(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 380**

(51) Int. CI.:

G06F 21/36 (2013.01)
G06F 21/57 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.07.2004 PCT/US2004/024343**

(87) Fecha y número de publicación internacional: **17.11.2005 WO05109736**

(96) Fecha de presentación y número de la solicitud europea: **29.07.2004 E 04779409 (4)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 1726115**

(54) Título: **Elemento de seguridad de visualización con una ventana de navegador**

(30) Prioridad:

15.04.2004 US 826139

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

SELTZER, ANN;
DIRICKSON, ROBERT, STEPHAN;
TOKUMI, ROLAND y
FRANCO, ROBERTO, A.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Elemento de seguridad de visualización con una ventana de navegador

Antecedentes de la invención

Preservar la seguridad de un ordenador cuando se accede a sitios de internet puede ser difícil. Todos los días aparecen nuevas formas de engañar a los usuarios para que seleccionen acciones creyendo que van a realizar una tarea segura, cuando en realidad van a realizar una tarea maliciosa. Por ejemplo, puede introducirse maliciosamente una ventana de navegador para imitar un cuadro de diálogo o una ventana asociada con una fuente de confianza. Puede inducirse a los usuarios que ven la ventana a creer que están cerrando la ventana cuando, en realidad, se les está redirigiendo a otro sitio o están descargando un archivo malicioso.

El documento US 6 366 912 B1 desvela zonas de seguridad de red. El documento WO 01/18636 A1 desvela un sistema y un procedimiento para autenticar una página web.

Sumario de la invención

La presente invención se dirige a proporcionar un procedimiento y un sistema para proporcionar un elemento de seguridad que se dirige a impedir una actividad maliciosa visualizando una ventana de navegador de tal manera que el usuario pueda confiar y conocer la fuente de la ventana.

La invención comprende un procedimiento para proporcionar una característica de seguridad para una ventana de navegador de acuerdo con la reivindicación 1, un medio legible por ordenador que tiene unas instrucciones ejecutables por ordenador para proporcionar una característica de seguridad para una ventana de navegador de acuerdo con la reivindicación 6 y un aparato para proporcionar una característica de seguridad para unas ventanas de navegador de acuerdo con la reivindicación 11.

Breve descripción de los dibujos

La figura 1 ilustra unos dispositivos informáticos a modo de ejemplo que pueden usarse en las realizaciones a modo de ejemplo de la presente invención;
la figura 2 muestra unas ventanas a modo de ejemplo que ilustran diferentes zonas a las que puede acceder un usuario;
la figura 3 ilustra un contenido no fiable visualizado dentro de una ventana de navegador de confianza;
la figura 4 ilustra un procedimiento para mejorar la seguridad para una ventana de navegador;
la figura 5 muestra un procedimiento para determinar ajustes de seguridad; y
la figura 6 ilustra un flujo de procedimiento para ajustar los parámetros de ventana asociados con un elemento de seguridad, de acuerdo con unos aspectos de la invención.

Descripción detallada de la realización preferida

En general, la presente invención se dirige a proporcionar un procedimiento y un sistema para proporcionar una característica de seguridad que se dirige a impedir una actividad maliciosa visualizando una ventana, de tal manera que el usuario pueda confiar y conocer el origen de la ventana. Un elemento de seguridad que incluye información y ornamentación adicionales se visualiza en la ventana para ayudar a garantizar que no se confunda ni se induzca ("se engañe") a un usuario final a creer que la ventana se origina a partir de una fuente de confianza. Por ejemplo, el usuario será capaz de distinguir visualmente una ventana generada a partir de una fuente de confianza, tal como el sistema operativo, frente a una ventana que tiene un contenido generado a partir de una fuente no fiable, tal como un sitio web externo.

De acuerdo con una realización, cuando se abre una ventana de navegador, se visualiza por defecto una barra de estado. La barra de estado proporciona al usuario información adicional, tal como la zona de seguridad, para ayudar al usuario a determinar la fuente del contenido. La zona de seguridad informa al usuario sobre la localización desde la que se origina el contenido. Por ejemplo, la zona de seguridad puede indicar que el contenido se origina desde internet. Esta información adicional ayuda a garantizar que el usuario tiene la información necesaria sobre si debe o no confiar en la fuente.

Entorno operativo ilustrativo

Con referencia a la figura 1, un sistema a modo de ejemplo para implementar la invención incluye un dispositivo informático, tal como el dispositivo 100 informático. En una configuración muy básica, el dispositivo 100 informático incluye habitualmente al menos una unidad 102 de procesamiento y una memoria 104 de sistema. Dependiendo de la configuración exacta y el tipo de dispositivo informático, la memoria 104 de sistema puede ser volátil (tal como RAM), no volátil (tal como ROM, memoria flash, etc.) o alguna combinación de las dos. La memoria 104 de sistema incluye habitualmente un sistema 105 operativo, una o más aplicaciones 106, y puede incluir unos datos 107 de programa. En una realización, la aplicación 106 puede incluir un programa 120 de seguridad de ventanas. En general, el programa 120 de seguridad de ventanas está configurado para garantizar que una ventana se abre con

las señales visuales y la información necesaria para que un usuario determine la fuente del contenido dentro de la ventana. Esta configuración básica se ilustra en la figura 1 mediante los componentes dentro de la línea 108 discontinua.

El dispositivo 100 informático puede tener características o funcionalidades adicionales. Por ejemplo, el dispositivo 100 informático también puede incluir unos dispositivos de almacenamiento de datos adicionales (extraíbles y/o no extraíbles) tales como, por ejemplo, discos magnéticos, discos ópticos, o cintas. Tal almacenamiento adicional se ilustra en la figura 1 mediante el almacenamiento 109 extraíble y el almacenamiento 110 no extraíble. Los medios de almacenamiento informáticos pueden incluir unos medios volátiles y no volátiles, extraíbles y no extraíbles, implementados en cualquier procedimiento o tecnología para el almacenamiento de información, tales como instrucciones legibles por ordenador, estructuras de datos, módulos de programa, u otros datos. La memoria 104 de sistema, el almacenamiento 109 extraíble y el almacenamiento 110 no extraíble son todos ejemplos de medios de almacenamiento informáticos. Los medios de almacenamiento informáticos incluyen, pero sin limitarse a, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticas, cintas magnéticas, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda accederse mediante el dispositivo 100 informático. Cualquier medio de almacenamiento informático de este tipo puede ser parte del dispositivo 100. El dispositivo 100 informático también puede tener un dispositivo(s) 112 de entrada, tal como un teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. También puede incluirse un dispositivo(s) 114 de salida tal como una pantalla, unos altavoces, una impresora, etc.

El dispositivo 100 informático también puede contener unas conexiones 116 de comunicación que permitan que el dispositivo se comunique con otros dispositivos 118 informáticos, tal como a través de una red. La conexión 116 de comunicación es un ejemplo de medios de comunicación. Habitualmente, los medios de comunicación pueden aplicarse mediante instrucciones legibles por ordenador, estructuras de datos, módulos de programa, u otros datos en una señal de datos modulada, tal como una onda portadora u otro mecanismo de transporte, e incluyen cualquier medio de suministro de información. La expresión “señal de datos modulada” significa una señal que tiene una o más de sus características establecidas o cambiadas de tal manera como para codificar información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados, tales como una red cableada o una conexión cableada directa, y medios inalámbricos, tales como medios acústicos, RF, infrarrojos y otros medios inalámbricos. La expresión medios legibles por ordenador, tal como se usa en el presente documento, incluye tanto medios de almacenamiento como medios de comunicación.

Ventanas ilustrativas que incluyen elementos de seguridad

La figura 2 muestra unas ventanas a modo de ejemplo que ilustran diferentes zonas a las que puede tener acceso un usuario, de acuerdo con unos aspectos de la invención. Las zonas de seguridad se usan para ayudar a proporcionar un nivel adecuado de seguridad para los diversos tipos de contenidos con los que los usuarios pueden entrar en contacto. Pueden implementarse muchas zonas de seguridad diferentes que tienen grados variables de fiabilidad asociados con las mismas. De acuerdo con una realización de la invención, hay cinco zonas diferentes, que incluyen una zona (205) de máquina local, una zona (230) de sitios de confianza, una zona (240) de intranet local, una zona (250) de internet, y una zona (260) restringida. Las diferentes zonas tienen niveles variables de seguridad asociados con las mismas. De acuerdo con una realización de la invención, un elemento de seguridad, tal como una barra 220 de estado, siempre se visualiza con la ventana.

La zona (225, 235, 245, 255 y 265) actual se visualiza en el lado inferior derecho de la barra 220 de estado. El usuario puede evaluar fácilmente el riesgo asociado con el contenido 215 haciendo referencia a la zona. Cuando un usuario navega a una zona diferente, esa zona se visualiza dentro de la barra de estado.

De acuerdo con una realización de la invención, hay ajustes de seguridad predeterminados asociados con cada una de las zonas. Sin embargo, estos ajustes de seguridad pueden cambiarse y configurarse de acuerdo con los ajustes basados en las necesidades de una organización y sus usuarios.

Por ejemplo, una organización puede especificar los ajustes para la manera en que un navegador maneja la visualización de contenidos, los programas de descarga y los archivos, dependiendo de la zona de la que proceda el contenido o el archivo. Por ejemplo, una organización puede confiar en que cualquier descarga dentro de su intranet corporativa es segura. Por lo tanto, los ajustes de seguridad para algunas zonas, tales como la zona (225) de máquina local o la zona (245) de intranet local pueden establecerse en un nivel bajo que permita la descarga con pocas o ninguna indicación. Sin embargo, los ajustes de seguridad para las fuentes no fiables, tales como el contenido de la zona de internet o la zona de sitios restringidos pueden ser mucho más estrictos. Por ejemplo, el usuario puede visualizar más información que indica el riesgo asociado con el contenido.

La zona de máquina local ilustrada por la ventana 205 es una zona para contenidos que existen en el ordenador local del usuario. Los contenidos encontrados en el ordenador del usuario, a excepción de los contenidos que pueden almacenarse en caché en el sistema local procedentes de una fuente no fiable, se tratan con un alto nivel de confianza. Por ejemplo, un navegador puede almacenar en caché contenidos procedentes de fuentes no fiable

obtenidas de internet. En general, se supone que todos los archivos que ya están en el ordenador local son muy seguros y, por los tanto, se les aplican unos ajustes de seguridad mínimos. De acuerdo con una realización, el elemento de seguridad puede desactivarse cuando la zona por la que se está navegando es la zona de máquina local.

Pueden añadirse y eliminarse sitios web de la zona (235) de sitios de confianza y la zona (265) de sitios restringidos. La zona (235) de sitios de confianza y la zona (265) de sitios restringidos contienen sitios en los que se confía más o menos que en los sitios de la zona de internet o la zona de intranet local.

La zona (235) de sitios de confianza hace referencia a los sitios que se cree que no son perjudiciales. Por ejemplo, se cree que el usuario puede descargar o ejecutar archivos de manera segura desde sitios contenidos dentro de la "zona de sitios de confianza" sin preocuparse de la fiabilidad de los datos. Esta zona está destinada para sitios de mucha confianza, tales como los sitios de compañeros de negocio de confianza. De acuerdo con una realización, el elemento de seguridad puede desactivarse cuando la zona por la que se está navegando es la zona de sitios de confianza.

La zona (265) de sitios restringidos es para sitios que no son de confianza y a los que se asigna un alto nivel de seguridad. Cuando un usuario está en un sitio restringido, se provee a la ventana 260 de suficiente información, de tal manera que el usuario sepa que el contenido procede de una fuente no fiable. De acuerdo con una realización, la barra (220) de estado y la barra (210) de título siempre se visualizan cuando el usuario está navegando dentro de una zona restringida.

La zona (245) de intranet local contiene habitualmente todas las direcciones que no requieren un servidor proxy, tal como se define por el administrador del sistema. Habitualmente, estas incluyen los sitios especificados por las rutas de red (tales como, \\nombre de ordenador\nombre de carpeta), y los sitios de intranet local (habitualmente direcciones que no contienen períodos, tales como http://interna). En general, puede confiarse en la zona 245 de intranet local, ya que la información en la intranet procede de la empresa del usuario. Por ejemplo, puesto que puede confiarse en los sitios de la intranet de la empresa del usuario, la organización quiere habitualmente que los usuarios puedan ejecutar todos los tipos de contenidos activos desde esta localización. De acuerdo con una realización de la invención, la barra (210) de título y la barra (220) de estado pueden desactivarse cuando el usuario está operando dentro de la zona (245) de intranet local.

La zona (255) de internet consiste en los sitios web que no se incluyen en el ordenador del usuario, en la intranet local de la empresa, o un sitio que no esté asignado a la zona de sitios de confianza o la zona de sitios restringidos. En general, los sitios localizados en internet no son de confianza. Por lo tanto, se aplica un nivel de seguridad más alto a la zona de internet. Este nivel de seguridad más alto ayuda a los usuarios a ejecutar contenidos activos y a descargar códigos en sus ordenadores. Cuando el usuario haya navegado por la zona (255) de internet, la ventana 250 tendrá la suficiente información necesaria para que el usuario sepa de dónde procede el contenido. Por ejemplo, de acuerdo con una realización, la ventana 250 incluye la barra (210) de título y la barra (220) de estado con la zona (255) de internet indicada dentro de la barra (220) de estado.

La figura 3 ilustra un contenido no fiable visualizado dentro de una ventana de navegador de confianza, de acuerdo con unos aspectos de la invención.

La ventana 300 de navegador de confianza incluye la barra 310 de título, la barra 330 de estado, la información 340 de zona, y el contenido 345 no fiable. El contenido 345 no fiable incluye la barra 350 de título con el botón 355 de cierre que está destinado a inducir al usuario a creer que al hacer clic en el botón 355 de cierre se cerrará la ventana 310 de navegador. De acuerdo con una realización de la invención, cualquier ventana que esté dentro de una zona que no sea de confianza se visualiza con la barra (330) de estado. En las zonas de mayor confianza, pueden desactivarse la barra (330) de estado de navegador y la barra (310) de título. De acuerdo con otra realización, el elemento(s) de seguridad puede no desactivarse nunca.

El contenido 345 se introduce como una ventana de publicidad a modo de ejemplo. El contenido 345 se introduce en un intento de engañar al usuario para que haga clic en el botón 355 de cierre dentro del contenido 345 en lugar de hacer clic en el botón 320 de cierre. Hacer clic en el botón 355 de cierre podría ser perjudicial para el usuario. Por ejemplo, cuando el usuario hace clic en el botón 355 de cierre ficticio, en lugar de cerrar la ventana como lo haría un navegador, puede hacerse que el usuario navegue a otra ventana, o peor, podría descargarse un virus en el ordenador del usuario. Obligar a la barra (330) de estado a visualizar el contenido no fiable ayuda a proveer al usuario de la información necesaria para distinguir dónde se origina el contenido. Como puede verse en referencia a la figura 3, el contenido 345 está claramente dentro de una ventana de navegador de confianza que tiene la barra (330) de estado en la que se informa claramente al usuario de que la ventana procede de una fuente (340) de internet.

La barra 330 de estado se visualiza por defecto con el fin de ayudar a distinguir las ventanas generadas por fuentes de confianza, tal como el sistema operativo del ordenador, y los contenidos generados por fuentes no fiables.

La actividad maliciosa se impide visualizando información y ornamentación adicionales en la ventana 300 de navegador para ayudar a garantizar que no se confunda ni se engañe al usuario final mediante el contenido 345. De

acuerdo con una realización de la invención, la información y la ornamentación adicionales son señales visuales para hacer que el contenido 345 parezca estar dentro de una ventana de página web. En el presente ejemplo, por ejemplo, si no se visualizara la barra 330 de estado, podría inducirse al usuario a creer que el contenido 345 es una ventana creada por el sistema operativo en lugar de una fuente exterior.

Cuando se abre una ventana de navegador con una barra de título, la barra de estado se visualiza por defecto con el fin de garantizar que la información de la barra de estado sea visible para el usuario. La zona (340) de seguridad se visualiza dentro de la barra 330 de estado para informar al usuario, por ejemplo, si está en la internet o en la intranet local.

La figura 4 ilustra un procedimiento para mejorar la seguridad de una ventana de navegador, de acuerdo con unos aspectos de la invención. Después de un bloque de inicio, el procedimiento fluye al bloque 410, donde se recibe una solicitud para abrir una nueva ventana. En general, la solicitud para abrir la ventana tiene unos ajustes de ventana asociados que definen las características de la ventana. En general, estos ajustes incluyen información tal como altura, anchura, localización, información de barra de desplazamiento, barra de título, información relacionada con la barra de estado, y similares.

Al moverse al bloque 420, se determinan los ajustes de seguridad asociados con la zona de seguridad. En general, los ajustes de seguridad se refieren a la zona por la que el usuario navega actualmente (véase la figura 5 y el análisis relacionado). Los ajustes de seguridad pueden usarse para determinar si se visualiza o no el elemento de seguridad.

Al trasladarse al bloque 430, los ajustes de ventana pueden modificarse basándose en los ajustes de seguridad. En general, los parámetros se modifican de tal manera que los ajustes de ventana se configuran de tal manera que haya suficiente información y ornamentación en la ventana para que el usuario sea capaz de reconocer los contenidos no fiable (véase la figura 6 y el análisis relacionado). Por ejemplo, se visualiza la barra de estado.

Al fluir al bloque 440, se visualiza la ventana. De acuerdo con una realización, la ventana se visualiza con la barra de título y la barra de estado de tal manera que el contenido pueda distinguirse claramente de la ventana de página web.

La figura 5 muestra un procedimiento para determinar los ajustes de seguridad, de acuerdo con unos aspectos de la invención. Después de un bloque de inicio, el procedimiento fluye al bloque 510 donde se determina la zona de seguridad. De acuerdo con una realización, la zona de seguridad puede ser una de entre cinco zonas, incluyendo una zona de máquina local, una zona de sitios de confianza, una zona de intranet local, una zona de internet, y una zona restringida.

Al moverse al bloque 520 de decisión, se realiza una determinación sobre si la zona es de confianza. Una zona de confianza es una zona que se considera que siempre tiene contenidos de confianza. En otras palabras, los contenidos recuperados de la zona de confianza no son maliciosos. Cuando la zona no es de confianza, el procedimiento fluye al bloque 530, donde la ventana solicitada para abrirse incluirá la ornamentación y la información necesarias para que el usuario determine que la localización del contenido procede de una fuente no fiable. De acuerdo con una realización, la barra de título y la barra de estado se visualizan para cualquier ventana que contenga un contenido de una zona no fiable. Cuando la zona es de confianza, el procedimiento fluye a un bloque final, donde termina el procesamiento. De acuerdo con otra realización, incluso cuando la zona es de confianza, la ventana incluye la ornamentación y la información necesarias para que el usuario determine que la localización del contenido procede de una fuente no fiable. A continuación, el procesamiento pasa a un bloque final y vuelve a procesar otras acciones.

La figura 6 ilustra un flujo de procedimiento para ajustar los parámetros de ventana asociados con un elemento de seguridad, de acuerdo con unos aspectos de la invención. Después de un bloque de inicio, el procedimiento fluye al bloque 610 donde se obtienen los parámetros de ventana. Como se ha tratado anteriormente, los parámetros de ventana pueden relacionarse con cualquier atributo asociado con la ventana, tal como: anchura, altura, barra de desplazamiento, colores, barra de título (activada/desactivada), barra de estado (activada/desactivada), y similares.

Al trasladarse al bloque 620, se analizan los parámetros de ventana para localizar atributos relativos a la barra de estado. De acuerdo con una realización, también se localizan los atributos de barra de título.

Al fluir al bloque 630, se activa el atributo de barra de estado. Esto ayuda a garantizar que el estado se visualizará incluso si los parámetros de ventana se han establecido para no visualizar la barra de estado.

A continuación, el procedimiento puede fluir al bloque 640 opcional, donde también se activa la barra de título. También pueden activarse y visualizarse otros atributos o información para ayudar a garantizar que la ventana contenga suficiente ornamentación e información para que el usuario determine que el contenido dentro de la ventana no es en sí una ventana. Por ejemplo, podría colocarse un borde especial alrededor de la ventana. A continuación, el procedimiento fluye a un bloque final y vuelve para procesar otras acciones.

La memoria descriptiva, los ejemplos y los datos anteriores proporcionan una descripción de la fabricación y el uso de la composición de la invención. La invención reside en las reivindicaciones anexadas a continuación en el presente documento.

REIVINDICACIONES

1. Un procedimiento para proporcionar una característica de seguridad para una ventana (300) de navegador, que comprende:

recibir una solicitud para abrir la ventana (300);
determinar un nivel de seguridad asociado con la ventana (300); y
cuando el nivel de seguridad indica que el contenido dentro de la ventana (300) procede de una fuente no fiable visualizar la ventana (300) con un elemento de seguridad que un usuario puede ver para determinar que el contenido (345) dentro de la ventana (300) procede de la fuente no fiable,

en el que el elemento de seguridad es una barra (330) de estado y comprende, además, una barra (310) de título, en el que el elemento de seguridad se desactiva cuando la zona por la que se está navegando es la zona de sitios de confianza.

2. El procedimiento de la reivindicación 1, en el que el nivel de seguridad se selecciona de entre al menos un nivel de seguridad no fiable y al menos un nivel de seguridad de confianza.

3. El procedimiento de la reivindicación 1, en el que determinar el nivel de seguridad asociado con la ventana comprende, además, determinar qué nivel de seguridad es el nivel no fiable cuando el usuario está navegando en al menos una de las siguientes zonas: una zona de internet y una zona restringida.

4. El procedimiento de la reivindicación 2, que comprende además:

examinar los atributos asociados con la solicitud para abrir la ventana;
ajustar al menos uno de los atributos dentro de la solicitud, de tal manera que el elemento de seguridad se visualice para el elemento de seguridad no fiable; y
enviar la solicitud modificada para abrir la ventana (300).

5. El procedimiento de la reivindicación 1, en el que se visualiza una zona dentro de la barra (330) de estado.

6. Un medio legible por ordenador que tiene unas instrucciones ejecutables por ordenador para proporcionar una característica de seguridad para una ventana (300) de navegador, comprendiendo las instrucciones:

recibir una solicitud para abrir la ventana (300);
determinar un nivel de seguridad asociado con la ventana (300); y
cuando el nivel de seguridad indica que el contenido dentro de la ventana (300) procede de una fuente no fiable visualizar la ventana (300) con un elemento de seguridad que un usuario pueda ver para determinar que el contenido (345) dentro de la ventana (300) procede de la fuente no fiable,

en el que el elemento de seguridad es una barra (330) de estado y comprende, además, una barra (310) de título, en el que el elemento de seguridad se desactiva cuando la zona por la que se está navegando es la zona de sitios de confianza.

7. El medio legible por ordenador de la reivindicación 6, que comprende además:

examinar los atributos asociados con la solicitud para abrir la ventana;
ajustar al menos uno de los atributos dentro de la solicitud, de tal manera que el elemento de seguridad se visualice para el elemento de seguridad no fiable; y
enviar la solicitud modificada para abrir la ventana (300).

8. El medio legible por ordenador de la reivindicación 7, en el que el nivel de seguridad se selecciona de entre al menos un nivel de seguridad no fiable y al menos un nivel de seguridad de confianza.

9. El medio legible por ordenador de la reivindicación 7, en el que determinar el nivel de seguridad asociado con la ventana comprende, además, determinar qué nivel de seguridad es el nivel no fiable cuando el usuario está navegando en al menos una de las siguientes zonas: una zona de internet y una zona restringida.

10. El medio legible por ordenador de la reivindicación 6, en el que se visualiza una zona dentro de la barra (330) de estado.

11. Un aparato para proporcionar una característica de seguridad para una ventana (300) de navegador, que comprende:

un procesador y un medio legible por ordenador;
un entorno operativo almacenado en el medio legible por ordenador y que se ejecuta en el procesador;
una pantalla; y
una aplicación que opera bajo el control del entorno operativo y que opera para realizar acciones, incluyendo:

recibir una solicitud para abrir la ventana (300);
determinar un nivel de seguridad asociado con la ventana (300); y
cuando el nivel de seguridad indica que el contenido dentro de la ventana (300) procede de una fuente no fiable, visualizar la ventana (300) con un elemento de seguridad que un usuario puede ver para determinar que el contenido (345) dentro de la ventana (300) procede de la fuente no fiable,

en el que el elemento de seguridad es una barra (330) de estado y comprende, además, una barra (310) de título,
en el que el elemento de seguridad se desactiva cuando la zona por la que se está navegando es la zona de sitios de confianza.

12. El aparato de la reivindicación 11, en el que el nivel de seguridad se selecciona de entre al menos un nivel de seguridad no fiable y al menos un nivel de seguridad de confianza.

13. El aparato de la reivindicación 12, en el que determinar el nivel de seguridad asociado con la ventana comprende, además, determinar qué nivel de seguridad es el nivel no fiable cuando el usuario está navegando en al menos una de las siguientes zonas: una zona de internet y una zona restringida.

14. El aparato de la reivindicación 11, en el que se visualiza una zona dentro de la barra (330) de estado.

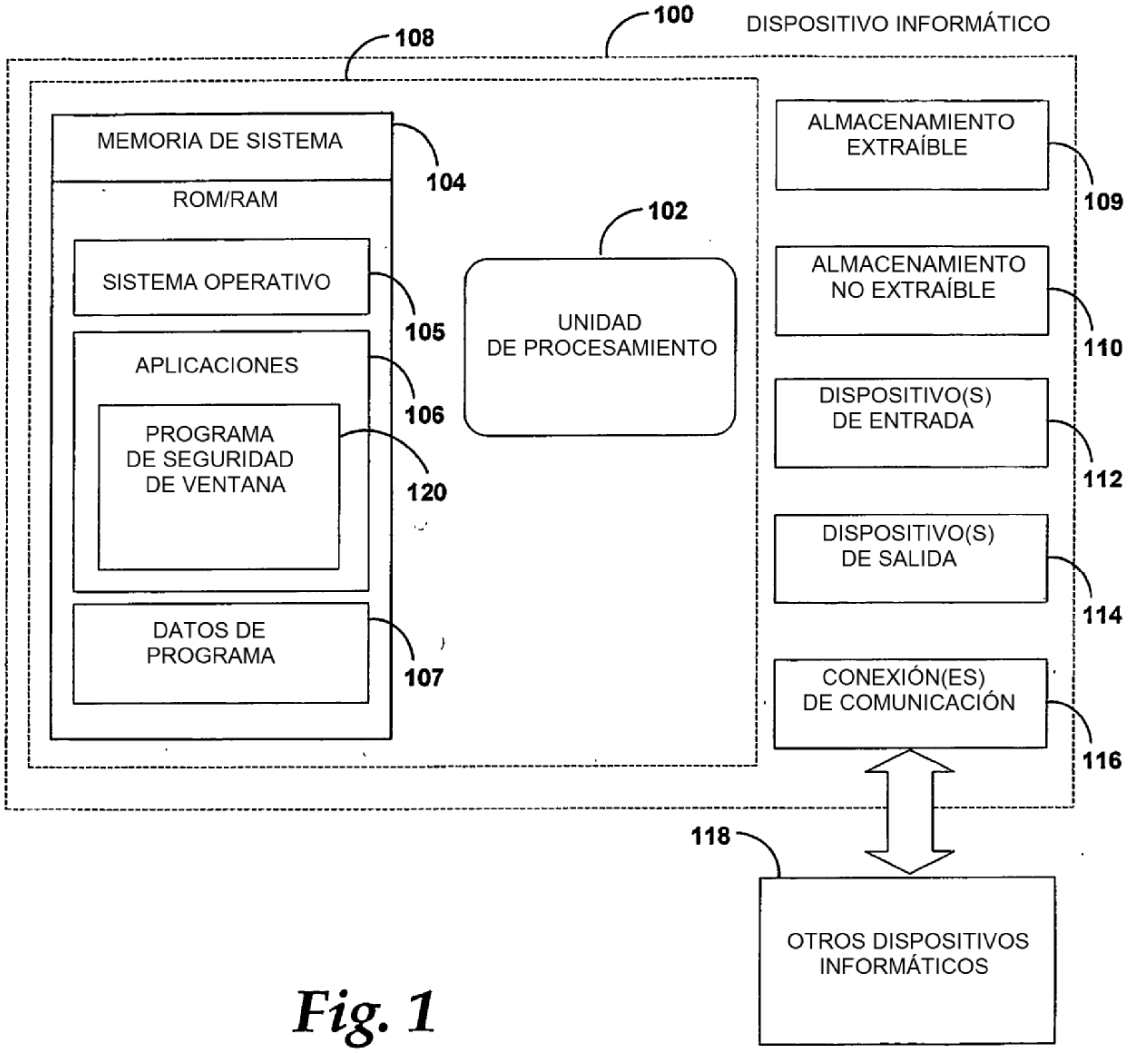
100
DISPOSITIVO INFORMÁTICO
108
MEMORIA DE SISTEMA
104
ROM/RAM
SISTEMA OPERATIVO
105
APLICACIONES
106
PROGRAMA DE SEGURIDAD DE VENTANA
120
DATOS DE PROGRAMA
107
102
UNIDAD DE PROCESAMIENTO
ALMACENAMIENTO EXTRAÍBLE
109
ALMACENAMIENTO NO EXTRAÍBLE
110
DISPOSITIVO(S) DE ENTRADA
112
DISPOSITIVO(S) DE SALIDA
114
CONEXIÓN(ES) DE COMUNICACIÓN
116
118
OTROS DISPOSITIVOS INFORMÁTICOS

Fig. 1

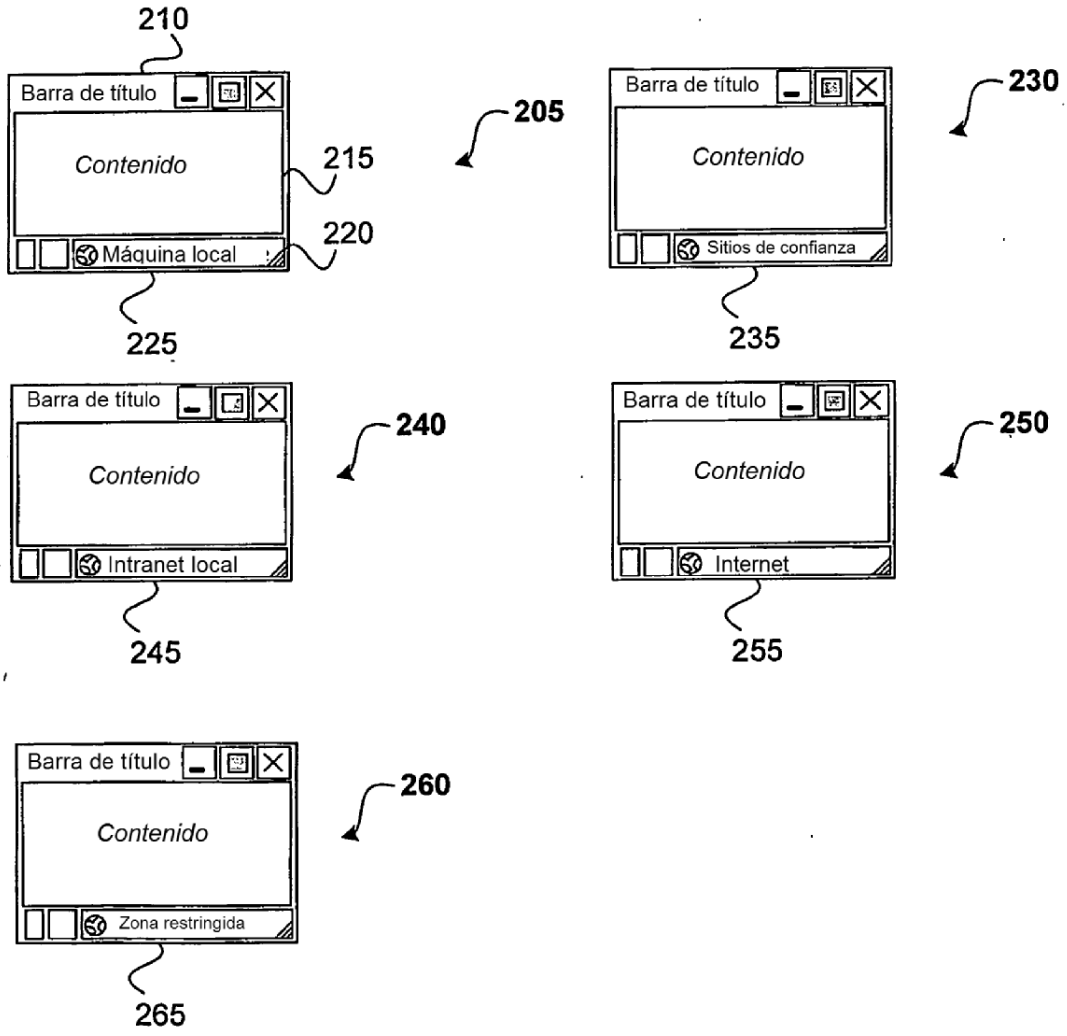
210
Barra de título
Contenido
Máquina local
215
220
225
205
Barra de título
Contenido
Sitios de confianza
230
235
Barra de título
Contenido
Intranet local
240
245
Barra de título
Contenido
Internet
250
255
Barra de título
Contenido
Zona restringida
260
265

Fig. 2

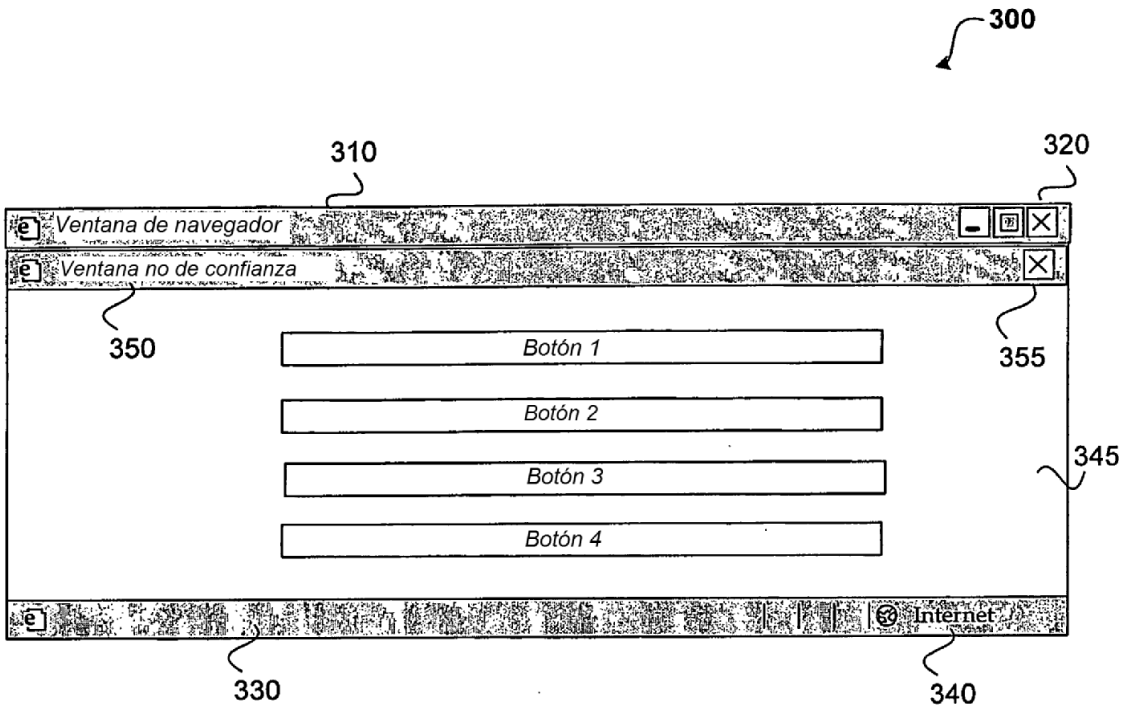
300
310
320
Ventana de navegador
Ventana no de confianza
350
355
Botón 1
Botón 2
Botón 3
Botón 4
345
Internet
330
340

Fig. 3

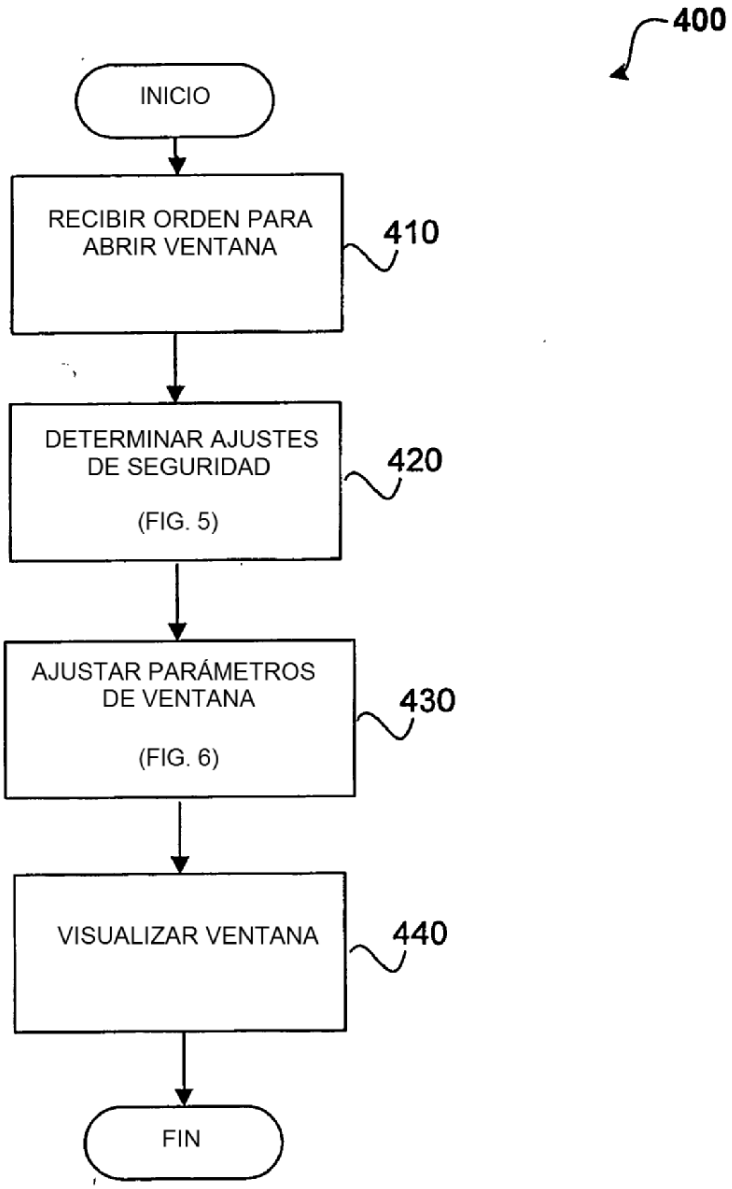
400
INICIO
RECIBIR ORDEN PARA ABRIR VENTANA
410
DETERMINAR AJUSTES DE SEGURIDAD
(FIG. 5)
420
AJUSTAR PARÁMETROS DE VENTANA
(FIG. 6)
430
VISUALIZAR VENTANA
440
FIN

Fig. 4

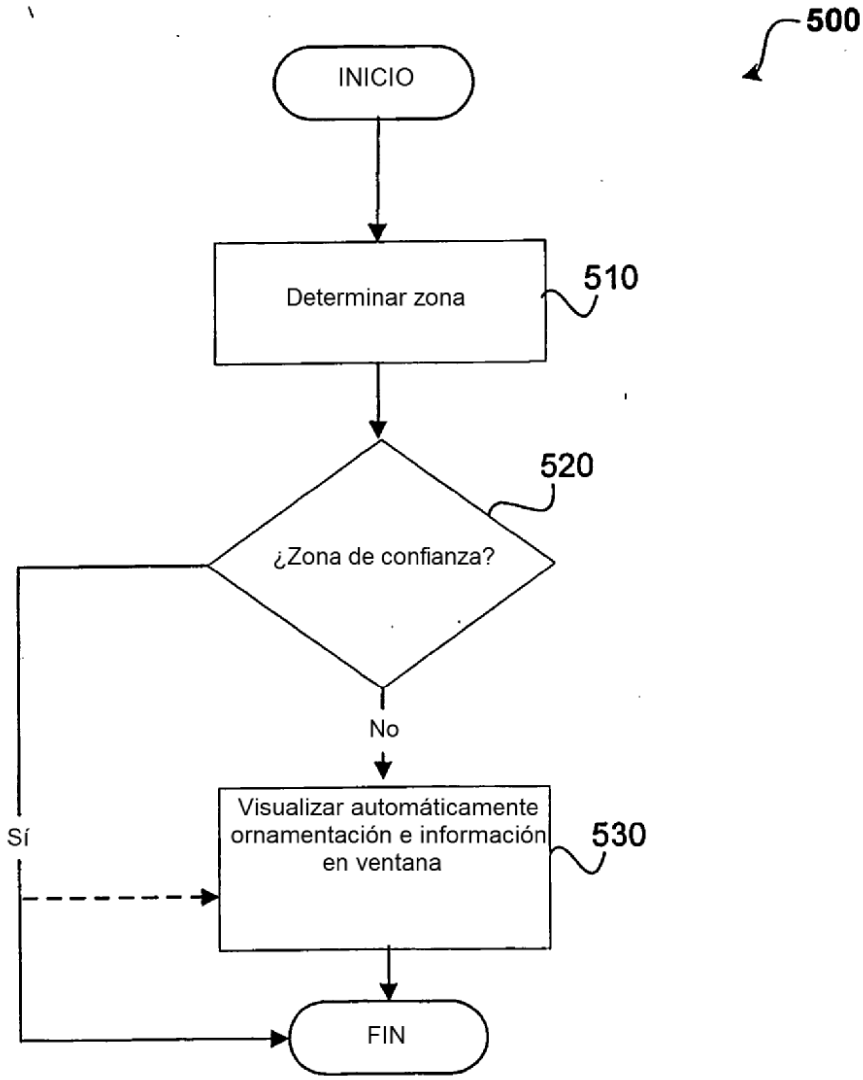
500
INICIO
Determinar zona
510
520
¿Zona de confianza?
No
Sí
Visualizar automáticamente ornamentación e información en ventana
530
FIN

Fig. 5

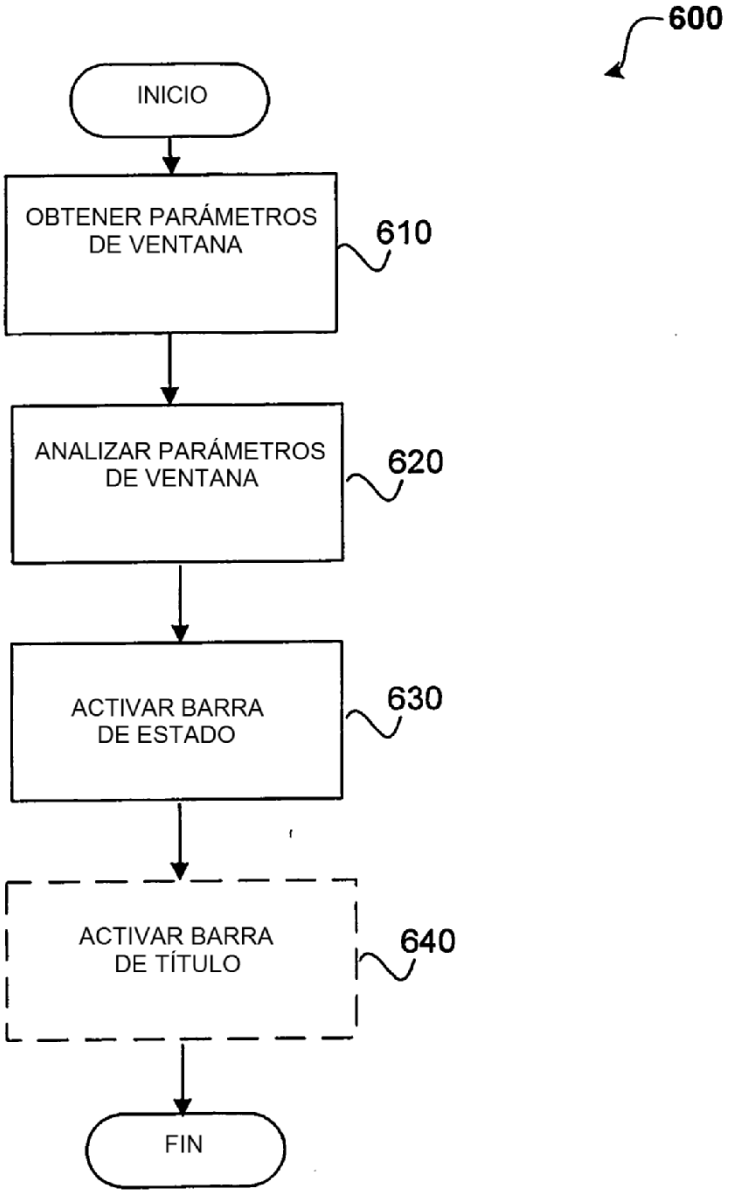
600
INICIO
OBTENER PARÁMETROS DE VENTANA
610
ANALIZAR PARÁMETROS DE VENTANA
620
ACTIVAR BARRA DE ESTADO
630
ACTIVAR BARRA DE TÍTULO
640
FIN

Fig. 6