



Aperçu des stratégies de sécurité Palm webOS pour l'entreprise

Introduction	2
Aperçu des stratégies de sécurité Palm webOS	3
Communication sécurisée	4
Protection des données sur l'appareil	5
Environnement des applications	5
Effacement à distance	6
Sauvegarde et restauration des données	6
Conclusion	7

Introduction

Les avantages que les professionnels peuvent tirer d'un accès mobile à leurs e-mails et données professionnelles sensibles sont nombreux. Les entreprises peuvent gagner en productivité, optimiser leurs processus professionnels et faciliter la prise de décisions. Le téléphone Palm® Pre™ et Pixi™ en version plus de la plate-forme Palm webOS™ est conçu pour aider les professionnels à être plus productifs quel que soit leur emplacement. Grâce à ses fonctions très utiles (messagerie, navigateur Internet RIA, Wi-Fi sécurisé, développement d'applications conformes aux protocoles Internet, possibilité d'utiliser plusieurs applications simultanément), la plate-forme webOS s'intègre facilement à tout environnement d'entreprise.

Bien sûr, cette facilité d'accès s'accompagne d'une nécessité de protéger les données sensibles de l'entreprise et l'investissement que représentent ces appareils mobiles. Avec Palm webOS et son intégration à Microsoft® Exchange, les administrateurs informatiques et les décideurs peuvent déployer les appareils webOS en toute confiance dans leur environnement professionnel.

Le présent document examine certains des problèmes majeurs en matière de sécurité mobile et décrit les solutions de sécurité utilisées par Palm webOS.

Aperçu des stratégies de sécurité Palm webOS

Les mêmes facteurs qui font tout l'intérêt des smartphones et appareils portables aux yeux des utilisateurs itinérants (portabilité et praticité) les rendent également faciles à perdre. Il peut arriver qu'un appareil soit volé ou égaré. Il est donc crucial pour la protection des données de l'entreprise de mettre en œuvre des stratégies de sécurité appropriées régissant l'accès au réseau et à l'appareil. Palm webOS prend en charge ces stratégies de sécurité de trois manières :

1. Communication sécurisée.

Il est capital de protéger les données en transit entre l'appareil et le réseau de l'entreprise. La plate-forme webOS dispose de technologies éprouvées permettant de contribuer à la sécurisation des données en transit, que ce soit en Wi-Fi, par le biais d'un réseau de données mobiles ou par la technologie sans fil Bluetooth. La sécurité est intégrée aux applications critiques telles que la messagerie et le navigateur ; de plus, les développeurs tiers peuvent utiliser des protocoles de communication Internet sécurisés comme SSL dans leurs applications webOS.

2. Protection des données locales.

L'authentification par mot de passe au démarrage empêche les utilisateurs non autorisés d'accéder à l'appareil. La plate-forme webOS comprend une protection intégrée par mot de passe solide qui maintient le verrouillage de l'appareil tant que le mot de passe correct n'a pas été saisi. Il est possible de configurer le mot de passe sur l'appareil ou de l'appliquer à distance dans un environnement d'entreprise.

3. Environnement des applications.

Les applications s'exécutent dans un environnement "bac à sable" sur webOS. Ce mécanisme contribue à protéger les données d'une application face à tout accès non autorisé provenant d'une autre application, ce qui permet de lutter efficacement contre d'éventuels logiciels malveillants.

Malgré toutes les précautions d'un utilisateur, il peut arriver qu'il perde son appareil. Pour réduire l'impact de cet incident sur l'entreprise, la plate-forme webOS fournit également des mesures de récupération robustes permettant à l'employé de retrouver au plus vite sa productivité :

Effacement à distance.

En cas de perte ou de vol d'un appareil webOS, l'administrateur ou le propriétaire peut effacer à distance toutes les données qu'il contient. Les protocoles d'effacement des données sont configurables sur l'appareil (effacement local) ou à distance (effacement à distance).

Sauvegarde de données.

En cas de perte d'un appareil, une sauvegarde récente peut minimiser le temps d'inactivité de l'utilisateur en lui permettant de récupérer rapidement ses données, ses applications et sa configuration. Par défaut, les appareils webOS effectuent une sauvegarde quotidienne ; en outre, le service de sauvegarde emploie des technologies éprouvées pour authentifier l'appareil/utilisateur et sécuriser les données du nuage.

Communication sécurisée

La plate-forme webOS propose divers moyens d'accès et de transmission des données : réseau de données mobiles, mode Wi-Fi et technologie sans fil Bluetooth®. La plate-forme met en œuvre des procédures de sécurité telles que l'authentification et le chiffrement des données pour permettre aux utilisateurs d'accéder au réseau de l'entreprise sans courir de risque de sécurité.

Mode Wi-Fi

La plate-forme webOS prend en charge les normes de sécurité professionnelles WPA et WPA2. WPA et WPA2 utilisent une authentification 802.1x, des vérifications d'intégrité des messages et des protocoles de chiffrement solides. Tandis que le WPA emploie un chiffrement par protocole TKIP (Temporal Key Integrity Protocol), le WPA2 emploie l'AES (Advanced Encryption Standard). Le 802.1x utilise le protocole EAP pour effectuer l'authentification entre un appareil sans fil et un point d'accès avant que l'appareil obtienne l'accès au réseau de l'entreprise. La plate-forme webOS est compatible avec tous les types d'EAP les plus répandus : EAP-TLS, PEAP v1/v2, EAP-TTLS, EAP-FAST et LEAP. Cette soupe alphabétique d'authentification signifie que les appareils webOS peuvent se connecter à un réseau Wi-Fi d'entreprise avec un niveau de certitude élevé quant à la protection et la sécurité de la communication.

Technologie sans fil Bluetooth

La plate-forme webOS prend également en charge les fonctions de sécurité stipulées par la spécification Bluetooth 2.1. Avant tout transfert de données, il est ainsi nécessaire de constituer une paire autorisée avec l'appareil webOS pour vérifier que l'appareil connecté est toujours "connu" (authentifié) grâce à un échange de clé d'authentification ayant fait l'objet d'un accord mutuel préalable. De plus, les données échangées entre les appareils sont chiffrées (au niveau de la couche de liaison) selon les normes établies par les spécifications Bluetooth.

Certificats numériques

Les certificats numériques sont des signatures électroniques qui valident l'identité du serveur. La plate-forme webOS utilise les certificats numériques pour :

- Établir une connexion SSL sécurisée au serveur depuis les applications E-mail, Calendrier, Contacts et Navigateur ;
- Sécuriser les connexions Wi-Fi avec les protocoles WPA et WPA2 ;

- Signer numériquement les applications pour lutter contre les logiciels malveillants et autres applications non autorisées.

La plate-forme webOS intègre nativement les certificats racines des principales autorités de certification. Par ailleurs, les entreprises peuvent installer leurs propres certificats privés et auto-signés de façon à autoriser les appareils webOS à établir une connexion réseau sécurisée. Tous les certificats sont stockés dans la bibliothèque de certificats de la plate-forme et sont accessibles par les applications Palm, les services Palm, le mode Wi-Fi et les applications tierces développées à l'aide du kit de développement Palm Mojo.

Pour plus de détails sur l'installation de certificats numériques et l'enregistrement dans la bibliothèque de certificats de la plate-forme, consultez kb.palm.com/wps/portal/kb/common/article/40069_en.html

Messagerie

La plate-forme webOS prend en charge les mécanismes de sécurité que propose Microsoft Exchange ActiveSync (EAS) ainsi que les protocoles de messagerie POP et IMAP.

Quand un appareil webOS est configuré pour se synchroniser avec le serveur Microsoft Exchange, il emploie le protocole professionnel EAS. La connexion SSL entre le serveur et l'appareil est sécurisée à l'aide d'un certificat auto-signé ou émis par une autorité de certification ; si les certificats exigés ne sont pas installés et enregistrés dans la bibliothèque de certificats de la plate-forme, la synchronisation EAS est refusée. Comme décrit dans la section suivante, la plate-forme prend en charge plusieurs stratégies EAS pour contribuer à assurer à l'administrateur réseau que les appareils webOS ne compromettent pas les données de l'entreprise. Avec EAS, l'utilisateur peut synchroniser ses e-mails (dossiers compris), contacts, calendriers et tâches de façon sécurisée ainsi que rechercher des adresses dans le répertoire professionnel avec la fonction Liste d'adresses globale (GAL, Global Address List). Cet équilibre entre facilité d'utilisation et sécurité optimise la productivité des utilisateurs.

Navigateur

Le puissant navigateur Internet de webOS permet aux utilisateurs de naviguer et interagir en toute sécurité avec les sites Web sécurisés (https://) à l'aide du protocole SSL. Ce faisant, il est nécessaire de surveiller l'apparition d'éventuels avertissements ou erreurs de certificat et de vérifier que la connexion est sécurisée (c'est-à-dire que l'URL commence par https://). En règle générale, il est conseillé aux utilisateurs d'éviter les activités sensibles sur un réseau non sécurisé comme un hotspot Wi-Fi public (qui n'emploie pas de sécurité WPA ou WPA2).

Protection des données sur l'appareil

Les utilisateurs ont besoin de sécurité non seulement des communications, mais aussi de leur appareil. La plate-forme webOS fournit divers moyens de protéger les données de l'appareil. Les utilisateurs peuvent verrouiller les appareils webOS avec un mot de passe qui empêche tout accès non autorisé quand l'appareil n'est pas utilisé.

Pour déverrouiller l'appareil et obtenir l'accès, les utilisateurs doivent s'authentifier en saisissant le bon mot de passe. Dans la mesure où il est difficile de sécuriser physiquement un téléphone, il est très important qu'aucune personne non autorisée ne soit en mesure d'y accéder. L'authentification contribue à la protection des données sensibles et de l'accès au réseau en cas de perte ou de vol de l'appareil.

Dans un environnement d'entreprise, l'administrateur réseau peut sécuriser les appareils webOS qui se connectent à son réseau en mettant en place des stratégies de mot de passe. Quand un appareil webOS est configuré pour accéder à Microsoft Exchange, les stratégies Exchange ActiveSync (EAS) sont transmises à distance à l'appareil et forcent l'utilisateur à protéger l'appareil à l'aide d'un mot de passe. De plus, un utilisateur peut configurer plusieurs comptes Exchange sur un même appareil webOS ; le cas échéant, la plate-forme utilise intelligemment l'intersection de stratégies la plus stricte. Aucune démarche supplémentaire n'est nécessaire pour l'utilisateur ou l'administrateur réseau ; la plate-forme webOS configure automatiquement l'appareil pour que l'utilisateur puisse y accéder sans enfreindre les stratégies mises en place par l'un ou l'autre des serveurs Exchange.

La plate-forme webOS prend en charge les stratégies EAS suivantes :

- Verrouillage par mot de passe de l'appareil.
- Définition d'une longueur minimale pour le mot de passe. Sur un téléphone webOS, les mots de passe alphanumériques peuvent comporter de 2 à 18 caractères. Les mots de passe numériques peuvent comporter jusqu'à 32 chiffres.
- Demande d'un mot de passe constitué à la fois de chiffres et de lettres. Les téléphones Palm webOS prennent en charge une combinaison de caractères numériques et non numériques pour renforcer les mots de passe. La solidité d'un mot de passe joue un rôle important dans la sécurité d'un appareil.

- Maximum d'échecs de saisie du mot de passe autorisés. L'administrateur peut limiter le nombre de tentatives de connexion incorrectes sur un téléphone webOS. Tout dépassement de cette limite entraîne l'effacement des données sur l'appareil (effacement local). Il s'agit en général du meilleur moyen de lutter contre une tentative d'intrusion par essais successifs en saisissant diverses permutations de mot de passe.
- Verrouillage automatique après un délai d'inactivité. L'écran se verrouille après 3 minutes d'inactivité et l'administrateur peut définir un délai avant saisie du mot de passe allant jusqu'à 30 minutes.

Pour plus de détails sur l'intégration des stratégies EAS à webOS, consultez kb.palm.com/wps/portal/kb/common/article/58353_en.html

Environnement des applications

Dans la plate-forme webOS, toutes les applications s'exécutent dans un environnement "bac à sable" qui contribue à limiter les accès non autorisés aux données et services des autres applications. Les applications peuvent uniquement interagir entre elles avec les API et services spécifiques proposés par le système d'exploitation dans l'environnement Mojo. Mojo fournit un certain nombre de mécanismes permettant le développement d'applications sécurisées, y compris des fonctions de cryptographie et l'utilisation du protocole SSL pour les connexions à distance. La validation des certificats a lieu lors de toute connexion SSL par l'intermédiaire de Mojo.

Les applications Palm webOS autres que celles préchargées sur l'appareil ne peuvent être téléchargées que depuis l'App Catalog Palm. Toutes les applications téléchargées depuis le catalogue comportent la signature numérique de Palm qui est vérifiée lors de l'installation.

Le kit de développement Mojo est disponible au téléchargement depuis developer.palm.com

Effacement à distance

En cas de perte ou de vol d'un appareil webOS, l'administrateur informatique de l'entreprise ou le propriétaire de l'appareil peut effacer à distance toutes les données qu'il contient. Les mécanismes suivants réduisent les risques d'utilisation frauduleuses en cas de perte ou de vol d'un appareil webOS :

- Comme indiqué précédemment dans le présent document, l'administrateur informatique de l'entreprise peut limiter le nombre d'échecs de saisie du mot de passe. Une fois cette limite dépassée, toutes les données et tous les paramètres de l'appareil sont effacés.
- Si l'appareil webOS se connecte à Microsoft Exchange, l'administrateur peut effectuer un effacement à distance depuis la console de gestion d'Exchange. Il est également possible d'ordonner l'effacement à distance en se connectant à Outlook Web Access (Exchange 2007 uniquement).
- Le propriétaire de l'appareil peut se connecter à la console de l'utilisateur Palm avec l'identifiant et le mot de passe de son profil Palm pour effacer à distance toutes les données de l'appareil perdu ou volé. Un utilisateur ne peut effacer un appareil que si l'appareil en question est enregistré avec un profil Palm. Pour renforcer encore la protection contre les programmes malveillants et l'effacement accidentel, l'utilisateur doit remplir une vérification CAPTCHA avant d'activer l'effacement à distance.

Sauvegarde et restauration des données

Si l'appareil est perdu ou compromis, les procédures de sauvegarde et de récupération appropriées peuvent restaurer rapidement la productivité de l'utilisateur. Palm propose des services de sauvegarde et de restauration pour les appareils webOS afin d'assurer la préservation de certaines données utilisateurs et certains paramètres de personnalisation de l'appareil¹ en cas de réinitialisation ou de remplacement. Les données sont sauvegardées sur des serveurs gérés par Palm et protégées à l'aide de procédures et stratégies de sécurités reconnues par l'industrie.

La connexion entre l'appareil et le serveur de sauvegarde fait l'objet d'une authentification mutuelle sécurisée par SSL et les données sont chiffrées lors du transit. Au repos, les données sont chiffrées à l'aide de clés AES-128 spécifiques à l'utilisateur. Lors d'une opération de restauration, l'utilisateur n'a accès aux données qu'après s'être connecté avec l'adresse e-mail et le mot de passe du profil Palm enregistré sur son appareil. De plus, tous les mots de passe stockés en local sur l'appareil sont chiffrés et l'appareil peut être verrouillé par un mot de passe ou code PIN local activé par l'utilisateur ou par un administrateur informatique via les paramètres Microsoft Exchange.

Les appareils Palm webOS sont configurés de façon à sauvegarder par défaut les données et préférences utilisateur sur les serveurs gérés par Palm. L'utilisateur peut désactiver les services de sauvegarde à tout moment grâce à l'application Sauvegarde incluse ; si un utilisateur désactive la sauvegarde de son appareil, les données de sauvegarde associées à son profil sont effacées des serveurs de Palm.

Pour consulter la liste des données et paramètres inclus dans la sauvegarde, consultez kb.palm.com/wps/portal/kb/common/article/19388_en.html

Conclusion



Environnement sécurisé des applications
Stockage de données "bac à sable"
Protection par code Pin / mot de passe
Mots de passe chiffrés / informations d'identification



Connexion sécurisée
128 bits SSL
Wi-Fi sécurisé (WPA, WPA2)



Stockage de données chiffrées en AES
Authentification mutuelle basée sur des certificats numériques, informations d'identification
Applications signées dans l'App Catalog
Application de la stratégie EAS, Effacement à distance

La plate-forme Palm webOS fournit une protection des données en transit, au repos, et sauvegardées avec le service de sauvegarde de Palm. Elle prend en charge les stratégies de sécurité professionnelles les plus couramment utilisées et fournit des méthodes de récupération rapide suite à la perte ou au vol de l'appareil. Palm webOS est une plate-forme mobile sécurisée que les entreprises peuvent déployer en toute confiance.

Au final, il incombe aussi en partie à l'utilisateur de se servir des fonctions de sécurité de la plate-forme. À ce titre, il peut être judicieux pour l'entreprise de former ses employés pour les sensibiliser aux pratiques et stratégies de sécurité et leur rappeler les précautions basiques d'utilisation, notamment verrouiller l'appareil quand ils ne l'utilisent pas, éviter les activités sensibles quand ils sont connectés à un réseau Wi-Fi non protégé, et prendre en compte tout avertissement relatif aux certificats numériques.

Pour en savoir plus sur les stratégies de sécurité Palm, rendez-vous sur palm.com/security

1. Les sauvegardes comprennent Contacts, Calendriers, Mémos et Tâches ainsi que les préférences et les logiciels téléchargés depuis l'App Catalog.

© 2010 Palm, Inc. Palm, Pre, Pixi, webOS, Mojo, Synergy et Touchstone sont des marques commerciales de Palm, Inc. Microsoft, ActiveSync et Outlook sont des marques commerciales ou déposées du groupe Microsoft.

Pour plus d'informations sur...

Stratégies de sécurité Palm :

palm.com/security

Palm webOS pour les professionnels :

palm.com/fr/fr/business/index.html

Information sur le Palm Pre et Pixi :

palm.com/fr

Gartner :

gartner.com/DisplayDocument?id=1122312&ref=g_fromdoc

Un rapport de Philippe Winthrop :

strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=4811

Un blog de Philippe Winthrop :

enterprisemobilitymatters.com