(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 277**

(21) Número de solicitud: 201131600

(51) Int. CI.:

G06Q 30/00 (2012.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

04.10.2011

(43) Fecha de publicación de la solicitud:

18.04.2013

(71) Solicitantes:

TELEFÓNICA, S.A. (100.0%)
C/ GRAN VÍA, 28
28013 MADRID ES

(72) Inventor/es:

AMAYA CALVO, Antonio Manuel;
DÍAZ FERNÁNDEZ, Enrique y
BECERRA GONZÁLEZ, Alejandro

(74) Agente/Representante:

ARIZTI ACHA, Monica

(54) Título: **MÉTODO PARA DETECTAR Y CONTROLAR EL USO DE SERVICIOS DE PAGO SALIENTES NO DESEADOS EN DISPOSITIVOS DE COMUNICACIÓN INTELIGENTES**

(57) Resumen:

Un método para detectar y controlar el uso de servicios de pago salientes no deseados en dispositivos de comunicación inteligentes.

En el método de la invención se solicita un servicio de pago saliente mediante una aplicación que se ejecuta en un dispositivo de comunicación inteligente y comprende el desarrollo de un software específico que reside en dicho dispositivo de comunicación inteligente y la red móvil para controlar y detectar si dicho servicio de pago saliente tiene la autorización correspondiente y puede ejecutarse o si es parte de un fraude.

ES 2 401 277 A2

DESCRIPCIÓN

Método para detectar y controlar el uso de servicios de pago salientes no deseados en dispositivos de comunicación inteligentes

Campo de la técnica

La presente invención se refiere, en general, a un método para detectar y controlar el uso de servicios de pago salientes no deseados en dispositivos de comunicación inteligentes, en el que se solicita un servicio de pago saliente mediante una aplicación que se ejecuta en un dispositivo de comunicación inteligente, y más particularmente a un método que comprende el desarrollo de software específico que reside en dicho dispositivo de comunicación inteligente y en la red móvil para controlar y detectar si dicho servicio de pago saliente tiene la autorización correspondiente y puede ejecutarse o si es parte de un fraude.

Estado de la técnica anterior

Hace algunos años el acceso telefónico era la manera habitual de que los usuarios residenciales se conectaran a Internet. En aquellos tiempos, para que un ordenador se conectara a Internet tenía que tener un módem, y marcar un número telefónico especial, proporcionado por el ISP del usuario. Habitualmente el ISP realizaba con la conexión algún tipo de autenticación y autorización del usuario, para garantizar que sólo los usuarios que pagan podían acceder a la red.

En aquellos tiempos nació una nueva amenaza para el ordenador. Denominado genéricamente “marcador”, era un tipo de programa que ofrecía acceso gratuito por marcación telefónica a Internet. O incluso a algunas páginas particulares en Internet (generalmente de pornografía) que sólo estaban disponibles si se realizaba el acceso por el programa marcador especial. Y de hecho el acceso a la red era gratuito. No se requería autenticación ni autorización, ni suscripción alguna a un ISP.

Lo que no era gratuito era el número de teléfono que marcaba el programa marcador. Por tanto los programas marcadores eran una especie de estafa: el acceso a la red era gratuito, pero la llamada telefónica, en lugar de ser un número local (o incluso una tarifa plana) como los que proporcionan generalmente ISP legales, eran números especiales, con un precio alto por minuto.

Esa amenaza desapareció al mismo tiempo que el acceso de banda ancha (xDSL, cable, etc.) pasó a ser la corriente dominante para los usuarios residenciales y el acceso telefónico se convirtió en una manera marginal de acceder a la red. Con este cambio, fue cada vez menos común que los ordenadores tuvieran cualquier tipo de módem telefónico, y por tanto el negocio ilegal se esfumó.

Pero los tiempos están cambiando de nuevo. Mientras que la plataforma informática dominante hasta ahora ha sido algún tipo de ordenador personal, en la actualidad hay un aumento de teléfonos inteligentes como plataforma informática. BusinessInsider [1] predice que en 2011 habrá alrededor de 400 millones de teléfonos inteligentes en el mundo, el mismo número que de ordenadores personales.

Los teléfonos inteligentes tienen algunas similitudes y diferencias con los ordenadores personales tradicionales.

Los ordenadores personales son generalmente plataformas abiertas. No hay restricción impuesta por el hardware o el sistema operativo en cuanto a qué aplicaciones o tipos de aplicaciones pueden instalarse. Además, las aplicaciones habitualmente funcionan de una manera todo o nada: o bien no pueden ejecutarse en absoluto o bien se ejecutan con los mismos permisos que tiene el usuario que los ejecuta.

Por otro lado, los teléfonos inteligentes son plataformas cerradas. Habitualmente el fabricante de dispositivos, el creador de OS, o ambos, imponen restricciones en cuanto a qué aplicaciones o tipo de aplicaciones pueden instalarse. Además, la mayoría de las aplicaciones de los dispositivos se ejecuta en algún tipo de entorno de aislamiento de procesos (en inglés, *sandbox*), en el que la interacción de la aplicación con el dispositivo físico está restringida y controlada.

La siguiente tabla resume las restricciones impuestas a las aplicaciones por el OS del teléfono inteligente principal.

Sistema	Aislamiento de procesos	Aplicaciones aisladas	Permiso	Modelo de distribución	Acceso a información personal	Segundo plano
iPhone	Sí, forzado por API	Sí	Global	Centralizado	Sí, global	No (sí en 4º)
Symbian	¿Sí?	¿Sí?	Por aplicación. Concedido por el usuario o por el fabricante del dispositivo.	Distribuido	Sí, concedido por aplicación	Sí
Android	Sí, forzado por API y OS	Sí	Por aplicación. Concedido en el momento de la instalación.	Centralizado, pero con una opción distribuida	Sí, concedido por aplicación	Sí
Windows Mobile (6.x)	No	No	Global	Centralizado, pero con una opción distribuida	Sí, global	Sí
Windows Phone 7	Aún no se sabe	Aún no se sabe	Por aplicación. Está previsto que se conceda en el momento de la instalación y en el tiempo de ejecución	Aún no se sabe	Sí. Probablemente por aplicación (aún no se ha definido)	¿Sí?

Y, naturalmente, una gran diferencia entre un ordenador personal tradicional y un teléfono inteligente es que un teléfono inteligente es, en primer lugar y sobre todo, un teléfono. Y como tal, tiene, obviamente, la posibilidad de realizar llamadas telefónicas, del mismo modo que puede hacerlo un ordenador personal tradicional que tiene un módem y se conecta a una línea terrestre.

Asimismo, de la misma manera que surgieron los marcadores cuando los ordenadores personales solían tener módems conectados a líneas terrestres, está surgiendo una nueva generación de marcadores diseñados para funcionar en teléfonos inteligentes. Y justo como la última vez, cuando los marcadores habitualmente dependían de usuarios impostores para su instalación y ejecución, ahora los marcadores también dependen del engaño para instalarse y evitar protecciones de OS.

Así, por ejemplo, se detectó un marcador no hace mucho tiempo [2] para el OS de Android. Android, tal como puede observarse en la tabla resumen, tiene protecciones de OS bastante fuertes. De hecho, según los desarrolladores de Android:

"La seguridad y privacidad de los datos de nuestros usuarios es de vital importancia para el proyecto de fuente abierta de Android. Nos dedicamos a construir y mantener una de las plataformas para móviles más seguras disponibles mientras aún cumplimos nuestra meta de abrir el espacio de los dispositivos móviles a la innovación y la competencia.

La plataforma de Android proporciona un buen modelo de seguridad que permite a los desarrolladores solicitar las capacidades, o el acceso, que necesita su aplicación y definir nuevas capacidades que otras aplicaciones puedan requerir. El usuario de Android puede elegir entre conceder o denegar la solicitud de una aplicación de determinadas capacidades en el aparato de teléfono".

Pero incluso con las restricciones y protecciones, el programa pudo enviar SMS especiales, tan sólo engañando a los usuarios para que proporcionaran los permisos adecuados para la aplicación. Asimismo, de nuevo según los desarrolladores de OS, ésta es la funcionalidad prevista del modelo de protección:

"Nuestro modelo de permisos para aplicaciones protege frente a este tipo de amenaza. Cuando se instala una aplicación, lo usuarios ven una pantalla que explica claramente a qué información y recursos de sistema la aplicación tiene permiso para acceder, tales como un número de teléfono del usuario o enviar un SMS. Los usuarios deben aprobar explícitamente este acceso para continuar con la instalación, y pueden desinstalar aplicaciones en cualquier momento. Constantemente aconsejamos a los usuarios que instalen sólo aplicaciones en las que confíen. En particular, los usuarios deben tener cuidado cuando instalan aplicaciones fuera de Android Market".

Y ahora el problema no va a desaparecer simplemente. Puesto que uno de los motivos del éxito de los teléfonos inteligentes es, precisamente, que son teléfonos, no es razonable asumir que perderán la parte de "teléfono" igual que los ordenadores personales tradicionales perdieron sus módems una vez que la banda ancha sustituyó a la marcación conmutada.

Problemas con las soluciones existentes

Otra diferencia que los teléfonos inteligentes tienen con los ordenadores personales tradicionales es que mientras que en los ordenadores hay una industria muy fuerte que sólo construye herramientas para luchar contra cualquier tipo de *malware*, en la actualidad no hay casi ninguna herramienta de protección contra *malware* para teléfonos inteligentes. En algunos teléfonos inteligentes es incluso por diseño. Por tanto, no hace mucho tiempo, cuando se detectaron los primeros gusanos para iPhone, también se informó de que la arquitectura de iPhone era "menos que óptima" para la implementación de cualquier tipo de software antivirus [3].

Para poder implementar con éxito algún tipo de software antivirus en un teléfono inteligente, el OS debería permitir:

- Aplicaciones en segundo plano para ejecutar y consumir ciclos de CPU.

- Interacción entre aplicaciones. Las aplicaciones antivirus deben poder analizar qué están haciendo otras aplicaciones mientras lo hacen.

Algunos OS de teléfonos inteligentes no permiten el primer punto, irónicamente por "motivos de seguridad". Y prácticamente todos prohíben el segundo punto, también debido a motivos de seguridad.

Y por último pero no menos importante, los teléfonos inteligentes tienen otra diferencia con los ordenadores tradicionales: están diseñados para funcionar habitualmente con potencia de batería. Y el tiempo de vida de su batería depende de cómo de ocupada esté la CPU. Así los enfoques antivirus tradicionales, en los que el antivirus se ejecuta y monitoriza constantemente el sistema, perjudicarían enormemente el tiempo de vida de batería.

Descripción de la invención

Es necesario ofrecer una alternativa al estado de la técnica que cubra las lagunas encontradas en la misma, particularmente relacionadas con la falta de propuestas que realmente permitan disminuir o incluso eliminar el fraude generado por aplicaciones de terceras partes que hacen uso de las características de teléfono (servicios de pago) de un teléfono inteligente.

Para ello, la presente invención proporciona un método para detectar y controlar servicios de pago salientes no deseados en dispositivos de comunicación inteligentes, en el que se solicita un servicio de pago saliente mediante una aplicación que se ejecuta en un dispositivo de comunicación inteligente.

A diferencia de las propuestas conocidas, el método de la invención, de una manera característica comprende

- asociar de una manera no falsificable, un desarrollador de aplicaciones, un primer número identificador a dicha aplicación;

- instalar dicha aplicación en dicho dispositivo de comunicación inteligente;

- detectar, dicho dispositivo de comunicación inteligente, que dicha aplicación está solicitando acceder a un servicio de pago saliente;

- generar, dicho dispositivo de comunicación inteligente, un segundo número identificador a partir de parámetros obtenidos desde dicha aplicación;

- comparar, dicho dispositivo de comunicación inteligente, dichos números identificadores primero y segundo y, dependiendo del resultado de dicha comparación:

- permitir, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente generando una señal saliente que incluye dicho primer número identificador y enviando dicha señal saliente a una red, o

- rechazar, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente.

- detectar, dicha red, la existencia de dicho primer número identificador en la solicitud de acceso desde el dispositivo de comunicación inteligente; y

- decidir, dicha red, permitir o rechazar la conexión basándose en las preferencias expresadas anteriormente de un usuario de dispositivo de comunicación inteligente o de dicha red.

Otras realizaciones del método del primer aspecto de la invención se describen según las reivindicaciones 3 a 21 adjuntas, y en una sección posterior relativa a la descripción detallada de varias realizaciones.

Descripción detallada de varias realizaciones

La invención propuesta se basa en el desarrollo de hardware y software específicos que residen en los terminales de usuario finales (teléfonos inteligentes) y la red móvil para permitir la detección y control de servicios de pago salientes no deseados (llamadas telefónicas y SMS).

El control se implementa basándose en los siguientes puntos amplios:

- Las aplicaciones que solicitan acceso a los servicios de pago de teléfono (llamadas, SMS, etc.) tendrán que estar firmadas. Obsérvese que en realidad esto es un requisito actual en la mayoría de los sistemas operativos para móviles más modernos, y por tanto la firma de aplicaciones, aunque sea un requisito previo para la invención, no forma parte de ésta.

- Los desarrolladores de aplicaciones que quieran acceder a los servicios de pago de teléfono (llamadas, SMS, etc.) tienen que solicitar un número identificador (IMAI de ahora en adelante) para sus aplicaciones.

- Los números IMAI se incluirán en el ejecutable de la aplicación. El ejecutable de la aplicación debe estar firmado con el certificado de desarrollador. Obsérvese que este requisito de firma existe en realidad en prácticamente todos los OS de teléfonos inteligentes.

- El OS del teléfono inteligente aplicará restricciones de acceso, como es habitual, pero sólo podrá concederse a las aplicaciones que tengan un IMAI acceso a la red móvil. Para cada llamada, mensaje o cualquier otro tipo de servicio de pago saliente, el IMAI de la aplicación de origen debe incluirse en la información de llamada que se pasa a la red.

- La red mantendrá una lista de IMAI aprobados por abonado o por red. Podrán aplicarse restricciones adicionales (tal como una lista de llamadas de número aprobado) a algunos IMAI.

El sistema propuesto tiene los siguientes módulos:

En el entorno de desarrollo de aplicaciones:

- Generador de IMAI.

En el teléfono inteligente, ejecutado como parte del sistema operativo del teléfono móvil:

- Ejecutor de políticas locales (LPE).

- Módulo de realimentación.

En la red celular del operador móvil

- Ejecutor de políticas de red (NPE).

- Configurador de políticas de red (NPC)

Generador de IMAI

La función de este módulo es generar números IMAI, cuando un desarrollador los solicite. El proceso de desarrollo para cualquier aplicación es tal como sigue:

- La aplicación se desarrolla siguiendo los métodos actuales.

- Una vez que la aplicación se ha desarrollado, el desarrollador de aplicaciones usa un módulo de generador de IMAI para generar un número válido.

- El número IMAI generado se asocia a la aplicación. La manera en que se asocia este número a la aplicación depende del sistema operativo real en el que vaya a ejecutarse la aplicación. Algunos métodos válidos son:

Si el sistema operativo permite el uso de metadatos de aplicación (tal como nombre de aplicación, versión, etc.) entonces se incluirá el número IMAI como metadatos.

Si el sistema operativo permite el uso de datos adicionales (datos no ejecutables) entonces se incluirá el número IMAI como datos adicionales.

Si el sistema operativo permite (o exige) el uso de archivos de manifiesto, entonces se incluirá el número IMAI como parte del archivo de manifiesto.

La aplicación, incluyendo el número IMAI, se firmará usando métodos de firmado actuales y un certificado de desarrollador. Los certificados de desarrollador los generará el fabricante del sistema operativo, como en la actualidad.

Un número IMAI es un valor de 8 bytes. Como una entrada para generar un número IMAI válido, el generador de IMAI requiere el nombre distinguido (DN) del certificado del desarrollador y el nombre distinguido de la autoridad de certificación que firma el certificado de desarrollador (o alternativamente, puesto que pueden obtenerse ambos datos directamente del certificado de firma del desarrollador, puede recibir el certificado de firma como entrada). El proceso que usa el generador de IMAI para generar un número IMAI válido es tal como sigue:

1. Genera un número aleatorio de 4 bytes. Este número se denomina RN1.

2. Calcula el DN-RN1 adjuntando el RN1 al nombre distinguido (DN) del desarrollador y al nombre distinguido (DN) de la autoridad de certificación tal como se incluye en el certificado de firma del desarrollador.

3. Usando una función unidireccional, tal como SHA-1 o una función similar (se denomina H() a esta función unidireccional genérica), genera H(DN-RN1).

4. Trunca H(DN-RN1) a los primeros 4 bytes (de valor superior). El valor así generado será los 4 bytes de valor superior del número IMAI.

5. RN1 será los 4 bytes de valor más bajo del número IMAI.

Ejecutor de políticas locales

Este módulo formará parte del sistema operativo (OS) de los teléfonos inteligentes. Tiene la siguiente función:

Cuando una aplicación solicita acceso a un servicio de red de pago (llamadas, SMS, etc.), verificar que la aplicación tiene un IMAI asociado. Si la aplicación no tiene un número IMAI, se deniega la solicitud. Por el contrario, si la aplicación tiene un número IMAI, el LPE debe verificar si es un número IMAI válido. Para comprobar si un IMAI es válido, debe ejecutarse todo el siguiente procedimiento:

a. Verificar que la aplicación está correctamente firmada. Si no está firmada, denegar la solicitud.

b. Calcular el DN-RN2 adjuntando el nombre distinguido (DN) del sujeto y el nombre distinguido del firmante del certificado de firma de aplicación con los 4 bytes más bajos del número IMAI incluido en la aplicación.

c. Verificar que la siguiente condición sea verdadera: H(DN-RN2)= los 4 bytes más altos del número IMAI de la aplicación. Si la condición no es verdadera, denegar la solicitud.

Si el número IMAI es válido (tal como se haya comprobado mediante el procedimiento mencionado anteriormente), entonces adjuntar el número IMAI a los datos de llamada saliente y enviarlo a la red celular.

El propósito del procedimiento descrito en las etapas a, b y c es evitar la posibilidad de que un desarrollador fraudulento use un número IMAI generado por un desarrollador legal para tratar de conseguir acceso a la red. Consideremos un número IMAI I, generado con el procedimiento descrito anteriormente. Además, supongamos que el DN del desarrollador de aplicaciones es DNA y el DN de la CA que firma el certificado de desarrollador de la aplicación es DNCA:

Por tanto I=High4 (H(DNA+DNCA+RN1))+RN1 donde High4 es una función que devuelve los primeros 4 bytes de una cadena de bytes, y + es una función de concatenación de bytes.

Si un desarrollador fraudulento desea conseguir acceso a su aplicación reutilizando los permisos de la aplicación del desarrollador legal, puede intentar incluir 'I' como el IMAI en su aplicación. No obstante, tendrá que firmar la aplicación con su propio certificado, que incluirá DNA' (el nombre distinguido del desarrollador fraudulento) y DNCA' (la CA que firma el certificado del desarrollador fraudulento). Obsérvese que DNCA' puede ser igual que DNCA (ambos certificados pueden firmarse por la misma CA) pero necesariamente DNA será diferente de DNA'.

El ejecutor de políticas locales calculará High4(H(DNA'+DNCA'+RN1)) y lo comparará con los 4 bytes superiores de I, que son High4(H(DNA+DNCA+RN1)). Puesto que DNA es diferente de DNA', los *hashes* serán

diferentes y por tanto la comparación fallará, dando como resultado que el ejecutor de políticas locales denegará el acceso a la red a la aplicación.

Ejecutor de políticas de red

Este módulo se incluirá como parte de la red celular del operador móvil (VLR y HLR) y realiza el siguiente procedimiento:

Para cada llamada procesada:

1. Si la llamada no tiene un número IMAI como parte de los datos de señalización, asume que se ha generado desde un terminal no conforme y la deja pasar tal como se hace actualmente.

2. Si la llamada incluye un número IMAI, comprueba si el IMAI está en la lista aprobada para el abonado que genera la llamada. El NPE tendrá una o más listas aprobadas, incluyendo:

- Una lista aprobada general de IMAI habilitados para todos los abonados, y todos los números de destino. En esta lista se incluyen, por ejemplo, las aplicaciones llamantes para los fabricantes de terminales.

- Una lista aprobada ilimitada de abonados, de IMAI habilitados para un abonado específico y todos los números de destino.

- Una lista aprobada limitada de abonados, de IMAI habilitados para un abonado específico y una lista concreta de números de destino.

3. Si el IMAI llamante (y el número de destino, si está en una lista limitada) están en una lista aprobada, deja que la llamada proceda tal como se hace actualmente.

4. Si el IMAI llamante no está en una lista aprobada, el NPE puede cortar la llamada sin acción adicional, o puede generar una solicitud de aprobación. Ambos modos de funcionamiento son correctos. En cualquier caso, tanto si se genera una solicitud de aprobación como si no se genera, la llamada se terminará.

5. Una solicitud de aprobación es un mensaje de señalización enviado al terminal que emite la llamada, y si se genera debe capturarse por el módulo de realimentación que se ejecuta en el terminal, o ignorarse por el terminal.

Módulo de realimentación

Este módulo se incluirá en el sistema operativo (OS) de los teléfonos inteligentes, y tiene la siguiente función:

1. Captura las solicitudes de aprobación generadas por el NPE. Obsérvese que las solicitudes de aprobación deben capturarse por el módulo de realimentación y no debe permitirse que se capturen por ninguna otra aplicación que se ejecute en el teléfono. Si el teléfono no tiene un módulo de realimentación en ejecución, las solicitudes de aprobación deben ignorarse.

2. Cuando se captura una solicitud de aprobación, el módulo de realimentación mostrará una pantalla al usuario del teléfono, informándole de que la red ha rechazado una llamada saliente realizada por la aplicación ‘X’ al número ‘N’, y permitiéndole la opción de añadir la aplicación/número llamado a su lista aprobada.

3. El usuario puede elegir aprobar la aplicación sólo para el número al que estaba intentando llamar, o para todos los números.

4. Si el usuario elige aprobar la aplicación (añadir la aplicación/número llamado a la lista), entonces el módulo de realimentación generará una “Autorización de aprobación” y la enviará al configurador de políticas de red. La autorización de aprobación contendrá los siguientes datos:

- El IMAI de la aplicación que va a autorizarse.

- El número de destino que se permitirá para la aplicación, o ‘0’ si la aplicación tiene acceso no restringido a la red.

- La IMSI del abonado que está aprobando la aplicación.

- Un código de autenticación de mensaje basado en *hash* (HMAC) de los datos anteriores, usando la clave de abonado de su SIM como clave de autenticación.

Configurador de políticas de red

El módulo de configurador de políticas de red residirá en la red celular del operador móvil, y tiene la siguiente función:

1. Captura las autorizaciones de aprobación, tal como se describe en las secciones anteriores.

2. Verifica el HMAC con los datos incluidos en la autorización. Si la verificación del HMAC falla, no hace nada y finaliza.

3. Si la verificación de HMAC tiene éxito, añade el número IMAI, y el número de destino si se especifica a la lista aprobada correspondiente al abonado (obtenida a partir de la IMSI en la autorización de aprobación).

Ventajas de la invención

La invención disminuirá significativamente o incluso eliminará el fraude generado por aplicaciones de terceras partes que hacen uso de las características de teléfono (servicios de pago) de un teléfono inteligente. Obsérvese que mientras que el operador celular es completamente inocente en este tipo de fraude, el operador celular será a quien el usuario estafado reclamará. Y también será el operador celular el que podría perder un cliente debido al fraude.

Puesto que el punto de implementación está en la red, no consumirá recursos en los teléfonos inteligentes, y no puede evadirse mediante la ejecución de software en el teléfono. Será imposible para una aplicación fraudulenta saber de antemano si está en la lista de aplicaciones aprobadas o no, y modificar las listas de llamadas aprobadas.

Con el método descrito el desarrollador de aplicaciones no verá aumentada su carga burocrática, puesto que pueden generar y administrar sus propios números IMAI. Al mismo momento, el número IMAI se asociará a su identidad, protegiendo tanto a ellos mismos como los usuarios frente a un uso fraudulento. Aunque se recomienda que los desarrolladores generen un número IMAI diferente para cada aplicación, el sistema en realidad no lo exige ni obliga a ello.

El hecho de introducir un valor adicional (número IMAI) en lugar de sólo basarse en firmas de aplicaciones tiene dos ventajas:

- Granularidad de permisos, que proporciona a los desarrolladores una manera fácil de especificar cuáles de sus aplicaciones tiene acceso a los servicios de pago de red.

- Permite que la implementación se ejecute en el nivel de red (en lugar del nivel de teléfono móvil), al tiempo que se altera el protocolo en la menor medida posible. Comprobar las firmas de aplicación en la red no sería práctico, seguro o incluso viable en la mayoría de los casos.

Un experto en la técnica puede introducir cambios y modificaciones en las realizaciones descritas sin apartarse del alcance de la invención según las reivindicaciones adjuntas.

SIGLAS

ADSL	*Asymmetric Digital Subscriber Line*; Línea de abonado digital asimétrica
API	*Application Programming Interface*; Interfaz de programación de aplicaciones
CA	Certificate Authority; Autoridad de certificación
CPU	*Central Processing Unit*; Unidad de procesamiento central
HLR	*Home Location Register*; Registro de posición base
HMAC	*Hash-based Message Authenticación Code*; Código de autenticación de mensaje basado en *hash*
IMSI	*International Mobile Subscriber Identity*; Identidad de abonado móvil internacional
ISP	*Internet Service Provider*; Proveedor de servicios de Internet
OS	*Operating System*; Sistema operativo
SHA	*Secure Hash Algorithm*; Algoritmo de *hash* seguro
SIM	*Subscriber Identity module*; Módulo de Identidad de Abonado
SMS	*Short Message Service*; Servicio de mensajes cortos
UMTS	*Universal Mobile Telecommunication System*; Sistema universal de telecomunicaciones móviles
VLR	*Visitor Location Register*; Registro de ubicación visitante

BIBLIOGRAFÍA

[1] Business Insider: http://www.businessinsider.com/chart-of-the-day-pcs-market-share-microsoft-vs-the-rest-2010-6

[2] Dialler detected on the wild: http://news.cnet.com/8301-27080_3-20013222-245.html

[3] No antivirus for iPhones: http://www.theregister.co.uk/2009/11/25/iphone_anti_malware/

REIVINDICACIONES

1. Método para detectar y controlar el uso de servicios de pago salientes no deseados en dispositivos de comunicación inteligentes, en el que se solicita un servicio de pago saliente mediante una aplicación que se ejecuta en un dispositivo de comunicación inteligente, caracterizado porque comprende

- asociar, un desarrollador de aplicaciones, un primer número identificador a dicha aplicación;

- instalar dicha aplicación en dicho dispositivo de comunicación inteligente;

- detectar, dicho dispositivo de comunicación inteligente, que dicha aplicación está solicitando acceder a un servicio de pago saliente;

- generar, dicho dispositivo de comunicación inteligente, un segundo número identificador a partir de parámetros obtenidos desde dicha aplicación;

- comparar, dicho dispositivo de comunicación inteligente, dichos números identificadores primero y segundo y, dependiendo del resultado de dicha comparación:

- permitir, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente generando una señal saliente que incluye dicho primer número identificador y enviar dicha señal saliente a una red, o

- rechazar, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente.

2. Método según la reivindicación 1, que comprende además:

- detectar, dicha red, la existencia de dicho primer número identificador en una solicitud de acceso procedente de dicho dispositivo de comunicación inteligente; y

- decidir, dicha red, permitir o rechazar una conexión de dicho dispositivo de comunicación inteligente a dicha red basándose en las preferencias previamente expresadas de un usuario de dispositivo de comunicación inteligente o dicha red.

3. Método según la reivindicación 1 ó 2, en el que dicha red es una red celular.

4. Método según la reivindicación 1, 2 ó 3, que comprende asociar dicho primer número identificador a un ejecutable de aplicación de dicha aplicación en forma de metadatos, datos adicionales o como parte de un archivo de manifiesto.

5. Método según cualquiera de las reivindicaciones anteriores 1 a 4, que comprende firmar conjuntamente dicha aplicación con dicho primer número identificador por medio de métodos de firmado y un certificado del desarrollador.

6. Método según la reivindicación 5, que comprende generar dicho primer número identificador haciendo uso de un nombre distinguido de dicho certificado del desarrollador y un nombre distinguido de la autoridad de certificación que firma dicho certificado del desarrollador.

7. Método según cualquiera de las reivindicaciones anteriores, en el que dicho primer número identificador es un número de 8 bytes.

8. Método según la reivindicación 7 cuando depende de la reivindicación 6, que comprende generar dicho primer número identificador tal como sigue:

- generar un número aleatorio de cuatro bytes;

- agrupar dicho nombre distinguido de dicho certificado del desarrollador, dicho nombre distinguido de la autoridad de certificación que firma dicho certificado del desarrollador y dicho número aleatorio de cuatro bytes en un número de grupo;

- usar una función unidireccional con dicho número de grupo como una entrada para obtener un número resultante;

- truncar dicho número resultante a los primeros, o más significativos, cuatro bytes; y

- adjuntar a dichos primeros cuatro bytes dicho número aleatorio de cuatro bytes como los cuatro bytes menos significativos.

9. Método según la reivindicación 8, en el que dicha función unidireccional es una función *hash*.

10. Método según cualquiera de las reivindicaciones anteriores, que comprende rechazar, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente si dicha aplicación no tiene dicho primer número identificador asociado.

11. Método según cualquiera de las reivindicaciones anteriores 5 a 10, que comprende rechazar, dicho dispositivo de comunicación inteligente, dicha solicitud para acceder a dicho servicio de pago saliente si dicha aplicación con dicho primer número identificador no está firmada correctamente.

12. Método según cualquiera de las reivindicaciones anteriores 7 a 11 cuando dependen de la reivindicación 6, que comprende realizar dicha generación de dicho segundo número identificador agrupando dicho nombre distinguido de dicho certificado del desarrollador, dicho nombre distinguido de la autoridad de certificación que firma dicho certificado del desarrollador y los cuatro bytes más bajos de dicho primer número identificador.

13. Método según la reivindicación 12, que comprende realizar dicha comparación entre dichos números identificadores primero y segundo tal como sigue:

- usar dicho segundo número identificador como una entrada de dicha función unidireccional;

- truncar el resultado de dicha función unidireccional a los primeros, o más significativos, cuatro bytes; y

- comparar dichos cuatro bytes con los primeros, o más significativos, cuatro bytes de dicho primer número identificador.

14. Método según cualquiera de las reivindicaciones anteriores, que comprende realizar dicho servicio de pago saliente, una vez que se ha permitido dicha solicitud para acceder a dicho servicio de pago saliente, si dicho primer número identificador incluido en dicha señal saliente pertenece a una lista aprobada que reside en dicha red.

15. Método según cualquiera de las reivindicaciones anteriores, que comprende

- cortar dicho servicio de pago saliente; o

- generar y enviar una solicitud de aprobación a dicho dispositivo de comunicación inteligente;

una vez que se ha permitido dicha solicitud para acceder a dicho servicio de pago saliente, si dicho primer número identificador incluido en dicha señal saliente no pertenece a una lista aprobada que reside en dicha red.

16. Método según la reivindicación 14 ó 15, en el que dicha lista comprende al menos una de: una lista aprobada general de primeros números identificadores para todos los abonados de dicha red y todos los números de destino, una lista aprobada ilimitada de abonados de primeros números identificadores para un abonado específico de dicha red y todos los números de destino o una lista limitada de abonados del primer número identificador para un abonado específico de dicha red y una lista específica de números de destino.

16. Método según la reivindicación 16 cuando depende de la reivindicación 15, que comprende capturar, dicho dispositivo de comunicación inteligente, dicha solicitud de aprobación y solicitar, mediante medios de visualización de dicho dispositivo de comunicación inteligente, a un abonado de dicho dispositivo de comunicación inteligente autorización para que una aplicación realice dicho servicio de pago saliente.

18. Método según la reivindicación 17, que comprende

- rechazar dicho servicio de pago saliente si dicho abonado deniega dicha autorización; o

- generar una autorización de aprobación y enviar dicha autorización de aprobación a dicha red si dicho abonado aprueba dicha autorización.

19. Método según la reivindicación 18, en el que dicha autorización de aprobación comprende como datos los siguiente parámetros: dicho primer número identificador, un número de destino permitido para dicha aplicación o un parámetro que indica que dicha aplicación tiene acceso no restringido a todos los números de destino de dicha red, una identidad de abonado móvil internacional de dicho abonado de dicho dispositivo de comunicación inteligente y un código de autenticación de mensaje basado en *hash*, o HMAC, que contiene dichos parámetros.

20. Método según la reivindicación 18 ó 19, que comprende capturar, dicha red, dicha autorización de aprobación.

21. Método según la reivindicación 20, que comprende verificar dicho HMAC con dichos parámetros de dicha autorización de aprobación y

- rechazar dicho servicio de pago saliente si dicha verificación falla; o

- añadir dicho primer número identificador a dicha lista si dicha verificación tiene éxito, permitiendo realizar dicho servicio de pago saliente.