ZEBRA

Solutions grand public / solutions professionnelles

Présentation

Ce dossier présente un résumé (données disponibles sur demande) des problèmes que rencontrent les clients qui tentent d'utiliser des appareils grand public dans le cadre d'applications professionnelles. Bien qu'aucun fournisseur de produits grand public en particulier ne soit visé, nombre des déclarations dans ce dossier concernent Apple, car sa plateforme et son modèle d'exploitation sont uniques. Ce document ne saurait être considéré comme une condamnation des appareils grand public. Il a pour objectif de sensibiliser le lecteur aux compromis que font les fabricants de produits professionnels et grand public.

Les acheteurs qui envisagent d'utiliser des appareils grand public dans un cadre professionnel sont invités à se poser les questions suivantes :

- Mon équipement sera-t-il sûr et capable de maintenir la confidentialité de mes données ?
- Survivra-t-il à l'usure d'une utilisation professionnelle typique ?
- L'équipement (fournisseur, appareil, accessoires) durera-t-il aussi longtemps que je l'exige ?
- En le choisissant, suis-je en mesure de permettre au service informatique de gérer et d'administrer le portefeuille des équipements de l'entreprise ?
- Le fournisseur m'assurera-t-il le support technique dont j'ai besoin si les choses ne se passent pas comme prévu ?
- Puis-je avoir la certitude que la solution sera suffisamment fiable pour ne pas affecter la productivité des employés ou l'expérience client ?
- Ai-je vraiment examiné toutes les questions entourant une solution constituée de plusieurs éléments ?
- La solution satisfait-elle vraiment aux exigences fonctionnelles actuelles et futures (performance sans fil, lecture de codes à barres, audio, température, etc.) ?
- Ai-je envisagé les questions secondaires telles que le vol d'équipement ?
- Mon fournisseur me permettra-t-il de planifier correctement pour l'avenir (visibilité de ma feuille de route, par ex.) ?
- Mes développeurs et mes ISV tiers ont-ils un accès adéquat à la programmation (API) ?
- Mon plan me permet-il de consolider ou d'unifier mon environnement en termes de système d'exploitation ?

Solutions grand public / solutions professionnelles

MISES À JOUR DU SYSTÈME D'EXPLOITATION : CONTRÔLE PAR L'UTILISATEUR OU PAR LE SERVICE INFORMATIQUE ?

Le consommateur recherche le côté pratique de l'utilisation et le contrôle de son appareil. L'entreprise, quant à elle, privilégie la productivité maximale et le contrôle par son service informatique. Dans le modèle grand public, les mises à jour sont « poussées » vers l'appareil. Les utilisateurs peuvent les accepter ou les ignorer.

Il arrive aussi que les clients tentent de bloquer les mises à jour des appareils de leurs collaborateurs à l'aide de filtres URL proxy. Mais si des adresses de téléchargement sont fournies, les collaborateurs arrivent à mettre leur appareil à jour. Ces mises à jour peuvent entraîner des incompatibilités avec les applications, voire un environnement global fragmenté. Malheureusement, une fois les mises à jour installées, il peut être impossible de revenir en arrière.

Pour l'entreprise, le paradigme est tout autre. C'est Zebra qui fournit les mises à jour aux clients. Elles sont chargées dans un outil de gestion des périphériques entièrement contrôlé par le service informatique. C'est ce service qui détermine le calendrier des mises à jour (souvent aux heures creuses, pour ne pas surcharger le réseau aux heures de pointe) et les appareils concernés (pour un déploiement progressif, afin de réduire le risque de défaillances catastrophiques). Et comme ce service peut effectuer les mises à jour sans intervention de l'utilisateur, elles se font indépendamment de sa volonté et de manière transparente. Et bien sûr, le service informatique peut déployer une nouvelle version ou revenir à une version antérieure en cas de problèmes.

PERFORMANCE WI-FI

Essentielle ou de base ?

En matière de performance Wi-Fi, les offres grand public et professionnelles diffèrent grandement. Les appareils grand public fonctionnent généralement dans les environnements avec peu de points d'accès, et l'itinérance efficace d'un point à l'autre n'est donc pas déterminante. Mais une mauvaise itinérance peut entraîner des écarts de latence importants, d'où un impact massif sur les temps de réponse de la voix et des applications et, par extension, sur la productivité.

Les fournisseurs d'appareils grand public privilégient souvent le coût et la taille au détriment de la connectivité Wi-Fi. Les appareils Zebra, par exemple, sont généralement fournis avec des antennes diversifiées commutées. L'intégration de deux antennes au lieu d'une a un impact sur la taille et le coût, mais assure une connectivité Wi-Fi robuste par activation transparente de l'antenne optimale. Cela permet d'éliminer les effets dits « fantômes » qui dégradent la connectivité affectée par le placement de la main ou de la tête par rapport à l'appareil (problème des appareils Apple sur le réseau mobile). En outre, les antennes diversifiées atténuent l'impact de la réflexion des radiofréquences (trajets multiples) omniprésente à l'intérieur des entreprises et entraînant de grandes fluctuations de connectivité.

Par ailleurs, la congestion grandissante des réseaux Wi-Fi et la hausse des interférences dans la bande 2,4 GHz justifient le besoin croissant d'une bande 5 GHz robuste. Apple n'a introduit la prise en charge de la bande 5 GHz que dans sa 5e génération d'appareils. À la différence du grand public, de nombreuses entreprises utilisent déjà la bande 5 GHz pour augmenter leur capacité et éviter les interférences dans la bande 2,4 GHz. Cela dit, la performance dans la bande 5 GHz peut varier. Comme le révèle une étude Gartner portant sur l'évaluation des iPad Apple, « à 5 GHz, l'entreprise informatique aura besoin de trois fois plus de points d'accès » (du fait d'une mauvaise performance). Ce rapport peut être acheté auprès de Gartner.

TAILLE DE L'ÉCRAN

Améliorer la productivité

En entreprise, les clients exigent une plus grande taille d'écran (dans un format qui toutefois tient dans la poche). Un client a signalé qu'il avait réussi à « aplatir » son interface utilisateur de 6 à 2 niveaux, grâce à la plus grande taille d'écran. Résultat ? Une plus grande productivité des employés. Les écrans plus grands permettent également d'utiliser l'appareil aux formats portrait et paysage.

Lorsqu'Apple est passé de la 4e à la 5e génération, l'écran et le rapport largeur/longueur ont changé. Les nouveaux modèles possèdent des écrans de 4 po pour un rapport de forme de 16:9. En revanche, le MC40 possède un écran de 4,3 po. À première vue, la différence (de 4 à 4,3 po) semble négligeable, mais il faut se souvenir que la zone d'écran est une fonction exponentielle de la diagonale. Par conséquent, le MC40 présente une surface d'écran supérieure de 19,3 % à celle des appareils Apple de 5e génération. En outre, sur la base du retour d'expérience d'entreprises clientes, Zebra a lancé en 2014 un produit de 4,7 po dont la surface d'écran est supérieure de 38,1 % à celle des appareils Apple de 5e génération.

VOLUME DES APPAREILS

Support + appareil, ou équipement intégré ?

Les appareils grand public sans périphériques ajoutés sont généralement plus petits et plus légers que les équipements professionnels totalement intégrés. Mais combinez-les à un support de type « sled » (en pistolet) pour leur ajouter une fonctionnalité de paiement, une plus grande capacité de batterie et/ou une fonction de lecture de codes à barres, et ces solutions en deux parties deviennent souvent plus encombrantes que les modèles professionnels intégrés.

Prenons, par exemple, l'iPod Touch Gen4, un appareil très compact (47 mm3 environ). Lorsqu'il est équipé d'un support Infinite Peripheral pour bénéficier de la lecture de codes à barres et d'une autonomie comparable à celle du MC40, le volume de la solution en deux parties atteint 199 mm3. Ce volume est supérieur à celui du MC40, 173 mm3 seulement. En outre, la taille d'écran de la solution iPod (Gen 4) est de 3 661 mm2, tandis que celle du MC40 est de 5 264 mm2 (soit 43 % de plus).

En bref, à fonctionnalités comparables, le MC40 présente un volume inférieur de 13,1 %, pour une surface d'écran supérieure de 43 %.

SOLUTION DE TYPE SLED

Résistance aux chutes

Les équipements professionnels sont souvent catégorisés en tant qu'appareils « durables » ou « tout-terrain ». Ils sont censés rester opérationnels après 26 chutes (6 chutes sur le côté, 8 sur l'angle, 12 sur le bord) d'une hauteur de 1,20 m sur du contreplaqué. Zebra a testé une solution de type sled bien connue (pour la lecture de codes à barres et une plus grande autonomie) selon la méthode des 26 chutes. Le test a entraîné 6 défaillances matérielles de la solution combinée support + iPod : 1) une partie du verrou de gauche est tombée ; 2) les deux boutons de volume du support ont cessé de fonctionner ; 3) les haut-parleurs ont totalement cessé de fonctionner de même que la fonction scanner ; 4) l'appareil n'a plus pu se recharger correctement ; 5) une partie du conduit de lumière à LED, au bas de l'appareil, est tombée ; 6) un cliquetis s'est fait entendre vers le haut de l'appareil. La solution a également présenté 3 pannes logicielles (défaillances corrigées par réinitialisation de l'appareil).

SOLUTION DE TYPE SLED

Nombre de cycles de mise en marche et contact

En général, le nombre de cycles de mise en marche et contact des solutions combinant un appareil grand public à un support de type sled n'est pas spécifié et il est difficile à déterminer. Ces solutions présentent toutefois un fort taux de pannes dans les cas d'usage professionnel. Par exemple, le bouton d'allumage du MC40 a un taux de fiabilité de 500 000 cycles, le bouton de lecture/caméra, de 1 000 000 cycles, et l'insertion de la batterie, de 2 000 cycles (6 000 pour le terminal).

SOLUTION DE TYPE SLED

Architecture de la batterie

Parmi les retours d'informations, Zebra a noté que certains supports de type sled isolent la batterie principale de la batterie du support (les deux batteries ne partagent pas leur capacité). Par conséquent, la batterie de l'iPod et la batterie du support doivent être chargées pour former une unité opérationnelle. De nombreux supports sont commercialisés, et les clients ont intérêt à s'assurer du type de fonctionnement de la batterie de la solution envisagée. Il faut reconnaître que le fonctionnement indépendant de la batterie peut créer des problèmes de cycles de vie au fil du temps.

ACOUSTIQUE

Niveaux de pression acoustique

La tendance des appareils grand public est à la minceur, même au détriment de fonctions professionnelles importantes. De plus en plus de clients professionnels recherchent un équipement qui combine la voix et les données. Les utilisateurs des équipements en intérieur combinent appareils PTT (push-to-talk) conventionnels et appareils de collecte de données. Dans tous les cas, les entreprises recherchent un appareil capable de transmettre la voix de manière audible dans un environnement relativement bruyant.

Pour obtenir le facteur de forme désiré, les fabricants d'appareils grand public sacrifient souvent le niveau de pression acoustique et la réponse en fréquence. Zebra a constaté que de nombreux appareils grand public populaires présentent un niveau de pression acoustique inférieur de 9 à 20 dB à celui de ses équipements professionnels. Bien que subjective et non linéaire par rapport au niveau de sortie absolu, cette différence de 9 dB correspond généralement à une perception de 2 fois le volume.

GRANULARITÉ FONCTIONNELLE DU SUPPORT

Intégration de la lecture de codes à barres

Dans de nombreux cas, les clients professionnels veulent une fonction de lecture intensive et constante sur tous les appareils, et une fonction de point de vente mobile sur certains appareils et/ou à certaines périodes de l'année. Lorsqu'ils comparent les différentes options avec support, ils sont forcés d'envisager deux configurations différentes : une pour la lecture seule, et une pour la lecture et le paiement. S'ils ne veulent retenir que l'une des options, celle-ci doit être la solution plus grande et plus coûteuse équipée de la lecture et du paiement. La plupart des clients préfèrent disposer de la lecture intégrée à l'appareil et reléguer le paiement à la solution avec support.

SLOT D'EXTENSION

Les clients professionnels demandent souvent le stockage amovible pour les données de portage, la sauvegarde des données et/ou les extensions de mémoire. Les appareils Apple n'offrent pas de supports amovibles (comme les cartes SD ou les disques flash).

COMMUNICATION EN CHAMP PROCHE (NFC)

Apple a spécifiquement réitéré sa décision de ne pas prendre en charge la communication en champ proche (NFC). Or, de nombreux clients professionnels veulent la NFC pour lire les balises de localisation, apparier les périphériques, lire les étiquettes sur les actifs de l'entreprise ou contrôler les accès.

FLEXIBILITÉ DU LANCEUR

Les utilisateurs de systèmes Apple ne peuvent pas remplacer ni modifier le lanceur d'applications.

TAUX DE PERTES

Perte et vol des appareils

La demande du marché des pièces de rechange en appareils grand public est extrêmement forte et peut motiver le vol. Dans le cas des appareils grand public sans batterie interchangeable, les clients se procurent souvent 2 jeux d'appareils : tandis qu'un appareil est utilisé, l'autre est dans son support de chargement. Les clients ont signalé que les appareils dans leur support de chargement disparaissent fréquemment.

TEMPÉRATURE

Fonctionnement et stockage

Les appareils grand public fonctionnent généralement sur une plage de températures très limitée. Les appareils Apple, par exemple, gèrent une température de fonctionnement de 0 à 35 ° Celsius. Lorsque l'appareil surchauffe, il cesse de fonctionner correctement et un point d'exclamation s'affiche, accompagné d'un message indiquant qu'il faut laisser l'appareil refroidir. Plusieurs clients ont signalé ce problème dans des environnements loin d'être extrêmes. En revanche, les équipements professionnels tels que le Zebra MC65 fonctionnent à des températures de -10 à 50° Celsius, soit une plage de températures supérieure de 25 degrés à celle des appareils Apple. Un client a même indiqué devoir placer les appareils dans un réfrigérateur sur site pour qu'ils puissent recommencer à fonctionner. Un autre client a signalé une surchauffe au Texas en novembre, lors d'un essai de livraison directe en magasin.

Il est important de noter que cette spécification concerne la température ambiante. Donc lorsque l'appareil est sur son support de type sled, la chaleur du support et le manque d'évacuation externe peuvent forcer une utilisation à une température inférieure à celle annoncée.

La température de stockage a été également signalée comme problématique pour les appareils Apple. Selon un client, l'exposition à une température de stockage légèrement supérieure au seuil maximal a entraîné une dégradation permanente de la durée de vie de la batterie. Les températures de stockage pour un appareil Apple sont de -20 à 45° Celsius, à comparer aux températures de stockage du Zebra MC65, qui sont de -40° à 70°.

CYCLES DE VIE DES ÉQUIPEMENTS PROFESSIONNELS

Les appareils grand public doivent suivre la dernière mode et les tendances du jour. La durée de vie typique (avant que l'article ne devienne impropre à la vente) pour un smartphone est de 6 à 9 mois. De nouveaux appareils Apple sont généralement commercialisés tous les 12 mois. La disponibilité des appareils grand public après leur introduction initiale sur le marché n'est pas précisée. Les clients professionnels peuvent être forcés à remplacer intégralement leur parc, initiative très coûteuse, ou à réaliser un roulement progressif, d'où un déploiement très fragmenté et complexe d'un point de vue logistique.

Dans la sphère grand public, la compatibilité des accessoires existants est prise en compte, mais rarement obligatoire. Chez Apple, l'introduction du connecteur Lightning (qui remplace le connecteur à 30 broches) et les changements de facteur de forme de l'iPhone 5 ont forcé les clients professionnels de remplacer intégralement leurs supports, baies de chargement et autres accessoires, pour opérer la migration vers le nouvel appareil.

Les appareils professionnels tels que les équipements Zebra présentent généralement un cycle de vie de 3+3 (6 ans) ou 5+5 (10 ans). Le premier chiffre indique la disponibilité de l'équipement et le second, la disponibilité du support technique. Par conséquent, les clients 3+3 peuvent acheter l'équipement pendant 3 ans et le faire réparer pendant 3 ans de plus, soit un cycle de vie total de 6 ans.

SÉCURITÉ ET CONFIDENTIALITÉ DES DONNÉES PROFESSIONNELLES

Apple et Google (via Google Mobile Services-GMS) s'appuient sur les appareils pour promouvoir et vendre des services. Ces derniers sont généralement assortis d'un accès aux données de l'appareil, sanctionné par une licence de l'utilisateur, ce qui peut contrevenir aux politiques de confidentialité de l'entreprise. IBM, par exemple, a publiquement annoncé son interdiction de Siri[1]. En effet, comme l'indique la licence d'utilisation de Siri, lorsque vous utilisez ce service, vous consentez à autoriser Apple, ses filiales et ses agents à transmettre, collecter, gérer, traiter et utiliser vos informations, y compris votre voix et vos données d'utilisateur. Et comme ces appareils requièrent la connectivité au Cloud, certaines entreprises ont été forcées de percer leur pare-feu. Des clients de Zebra, notamment 10 enseignes majeures, ont déclaré qu'ils n'autorisent pas les appareils GMS sur leur réseau d'entreprise, à cause de soucis de confidentialité de ce type.

FEUILLE DE ROUTE DES APPAREILS GRAND PUBLIC

Une atmosphère de secret

Une feuille de route confidentielle et le secret du calendrier de lancement sont essentiels à l'offre grand public, mais en conflit direct avec la planification d'entreprise et la continuité du service. Apple est fier de son calendrier secret :

- « L'absence d'information est garante d'un fort intérêt de la part du public, puisque les consommateurs ne peuvent que spéculer » – Regis McKenna, consultant marketing de l'équipe Apple d'origine
- « Sans feuille de route claire, de nombreux acheteurs hésitent à acquérir les produits Apple » – Jeff Gamet, MAC Observer

PROGRAMMES MALVEILLANTS SUR L'APP STORE

Verrouillage des périphériques (gestion des applications mobiles)

Comme l'indiquent les directives de sécurité NIST Mobile, les meilleures pratiques consistent à interdire l'accès public à l'App Store. Bien sûr, pour les appareils grand public tels que ceux d'Apple, l'App Store représente une proposition de valeur alléchante et ne peut pas être désactivé.

Bien que le Google Play Store d'Android ait connu une forte proportion de contenu malveillant, les applications de l'Apple App Store peuvent également enfreindre les règles de sécurité des données d'entreprise. Si Apple filtre les applications, celles-ci sont autorisées à extraire et à télécharger des données sensibles de l'appareil.

Parmi les ressources clé immédiatement accessibles (et donc vulnérables) par le biais d'applications IOS valides :

- Communications sans fil avec d'autres appareils
- Carnet d'adresses, adresses e-mail, notes sur les contacts, etc.
- Calendrier
- Identificateur de l'appareil (ID unique attribué à chaque appareil par Apple)
- Numéro de téléphone (peut être désactivé par modification de la configuration)
- Fichiers de musique et vidéo et galerie de photos
- Historique des recherches sur Safari
- Historique des saisies automatiques
- Pages YouTube vues récemment
- Journaux de connexions Wi-Fi
- Microphone et caméra vidéo

[1] http://www.zdnet.com/blog/btl/ibm-bans-siriprivacy-risk-or-corporateparanoia-at-its-best/77843

ÉLIMINATION DES SERVICES INDÉSIRABLES

Face aux vulnérabilités provenant des magasins d'applications publics, plusieurs clients ont tenté de retirer l'Apple App Store de leurs appareils IOS et ont indiqué qu'il « revient toujours ».

GESTION DES APPLICATIONS MOBILES — LISTE BLANCHE IMPOSSIBLE

Les appareils entraînant la responsabilité de l'entreprise, ou « CLD » (Corporate Liable Devices) sont fréquemment verrouillés pour limiter la possibilité de charger et d'exécuter certaines applications. Les clients ont exprimé leur frustration de ne pouvoir établir de « listes blanches » d'applications (listes d'applications autorisées) sur les appareils tels que ceux qui exécutent un système Apple/iOS (la liste blanche est une fonctionnalité standard des appareils Android/Mx).

ATTENTION PARTICULIÈRE

Choisir un partenaire, et non un appareil

Au troisième trimestre 2013, Apple a vendu 33,8 millions d'iPhone et Samsung, 88,4 millions de smartphones. Le nombre d'appareils vendus sur l'année par les deux marques se montait à 135,2 millions et 353,6 millions, respectivement. Samsung vend près d'un million d'unités par jour. Un déploiement de 10 000 unités dans une grande entreprise ne représente par conséquent que 10 % de la vente quotidienne du fabricant. En revanche, les constructeurs d'équipements professionnels ne vendent pas plus d'un million et demi d'unités par an. Une opportunité de 10 000 unités représente donc une part significative du chiffre d'affaires et garantit un degré d'attention important.

Comme l'a indiqué un client de Zebra, « lorsque nous choisissons une offre grand public, nous sélectionnons un appareil, pas un partenaire. » Cela reflète bien les sentiments exprimés récemment dans un article du Wall Street Journal[3].

FRAIS DE LOGISTIQUE

Mises à jour des certificats de distribution

Pour distribuer les applications Apple, vous devez vous inscrire au programme des développeurs Apple Enterprise (le certificat d'entreprise dure 3 ans) et obtenir un certificat de distribution. Les applications sont ensuite déployées, mais après expiration du certificat de distribution (1 an), vous devez reconstruire vos applications sur la base d'un certificat renouvelé et les redéployer. Plusieurs clients professionnels ont signalé que les applications installées ne fonctionnent tout simplement pas (ou elles fonctionnent pendant quelques jours, après quoi le certificat n'est plus valable pour le serveur OCSP d'Apple).

REDÉMARRAGE À DISTANCE

Malgré toutes les précautions prises, les appareils requièrent parfois un redémarrage. Le redémarrage par programme requiert l'accès à une API, ce qui n'est pas souvent autorisé sur les appareils grand public (par ex. iOS d'Apple). En revanche, sous Zebra Android/Mx, les API sont accessibles aux applications sécurisées/authentifiées, pour redémarrage de l'équipement par programme (généralement à distance, par outil de gestion des périphériques).

GESTION DE LA BATTERIE

Optimisation du temps de fonctionnement

En cas d'utilisation professionnelle, l'autonomie des équipements (à court terme, mais aussi à long terme) revêt souvent une importance considérable. Or de nombreux appareils grand public ne permettent pas le remplacement de la batterie (Apple, par exemple). Les clients professionnels en sont alors réduits à acquérir 2 appareils, au lieu d'un seul appareil et d'une batterie de rechange. Il arrive aussi que la batterie soit remplaçable, mais que le mécanisme de fermeture ne soit pas conçu pour une utilisation répétée, et celui-ci se casse au bout d'un certain temps.

« Selon une enquête rapide réalisée par le concepteur Dustin Curtis auprès de 15 développeurs d'applications iOS populaires, 13 d'entre eux détiennent une base de données de plusieurs millions de contacts. L'une de ces bases de données contient le numéro de portable de Mark Zuckerberg et de Bill Gates, et le numéro de domicile de Larry Ellison. »[2]

[2] http://www.pcworld.com/article/250007/path_isnt_only_app_to_upload_store_address_book_data.html
[3] http://blogs.wsj.com/cio/2013/06/12/apple-stilllags-in-enterprise-support/

ACCÈS À L'ÉQUIPEMENT

Contrôle à distance

La plateforme iOS d'Apple est, par conception, relativement fermée. Bien que cette caractéristique la protège, dans une certaine mesure, des contenus malveillants, elle limite également limite la capacité des développeurs professionnels de lui ajouter des fonctions avancées. Parmi les fonctions fréquemment demandées par les entreprises figure la capacité de contrôler un appareil à distance, notamment à des fins de formation et de diagnostic. Pour installer cette fonction, une application approuvée doit pouvoir accéder à la mémoire tampon de l'écran, ce qui est interdit sur les plateformes Apple. En revanche, les solutions Zebra Android/Mx permettent aux applications approuvées (authentifiées par les signatures appropriées) d'accéder aux ressources telles que la mémoire d'image.

En bref, le processus de signature Android confère aux applications approuvées, signées ou authentifiées le niveau d'accès nécessaire pour activer les fonctions professionnelles désirées.

ULTRA-HAUTE RÉSOLUTION

Compromis pour l'entreprise

Les appareils grand public tendent tous vers l'ultra-haute résolution. Apple, par exemple, est passé des 1024 x 768 de l'iPad 2 aux 2048 x 1536 de l'iPad New. Des rapports indiquent que cette transition a requis le double de LED pour le rétroéclairage, d'où une hausse de 68 % pour la batterie de l'iPad New. Comme le démontre une étude[4], l'efficacité énergétique de l'écran a baissé de manière significative (à savoir deux fois et demie la puissance pour la même luminosité). En outre, les applications tentant de profiter de l'ultra-haute résolution se sont fortement alourdies (Bjango, par exemple, est passée de 18,3 Mo à 35 Mo). Ces charges plus importantes peuvent avoir des incidences sur les coûts, lorsque le client utilise les services d'un opérateur appliquant un modèle tarifaire progressif en fonction de la quantité de données.

Bien que la haute résolution soit importante pour les clients professionnels, les extrêmes des appareils grand public qui sacrifient l'autonomie de la batterie et/ou le poids de l'équipement ne sont pas nécessairement des atouts.

GESTION DES FICHIERS

Les responsables informatiques des grandes entreprises souhaitent souvent pouvoir afficher et gérer les fichiers et les dossiers à l'intérieur des appareils. Malheureusement, le système de fichiers iOS d'Apple n'est pas ouvert. Bien qu'il existe des applications tierces, leur efficacité est limitée par l'architecture d'iOS.

ENCRYPTAGE

Compromis en faveur de l'optimisation de la taille des fichiers

L'efficacité de l'encryptage peut varier en fonction du but recherché. Apple et Samsung appliquent un encryptage matériel. Les tests réalisés par Zebra indiquent que l'encryptage matériel d'Apple est efficace sur les très gros fichiers (environ 128 Mo, comme pour les fichiers multimédias). Cependant, pour les petits fichiers (1 Ko), les tests montrent que l'encryptage Zebra est trois fois plus rapide. Il est considéré comme acquis que l'encryptage matériel requiert une initialisation et une configuration qui sont amorties dans le cas de gros fichiers, mais qui ont un impact sur les petits fichiers. Bien que l'encryptage matériel puisse être très efficace pour les gros fichiers multimédias (gestion des droits numériques sur les films), il n'est pas forcément optimal pour les fichiers plus petits, souvent utilisés dans le cadre d'applications professionnelles.

STOCKAGE CENTRALISÉ

Sous iOS, les applications sont des entités autonomes qui gèrent leur propre stockage et qui, seules, peuvent y accéder. Cela complique le partage de grandes structures de données (des applications étant généralement nécessaires pour faire une autre copie). Lorsque les applications partagent des données, le profil (l'encryptage) de la structure originale des données peut ne pas être maintenu dans la structure copiée, enfreignant ainsi les politiques de sécurité.

Les clients professionnels demandent souvent le stockage amovible pour les données de portage, la sauvegarde des données et/ou les extensions de mémoire. Les appareils Apple n'offrent/ne gèrent pas les supports amovibles (comme les cartes SD ou les disques flash).

[4] http://www.slashgear.com/ipad-retina-displaysquashes-rivals-but-its-notperfect-20219167/

CORRUPTION DE LA MÉMOIRE FLASH À CELLULE MULTINIVEAU APRÈS USAGE PROLONGÉ

La mémoire flash est généralement configurée en tant que mémoire à cellule multiniveau ou à cellule binaire. Les configurations à cellule multiniveau fournissent généralement deux fois la capacité des mémoires à cellule binaire comparables, mais peuvent entraîner des corruptions de données sur la durée. Après utilisation répétée, les niveaux de tension de grille flottante représentant des bits d'information dans la cellule multiniveau fluctuent, et des bits sont lus par erreur.

Du fait des cycles de vie relativement courts et d'un usage relativement peu intensif (comparé à un environnement d'entreprise), les appareils grand public et certains équipements professionnels ont recours à la mémoire Flash à cellule multiniveau. Les clients devraient valider leur modèle d'utilisation/cycle de vie pour déterminer la configuration flash optimale.

VERROUILLAGE DES PROFILS DE CONFIGURATION IMPOSSIBLE AVEC UN OUTIL DE GESTION DES PÉRIPHÉRIQUES

Les appareils Apple peuvent être configurés à l'aide de « profils de configuration ». Les profils de configuration sont des fichiers XML spécifiés par Apple. Lorsqu'un administrateur configure un appareil à l'aide d'un profil de configuration, ce profil peut être ouvert (librement modifiable), modifiable uniquement sur mot de passe, ou verrouillé (toute modification efface intégralement l'appareil).

Lorsque des profils générés par un outil de gestion des périphériques sont utilisés, il n'existe aucun moyen équivalent de verrouiller les profils de configuration. Les profils de l'appareil provenant d'un outil de gestion des périphériques peuvent donc être modifiés, voire supprimés, par l'utilisateur final.

UN SEUL SYSTÈME D'EXPLOITATION DE L'ENTREPÔT AU MAGASIN ? PEU PROBABLE AVEC UN APPAREIL GRAND PUBLIC

Une grande enseigne (parmi tant d'autres) a affirmé sa volonté de déployer « un seul système d'exploitation, de l'entrepôt au magasin ». Les entrepôts requièrent généralement des équipements propres aux applications, peu susceptibles d'être fournis par Apple. En revanche, Zebra (et, selon nous, le secteur dans son ensemble) offre des solutions Android pour l'entrepôt, l'arrière-boutique, l'espace de vente, et même le personnel sur le terrain.

CHOIX ET SÉLECTION

Intérêt de la concurrence

En ce qui concerne Apple, la marque offre un portefeuille exclusif de trois produits de base : l'iPod, l'iPhone et l'iPad. Il n'existe aucun appareil propre à une application donnée. La spécialisation ne peut se faire qu'à l'aide d'un support de type sled. En revanche, en mars 2013, il existait plus de 550 appareils Android proposés par 48 fabricants. Parmi ces derniers, on comptait des fabricants d'appareils grand public, et des fabricants d'appareils professionnels (par ex. Zebra, Honeywell ou Bluebird). Un paysage aussi varié permet aux entreprises de faire jouer la concurrence et de bénéficier de sources multiples (d'où une réduction du risque).

ACCÈS LIMITÉ AUX API

Autoriser l'accès professionnel

Dans le cas d'iOS et de WP8, les API sont verrouillées pour minimiser les attaques par les applications malveillantes. Bien qu'elle présente un intérêt potentiel pour les consommateurs qui téléchargent des applications inconnues de sources également inconnues, cette approche verrouillée limite énormément les fonctions intégrées aux applications approuvées d'entreprise (de nombreux clients professionnels souhaitent exercer le contrôle ou l'accès à distance).

VULNÉRABILITÉ DU TROUSSEAU

Les chercheurs de Fraunhofer ont identifié une importante vulnérabilité dans IOS. De nombreux mots de passe (accès au VPN, à Exchange Active Sync, au Wi-Fi, à la boîte vocale) sous iOS sont stockés dans le « trousseau » iOS. Ce trousseau est crypté par des données qui sont stockées sur l'appareil lui-même. Un pirate peut donc extraire ces données de l'appareil et décrypter le trousseau, accédant ainsi facilement aux mots de passe. Remarque : nous attendons une mise à jour de cette analyse pour la version la plus récente d'iOS 7.[5]

MENACES À LA SÉCURITÉ DE SIRI

Siri est une application de reconnaissance vocale en langage naturel, lancée sur l'iPhone 4S. Son intérêt réside en grande partie dans sa capacité à gérer les questions posées rapidement dans la langue courante de l'utilisateur final.
En configuration standard,

[5] *Fraunhofer researchers circumvent encryption devices iPhone*, Latest IT News, 9 février 2011

Siri est activée par simple pression sur un bouton indépendant du verrouillage de l'appareil. Par conséquent, si l'appareil est perdu ou volé, n'importe qui peut accéder instantanément aux e-mails, contacts et SMS de son propriétaire. Bien que Siri puisse être replacée derrière le mur de protection, une telle migration diminuerait grandement sa valeur.

CAMÉRAS GRAND PUBLIC POUR LA CAPTURE DE CODES À BARRES

Zebra distingue généralement entre deux sous-systèmes d'imagerie : la caméra et l'imageur. Comme son nom l'indique , la caméra est un système polyvalent, à l'instar d'un appareil photo grand public. Les caméras sont généralement dotées de la couleur, de l'autofocus, d'un nombre très élevé de pixels et d'un grand-angle, et excluent toute forme de mécanisme de visée autre que le viseur. En outre, les caméras de smartphones photographient depuis l'arrière de l'appareil. En revanche, un imageur est généralement monochrome, avec mise au point fixe, un nombre moindre de pixels, de plus grandes ouvertures de pixels, un obturateur global (tous les pixels sont exposés en même temps), un angle de champ plus étroit et un mécanisme/cadre de visée. Il capture généralement l'image depuis le devant de l'équipement.

Autres fonctions importantes pour un système robuste de capture de codes à barres, les algorithmes de traitement de signaux pour l'acquisition et le décodage des codes à barres de l'image. Les appareils Apple utilisés pour le décodage des codes à barres à l'aide de leur caméra utilisent souvent le logiciel Red Laser. Les tests empiriques sur Red Laser ont révélé de fréquentes erreurs de décodage, la prise en charge d'un nombre limité de symboles et des problèmes de décodage des codes à barres endommagés ou mal imprimés.

Avantages pour les applications de lecture de codes à barres : le sous-système de l'imageur présente un cycle de vie plus long, une plus grande sensibilité, une meilleure acquisition (visée) des codes et une résistance supérieure aux tremblements de la main.

ENCRYPTAGE FIPS WI-FI

Des organisations gouvernementales, des clients du secteur de la santé et certaines enseignes (équipées de points de vente mobiles pharma et/ou PCI) demandent que les modules cryptographiques des équipements (utilisés pour l'encryptage et le décryptage) soient certifiés FIPS 140-2 niveau 1. Ce niveau de certification FIPS assure une conception conforme aux meilleures pratiques commerciales. Les modules cryptographiques certifiés FIPS sont généralement disponibles pour les équipements professionnels et grand public. Mais ils ne s'appliquent pas forcément à la cryptographie de la liaison Wi-Fi (à usage applicatif uniquement). Par le passé, Zebra a proposé la certification FIPS pour les produits Wi-Fi sous systèmes Microsoft et a commencé à proposer, en 2014, la certification FIPS Wi-Fi sur un certain nombre de ses produits Android.

Pour toute information complémentaire, rendez-vous sur
www.zebra.com/mobilecomputers

Siège social général et siège Amérique du Nord
+1 800 423 0442
inquiry4@zebra.com

Siège Asie-Pacifique
+65 6858 0722
contact.apac@zebra.com

Siège EMEA
zebra.com/locations
mseurope@zebra.com

Siège Amérique latine
+1 847 955 2283
la.contactme@zebra.com