CCN-CERT

BP/03

Dispositifs mobiles

RAPPORT DE LES MEILLEURES PRACTIQUES

MAI **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément toute garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et du logiciel indiqués, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Index

1. À propos de CCN-CERT

Le **CCN-CERT** est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de **contribuer à l'amélioration de la cybersécurité espagnole**, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN.

2. Introduction

La prolifération des appareils mobiles rendent nécessaire une réflexion sur la sécurité offerte par ce type d'appareils en ce qui concerne les informations qu'ils gèrent, tant dans les environnements d'entreprise que dans la sphère privée.

Ces dernières années, le développement des appareils et des communications mobiles ainsi que des technologies sans fil a révolutionné notre façon de travailler et de communiquer. L'utilisation croissante de ces technologies fait des appareils mobiles une cible de choix pour les attaquants.

La prolifération des appareils mobiles, ainsi que le développement de leurs capacités, de leurs fonctionnalités et de leurs possibilités d'utilisation, rendent nécessaire une réflexion sur la sécurité offerte par ce type d'appareils en ce qui concerne les informations qu'ils gèrent, tant dans les environnements d'entreprise que dans la sphère privée.

Un appareil mobile est considéré comme un appareil électronique à usage personnel ou professionnel de petite taille qui permet la gestion (stockage, échange et traitement) d'informations et l'accès à des réseaux de communication et à des services à distance, tant pour la voix que pour les données, et qui possède généralement des capacités de téléphonie, comme les téléphones mobiles, les *smartphones* (téléphones mobiles avancés ou intelligents), les *tablettes* (tablettes) et les agendas électroniques (*Personal Digital Assistant*), indépendamment du fait qu'ils possèdent un clavier physique ou un écran tactile.

2. Introduction

Le niveau de sensibilisation à la menace réelle n'a pas été suffisamment élevé parmi les utilisateurs finaux et les organisations, malgré le fait que les appareils mobiles sont utilisés pour les communications personnelles et professionnelles, privées et pertinentes, et pour le stockage et l'échange d'informations sensibles. Non seulement les organisations sont souvent la cible de nombreuses attaques, mais aussi les informations non professionnelles des utilisateurs (données personnelles).

Ces derniers temps, on a constaté une augmentation notable non seulement du nombre d'exemplaires de codes malveillants destinés aux appareils mobiles (maliciels mobiles), mais aussi de leur complexité et de leur sophistication, l'Espagne étant l'un des pays les plus touchés au monde par le nombre d'infections.

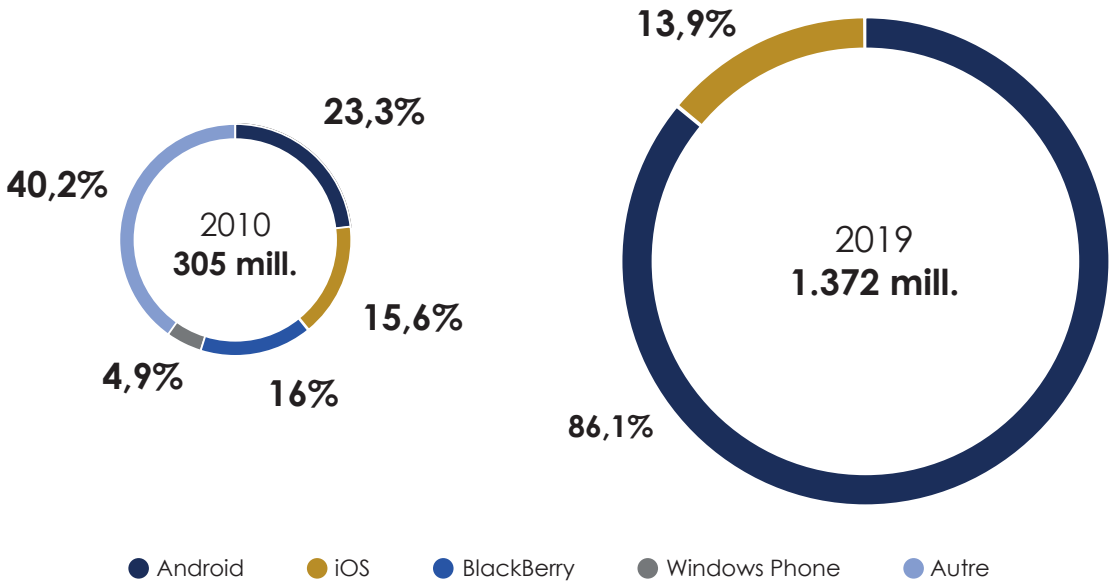


Figure 2-1 Part du marché mondial des appareils mobiles. Source : IDC[1]

La sensibilisation, le bon sens et les bonnes pratiques en matière de configuration et d'utilisation des appareils mobiles constituent la meilleure défense pour prévenir et détecter ces incidents et menaces.

1. "Worldwide Smartphone OS Market Share". IDC. Rapport. Q2 2015. http://www.idc.com/prodserv/smartphone-os-market-share.jsp

2. Introduction

En raison de l'adoption généralisée par l'industrie, tant par les entreprises que par les particuliers, de deux des plateformes mobiles avant toutes les autres, Android (Google) et iOS (Apple), la plupart des exemples utilisés dans ce guide font référence à ces deux plateformes mobiles[2].

L'objectif de ce document est de décrire ces pratiques afin d'**aider les utilisateurs** finaux à **protéger et à faire l'usage le plus sûr possible des appareils mobiles**, en allant jusqu'à la configuration et l'utilisation des mécanismes de protection existants.

À cette fin, un **ensemble de lignes directrices et de recommandations** en matière de sécurité sera proposé pour atténuer les éventuelles actions nuisibles, en fournissant des informations sur les techniques d'attaque les plus courantes, ainsi que sur les ressources utilisées par les attaquants pour infecter un appareil mobile ou obtenir des informations personnelles d'un utilisateur victime.

2. Il convient de noter qu'il existe des différences importantes dans la configuration et l'utilisation des appareils mobiles en fonction de la version particulière d'Android ou d'iOS disponible.

3. Les bonnes pratiques en matière de configuration et d'utilisation des appareils mobiles

L'ensemble des recommandations présentées ci-dessous est divisé en plusieurs groupes, chacun d'entre eux étant lié aux différentes capacités et fonctionnalités offertes par les dispositifs mobiles, telles que : **l'amélioration de la protection contre l'accès physique non autorisé au dispositif lui-même**, la **réduction de l'impact de la perte ou du vol**, ou **l'amélioration de la confidentialité et de la sécurité du stockage des informations** et **des communications avec d'autres équipements et services à distance**.

L'objectif de ces recommandations est que l'utilisateur puisse augmenter le niveau de protection et de sécurité de ses appareils mobiles, tant du point de vue de leur configuration que de leur utilisation quotidienne, évitant ainsi d'être victime de l'une des attaques susmentionnées.

Il faut tenir compte du fait que certaines des caractéristiques décrites et, par conséquent, des recommandations de sécurité proposées, dépendent du type de système d'exploitation utilisé par l'appareil mobile (Android, iOS, Windows Phone, etc.), de sa version et du fabricant et du modèle spécifiques qui lui sont associés.

Par conséquent, toutes les recommandations proposées ne seront pas nécessairement applicables à tous les appareils mobiles existants. Dans tous les cas, il est recommandé d'appliquer autant de recommandations que possible.

L'objectif de ces recommandations est que l'utilisateur puisse augmenter le niveau de protection et de sécurité de ses appareils mobiles, tant du point de vue de leur configuration que de leur utilisation quotidienne, évitant ainsi d'être victime de l'une des attaques susmentionnées.

3.1 Écran de verrouillage

L'écran de verrouillage est le principal mécanisme de défense contre l'accès physique non autorisé au dispositif mobile par un attaquant potentiel.

Les appareils mobiles modernes sont très attrayants pour le vol ou le cambriolage en raison de leur valeur économique (le *matériel* lui-même) et de la valeur associée aux informations sensibles et personnelles qu'ils stockent.

Pour cette raison, l'écran doit être protégé par un code d'accès et rester verrouillé le plus longtemps possible. Il est également recommandé de limiter les fonctionnalités disponibles sur l'écran de verrouillage à un tiers qui ne connaît pas le code d'accès.

3.1.1 Code d'accès ou empreinte digitale

Pour pouvoir accéder à l'appareil mobile et disposer de toutes les fonctionnalités offertes par celui-ci, il **est recommandé de protéger l'appareil mobile par un code d'accès associé à l'écran de verrouillage.**

Bien que ce code soit demandé à l'utilisateur à de multiples reprises au cours de la journée, il **est nécessaire de choisir un code d'accès robuste**, d'au moins six (6) ou huit (8) chiffres, et combinant de préférence des lettres et des chiffres. Il n'est en aucun cas recommandé d'utiliser un code PIN ou un code d'accès à quatre (4) chiffres, qui est par contre couramment utilisé.

En outre, afin que le dispositif mobile soit exposé à un accès non autorisé le moins longtemps possible, même temporairement, il **est recommandé de configurer le dispositif de manière à ce que le code d'accès soit demandé immédiatement après l'extinction de l'écran, qui devrait se verrouiller automatiquement dès que possible s'il n'y a pas d'activité de l'utilisateur** (par exemple, après une minute).

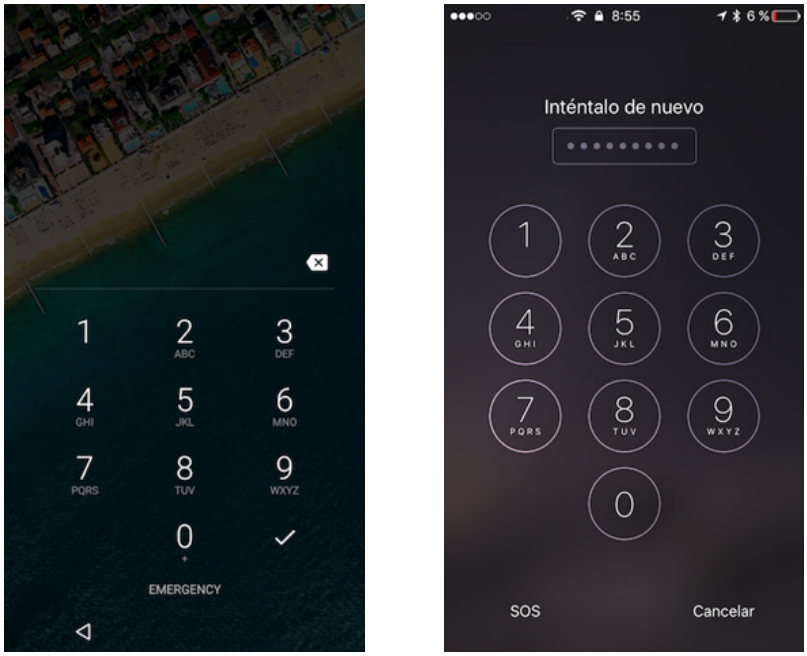


Figure 3-1 Écran de verrouillage avec code d'accès sur Android et iOS.

Afin de trouver le bon équilibre entre sécurité et fonctionnalité, en tenant compte du fait que l'utilisateur doit déverrouiller son appareil mobile des dizaines de fois par jour pour l'utiliser, il est recommandé de configurer la fonctionnalité de déverrouillage à l'aide d'une empreinte digitale (dans les appareils qui en sont dotés et qui possèdent un capteur d'empreintes digitales) complétée par un code d'accès fort.

Cette fonctionnalité permet au dispositif mobile de disposer d'un mécanisme de protection et de rendre son utilisation aussi confortable que possible pour l'utilisateur.

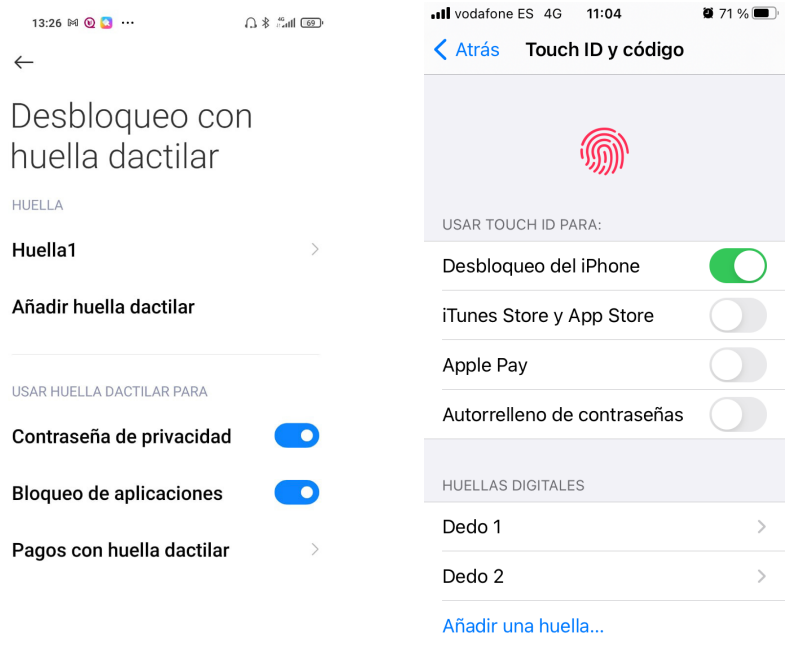


Figure 3-2 Écran de verrouillage par empreinte digitale sur Android et iOS.

3.1.2 Fonctionnalité de l'écran de verrouillage

L'écran de verrouillage du dispositif mobile permet à l'utilisateur d'accéder rapidement et facilement à de nombreuses capacités et fonctionnalités sans avoir à le déverrouiller, comme recevoir et répondre à des messages ou des appels téléphoniques, recevoir des notifications d'événements et des rappels, accéder à l'appareil photo, modifier certains paramètres tels que les capacités de communication sans fil (Bluetooth, Wi-Fi, 2/3/4G, etc.).) et gérer l'état du mode avion, accéder à des informations provenant d'applications spécifiques (*apps*), comme la météo ou des informations sur les investissements, ou interagir avec des assistants numériques personnels, comme Siri sur iOS, Google Assistant (ou Google Now) sur Android ou Cortana sur Windows (Phone).

La possibilité pour un tiers d'interagir avec certaines de ces capacités sans connaître le code d'accès a des implications très pertinentes du point de vue de la sécurité.

Par exemple, un attaquant potentiel qui obtiendrait un accès non autorisé à l'appareil mobile (après sa perte ou son vol) pourrait activer le mode avion de l'appareil mobile, interrompant toutes les communications de l'appareil mobile avec d'autres réseaux et services à distance, et rendant impossible les capacités de gestion à distance qui permettent à l'utilisateur de localiser l'emplacement actuel de l'appareil mobile ou de supprimer à distance les données qui y sont stockées (voir la section "3.7. Gestion à distance de l'appareil mobile").

En outre, de multiples vulnérabilités ont été identifiées au fil du temps sur la base de l'interaction avec ces capacités, qui permettent de contourner l'écran de verrouillage et le code d'accès de l'appareil mobile [3].

3. "Bypassing iOS Lock Screens: A Comprehensive Arsenal of Vulns". DinoSec. Blog Post. October 2016. http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html

Il est donc recommandé de limiter et de minimiser autant que possible les fonctionnalités disponibles sur l'écran de verrouillage si le code d'accès n'est pas saisi. Pour ce faire, il est recommandé de désactiver Google Assistant (ou Now) et de supprimer les icônes les plus critiques du panneau de contrôle d'accès aux Paramètres rapides disponible en haut d'Android (fonctionnalité disponible sur les versions Android 7.0 ou supérieures), tandis que pour iOS, il est recommandé de désactiver Siri, le Centre de contrôle disponible en bas ou le Centre de notification, ainsi que toute autre fonctionnalité pertinente.

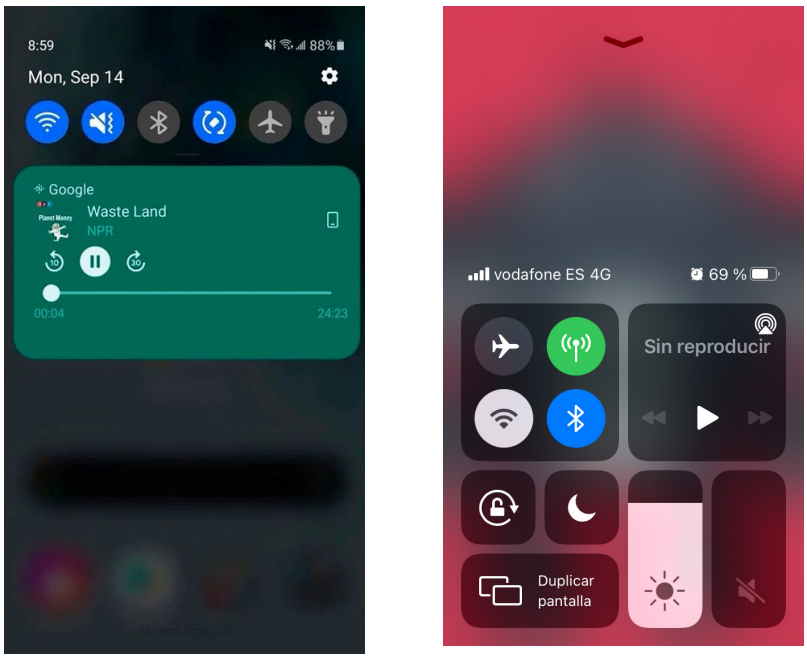


Figure 3-3 Fonctionnalités sensibles disponibles sur l'écran de verrouillage sur Android et iOS.

3.2 Communications USB

Les ports de charge et de synchronisation des appareils mobiles, normalement situés sur la partie inférieure, permettent la connexion par câble, via un port USB, à un ordinateur ou à une prise. La connexion USB offre deux (2) fonctionnalités : d'une part, elle permet la transmission d'énergie électrique pour charger la batterie de l'appareil mobile, et d'autre part, elle permet l'établissement de communications de données.

Étant donné que l'une des limites actuelles des appareils mobiles est la capacité et la durée de la batterie, et que les utilisateurs doivent parfois recharger leurs appareils mobiles au milieu de la journée et dans une certaine urgence, les attaquants ont utilisé cette double fonctionnalité des connexions ou communications USB pour compromettre les appareils mobiles par le biais de la connexion de données, en se faisant passer pour une station de recharge dans les lieux publics, une attaque connue sous le nom de *juice jacking*.

Grâce à cette attaque, il est potentiellement possible d'extraire des données personnelles stockées sur l'appareil mobile, ainsi que de mener des actions plus néfastes, comme l'installation *d'applications* malveillantes:

Ceci est connu sous le nom de la *prise de jus* est l'attaque qui consiste à voler les données des utilisateurs ou à installer des applications nuisibles sur leurs appareils lorsqu'ils les connectent à de fausses stations de recharge.

Figure 3-4 Attaques de juice jacking. Source : KrebsonSecurity[4]

4. "Beware of Juice-Jacking". KrebsonSecurity. Blog Post. Août. 2011. https://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Les systèmes d'exploitation modernes ont mis en place des mesures de protection contre ces attaques, et une relation de confiance doit être établie dès la première connexion de l'appareil mobile à un ordinateur via USB.

Le dispositif mobile demandera à l'utilisateur s'il souhaite établir cette relation de confiance, étant nécessaire de déverrouiller préalablement le dispositif mobile pour confirmer cette demande.

Il est donc recommandé de ne pas connecter votre appareil mobile à des ports USB inconnus et de n'accepter aucune relation de confiance via USB si vous ne savez pas que vous connectez votre appareil mobile à un ordinateur de confiance.

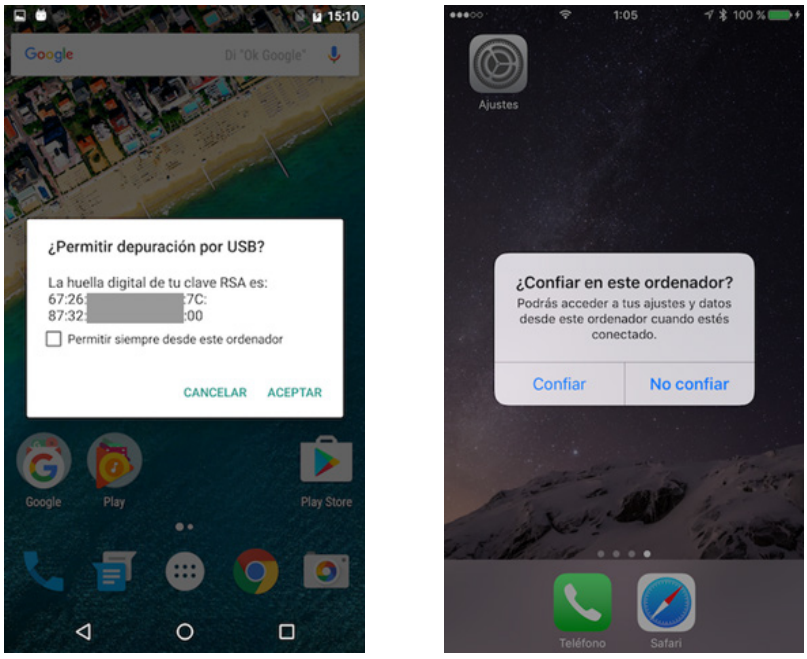


Figure 3-5 Établissement de relations de confiance via USB sur Android et iOS.

3. Les bonnes pratiques en matière de configuration et d'utilisation des appareils mobiles

Les capacités de communication USB des appareils mobiles permettent également d'y installer des applications (voir section 3.9). Pour qu'un attaquant potentiel réussisse à installer une *application*, l'appareil mobile doit avoir une configuration non sécurisée qui facilite ce type de communication (dans le cas d'Android) et/ou l'appareil mobile ne doit pas être verrouillé (dans le cas d'Android et iOS).

Pour empêcher l'installation d'applications via USB, il **est recommandé (selon la plateforme mobile) de ne pas activer les fonctions de débogage USB de l'appareil mobile**, qui sont disponibles spécifiquement pour les développeurs d'*applications*, **et de ne pas laisser l'appareil mobile sans surveillance sans le verrouiller**.

3.3 Mises à jour du système d'exploitation et des applications

Les appareils mobiles sont dotés d'un système d'exploitation mobile (Android, iOS, Windows Phone, etc.), également appelé *firmware*, qui fournit par défaut toutes les fonctionnalités existantes, et comprend également un ensemble d'applications mobiles qui ont été installées par défaut par le fabricant du système d'exploitation, de l'appareil ou de l'opérateur de télécommunications.

En outre, l'utilisateur peut installer d'autres *applications* tierces à partir des marchés d'applications officiels ou d'autres référentiels (voir la section 3.9 "Applications mobiles (apps)").

Il est recommandé de toujours disposer d'un système d'exploitation à jour sur l'appareil mobile. Il est également recommandé de **toujours disposer de la dernière mise à jour de toutes les *applications* installées sur l'appareil mobile.**

La dernière version du système d'exploitation et des *applications* corrige les vulnérabilités connues du public et réduit donc considérablement l'exposition de l'appareil aux attaques.

Il existe des outils offensifs pour exploiter les vulnérabilités des appareils mobiles qui ont la capacité de compromettre l'appareil en ouvrant simplement un message texte (SMS) ou un message multimédia (MMS), ou en visitant un lien web (sans avoir besoin de télécharger ou d'exécuter un fichier) en exploitant les faiblesses du navigateur web ou du système d'exploitation.

Étant donné que les outils incriminés ont parfois des *jours 0* (*exploits* pour des vulnérabilités inconnues qui n'ont pas été corrigées), il **est conseillé à l'utilisateur d'être très prudent lorsqu'il ouvre des messages ou des liens web non sollicités, inconnus ou étranges**.

La dernière version du système d'exploitation et des *applications* corrige les vulnérabilités connues du public et réduit donc considérablement l'exposition de l'appareil aux attaques.

3.4 Cryptage des appareils mobiles

Une caractéristique essentielle de la protection des données et des informations stockées localement par le dispositif mobile est le cryptage de sa mémoire interne, utilisée comme unité de stockage primaire, ainsi que de toute autre unité de stockage externe, telle qu'une carte SD (*Secure Digital*).

Les capacités de cryptage de la mémoire du dispositif mobile sont essentielles pour éviter qu'un tiers n'y accède physiquement sans autorisation, sinon il serait possible d'extraire le contenu de la puce mémoire du dispositif mobile et d'accéder à toutes les informations stockées.

Indépendamment du fait que certaines applications existantes sur le dispositif mobile chiffrent vos données avant de les stocker, il est recommandé d'utiliser les capacités de chiffrement natives du dispositif mobile, afin de protéger toutes les données et informations associées à l'utilisateur ou à l'organisation qui y sont stockées.

Pour utiliser ces capacités, il est essentiel d'établir un code d'accès sur le dispositif mobile, dont il est en outre recommandé qu'il soit robuste (voir section 3.1.1 "Code d'accès ou empreinte digitale"), car il sera utilisé pendant le processus de cryptage.

Est recommandé d'utiliser les capacités de chiffrement natives du dispositif mobile, afin de protéger toutes les données et informations associées à l'utilisateur ou à l'organisation qui y sont stockées.

Certains appareils mobiles, comme iOS, activent automatiquement les capacités de cryptage dès qu'un code d'accès est défini, un scénario indiqué par le texte *"La protection des données est activée"*, tandis que d'autres, comme Android, exigent que les mécanismes de cryptage soient activés intentionnellement.

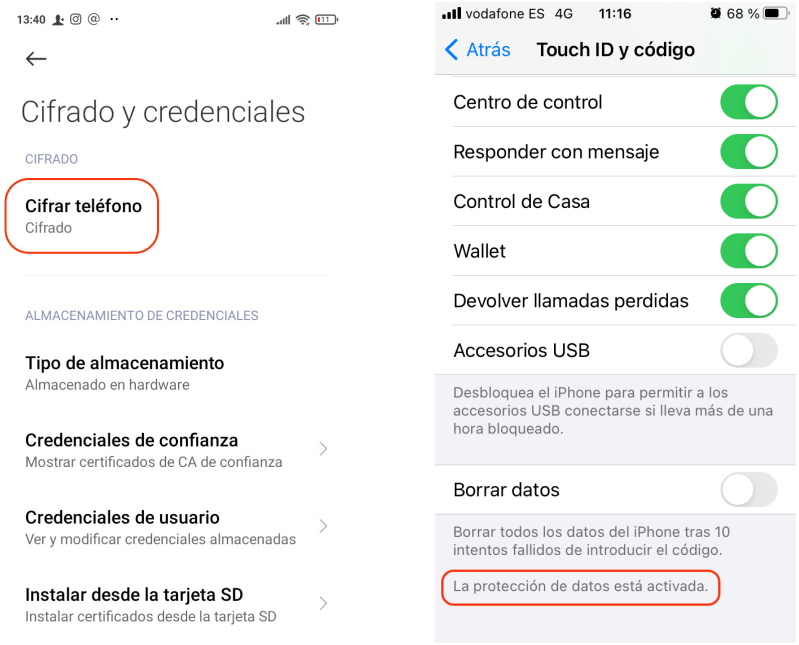


Figure 3-6 Activation des capacités de chiffrement natif sur Android et iOS. Source : EFF[5]

Si l'appareil mobile dispose d'un emplacement pour un disque de stockage externe, généralement basé sur l'utilisation de cartes mémoire SD, il **est recommandé d'utiliser des fonctions de cryptage qui permettent de protéger également le contenu du disque de stockage externe**.

Dans de nombreux cas, il n'est pas possible de chiffrer ce type de contenu. Il est donc recommandé de ne pas stocker de données ou d'informations sensibles sur la carte SD, comme des documents d'entreprise.

5. https://ssd.eff.org/en/module/how-encrypt-your-iphone

3.5 Paramètres par défaut

Les dispositifs mobiles, après leur activation initiale, ont une configuration par défaut qui, d'une part, peut être peu sûre et permettre des fonctionnalités qui pourraient être utilisées par un attaquant potentiel pour les compromettre et, d'autre part, contribuer à révéler des informations inutiles sur le dispositif lui-même et/ou son propriétaire.

Par exemple, il est courant que lorsque le dispositif mobile est activé, la plupart de ses services et capacités restent actifs, de sorte que l'utilisateur puisse les utiliser immédiatement, comme l'interface sans fil Bluetooth ou Wi-Fi, l'assistant numérique personnel ou les services de synchronisation en nuage.

Dans les appareils mobiles les plus modernes, d'autres services, considérés comme plus critiques du point de vue de la vie privée de l'utilisateur, tels que les services de localisation, doivent être activés manuellement par l'utilisateur au cours du processus de configuration initiale de l'appareil mobile.

Il est recommandé de désactiver tous les services et fonctionnalités de l'appareil mobile qui ne seront pas utilisés en permanence par l'utilisateur.

Il est plutôt recommandé de les activer uniquement lorsqu'ils vont être utilisés et de les désactiver à nouveau lorsque leur utilisation est terminée.

En outre, les informations relatives au dispositif lui-même et/ou à son propriétaire, telles que le fabricant et le modèle du dispositif ou le nom du propriétaire, peuvent être divulguées par le biais du nom du dispositif mobile, qui est diffusé sur les réseaux de communication de données ou par d'autres communications sans fil, telles que Bluetooth, ou par la mise en place d'un *point d'accès* Wi-Fi pour partager la connexion de données mobiles 2/3/4G.

Il est recommandé de modifier la configuration par défaut existante de l'appareil mobile, en supprimant toute référence aux caractéristiques techniques de l'appareil lui-même et/ou de son propriétaire.

3.6 Sauvegardes

La protection des informations et des données stockées et gérées par le dispositif mobile doit être étendue contre les scénarios de perte ou de vol du dispositif, ainsi que contre les dommages au matériel qui ne permettent pas d'accéder aux contenus existant sur son unité de stockage principale (ou les unités externes).

Pour éviter la perte de données, **l'utilisateur doit effectuer des sauvegardes régulières et de préférence automatiques de tout le contenu de l'appareil mobile à protéger et à préserver**, de préférence localement via une communication USB ou Wi-Fi sans fil avec l'ordinateur de l'utilisateur.

Vous pouvez également utiliser les capacités de sauvegarde en nuage associées aux principales plateformes mobiles, via une communication sans fil.

Toutefois, l'utilisateur doit être conscient que la facilité et la commodité associées à ces mécanismes de sauvegarde à distance ont des répercussions sur la confidentialité et la sécurité de ses données, car celles-ci seront transférées et stockées sur un serveur géré par un tiers (dans le nuage).

3.7 Gestion à distance du dispositif mobile

Les appareils mobiles modernes et les capacités de gestion à distance fournies par les fabricants d'appareils par l'intermédiaire de leurs plateformes mobiles et de leurs services en nuage, tels que iCloud[6] dans le cas d'iOS ou Device Manager[7] dans le cas d'Android, permettent à tout utilisateur de localiser potentiellement l'emplacement actuel de son appareil mobile, de le verrouiller s'il est actuellement déverrouillé, de le faire sonner pour identifier l'endroit où il se trouve, d'afficher un message pour que la personne qui le trouve puisse contacter son propriétaire, ou d'effacer à distance les données qui y sont stockées.

Il est recommandé à l'utilisateur de se familiariser avec les capacités de gestion à distance de l'appareil mobile et de sa plateforme mobile associée, et de vérifier le bon fonctionnement de ce service et de toutes ses fonctionnalités avant de devoir les utiliser dans un scénario réel après la perte ou le vol de l'appareil mobile.

Pour utiliser ces services, l'utilisateur doit disposer d'un compte sur la plateforme du fabricant, tel qu'un identifiant Apple (user ID) pour iCloud (iOS) ou un compte utilisateur Google pour Device Manager (Android). De plus, l'appareil mobile doit être associé au compte de l'utilisateur sur la plateforme du fabricant.

6. iCloud. Apple. Web. https://www.icloud.com
7. Android Device Manager (o Gestionnaire de périphériques Android). Google. Web. https://www.google.com/android/devicemanager

En outre, la fonctionnalité "Find My iPhone" (ou iPad, sur iOS) et "Device Manager" (sur Android) doit être activée et correctement configurée sur l'appareil mobile:

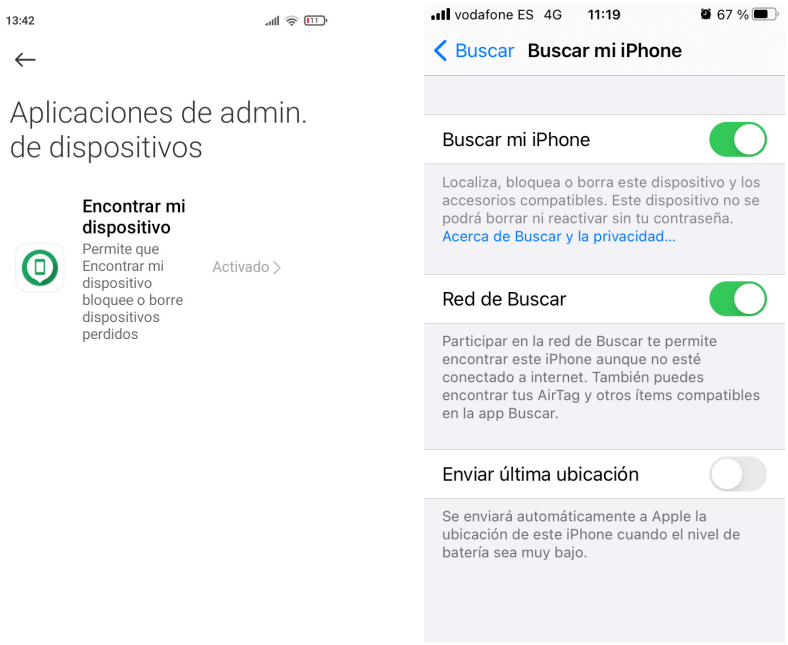


Figure 3-7 Activation des fonctions de gestion à distance sur Android et iOS.

Il convient de noter que nombre de ces capacités à distance ne seront pas réellement opérationnelles si la plate-forme de gestion ne peut pas contacter le dispositif mobile (ou vice versa) ou si le dispositif n'a pas la possibilité d'obtenir sa localisation.

Il existe de nombreuses raisons et scénarios dans lesquels la communication entre la plate-forme de gestion et le dispositif mobile ne peut pas être établie, ou la localisation actuelle ne peut pas être obtenue, par exemple le dispositif mobile est éteint, la batterie est épuisée, il n'y a pas de couverture des réseaux de données mobiles 2/3/4G ou aucun réseau Wi-Fi connu à proximité, le mode avion est activé, le dispositif se trouve dans le sous-sol ou le garage d'un bâtiment, etc.

3.8 Capacités de communication sans fil

D'autres aspects importants de la sécurité liés à la confidentialité et à l'intégrité des données échangées sur les réseaux de communication sont décrits ci-dessous.

De nombreuses fonctionnalités existantes dans les appareils mobiles impliquent l'utilisation de communications de données avec des plateformes distantes, dans lesquelles interviennent diverses technologies et services. La compréhension des scénarios d'utilisation et de fonctionnement, au moins de manière générique, de ces technologies nous permettra de connaître de manière plus approfondie, d'une part, les lacunes de sécurité qu'elles présentent et, d'autre part, les raisons pour lesquelles il est nécessaire de prendre certaines mesures de protection pour combler et améliorer ces lacunes.

En général, il **est recommandé de désactiver toutes les interfaces de communication sans fil du dispositif mobile qui ne seront pas utilisées en permanence par l'utilisateur**. Il est plutôt recommandé de les activer uniquement lorsqu'ils doivent être utilisés et de les désactiver à nouveau lorsque leur utilisation est terminée.

3.8.1 NFC (*Near Field Communications*)

Les capacités NFC des appareils mobiles permettent des communications sans fil à courte portée et sont actuellement utilisées pour le contrôle d'accès et pour effectuer des paiements à partir de l'appareil mobile, car elles sont intégrées aux *applications* et aux cartes bancaires.

Le fait d'avoir l'interface NFC active à tout moment pourrait permettre à un attaquant potentiel, suffisamment proche de l'appareil mobile, de forcer des transactions et des paiements frauduleux [8].

Le fait d'avoir l'interface NFC active à tout moment pourrait permettre à un attaquant potentiel, suffisamment proche de l'appareil mobile, de forcer des transactions et des paiements frauduleux.

3.8.2 Bluetooth et Bluetooth Low Energy (BLE)

Les technologies Bluetooth et BLE sont aujourd'hui largement utilisées pour l'intégration, la surveillance et le contrôle de multiples appareils électroniques, tels que les appareils personnels ou les *wearables* (comme les montres intelligentes ou *smartwatches*), les véhicules (mains libres) ou les appareils associés à l'Internet des objets (IoT, *Internet of Things*), à partir de l'appareil mobile lui-même, agissant comme le cerveau ou le contrôleur central du monde numérique qui l'entoure.

Par conséquent, le fait d'avoir l'interface Bluetooth active à tout moment pourrait permettre à un attaquant potentiel de manipuler les communications et les actions associées aux autres dispositifs ou les informations échangées entre eux[9].

---

8. "New Android NFC Attack Could Steal Money From Credit Cards Anytime Your Phone Is Near". Blog Post. May 2015. https://www.player.one/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497#:~:text=Gadgets-,New%20Android%20NFC%20Attack%20Could%20Steal%20Money%20From,Anytime%20Your%20Phone%20Is%20Near&text=This%20attack%2C%20delivered%20through%20poisoned,are%20near%20the%20victims'%20phone

9. "Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable". Blog Post. August 2016. https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

3.8.3 Wi-Fi

L'interface Wi-Fi est probablement le mécanisme de communication le plus utilisé aujourd'hui dans les appareils mobiles pour échanger des données et accéder à des services et applications à distance.

Le fait d'avoir l'interface Wi-Fi active à tout moment peut permettre à un attaquant potentiel de se faire passer pour n'importe lequel des différents réseaux Wi-Fi connus de l'appareil mobile et auxquels il se connecte habituellement (comme le réseau Wi-Fi du bureau, de la maison, de la bibliothèque, de la cafétéria, etc.), en le forçant à s'y connecter automatiquement, en étant capable de capturer tout le trafic généré/reçu par l'appareil mobile et d'effectuer des attaques directement sur celui-ci[10].

En outre, il **est recommandé de ne pas connecter votre appareil mobile à des réseaux Wi-Fi publics ouverts (ou *points* d'accès Wi-Fi) qui ne mettent en œuvre aucun type de sécurité**. Même si leur utilisation n'entraîne aucun coût, les informations personnelles de l'utilisateur sont mises en danger. L'utilisation de tels réseaux permet à un attaquant potentiel d'intercepter et de manipuler tout le trafic échangé par l'appareil mobile[11].

Au lieu de cela, utilisez des réseaux Wi-Fi qui sont fiables et pour lesquels des mécanismes de sécurité (tels que WPA2-PSK) sont configurés. Dans les rares cas où un réseau Wi-Fi public doit être utilisé, il convient d'utiliser un service VPN (*réseau privé virtuel*) pour crypter tout le trafic transmis sur le réseau Wi-Fi.

10. "Why Do Wi-Fi Clients Disclose their PNL for Free Still Today?". DinoSec. Blog Post. February 2015. http://blog.dinosec.com/2015/02/why-do-wi-fi-clients-disclose-their-pnl.html

11. "Avast free Wi-Fi experiment fools Mobile World Congress attendees". Avast. Blog Post. February 2016. https://blog.avast.com/2016/02/24/avast-free-wi-fi-experiment-fools-mobile-world-congress-attendees/

3.8.4 Réseaux de téléphonie: messagerie/ voix et données mobiles (2/3/4G)

L'une des capacités fondamentales offertes par la plupart des appareils mobiles modernes est la possibilité de se connecter aux réseaux de téléphonie mobile pour utiliser leurs services de voix, de messagerie et de données (2/3/4G).

On suppose que ces capacités seront actives sur les appareils mobiles la plupart du temps, afin de pouvoir passer et recevoir des appels, des messages et communiquer avec des services et des applications à distance lorsqu'un réseau Wi-Fi de confiance n'est pas disponible à proximité. Il est donc nécessaire d'être conscient des faiblesses de ces technologies qui ont commencé à se répandre à la fin des années 1980[12] en Europe (GSM).

Les réseaux de téléphonie 2G, qui existent encore aujourd'hui, ne font pas appel à des mécanismes de sécurité permettant au dispositif mobile d'être sûr qu'il se connecte au réseau légitime de l'opérateur de télécommunications (connu sous le nom d'authentification mutuelle).

Par conséquent, un attaquant peut se faire passer pour un réseau légitime (similaire aux réseaux Wi-Fi), forcer l'appareil mobile à s'y connecter automatiquement et intercepter à nouveau ses communications à l'aide de dispositifs appelés IMSI-Catchers ou Stingrays[13].

Il est recommandé à l'utilisateur de ne privilégier en aucun cas les réseaux 2G sur son appareil mobile par rapport aux réseaux 3G ou 4G, même si la consommation de la batterie est plus élevée sur ces derniers en raison, notamment, de leurs capacités élevées de transfert de données. Si possible, l'utilisation des réseaux 2G doit être désactivée.

12. http://www.gsmhistory.com/who_created-gsm/
13. "Surprise! Scans Suggest Hackers Put IMSI-Catchers All Over Defcon". Blog Post. August 2016. http://motherboard.vice.com/read/surprise-scans-suggest-hackers-put-imsi-catchers-all-over-defcon

3.8.5 Capacités et services de localisation

Enfin, la disponibilité de capacités et de services de localisation dans les appareils mobiles modernes, qui leur permettent de connaître leur emplacement dans le monde entier grâce au système de satellites GPS ou aux réseaux Wi-Fi et aux tours de téléphonie mobile, a ouvert un large éventail de services et de possibilités.

Cependant, l'obtention et le partage de la localisation du dispositif mobile en permanence, voire en temps réel, et donc de son propriétaire, ont des implications très pertinentes du point de vue de la vie privée et de la sécurité des utilisateurs.

D'une part, les services qui exploitent ces capacités peuvent surveiller et contrôler l'endroit où se trouve l'utilisateur à tout moment. D'autre part, l'utilisateur, volontairement ou par inadvertance, peut diffuser sa localisation actuelle ou passée par le biais des métadonnées des photographies prises avec l'appareil mobile et publiées par la suite, par des messages sur les réseaux sociaux ou par l'utilisation d'autres *apps*[14].

Il est recommandé à l'utilisateur de désactiver les services de localisation s'ils ne sont pas utilisés, et s'ils le sont, de limiter autant que possible leur utilisation intentionnelle, ainsi que l'accès à ces services par les applications installées sur l'appareil mobile, en désactivant la permission associée pour la plupart des *applications*.

14. "How mobile apps leak user data that's supposedly off-limits". Sophos. Blog Post. February 2016. https://nakedsecurity.sophos.com/2016/02/29/how-mobile-apps-leak-user-data-thats-supposedly-off-limits/

3.9 Applications mobiles (*apps*)

Les appareils mobiles tels que les *smartphones* sont considérés comme intelligents car, entre autres, ils ont la possibilité d'étendre les fonctionnalités par défaut existantes en installant de nouvelles applications mobiles (*apps*).

3.9.1 Installation d'*applications*

L'utilisateur peut installer de nouvelles *applications* à partir de magasins ou de marchés officiels, tels que Google Play (Android), App Store (iOS) ou Microsoft Store (Windows Phone), ou à partir d'autres dépôts ou marchés tiers non officiels (selon la plateforme mobile).

Certaines plateformes mobiles, comme iOS, n'autorisent par défaut que l'installation d'applications provenant du marché officiel. Par conséquent, bien qu'une infection par un code malveillant puisse se produire, celui-ci doit être introduit et propagé au préalable sur le marché officiel.

Bien qu'il y ait eu plusieurs cas de codes malveillants dans l'App Store d'Apple, les contrôles en place signifient que la probabilité d'infection est plus faible que sur d'autres plateformes mobiles, et une fois détecté, le code est retiré du marché dès que possible (bien que les appareils mobiles déjà infectés le restent).

D'autres plates-formes mobiles telles qu'Android sont plus flexibles et permettent, si l'utilisateur le souhaite, d'installer des *applications* à partir du marché d'*applications* officiel et d'autres marchés non officiels, ainsi que directement à partir de serveurs web ou par le biais de messages électroniques incluant l'*application* en pièce jointe[15]. Cette flexibilité est utilisée par les attaquants pour distribuer des codes malveillants et infecter les appareils mobiles des utilisateurs victimes.

Depuis peu, dans les versions plus modernes d'iOS (9 ou plus), il est également possible d'installer des *applications* via USB (voir section 3.2 "Communications via USB"), une technique connue sous le nom de *sideloading*, comme dans les versions précédentes d'Android, si l'appareil a une configuration non sécurisée ou n'est pas verrouillé (selon la plate-forme mobile).

Compte tenu de ces capacités, il est important que l'utilisateur n'installe aucune *application* qui ne provient pas d'une source de confiance, comme les marchés d'*applications* officiels.

Sur les plates-formes mobiles qui disposent de cette flexibilité, il est recommandé de ne pas activer la fonctionnalité qui permet l'installation d'*applications* provenant de dépôts tiers non fiables (sources inconnues) et de n'installer en aucun cas des *applications* provenant de sources peu recommandables, même si elles sont gratuites.

Il est préférable de payer le prix d'une *application* (entre 0,99€ et 2,99€ pour la plupart d'entre elles), plutôt que d'exposer toutes nos informations personnelles juste pour économiser quelques euros.

Il est important que l'utilisateur n'installe aucune application qui ne provient pas d'une source de confiance.

15. "Alternative (Open) Distribution Options". Android Developers. Documentation. https://developer.android.com/distribute/tools/open-distribution.html

3.9.2 Autorisations de l'application

Les appareils mobiles ont un environnement d'exécution restreint, où une *application* n'a pas accès aux fichiers et aux données des autres *applications* ou du système d'exploitation par défaut. Pour avoir accès à ces données et/ou à des fonctionnalités supplémentaires, l'*application* doit demander des autorisations à l'utilisateur, par exemple pour accéder à ses contacts, à son calendrier, aux composants matériels de l'appareil mobile, tels que l'appareil photo ou le microphone, ou aux photos.

En fonction de la plateforme mobile et de la version du système d'exploitation, des autorisations seront demandées à l'utilisateur lors de l'installation de l'*application*, ou pendant son exécution, lors de l'utilisation de certaines fonctionnalités pour lesquelles une autorisation spécifique est requise, comme, par exemple, une application qui permet de scanner des codes-barres et qui demande l'autorisation d'accéder à l'appareil photo de l'appareil mobile.

Il est recommandé de ne pas accorder de permissions inutiles ou excessives aux *apps*, limitant ainsi les données et les fonctionnalités auxquelles elles auront accès. Pour ce faire, il est nécessaire que l'utilisateur comprenne d'abord pourquoi une application demande une autorisation particulière et à quoi sert cette autorisation dans le cadre de la fonctionnalité fournie par l'*application*.

Les *applications* correctement développées doivent informer l'utilisateur des raisons spécifiques de la demande d'autorisation.

Il est recommandé de ne pas accorder de permissions inutiles ou excessives aux apps, limitant ainsi les données et les fonctionnalités auxquelles elles auront accès.

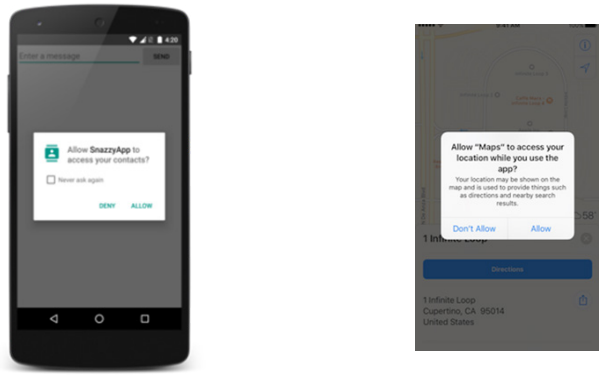


Figure 3-8 Demandes de permission par les applications sur Android et iOS. Source: Développeurs Android[16] et Développeurs Apple[17].

16. Requesting Permission. Apple Developers. https://developer.apple.com/ios/human-interface-guidelines/interaction/requesting-permission/
17. Requesting Permissions at Run Time. Android Developers. https://developer.android.com/training/permissions/requesting.html

3.9.3 Adresse électronique

L'une des tâches les plus courantes pour lesquelles les appareils mobiles sont utilisés est l'accès au courrier électronique, avec une *application* par défaut pour l'utilisation de ce service.

Il est recommandé de consulter le guide des meilleures pratiques en matière de messagerie électronique du CCN-CERT[18], car nombre des recommandations qu'il contient s'appliquent non seulement aux ordinateurs traditionnels (tels que les PC), mais aussi aux appareils mobiles.

3.9.4 Applications de messagerie

En outre, les appareils mobiles sont fréquemment utilisés pour établir des communications personnelles et professionnelles avec la famille, les amis, les connaissances, les collègues et d'autres contacts professionnels par le biais d'applications de messagerie, soit en envoyant et en recevant des messages texte (SMS) ou des messages multimédia (MMS), soit en utilisant d'autres services de messagerie tels que WhatsApp, Telegram, Line, etc.

Par l'intermédiaire de ces services, il est possible de recevoir des messages contenant des liens Internet avec du code malveillant, dans le but d'infecter et de compromettre l'appareil mobile de l'utilisateur victime. L'utilisation de liens malveillants est l'une des techniques les plus couramment utilisées pour exécuter du code sur l'appareil mobile de la victime ou pour obtenir des informations de celle-ci. Le type de lien (où il pointe, quel type d'actions il va exécuter, etc.) dépendra des objectifs des attaquants.

18. "Bonnes pratiques. CCN-CERT BP-02/16. Courrier électronique". CCN-CERT. Rapport. Juillet 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html

Les utilisations les plus courantes des liens malveillants sont décrites dans le guide des bonnes pratiques de messagerie du CCN-CERT[19], et s'appliquent aux communications par messagerie : hameçonnage, téléchargement de fichiers malveillants ou de *kits d'exploitation Web*.

Les attaques basées sur des liens malveillants distribués via des applications de messagerie sont souvent appelées SMiShing , plutôt que phishing (terme utilisé dans la distribution de courriers électroniques), et comprennent également des messages attrayants, suggestifs ou pour lesquels l'utilisateur doit prendre des mesures urgentes:

Les attaques basées sur des liens malveillants distribués via des applications de messagerie sont souvent appelées SMiShing.

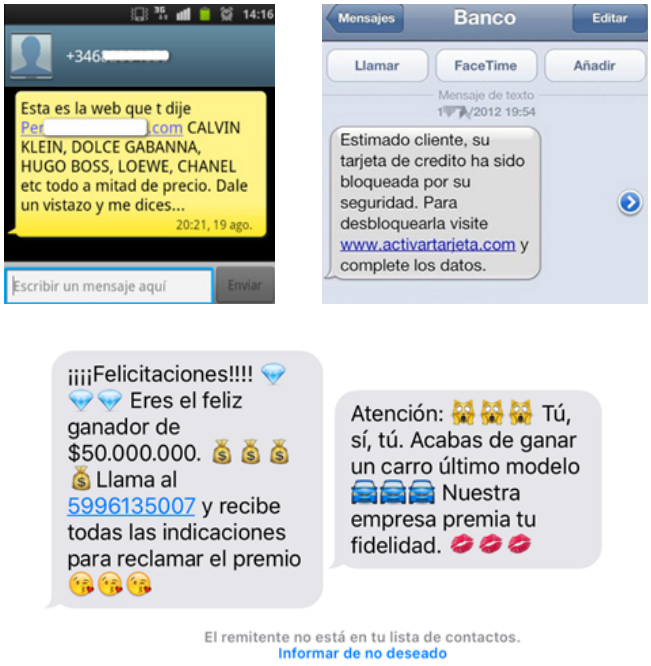


Figure 3-9 Exemples de messages SMiShing. Sources: OSI[20], Hora Jaén[21], MDE[22].

19. "Bonnes pratiques. CCN-CERT BP-02/16. Courrier électronique". CCN-CERT. Rapport. Juillet 2016. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-correo-electronico/file.html
20. https://www.osi.es/es/actualidad/blog/2013/09/09/fraudes-online-vii-smishing-estafa-que-llega-traves-de-un-sms
21. http://horajaen.com/detienen-a-siete-jiennenses-por-una-estafa-de-pishing/
22. http://descubre.mdeinteligente.co/smishing-5-consejos-para-cuidarte-de-las-estafas-via-mensaje-de-texto/

L'attaque baptisée Pegasus[23] qui s'est déroulée en août 2016 contre Ahmed Mansoor, un défenseur des droits de l'homme de renommée internationale basé aux Émirats arabes unis, a utilisé de telles techniques basées sur l'envoi d'un SMS malveillant pour tenter d'infecter l'iPhone de la victime et d'en prendre le contrôle total à l'aide d'un *logiciel espion* sophistiqué, en employant trois nouvelles vulnérabilités (0 jours) jusque-là inconnues du public:

Figure 3-10 SMS nuisibles reçus par Mansoor avec un expéditeur usurpé (Pegasus). Août: Citizenlab[23]

Sans aucun doute, le conseil le plus efficace pour identifier les messages nuisibles est le bon sens, tout comme pour le courrier électronique. Cela signifie **que tout symptôme ou tendance en dehors de ce qui est considéré comme normal ou habituel doit éveiller les soupçons de l'utilisateur**.

Un schéma ou un symptôme irrégulier peut signifier: recevoir un message d'un expéditeur inconnu, recevoir un message demandant des informations personnelles, le contenu du message étant trop attrayant pour être vrai, etc.

23. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender". Citizenlab. Blog Post. Août 2016. https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Par exemple, un message envoyé par une entreprise digne de confiance qui présente un sujet ou une demande inhabituelle et inclut un lien devrait susciter une certaine méfiance de la part de l'utilisateur. Dans ce cas, la meilleure chose à faire avant de cliquer sur le lien est de contacter l'expéditeur supposé en utilisant un autre moyen de contact, comme le téléphone, le courrier électronique, etc. De cette façon, il sera possible de corroborer si le message reçu est légitime ou non.

Il faut garder à l'esprit que, comme pour les courriels, un attaquant peut parfois se faire passer pour l'expéditeur du message, en essayant d'usurper son identité, de sorte que ces informations ne doivent pas faire l'objet d'une confiance aveugle.

3.9.5 Réseaux sociaux

Une autre utilisation courante des appareils mobiles par les utilisateurs est l'interaction avec les réseaux sociaux, tels que Facebook, Twitter, Instagram, etc.

Lors de la publication de tout type d'informations ou d'images personnelles sur les réseaux sociaux, il **est recommandé d'évaluer la sensibilité et la confidentialité des données à publier et de tenir compte du fait que ces contenus seront potentiellement accessibles à de nombreuses personnes**, et pas seulement au cercle fermé des amis de l'utilisateur.

Ces informations sont souvent utilisées pour contraindre l'utilisateur à les diffuser ou le faire chanter, ainsi que pour obtenir des données décisives ou établir des relations et des communications qui déterminent le succès ou l'échec d'une campagne de *spear phishing* contre l'utilisateur ou l'organisation dans laquelle il travaille.

3.9.6 Navigation sur le Web

De même, il est très courant que les appareils mobiles soient utilisés pour des tâches de navigation sur le web, dans le but de consulter des contenus web ou d'interagir avec une multitude de services disponibles sur l'internet, en utilisant le navigateur web standard ou une application spécifique pour son utilisation.

Le protocole impliqué dans le processus de navigation sur le web pour accéder au contenu et aux services du web est le HTTP. Ce protocole est utilisé depuis 1991[24] et, lors de sa mise en œuvre, aucune mesure de sécurité, telle que le cryptage ou l'authentification forte des communications, n'a été prise en compte.

Cela signifie que l'ensemble du processus de demande et de réponse au contenu entre l'appareil mobile et un serveur ou une application web se fait en texte clair, ce qui signifie qu'à tout moment de la transmission, un attaquant peut voir et manipuler le contenu des pages web.

En raison de ces lacunes du protocole HTTP, diverses technologies et extensions ont été développées pour intégrer des mesures de sécurité aux communications web, par exemple pour assurer le cryptage des données transmises. C'est pourquoi le protocole HTTPS a été créé, sur la base de TLS, en indiquant ses caractéristiques de sécurité supplémentaires par la lettre "S".

L'utilisation du protocole HTTPS permet, par exemple, d'initialiser un échange TLS avec le serveur web avant d'envoyer des données sensibles, telles que les informations d'identification de l'utilisateur nécessaires pour accéder à un service web comme le courrier électronique, les réseaux sociaux ou une banque ou un magasin en ligne. De cette façon, un attaquant qui surveillerait les communications ne pourrait pas accéder à ces informations sensibles.

24. http://info.cern.ch/hypertext/WWW/History.html

Dans le cas de la navigation web à travers un dispositif mobile, tel que Safari, Chrome, Firefox, etc., l'utilisateur a la possibilité d'indiquer qu'il veut utiliser le protocole HTTPS, contrairement aux communications utilisées par les applications mobiles, où la connexion est effectuée automatiquement par l'*application*, sans que l'utilisateur ne doive ou ne puisse indiquer le serveur auquel il veut se connecter ou comment il veut se connecter.

Les fournisseurs les plus populaires, les organisations et les entreprises qui ont un site web permettent l'accès à leurs serveurs web via HTTPS, bien que de nombreuses organisations utilisent encore exclusivement HTTP.

Il est donc recommandé, dans la mesure du possible, d'utiliser le protocole HTTPS en insérant le texte "https://" avant de saisir l'adresse web du serveur auquel vous souhaitez vous connecter.

Il convient de noter que ces mesures de sécurité sont susceptibles d'être attaquées. Par exemple, le protocole HTTPS est vulnérable aux attaques de type *"Man-in-the-Middle"* (MitM), où un attaquant se place au milieu de la communication entre l'appareil mobile et le serveur ou l'application web distant afin de manipuler la communication.

D'une part, l'attaquant peut essayer de se faire passer pour le serveur ou l'application web légitime, en proposant à l'utilisateur victime un certificat numérique qui peut être similaire au certificat légitime, mais qui ne sera pas accepté comme valide ou digne de confiance par son navigateur web.

En conséquence, le navigateur Web génère un message d'erreur de certificat qui, s'il est accepté par l'utilisateur, entraîne l'établissement d'une connexion cryptée avec l'attaquant, ce qui permet à ce dernier d'intercepter toutes les données échangées, y compris les identifiants de connexion et d'autres informations sensibles et critiques.

D'autre part, l'attaquant peut essayer d'éliminer l'utilisation de HTTPS dans toutes les communications entre l'utilisateur et le serveur ou l'application web légitime, en utilisant une attaque connue sous le nom de sslstrip, avec des conséquences similaires pour l'utilisateur.

L'utilisateur ne doit jamais accepter un message d'erreur du navigateur web associé à un certificat numérique invalide, et il est recommandé d'annuler la connexion. Au lieu de cela, vous devriez vérifier que vous vous connectez réellement au serveur web auquel vous essayez de vous connecter via l'adresse web et essayer d'obtenir plus de détails sur la raison pour laquelle l'erreur de certificat a été générée.

S'il est nécessaire d'établir la connexion, il est recommandé d'utiliser un autre réseau, par exemple, le réseau de données mobiles 2/3/4G, si vous utilisiez un réseau Wi-Fi, ou même un ordinateur connecté à un réseau différent, comme le réseau du bureau ou de la maison.

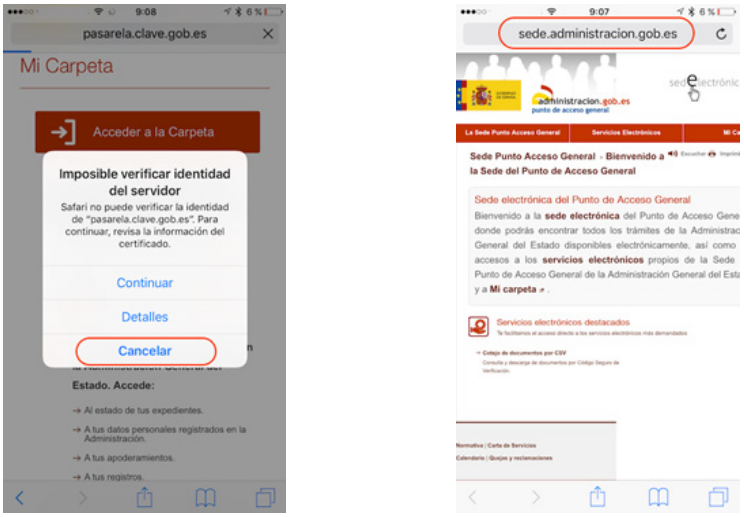


Figure 3-11 Attaques MitM et sslstrip: erreur de certificat ou absence de HTTPS.

Pour vérifier si la connexion à un serveur ou une application web est cryptée, il faut vérifier que la barre d'adresse du navigateur web utilise le protocole HTTPS, indiqué par le texte "https://" au début de l'adresse web.

Malheureusement, par défaut, la barre d'adresse des navigateurs web sur les appareils mobiles modernes a tendance à minimiser les informations affichées à l'utilisateur, ne mettant en évidence que le domaine vers lequel la connexion a été établie.

Pour obtenir tous les détails du serveur web et de la ressource consultée, ainsi que pour vérifier si la méthode de connexion utilisée est HTTPS (vérifier qu'un cadenas apparaît n'est pas toujours suffisant), il peut être nécessaire de sélectionner la barre d'adresse et de la faire défiler vers la gauche pour afficher tous les détails:

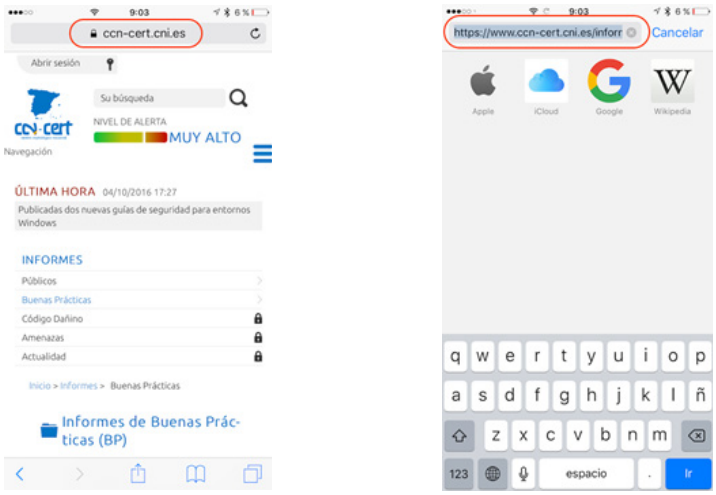


Figure 3-12 Attaques MitM et ssltrip: vérification manuelle de l'utilisation de HTTPS.

4. Autres recommandations de nature générique

Du point de vue de l'entreprise, il est recommandé d'utiliser des solutions de *gestion des appareils mobiles d'entreprise* (MDM), dans le but de disposer de capacités permettant de définir, d'établir et de surveiller les différentes recommandations de sécurité sur tous les appareils mobiles de l'organisation de manière homogène.

Ces solutions permettent d'appliquer des configurations de sécurité aux appareils mobiles en fonction des politiques de sécurité préalablement définies par l'organisation.

Le processus de *jailbreaking* (iOS) ou de *rooting* (Android) consiste à effectuer certaines actions (en exploitant intentionnellement des vulnérabilités) sur l'appareil mobile pour en prendre le contrôle total et disposer d'un maximum de privilèges.

Bien que certains utilisateurs effectuent ce processus pour disposer de capacités et de fonctionnalités qui n'existent pas par défaut, en raison des limitations imposées par le fabricant, son utilisation n'est pas recommandée.

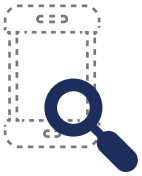
Par conséquent, un grand nombre des mécanismes de sécurité existants sur les plateformes mobiles sont désactivés. Sans connaissances techniques suffisantes, après un *jailbreaking* ou un *rooting*, l'utilisateur disposera d'un appareil

4. Otras recomendaciones de carácter genérico

Il est recommandé d'utiliser des mots de passe forts[25] pour chacun des services et des applications auxquels on accède depuis le dispositif mobile. Ces mots de passe ne doivent pas être réutilisés entre différents services ou applications.

De plus, pour les services ou applications qui disposent de cette fonctionnalité, et notamment pour les plus critiques, il est recommandé d'utiliser un second facteur d'authentification.

Dans la mesure du possible, il est recommandé de ne pas stocker les informations d'identification des différents services et applications utilisés sur l'appareil mobile lui-même, car elles pourraient être récupérées en cas d'infection de l'appareil.



Si l'appareil mobile est perdu ou égaré, ou si un comportement anormal ou suspect est identifié lors de son utilisation, il doit être signalé immédiatement au responsable de la sécurité de l'organisation.

Outre le code d'accès, il est recommandé de définir le code PIN associé à la carte SIM afin d'éviter les abus et l'utilisation non autorisée des fonctions de communication téléphonique, comme les appels téléphoniques. Le code d'accès et le code PIN de la carte SIM doivent être différents.

Afin d'identifier d'éventuelles infections de l'appareil mobile ou tout autre type de fraude liée, l'utilisateur doit vérifier mensuellement la consommation associée à son contrat à travers la facture de l'opérateur de téléphonie mobile et identifier dès que possible les anomalies, telles que l'envoi de messages texte (SMS) ou multimédia (MMS), ou la réalisation d'appels vocaux non reconnus.

25. Schneier on Security. Blog Post. March 2014. https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

5. Décalogue de recommandations

L'objectif de ce décalogue de bonnes pratiques est d'améliorer le niveau de protection et de sécurité des appareils mobiles.

Décalogue de sécurité pour les appareils mobiles

1. **Le dispositif mobile doit être protégé par un code d'accès fort** associé à l'écran de verrouillage (ou, à défaut, par une empreinte digitale).

   Le code d'accès doit être demandé immédiatement après l'extinction de l'écran, et l'écran doit se verrouiller automatiquement dès que possible en l'absence d'activité de l'utilisateur. L'appareil mobile ne doit pas être laissé sans surveillance sans verrouillage.

2. **Utilisez les capacités de cryptage natives de l'appareil mobile** pour protéger toutes les données et informations stockées sur l'appareil.

3. **Le système d'exploitation de l'appareil mobile doit toujours être à jour**, de même que toutes les applications mobiles (*apps*).

4. **Ne connectez pas votre appareil mobile à des ports USB inconnus et n'acceptez aucune relation de confiance via USB** si vous ne savez pas que vous connectez votre appareil mobile à un ordinateur de confiance.

5. **Désactivez toutes les interfaces de communication sans fil de l'appareil mobile** (NFC, Bluetooth et BLE, Wi-Fi, services de localisation, etc.) qui ne seront pas utilisées en permanence par l'utilisateur. Ils doivent être activés uniquement lorsqu'ils doivent être utilisés et désactivés à nouveau à la fin de leur utilisation.

6. **Ne connectez pas votre appareil mobile à des réseaux Wi-Fi publics ouverts** (ou *points d'accès* Wi-Fi) qui ne mettent en œuvre aucun type de sécurité.

7. **N'installez pas d'application mobile (app) qui ne provient pas d'une source de confiance,** comme les marchés d'applications officiels (Google Play, App Store, etc.).

8. **Il est recommandé de ne pas accorder de permissions inutiles ou excessives aux apps**, limitant ainsi les données et les fonctionnalités auxquelles elles auront accès.

9. **Dans la mesure du possible, il convient d'utiliser le protocole HTTPS** (en insérant le texte "https://" devant l'adresse web du serveur à contacter).

   Un message d'erreur concernant un certificat numérique invalide ne doit jamais être accepté.

10. **Il convient d'effectuer des sauvegardes régulières,** et de préférence automatiques, de tout le contenu du dispositif mobile à protéger et à préserver.

CCN centro criptológico nacional

CCN cert centro criptológico nacional

Figure 5-1. Décalogue de sécurité

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es