Informe técnico de seguridad y capacidad de administración

Dispositivos Android preparados para empresas HP

Mayo de 2015

Índice

Resumen ejecutivo

Una de las plataformas de sistema operativo (SO) para dispositivo móvil más populares, Android está equipada con una serie de medidas de seguridad para proteger a los usuarios de las amenazas y los ataques de la era moderna. Sin embargo, muchas decisiones de seguridad son dejadas a merced de cada proveedor de hardware, lo que deja a los dispositivos Android abiertos a vacíos y debilidades críticas si la seguridad no recibe prioridad total.

Los dispositivos Android preparados para la empresa HP ayudan al personal de TI a superar estos desafíos clave al implementar, asegurar y administrar dispositivos Android en un entorno comercial. El enfoque integral de la seguridad de Android preparado para la empresa HP se extiende desde el diseño del producto y la fabricación hasta la actualización de dispositivos en el campo. HP refuerza la seguridad del dispositivo al sacar provecho de las capacidades de hardware, firmware y nube sin fragmentar las interfaces de programación de aplicaciones (API) de Android ni romper la compatibilidad con las aplicaciones de Android y las soluciones de administración de movilidad empresarial (EMM).

Este informe técnico ofrece una descripción general de las características de seguridad y capacidad de administración de Android preparado para la empresa HP, entre las que se incluye:

- Funciones de cargador de arranque, cifrado y raíz de confianza reforzadas por hardware
- La función de almacenamiento de clave seguro que impide el acceso no autorizado a las claves criptográficas utilizadas por el cifrado y las aplicaciones del dispositivo
- Endurecimiento de la seguridad que minimiza el daño de tipos específicos de amenazas
- Protección antirrobo que permite al personal de TI identificar, bloquear y borrar un dispositivo perdido o robado
- Capacidad de administración inmediata desde la caja con HP Touchpoint Manager[1], lo que brinda a las organizaciones una única solución para administrar a sus usuarios, datos y dispositivos Android

Público

Administradores de TI y administradores de sistemas que buscan comprender las características de seguridad y de capacidad de administración de los dispositivos Android preparados para la empresa HP. Este público ya debe estar familiarizado con los siguientes temas:

- Dispositivos móviles
- Seguridad móvil
- Administración de dispositivos móviles
- Sistema operativo Android

Productos aplicables

Las características descriptas en este documento son aplicables a los siguientes productos de 2015-16:

- Tablet HP Pro Slate 8
- Tablet HP Pro Slate 12

Descargo de responsabilidad

Algunos de los detalles incluidos en este documento pueden variar dependiendo del paquete de semiconductor del system-on-chip (SoC) utilizado en un modelo de dispositivo en particular. Los dispositivos Android preparados para la empresa futuros se incluirán en informes técnicos adicionales o actualizaciones a este informe técnico.

[1] HP Touchpoint Manager es compatible con los sistemas operativos Android, iOS y Windows y equipos, notebooks, tablets y smartphones de varios fabricantes. No está disponible en todos los países. Se requiere un plan de suscripción. Consulte hp.com/touchpoint para obtener información de disponibilidad, precios y requisitos del sistema.

Glosario de acrónimos y términos

AD	Directorio Activo Microsoft
AES	Sistema de cifrado de avanzada Consulte http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
ARM	Máquinas RISC de avanzada: se refiere a la arquitectura de microprocesador utilizada en dispositivos Android preparados para la empresa HP. Consulte http://www.arm.com/products/processors
BYOD	Traiga su propio dispositivo
CBC	Cifrado por bloques. Consulte CBC-AES
CBC-AES	Cifrado por bloques: un modo de operación AES Consulte http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
DDR-SDRAM	Memoria de acceso aleatorio dinámica y sincrónica de doble velocidad de datos
DPM	Administrador de política de dispositivos Android. Consulte http://developer.android.com/reference/android/app/admin/DevicePolicyManager.html
EAS	Exchange ActiveSync: se refiere al protocolo de Microsoft para sincronizar el correo, los contactos, el calendario y las tareas entre clientes móviles y servidores de Microsoft Exchange
EMM	Administración de movilidad empresarial: se refiere a los servidores utilizados para asegurar y administrar el acceso a datos y aplicaciones empresariales. Incluye MDM, MAM, MCM, entre otros.
FIPS	Estándares federales de procesamiento de información Consulte http://www.nist.gov/itl/fipsinfo.cfm
HMAC	Código de autenticación de mensajes en hash: un mecanismo para la autenticación de mensajes mediante funciones hash criptográficas. Consulte http://tools.ietf.org/html/rfc2104
MAC	Código de autenticación de mensaje Además, consulte HMAC
MAM	Administración de aplicaciones móviles
MCM	Administración de contenido móvil
MDM	Administración de dispositivos móviles
NIST	Instituto nacional de estándares y tecnología Consulte http://nist.gov
OEM	Fabricante de equipo original: hace referencia a los fabricantes de dispositivos
PBL	Cargador de arranque principal: hace referencia al primer código que se ejecuta cuando se enciende un procesador. Este código inicializa el procesador principal y carga los cargadores de arranque secundarios del procesador (SBL).
PKI	Infraestructura de clave pública: admite la distribución de las claves de cifrado públicas. De ese modo permite a los usuarios y a los equipos intercambiar datos en forma segura y verificar las identidades. Consulte http://en.wikipedia.org/wiki/Public_key_infrastructure
ROM	Memoria de solo lectura
RSA	Hace referencia a un sistema criptográfico de clave pública ampliamente utilizado para proteger los intercambios de datos entre dos equipos Consulte http://en.wikipedia.org/wiki/RSA_(cryptosystem)
SBL	Cargador de arranque secundario: realiza la inicialización específica del procesador
SHA	Algoritmos hash seguros Consulte http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf
SoC	System on chip: hace referencia a un paquete de semiconductor que incluye la CPU, la ROM y otros procesadores y componentes
TEE	Entorno de ejecución de confianza: hace referencia al entorno de confianza creado con ARM TrustZone para ejecutar las aplicaciones de confianza
TZ	TrustZone: hace referencia a la tecnología ARM TrustZone
VPN	Redes privadas virtuales
AES-XTS	Cipher text stealing: un modo de operación AES Consulte http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

Introducción

Cómo asegurar un Android

Una de las plataformas de sistema operativo (SO) para dispositivo móvil más populares, Android,™ está diseñada para proteger a los usuarios de las amenazas y los ataques de la era moderna. Entre sus beneficios y capacidades de seguridad clave se incluyen:[2]

- Aprovechamiento de las medidas de seguridad a nivel SO integradas en el kernel Linux® endurecido para dar batalla
- Ofrecimiento de seguridad reforzada a nivel kernel mediante las capacidades de seguridad mejorada (SE) de Linux
- Minimización del daño ocasionado por el malware o las aplicaciones de mal comportamiento por medio del aislamiento de las aplicaciones en "sandboxes"
- Seguridad de las aplicaciones respecto de cambios no autorizados o al permitir que las aplicaciones colaboren en forma segura mediante el uso de firmas criptográficas
- Protección de los recursos del sistema mediante la limitación de los privilegios de las aplicaciones al nivel mínimo necesario y al asegurar las comunicaciones entre procesos
- Otorgamiento de visibilidad y control a los usuarios sobre lo que puede hacer una aplicación mediante el uso de un modelo de permisos otorgados por el usuario
- Habilitación de características de seguridad adicionales y específicas de hardware, tal como ARM eXecute-Never y almacenes de clave con el respaldo de hardware

Debido a que Android alimenta a todo tipo de dispositivos, grandes y pequeños, costosos y económicos, muchas de las decisiones que afectan la seguridad del dispositivo quedan a criterio del proveedor de hardware. Si bien ciertas características de seguridad son inherentes al SO Android en sí mismo, estas características se pueden ver comprometidas si el proveedor de hardware no realiza un trabajo adicional a fin de asegurar el sistema. En un escenario típico, el proveedor de SoC toma el código fuente del Proyecto de código abierto de Android y los puertos al SoC. Algunos SoC admiten características de seguridad a nivel hardware, como TrustZone, raíz de confianza de hardware y módulos criptográficos; otros pueden no admitir ninguno de estos. Los fabricantes de dispositivos realizan funciones críticas, tales como habilitar el arranque seguro, la integración con TrustZone y los módulos criptográficos de hardware, la firma de imágenes del sistema, aseguran las claves de la plataforma, realizan parches de seguridad en forma permanente y mucho más. El proceso puede dejar atrás vacíos y debilidades críticas. Por ejemplo:

- Cuando el arranque seguro no está implementado o se implementa en forma incorrecta, la imagen del software del dispositivo de un usuario desprevenido se puede alterar para recolectar las credenciales de usuario y datos sensibles.
- Cuando la clave de la plataforma no está bien protegida en el proceso de fabricación, puede terminar en manos de criminales cibernéticos. Con la clave de la plataforma, un creador de malware puede obtener privilegios de raíz y acceso ilimitado a los datos del usuario, credenciales de la aplicación y mucho más. Esto puede generar la filtración de información privada del cliente de importancia crítica, de secretos comerciales u otra información, y provocar un daño a la empresa y a sus clientes.
- Cuando se utiliza un cifrado de dispositivo en función de software, un atacante sofisticado puede vaciar la RAM del dispositivo para recuperar la clave de cifrado y descifrar los datos.
- Cuando se descubre una nueva vulnerabilidad en el dispositivo, los proveedores del dispositivo tienen la responsabilidad de hacer un parche del firmware del dispositivo y reparar la vulnerabilidad de inmediato. No muchos proveedores de dispositivos tienen la capacidad y los recursos necesarios para hacer el parche de inmediato. Cuando no se aplica el parche, los dispositivos se convierten en blancos fáciles para la explotación de las debilidades conocidas.

El enfoque de HP

Los dispositivos Android preparados para la empresa HP están diseñados para ocuparse de los puntos débiles clave en la implementación, la protección y la administración de dispositivos Android para las empresas. HP refuerza la seguridad al sacar provecho de las capacidades de hardware, firmware y nube sin fragmentar las interfaces de programación de aplicaciones (API) de Android, ni quebrar la compatibilidad con las aplicaciones de Android y las soluciones de administración de movilidad empresarial (EMM). Este enfoque brinda seguridad de clase empresarial sin crear dependencia respecto de un único proveedor.

Además, la aplicación HP Touchpoint Manager ofrece una única solución basada en la nube para administrar usuarios, datos y los dispositivos Android de los usuarios, además de dispositivos que funcionan sobre una plataforma Microsoft® Windows® o iOS, desde un panel de mando fácil de usar. Con HP Touchpoint Manager, el personal de TI puede acceder a herramientas de administración, seguridad y soporte de usuario desde prácticamente cualquier lugar para resolver problemas en tiempo real, y de ese modo mejorar la eficacia de la TI y la productividad de los empleados. Los gerentes de TI y los usuarios finales por igual pueden usar el asistente de instalación basado en un agente para registrar dispositivos que funcionan sobre las plataformas Microsoft® Windows®, Android™ e iOS.

[2] Si desea obtener información adicional sobre la seguridad de Android, consulte https://source.android.com/devices/tech/seguridad.

Entre los pilares clave de los dispositivos Android preparados para la empresa HP seguros se incluyen los siguientes:

Hardware de confianza. Los SoC brindan raíz de confianza reforzada por el hardware, cifrado y funciones de cargador de arranque que desempeñan un papel fundacional en términos de la seguridad del dispositivo. Los dispositivos Android preparados para la empresa HP están creados sobre plataformas SoC comprobadas con características de seguridad sólidas de proveedores de confianza, con inclusión de Qualcomm e Intel, que cuentan con procesos establecidos para asegurar las plataformas desde el diseño hasta la producción. Sumado a ello, en el caso de los dispositivos con procesadores basados en ARM, los dispositivos Android preparados para la empresa HP utilizan la tecnología ARM TrustZone para suministrar un entorno de ejecución de confianza (TEE) para implementar funciones de seguridad sensibles, tal como asegurar las claves de cifrado y las claves del almacén de claves.

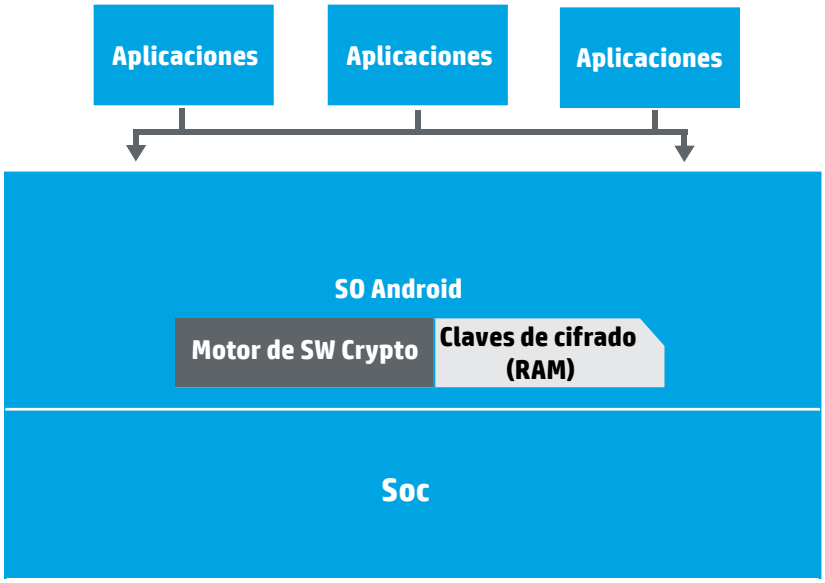
Firmware de confianza. Solo las imágenes de firmware autorizadas por HP se pueden ejecutar en dispositivos Android preparados para la empresa, protegiendo al usuario del daño resultante del uso de firmware no autorizado o que no es de confianza.

Endurecimiento constante. En un entorno de amenazas en evolución constante, los productos también deben evolucionar para soportar nuevas vulnerabilidades y ataques. Los dispositivos Android preparados para la empresa HP son sometidos a un endurecimiento adicional de la seguridad por medio de una serie de políticas de seguridad mejorada de Android; además, HP perfecciona estas políticas con regularidad para enfrentar el escenario de amenazas en evolución. HP asume un enfoque integral de la seguridad en el diseño de nuestros productos, tal como las tablets HP Pro Slate 8 y HP Pro Slate 12, al proteger el proceso de fabricación e implementar actualizaciones de seguridad a dispositivos en el campo por medio de parches por aire.

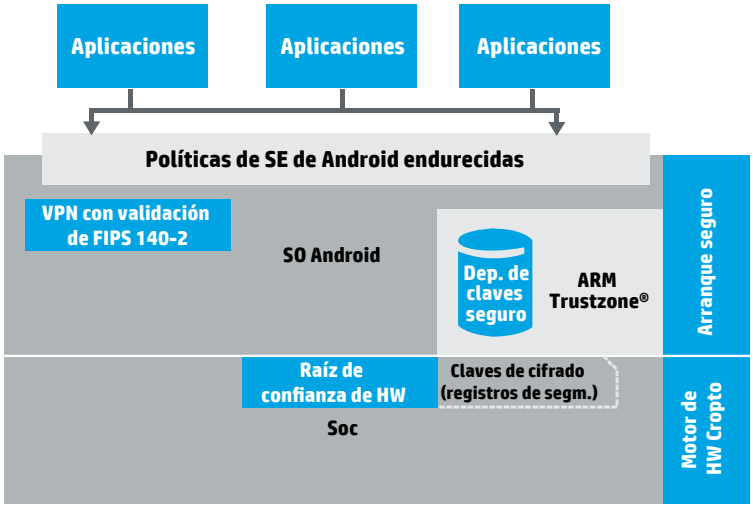
Sin fragmentación de API. Debido a que la mayoría de las empresas usan dispositivos de múltiples proveedores, las API específicas del proveedor y las políticas de seguridad solo aumentarán la complejidad de proteger y administrar una flota de dispositivos. HP ayuda a evitar dichos problemas mediante el enfoque de no desfragmentación, que permite a los administradores de TI utilizar el mismo proceso para administrar dispositivos Android preparados para la empresa HP y dispositivos Android existentes. Los dispositivos Android preparados para la empresa HP también trabajan con la mayoría de las soluciones EMM que admiten Android, lo que permite a los administradores de TI reutilizar las soluciones EMM existentes. Esta es una de las muchas maneras en que HP brinda compatibilidad con los complejos entornos de SO múltiples que las empresas deben administrar en forma cotidiana.

Características del dispositivo Android preparado para la empresa HP

Los dispositivos Android preparados para la empresa HP implementan características de seguridad críticas necesarias para proteger los datos del usuario y que van más allá de los recursos disponibles en la mayoría de los dispositivos Android comercialmente disponibles dirigidos a los consumidores. Las imágenes que siguen ayudan a visualizar la diferencia.



Una implementación de dispositivos Android existentes



Implementación segura de dispositivos Android preparados para la empresa HP

Las características de seguridad de dispositivos Android preparados para la empresa HP ofrecen los siguientes beneficios:

ARM TrustZone® brinda un entorno de confianza para enfrentar los ataques de hardware y software.

El arranque seguro garantiza que solo imágenes Android autorizadas se ejecuten en los dispositivos.

El almacenamiento de clave seguro impide el acceso no autorizado a las claves criptográficas utilizadas por el cifrado del dispositivo y las aplicaciones.

El cifrado de dispositivo acelerado por hardware refuerza la seguridad, reduce los tiempos de espera y conserva la energía.

La VPN validada por FIPS 140-2 opera para las industrias reguladas tal como el sector de finanzas y del cuidado de la salud, junto con agencias gubernamentales de los EE. UU. que requieren el cifrado validado para pilas de redes privadas virtuales (VPN).

El endurecimiento de la seguridad minimiza el daño de tipos específicos de amenazas, tales como ataques de escalamiento de privilegios.

La compatibilidad con Microsoft Exchange ActiveSync funciona con entornos Microsoft Exchange existentes para habilitar el acceso móvil al correo electrónico, contactos y calendario.

La capacidad de actualización por aire lo ayuda a garantizar que los dispositivos permanezcan actualizados en términos de parches de seguridad, tal como correcciones de la vulnerabilidad de Heartbleed, nuevos recursos como Android Work y nuevos lanzamientos como Android Lollipop.

La protección antirrobo de HP Touchpoint Manager lo ayuda a evitar poner en riesgo los documentos y datos sensibles al permitir al personal de TI ubicar, bloquear y eliminar un dispositivo robado o perdido.

La compatibilidad con EMM posibilita una administración estandarizada con soluciones de MDM de terceros.

La capacidad de administración inmediata desde la caja con HP Touchpoint Manager permite que las empresas protejan y administren los dispositivos Android listos para la empresa sin necesidad de infraestructuras adicionales, grandes inversiones ni recursos de TI adicionales.

Seguridad

ARM TrustZone®

Brinda un entorno seguro para mitigar los riesgos de los ataques de hardware y software

En su núcleo, los dispositivos Android preparados para la empresa HP, utilizan la tecnología ARM TrustZone (TZ) comprobada que ofrece un entorno seguro e independiente del hardware, un espacio de memoria independiente y un TEE. El TEE ejecuta funciones de seguridad para minimizar las vulnerabilidades de firmware y del SO, además de los riesgos del malware y las aplicaciones con mala conducta que se ejecutan en el SO.

Los dispositivos Android preparados para la empresa HP sacan provecho de TrustZone para asegurar el proceso de arranque, las claves de cifrado de los datos en reposo y las claves de aplicación almacenadas en Android KeyStore. En las siguientes secciones se brinda más información.

Escenario de ejemplo

Un empleado intenta instalar una imagen personalizada en el dispositivo móvil, que podría introducir vulnerabilidades desconocidas.

Los dispositivos Android preparados para la empresa HP usan la característica de arranque seguro para impedir que los usuarios y hackers carguen imágenes de SO no autorizadas para obtener acceso a redes y datos corporativos.

Arranque seguro

Establece una plataforma de confianza para las aplicaciones Android al impedir el uso de un código no autorizado en el proceso de arranque

Los dispositivos Android preparados para la empresa HP admiten que la secuencia de arranque seguro ofrezca una plataforma de confianza para las aplicaciones de Android. La secuencia usa métodos criptográficos para autenticar el software mediante la verificación de que HP haya firmado la imagen de software. Este proceso impide la inyección de código malicioso y no autorizado durante el proceso de arranque.

El arranque seguro empieza desde una raíz de confianza de hardware que consiste en un conjunto de fusibles de hardware que se configuran por única vez (memoria no volátil que solo se puede escribir una vez) y Cargadores de arranque primarios (PBL). Uno de los fusibles de hardware contiene una clave pública HP que autentica el software. Escribir esta clave en la fábrica impide la subsiguiente manipulación que puede, por ejemplo, permitir que imágenes de firmware no autorizadas se ejecuten y pongan en riesgo los datos del usuario. El código PBL reside en el área de la memoria de solo lectura (ROM) dentro del SoC, hecho que garantiza que el código PBL permanezca sin modificar. Esta combinación es inmutable y funciona como la raíz de confianza para brindar un cimiento de confianza desde donde se inicia la secuencia de arranque. Cada paso de la secuencia de arranque carga y autentica el código utilizado en el paso subsiguiente antes de ejecutar este código y, de este modo, establece una cadena de confianza para autenticar todo el código que se ejecuta desde el inicio del arranque hasta el inicio de las aplicaciones.

Ante el encendido, PBL carga, ejecuta y autentica el código del Cargador de Arranque Secundario (SBL). El primer código mutable que se ejecuta en el proceso de arranque, SBL inicializa la DDR-SDRAM y luego carga y autentica el software TrustZone. Ejecutar el código TrustZone antes que el resto del código mutable lo ayuda a proteger la integridad del entorno seguro TrustZone. El código TrustZone configura un entorno seguro en el cual se puede almacenar claves criptográficas en forma segura, con verificación permanente y realizar su supervisión.

En forma subsiguiente, SBL carga y autentica el código que inicializa el resto del SoC y los procesadores de aplicación. Cuando está disponible, SBL también carga y autentica el firmware moderno antes de la ejecución. El proceso culmina con la carga y la autenticación del kernel Android. El software TrustZone verifica el código que inicializa y opera los periféricos.

Los dispositivos Android preparados para la empresa HP utilizan pares de clave PKI para verificar el software. Tal como se explicó más arriba, la clave pública se fusionó en el dispositivo de fábrica en un fusible programable por única vez. La clave privada se usa para firmar la imagen de software cargada en los dispositivos. La clave privada está segura dentro de las instalaciones de HP y con acceso limitado a cierto personal de HP autorizado. El mecanismo de verificación no requiere que las claves públicas sean secretas, lo que permite a HP programarlas de fábrica sin poner en juego la integridad del proceso de arranque seguro.

La implementación del arranque seguro de Android preparado para la empresa HP utiliza 65537 claves RSA públicas de exponente de 2048 bits para certificados y firmas de imagen. El algoritmo SHA256 se usa para firmar los certificados PKI, mientras que el código en sí se firma mediante un algoritmo de propiedad exclusiva.

Escenario de ejemplo

Los criminales cibernéticos intentan extraer la clave de cifrado mediante la carga lateral de malware y el vaciado de la memoria del dispositivo.

Si bien este ataque podría funcionar en un dispositivo Android existente, los dispositivos Android preparados para la empresa HP utilizan un sistema de administración de clave en función de ARM TrustZone para proteger las claves. Dado que las claves no se almacenan en la RAM, vaciar la memoria del dispositivo no revela la clave de cifrado.

Almacenamiento seguro de claves

Garantiza la integridad de las capacidades criptográficas al proteger las claves en la TrustZone

Android brinda un componente de clave maestra como un servicio para las aplicaciones. Este componente implementa la generación, firma y verificación de clave. Los servicios y las aplicaciones de Android usan estas funciones para proteger los datos mediante el cifrado y para verificar la integridad de los datos mediante las firmas. Cuando la integridad de la función de administración de claves o las claves mismas se ven comprometidas, la seguridad de los datos también se ve comprometida.

Para evitar dichos riesgos, los dispositivos Android preparados para la empresa HP implementan un entorno de clave maestra con el soporte de hardware en el cual se realiza la generación, el almacenamiento, la firma y la verificación de la clave. Las claves almacenadas pueden ser accedidas por aplicaciones de confianza que se ejecutan dentro de TrustZone y las claves nunca dejan la TrustZone. Este enfoque impide la presencia de cualquier malware del lado Android desde las teclas de acceso.

Asimismo, los dispositivos Android preparados para la empresa HP protegen la integridad de las funciones de administración de clave mediante su implementación con el entorno TrustZone. Las API de clave maestra estándar luego exponen estas funciones a Android.

Escenarios de ejemplo

Criminales cibernéticos roban la tablet de un ejecutivo para extraer información corporativa muy sensible.

Mediante HP Touchpoint Manager o una solución EMM compatible, el personal de TI aplica una política que exige el cifrado del dispositivo como requisito para proteger datos confidenciales. Esta política ayuda a minimizar el riesgo al evitar que dispositivos no cifrados accedan al correo electrónico laboral, sus contactos y datos del calendario. Cualquier dato de usuario extraído de dispositivos cifrados carece de utilidad para los criminales cibernéticos.

Los criminales cibernéticos intentan adivinar la contraseña del usuario para descifrar los datos.

Los dispositivos Android preparados para la empresa HP usan un cifrado basado en hardware que elimina los datos automáticamente después de 32 intentos fallidos. Esta conducta tiene un código duro y es resistente a las violaciones.

Cifrado de dispositivo acelerado por hardware

Brinda una seguridad mejorada para los datos en reposo mediante un cifrado contra falsificaciones, de consumo eficiente de energía y basado en hardware

Android brinda un mecanismo de cifrado de dispositivo para proteger los datos del usuario almacenados en el dispositivo. En forma predeterminada, este mecanismo usa un motor de cifrado implementado en el software y emplea AES-CBC-ESSIV: algoritmos SHA-256 con claves de 128 bits.

Los dispositivos Android existentes implementan un cifrado basado en software para minimizar los costos relacionados con los módulos de hardware adicionales y los esfuerzos de integración específicos de hardware. Este enfoque presenta varias desventajas. En primer lugar, la clave de cifrado puede verse comprometida, ya que se almacena en el área RAM. En segundo lugar, el cifrado basado en software hace que el sistema sea más lento, ya que las operaciones de cifrado intensivas en informática se realizan en el software más que en el hardware. En tercer lugar, este enfoque consume energía en exceso.

Los dispositivos Android preparados para la empresa HP utilizan motores de cifrado basado en hardware para el cifrado y descifrado y un mecanismo basado en hardware para almacenar y recuperar las claves de cifrado. Juntas, estas características ofrecen mejor seguridad, velocidad y consumo de energía más eficiente. Los dispositivos Android preparados para la empresa HP utilizan AES-XTS-plain64: algoritmos SHA-256 con claves de 256 bits para el cifrado de sistema de archivo. Un generador de cifra aleatoria de hardware genera una clave, que se codifica mediante un hash derivado de la contraseña informada por el usuario. La clave cifrada se almacena en un depósito de claves. Este dato se cifra aún más mediante un componente de TrustZone usando un algoritmo AES-256 CBC y se la verifica con HMAC-SHA-256, lo que brinda otra capa de seguridad. Los datos del depósito de claves cifradas están asegurados mediante un mecanismo con versiones y protección contra reproducciones seguro para evitar las manipulaciones.

Asimismo, los dispositivos Android preparados para la empresa HP permiten a las empresas aplicar políticas de seguridad que requieran a los usuarios encender el cifrado del dispositivo mediante una solución compatible con EMM.

VPN validada por las FIPS 140-2

Cumple con los requisitos del gobierno de EE. UU., defensa e industrias reguladas tal como el sector del cuidado de la salud y finanzas

Los dispositivos Android preparados para la empresa HP implementan el cifrado de 256 bits validado por FIPS 140-2 para la conectividad de Redes privadas virtuales (VPN). Esta característica garantiza una conectividad segura a las redes corporativas y utiliza SSL y estándares IPsec VPN. Además, admite la autenticación segura con directorios corporativos, incluso Microsoft Active Directory (AD).

Esta implementación de VPN está certificada por el consorcio de VPN (VPNC) para la interoperabilidad con proveedores y aplicaciones gateway VPN líderes.

Escenario de ejemplo

Un competidor toma control de la tablet de un vicepresidente de ventas de la empresa e intenta obtener acceso permanente a la información confidencial.

El competidor instala malware para espiar información del dispositivo e informarla a un servidor oculto en forma constante. El malware requiere de privilegios a nivel sistema para obtener acceso ilimitado, y la tablet está arraigada para obtener dichos privilegios.

En dispositivos Android preparados para la empresa HP, las políticas de SE Android endurecidas protegen los datos mediante la limitación de este tipo de ataque de escalamiento de privilegio.

Endurecimiento de la seguridad

Mitiga los ataques a nivel aplicación mediante políticas de SE de Android endurecidas y configuraciones de seguridad

La seguridad mejorada (SE) de Android, basada en la SE de Linux, habilita el control del acceso basado en normas para proteger los recursos del sistema Android, sus servicios y datos de aplicaciones. Los dispositivos Android incluyen un conjunto de políticas de SE de Android endurecidas que:

- Protegen los datos de la aplicación al reforzar los “sandboxes” de la aplicación para evitar el acceso de aplicaciones con mala conducta y malware
- Impiden el acceso no autorizado a los servicios del sistema, el almacenamiento y los sensores al impedir ataques de escalamiento de privilegio, tal como ataques de raíz, que obtienen acceso ilimitado al dispositivo y toman control del mismo

HP verifica las políticas endurecidas respecto de muchos ataques conocidos y sigue perfeccionando sus políticas de SE de Android para brindar más protección.

Capacidad de administración

Compatibilidad de EMM con ARM TrustZone®

Garantiza la compatibilidad con soluciones EMM titulares a través de estándares y pruebas de compatibilidad

Las soluciones de administración de dispositivo móvil (MDM) permiten que las empresas protejan los dispositivos y los datos mediante el aprovisionamiento remoto de políticas de seguridad y mediante la realización de operaciones de bloqueo y eliminación de datos de forma remota en dispositivos perdidos o robados.

Mediante su compatibilidad con la administración de dispositivos estándar de Android (también llamado Administrador de política de dispositivo o DPM API), los dispositivos Android preparados para la empresa HP son compatibles con la mayoría de las soluciones MDM compatibles con Android. Además, las empresas sin una solución EMM pueden suscribirse a HP Touchpoint Manager.

La implementación del arranque seguro de Android preparado para la empresa HP utiliza 65537 claves RSA públicas de exponente de 2048 bits para certificados y firmas de imagen. El algoritmo SHA256 se usa para firmar los certificados PKI, mientras que el código en sí se firma mediante un algoritmo de propiedad exclusiva.

Capacidad de administración inmediatamente desde la caja con HP Touchpoint Manager

Brinda una solución EMM simplificada e implementable en forma instantánea para administrar equipos y dispositivos móviles

Muchas pequeñas empresas carecen de personal de TI que comprenda las sutilezas de la implementación, protección o administración adecuada de dispositivos móviles. Estas empresas necesitan una herramienta que simplifique estas tareas.

El servicio de HP Touchpoint Manager basado en la nube permite a las empresas proteger y administrar dispositivos Android preparados para la empresa HP, equipos y otros dispositivos móviles desde un panel de control único y fácil de usar. Esta solución está disponible en función de una suscripción y no requiere de infraestructura de TI adicional.

Escenario de ejemplo

El propietario de una empresa está preocupado porque los empleados no están haciendo lo suficiente para proteger los datos de la empresa.

Por medio de HP Touchpoint Manager, o una solución EMM compatible, el propietario de la empresa establece una política para solicitar una contraseña o cifrado del dispositivo. El propietario también puede aplicar normas para evitar contraseñas simples y obvias. Juntos, estos mecanismos, protegen los datos confidenciales.

Escenarios de ejemplo

Un profesional de ventas olvida su tablet en el hotel después de una escapada de fin de semana.

El centro de soporte de TI (o el usuario, mediante un portal de auto-servicio) emite un comando de bloqueo remoto con HP Touchpoint Manager u otra solución EMM compatible. Este comando bloquea la pantalla del dispositivo hasta que se recupera el dispositivo.

Un ejecutivo de la empresa pierde su tablet con información confidencial.

El centro de soporte de TI o el usuario emite un comando de eliminación remota con HP Touchpoint Manager u otra solución EMM compatible[3], y de ese modo elimina los datos del usuario almacenados en el dispositivo para ayudar a evitar la pérdida de datos confidenciales.

Características y políticas de Microsoft Exchange ActiveSync (EAS)

Habilite el acceso móvil seguro al correo de la empresa y al calendario y, al mismo tiempo, aproveche la infraestructura de TI existente y Microsoft Exchange

Los dispositivos Android preparados para la empresa HP funcionan con Microsoft Exchange Server 2003 SP2 y versiones posteriores para sincronizar el correo electrónico, los contactos y los calendarios. Este soporte está disponible a través de las aplicaciones nativas del cliente de agenda, contactos y correo que se incluyen en la versión Android KitKat.

Para brindar una mejor protección a los datos de Exchange, los dispositivos Android preparados para la empresa habilitan a los administradores de TI para que apliquen políticas EAS en forma remota, tal como el cifrado y políticas de contraseña. Entre las políticas compatibles se incluyen:

- Solicitar un PIN o una contraseña para proteger los dispositivos del personal no autorizado
- Requerir una complejidad mínima para la contraseña (largo, alfabética o caracteres alfanuméricos, caracteres especiales, etc.)
- Controlar el tiempo de bloqueo de la pantalla
- Solicitar el cifrado del dispositivo
- Desactivar la cámara

Todas están disponibles a través de las capacidades nativas de administración del dispositivo admitidas en la versión KitKat. Las características y las políticas compatibles varían en función de la versión de servidor Microsoft Exchange. Consulte el “Apéndice A: Características y políticas de Microsoft Exchange”.

La administración remota y la aplicación de las políticas de EAS requieren una solución EMM o MDM compatible.

Características antirrobo

Permita a las empresas desalentar el robo del dispositivo y proteger los datos

Las tablets y smartphones son vulnerables a robos y pérdidas. Para ocuparse de este problema, los dispositivos Android preparados para la empresa HP admiten las siguientes características:

- Hacer sonar una alarma
- Bloquear el dispositivo
- Eliminación remota
- Enviar un mensaje

Estas características requieren de HP Touchpoint Manager o una solución EMM o MDM de terceros compatible[3] desde donde se emitan los comandos antirrobo.

[3] Solución EMM o MDM de terceros vendida por separado

Escenario de ejemplo

Un empleado desprevenido descarga malware que se presenta como una aplicación legítima.

El agente antivirus instalado previamente en el dispositivo Android preparado para la empresa HP escanea la aplicación antes de la instalación y advierte al usuario que es malware.

Protección antivirus

Para ayudar a evitar que los usuarios instalen aplicaciones con malware, los dispositivos Android preparados para la empresa HP, incluyen una aplicación antivirus líder del mercado cargada previamente que ofrece protección esencial contra malware sospechado. Para una protección mejorada, los clientes pueden actualizarla a una versión superior.

Escenario de ejemplo

Los hackers lanzan una vulnerabilidad nueva, similar al virus OpenSSL muy promocionado "Heartbleed", para robar información confidencial de los dispositivos afectados.

Los dispositivos Android preparados para la empresa HP reciben parches inmediatos por aire, lo que reduce la ventana de oportunidad para ataques potenciales y minimiza el daño.

Parches de seguridad a través de entrega de firmware por aire

Cuando se descubren nuevas vulnerabilidades, se deben aplicar los parches a todos los sistemas afectados en forma inmediata. Un sistema sin parches es un objetivo fácil y atractivo para los hackers.

Los dispositivos Android preparados para la empresa HP están protegidos mediante la entrega por aire inmediata de parches de firmware para las vulnerabilidades críticas durante un plazo de dos años. HP tiene en cuenta la severidad de una vulnerabilidad y, de ese modo, permite respuestas rápidas a situaciones críticas.

HP funciona con Google™ y con los proveedores de SoC para establecer prioridades, desarrollar e implementar parches. Los dispositivos están configurados para verificar al servidor de aire a intervalos regulares. El servidor verifica la existencia de actualizaciones disponibles, según el modelo de dispositivo y la versión de firmware, y las descarga al dispositivo. Para evitar la interrupción de las actividades del usuario o provocar otros inconvenientes, el servidor aplica las actualizaciones solo después de obtener el consentimiento del usuario. En congruencia con las mejores prácticas de seguridad para proteger a los usuarios de ataques que se aprovechan de las vulnerabilidades conocidas, los dispositivos no admiten la regresión a versiones anteriores.

Además de los parches de seguridad, los dispositivos Android preparados para la empresa HP también admiten las actualizaciones por aire para el firmware del dispositivo, lo que permite al dispositivo mantenerse al día respecto de las características y las versiones nuevas que se introducen como parte del plan de acción de Android.

Conclusión

La seguridad mejorada, las capacidades de administración y de soporte de los dispositivos Android preparados para la empresa HP están diseñadas para resolver desafíos clave que el personal de TI enfrenta al implementar dispositivos Android en un entorno comercial.

HP brinda un cimiento de hardware y firmware de confianza sólido junto con un endurecimiento adicional de la seguridad mediante políticas de SE de Android que se someten un proceso de perfeccionamiento frecuente para salvaguardar los dispositivos de las amenazas en evolución. Este enfoque integral de la seguridad se extiende desde el diseño del producto y la fabricación, hasta la actualización de dispositivos en el campo.

Además, HP asume una visión de no fragmentación que permite a los administradores de TI administrar los dispositivos Android preparados para la empresa HP y dispositivos Android existentes de la misma manera, y usar las soluciones EMM existentes.

Obtenga más información acerca de dispositivos Android preparados para la empresa HP en hp.com/go/android-tablets.

Apéndice A: Características y políticas de Microsoft Exchange

En esta sección se detallan las características y las políticas admitidas por dispositivos Android preparados para la empresa al trabajar con varias versiones de Exchange. Tenga en cuenta que las características y las políticas mencionadas para cada versión se suman a las versiones anteriores.

Exchange ActiveSync 2.5 - Exchange Server 2003 SP2

Características

- Ejecución directa
- Sincronización con correo electrónico
- Sincronización con calendario
- Sincronización con contactos
- Eliminación remota
- Sincronización de carpetas múltiples
- Búsqueda en GAL
- Transmisión cifrada SSL

Exchange ActiveSync 12.0 - Exchange Server 2007

Características

- Eliminación remota iniciada por el usuario (del lado del servidor)
- Correo electrónico HTML
- Búsqueda de servidor
- Etiquetas de seguimiento
- Descubrimiento automático
- Reducción de ancho de banda

Políticas

- Permitir la descarga de los adjuntos (del lado del cliente)
- Tamaño máximo de los adjuntos
- Permitir una contraseña simple
- Vencimiento de la contraseña (días)
- Aplicar historial de contraseña

Exchange ActiveSync 12.1 - Exchange Server 2007 SP1

Características

- Sin características adicionales

Políticas

- Desactivar la cámara
- Cifrado del dispositivo
- Cantidad mínima de caracteres complejos para contraseñas
- Incluir elementos de correos electrónicos anteriores (días)
- Incluir elementos de calendario anteriores (días)
- Solicitar sincronización manual mientras se realiza el enrutamiento

Exchange ActiveSync 14.0 - Exchange Server 2010

Características

- Estado de respuesta

Políticas

- Sin políticas adicionales

Exchange ActiveSync 14.1 - Exchange Server 2010 SP1

Características

- Sin características adicionales

Políticas

- Solicitar contraseña
- Solicitar contraseña alfanumérica
- Solicitar cifrado en el dispositivo
- Permitir una contraseña simple
- Cantidad de intentos fallidos permitidos (ante de eliminar el dispositivo)
- Largo mínimo de la contraseña
- Tiempo sin ingreso del usuario antes de tener que volver a ingresar la contraseña (tiempo fuera por inactividad después del cual la pantalla se bloquea)

Suscríbase para recibir actualizaciones
hp.com/go/getupdated

Compartir con colegas

Calificar este documento

4AA5-8533SPL, Mayo de 2015