Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 28 juillet 2015

N° DAT-NT-010/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 10

Note technique

Recommandations de sécurité relatives aux ordiphones

Public visé:

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Recommandations de sécurité relatives aux ordiphones** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (`www.etalab.gouv.fr`). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document:

Contributeurs	Rédigé par	Approuvé par	Date
BSS, LAM	DAT	SDE	28 juillet 2015

Évolutions du document :

Version	Date	Nature des modifications
1.0	15 mai 2013	Version initiale
1.1	19 juin 2013	Corrections mineures
1.2	28 juillet 2015	Reformulation de la recommandation R9

Pour toute remarque:

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule

L'usage des ordiphones (smartphones) ou des tablettes est de plus en plus répandu en environnement professionnel. Ces terminaux disposent de nombreuses fonctionnalités :

- capteurs divers (GPS, altimètre, gyromètre, accéléromètre, microphone, caméra, etc.) ;
- communication par liaison sans-fil ;
- grande capacité de stockage ;
- performances permettant l'usage d'applications sophistiquées ;
- etc.

Ces terminaux permettent par exemple, en plus d'être joignable, de consulter ses courriels et de naviguer sur internet à la recherche de tout type d'information. Plus encore, ils rendent possible la connexion à un réseau d'entreprise pour travailler sur des applications métier ou accéder à des documents comme tout un chacun le ferait depuis son poste de travail professionnel. En parallèle, de nombreux usages personnels, souvent ludiques, de ces appareils sont entrés dans les mœurs.

On observe une volonté des utilisateurs de pouvoir bénéficier de toutes ces fonctionnalités, dans la sphère privée comme dans la sphère professionnelle, ce qui se traduit par une demande accrue auprès des directions de systèmes d'information de déployer les moyens nécessaires. Leur usage est toutefois problématique. En effet, les solutions de sécurisation actuelles sont peu efficaces pour assurer une protection correcte des données professionnelles. En outre, les vulnérabilités engendrées sur les systèmes d'information de l'entreprise étant fréquemment mal appréhendées, ce document a pour objectif de sensibiliser le lecteur aux principaux risques de sécurité des terminaux mobiles et d'indiquer des recommandations de sécurité génériques à appliquer pour les limiter.

Lorsque les systèmes d'information traitent d'informations sensibles, les terminaux permettant d'y accéder doivent impérativement être dédiés et avoir fait l'objet d'une évaluation de sécurité, idéalement être labellisés par l'ANSSI. Cette labellisation permet en effet d'attester de la robustesse de la solution par rapport aux principales menaces a contrario de celles qui consistent simplement en un développement applicatif (une « application de sécurité ») qui n'apporteront, au mieux, qu'une protection partielle des données sensibles. Lorsque les données sont classifiées, portent la mention Diffusion Restreinte ou Spécial France, une réglementation spécifique s'applique.

2 Les terminaux mobiles : quels risques de sécurité ?

Les terminaux mobiles stockent des données qui sont enregistrées volontairement (courriels, agenda, contacts, photos, documents, SMS, etc.) ou involontairement (cache de navigation, historique de déplacements datés et géo-localisés, etc.). Ces données peuvent être sensibles pour l'entité qui en a la propriété [1]. C'est le cas également des codes de sécurité, mots de passe et certificats qui pourraient être indirectement utilisés afin d'accéder à des biens essentiels du système d'information professionnel. En particulier, la tendance inopportune des utilisateurs à utiliser des mots de passe identiques pour accéder à plusieurs services différents laisse craindre que les mots de passes stockés dans un ordiphone correspondent potentiellement à ceux de services sensibles. Pèsent alors des risques de modification, de

1. Il est important de considérer l'ensemble des données exposées comme un tout : le regroupement de données individuellement anodines peut parfois permettre d'obtenir des informations sensibles. L'attaque d'un ordiphone permet la confrontation des courriels, des SMS, de l'historique de navigation, du journal des appels, de l'agenda, etc. Il est aisé, dans ces conditions, de déduire des informations stratégiques sur l'organisation ou encore d'obtenir des informations personnelles permettant de faire pression sur l'utilisateur du terminal.

destruction ou encore de divulgation de données professionnelles.

Le risque de fuite d'informations concerne tout terminal mobile mais, aujourd'hui, il est encore plus grand de par les nombreuses fonctionnalités présentes sur les ordiphones et les tablettes. Il convient de le prendre en compte sérieusement dans un contexte professionnel. Un attaquant pourra par exemple chercher à pénétrer le système d'information d'une organisation en utilisant comme point d'entrée un terminal mobile. Cela est dû principalement à la multitude de vulnérabilités que présentent les systèmes d'exploitation mobiles mais aussi aux erreurs de comportement d'utilisateurs non avertis.

3 Recommandations de sécurité

L'ANSSI estime qu'il est primordial d'appliquer l'ensemble des 21 recommandations qui suivent afin de sécuriser au mieux l'emploi d'ordiphones en environnement professionnel. Différents *scenarii* d'attaque justifiant ces recommandations sont présentés en annexe.

En tout état de cause, il est illusoire d'espérer atteindre un haut niveau de sécurité avec un ordiphone ou une tablette ordinaire, quel que soit le soin consacré à son paramétrage. Les recommandations de ce document ont simplement pour objectif de protéger au mieux possible les données contenues dans le terminal contre les attaques triviales. L'accès depuis ces terminaux à tout système d'information interne à l'entreprise doit par ailleurs être protégé par des moyens dédiés (Voir le guide publié par l'ANSSI pour la définition d'une architecture de passerelle d'interconnexion sécurisée [2]).

3.1 Généralités

Les différentes recommandations mentionnées dans ce document doivent être reprises dans un profil de configuration non modifiable par l'utilisateur et qu'il convient d'appliquer à l'aide de solutions de « gestion de terminaux mobiles » [3]. Ce dernier doit être tel qu'il n'est pas possible de modifier localement les paramètres de sécurité du mobile. Ces profils de sécurité sont idéalement télé-déployés depuis un point central de manière à permettre des modifications rapides à grande échelle. Ceci n'étant pas faisable sur tous les types de terminaux du marché, il convient de bien étudier les solutions de gestion de flotte en amont du choix des terminaux.

R1	Utiliser des solutions de gestion de terminaux mobiles permettant de déployer rapidement depuis un point central des profils de sécurité sur l'ensemble d'une flotte d'ordiphones.

D'autre part, en complément des mesures de sécurité techniques, les mesures organisationnelles (charte d'utilisation, politique de sécurité, procédures d'exploitation, etc.) restent primordiales comme lors de toute sécurisation d'un système d'information.

Enfin, la sécurité doit être prise en compte tout au long du cycle de vie du terminal :
- sécurité intrinsèque lors du choix d'un produit ;
- sécurisation du système avant délivrance des mobiles aux utilisateurs ;
- maintien en conditions de sécurité de l'ensemble du parc (application des correctifs de sécurité, mises à jour du système d'exploitation et des applications) ;
- suppression des données et remise à zéro des terminaux avant toute réaffectation ou mise au rebut.

2. http://www.ssi.gouv.fr/IMG/pdf/2011_12_08_-_Guide_3248_ANSSI_ACE_-_Definition_d_une_architecture_de_passerelle_d_interconnexion_securisee.pdf
3. Mobile Device Managment (MDM)

3.2 Contrôle d'accès

R2	Configurer une durée d'expiration du mot de passe de 3 mois maximum.

R3	Configurer le verrouillage automatique de terminal au bout de 5 minutes maximum.

R4	Si le terminal contient des informations sensibles, il est recommandé d'exiger un mot de passe fort en remplacement des méthodes de déverrouillage par défaut. Dans tout autre cas, l'utilisation d'un code PIN sera suffisant dès lors que la recommandation R5 est strictement respectée.

Note : Il convient d'analyser, en fonction de la technologie du terminal, la robustesse des mécanismes de verrouillage offerts. On notera que le déverrouillage par symbole (points à relier) ne dispose pas d'une richesse combinatoire suffisante pour être conforme au niveau minimal recommandé. Ce type de solution est donc à proscrire ainsi que toute solution biométrique lorsque l'efficacité n'est pas établie. La note précisant les recommandations de sécurité relatives aux mots de passe [4] publiée par l'ANSSI donne des éléments qui peuvent être utiles à la définition d'un mot de passe correct.

R5	Limiter le nombre de tentatives de déverrouillage, puis configurer un temps de blocage de plus en plus long ainsi qu'un effacement automatique après une dizaine de tentatives ayant échoué.

R6	Ne pas laisser le terminal sans surveillance. Un accès très temporaire à un terminal mobile peut suffire à sa compromission sans que l'utilisateur en ait conscience même lorsqu'il est verrouillé.

R7	Ne pas brancher le terminal à un poste de travail non maîtrisé ou à un quelconque périphérique qui ne soit pas de confiance, lesquels établiront une connexion directe non contrôlée.

3.3 Sécurité des applications

R8	Interdire l'utilisation du magasin d'applications par défaut, ainsi que l'installation d'applications non explicitement autorisées par l'entreprise. Cette recommandation vaut également pour les applications pré-installées.

R9	Les applications installées doivent avoir fait l'objet d'une analyse de sécurité préalable à toute autorisation de déploiement. Une telle analyse consiste à apprécier le niveau de sécurité de l'application sur la base d'informations publiques (pertinence des permissions, réputation, vulnérabilités publiées, évaluations de sécurité, etc.) et si possible à l'auditer (par analyse comportementale ou analyse de code, entre autres). Cette recommandation vaut encore une fois pour les applications pré-installées qui doivent être désinstallées si nécessaire.

4. http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

R10	Les applications déployées doivent avoir les permissions strictement suffisantes à leurs fonctions, que ce soit pour l'accès aux données ou à Internet, mais également pour le contrôle des divers capteurs. Les permissions octroyées doivent être vérifiées a minima lors de leur installation et à chaque mise jour pour s'assurer qu'elles n'ont pas évolué.

R11	L'accès au service de géolocalisation doit être interdit aux applications dont les fonctions liées à la position géographique ne sont pas utilisées. Si cette option n'est pas disponible sur le terminal considéré, il convient d'éteindre le service de géolocalisation lorsqu'il n'est pas utilisé.

Note : Ceci doit bien sûr être apprécié en fonction de l'usage professionnel qui est fait du terminal.

R12	Les applications déployées doivent appliquer des profils de sécurité appropriés (principalement en ce qui concerne le navigateur Web et le client de courriels), distribués dans le cadre des politiques de sécurité centralisées.

R13	Les applications déployées doivent être mises à jour régulièrement et rapidement dès lors que des correctifs de sécurité sont proposés.

3.4 Sécurité des données et des communications

R14	Les interfaces sans-fil (Bluetooth et WiFi) ou sans contact (NFC par exemple) doivent être désactivées lorsqu'elles ne sont pas utilisées.

R15	Désactiver systématiquement l'association automatique aux points d'accès WiFi configurés dans le terminal afin de garder le contrôle sur l'activation de la connexion sans-fil.

R16	Éviter tant que possible de se connecter à des réseaux sans fil inconnus et qui ne sont pas de confiance.

Note : La note publiée par l'ANSSI précisant les recommandations de sécurité relatives aux réseaux WiFi [5] donne d'autres éléments à prendre en compte pour un usage de terminaux WiFi professionnels.

R17	Le stockage amovible ainsi que le stockage interne du terminal doivent être chiffrés par l'utilisation d'une solution de chiffrement robuste.

Note : Lorsque cela est possible, l'utilisation de produits de chiffrement ayant fait l'objet d'une qualification par l'ANSSI, à défaut d'une certification (CSPN [6], etc.), sera préférée.

R18	Tout échange d'informations sensibles doit se faire par un canal chiffré de manière à assurer confidentialité et intégrité des données de point à point.

Note : L'utilisation de solutions VPN dédiées de préférence qualifiées par l'agence peut s'avérer nécessaire pour palier l'absence native de chiffrement ou un chiffrement peu robuste. Le chiffrement ne sera toutefois pas possible sur les services de base tels que la téléphonie ou les SMS à moins d'être équipé de solutions spécifiques.

5. http://www.ssi.gouv.fr/IMG/pdf/NP_WIFI_NoteTech.pdf
6. Certification de sécurité de premier niveau.

3.5 Sécurité du système d'exploitation et du terminal

R19	Le système d'exploitation doit être régulièrement et automatiquement mis à jour de manière à intégrer les derniers correctifs de sécurité publiés. Tout terminal qui ne peut plus prendre en charge les évolutions du système d'exploitation doit être remplacé.

Note : En fonction du modèle de terminal et du fournisseur d'accès utilisé, les mises à jour peuvent tarder à être disponibles. Il est alors important de se renseigner préalablement à tout choix de matériel et d'éviter de se disperser dans la gestion d'une flotte de terminaux trop hétérogène.

R20	Si les terminaux sont jugés suffisamment sensibles pour le nécessiter, il est conseillé de procéder régulièrement (a minima tous les ans) à la ré-initialisation complète du terminal, c'est à dire à un nouveau déploiement du système d'exploitation et un changement des clés de chiffrement, de manière à mettre fin à une éventuelle atteinte en sécurité du système à bas niveau.

Note : Ceci n'est toutefois pas la solution à l'ensemble des attaques dont certaines pourraient perdurer malgré une ré-initialisation complète.

4 Cohabitation des usages privés et professionnels

Du fait des recommandations précédentes, la cohabitation des usages privés et professionnels sur un même terminal doit être étudiée avec attention. Le respect des exigences du présent document n'est en tout état de cause pas compatible d'une politique *AVEC*[7] (*BYOD*[8]) au sein d'un organisme. Dans la plupart des cas, le terminal professionnel devra être dédié à cet usage (l'utilisateur pouvant généralement utiliser son propre terminal pour les usages personnels).

Si l'utilisation d'un seul ordiphone pour les deux contextes ne peut pas être évité, selon la sensibilité des données de l'entreprise traitées sur le mobile, il convient de mettre en œuvre des solutions dédiées pour cloisonner efficacement chaque environnement (personnel, professionnel) en étant vigilant sur les niveaux de sécurité variés des solutions du marché. Une qualification par l'ANSSI doit être un critère de choix d'une telle solution.

R21	Sauf à utiliser des solutions de cloisonnement dont il a été vérifié qu'elles répondent aux besoins de sécurité de l'entreprise, utiliser des ordiphones professionnels dédiés à cet usage.

7. Apportez Votre Équipement personnel de Communication.
8. Bring Your Own Device.

Annexe
Divers *scenarii* d'attaque aboutissant à une fuite d'informations

A Par vol ou perte de terminal

Les vols de terminaux mobiles sont fréquents. Dès lors, l'attaquant peut accéder rapidement aux données sensibles qu'ils contiennent en passant outre les mesures de sécurité basiques. Seule une solution de chiffrement robuste des données permet de réduire fortement le risque de fuite d'informations et toute barrière complémentaire participe à la défense en profondeur du terminal.

B Par le biais d'applications malveillantes

Souvent, les applications ont des droits non justifiés. En même temps, les systèmes de permissions manquant souvent de finesse, il est donc difficile d'octroyer des droits de manière précise. Ainsi, une application qui a la permission d'accéder à la fois à Internet et aux données de la carte de stockage amovible pourra par exemple les exfiltrer complètement vers un serveur détenu par des individus malveillants. Une grande partie des applications aujourd'hui disponibles dans les magasins d'applications effectuent des opérations qui ne relèvent pas de leur fonction première, le tout à l'insu des utilisateurs. Ces applications sont la plupart du temps gratuites et proposent des services volontairement très séduisants.

Sachant qu'il est difficile de savoir concrètement ce que fait une application, chacune est potentiellement un cheval de Troie et, sans analyse poussée, doit être considérée comme tel. Il est donc primordial de contrôler rigoureusement les applications installées sur les terminaux. Une attaque fréquemment observée consiste pour un attaquant à obtenir une application populaire sur un marché d'application, à y ajouter une charge malveillante puis à distribuer le produit résultant sur un autre marché. Une application réputée et initialement fiable peut ainsi s'avérer être un logiciel piégé. Il est donc extrêment important de s'assurer que l'application obtenue provient bien de son éditeur légitime, au besoin en se renseignant auprès de celui-ci.

C Par exploitation de failles du système d'exploitation ou d'applications

Les systèmes d'exploitation des terminaux mobiles présentent des vulnérabilités. Ces dernières permettent parfois d'accéder aux couches basses du système et peuvent être utilisées par exemple pour y ajouter des portes dérobées ou des codes d'interception. Ces vulnérabilités sont souvent exploitables par le biais d'applications ou directement à travers les interfaces du terminal (port USB, carte WiFi ou Bluetooth, etc.). Difficilement détectable, la compromission résultante permet à une personne malveillante d'avoir un contrôle total du terminal pour intercepter discrètement toutes les données présentes voire pour activer les caméra et microphone de l'équipement.

Il est à noter à ce propos que les terminaux « jailbreakés » ou « rootés » par l'utilisateur exposent d'autant plus leur système à des compromissions bas niveau et font souvent obstacle à l'application des correctifs de sécurité, raison pour laquelle ils sont fortement proscrits. En effet, le « jailbreak » des terminaux s'appuie généralement sur l'exploitation d'une faille qui vise à exécuter du code très privilégié et souvent non maîtrisé voire à désactiver des protections imposées par le fabricant du terminal (par exemple, la vérification d'intégrité des mises à jour logicielles). De la même façon, les systèmes alternatifs disponibles pour certains équipements sont à déconseiller en raison de leur qualité très variable

et difficile à évaluer mais aussi de par le manque de visibilité sur leur maintien en conditions de sécurité.

D'autre part, les applications légitimes et de confiance peuvent également faire l'objet de vulnérabilités. Tout comme sur les systèmes d'exploitation de postes de travail, les applications de lecture de fichiers PDF ou de navigation Web sont par exemple souvent touchées. On retrouve alors sur les terminaux mobiles les mêmes problématiques de sécurité que sur les postes de travail. Il est par conséquent nécessaire d'appliquer des profils de configurations sécurisés adaptés et non modifiables par l'utilisateur. En outre, beaucoup d'applications pour terminaux mobiles sont d'une qualité assez faible. Il n'est pas rare que les applications présentent des vulnérabilités importantes, devenant de fait des portes dérobées involontaires. C'est pour cette raison qu'il est primordial de limiter le nombre d'applications validées.

D Par exploitation des fonctions intégrées au matériel

Différents composants d'un terminal mobile intègrent en effet des fonctions bas niveau (debug, etc.) qu'un attaquant peut utiliser à son profit afin de prendre le contrôle du terminal. Ce risque, bien que faible, est tout de même à garder à l'esprit dans des contextes d'utilisation sensibles.