(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 683 338**

(51) Int. CI.:

G06F 21/83 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.12.2009 E 09181050 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.05.2018 EP 2211286**

(54) Título: **Procedimiento de securización de una interfaz entre un usuario y una aplicación, y sistema, terminal y producto de programa de ordenador correspondientes**

(30) Prioridad:

19.01.2009 FR 0950286

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.09.2018

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

GRANDEMENGE, JÉRÔME

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de securización de una interfaz entre un usuario y una aplicación, y sistema, terminal y producto de programa de ordenador correspondientes

1. Campo de la invención

El campo de la invención es el correspondiente a la securización de una interfaz entre usuarios y aplicaciones informáticas para dispositivos electrónicos, y, más particularmente, dispositivos electrónicos securizados.

De manera más precisa, la invención se refiere al control o la supervisión de la implementación de aplicaciones no securizadas, por ejemplo, no certificadas, en terminales que garantizan asimismo la implementación de aplicaciones certificadas.

De este modo, la invención se refiere especialmente a los terminales de pago.

2. Técnica anterior

Debido a la naturaleza de las operaciones a las que están destinados, dichos terminales que permiten pagos electrónicos, y, de manera más general, operaciones que requieren una securización, y que suponen por ejemplo la comunicación de un código secreto, constituyen objetivos preferentes de las agresiones informáticas.

En particular, una aplicación informática malintencionada que se ejecuta en un terminal de pago podría ser nociva para la disponibilidad o el funcionamiento de este terminal, o podría utilizar las informaciones suministradas por un usuario para llevar a cabo operaciones fraudulentas.

Por ejemplo, fragmentos de código pueden ser activados por el propio usuario, sin él saberlo, durante su interacción con el terminal. Una aplicación malintencionada puede obtener especialmente del usuario datos sensibles, tales como datos bancarios por ejemplo.

Se utilizan asimismo técnicas de suplantación de identidad (denominadas también en inglés “phishing”) con el fin de incitar al usuario a suministrar datos confidenciales por usurpación de la identidad de una sociedad respetable. Por ejemplo, el usuario puede ser dirigido, sin él saberlo, a un sitio de Internet malintencionado que se hace pasar por el sitio bancario del usuario o por un sitio de compras en línea.

Según otro planteamiento, la aplicación más intencionada puede reproducir un vídeo, que solicita una información confidencial simulando la interfaz habitual de una aplicación securizada. La aplicación que se encuentra “detrás” del vídeo puede recuperar entonces la información confidencial, y transmitirla a un usuario fraudulento.

Conscientes de lo que está en juego, los actores implicados en el sector han buscado proteger los terminales de este tipo de ataques.

Una de las soluciones seleccionadas consiste en, por una parte, definir exigencias en materia de seguridad de los terminales de pago y de las aplicaciones destinadas a estos terminales y, por otra parte, certificar los terminales y las aplicaciones que respetan estas exigencias.

Se puede citar, en particular, la norma “PA DSS” (en inglés “Payment Application Data Security Standard”, por “Norma de Securización de los Datos de las Aplicaciones de Pago”), definida por la agrupación de interés de organismos bancarios PCI, las exigencias de seguridad requeridas por el EPC (*European Payment Council*) o por la Agrupación de Tarjetas Bancarias “CB”.

Asimismo, el organismo EMVCo (*Europay Mastercard Visa Corporation*) emite certificaciones EMV para aplicaciones o terminales de pago, por medio de laboratorios acreditados.

La certificación de una aplicación se puede traducir, por ejemplo, en la inserción de un marcador en el código de la aplicación o en uno de sus archivos de configuración.

El terminal verifica, a continuación, la presencia de este marcador en el arranque de la aplicación.

Así, la certificación de una aplicación se convierte en uno de los criterios exigidos por los organismos bancarios para integrarla en un sistema de pago.

Uno de los inconvenientes de estos planteamientos de la técnica anterior reside en la obligación, para los industriales proveedores de aplicaciones informáticas destinadas a terminales de pago, de hacer que cada versión de su aplicación sea certificada por un auditor certificado por una agrupación de normalización.

Así, un editor de aplicaciones se ve obligado a hacer que una aplicación sea certificada según diferentes normas si esta aplicación está destinada a utilizarse en varios sistemas de pago.

Otro de los inconvenientes reside en el hecho de que esta operación de certificación puede resultar costosa, en

cuanto a tiempo y en cuanto a recursos, en el caso de aplicaciones que evolucionan frecuentemente.

Asimismo, la técnica anterior tiene como inconveniente la imposición de una certificación a todas las aplicaciones implementadas en un terminal, mientras que la misma no es necesaria más que para las aplicaciones que requieren efectivamente una securización. Así, en un terminal de pago, una aplicación de pago debe certificarse. En cambio, esto no es necesario para una aplicación de juego, o una aplicación que emita informaciones o publicidad. El documento US2005182924 bloquea la acción o acciones de un componente detectado como sospechoso.

3. Objetivos de la invención

La invención tiene como objetivo especialmente paliar estos inconvenientes de la técnica anterior. La invención se define por las reivindicaciones que se presentan posteriormente. De forma más precisa, un objetivo de la invención, según al menos un modo de realización, es limitar, para un editor de aplicaciones, los contratiempos de la certificación de sus aplicaciones, especialmente cuando se trata de aplicaciones para las cuales la exigencia de seguridad para la propia aplicación es débil o inexistente.

Otro objetivo de la invención es, según al menos un modo de realización, ofrecer una solución poco costosa en términos de certificación para los editores de aplicaciones y adaptada, por tanto, a la certificación de aplicaciones que evolucionan frecuentemente o a la certificación de aplicaciones destinadas a varios tipos de terminales y de sistemas de pago.

Todavía otro objetivo de la invención es, según al menos un modo de realización, proponer una solución fácil de implementar por los editores de aplicaciones.

Un objetivo particular de la invención es, según al menos un modo de realización, proponer una solución evolutiva a los fabricantes de sistemas de pago.

La invención tiene asimismo como objetivo, según al menos un modo de realización, aportar una técnica que permite la convivencia, en un mismo terminal, de aplicaciones certificadas y de aplicaciones no certificadas, sin perjudicar la seguridad de las aplicaciones certificadas.

Todavía otro objetivo de la invención es, según al menos un modo de realización, reducir los riesgos, para el usuario, de transmitir involuntariamente informaciones confidenciales a una aplicación no certificada.

4. Exposición de la invención

En lo sucesivo en el documento, se denomina “componente de control” a un componente de interfaz de una aplicación, susceptible de permitir que la misma realice operaciones de entrada/salida, pudiéndose realizar dichas operaciones a través de medios materiales diversos, tales como, por ejemplo, un ratón, un teclado, un lápiz óptico, una pantalla o un altavoz. La expresión “componente de control de entrada” o “componente de entrada” se aplica, más particularmente, a los componentes de control que permiten operaciones de entrada (teclados y otros medios de introducción de informaciones especialmente) y la expresión “componente de control de salida” o “componente de control de salida” se aplica a los componentes de control que permiten operaciones de salida (pantallas, altavoces, ...).

Estos componentes de control están dotados de un cierto número de propiedades tales como, por ejemplo, un conjunto de acciones potenciales de un usuario, o, en el caso de componentes de control asociados a una interfaz gráfica, una posición en la pantalla, un tamaño, un color, la asociación a una imagen y/o un texto y a sus parámetros.

Durante su ejecución, la aplicación genera vistas sucesivas que constituyen su interfaz con el usuario.

La invención propone una solución novedosa que no presenta todas las limitaciones de la técnica anterior, en forma de un procedimiento de securización de una interfaz entre un usuario y una aplicación no certificada que se ejecuta en un dispositivo electrónico y que entrega por lo menos una vista a renderizar en una pantalla, comprendiendo o estando asociada una de las vistas a por lo menos un componente de control de interfaz,

que implementa, durante la ejecución de dicha aplicación, las siguientes etapas:

- análisis de componentes de control de interfaz de dicha vista, para detectar por lo menos un componente de control de interfaz susceptible de presentar un problema de seguridad al incitar a dicho usuario a suministrar una información sensible, denominado componente sospechoso;

- si se detecta por lo menos un componente sospechoso, restricción o invalidación de las funcionalidades de al menos un componente de control de entrada de dicho dispositivo electrónico, distinto de dicho por lo menos un componente sospechoso y susceptible de permitir el suministro de dicha información por parte de dicho usuario a dicha aplicación no certificada;

- generación del renderizado de dicha vista y reproducción de dicha vista.

Así, la invención permite autorizar la implementación de aplicaciones no certificadas, en un terminal securizado. Para ello, la invención prevé así un control dinámico de cada aplicación no certificada, y, llegado el caso, la implementación de una acción adaptada, tal como la limitación o la prohibición del uso de un teclado o de cualquier otro medio de entrada de información que puede ser confidencial.

En ciertos modos particulares de implementación de la invención, dicha etapa de análisis tiene en cuenta un conjunto de reglas de restricción de utilización predeterminadas de por lo menos uno de dichos componentes de control de interfaz y/o de por lo menos una combinación de al menos dos de dichos componentes de control de interfaz.

En un modo particular de realización de la invención, dicha etapa de análisis puede considerar como componente sospechoso todo teclado virtual, o un teclado virtual situado en una zona particular de la pantalla.

Según ciertos modos preferentes de realización de la invención, dicha etapa de restricción o de invalidación adapta dicha restricción o invalidación en función de dicha regla o reglas no respetadas. Por ejemplo, en el caso particular en el que un teclado virtual visualizado en una zona particular de la pantalla se considera como componente sospechoso, la etapa de restricción puede restringir especialmente las posibilidades de posicionamiento del puntero de un ratón, para mantenerlo fuera de esta zona de pantalla.

Según diferentes modos de realización de la invención, la etapa de restricción o de invalidación puede referirse a por lo menos un elemento perteneciente al grupo que comprende:

- la prohibición de una visualización,
- la limitación de una zona de captura,
- la limitación de la utilización de al menos un medio de control de entrada.

En un modo preferente de realización de la invención, dicha etapa de restricción o de invalidación puede limitar las acciones posibles del usuario sobre ciertos componentes de control de entrada, y, especialmente, sobre componentes que no sean el componente sospechoso detectado.

Así, en ciertos modos particulares de realización de la invención, dicha etapa de restricción o de invalidación comprende una subetapa de prohibición de la introducción de información por medio de un teclado real o virtual.

Según modos de realización de la invención, puede considerarse un teclado de dicho dispositivo electrónico o un teclado perteneciente a otro aparato, por ejemplo, un equipo periférico de dicho dispositivo. Así, en el caso en el que el dispositivo electrónico es un terminal de pago, puede considerarse, por ejemplo, el teclado de un “pin-pad” (equipo periférico utilizado para la introducción del código secreto del usuario con el fin de cifrarlo).

Así, dicha etapa puede conducir a la invalidación sistemática de las entradas de un teclado real o virtual.

En otros modos de realización de la invención, dicha etapa de restricción o de invalidación puede, por ejemplo, inactivar todo carácter alfanumérico de un teclado real o virtual y no autorizar más que flechas de desplazamiento.

En otros modos de realización de la invención, dicha etapa de restricción o de invalidación comprende una subetapa de prohibición de la introducción de información en al menos una zona de una pantalla de presentación visual, identificándose dicha zona en función de una zona de visualización asociada a por lo menos un componente sospechoso.

Así, en un modo particular de realización de la invención, dicha etapa de restricción o de invalidación puede prohibir, por ejemplo, ciertas posiciones conjuntas de una zona de captura táctil y de una imagen no certificada, asimilada durante la etapa de análisis a un componente sospechoso, para constituir un perímetro de seguridad en torno a dicha imagen.

Finalmente, otros modos de implementación del procedimiento según la invención pueden prever que dicha etapa de restricción o de invalidación comprenda una subetapa de modificación dinámica del renderizado de al menos uno de dichos componentes de control de interfaz de dicha vista.

En ciertos modos de realización de la invención, dichas reglas de restricción pueden comprender, por ejemplo, al menos una regla de prohibición de por lo menos una combinación, determinada como arriesgada, de componentes de control en una misma vista. En este caso, la etapa de restricción o de invalidación puede conducir a la declinación de la visualización de al menos uno de estos componentes de control en dicha vista, y, llegado el caso, visualizar, en su lugar o complementariamente, un mensaje de alerta.

Por ejemplo, dichas reglas de restricción o de invalidación pueden prohibir la visualización conjunta de un componente de control de entrada de tipo teclado virtual y de un componente de control de salida de tipo imagen no certificada; y dicha etapa de restricción o de invalidación puede conducir a la declinación de la visualización de dicho componente de control de entrada de tipo teclado virtual.

Todavía en otros modos de implementación de la invención, dichas reglas de restricción pueden prohibir por lo menos una combinación de ciertas propiedades de dichos componentes de control.

En un modo particular de realización de la invención, adaptado a un terminal de pago, dicha etapa de restricción o de invalidación puede conducir, por ejemplo, a la declinación de la visualización de un componente de control de entrada de tipo teclado virtual en presencia de un componente de control de salida de tipo texto que contenga, por ejemplo, el término “pin”.

Así, el procedimiento de la invención suministra una técnica que permite limitar las posibilidades de perjuicio de una aplicación no securizada.

Además, una de las ventajas de la invención, según al menos un modo de realización, es preservar, sin embargo, las posibilidades de ejecución de una aplicación no certificada.

En efecto, gracias al procedimiento de la invención, una aplicación no certificada se podrá ejecutar en un dispositivo electrónico, tal como un terminal de pago por ejemplo, si la misma respeta el conjunto de las reglas de restricción definidas.

Por ejemplo, la etapa de restricción o de invalidación puede autorizar acciones sin riesgo, tales como la utilización de menús desplegables, o la visualización de una ventana de mensajes, o la utilización de botones simples.

Según los modos de realización de la invención, dicho procedimiento de securización de la interfaz puede comprender una verificación de una certificación de al menos uno dichos componentes de control de interfaz utilizados por dicha aplicación.

En ciertos modos de realización de la invención, dicha verificación de una certificación de dichos componentes de control puede ser común a varias aplicaciones.

En efecto, si varias aplicaciones utilizan los mismos componentes de control, es suficiente con que el editor haga que el conjunto de estos componentes de control se certifique una sola vez.

Por ejemplo, la certificación de un teclado virtual puede comprender la verificación de cada tecla del teclado, debiéndose traducir la selección de una tecla “N” únicamente en la introducción del carácter “N” así como la verificación de la ausencia de una zona de selección diferente a las teclas visualizadas.

Otra de las ventajas de la aplicación es ofrecer la posibilidad a un editor de que modifique el aspecto de un conjunto de aplicaciones, haciendo que se certifique un nuevo juego de componentes de control, asociados, por ejemplo, a nuevas hojas de estilos o nuevas animaciones.

En ciertos modos particulares de realización de la invención, dicha por lo menos una regla de restricción de utilización se memoriza en el interior del dispositivo electrónico durante su instalación. En otros modos de realización, pueden considerarse reglas actualizadas durante una operación de mantenimiento local o a distancia.

Según los modos de implementación de la invención, el procedimiento puede comprender una etapa de descarga de por lo menos una de dichas reglas de restricción de utilización, desde un sitio remoto.

En ciertos modos de implementación de la invención, el dispositivo puede, por ejemplo, interrogar a un servidor remoto previamente a la ejecución de la aplicación, con el fin de obtener dicha por lo menos una regla de restricción de utilización.

En ciertos modos particulares de realización de la invención, dichos componentes de control de interfaz pertenecen al grupo que comprende:

- botones;
- ventanas;
- textos;
- imágenes;
- pestañas;
- zonas de introducción de datos;
- teclados virtuales;
- menús;
- marcos;

- tablas;
- zonas de captura táctil;
- listas de selección;
- casillas de selección;
- barras de progreso;
- cursores deslizantes;
- árboles desplegables;
- barras de desplazamiento;
- seleccionadores de fechas y/o de horas (“datepicker” y/o “timepicker” en terminología anglosajona);
- altavoces;
- teclados físicos;
- ratones;
- cámaras;
- lápices ópticos;
- lectores de informaciones biométricas;
- combinaciones de estos controles elementales.

En un modo preferente de implementación de la invención, el procedimiento de securización de la interfaz está adaptado para una implementación en un entorno de Internet.

En un modo particularmente ventajoso de realización de la invención, el procedimiento se puede adaptar a una utilización en un entorno que respete las recomendaciones del W3C (*World Wide Web Consortium*).

En particular, en ciertos modos de realización de la invención, dicha aplicación no certificada presenta una interfaz de usuario escrita en un lenguaje compatible con la norma XML (*eXtensible Markup Language*).

En ciertos modos de realización de la invención, la descripción de dicha vista y de sus componentes de control de interfaz se puede realizar, por ejemplo, con el XML, para definir una representación en memoria con la ayuda de una estructura de árbol de los componentes de control. Así, a continuación es posible aplicar en la misma un algoritmo automático.

En un modo de realización ventajoso de la invención, dicha vista y/o sus componentes de control de interfaz se representan en una memoria con la ayuda de la tecnología *Document Object Model*.

En otros modos de realización de la invención en los que la interfaz de usuario de la aplicación está constituida por un conjunto finito de vistas fijas, no modificables dinámicamente por la aplicación, dicha descripción se puede implementar para reaccionar a las acciones realizadas sobre los componentes de control. dicha descripción se puede implementar entonces, por ejemplo, según una tecnología SAX (*Simple API for XML*).

Finalmente, en ciertos modos de implementación de la invención, dichas reglas de restricción se pueden describir con un lenguaje basado en XML.

La invención se refiere además a un producto de programa de ordenador descargable desde una red de comunicación y/o grabado en un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado por que comprende instrucciones de código de programa para la implementación de dicho procedimiento de securización de interfaz.

En particular, dicho análisis y/o dicha etapa de restricción o de invalidación se puede implementar en un lenguaje que permita el análisis de un archivo de reglas compatibles con la norma XML, tal como los lenguajes C, C++ o Java por ejemplo.

La invención se refiere también a un terminal que implementa el procedimiento descrito anteriormente en la presente y que consta de medios de interfaz entre un usuario y una aplicación no certificada que se ejecuta en dicho terminal y que entrega por lo menos una vista que se va a renderizar en una pantalla, comprendiendo o estando asociada una de las vistas a por lo menos un componente de control de interfaz.

Un terminal de este tipo implementa, durante la ejecución de dicha aplicación:

- medios de análisis de componentes de control de interfaz de dicha vista, para detectar por lo menos un componente de control de interfaz susceptible de plantear un problema de seguridad al incitar a dicho usuario a suministrar una información sensible, denominado componente sospechoso;

- si se detecta por lo menos un componente sospechoso, medios de restricción o de invalidación de las funcionalidades de por lo menos un componente de control de entrada de dicho dispositivo electrónico, distinto de dicho por lo menos un componente sospechoso y susceptible de permitir el suministro de dicha información por dicho usuario a dicha aplicación no certificada;

- medios de generación del renderizado de dicha vista y de la reproducción de dicha vista.

En un modo preferente de realización de la invención, dicho terminal está dotado de una interfaz gráfica hombre/máquina (GUI – “Graphical User Interface” en inglés).

Según un modo preferente de realización de la invención, el terminal comprende medios de gestión de pago electrónico que cooperan con dicha pantalla.

5. Lista de las figuras

Otras características y ventajas de la invención se pondrán de manifiesto más claramente al leer la siguiente descripción de un modo de realización preferente, ofrecido a título de ejemplo simple ilustrativo y no limitativo, y de los dibujos adjuntos, en los cuales:

- la figura 1 presenta un esquema sinóptico funcional de la invención en un modo de realización;

- la figura 2 ilustra el funcionamiento dinámico de la invención, basado en el esquema sinóptico estático de la figura 1;

- la figura 3 ilustra posibles acciones sobre el renderizado de las vistas de la aplicación durante el funcionamiento dinámico de la invención, tal como se ilustra en la figura 2.

6. Descripción de un modo de realización de la invención

6.1 Principio general

El principio general de la invención consiste, por tanto, en limitar de manera dinámica los riesgos de perjuicios de una aplicación no certificada que se ejecuta en un dispositivo electrónico por la aplicación dinámica de reglas de seguridad predefinidas sobre los componentes de control de interfaz de la aplicación.

Por ejemplo, la invención permite autorizar la ejecución de una aplicación no certificada, tal como una animación de vídeo, en un dispositivo electrónico, tal como un terminal de pago. El planteamiento de la invención es no dejar a una aplicación de este tipo, en la medida de lo posible, la posibilidad de implementar acciones malintencionadas analizando dinámicamente sus componentes de control de entrada y/o de salida, en el momento de la generación de una vista que se va a reproducir, o a renderizar, especialmente en una pantalla.

Un ejemplo simple consiste en prohibir a una aplicación de vídeo la utilización de cualquier componente de interfaz de control de entrada durante el transcurso de la secuencia de vídeo. Otro ejemplo consiste en permitir únicamente componentes de interfaz de control de entrada certificados, vinculados al desarrollo de la secuencia de vídeo, tales como botones “play”, “pausa”, “stop”. Este segundo planteamiento permite autorizar ciertas funcionalidades de la aplicación aún protegiendo al usuario.

Así, no resultará posible responder a una invitación malintencionada en el vídeo para suministrar un dato, y, por ejemplo, introducir un código secreto por medio de un teclado, debido a que este teclado se habrá invalidado. Asimismo, si la aplicación no certificada presenta un teclado virtual de introducción de datos (lo cual supone la presencia, en la aplicación, de un componente de control de introducción de datos en el teclado virtual), la invención preverá la invalidación de un dispositivo señalador, por ejemplo, un ratón, al menos en las proximidades de este teclado virtual, y/o la invalidación de la función de validación o de utilización de un teclado. Sin embargo, no se interrumpirá la emisión de la vista.

La invención propone, por tanto, un planteamiento original, según el cual no es la aplicación no certificada la que se invalida, sino la utilización de ciertos componentes de entrada. En otras palabras, se condiciona la utilización de los componentes de entrada a la presencia y/o a las características de otros componentes de interfaz no certificados, sin actuar directamente sobre estos últimos.

6.2 Descripción de un modo particular de realización

A continuación se considera un ejemplo de implementación de la invención para un terminal de pago.

En relación con la figura 1, se presenta un modo particular de implementación del procedimiento según la invención, en el cual dicho procedimiento se utiliza en un entorno tecnológico de tipo Internet.

En este modo particular de realización de la invención, un terminal de pago 100 permite que un usuario efectúe pagos y transmite informaciones relativas a estos pagos hacia un sistema de gestión remoto 120.

En el modo particular descrito en este caso, el usuario utiliza, para el suministro de sus datos personales, una tarjeta electrónica de pago 130 ó una tarjeta de fidelización. Sin embargo, otros modos de realización del procedimiento pueden utilizar otros medios de suministro de los datos personales del usuario. Puede considerarse, por ejemplo, el suministro de un código de acceso a un sitio de Internet específico que contiene datos personales o de un código de acceso que permite identificar una operación realizada anteriormente por el operador, tal como, por ejemplo, la compra de un título de transporte. Puede considerarse asimismo una información biométrica, leída por un sensor previsto a tal efecto.

El terminal 100 consta de medios de interfaz con el usuario. En particular, en el modo de realización particular descrito mediante la figura 1, el terminal está dotado de una pantalla táctil 102. Puede considerarse, por ejemplo, una pantalla a color adaptada para el visionado de secuencias de vídeo.

En el ejemplo ilustrado mediante la figura 1, el terminal está dotado también de un teclado físico 112 así como de un lector 114 apto para leer las informaciones contenidas en la tarjeta electrónica 130.

El terminal consta de medios de ejecución de por lo menos dos aplicaciones, por ejemplo, al menos una aplicación certificada 110C y al menos una aplicación no certificada 110NC.

Después de la verificación de su certificación, las aplicaciones 110C se pueden ejecutar de la manera típica. En cambio, una aplicación no certificada 110NC, por ejemplo, un juego o una aplicación con intenciones publicitarias, tal como una secuencia de vídeo, que se ejecuta en el terminal cuando este último no se utiliza, por ejemplo, para un pago, debe ser controlada.

En el ejemplo presentado, la interfaz de usuario de la aplicación 110NC está contenida dentro de archivos de descripción de interfaz escritos en un lenguaje compatible con la norma XML, tal como un lenguaje HTML o XUL (“XML – based User interface Language”).

El terminal 100 consta de un módulo de control 106, apto para extraer reglas contenidas en una memoria securizada 108 y para verificar que son respetadas por las vistas de la aplicación 110NC.

Finalmente, un motor de renderizado 104, típico, es apto para garantizar consecuentemente la reproducción de la vista en la pantalla 102.

Según un modo de implementación de la invención, el módulo de control puede comprender por lo menos un analizador (“parser”), por ejemplo, un analizador XML, implementado en un lenguaje compatible con el XML, tal como C, C++ o Java. Dicho analizador puede ser apto para generar un árbol DOM (“Document Object Model”) con el fin de describir la estructura de las diferentes vistas de la aplicación y/o para controlar dinámicamente la validez, según las reglas de seguridad definidas. En el ejemplo ilustrado, el árbol DOM se genera a partir de los archivos XML de descripción de interfaz durante la puesta en marcha de la aplicación y, a continuación, se vuelve a generar y/o modificar durante la ejecución de la aplicación.

El motor de control es también apto para modificar el árbol DOM en función de las reglas de restricción. Este árbol DOM podrá ser utilizado, a continuación, por el motor de renderizado para la visualización de una vista.

Otros modos de realización se pueden basar en una tecnología SAX.

En ciertos modos ventajosos de realización, la invención se puede implementar en un navegador web, tal como un navegador “WebC” por ejemplo, tal que las modificaciones dinámicas del DOM permitidas por un lenguaje como por ejemplo el lenguaje javascript puedan ser cotejadas sistemáticamente con las reglas de seguridad definidas.

La figura 2 ilustra el funcionamiento dinámico de la invención.

En el modo de realización descrito en este caso, el procedimiento según la invención se implementa durante la ejecución de la aplicación, cuando esta última solicita la visualización de una de sus vistas 200. En primer lugar se efectúa una verificación 202 de la certificación de la aplicación. Si la aplicación está certificada, no se lleva a cabo ningún control sobre la vista de la aplicación antes de su renderización.

En caso de que la aplicación no esté certificada, el procedimiento prevé una etapa de análisis 210, en relación con los componentes de control de dicha vista.

Según un modo particular de realización de la invención, este análisis se basa en el respeto de reglas de restricción de utilización 230 almacenadas, por ejemplo, en una zona de memoria 108 del terminal.

Estas reglas pueden estar descritas, por ejemplo, en un lenguaje compatible con la norma XML.

En el modo de realización presentado en la figura 2, el procedimiento prevé, para cada regla a examinar 212, un análisis 214 de si se respeta dicha regla mediante el árbol DOM 240 correspondiente a dicha vista.

En ciertas implementaciones de la invención, dichas reglas pueden incluir una exigencia de certificación de los componentes de control de interfaz presentes en el árbol DOM.

La etapa de análisis 210 puede incluir, entonces, por ejemplo, una verificación de la certificación para cada componente de control de interfaz presente en el árbol DOM.

En otros modos de realización, el procedimiento puede constar, en cuanto se ponga en marcha la aplicación, y/o en instantes predeterminados, de una etapa de verificación de la certificación de la aplicación y/o de ciertos conjuntos de componentes de control de la aplicación, por ejemplo, de bibliotecas gráficas de componentes de control.

Una de las ventajas de la invención, al menos en ciertos modos particulares de realización, es, por tanto, que permite limitar la necesidad de certificación de una aplicación para su ejecución en un terminal, a la certificación de sus componentes de control de interfaz, en la medida en la que dicha aplicación respete las reglas de restricción definidas.

Si una regla no es respetada (prueba 216), la etapa de análisis se pronuncia por la identificación 218 de por lo menos un componente sospechoso. El contexto de dicha regla no respetada se puede guardar también para una utilización en la etapa siguiente 220 de restricción/invalidación.

En otros modos de realización de la invención, la identificación 218 de por lo menos un componente sospechoso también puede conllevar la asociación de un nivel de riesgo a este componente sospechoso. Este nivel de riesgo puede estar en función, por ejemplo, de la certificación o de la naturaleza de dicho componente sospechoso.

Según la invención, el procedimiento prevé a continuación una etapa 220 de restricción o la invalidación de un componente de entrada, distinto del componente sospechoso identificado.

Esta etapa 220 comprende una subetapa 222 de determinación de la acción de restricción o de invalidación a emprender en función del componente sospechoso y de la regla no respetada. Esta subetapa 222 de determinación se puede basar asimismo en reglas de restricción suplementarias con respecto a las utilizadas en la etapa 210 de análisis.

Por ejemplo, una regla suplementaria puede ser interrumpir la ejecución de la aplicación en cuanto se detecte un componente sospechoso.

Si la acción a emprender no es la de interrumpir la aplicación, el procedimiento prevé, a continuación, una subetapa 224 de identificación de por lo menos un componente de control de entrada, distinto del componente sospechoso identificado, sobre el cual debe recaer la acción de restricción/o la invalidación. Esta identificación se puede realizar, por ejemplo, en relación con el árbol DOM 240 que describe la vista.

Finalmente, el procedimiento prevé la implementación de una acción 226 sobre el renderizado de la vista antes de la etapa de generación y de reproducción 250 del renderizado de la vista.

Esta acción sobre el renderizado puede variar según los modos de realización de la invención, tal como se ilustra en el ejemplo de la figura 3.

Una de las acciones puede consistir, por ejemplo, en interrumpir la ejecución de la aplicación 302 ó declinar la visualización de la vista 304.

Según los modos de realización de la invención, pueden aportarse restricciones en el renderizado de dicha vista. Por ejemplo, se puede considerar una invalidación 308 de un teclado físico o virtual, una prohibición 310 de cualquier introducción de datos en por lo menos una zona particular de la pantalla o una modificación 312 del renderizado de dicha vista de la aplicación y, especialmente, de los componentes de entrada identificados en la etapa 224.

Así, ciertos modos de realización prevén que al menos un componente de control de entrada, y eventualmente dichos componentes sospechosos, no se puedan visualizar.

En el modo de realización particular descrito en este caso, una regla de restricción simple puede consistir en inhibir todas las acciones posibles de un usuario sobre la pantalla 102 durante el transcurso de una secuencia de vídeo.

Una acción sobre el renderizado puede consistir, por tanto, en suprimir la visualización del conjunto de los componentes de control de entrada previstos en la vista.

Otra regla puede permitir, por ejemplo, únicamente la utilización de componentes de control de interfaz certificados y vinculados a la lectura de dicha secuencia de vídeo, tales como botones “lectura”, “pausa”, “stop”, por ejemplo.

En este caso, una de las acciones sobre el renderizado puede consistir, por ejemplo, en suprimir la visualización de los componentes de control de entrada que sean diferentes de dichos botones. Otra acción puede ser la de conservar su visualización aunque volviéndolos inactivos.

En un modo particular de realización de la invención, también puede visualizarse un mensaje que explique la detección de un riesgo.

En ciertos modos particulares de realización, por ejemplo cuando la etapa de análisis 210 ha asociado niveles de riesgo a dichos componentes sospechosos, la etapa 220 de restricción o de invalidación de un componente de entrada puede variar en función del nivel de riesgo del componente sospechoso detectado.

Por ejemplo, la etapa 220 de restricción o de invalidación puede derivar, en caso de riesgo menor, en la declinación de la visualización de un componente de control de entrada, de manera que la aplicación continúa con su ejecución, mientras que, en caso de detección de un riesgo importante esta etapa puede conllevar la interrupción de la aplicación.

En una variante de implementación de la invención, el procedimiento comprende una etapa previa de determinación de las reglas de restricción 230. Esta etapa puede comprender, por ejemplo, la determinación de las reglas de restricción aplicables por acceso a un sitio remoto del fabricante durante la puesta en marcha de la aplicación.

En una variante de la invención, el procedimiento se puede aplicar a una aplicación certificada con el fin de reforzar la seguridad de las transacciones efectuadas por el terminal de pago.

REIVINDICACIONES

1. Procedimiento de securización de una interfaz entre un usuario y una aplicación no certificada que se ejecuta en un dispositivo electrónico y que entrega por lo menos una vista a renderizar en una pantalla, comprendiendo o estando asociada una de las vistas a por lo menos un componente de control de interfaz,

caracterizado por que implementa, durante la ejecución de dicha aplicación, las siguientes etapas:

- análisis de componentes de control de interfaz de dicha vista, para detectar por lo menos un componente de control de interfaz susceptible de presentar un problema de seguridad al incitar a dicho usuario a suministrar una información confidencial, denominado componente sospechoso, teniendo en cuenta dicha etapa de análisis un conjunto de reglas de restricción de utilización predeterminadas de por lo menos uno de dichos componentes de control de interfaz y/o de por lo menos una combinación de al menos dos de dichos componentes de control de interfaz;

- si se detecta por lo menos un componente sospechoso, restricción o invalidación de las funcionalidades de al menos un componente de control de entrada de dicho dispositivo electrónico, distinto de dicho por lo menos un componente sospechoso y susceptible de permitir el suministro de dicha información por parte de dicho usuario a dicha aplicación no certificada, de manera que dicha etapa de restricción o de invalidación adapta dicha restricción o invalidación en función de dicha regla o reglas no respetadas, comprendiendo dicha etapa de restricción o de invalidación una subetapa de prohibición de la introducción de información por medio de un teclado real o virtual;

- generación del renderizado de dicha vista y reproducción de dicha vista.

2. Procedimiento de securización de una interfaz según la reivindicación 1, caracterizado por que dicha etapa de restricción o de invalidación comprende una subetapa de prohibición de la introducción de información en al menos una zona de una pantalla de visualización, identificándose dicha zona en función de una zona de visualización asociada a por lo menos un componente sospechoso.

3. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 2, caracterizado por que dicha etapa de restricción o de invalidación comprende una subetapa de modificación dinámica del renderizado de al menos uno de dichos componentes de control de interfaz de dicha vista.

4. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que comprende una verificación de una certificación de por lo menos uno de dichos componentes de control de interfaz utilizados por dicha aplicación.

5. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que comprende una etapa de descarga de por lo menos una de dichas reglas de restricción de utilización, desde un sitio remoto.

6. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que dichos componentes de control de interfaz pertenecen al grupo que comprende:

- botones;
- ventanas;
- textos;
- imágenes;
- pestañas;
- zonas de introducción de datos;
- teclados virtuales;
- menús;
- marcos;
- tablas;
- zonas de captura táctil;
- listas de selección;
- casillas de selección;

- barras de progreso;
- cursores deslizantes;
- árboles desplegables;
- barras de desplazamiento;
- seleccionadores de fechas y/o de horas;
- altavoces;
- teclados físicos;
- ratones;
- cámaras;
- lápices ópticos;
- lectores de informaciones biométricas;
- combinaciones de estos controles elementales.

7. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que está adaptado para una implementación en un entorno de Internet.

8. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que dicha aplicación no certificada presenta una interfaz de usuario escrita en un lenguaje compatible con la norma XML.

9. Procedimiento de securización de una interfaz según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que dicha vista y/o sus componentes de control de interfaz se representan en una memoria con la ayuda de la tecnología *Document Object Model*.

10. Producto de programa de ordenador descargable desde una red de comunicación y/o grabado en un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado por que comprende instrucciones de código de programa para la implementación del procedimiento de securización de una interfaz según al menos una de las reivindicaciones 1 a 9.

11. Terminal que implementa el procedimiento de securización de una interfaz según al menos una de las reivindicaciones 1 a 9, y que consta de medios de interfaz entre un usuario y una aplicación no certificada que se ejecuta en dicho terminal y que entrega por lo menos una vista que se va a renderizar en una pantalla, comprendiendo o estando asociada una de las vistas a por lo menos un componente de control de interfaz,

caracterizado por que implementa, durante la ejecución de dicha aplicación:

- medios de análisis de componentes de control de interfaz de dicha vista, para detectar por lo menos un componente de control de interfaz susceptible de plantear un problema de seguridad al incitar a dicho usuario a suministrar una información confidencial, denominado componente sospechoso, teniendo en cuenta dichos medios de análisis un conjunto de reglas de restricción de utilización predeterminadas de por lo menos uno de dichos componentes de control de interfaz y/o de por lo menos una combinación de al menos dos de dichos componentes de control de interfaz;

- si se detecta por lo menos un componente sospechoso, medios de restricción o de invalidación de las funcionalidades de por lo menos un componente de control de entrada de dicho dispositivo electrónico, distinto de dicho por lo menos un componente sospechoso y susceptible de permitir el suministro de dicha información por dicho usuario a dicha aplicación no certificada, de manera que dichos medios de restricción o de invalidación adaptan dicha restricción o invalidación en función de dicha regla o reglas no respetadas, comprendiendo dichos medios de restricción o de invalidación medios de prohibición de la introducción de información por medio de un teclado real o virtual;

- medios de generación del renderizado de dicha vista y de la reproducción de dicha vista.

12. Terminal según la reivindicación 11, caracterizado por que comprende medios de gestión de pago electrónico que cooperan con dicha pantalla.

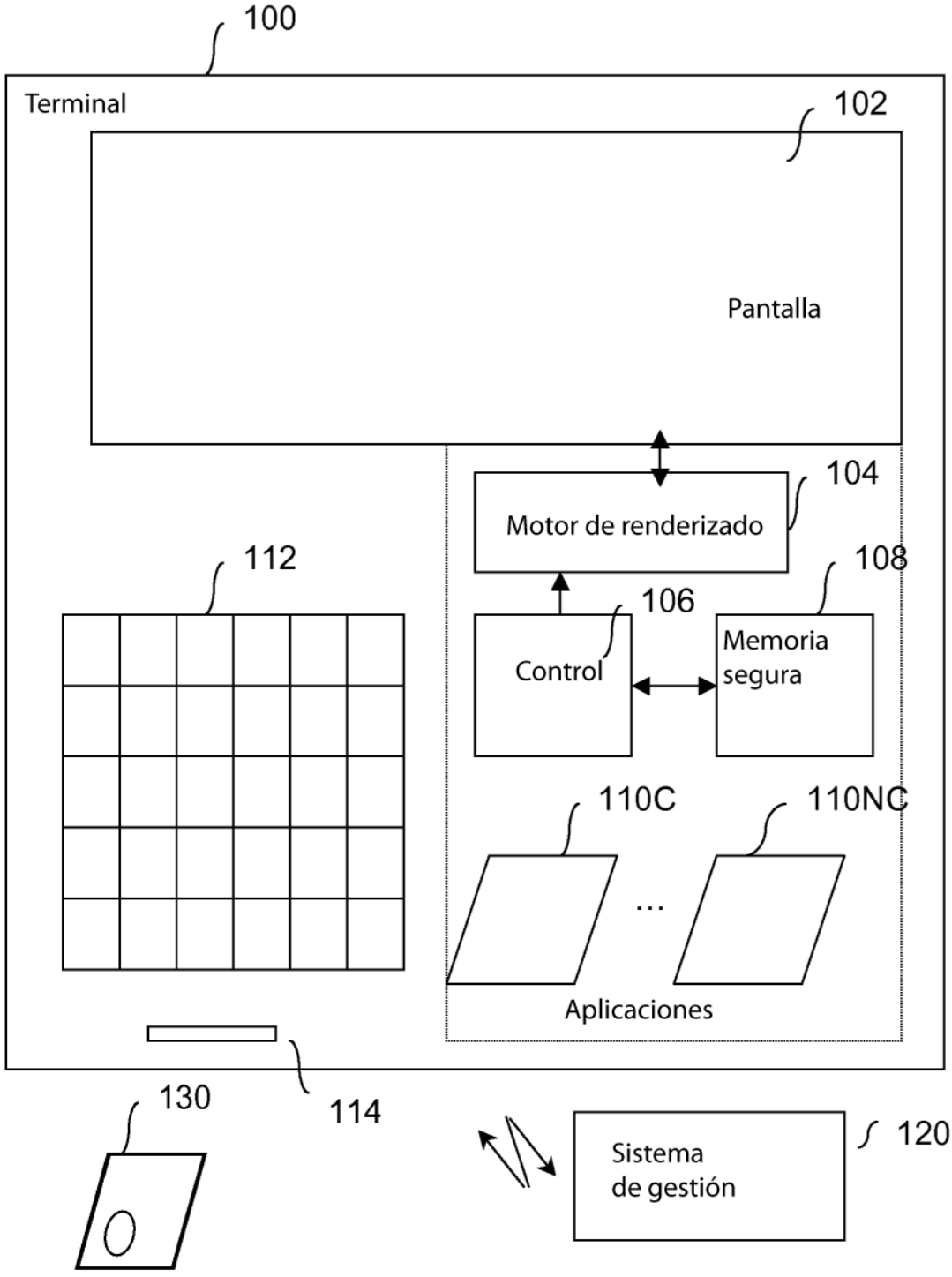
100
Terminal
102
Pantalla
104
Motor de renderizado
108
112
106
Control
Memoria segura
110C
110NC
...
Aplicaciones
130
114
120
Sistema de gestión

Figura 1

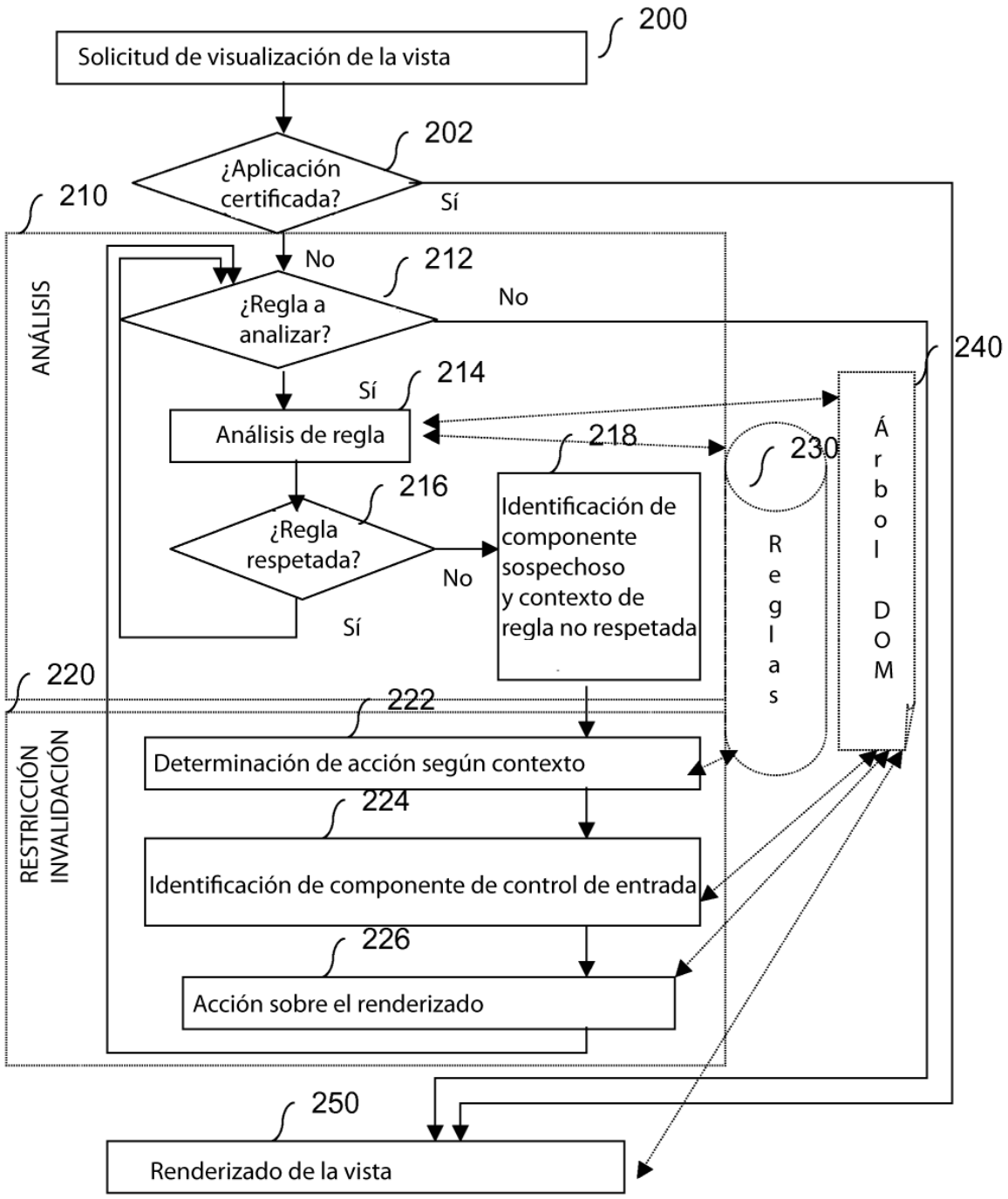
200
Solicitud de visualización de la vista
202
¿Aplicación certificada?
Sí
210
ANÁLISIS
No
212
¿Regla a analizar?
No
240
Sí
214
Análisis de regla
218
230
216
¿Regla respetada?
No
Identificación de componente sospechoso y contexto de regla no respetada
Reglas
Árbol DOM
Sí
220
RESTRICCIÓN INVALIDACIÓN
222
Determinación de acción según contexto
224
Identificación de componente de control de entrada
226
Acción sobre el renderizado
250
Renderizado de la vista

Figura 2

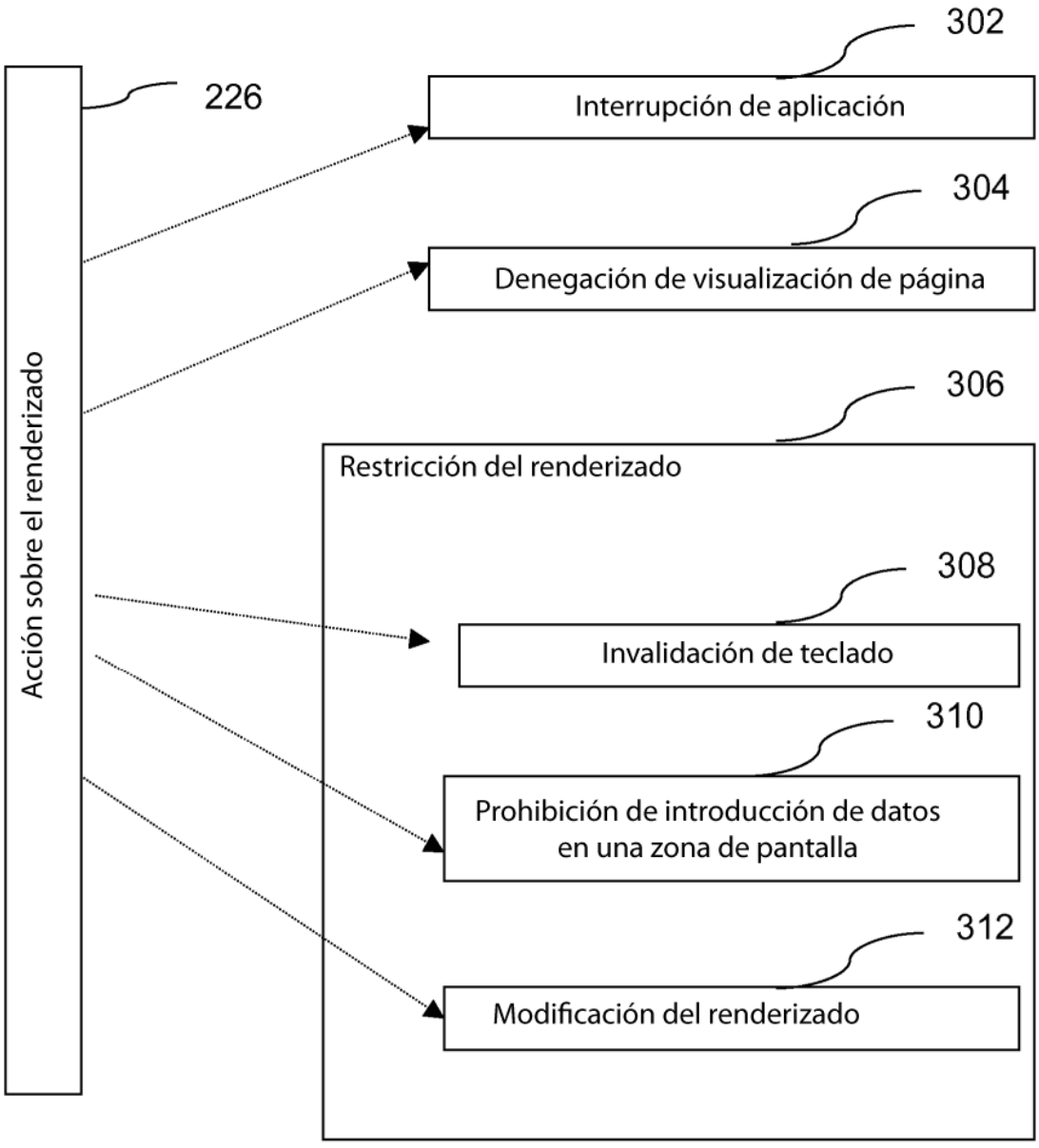
302
226
Interrupción de aplicación
304
Denegación de visualización de página
306
Acción sobre el renderizado
Restricción del renderizado
308
Invalidación de teclado
310
Prohibición de introducción de datos en una zona de pantalla
312
Modificación del renderizado

Figura 3