises privées ou des gouvernements étrangers, au détriment d'Apple qui explique pourtant que les développeurs certifiés respectent bien le manifeste confidentialité.

3. La sécurité au-delà des engagements de vie privée d'Apple

Si Apple communique beaucoup sur la gestion de la vie privée de ses utilisateurs, elle a également conçu un éco-système avec une architecture logicielle bien particulière et très fermée. Posons les bases du fonctionnement de cette architecture et prenons un exemple concret, celui du jailbreak, qui compromet partiellement la sécurité des informations stockées sur un appareil iOS ou iPadOS.

Architecture interne et stockage des données

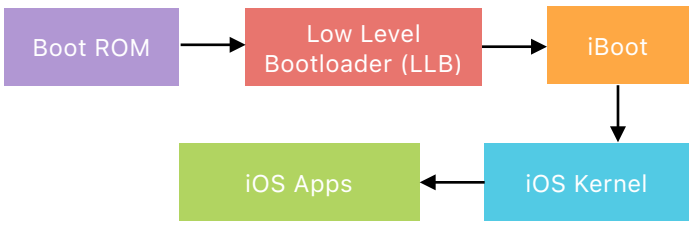
Secure Enclave

Les appareils sous iOS (ou iPadOS) sont basés sur une architecture Apple Silicon *(ARM)* : chaque iPhone possède un co-processeur sécurisé, ***Secure Enclave***, qui est isolé du processeur principal et qui fournit une couche de sécurité supplémentaire. Il est présent dans les iPhones 5s jusqu'aux modèles les plus récents. C'est un gestionnaire de clés, ces clés sont chiffrées dans la puce-sytème (circuit intégré incorporant plusieurs composants dont le *Secure Enclave*).

Il comprend une mémoire morte d'amorçage. C'est le premier code exécuté par le processeur lors du démarrage de l'appareil. Ce code fait partie intégrante du processeur, il est en *read-only*, ainsi il ne peut être modifié, par Apple ou qui que ce soit.

Au démarrage de l'appareil, le *Secure Enclave* :
- génère une clé éphémère de protection de mémoire
- combine cette clé avec l'UID spécifique de l'appareil

Secure Boot Chain



Au démarrage d'un appareil iOS, chaque étape du processus de démarrage contient des composants qui sont signés de manière cryptographique par Apple pour activer la vérification de l'intégrité afin que le démarrage ne se poursuive qu'après vérification de la chaîne de confiance, le graphique ci-dessus décrit ces étapes :
- **Boot ROM :** commence par l'exécution du code dans la mémoire morte d'amorçage (code immuable).
- **LLB** : étape supplémentaire du code invoqué par la mémoire morte d'amorçage pour les appareils dotés d'un processeur Apple Silicon A9 ou une version antérieure de la série A.
- **iBoot** : programme chargeant XNU (système d'exploitation Apple) suite au LLB ou à la mémoire morte d'amorçage.
- **iOS Kernel** : programme vérifiant les balises du code et confirmant que la signature de l'application existe.
- **iOS Apps** : va de pair avec le kernel. Pour iOS, toutes les applications doivent être signées depuis le lancement de l'App Store (iOS 2.0), cela inclut les binaires systèmes fournis avec iOS. Pour l'utilisateur final, cette application de signature de code ne peut pas être désactivée, ce qui fait qu'un utilisateur final ne peut installer que des applications à partir de l'App Store.

iOS va également à chaque *Secure Boot Chain* vérifier l'intégralité et la protection du :
- noyau : le contrôleur de mémoire offre une zone de mémoire physique protégée à iBoot (une fois l'étape terminée, cette zone refuse toute écriture).
- co-processeur : même mécanisme que pour le noyau, le matériel est « verrouillé » après le processus de démarrage.

Chiffrement et protection des données

La technologie de protection des données renforce la sécurité du stockage flash. En effet, la protection des données est mise en œuvre en élaborant et en gérant une hiérarchie de clés, et repose sur les technologies de chiffrement matériel intégrées à chaque appareil iOS : elle est contrôlée fichier par fichier en attribuant une classe à chacun d'eux, et l'accessibilité est déterminée en fonction de l'état de déverrouillage des clés de classe.

Il existe deux volumes APFS (*Apple File System*, un système de fichiers propre à Apple) sur iOS :
- **Volume système** : contient le système d'exploitation
- **Volume de données** : contient les données utilisateurs, à chaque fois qu'un fichier est créé sur le volume de données, la protection des données génère une nouvelle clé de 256 bits (la clé « par fichier ») et la transmet au programme qui gère le matériel. Celui-ci utilise cette clé pour chiffrer le fichier au moment de son écriture dans le stockage flash en utilisant le mode AES128-XTS, selon lequel la clé par fichier de 256 bits est répartie pour offrir une clé *« tweak »* de 128 bits et une clé de chiffre de 128 bits.

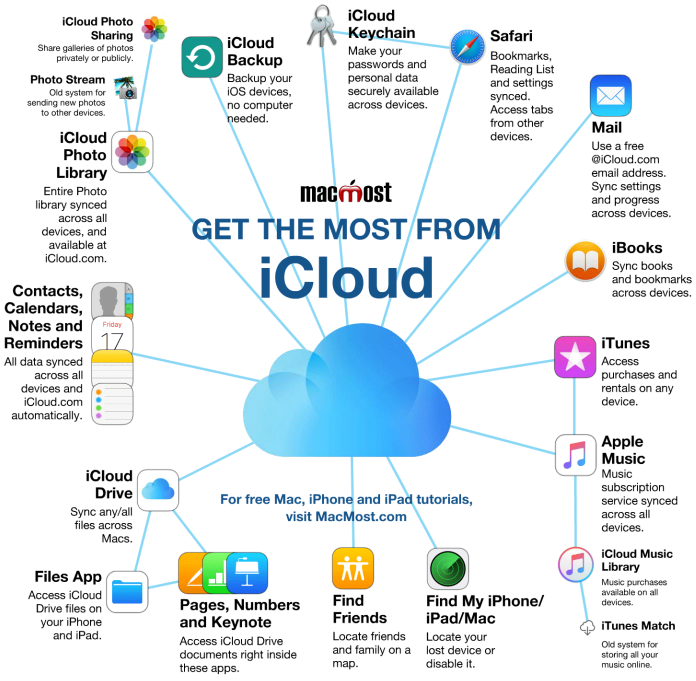
Différencier les données critiques des données personnelles et des données d'utilisateurs

De nombreuses données transitent aujourd'hui sur iOS ou les serveurs d'Apple, on peut regrouper cela sous forme de trois catégories distinctes :
- **les données stockées dans le disque nuagique ou les serveurs d'Apple** : ces données sont chiffrées puis partagées sur les serveurs d'Apple où ces derniers ne peuvent y accéder sans vos identifiants. Cela peut être par exemple vos photos, messages, contacts ou encore des sauvegardes automatiques de votre appareil.
- **les données sensibles de l'utilisateur stockées sur l'appareil** : ces données, souvent des données biométriques, médicales ou bancaires, sont conservées sur une puce dédiée sur l'appareil afin d'éviter que ces dernières ne soient déchiffrées.

- **les données publicitaires partagées** : il s'agit des « identifiants publicitaires » que les applications et services se partagent sur votre appareil, cela regroupe souvent des données anonymisées comme votre âge, sexe, ville ou vos préférences et goûts, pour vous proposer des offres publicitaires adaptées.

  Important : avec iOS 14.5 et l'*App Tracking Transparency* (abordé dans la deuxième section de cette fiche), Apple demande à chaque démarrage d'app si l'utilisateur désire partager cet identifiant avec des tiers.

Ces différentes données nous permettent de mieux comprendre ce qu'un tiers peut dérober sur un appareil iOS. En l'occurrence, les données stockées sur le disque nuagique, comme iCloud, peuvent facilement se faire dérober par une simple authentification sur un intranet par exemple (sans forcément parler des solutions en deux étapes mises en place par Apple).



Exemple de ce que iCloud, le service nuagique (ou cloud) d'Apple, peut stocker (Source : MacMost)

Si iOS est conçu comme un éco-système inviolable par son architecture et son mode de fonctionnement, il est cependant victime depuis plus d'une dizaine d'années de failles importantes de vulnérabilité ou failles zero-day, permettant de débrider son appareil iOS.

Débridage des appareils iOS : le cas du jailbreak

Présent depuis les premiers appareils iOS en 2007, le jailbreak est une solution de débridage visant à permettre aux utilisateurs iOS d'obtenir un accès complet en éliminant les restrictions et sécurités posées par Apple et évoquées précédemment. Il existe à ce jour trois catégories de jailbreak disponibles :

- **Tethered** : Jailbreak temporaire, avec besoin de le réinstaller à chaque redémarrage de l'appareil.
- **Semi-tethered** : Jailbreak présent au redémarrage mais avec des fonctionnalités réduites.
- **Untethered** : le jailbreak est complet et est conservé à chaque redémarrage.

En 2019, une équipe de chercheurs en cybersécurité présentait ***« checkm8 »***, un ensemble de failles impatchables par Apple permettant de débrider n'importe quel appareil iOS depuis l'iPhone 4s (puce A5) en octroyant un accès bas niveau. Ces failles rendues publiques ont permis la création de dizaines de logiciels de jailbreak, utilisés par des millions d'utilisateurs, par des autorités ou des entreprises privées pour accéder à des appareils iOS verrouillés.

La position d'Apple est très stricte concernant le jailbreak, les ingénieurs et chercheurs de l'entreprise américaine tentent de *patcher* quotidiennement ces failles. La justice américaine a par ailleurs autorisé l'installation des solutions issues du jailbreak sur des appareils iOS, les moyens légaux d'Apple sont ainsi limités.

Avantages	Défauts
Installer ce que l'on veut et donner le choix à l'utilisateur d'octroyer des accès	Un accès root est donné par défaut à l'ensemble des applications
« Tweaks » : scripts permettant de rajouter des fonctionnalités, y compris relatives à la sécurité	Des problèmes relatifs au SSH subsistent : ce dernier est installé par défaut

Le jailbreak représente un véritable risque pour la sécurité et la gestion des données relatives à la vie privée sur iOS. En effet, si à une époque le réel risque apparaissait lorsqu'un utilisateur installait sciemment un patch jailbreak sur son téléphone et qu'une application malicieuse dérobait ses données, le risque aujourd'hui est que des tiers puissent, à partir d'outils basés sur des technologies du jailbreak, accéder aux données critiques de n'importe quel appareil iOS.

Ainsi, si Apple vante les mérites de la sécurité d'iOS et de sa philosophie relative au strict respect de la vie privée de ses utilisateurs, elle ne peut les protéger des failles critiques qui apparaissent régulièrement sur Internet depuis de nombreuses années. Cependant et à ce jour, un utilisateur qui n'installera pas volontairement une solution de débridage sur son appareil ne verra pas ses données partagées avec des tiers car cela reste minoritaire, mais les failles évoluent rapidement et cela pourrait tendre à changer.

Sources

- *« Techniques and Types of Jailbreak »* — **UKEssays** (www.ukessays.com/essays/information-technology/techniques-types-jailbreak-5510.php)
- *« Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer »* — **ArsTechnica** (www.arstechnica.com/information-technology/2019/09/developer-of-checkm8-explains-why-idevice-jailbreak-exploit-is-a-game-changer)
- *« Technical analysis of the checkm8 exploit »* — **Habr** (www.habr.com/en/company/dsec/blog/472762)
- *« iOS Secure Boot »* — **Ashish Jha** (www.slideshare.net/pavj/ios-secure-boot)
- *« Apple appelle à la création d'un RGPD américain »* — **Le Big Data** (www.lebigdata.fr/donnees-apple-rgpd-usa)
- *« La confidentialité chez Apple »* — **Apple** (www.apple.com/fr/privacy)
- *« Interview de Craig Federighi »* — **MacGeneration** (www.macg.co/video/2021/04/apple-et-craig-federighi-font-le-service-apres-vente-de-lapp-tracking-transparency-121077)