Revista Digital Universitaria
1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-6079

ARTÍCULO

DESARROLLO DE UNA PLATAFORMA DE SEGURIDAD EN DISPOSITIVOS MÓVILES DE COMUNICACIÓN, ¿NECESIDAD O PARANOIA?

Javier Silva Pérez y Guillermo Morales Luna

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de
Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

Desarrollo de una plataforma de seguridad en dispositivos móviles de comunicación, ¿necesidad o paranoia?

Resumen

La creación de sistemas de cómputo en ambientes móviles va de la mano con el uso de medios inalámbricos para transmitir la información necesaria. Dichos medios son ampliamente vulnerables a diversos ataques informáticos que atentan (entre otros) contra la confidencialidad, la integridad y la autenticación tanto de los datos como de los participantes en la comunicación. Debido a esto, es necesario crear mecanismos que permitan una comunicación segura. Uno de los mecanismos mas ampliamente utilizados para ofrecer este servicio es sin duda la criptografía, la cual permite el desarrollo de diversos bloques de seguridad dependiendo de las necesidades del sistema, específicamente la infraestructura de clave pública (PKI, del inglés Public Key Infrastructure) ofrece servicios como integridad y autenticación. En este trabajo se realiza un análisis de la importancia del desarrollo de una PKI tomando en cuenta un ambiente de dispositivos móviles, considerando ventajas y desventajas. En el análisis se hace una comparación entre los diferentes desarrollos existentes en la actualidad para la plataforma de desarrollo Android la cual ha ido ganando una enorme popularidad en los últimos años.

Palabras claves: PKI, Android, Dispositivos móviles, Seguridad, Criptografía

Development of a security platform for communicating mobile devices, necessity or paranoia?

Abstract

The creation of computer systems in mobile environments is closely related to wireless technologies for information transmission. However, the technologies are vulnerable to several attacks threatening confidentiality, integrity and authentication of both data and participants. Thus, the creation of mechanisms for secure communication is capital. Cryptographic methods provide mechanisms for this service allowing several security measures; in fact, public key infrastructure (PKI) offers services such as integrity and authentication. This paper analyzes the development of PKI environment into the context of mobile devices. The analysis compares several applications for the Android platform which has gained enormous popularity in recent years.

Keywords: PKI, Android, Mobile Devices, Security, Cryptography

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

Introducción

Por siglos, reyes, reinas, jefes de estado y generales militares han confiado en comunicaciones eficientes para gobernar sus territorios y comandar sus ejércitos. Al mismo tiempo todos ellos han estado conscientes de las consecuencias que se pueden generar si los mensajes caen en manos hostiles, revelando así secretos importantes a rivales. Esto fue lo que motivó en un inicio el desarrollo de diversos códigos y cifradores, los cuales son técnicas para disfrazar los mensajes de tal manera que la única persona capaz de leerlos sea la persona a la cual se enviaron dichos mensajes. El deseo de secrecía ha hecho que las naciones creen departamentos desarrolladores de códigos y cifrados, los cuales son los responsables de garantizar la seguridad de las comunicaciones. Al mismo tiempo se han ido generando diversos ataques para quebrantar estos códigos y revelar los secretos. La historia de códigos y cifradores es la historia de la batalla antagónica entre criptógrafos y criptoanalistas, la cual ha tenido un impacto dramático en el cuso de la historia (Singh, 2001). A grandes rasgos, codificar es colocar un mensaje en un alfabeto apropiado para garantizar su transmisión fiel, en tanto que cifrar es transformar un mensaje en otro de manera que el mensaje original no sea recuperable del cifrado a menos de contar con una clave para hacerlo.

A medida que la información se convierte en un producto cada día más valioso, las técnicas de comunicación y tecnologías de la información van cambiando a la sociedad hasta convertirse en una parte fundamental de la misma, por lo que es de vital importancia crear conciencia de que a pesar de todos los beneficios que estas tecnologías nos ofrecen, también hay riesgos al transmitir cualquier información a través de medios no seguros como lo son, ya en nuestros tiempos, internet o las redes inalámbricas. Es por esto que el proceso de convertir mensajes, conocido como cifrado, jugará un papel cada día más fundamental en la vida diaria, ayudando a garantizar la integridad de los datos, la autenticidad tanto del mensaje como de las partes que participan en la comunicación y la confidencialidad de la información que se transmite dentro de una red.

Por otro lado, la necesidad de acceder a dicha información a cualquier hora y en cualquier lugar ha sido el principal impulsor del crecimiento de diversas tecnologías entre las cuales destacan los dispositivos móviles. El cómputo móvil aparece con el objetivo de proveer ambientes de cómputo ubicuos para usuarios móviles (B'Far, 2005). Hoy en día, las empresas buscan que sus empleados y usuarios tengan acceso a la información que requieren de forma rápida y sin importar el lugar en el que se encuentren. Es aquí donde los dispositivos móviles han jugado un papel fundamental en las actividades cotidianas de todas las personas, el cual se ha ido incrementando rápidamente en los últimos años sustituyendo en gran medida a las computadoras personales (Llamas, 2011),

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de
Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

esto debido a que es práctico, a su gran capacidad de movilidad y a que facilita el acceso a fuentes de información mediante redes de comunicación inalámbrica. Sin embargo, lo anterior supone un gran riesgo en cuanto a seguridad se refiere. Naturalmente la disponibilidad de recursos de comunicación plantea importantes problemas, algunos relevantes a los aspectos físicos de la seguridad, pero aquí nos ocuparemos de la seguridad en cuanto a preservar la privacidad de los corresponsales (confidencialidad), a evitar que las comunicaciones sea alterada (integridad) y a garantizar que no haya suplantación de corresponsales (autenticación).

Los ambientes de cómputo móvil se caracterizan por tener restricciones importantes de recursos y cambios frecuentes en las condiciones de operación (B'Far, 2005). Por otra parte, la rápida evolución, tanto de las capacidades de cómputo como de los sistemas operativos que hoy en día se pueden encontrar en los dispositivos, propicia la creación de todo tipo de sistemas, pensados y diseñados específicamente para funcionar en un dispositivo móvil, planteando a los diseñadores y desarrolladores retos adicionales para garantizar servicios efectivos y eficientes de comunicación, disponibilidad y seguridad.

La conectividad de los dispositivos móviles ha generado un crecimiento exponencial en el tráfico de todo tipo de contenido digital a través de redes inalámbricas inseguras, por lo que la protección, autenticación e integridad de esos datos debe ser considerada una prioridad fundamental en el diseño de cualquier sistema informático. El problema se acrecienta en aplicaciones empresariales donde la información que viaja por tales medios inseguros puede ser sumamente delicada y con un gran valor comercial. Debido a esto, el uso de esquemas criptográficos se vuelve algo fundamental en todo sistema informático si se quiere estar protegido contra diversos ataques.

La infraestructura de clave pública, o PKI, ofrece diversos servicios de seguridad como lo son: integridad, confidencialidad, autenticación, no-repudio. Éstos pueden ser cubiertos asignándole una clave única e infalsificable a cada usuario. De esta manera los usuarios pueden firmar digitalmente la información, el receptor puede verificar dicha firma y comprobar su validez. Adicionalmente una PKI puede ofrecer servicios de cifrado para asegurar la confidencialidad de la información, de manera que únicamente el destinatario original de un mensaje pueda descifrarlo (Kuhn-PKIIntro, 2001), (Schmeh, 2003).

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

Los cuatro servicios básicos de seguridad que toda PKI debe ofrecer (Kuhn-PKIIntro, 2001), (Schmeh, 2003) son:

• Integridad: este servicio está dirigido a evitar la modificación no autorizada o accidental de la información. Esto incluye la inserción, la eliminación y la modificación de los datos originales. Para asegurar la integridad, el sistema debe ser capaz de detectar modificaciones no autorizadas. La meta principal es que el receptor sea capaz de verificar si acaso la información fue alterada durante la comunicación.

• Confidencialidad: este servicio restringe el acceso a la información sensible únicamente a los usuarios que estén autorizados a consultarla. Impide la revelación no autorizada de información sensible de una empresa o persona.

• Autenticación: establece la validez del mensaje y de los participantes en la comunicación. La meta es permitir a los participantes de la comunicación determinar si el origen del mensaje es válido o no.

• No-repudio: ofrece protección a un usuario o entidad frente a la posibilidad de que otro usuario niegue posteriormente que se realizó cierta transacción, por ejemplo, haber hecho un pedido a una empresa.

Una PKI se caracteriza también por sus elementos funcionales. A continuación describiremos brevemente cada uno de ellos (RFC4158, 2005), (Kuhn-PKIIntro, 2001), (RFC5280, 2008):

• Autoridad Certificadora (CA): es similar a un notario, la CA confirma la identidad de los usuarios del sistema. Los demás elementos de la infraestructura deben confiar en ésta para que la PKI funcione correctamente. Sus responsabilidades son:

• Generación de claves: una de las tareas de una CA puede ser la generación segura del par de claves que los usuarios de la PKI utilizará, o en su caso verificar que el par de claves que el usuario posea cumpla con los requerimientos básicos de seguridad (tamaño de clave, algoritmo, formato, etc.) que los servicios que la PKI requieren para un funcionamiento optimo.

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

• Emisión de Certificados Digitales: para cada identidad registrada típicamente se incluye la clave pública del usuario, la información acerca de la identidad del mismo, el tiempo operacional del certificado (vigencia) y la firma digital de la CA.

• Emisión de lista de revocación de certificados (CRL, por sus siglas en inglés Certificate Revocation List): son listas de certificados que han sido revocados, debe estar firmada por la CA. Un certificado puede ser revocado por diferentes razones, por ejemplo, la clave privada de un usuario fue comprometida, el usuario abandonó el sistema criptográfico o bien por un cambio de nombre.

• Autoridad de Registro (RA): es una entidad de confianza para la CA, la cual está a cargo del registro de las identidades de los usuarios en la CA.

• Repositorio: es una base de datos de certificados digitales expedidos por la CA. El uso principal de este repositorio es proveer datos que permitan a los usuarios confirmar el estatus de un certificado digital.

• Usuarios de la PKI: son las entidades que usan la PKI, deben confiar en los demás elementos para obtener certificados y para verificar la validez de los mismos.

Desarrollo

La siguiente generación de sistemas operativos abiertos no será para equipos de escritorio, sino, para pequeños dispositivos móviles, llevados por los usuarios en cualquier momento. La apertura de estos nuevos ambientes ha llevado a la creación de nuevas aplicaciones y mercados, adicionalmente tales ambientes han permitido una mayor integración con servicios en línea existentes. Sin embargo, a medida que la importancia de los datos comunicados y de los servicios proporcionados por los dispositivos crece, también lo hacen las vulnerabilidades (Enck, 2009). Debido a esto, es esencial contar con mecanismos que ayuden a garantizar la seguridad de los datos intercambiados en cualquier transmisión entre el dispositivo móvil y el servidor, éste es el principal tema del presente trabajo. A continuación se hará una revisión de los diferentes desarrollos existentes de PKI sobre dispositivos móviles, nos enfocaremos particularmente en las aplicaciones y los sistemas que utilizan Android debido a su gran popularidad la cual asciende a las 300,000 activaciones diarias colocándolo como el sistema operativo más popular durante el cierre del 2010 y 2011 (Llamas, 2011).

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

La criptografía de clave pública fue propuesta por Diffie y Hellman en 1976 en su célebre artículo "New Directions in Cryptography" (Hellman, 1976), en el cual se propone, para cada usuario, un par de claves (pública y privada) y su utilidad para demostrar la posesión de un secreto (clave pública) mediante alguna operación entre los datos y la clave pública. Por sí, misma la criptografía de clave pública únicamente provee una serie de operaciones matemáticas asimétricas, pero no ofrece una conexión a aplicaciones o ambientes. Para establecer esta conexión se necesitan piezas o componentes, las cuales forman la PKI, una "infraestructura" que hace que la tecnología de clave pública esté disponible a aplicaciones y ambientes que deseen utilizarla (Adams, 2004).

Desde sus inicios, han surgido diversas implementaciones de PKI's y en dichas implementaciones existen variaciones en la forma de definir cada uno de los componentes que conforman una infraestructura, principalmente por la forma de ligar la identidad del usuario de la PKI con su clave pública, ya que las partes que utilicen la criptografía de clave pública dependerán de esta liga para asociar la clave con una entidad. Diffie y Hellman propusieron un modelo en el cual las claves públicas son entregadas por un repositorio seguro, pero no fue hasta 1978 que en (Kohnfelder, 1978) la definición de certificado fue propuesta, donde la clave pública y el identificador son almacenados en una estructura de datos y firmados por la autoridad certificadora (CA).

Actualmente existen diversas propuestas e implementaciones de PKI's, las cuales han surgido para posteriormente convertirse en estándares, por lo que si se desea que una PKI sea aceptada y utilizada ampliamente es necesario que tenga compatibilidad con al menos alguna de ellas. Entre los esquemas más utilizados destacan dos:

X.509 (RFC5280, 2008)

> Es un estándar para infraestructuras de clave pública que especifica entre otras cosas, los formatos para certificados (codificados utilizando ANSI X9), los algoritmos de validación para rutas de certificación y el formato para las listas de revocación de certificados. La primera versión del estándar surgió en 1988 y se basa en una estructura estrictamente jerárquica de las autoridades de certificación. Actualmente se encuentra en su tercera versión.
>
> En la primera versión del estándar existían restricciones estructurales impuestas para asociar claramente la cadena de certificación. Ahí se requería una estructura jerárquica en donde todas las rutas de certificación iniciaban con la llamada IPRA (del inglés, Internet Policy Registration Authority), en el segundo nivel se encontraban las PCA's (del inglés, Policy Certification Authorities) y por último las CA's. La

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

tercera versión es mucho más flexible ya que se pueden utilizar extensiones de certificados, sin la necesidad de una estructura de certificación como tal, permitiendo además que un usuario pueda ser tanto una entidad como una autoridad certificadora.

Los certificados X.509 pueden tener diferentes extensiones entre las que destacan:

• .CER: Certificado codificado en CER (mnemónico por certificado), algunas veces es una secuencia de certificados.

• .DER: Certificado codificado en DER (del inglés Distinguished Encoding Rules).

• .PEM: Certificado codificado en Base64, encerrado entre -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.

• .P7C: Estructura PKCS#7, sin datos, solo certificado(s) o CRL(s).

• .P12: PKCS#12, puede contener certificado(s) (público) y claves privadas (protegido con clave)

PGP (RFC4880, 2007)

Pretty Good Privacy fue desarrollado inicialmente por Phil Zimmermann con la finalidad de proteger la información distribuida a través de Internet utilizando criptografía de clave pública. Este esquema sirvió como base para el desarrollo de OpenPGP y posteriormente GnuPG. Éste se basa en la creación de redes de confianza utilizando servidores de claves, también puede utilizar certificados X.509.

Por otra parte las implementaciones en ambientes móviles son muy limitadas, aún más si se quiere hablar de los desarrollos hechos específicamente para Android. En la industria privada existen aplicaciones que ponen a disposición de los usuarios diversas operaciones criptográficas como cifrar y descifrar ciertos tipos de información dentro del dispositivo, tales como: archivos, correos electrónicos, mensajes (Messerman, 2011), (Echoworx Corporation, 2011), (Rodriguez, 2011), (Thialfihar, 2011), (Sandbox, 2011), o bien, firmar y verificar información digital contenida en el dispositivo (Thialfihar, 2011), (Sandbox, 2011). Sin embargo, la mayoría de estas aplicaciones ofrecen únicamente funciones de criptografía simétrica, particularmente utilizando el estándar AES (del inglés Advanced Encryption Standard) como esquema de cifrado/descifrado. En el caso de las aplicaciones que utilizan esquemas de clave pública, éstas carecen de la definición de uno

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

o de varios de los componentes esenciales de una PKI o bien dan lugar a algunas vulnerabilidades en la definición de los mismos. A continuación se presenta una breve reseña de las características, ventajas y desventajas de algunas de las aplicaciones disponibles en Android Market.

DroidCrypt (Messerman, 2011)

Es una aplicación que permite cifrar y descifrar archivos dentro del dispositivo, utilizando criptografía simétrica, particularmente AES como bloque de cifrado y descifrado. Una de las innovaciones más atractivas de esta aplicación es el uso de tres tipos de contraseñas para las operaciones criptográficas: palabra clave, orientación del dispositivo y gesto táctil. Es capaz de manejar cualquier tipo de contenido digital como imágenes, música, documentos, etc.

Esta aplicación es eficiente en cuanto a recursos y cumple con el objetivo de cifrar archivos en el dispositivo, sin embargo el uso de criptografía simétrica hace que sea complicado enviar los archivos cifrados a otros usuarios (debido al manejo de claves). Adicionalmente, la aplicación no hace uso de ningún estándar, por lo que la compatibilidad con aplicaciones existentes es muy baja, con lo que el compartir archivos o claves generadas con esta aplicación es sumamente complicado. Por último, esta aplicación está disponible en dos versiones dentro del Android Market, una de prueba con funcionalidad limitada y otra con un costo para obtener la funcionalidad completa de la aplicación.

mobilEncrypt (Echoworx Corporation, 2011)

Forma parte de una plataforma de cifrado para correo electrónico creada por Echoworx, por lo que únicamente es útil si se compra toda la plataforma, ya que por sí sola esta aplicación sólo tiene la funcionalidad de enviar y recibir correos electrónicos, los cuales son cifrados y firmados. Sin embargo esta aplicación tiene algunos puntos importantes a su favor:

- Es capaz de utilizar tanto esquemas de cifrado simétrico como asimétrico, utilizando estándares como RSA-1024, RSA-2048, y AES-256 entre otros

- Tiene soporte para certificados X.509, por lo que podría interactuar con otras aplicaciones que utilicen este tipo de certificados, sin embargo en la página oficial de la aplicación no se menciona ninguna.

- La plataforma completa de Echoworx conforma una PKI ya que las aplicaciones de escritorio tienen utilidades para la administración de certificados, listas de

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

revocación de certificados, manejo de claves, validación y búsqueda de certificados, entre otras. No obstante estas opciones no están disponibles para la aplicación móvil, la cual únicamente tiene un cliente de correo electrónico seguro.

Por otro lado, al no ser una aplicación de software libre no se tiene acceso al código original de la aplicación ni al API utilizado para la implementación de estos servicios, por lo que la generación de aplicaciones empresariales particulares con estas características no seria posible.

OpenPGP Manager (Rodriguez, 2011)

Actualmente se encuentra en la versión 1.44, es una implementación de PGP para Android y es compatible con la versión de escritorio. Desde su versión inicial se ha ido agregando funcionalidad poco a poco, e incorpora entre otros servicios: la creación de claves OpenPGP (utilizando RSA, DSA o El-Gammal), importar y exportar las claves desde OpenPGP (las cuales pueden estar almacenadas en el dispositivo o en servidores de claves), adicionalmente provee un módulo de administración de claves y ofrece una variedad de algoritmos de cifrado simétrico para que el usuario elija el que desee.

Esta aplicación tiene la funcionalidad de cifrar, descifrar, firmar y verificar tanto mensajes de correo electrónico como archivos dentro del dispositivo. Una de las ventajas de esta aplicación es que después de su instalación es posible realizar cualquiera de las operaciones disponibles sin la necesidad de estar conectado a una red, ya que realiza todas las operaciones criptográficas dentro del dispositivo móvil. A pesar de que las funciones de esta aplicación son muy atractivas, su interfaz de usuario es muy sencilla y nada estilizada, lo cual puede desanimar a un usuario a explotar al máximo las capacidades de la aplicación.

Por otra parte, esta aplicación también tiene un costo por instalación en el dispositivo, además de esto, en la página del desarrollador no hay acceso al código fuente o información del API utilizado, por lo que la reutilización de esta aplicación no es posible.

Android Privacy Guard (APG) (Thialfihar, 2011)

Al igual que la aplicación anterior, ésta es una implementación del estándar PGP que permite cifrar, descifrar, firmar y verificar tanto archivos dentro del dispositivo como correos electrónicos, con la diferencia de que esta aplicación es software libre, por lo que el código fuente esta disponible para su uso y modificación. Esta aplicación utiliza el API de desarrollo SpongyCastle (Tyley, 2011) como capa criptográfica base. Es importante mencionar que esta API es una migración de la

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

implementación de Bouncy Castle (BouncyCastle, 2011), la cual es una biblioteca criptográfica ampliamente utilizada disponible para varios lenguajes de programación. APG tiene una interfaz de usuario más estilizada y útil que la aplicación anterior, por lo que permite al usuario aprovechar al máximo las capacidades del API desarrollada, adicionalmente tiene un amplio soporte de algoritmos criptográficos (asimétricos, simétricos y funciones de síntesis (hash)) y es totalmente compatible con la versión de escritorio de OpenPGP en cuanto a claves y archivos (cifrados/ firmados) se refiere.

Al igual que la aplicación anterior, ésta realiza todo el procesamiento requerido en el dispositivo, por lo que si se requiere hacer una operación sobre archivos muy grandes puede ser algo tardado pero en general tiene un desempeño muy bueno en diversos dispositivos móviles. A pesar de sus buenas cualidades, este software aún está lejos de constituir una PKI como tal, debido a que no contempla ninguna definición o implementación de una autoridad certificadora, la cual es el corazón de toda PKI.

PKI Webtop (Sandbox, 2011)

Esta aplicación fue desarrollada como parte de un proyecto financiado por el gobierno de España. Es la única disponible en Android que define un esquema completo de PKI dentro de este sistema y además que contempla el uso de un dispositivo móvil como parte del diseño. Para utilizar dicha aplicación se requiere instalarla en el dispositivo y registrarse en la página de los desarrolladores (sin costo alguno). Para hacer el registro, únicamente solicita que se ingrese un nombre de usuario y contraseña, los cuales se utilizan en el dispositivo para ingresar a la aplicación. Al finalizar el registro se genera el par de claves, las cuales se encuentran almacenadas en un solo archivo, el cual se puede descargar. Dicho archivo utiliza el estándar PKCS #12 (RSA Laboratories, 1999), en el cual se incluye tanto la clave privada como la pública, protegidas utilizando la contraseña ingresada en el registro y criptográfica simétrica.

Esta aplicación tiene su versión para equipos de escritorio y ambas versiones utilizan el enfoque de cómputo de nube, en el cual las aplicaciones se ven como terminales "tontas" y toda la información es almacenada en la nube. La versión para Android solamente permite al usuario firmar y verificar archivos digitales que se encuentren en el dispositivo sin tomar en cuenta la confidencialidad de los mismos

Una de las principales desventajas de esta aplicación es que se requiere de una conexión a internet en todo momento, ya que desde que se abre la aplicación se le solicita al usuario que se identifique en el portal de Webtop utilizando las credenciales correspondientes. Una vez dentro

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de
Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

de la aplicación se muestra una lista con las opciones disponibles. Por otra parte, esta aplicación permite registrar y contestar peticiones de firmas digitales de archivos en la nube, es decir, solicitar a otro usuario que se firme algún documento, lo cual es algo innovador y atractivo.

Adicionalmente, una de las características mas destacadas de esta PKI también se puede ver como su mayor debilidad, ya que al utilizar el enfoque de cómputo de nube, la aplicación almacena una copia de la clave privada en el servidor. Además de esto, las operaciones criptográficas no se realizan dentro del dispositivo, sino que se hacen en el servidor, por lo que al realizar cualquier operación el archivo es enviado al servidor (en claro) y al terminar se retorna la versión firmada del archivo. Otro punto en contra es que el servidor almacena una copia de los archivos firmados, por lo que es indispensable confiar ciegamente en el servidor, para que la PKI funcione correctamente.

Además de esto, en la PKI no se encuentra definida una autoridad certificadora como tal (sin embargo, la nube podría desempeñar este papel), tampoco se menciona ningún mecanismo para revocar certificados, manejar tiempo de validez de los mismos o algún tipo de liga entre el certificado y la identidad del usuario, los cuales son servicios descritos más arriba en la descripción funcional de una PKI, lo más parecido a esto es el identificador que se registró en la página.

Por último, en la página web del desarrollador no se da información acerca de los algoritmos utilizados ni si acaso se usa algún estándar aparte del PKCS #12. A pesar de que esta aplicación no tiene ningún costo, no se tiene acceso ni al código original de la aplicación ni información sobre el uso de un API basado en la implementación realizada.

Las características de las aplicaciones anteriormente mencionadas se pueden resumir en las tablas siguientes. En la Tabla 1 presentamos los servicios de seguridad contemplados en el desarrollo de estas aplicaciones, ahí observamos que algunas aplicaciones como OpenPGP Manager y APG contemplan todos los servicios de seguridad deseables.
En la Tabla 2 enlistamos las características funcionales de las aplicaciones entre las cuales destacan sus grados de compatibilidad respecto a otras aplicaciones en el mercado y la reutilizabilidad de dicha aplicación para la creación de otras.
Por último, en la Tabla 3 mostramos los elementos deseables en una PKI y cuáles de éstos están definidos en el diseño de la aplicación. En algunos casos, como en el de mobilEncrypt, estos elementos no están definidos por sí solos para la aplicación disponible para Android, sino que se encuentran definidos en la suite de Echoworx.

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

	Confidencialidad	Integridad	Autenticación	No-Repudio
X. 509	X	X	X	X
PGP	X	X	X	X
DroidCrypt	X			
mobilEncrypt	X	X	X	
OpenPGP Manager	X	X	X	X
APG	X	X	X	X
PKI Webtop		X	X	X

Tabla 1 - Servicios de seguridad contemplados

	Uso de estándares	Compatibilidad	Criptografía simétrica	Criptografía asimétrica	Versatilidad algorítmica	Reusabilidad	Costo
X. 509	Alto	Alto	X	X	Alta	Alta	Gratuita
PGP	Alto	Media	X	X	Alta	Media	Gratuita
DroidCrypt	Bajo	Ninguna	X		Baja	Nula	Disponible una versión de prueba sin costo
mobilEncrypt	Bajo	Ninguna	X		Baja	Nula	Bajo
OpenPGP Manager	Medio	Media	X	X	Alta	Nula	Medio
APG	Alto	Alta	X	X	Alta	Alta	Gratuito
PKI Webtop	Bajo	Media		X	Media	Nula	Gratuita

Tabla 2 - Características de la aplicación

	Autoridad Certificadora	Autoridad de Registro	CRL	Repositorio	Usuario de PKI
X. 509	Definida	Definida	Definida	Definido	Definido
PGP	Considerada	No definida formalmente	Considerada	Considerada	Definido
DroidCrypt	No Definida	No Definida	No Definida	No Definida	Definido
mobilEncrypt	Definida en el paquete completo	Definida en el paquete completo	Definida en el paquete completo	Definida en el paquete completo	Definido
OpenPGP Manager	Considerada	No definida formalmente	Considerada	Considerada	Definido
APG	Considerada	No Definida	No Definida	No Definida	Definido
PKI Webtop	No definida formalmente	Definida	Definida		Definido

Tabla 3 - Elementos de una PKI considerados

Conclusiones

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

1 de agosto 2012 • Volumen 13 Número 8 • ISSN: 1067-60710

Como se ha mencionado a lo largo de este trabajo, la seguridad juega un papel fundamental en todo sistema de cómputo actual, ya que mientras se manejen datos, éstos pueden ser valiosos para diversas entidades y por lo tanto atacados si no se protegen de manera adecuada. En la actualidad las compañías lideres en la creación de aplicaciones dedicadas a proteger a los equipos de accesos no autorizados, como lo son los antivirus, han creado versiones de éstas aplicaciones para Android, entre las cuales destacan AVG, Avast, McAfee y Kaspersky Lab, entre otras. Las cuales ayudan a proteger a los dispositivos contra malwares y los diferentes virus que se encuentran en cualquier red informática, sin embargo, éstas aplicaciones no pueden proveer ninguno de los servicios de seguridad mencionados en este articulo, por lo que uno de los mecanismos mas utilizados en la actualidad para proteger la información que viaja por la red es la criptografía de llave pública. En particular, una PKI ofrece diversos servicios para proteger la información contra diversos ataques. De ahí la importancia de diseñar y desarrollar una PKI en dispositivos móviles que cumplan con los requerimientos, ya que, actualmente los desarrollos existentes para la plataforma Android tienen algunas ventajas, sin embargo ninguno posee todas las características deseables en una PKI. Pero la pregunta fundamental es si desarrollar una PKI para dispositivos móviles, ¿es una necesidad o es simplemente paranoia de los usuarios? Naturalmente, nosotros nos inclinamos por lo primero.

Referencias

Adams, Carlisle, Just, Mike. “PKI: Ten Years Later” en 3rd Annual PKI R&D Workshop, 2004

B’Far, Reza. Mobile computing principles, Cambridge University Press, 2005

Diffie, W., Hellman, M. “New Directions in Cryptography”, IEEE Transactions on Information Theory, 22 (1976): 644.

Echoworx Corporation. “mobilEncrypt Cloud“ [en linea]. 2011. <http://www.echoworx.com/mobile/> [Consulta: 30 Diciembre 2011]

Enck, William, Ongtang, Machigar, McDaniel, Patrick. “Understanding Android Security”, IEEE Security & Privacy Magazine, 7 (2009):50-57.

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, Mayo 2008

Internet X.509 Public Key Infrastructure: Certification Path Building, RFC 4158, Septiembre 2005

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.

Kohnfelder, L. "Towards a Practical Public-key Cryptosystem", MIT Thesis, Mayo 1978.

Kuhn, D. Richard, Hu, Vincent C., Polk, W. Timothy, Chang, Shu-Jen. "Introduction to Public Key Technology and the Federal PKI Infrastructure", NIST, Febrero 2001

Llamas Ramos, T. et al. "Worldwide Smartphone 2011–2015 Forecast and Analysis", IDC Analyze the Future, FRAMINGHAM, Mass. Marzo 29, 2011

Messerman, Arik, Mustafic, Tarik. "Droid Crypt" [en línea]. Septiembre 19, 2011. <https://market.android.com/details?id=de.atm.android.security.encryption.full> [Consulta: 30 Diciembre 2011]

OpenPGP Message Format, RFC 4880, Noviembre 2007

Rodriguez, R. "OpenPGP Manager" [en línea]. 2011. <https://market.android.com/details?id=com.harpago.pgpmanager> [Consulta: 30 Diciembre 2011]

RSA Laboratories, "PKCS 12 v1.0: Personal Information Exchange Syntax" [en línea], RSA Laboratories , Enero 1999. <http://www.rsa.com/rsalabs/node.asp?id=2138> [Consulta: 23 Diciembre 2011]

SAFELAYER SANDBOX. "PKI Webtop for Android" [en línea]. 2011. <http://sandbox.safelayer.com/en/experimental-applications/1-semantic-web-trust-portal/485-pki-webtop-for-android> [Consulta: 10 Diciembre 2011]

Schmeh, K. Cryptography and Public Key Infraestruture on the Internet, John Viley & Sons, 2003.

Singh, Simon. The Code Book: How To Make It, Break It, Hack It, Crack It, Delacorte Press 2001

The Legion of the Bouncy Castle. "Bouncy Castle Java cryptography APIs" [en línea]. 2011. <http://www.bouncycastle.org/> [Consulta: 11 Enero 2012]

Thialfihar. "Android Privacy Guard (APG)" [en línea]. 2011. <https://market.android.com/details?id=org.thialfihar.android.apg> [Consulta: 15 Diciembre 2011]

Tyley, Roberto. "Spongy Castle" [en línea]]. 2011. <https://github.com/rtyley/spongycastle> [Consulta: 12 Enero 2012]

© Coordinación de Acervos Digitales. Dirección General de Cómputo y de Tecnologías de Información y Comunicación -UNAM
Se autoriza la reproducción total o parcial de este artículo, siempre y cuando se cite la fuente completa y su dirección electrónica.