(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 736 673**

(51) Int. CI.:

G06F 21/51 (2013.01)
G06F 21/57 (2013.01)
G06F 21/56 (2013.01)
G06F 21/52 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2013 PCT/US2013/061054**

(87) Fecha y número de publicación internacional: **04.12.2014 WO14193451**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2013 E 13771331 (9)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2019 EP 3005216**

(54) Título: **Protección de procesos antimalware**

(30) Prioridad:

31.05.2013 US 201313907331

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.01.2020

(73) Titular/es:

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

(72) Inventor/es:

PULAPAKA, HARI;
JUDGE, NICHOLAS S.;
KISHAN, ARUN U.;
SCHWARTZ, JAMES A.;
KINSHUMANN, KINSHUMANN;
LINSLEY, DAVID J.;
MAJMUDAR, NIRAJ V. y
ANDERSON, SCOTT D.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Protección de procesos antimalware

Antecedentes

Los dispositivos informáticos se han convertido cada vez más en repositorios de datos confidenciales de corporaciones y usuarios. Esto ha dado lugar a un surgimiento de usuarios malintencionados que intentan obtener acceso a estos dispositivos informáticos. Además, los usuarios malintencionados a menudo intentan instalar programas que rastrean las interacciones de los usuarios o utilizan los recursos informáticos de los dispositivos informáticos con fines maliciosos.

En consecuencia, se ha desarrollado software antimalware para impedir que estos usuarios malintencionados accedan a dispositivos informáticos. Sin embargo, los usuarios malintencionados intentan continuamente eludir la protección que brinda el software antimalware. Estos usuarios malintencionados pueden intentar operar como el software antimalware, también conocido como "falsificación" del software antimalware, interrumpir el software antimalware, etc. Una forma en que los programas maliciosos obtienen acceso al software antimalware es haciéndose pasar por un usuario administrativo. Dado que los usuarios administrativos tienen amplios permisos para interrumpir o alterar de otro modo los procesos, los usuarios malintencionados que se hacen pasar por usuarios administrativos pueden abrir un dispositivo informático para atacar deshabilitando la protección provista por el software antimalware.

El documento "Utilize Windows 8 ELAM to secure the boot process, detect rootkits", Michael Cobb, 15 de marzo de 2013, obtenido de la URL de Internet http://searchsecurity.techtarget.com/answer/Utilize-Windows8-ELAM-to-secure-the-boot-process-detect-rootkits?vgnextfmt=print, describe el Early Launch AntiMalware (ELAM), que es el primer controlador de software que se carga en el sistema operativo (OS) Windows 8. Los controladores ELAM deben pasar un conjunto de pruebas de certificación para verificar el rendimiento y otros comportamientos, después de lo cual Microsoft los firma para que el núcleo de Windows pueda iniciarlos.

El documento US2007094496 divulga sistemas y procedimientos para gestionar software malicioso en una computadora protegida. Una realización está configurada para redireccionar una llamada para crear un proceso a un monitor de procesos a nivel de núcleo, identificar un archivo asociado con el proceso y analizar el archivo para determinar si el archivo es un archivo de software malintencionado. Si el archivo es un archivo de software malintencionado, se evita que el proceso se cree. En variaciones, el monitor de proceso a nivel de núcleo es un controlador de modo de núcleo adaptado para comunicarse con una aplicación de software malicioso que reside en un nivel de usuario de memoria.

Sumario

Se describen técnicas para proteger procesos antimalware. En una o más implementaciones, un proceso antimalware asociado con un controlador antimalware se verifica, al menos en parte, en base a los certificados contenidos en un controlador antimalware. Los certificados están registrados con un sistema operativo para su uso futuro.

En una o más implementaciones, un dispositivo informático comprende uno o más procesadores y uno o más módulos implementados al menos parcialmente en hardware. El módulo o los módulos están configurados para iniciar un proceso antimalware. El módulo o los módulos también asignan el proceso antimalware a un nivel de protección definido por un firmante y un tipo de protección basado, al menos en parte, en certificados contenidos en un controlador antimalware. El módulo o los módulos también pueden ejecutar el proceso antimalware en el dispositivo informático.

En una o más implementaciones, uno o más medios de almacenamiento legibles por ordenador comprenden instrucciones almacenadas en los mismos que, en respuesta a la ejecución por parte del dispositivo informático, hacen que el dispositivo informático ejecute un módulo de protección de proceso antimalware. El módulo de protección de proceso antimalware está configurado para realizar operaciones que comprenden la verificación, durante un proceso de arranque, de un controlador antimalware asociado con un programa antimalware basado, al menos en parte, en los certificados contenidos en el controlador antimalware, conteniendo los certificados una identidad firmada con un certificado de confianza de una fuente verificada, registrando los certificados con el núcleo de un sistema operativo, verificando un proceso antimalware asociado con el programa antimalware basado, al menos en parte, en los certificados registrados y sin tener en cuenta un nivel de permiso asociado con el usuario asociado con el proceso antimalware, asignando un nivel de protección al proceso antimalware basado al menos en parte en los certificados registrados, e impidiendo que el usuario altere el proceso antimalware, incluyendo la alteración la finalización del proceso antimalware, la inyección de código o la carga de archivos binarios relacionados con el proceso antimalware.

En una o más implementaciones, un controlador antimalware se firma y luego es proporcionado a un dispositivo informático.

Este Sumario se proporciona para introducir una selección de conceptos en una forma simplificada que se describen con más detalle a continuación en la descripción detallada. Este Sumario no tiene la intención de identificar características clave o características esenciales del objeto reivindicado, ni está destinado a ser utilizado como una ayuda para determinar el alcance del objeto reivindicado.

La invención se define por el alcance de las reivindicaciones adjuntas.

Breve descripción de los dibujos

La descripción detallada se describe con referencia a las figuras adjuntas. En las figuras, el (los) dígito(s) más a la izquierda de un número de referencia identifica(n) la figura en la que aparece por primera vez el número de referencia. El uso de los mismos números de referencia en diferentes casos en la descripción y en las figuras puede indicar elementos similares o idénticos.

La FIG. 1 es una ilustración de un ejemplo de dispositivo informático que es operable para implementar las técnicas de protección de procesos antimalware descritas en el presente documento.

La FIG. 2 ilustra una jerarquía de niveles de protección relacionados con las técnicas de protección de procesos antimalware.

La FIG. 3 muestra un sistema en una implementación de ejemplo para firmar un controlador antimalware.

Las FIGS. 4A y 4B representan un procedimiento en una implementación de ejemplo para proteger procesos antimalware.

La FIG. 5 muestra un procedimiento en una implementación de ejemplo para firmar un controlador antimalware.

La FIG. 6 muestra un procedimiento en una implementación de ejemplo para proporcionar un controlador antimalware al dispositivo informático.

La FIG. 7 ilustra un sistema de ejemplo que incluye el dispositivo informático como se describe con referencia a la FIG. 1.

La FIG. 8 ilustra diversos componentes de un dispositivo de ejemplo que pueden implementarse como cualquier tipo de dispositivo informático como se describe con referencia a las FIGS. 1-7 para implementar realizaciones de las técnicas descritas en el presente documento.

Descripción detallada

Visión general

Cuando surgieron usuarios malintencionados, se desarrolló una relación entre los fabricantes de sistemas operativos y los fabricantes de software antimalware para proteger los datos de los usuarios. Sin embargo, estas técnicas tienen que desarrollarse y avanzar continuamente para abordar el desarrollo continuo de técnicas malintencionadas que se utilizan para comprometer estos datos. Las técnicas convencionales para proteger un entorno informático contra usuarios malintencionados y programas antimalware, por ejemplo, pueden no proteger el entorno informático de los ataques de los usuarios que utilizan permisos administrativos. En consecuencia, estos usuarios malintencionados pueden realizar actividades no deseadas dentro del entorno informático, tales como suspender un proceso.

En consecuencia, se describen técnicas para verificar un proceso antimalware y asignar al proceso un nivel de protección basado en una firma asociada con un controlador antimalware. De esta manera, se comprueba el código real que se está ejecutando, en lugar de los permisos de usuario asociados con un usuario que inició el proceso. Por ejemplo, puede ser más difícil "falsificar" quién firmó una parte del código que "falsificar" a un usuario.

Para permitir que el proceso antimalware aproveche estas operaciones de comprobación de código, el fabricante del sistema operativo y el fabricante de software antimalware pueden llegar a un acuerdo entre sí con respecto a lo que se considera una "firma verificada" para el controlador antimalware. El fabricante de software antimalware y el fabricante del sistema operativo, por ejemplo, pueden participar en un proceso estrechamente controlado para generar la firma verificada, y por lo tanto, la firma verificada no puede ser "falsificada" o manipulada fácilmente. Además, dado que el fabricante del sistema operativo puede usar firmas verificadas para proteger los procesos verificados por el sistema operativo a través de la jerarquía de niveles jerárquicos de protección, el uso de una firma verificada para proteger los procesos de software antimalware otorga a los procesos de software antimalware un nivel de protección acorde con la protección dada al propio sistema operativo.

Por lo tanto, el proceso de comprobación de código puede proteger el proceso del software antimalware, ya que el proceso del software antimalware protege el entorno informático de los usuarios malintencionados. En un escenario de uso de ejemplo, un proceso del software antimalware puede ser iniciado por un sistema operativo que tiene un nivel de protección reservado para los procesos del software antimalware. El nivel de protección puede incluirse

dentro de una jerarquía de niveles de protección asociados con otros procesos, o puede ser un nivel de protección reservado que opera fuera de la jerarquía de niveles de protección para otros procesos. Al asignar el proceso del software antimalware a un nivel de protección, el proceso del software antimalware puede funcionar sin tener que monitorear si otros procesos intentan alterar o manipular el proceso del software antimalware. Por lo tanto, los recursos informáticos que de otro modo serían utilizados por el proceso del software antimalware para protegerse de los ataques pueden ser liberados y utilizados por el dispositivo informático para otras operaciones.

Además, las protecciones al proceso antimalware pueden extenderse para evitar que los usuarios administrativos malintencionados finalicen o alteren de otro modo el proceso antimalware. La alteración del proceso antimalware puede incluir abrir una referencia abstracta invasiva en el proceso antimalware, inyectar código en el proceso antimalware, leer o escribir en la memoria utilizada por el proceso antimalware o acceder de otro modo al proceso antimalware.

Además, los usuarios administrativos malintencionados pueden ser motivo de preocupación, ya que los usuarios administrativos normalmente tienen permiso para realizar operaciones que son vitales para la función del dispositivo informático, tales como habilitar copias de seguridad, restaurar privilegios, apropiarse de procesos, terminar procesos e iniciar procesos desde el núcleo del sistema operativo. Las técnicas descritas en este documento pueden usarse para evitar que los usuarios administrativos malintencionados ejerzan estas operaciones contra un proceso antimalware.

Cuando se otorga un nivel de protección al proceso antimalware, el dispositivo informático puede verificar que el proceso antimalware está asociado con un programa antimalware. Por ejemplo, un sistema operativo del dispositivo informático puede verificar el proceso antimalware cargando un controlador asociado con el programa antimalware. Este controlador antimalware puede contener una firma. El sistema operativo también puede haber recibido una firma verificada de una fuente confiable. Si la firma contenida en el controlador antimalware y la firma verificada de la fuente de confianza coinciden, el proceso antimalware se verifica como legítimo y se le otorga el nivel de protección reservado para los procesos antimalware.

En la siguiente discusión, primero se describe un entorno de ejemplo que puede emplear las técnicas de protección de procesos antimalware descritas en este documento. A continuación, se describen procedimientos de ejemplo que se pueden realizar en el entorno de ejemplo, así como en otros entornos. En consecuencia, el rendimiento de los procedimientos de ejemplo no se limita al entorno de ejemplo y el entorno de ejemplo no se limita al rendimiento de los procedimientos de ejemplo.

Entorno de ejemplo

La FIG. 1 es una ilustración de un entorno 100 en una implementación de ejemplo que es operable para mantener las técnicas de protección de procesos antimalware descritas en el presente documento. El entorno 100 ilustrado incluye un dispositivo 102 informático que tiene un medio de almacenamiento legible por ordenador que se ilustra como una memoria 104 y un sistema 106 de procesamiento, aunque también se contemplan otras confirmaciones como se describe más adelante.

El dispositivo 102 informático se puede configurar de varias maneras. Por ejemplo, el dispositivo 102 informático puede configurarse como un ordenador que es capaz de comunicarse a través de una red, tal como un ordenador de sobremesa, un dispositivo de entretenimiento, un decodificador acoplado comunicativamente a un dispositivo de visualización, una consola de juegos, etc. El dispositivo 102 informático también puede configurarse como un dispositivo móvil de comunicaciones, tal como un ordenador portátil como se ilustra, una tableta, un teléfono móvil, un dispositivo de juegos portátil, un dispositivo de música portátil, un cuaderno electrónico, etc. Por lo tanto, el dispositivo 102 informático puede abarcar desde dispositivos de recursos completos con recursos substanciales de memoria y procesador (por ejemplo, ordenadores personales, consolas de juegos) hasta un dispositivo de bajos recursos con memoria limitada y/o recursos de procesamiento (por ejemplo, decodificadores tradicionales, consolas de juegos de mano) como se describe con más detalle en relación con la FIG. 7. Además, aunque se muestra un solo dispositivo 102 informático, el dispositivo 102 informático puede ser representativo de una pluralidad de dispositivos diferentes, tales como múltiples servidores utilizados por una empresa para realizar operaciones tales como un servicio web, una combinación de control remoto y descodificador, un dispositivo de captura de imágenes y una consola de juegos configurada para capturar gestos, etc.

El dispositivo 102 informático también incluye un sistema operativo. El sistema operativo está configurado para abstraer la funcionalidad subyacente del dispositivo 102 informático a los procesos que son ejecutables en el dispositivo 102 informático. Por ejemplo, el sistema operativo puede abstraer la memoria 104, el sistema 106 de procesamiento, la red y/o la funcionalidad del dispositivo de pantalla del dispositivo 102 informático, de modo que las aplicaciones puedan escribirse sin saber "cómo" se implementa esta funcionalidad subyacente. Un proceso, por ejemplo, puede proporcionar datos al sistema operativo para que sean representados y mostrados por el dispositivo de visualización sin entender cómo se puede realizar esta representación. El sistema operativo también puede representar una variedad de otras funcionalidades, tales como administrar un sistema de archivos y una interfaz de usuario que sea navegable por un usuario del dispositivo informático.

La memoria 104 se ilustra incluyendo un módulo 108 de inicio de proceso, un módulo 110 de verificación y procesos 112 en ejecución. El módulo 108 de inicio de proceso es representativo de la funcionalidad para iniciar procesos

para su ejecución en el dispositivo 102 informático, por ejemplo, un proceso 114 antimalware. El proceso 114 antimalware puede tener un atributo 116 de protección, que es el nivel de protección solicitado por el proceso 114 antimalware, cuya discusión adicional se puede encontrar en relación con la FIG. 2.

El proceso 114 antimalware se pasa luego al módulo 110 de verificación, donde el atributo 116 de protección se utiliza para obtener un nivel de protección para el proceso 114 antimalware. Por ejemplo, el módulo 110 de verificación puede contener un controlador 118 antimalware que incluye una firma 120 con un huella digital 122 y, opcionalmente, uno o más EKU 124. El módulo 110 de verificación puede utilizar la firma 120, la huella digital 122 y/o el/los EKU 124 para verificar que el proceso 114 antimalware es elegible para recibir el nivel de protección asociado con el atributo 116 de protección. Si el proceso antimalware 114 pasa la verificación por el módulo 110 de verificación, al proceso 114 antimalware se le puede otorgar un nivel de protección asociado con el atributo 116 de protección. El proceso 114 antimalware se puede agregar a los procesos 112 en ejecución.

Alternativamente, si el proceso 114 antimalware no pasa la verificación por el módulo 110 de verificación, se puede permitir al proceso antimalware ejecutarse como un proceso 128 antimalware no verificado, el proceso 114 antimalware se puede interrumpir, etc. Un proceso 128 antimalware no verificado no tiene un nivel de protección asociado, y por lo tanto no se le otorga el nivel de protección asociado con el atributo 116 de protección. Por lo tanto, el proceso 128 antimalware no verificado tiene acceso limitado al dispositivo informático y puede ser modificado por uno o más de los procesos 112 en ejecución. En consecuencia, un proceso 128 antimalware no verificado puede tratarse como una aplicación desprotegida, cuya discusión adicional también se puede encontrar en relación con la FIG. 2.

Por lo tanto, el entorno 100 puede aprovechar un proceso de acuerdo estrechamente controlado entre el fabricante del sistema operativo y el fabricante de software antimalware para asegurar el entorno 100. Este proceso, específicamente la generación del controlador antimalware, se describe con más detalle a partir de relación con la FIG. 3.

La FIG. 2 ilustra una jerarquía 200 de niveles 202 de protección asociados con las técnicas de protección de procesos antimalware. Estos niveles 202 de protección se utilizan para indicar qué procesos pueden obtener una referencia abstracta invasiva sobre qué otros procesos. En general, lo que se describirá con más detalle a continuación, los procesos con un nivel 202 de protección que se encuentran hacia la izquierda y la parte superior de la ilustración pueden obtener una referencia abstracta invasiva sobre los procesos con un nivel 202 de protección hacia la parte inferior y derecha de la ilustración. Por lo tanto, tanto el eje "x" como el eje "y" de los niveles 202 de permisos tienen importancia. En consecuencia, las líneas discontinuas en la FIG. 2 indican los diferentes niveles 202 de protección, de arriba a abajo, como se describe a continuación.

La jerarquía 200 define los tipos de protección desde el más alto al más bajo de izquierda a derecha, a saber, protegido 204, protegido leve 206, y desprotegido 208. Dentro de un tipo de protección, se identifican varios firmantes, y los firmantes que tienen un nivel de protección más alto están situados hacia la parte superior de los niveles 202 de protección. Las líneas discontinuas en la FIG. 2 indican los diferentes niveles 202 de protección asignados a los firmantes dentro del mismo tipo de protección.

En el tipo de protección protegido 204 de la FIG. 2, se identifican tres firmantes, a saber, los componentes 210 críticos del sistema operativo, los componentes 212 del sistema operativo y el contenido 214 DRM alojado. A los componentes 210 críticos del sistema operativo se les asigna el nivel de protección más alto en el dispositivo 102 informático, y generalmente consisten en el núcleo del sistema operativo más un conjunto de procesos críticos del sistema.

Dentro del tipo de protección de protegido leve 206, se identifican cuatro firmantes, a saber, los componentes 216 críticos del sistema operativo, los componentes 218 del sistema operativo, los servicios 220 antimalware y las aplicaciones 222 firmadas de la tienda virtual. Dentro del tipo de protección desprotegido 208, se identifica un firmante, a saber, las aplicaciones 224 desprotegidas.

De este modo, a cada combinación de tipo de protección y firmante se le otorga un nivel de firma único. Se puede crear una variable para almacenar los niveles de firma, que pueden tener un tamaño máximo de 4 bits en una o más implementaciones. Por ejemplo, al atributo 116 de protección se le puede asignar un valor asociado con la variable, y el proceso 114 antimalware se puede verificar mediante el módulo 110 de verificación y se le puede asignar un nivel 202 de protección en función de la información contenida en el controlador 118 antimalware, específicamente la firma 120, la huella digital 122 y el/los EKU 124.

Los procesos pueden verificarse en función de los niveles 202 de protección, en lugar de en los privilegios de usuario asociados con un usuario que intenta iniciar un proceso. Por lo tanto, el proceso 114 antimalware, incluso si es iniciado por un usuario administrativo, aún puede ser verificado por el módulo 110 de verificación en función del atributo 116 de protección y la información contenida en el controlador 118 de antimalware. Del mismo modo, el proceso 114 antimalware, incluso si es iniciado por un usuario que tiene privilegios de copia de seguridad o restauración, también puede ser verificado por el módulo 110 de verificación.

A varios procesos se les puede dar un nivel de protección asociado con un tipo de protección y un firmante. Por ejemplo, al proceso 114 antimalware se le puede otorgar un nivel de protección asociado con el tipo de protección

protegido leve 206 y con los servicios 220 antimalware del firmante, si el atributo 116 de protección está asociado con los servicios 220 antimalware. Para que un primer proceso acceda a un segundo proceso, el nivel 202 de protección del primer proceso debe ser más alto que el nivel 202 de protección del segundo proceso. Un nivel 202 de protección de un primer proceso es más alto que un nivel 202 de protección de un segundo proceso cuando tanto el tipo de protección como el firmante del primer proceso son mayores o iguales que un tipo de protección y un firmante del segundo proceso.

Por ejemplo, un proceso firmado por los componentes 210 críticos del sistema operativo con un nivel 202 de protección de protegido 204 puede alterar o acceder de otro modo a cualquier proceso en el sistema 102 informático. Además, un proceso firmado por los servicios 220 antimalware con el nivel 202 de protección protegido leve 206 puede alterar o acceder de otro modo a los procesos firmados por servicios 220 antimalware, a los procesos firmados por las aplicaciones 222 firmadas de la tienda virtual o a los procesos firmados por aplicaciones 224 desprotegidas. Del mismo modo, un proceso firmado por el contenido 214 DRM alojado puede ser limitado a modificaciones o acceso a procesos firmados por contenido 214 DRM alojado o aplicaciones 224 desprotegidas, incluso aunque el contenido 214 DRM alojado tenga un tipo de protección mayor (por ejemplo, protegido 204) que un proceso firmado por servicios 220 antimalware.

Alternativamente, a un proceso con un nivel de protección inferior se le pueden otorgar derechos de acceso limitados a un proceso con un nivel de protección superior. Por ejemplo, al proceso del nivel de protección más bajo se le puede otorgar el derecho a interrumpir un proceso con un nivel de protección más alto. Sin embargo, al proceso con el nivel de protección más bajo no se le pueden otorgar estos derechos de acceso limitado cuando el proceso del nivel de protección más alto se firma con un nivel de protección particular. Por ejemplo, los componentes 210 críticos del sistema operativo, los componentes 216 críticos del sistema operativo y los servicios 220 antimalware pueden no permitir que un proceso con un nivel de protección inferior tenga derechos de acceso limitados, tales como los derechos de terminación. Por lo tanto, la terminación del proceso 126 antimalware verificado se limita a los procesos firmados por los componentes 210 críticos del sistema operativo, por los componentes 216 críticos del sistema operativo y por los servicios 220 antimalware. Esto se puede usar para proporcionar un nivel adicional de protección al proceso 126 antimalware verificado.

Según los niveles 202 de protección descritos anteriormente, puede haber situaciones en las que dos procesos no puedan alterarse entre sí. Por ejemplo, un proceso firmado por el contenido 214 DRM alojado no puede alterar un proceso firmado por los servicios 220 antimalware, y un proceso firmado por los servicios 220 antimalware no puede alterar un proceso firmado por el contenido 214 DRM alojado. Por lo tanto, los procesos firmados por los servicios 220 antimalware o por el contenido 214 DRM alojado están aislados entre sí en los niveles 202 de protección, lo que proporciona una mayor seguridad.

Alternativamente, se puede definir un nivel 202 de protección que no esté dentro de la jerarquía de los niveles 202 de protección, lo que puede denominarse un nivel de protección reservado. Los procesos firmados con el nivel de protección reservado pueden restringir el acceso de los procesos firmados con un nivel de protección más alto. Por ejemplo, si a las aplicaciones 222 firmadas de la tienda virtual se les asigna un nivel de protección de "8" y a los servicios 220 antimalware se les asigna un nivel de protección "7", los procesos típicamente firmados por los servicios 220 antimalware no podrían restringir el acceso desde los procesos firmados por las aplicaciones 222 firmadas de la tienda virtual. Sin embargo, si a los servicios 220 antimalware se les asignó un nivel de protección reservado, los procesos firmados por los servicios 220 antimalware, tales como el proceso 126 antimalware verificado, podrían restringir el acceso desde los procesos firmados por las aplicaciones 222 firmadas de la tienda virtual.

Además, los tipos de protección pueden determinarse en función de qué tipo de procedimiento de firma se requiere para los certificados extraídos de un controlador. Por ejemplo, los niveles 202 de protección del tipo de protección protegido 204 pueden requerir un procedimiento de firma de huella digital de página. Además, los niveles 202 del tipo de protección protegido leve 206 pueden requerir un procedimiento de firma de huella digital de archivo. Por lo tanto, se puede requerir un procedimiento de firma más seguro para que un proceso reciba un tipo de protección más alto.

Además, los procesos pueden crear procesos hijo. Un proceso que ha recibido un nivel 202 de protección puede crear un proceso hijo desprotegido. El proceso que ha recibido un nivel 202 de protección solo puede pasar referencias abstractas al proceso hijo desprotegido explícitamente a través de una lista de referencias abstractas transmitidas. El proceso que ha recibido un nivel 202 de protección puede no pasar todas las referencias abstractas heredables a un proceso hijo desprotegido. Por lo tanto, un proceso que ha recibido un nivel 202 de protección puede no crear un proceso hijo desprotegido que tenga una referencia abstracta sobre un proceso con un nivel 202 de protección.

Por ejemplo, si el proceso 126 antimalware verificado creó un proceso hijo al que se le asignó un nivel de protección de aplicaciones 224 desprotegidas, se evita que el proceso 126 antimalware verificado permita que el proceso hijo tenga una referencia abstracta sobre el proceso 126 antimalware, o sobre cualquier otro proceso de los procesos 112 en ejecución que tenga un nivel 202 de protección asignado.

Alternativamente, si el proceso 126 antimalware verificado creó un proceso hijo al que se asignó un nivel de protección de aplicaciones 224 desprotegidas, el proceso 126 antimalware verificado puede pasar explícitamente

referencias abstractas individuales al proceso hijo. En esta última situación, el proceso hijo recibe una referencia abstracta sobre un proceso de los procesos en ejecución que tenía un nivel 202 de protección asignado.

La FIG. 3 muestra un sistema 300 en una implementación de ejemplo para firmar un controlador antimalware. Un fabricante 302 de software antimalware y un fabricante 304 de sistemas operativos se comunican y llegan a un acuerdo para producir una firma 306 antimalware verificada, tal como la firma 120. La firma 306 antimalware verificada se envía a un servicio 308 antimalware. El servicio 308 antimalware envía un controlador 118 antimalware a un dispositivo 102 informático. El controlador 118 antimalware puede ser independiente de la plataforma, de manera que el controlador 118 antimalware se puede utilizar en una variedad de diferentes tipos de dispositivos 102 informáticos.

Procedimientos de ejemplo

La siguiente discusión describe técnicas de protección de procesos antimalware que pueden implementarse utilizando los sistemas y dispositivos descritos anteriormente. Los aspectos de cada uno de los procedimientos pueden implementarse en hardware, en firmware o en software, o en una combinación de los mismos. Los procedimientos se muestran como un conjunto de bloques que especifican las operaciones realizadas por uno o más dispositivos y no están necesariamente limitados a las órdenes mostradas para realizar las operaciones por los respectivos bloques. En partes de la siguiente discusión, se puede hacer referencia a los entornos 100 y 300 de las FIGS. 1 y 3, y a los niveles 200 de protección de la FIG. 2, respectivamente.

Las FIGS. 4A y 4B representan un procedimiento 400 para verificar que un proceso antimalware puede ejecutarse en un nivel de protección específico. Por ejemplo, el proceso 114 antimalware que busca un nivel 202 de protección asociado con el atributo 116 de protección puede ser verificado por el módulo 110 de verificación, que utiliza el controlador 118 antimalware.

Un dispositivo informático recibe un certificado de confianza de una fuente verificada (bloque 402). El certificado de confianza puede incluir una identidad asociada con el certificado, que indica la fuente verificada. La fuente verificada puede ser, por ejemplo, un fabricante 302 de software antimalware. Alternativamente, la fuente verificada puede ser, por ejemplo, el controlador 118 antimalware. El controlador antimalware puede ser una fuente verificada ya que el controlador 118 antimalware contiene la firma 306 antimalware verificada. La firma 306 antimalware verificada es de confianza porque proviene del fabricante 302 de software antimalware.

El dispositivo informático recibe el controlador 118 antimalware (bloque 404). El controlador 118 antimalware puede enviarse desde un creador de un programa antimalware, tal como un fabricante o proveedor de un programa 302 antimalware. La instalación del controlador 118 antimalware no requiere un reinicio del dispositivo 102 informático.

El dispositivo 102 informático carga el controlador 118 antimalware durante un proceso de arranque (bloque 406). El controlador 118 antimalware se puede volver a registrar durante cada proceso de arranque. Un fabricante 304 de sistema operativo puede definir una estructura estándar para el controlador 118 antimalware, y esta estructura se puede pasar entre el módulo 108 de inicio de proceso y el módulo 110 de verificación. Alternativamente, el dispositivo 102 informático puede cargar el controlador 118 antimalware durante la instalación de un programa antimalware.

El dispositivo informático extrae una identidad del controlador antimalware (bloque 408). La identidad puede estar asociada con el fabricante 302 de software antimalware. La identidad puede comprender una huella digital para mejorar aún más la seguridad. La huella digital puede tener un requisito mínimo de huella digital que puede ser SHA256 por defecto.

El dispositivo 102 informático determina que la identidad extraída del controlador 118 antimalware está firmada con el certificado de confianza recibido desde la fuente verificada (bloque 410). Este apretón de manos asegura que el controlador 118 antimalware sea legítimo.

El dispositivo informático extrae certificados del controlador 118 antimalware (bloque 412). Estos certificados pueden utilizarse para verificar que un proceso antimalware sea legítimo, de modo que el proceso antimalware no sea el resultado de un ataque de un programa malware o de un usuario malintencionado. Los certificados pueden designar una identidad de un fabricante 302 antimalware.

El dispositivo informático registra los certificados extraídos con un núcleo de un sistema operativo (bloque 414). Esto proporciona protección adicional para los certificados, ya que el acceso al núcleo es limitado. Se puede acceder a estos certificados desde el núcleo a través de las interfaces de programas de aplicación (API). Estas API no se exportan desde el núcleo.

El dispositivo 102 informático inicia el proceso 114 antimalware (bloque 416). El proceso 114 antimalware puede tener un atributo 116 de protección asociado, que designa un nivel de protección buscado.

El dispositivo informático verifica que el proceso 114 antimalware es legítimo, en función de los certificados previamente registrados con el núcleo del sistema operativo.

La verificación puede no usar una ruta. No usar una ruta evita que el código malicioso cambie un archivo debajo de la llamada para verificar el archivo y luego extraer los certificados del archivo. Si el proceso 114 antimalware se verifica con éxito, al proceso 126 antimalware verificado se le asigna un nivel 202 de protección (bloque 418). La verificación puede no tener éxito si el atributo 116 de protección busca un nivel de protección que no está incluido en los niveles 202 de protección. El proceso de verificación es asíncrono, de modo que otros controladores no pueden retrasar la finalización de una carga a través del proceso de verificación.

Se impide que un usuario altere el proceso 126 antimalware verificado (bloque 420). Esto incluye evitar que un usuario administrativo altere el proceso 126 antimalware verificado. Específicamente, para alterar el proceso 126 antimalware verificado, el proceso que intenta acceder al proceso 126 antimalware verificado debe tener un nivel 202 de protección que sea mayor o igual que el nivel de protección asociado con el proceso 126 antimalware verificado.

Como se discutió anteriormente y se muestra en la FIG. 2, para tener un nivel de protección que sea mayor que un proceso firmado por un servicio 220 antimalware, un proceso debe ser firmado por uno de entre: un componente 210 crítico del sistema operativo con un nivel de protección de protegido 204, un componente 216 crítico del sistema operativo con un nivel de protección protegido leve 206, un componente 212 del sistema operativo con un nivel de protección protegido 204, o un componente 218 del sistema operativo con un nivel de protección protegido leve 206. Así, incluso los procesos firmados por un fabricante 304 del sistema operativo pueden no tener acceso a los procesos firmados por los servicios 220 antimalware. Los procesos firmados por un servicio 220 antimalware pueden tener acceso a los procesos firmados por un servicio antimalware diferente.

La FIG. 5 muestra un procedimiento 500 en una implementación de ejemplo para la firma del controlador 118 antimalware por un fabricante 302 de software antimalware. El fabricante 302 de software antimalware firma el controlador 118 antimalware con la firma 306 antimalware verificada (bloque 502). Esta firma puede realizarse utilizando una CA pública o una CA privada.

El controlador 118 antimalware se firma utilizando una CA pública (bloque 504). Por ejemplo, el fabricante 302 de software antimalware puede utilizar un producto CA tal como VeriSign. Como resultado de esta firma, el fabricante 302 de software antimalware podría proporcionar una huella digital de su certificado de editor de software para ayudar en la protección del proceso antimalware. Cuando se utiliza una CA pública, se requiere que el fabricante 302 de software antimalware actualice el controlador 118 antimalware y el programa antimalware cada vez que se alcance un nuevo acuerdo con el fabricante 304 del sistema operativo. El nuevo acuerdo puede dar lugar a que se emitan nuevos certificados para el fabricante 302 de software antimalware.

El controlador 118 antimalware se firma utilizando una CA privada (bloque 506). Cuando se utiliza una CA privada, el fabricante 302 de software antimalware no está obligado a actualizar el controlador 118 antimalware y el programa antimalware cada vez que se alcance un nuevo acuerdo con el fabricante 302 del sistema operativo.

Como resultado de la firma en 506, el fabricante 302 de software antimalware podría suministrar la huella digital del certificado de CA y uno o más EKU al controlador 118 antimalware (bloque 508). El servicio 308 antimalware proporciona el controlador 118 antimalware firmado al dispositivo 102 informático (bloque 510).

La FIG. 6 un procedimiento 600 en una implementación de ejemplo para proporcionar un controlador antimalware al dispositivo informático. Se genera un controlador 410 antimalware para el servicio 308 antimalware (bloque 602). Se genera una firma basada, al menos en parte, en un acuerdo entre el fabricante 302 de software antimalware y el fabricante 304 del sistema operativo (bloque 604). El controlador 118 antimalware está firmado con la huella digital que identifica al fabricante 302 de software antimalware (bloque 606). El controlador 118 antimalware se proporciona al dispositivo 102 informático (bloque 608).

Sistema y dispositivo de ejemplo

La FIG. 7 ilustra un sistema 700 de ejemplo que incluye el dispositivo 102 informático como se describe con referencia a la FIG. 1. El sistema 700 de ejemplo permite entornos ubicuos para una experiencia de usuario sin contratiempos cuando se ejecutan aplicaciones en un ordenador personal (PC), en un dispositivo de televisión y/o en un dispositivo móvil. Los servicios y las aplicaciones se ejecutan de manera substancialmente similar en los tres entornos para una experiencia de usuario común cuando se realiza la transición de un dispositivo al siguiente mientras se utiliza una aplicación, se juega un juego de vídeo, se ve un vídeo, etc.

En el sistema 700 de ejemplo, múltiples dispositivos están interconectados a través de un dispositivo informático central. El dispositivo informático central puede ser local a los múltiples dispositivos o puede estar ubicado de manera remota desde los múltiples dispositivos. En una realización, el dispositivo informático central puede ser una nube de uno o más servidores que están conectados a los múltiples dispositivos a través de una red, Internet u otro enlace de comunicación de datos. En una realización, esta arquitectura de interconexión permite que la funcionalidad se entregue a través de múltiples dispositivos para proporcionar una experiencia común y sin contratiempos a un usuario de los múltiples dispositivos. Cada uno de los múltiples dispositivos puede tener diferentes requisitos físicos y capacidades, y el dispositivo informático central utiliza una plataforma para permitir la entrega de una experiencia al dispositivo que a la vez está adaptada al dispositivo y es común a todos los dispositivos. En una realización, se crea una clase de dispositivos de destino y las experiencias se adaptan a la

clase genérica de dispositivos. Una clase de dispositivos puede definirse por características físicas, tipos de uso u otras características comunes de los dispositivos.

En diversas implementaciones, el dispositivo 102 informático puede asumir una variedad de configuraciones diferentes, tales como para los usos de ordenador 702, móvil 704 y televisión 706. Cada una de estas configuraciones incluye dispositivos que pueden tener construcciones y capacidades generalmente diferentes, y por lo tanto el dispositivo 102 informático puede configurarse conforme a una o más de las diferentes clases de dispositivos. Por ejemplo, el dispositivo 102 informático puede implementarse como la clase de ordenador 702 de un dispositivo que incluye un ordenador personal, un ordenador de sobremesa, un ordenador multipantalla, un ordenador portátil, un netbook, etc.

El dispositivo 102 informático también puede implementarse como la clase de dispositivo móvil 704 que incluye dispositivos móviles, tales como un teléfono móvil, un reproductor de música portátil, un dispositivo de juegos portátil, una tableta, un ordenador multipantalla, etc. El dispositivo 102 informático también puede implementarse como la clase de dispositivo de televisión 706 que incluye dispositivos que tienen o están conectados a pantallas generalmente más grandes en entornos de visualización informales. Estos dispositivos incluyen televisores, descodificadores, consolas de juegos, etc. Las técnicas descritas en el presente documento pueden estar admitidas por estas diversas configuraciones del dispositivo 102 informático y no están limitadas a los ejemplos específicos de las técnicas descritas en el presente documento.

La nube 708 incluye y/o es representativa de una plataforma 710 para los servicios 712 de contenido. La plataforma 710 extrae la funcionalidad subyacente del hardware (por ejemplo, los servidores) y los recursos de software de la nube 708. Los servicios 712 de contenido pueden incluir aplicaciones y/o datos que pueden utilizarse mientras el procesamiento del ordenador se ejecuta en servidores que están alejados del dispositivo 102 informático. Los servicios 712 de contenido se pueden proporcionar como un servicio a través de Internet y/o a través de una red de suscriptores, tales como una red de telefonía móvil o una res Wi-Fi.

La plataforma 710 puede extraer recursos y funciones para conectar el dispositivo 102 informático con otros dispositivos informáticos. La plataforma 710 también puede servir para extraer la escala de recursos para proporcionar un nivel de escala correspondiente a la demanda encontrada para los servicios 712 de contenido que se implementan a través de la plataforma 710. Por consiguiente, en una realización de dispositivo interconectado, la implementación de la funcionalidad de la funcionalidad descrita en el presente documento puede distribuirse por todo el sistema 700. Por ejemplo, la funcionalidad puede implementarse en parte en el dispositivo 102 informático, así como a través de la plataforma 710 que extrae la funcionalidad de la nube 708.

La FIG. 8 ilustra diversos componentes de un dispositivo 800 de ejemplo que pueden implementarse como cualquier tipo de dispositivo informático como se describe con referencia a las FIGS. 1-8 para implementar realizaciones de las técnicas descritas en el presente documento. El dispositivo 800 incluye dispositivos 802 de comunicación que permiten la comunicación por cable y/o inalámbrica de los datos 804 del dispositivo (por ejemplo, datos recibidos, datos que se están recibiendo, datos programados para su retransmisión, paquetes de datos de los datos, etc.). Los datos 804 del dispositivo u otro contenido del dispositivo pueden incluir ajustes de configuración del dispositivo, contenido multimedia almacenado en el dispositivo y/o información asociada con un usuario del dispositivo. El contenido multimedia almacenado en el dispositivo 800 puede incluir cualquier tipo de audio, vídeo y/o datos de imagen. El dispositivo 800 incluye una o más entradas 806 de datos a través de las cuales se puede recibir cualquier tipo de datos, contenido multimedia y/o entradas, tales como entradas que pueden ser seleccionadas por el usuario, mensajes, música, contenido de medios de televisión, contenido de vídeo grabado y cualquier otro tipo de audio, vídeo y/o datos de imagen recibidos desde cualquier fuente de datos y/o contenido.

El dispositivo 800 también incluye interfaces 808 de comunicación que pueden implementarse como una cualquiera o más de entre: una interfaz en serie y/o paralela, una interfaz inalámbrica, cualquier tipo de interfaz de red, un módem y cualquier otro tipo de interfaz de comunicación. Las interfaces 808 de comunicación proporcionan una conexión y/o enlaces de comunicación entre el dispositivo 800 y una red de comunicación mediante la cual otros dispositivos electrónicos, informáticos y de comunicación se comunican datos con el dispositivo 800.

El dispositivo 800 incluye uno o más procesadores 810 (por ejemplo, cualesquiera de los microprocesadores, controladores y similares) que procesan varias instrucciones ejecutables por el ordenador para controlar el funcionamiento del dispositivo 800 y para implementar realizaciones de las técnicas descritas en el presente documento. De manera alternativa o adicional, el dispositivo 800 puede implementarse con una cualquiera o con una combinación de hardware, firmware o circuitos lógicos fijos que se implementa en conexión con los circuitos de control y procesamiento que generalmente se identifican en 812. Aunque no se muestra, el dispositivo 800 puede incluir un sistema de bus o sistema de transferencia de datos que acopla los diversos componentes dentro del dispositivo. Un bus de sistema puede incluir una cualquiera o una combinación de diferentes estructuras de bus, tales como un bus de memoria o un controlador de memoria, un bus periférico, un bus de serie universal y/o un procesador o bus local que utiliza una cualquiera de una variedad de arquitecturas de bus.

El dispositivo 800 también incluye medios legibles por ordenador 814, tales como uno o más componentes de memoria, ejemplos de los cuales incluyen la memoria de acceso aleatorio (RAM), la memoria no volátil (por ejemplo, una o más memorias de entre: solo lectura (ROM), memoria instantánea, EPROM, EEPROM, etc.) y un dispositivo de almacenamiento en disco. Un dispositivo de almacenamiento en disco puede implementarse como cualquier tipo

de dispositivo de almacenamiento magnético u óptico, tal como una unidad de disco duro, un disco compacto (CD) grabable y/o regrabable, cualquier tipo de disco digital versátil (DVD) y similares. El dispositivo 800 también puede incluir un dispositivo 816 de almacenamiento masivo.

Los medios 814 legibles por ordenador proporcionan mecanismos de almacenamiento de datos para almacenar los datos 804 del dispositivo, así como diversas aplicaciones 818 del dispositivo y cualquier otro tipo de información y/o datos relacionados con los aspectos operativos del dispositivo 800. Por ejemplo, un sistema 820 operativo puede mantenerse como una aplicación de ordenador con los medios 814 legibles por ordenador y ejecutarse en los procesadores 810. Las aplicaciones 818 de dispositivo pueden incluir un administrador de dispositivo (por ejemplo, una aplicación de control, una aplicación de software, un módulo de procesamiento de señales y control, un código que es nativo a un dispositivo en particular, una capa de extracción de hardware para un dispositivo en particular, etc.). Las aplicaciones 818 de dispositivos también incluyen cualquier componente del sistema o módulos para implementar las realizaciones de las técnicas descritas en el presente documento. En este ejemplo, las aplicaciones 818 de dispositivo incluyen un módulo 822 de inicio de proceso y un módulo 824 de verificación que se muestran como módulos de software y/o aplicaciones de ordenador. Puede haber módulos de software adicionales que se utilizan para proporcionar una interfaz con un dispositivo configurado para capturar entradas, tales como una pantalla táctil, un panel de control, una cámara, un micrófono, etc. De manera alternativa o adicional, el módulo 822 de inicio de proceso y el módulo 824 de verificación pueden implementarse como hardware, software, firmware o cualquier combinación de los mismos. Además, los módulos de software adicionales pueden configurarse para admitir múltiples dispositivos de entrada, tales como dispositivos separados para capturar entradas visuales y de audio, respectivamente.

El dispositivo 800 también incluye un sistema 826 de entrada y salida de audio y/o vídeo que proporciona datos de audio a un sistema 828 de audio y/o proporciona datos de vídeo a un sistema 830 de visualización. El sistema 828 de audio y/o el sistema 830 de visualización pueden incluir cualquier dispositivo que procese, muestre y/o que de otro modo represente datos de audio, vídeo e imágenes. Las señales de vídeo y las señales de audio se pueden comunicar desde el dispositivo 800 a un dispositivo de audio y/o a un dispositivo de visualización a través de un enlace de RF (radio frecuencia), de un enlace de S-vídeo, de un enlace de vídeo compuesto, de un enlace de vídeo componente, de DVI (interfaz de vídeo digital), de una conexión de audio analógico u de otro enlace de comunicación similar. En una realización, el sistema 828 de audio y/o el sistema 830 de pantalla se implementan como componentes externos al dispositivo 800. Alternativamente, el sistema 828 de audio y/o el sistema 830 de pantalla se implementan como componentes integrados del dispositivo 800 de ejemplo.

Conclusión

Aunque la invención se ha descrito en un lenguaje específico para características estructurales y/o actuaciones metodológicas, debe entenderse que la invención definida en las reivindicaciones adjuntas no se limita necesariamente a las características o actuaciones específicas descritas. Por el contrario, las características y las actuaciones específicas se describen como formas de ejemplo de implementación de la invención reivindicada.

REIVINDICACIONES

1. Un procedimiento que comprende:

recibir (402), mediante un dispositivo (102) informático, un certificado de confianza de una fuente verificada;

extraer (408), mediante el dispositivo informático (102), una identidad de un controlador (118) antimalware;

determinar (410), mediante el dispositivo (102) informático, que la identidad está firmada con el certificado de confianza;

registrar (414), mediante el dispositivo (102) informático, los certificados extraídos del controlador (118) antimalware con un sistema operativo;

iniciar (416), mediante el dispositivo (102) informático, un proceso (114) antimalware asociado con el controlador (118) antimalware; verificar, mediante (102) el dispositivo informático, el proceso (114) antimalware en función, al menos en parte, de los certificados contenidos en el controlador (118) antimalware; y asignar (418), mediante el dispositivo (102) informático, un nivel de protección a dicho proceso (114) antimalware si el proceso (114) antimalware se verifica con éxito, para evitar que el proceso (114) antimalware sea alterado por un proceso diferente con un nivel de protección más bajo, estando dicho nivel de protección especificado por dicho proceso (114) antimalware.

2. El procedimiento de la reivindicación 1, en el que la alteración incluye interrumpir, inyectar código o cargar archivos binarios relacionados con el proceso antimalware.

3. El procedimiento de la reivindicación 1, en el que el proceso antimalware se inicia durante un proceso de arranque.

4. El procedimiento de la reivindicación 1, en el que los certificados se registran con un núcleo del sistema operativo.

5. El procedimiento de la reivindicación 1, en el que la verificación del proceso antimalware se produce sin tener en cuenta una cuenta de usuario que está intentando cargar el proceso.

6. El procedimiento de la reivindicación 1, que comprende además la asignación de un nivel de protección definido por un firmante y un tipo de protección al proceso antimalware en función, al menos en parte, de los certificados.

7. Un dispositivo informático (102) que comprende:

uno o más procesadores;

un módulo (108) de inicio de proceso configurado para iniciar un proceso (114) antimalware; un módulo (110) de verificación configurado para extraer una identidad de un controlador (118) antimalware asociado con el proceso (114) antimalware, para determinar que la identidad está firmada con un certificado de confianza de una fuente verificada, para verificar el proceso (114) antimalware en función de los certificados contenidos en el controlador (118) antimalware, y para asignar un nivel de protección definido por un firmante y un tipo de protección al proceso (114) antimalware si el proceso (114) antimalware se verifica con éxito, para evitar que el proceso (114) antimalware sea alterado por un proceso diferente con un nivel de protección más bajo, siendo dicho nivel de protección especificado por dicho proceso (114) antimalware; y

un módulo (112) de procesos en ejecución configurado para ejecutar el proceso antimalware en el dispositivo informático.

8. El dispositivo informático como se describe en la reivindicación 7, en el que el proceso antimalware tiene un nivel de protección mayor si tanto el firmante como el tipo de protección asociado con el proceso antimalware tienen un nivel de protección más alto que el firmante y un tipo de protección asociado con otro proceso.

9. El dispositivo informático como se describe en la reivindicación 7, en el que el firmante está asociado con uno de entre:

los componentes críticos del sistema operativo;

los componentes regulares del sistema operativo;

los componentes antimalware;

los componentes asociados con aplicaciones

firmadas por entidades reconocidas;

los componentes de alojamiento DRM; y

los componentes desprotegidos.

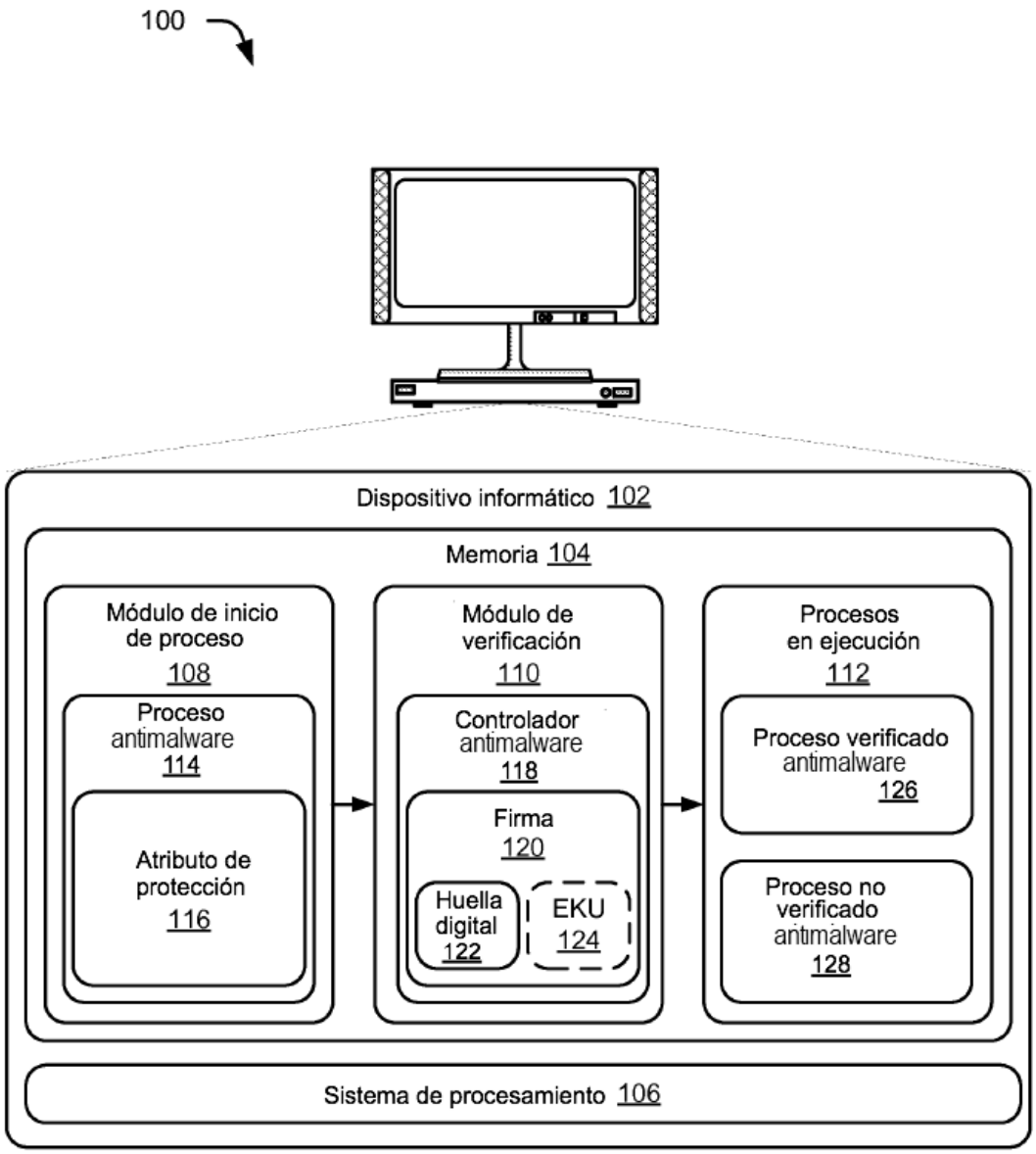
100
Dispositivo informático 102
Memoria 104
Módulo de inicio de proceso
108
Proceso antimalware
114
Atributo de protección
116
Módulo de verificación
110
Controlador antimalware
118
Firma
120
Huella digital
122
EKU
124
Procesos en ejecución
112
Proceso verificado antimalware
126
Proceso no verificado antimalware
128
Sistema de procesamiento 106

Fig. 1

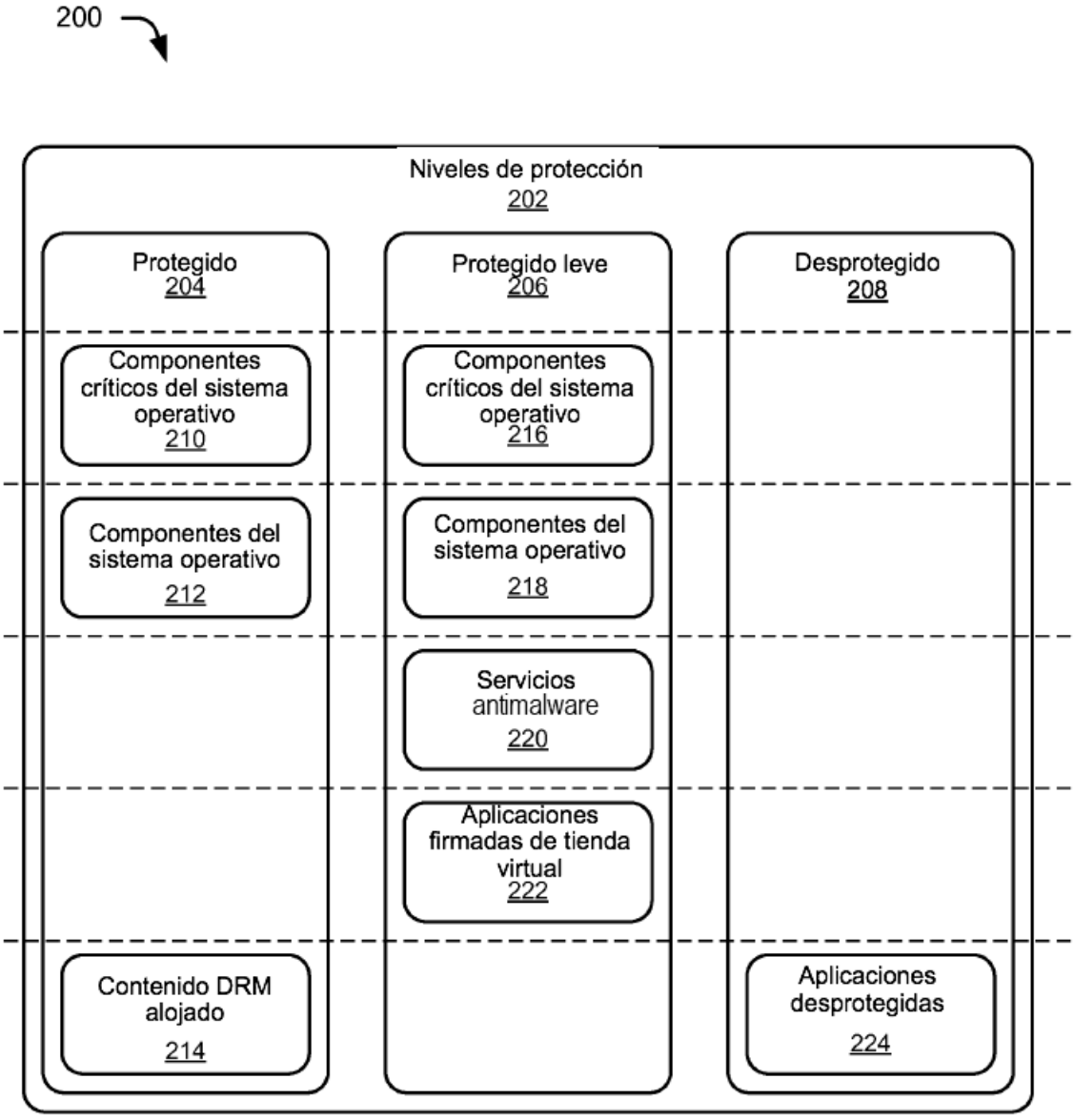
200
Niveles de protección
202
Protegido
204
Protegido leve
206
Desprotegido
208
Componentes críticos del sistema operativo
210
Componentes críticos del sistema operativo
216
Componentes del sistema operativo
212
Componentes del sistema operativo
218
Servicios antimalware
220
Aplicaciones firmadas de tienda virtual
222
Contenido DRM alojado
214
Aplicaciones desprotegidas
224

Fig. 2

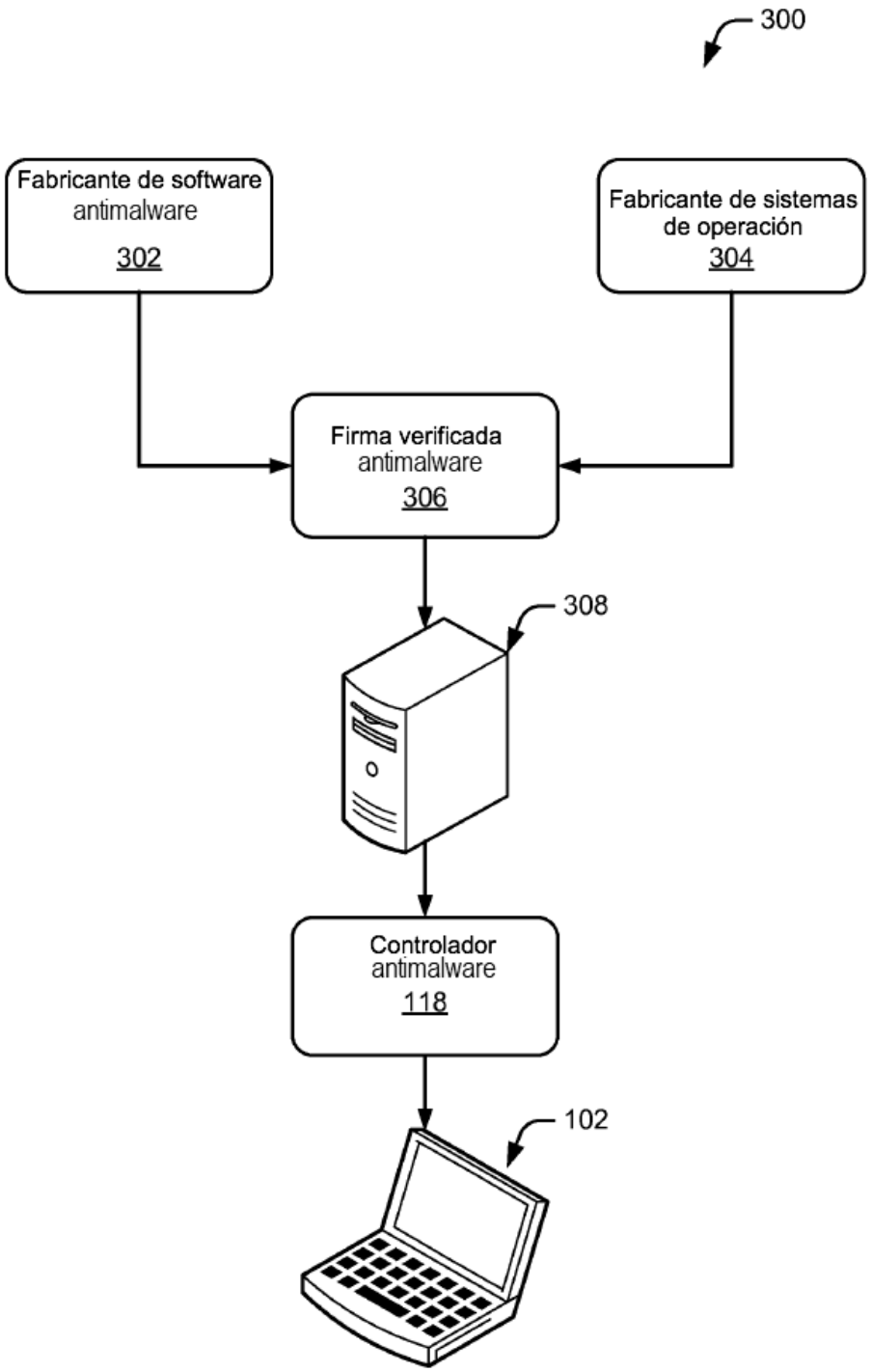
300
Fabricante de software antimalware 302
Fabricante de sistemas de operación 304
Firma verificada antimalware 306
308
Controlador antimalware 118
102

Fig. 3

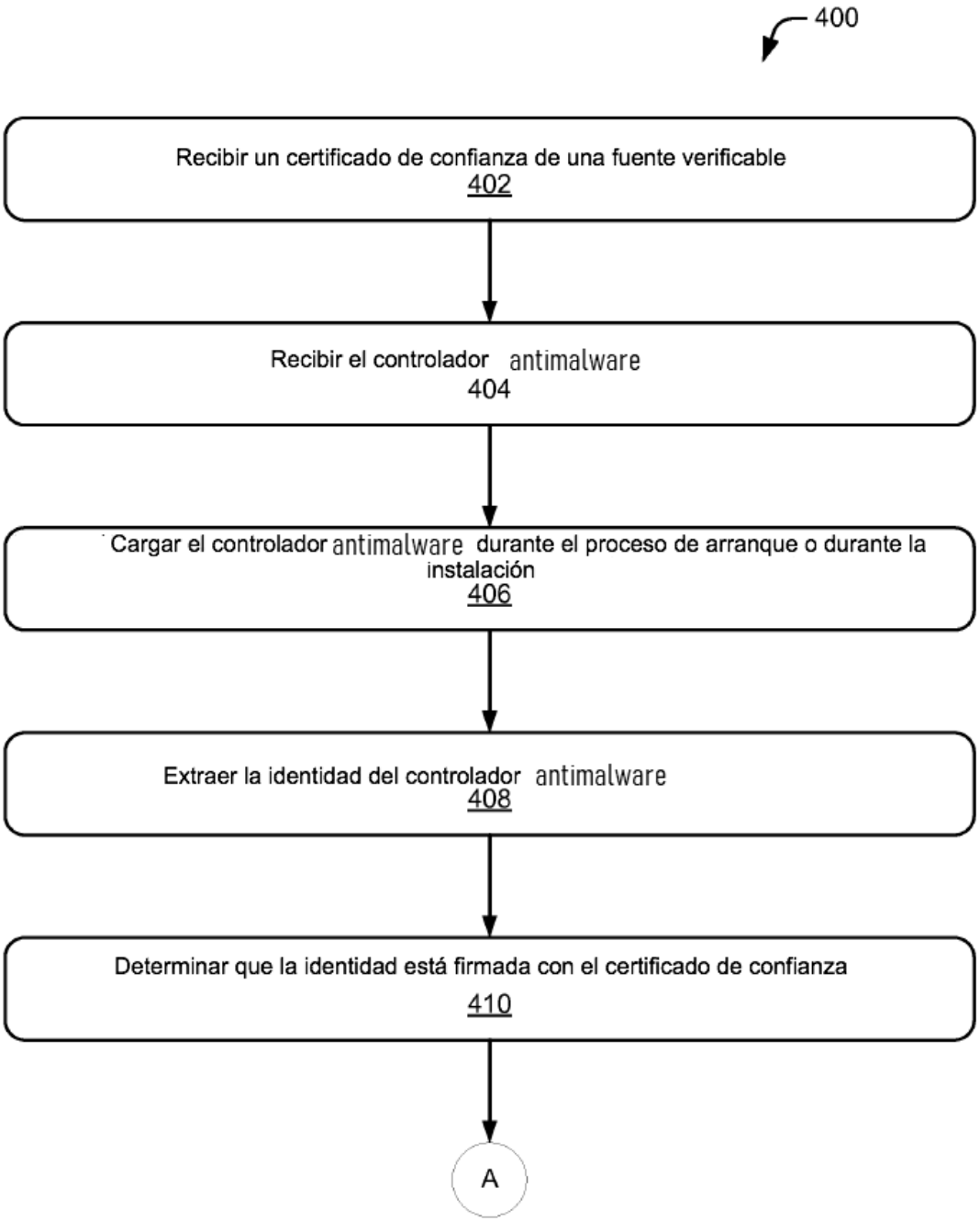
400
Recibir un certificado de confianza de una fuente verificable
402
Recibir el controlador antimalware
404
Cargar el controlador antimalware durante el proceso de arranque o durante la instalación
406
Extraer la identidad del controlador antimalware
408
Determinar que la identidad está firmada con el certificado de confianza
410
A

Fig. 4A

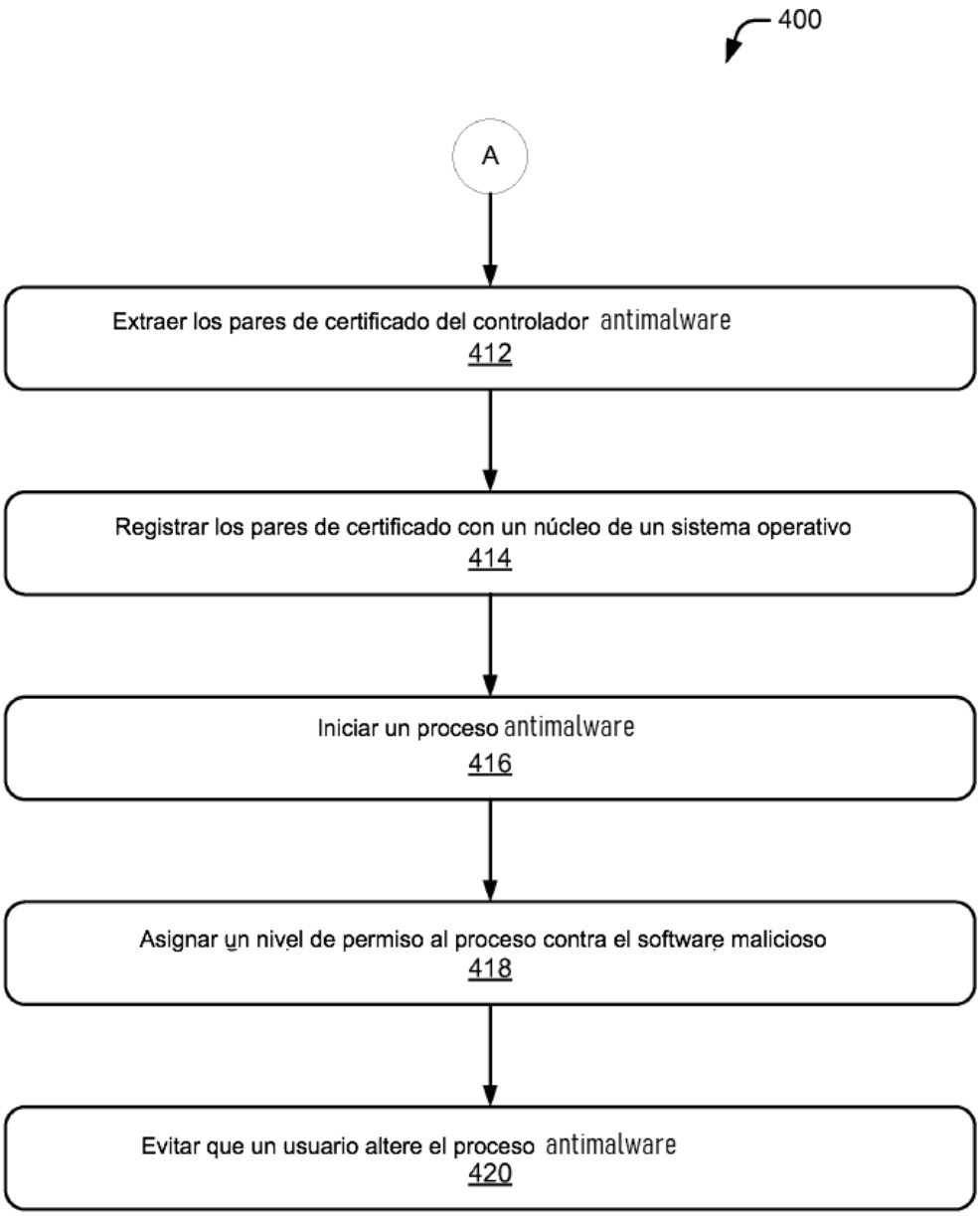
400
A
Extraer los pares de certificado del controlador antimalware
412
Registrar los pares de certificado con un núcleo de un sistema operativo
414
Iniciar un proceso antimalware
416
Asignar un nivel de permiso al proceso contra el software malicioso
418
Evitar que un usuario altere el proceso antimalware
420

Fig. 4B

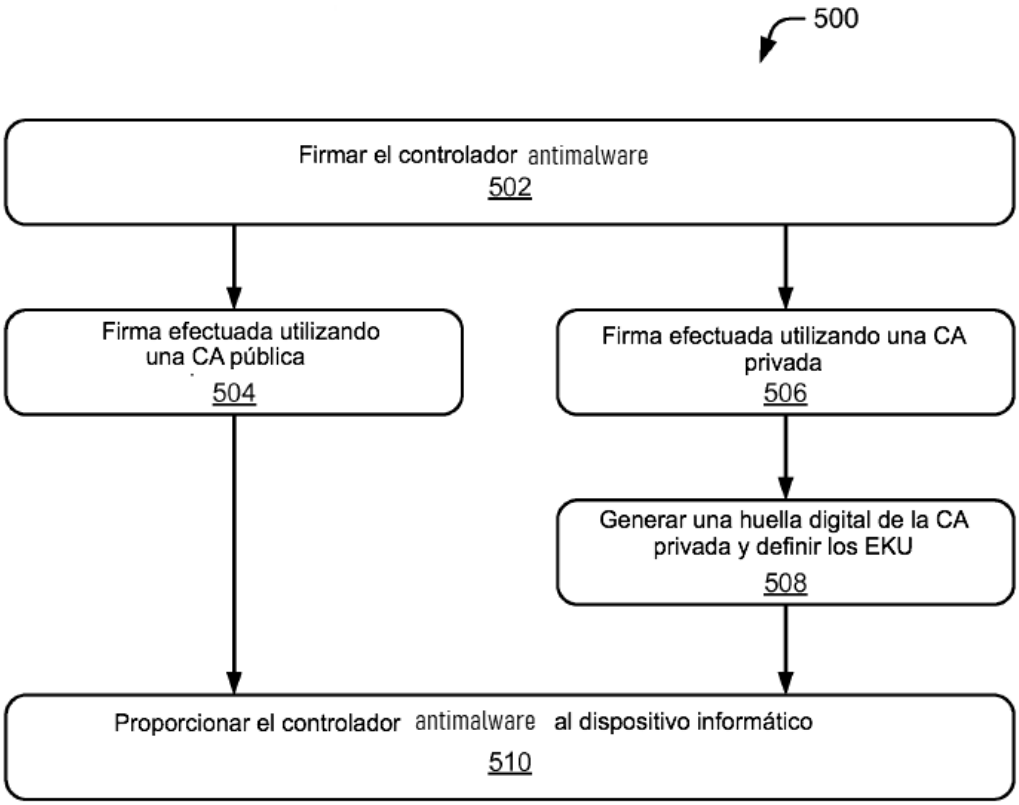
500
Firmar el controlador antimalware
502
Firma efectuada utilizando una CA pública
504
Firma efectuada utilizando una CA privada
506
Generar una huella digital de la CA privada y definir los EKU
508
Proporcionar el controlador antimalware al dispositivo informático
510

Fig. 5

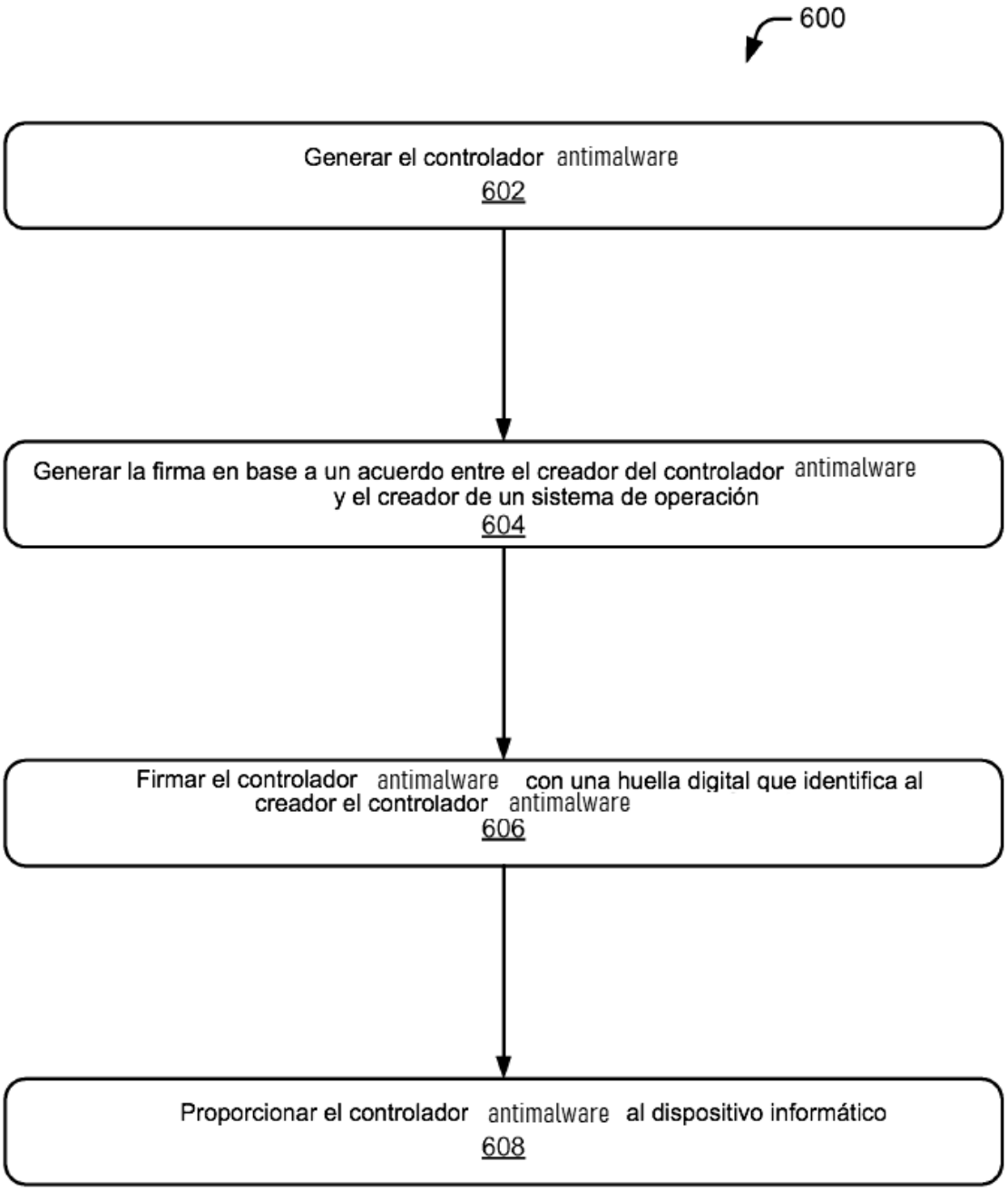
600
Generar el controlador antimalware
602
Generar la firma en base a un acuerdo entre el creador del controlador antimalware y el creador de un sistema de operación
604
Firmar el controlador antimalware con una huella digital que identifica al creador el controlador antimalware
606
Proporcionar el controlador antimalware al dispositivo informático
608

Fig. 6

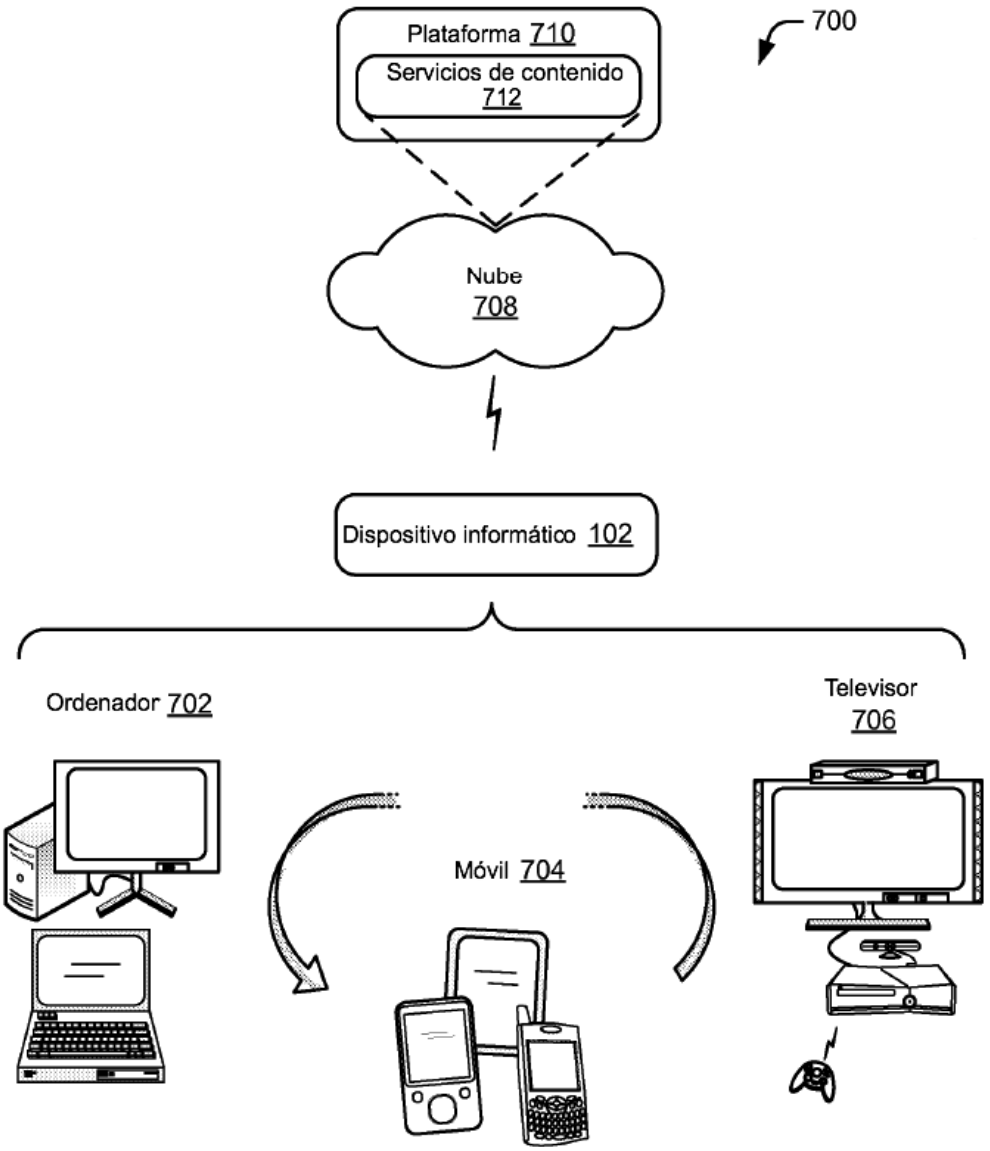
700
Plataforma 710
Servicios de contenido 712
Nube 708
Dispositivo informático 102
Ordenador 702
Televisor 706
Móvil 704

Fig. 7

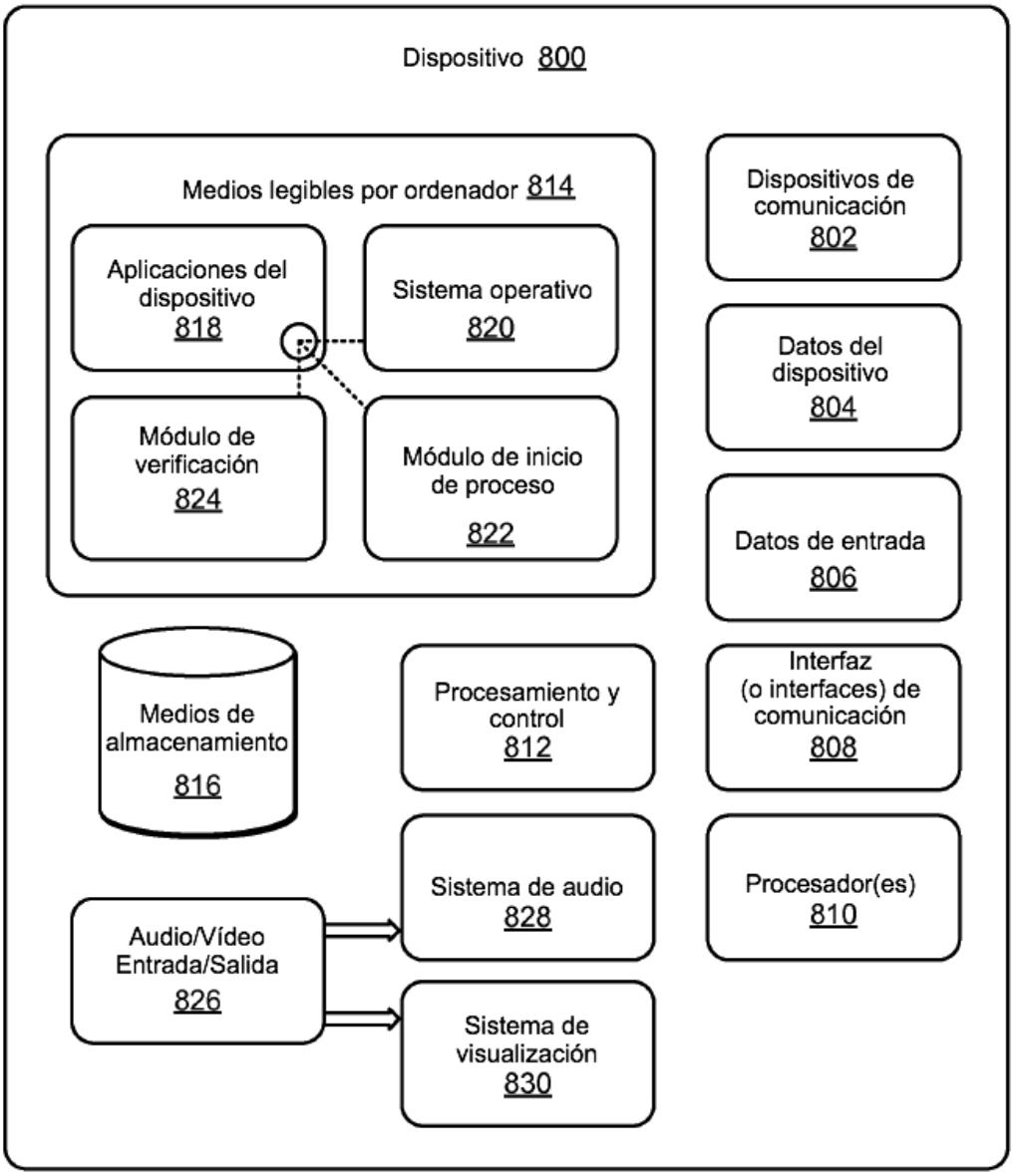
Dispositivo 800
Medios legibles por ordenador 814
Aplicaciones del dispositivo 818
Sistema operativo 820
Módulo de verificación 824
Módulo de inicio de proceso 822
Dispositivos de comunicación 802
Datos del dispositivo 804
Datos de entrada 806
Interfaz (o interfaces) de comunicación 808
Procesador(es) 810
Medios de almacenamiento 816
Procesamiento y control 812
Sistema de audio 828
Audio/Vídeo Entrada/Salida 826
Sistema de visualización 830

Fig. 8