(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 683 074**

(51) Int. CI.:

G06F 12/14 (2006.01)
G06F 9/455 (2008.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.12.2007 PCT/US2007/087225**

(87) Fecha y número de publicación internacional: **31.07.2008 WO08091452**

(96) Fecha de presentación y número de la solicitud europea: **12.12.2007 E 07869154 (0)**

(97) Fecha y número de publicación de la concesión europea: **13.06.2018 EP 2115570**

(54) Título: **Agentes de protección y modos de privilegio**

(30) Prioridad:

25.01.2007 US 627320

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.09.2018

(73) Titular/es:

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

(72) Inventor/es:

TRAUT, ERIC;
FOLTZ, FORREST;
THORNTON, ANDREW y
SINHA, SUYASH

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Agentes de protección y modos de privilegio

Antecedentes

Los procesadores en dispositivos informáticos a menudo incluyen modos privilegiados y modos no privilegiados. El software que se ejecuta en un modo privilegiado en general puede ejecutar cada instrucción soportada por el procesador. Típicamente, el núcleo del sistema operativo se ejecuta en el modo privilegiado, que en ocasiones se denomina como "Anillo 0", "Modo de Supervisor", o "Modo de Núcleo".

En contraste, algún software que se ejecute en el dispositivo informático puede estar restringido a ejecutarse únicamente en un modo no privilegiado. Este modo en general permite que el software ejecute un subconjunto de las instrucciones del procesador. Un sistema operativo puede por lo tanto usar el modo no privilegiado para limitar la actividad de software que se ejecuta en este modo. Por ejemplo, el software puede estar restringido a un subconjunto particular de la memoria del dispositivo informático. Este modo no privilegiado en ocasiones es conocido como "Anillo 3" o "Modo de Usuario". En general, las aplicaciones de usuario de dispositivo informático operan en este modo no privilegiado.

Si una aplicación de software opera en este modo no privilegiado, la aplicación puede solicitar acceso a una porción de memoria que no puede accederse directamente desde el modo no privilegiado. La aplicación puede desear realizar, por ejemplo, una operación en esta porción de memoria tal como "crear un nuevo fichero". Esta solicitud se encamina típicamente a través de una puerta de llamada u otra instrucción de llamada de sistema, que pasa este código de modo no privilegiado a código de modo privilegiado. Este paso asegura que el modo no privilegiado no tiene acceso directo a memoria que está designada como accesible desde modo privilegiado únicamente.

De acuerdo con estos modos, un autor de código malicioso puede acceder al modo privilegiado e instalar software maligno que cambia el comportamiento del dispositivo informático. Este software maligno puede modificar, por ejemplo, la localización de ficheros, ficheros ocultos, modificar ficheros, cambiar pulsaciones de teclas o similares. Alguno de este software maligno puede comprender un "encubridor de inicio" (rootkit), que no cambia únicamente el comportamiento del dispositivo informático sino también se oculta a sí mismo en la memoria del modo privilegiado. Las aplicaciones de antivirus que se ejecutan en el dispositivo informático pueden en consecuencia fallar al descubrir este encubridor de inicio oculto, permitiendo por lo tanto que el software maligno continúe sus acciones maliciosas. Adicionalmente, tal software maligno puede parchearse a través de un sistema de protección integrado del sistema operativo, como se analiza a continuación.

Un autor de software maligno puede acceder al modo privilegiado y cargar software maligno en un dispositivo informático en una diversidad de maneras, incluyendo engañando al usuario del dispositivo informático para que instale inconscientemente el software maligno en el propio dispositivo informático del usuario. Como resultado, los sistemas operativos actuales a menudo emplean uno o más sistemas de protección para detectar tal software maligno. Estos sistemas de protección en general monitorizan ciertos recursos de sistema operativo importantes para detectar cualquier cambio a estos recursos. Si un sistema de protección de este tipo detecta un cambio de este tipo, entonces el sistema de protección puede decidir que el recurso particular ha sido infectado por software maligno. Estos sistemas de protección pueden proporcionar también, a la aplicación de antivirus del usuario, una lista de aplicaciones actualmente residentes en la memoria del modo no privilegiado. Por supuesto, si el software maligno estaba oculto con éxito, entonces no aparecerá en la lista proporcionada. Adicionalmente, si el software maligno tuvo éxito al parchear el sistema de protección, entonces el sistema de protección puede fallar al ejecutar o de otra manera fallar al detectar cualquier cambio a los recursos de sistema operativo importantes.

Aunque estos sistemas de protección pueden ser eficaces, también sufren de unas pocas debilidades. En primer lugar, estos sistemas se basan a menudo en la oscuridad y por lo tanto son vulnerables a que se aprovechen si se identifican por el software maligno. Es decir, si el software maligno descifra la identidad de, y localiza el sistema de protección, puede desactivar el mismo sistema de protección. El autor de software maligno puede enseñar a otros cómo hacer lo mismo. Adicionalmente y relacionado con lo primero, estos sistemas de protección operan en general en un mismo dominio de protección que el del sistema operativo (por ejemplo, en el mismo modo privilegiado). Por lo tanto, el sistema de protección se ve sometido a sí mismo a ataque si el software maligno obtiene acceso al modo privilegiado y puede desenmascarar el sistema de protección oscurecido. Finalmente, estos sistemas de protección se inicializan al mismo tiempo que el sistema operativo o el modo privilegiado. Por lo tanto, si el software maligno o el autor de software maligno obtiene control del dispositivo informático antes de esta inicialización, puede evitar que se inicialice el sistema de protección.

El documento WO 2006/063274 A1 se refiere a técnicas para ejecutar componentes de un monitor de máquina virtual a un nivel de privilegio reducido. La funcionalidad de un monitor de máquina virtual (VMM) tradicional se particiona en una pequeña parte dependiente de la plataforma denominada un micro-hipervisor (MH) y una o más partes independientes de plataforma denominadas máquinas virtuales de servicio (SVM). El MH es un módulo que sirve de solicitud de intermediario entre máquinas virtuales, incluyendo SVM, y aplica aislamiento y políticas de seguridad. El micro-hipervisor se ejecuta en el modo más privilegiado. El micro-hipervisor puede implementarse

como un módulo que se carga de manera temprana en el arranque de sistema, se lanza como un controlador desde un SO de anfitrión o como parte del firmware de sistema. En un ejemplo, hay dos niveles de privilegio de máquina virtual. El nivel de privilegio de máquina virtual más alto se denomina como operación de raíz mientras que el nivel de privilegio de máquina virtual inferior se denomina como una operación no de raíz. La VMM o el micro-hipervisor se ejecutan en operación de raíz. El micro-hipervisor proporciona a una SVM la capacidad de acceder a componentes de la plataforma de hardware subyacente que no son accesibles para todas las VM. El micro-hipervisor proporciona funcionalidad de seguridad necesaria para asegurar la integridad del sistema de máquina virtual sin interacciones con una VM de servicio.

El documento EP 1271313 A2 se refiere a técnicas para ejecutar un procedimiento. Un procedimiento se ejecuta directamente en un sistema operativo anfitrión, hasta que el procedimiento intenta una operación que puede afectar a la seguridad del sistema operativo anfitrión. Un sistema operativo invitado se proporciona a continuación ejecutándose como una sesión de máquina virtual en un compartimento del sistema operativo anfitrión y que ejecuta el procedimiento continuo usando el sistema operativo de invitado. Las operaciones del procedimiento que pueden afectar la seguridad del sistema operativo anfitrión se realizan en su lugar en el sistema operativo de invitado, proporcionando mayor seguridad. El sistema operativo invitado se invoca únicamente de manera selectiva, conduciendo a mayor eficacia global.

El documento US 2007/005919 A1 se refiere a la protección de sistemas informáticos. Un sistema informático protegido comprende un monitor de máquina virtual, una máquina virtual y un sistema de protección. El monitor de máquina virtual está configurado para virtualizar al menos una porción de hardware del sistema informático. La máquina virtual está configurada como un cliente del monitor de máquina virtual y se ejecuta en un sistema operativo invitado. El sistema de protección está acoplado al monitor de máquina virtual y está configurado para evitar el acceso de escritura al área de memoria por un sistema operativo invitado de núcleo que se ejecuta dentro de la máquina virtual.

Sumario

Es el objeto de la presente invención mejorar la seguridad de los sistemas de la técnica anterior. Este objeto se soluciona mediante la materia objeto de las reivindicaciones independientes. Se definen realizaciones preferidas en las reivindicaciones dependientes.

El presente documento describe herramientas que pueden hacer una porción de memoria de sistema operativo asociada con un agente de protección inalterable o inaccesible de un modo de privilegio de sistema operativo. En algunas realizaciones, estas herramientas pueden crear un modo de privilegio de agente de protección solicitando que un monitor de máquina virtual proteja esta porción de memoria de sistema operativo. En otras realizaciones, estas herramientas pueden crear el modo de privilegio de agente de protección virtualizando un procesador físico en múltiples procesadores virtuales, al menos uno de los cuales es un procesador virtual de agente de protección designado para ejecutar el agente de protección. Haciendo esta porción de memoria de sistema operativo inalterable o inaccesible desde el modo de privilegio de sistema operativo, el agente de protección puede ser menos vulnerable a ataques por entidades que operan en el modo de privilegio de sistema operativo.

Este resumen se proporciona para introducir una selección de conceptos en una forma simplificada que se describen adicionalmente a continuación en la descripción detallada. Este sumario no se pretende para identificar características clave o esenciales de la materia objeto reivindicada, ni se pretende que se use como una ayuda al determinar el alcance de la materia objeto reivindicada. El término "herramientas", por ejemplo, puede hacer referencia a sistema o sistemas, procedimiento o procedimientos, instrucciones legibles por ordenador, y/o técnica o técnicas según se permite por el contexto anterior y a través de todo el documento.

Breve descripción de los dibujos

La Figura 1 ilustra un entorno de operación ejemplar en el que pueden operar diversas realizaciones de las herramientas.

La Figura 2 demuestra derechos de memoria de dispositivo informático variables de los módulos ilustrados en la Figura 1.

La Figura 3 representa porciones de memoria de dispositivo informático variables en las que residen algunos de los módulos ilustrados en la Figura 1.

La Figura 4 es un diagrama de flujo que ilustra una manera ejemplar en la que un monitor de máquina virtual puede proteger una porción de memoria asociada con un agente de protección y establecer un temporizador para ejecutar el agente.

La Figura 5 ilustra una arquitectura ejemplar que tiene un monitor de máquina virtual que puede virtualizar procesadores físicos en múltiples procesadores virtuales de sistema operativo y un procesador virtual de agente de protección.

La Figura 6 ilustra cómo el ancho de banda de los procesadores físicos de la Figura 5 puede asignarse entre los diversos procesadores virtuales.

La Figura 7 es un procedimiento ejemplar que ilustra algunas maneras en las que las herramientas pueden activar y ejecutar un agente de protección que reside en una localización que es inaccesible desde un modo de

privilegio de sistema operativo.

La Figura 8 es un procedimiento ejemplar que ilustra algunas maneras en las que las herramientas pueden modificar un monitor de máquina virtual para activar y ejecutar un agente de protección que reside en una localización que es inaccesible desde un modo de privilegio de sistema operativo.

La Figura 9 es un procedimiento ejemplar que ilustra algunas maneras en las que las herramientas pueden crear un modo de privilegio de agente de protección haciendo una solicitud a un monitor de máquina virtual.

La Figura 10 es un procedimiento ejemplar que ilustra algunas maneras en las que las herramientas pueden crear un modo de privilegio de agente de protección virtualizando un procesador informático real en procesadores informáticos virtuales, al menos uno de los cuales es para ejecutar un agente de protección.

La Figura 11 es un procedimiento ejemplar que ilustra algunas maneras en las que las herramientas pueden activar una adición de un modo de privilegio no presente en un procesador físico subyacente.

Los mismos números se usan a través de toda la divulgación y las figuras para hacer referencia a componentes y características similares.

Descripción detallada

Vista general

El siguiente documento describe herramientas que pueden operar un agente de protección de tal manera que hacen al agente de protección inalterable o inaccesible desde un modo de privilegio de sistema operativo. Estas herramientas por lo tanto posibilitan protección del mismo agente de protección, asegurando de esta manera la capacidad del agente de protección para detectar modificaciones a recursos de sistema operativo importantes. Además, estas herramientas pueden apagar un sistema operativo o un modo de privilegio de sistema operativo en respuesta a detectar modificaciones de recursos o en respuesta a una modificación intentada del mismo agente de protección. Adicionalmente, estas herramientas pueden posibilitar que el agente de protección aplique invariancia en recursos de sistema operativo, sin la necesidad de detectar modificación de recursos posteriormente.

Un entorno en el que las herramientas pueden posibilitar estas y otras acciones se expone a continuación en una sección titulada *Entorno de operación ejemplar.* Sigue una sección titulada *Agentes de protección autónomos* e incluye dos sub-secciones. La primera sub-sección, titulada *Agentes de protección de monitor de máquina virtual,* describe una manera ejemplar en la que un agente de protección puede residir y ejecutarse en un monitor de máquina virtual. Esta es seguida por otra sub-sección, titulada *Agentes de protección de partición virtual,* que describe una manera ejemplar en la que un agente de protección puede ocupar y ejecutarse en una partición virtual separada de una partición del sistema operativo.

Sigue otra sección titulada *Modos de privilegio de agente de protección autónomos* y también incluye dos sub-secciones. La primera sub-sección describe una manera ejemplar que un temporizador de monitor de máquina virtual puede añadir un modo de privilegio de agente de protección a un procesador subyacente, y se titula *Solicitudes de protección a un monitor de máquina virtual.* Sigue una sub-sección titulada *Procesadores virtuales de agente de protección* y describe otra manera en la que puede crearse un modo de privilegio de agente de protección, en este caso con el uso de múltiples procesadores virtuales, incluyendo uno configurado para ejecutar el agente de protección en el modo de privilegio de agente de protección. Sigue una sección titulada *Uso ejemplar de las herramientas* y describe un ejemplo de las herramientas previamente descritas en la operación. Finalmente, una sección titulada *Otras realizaciones de las herramientas* describe diversas otras realizaciones y maneras en las que pueden actuar las herramientas. Esta vista general, incluyendo estos títulos de sección y resúmenes, se proporciona para la conveniencia del lector y no se pretende que limite el alcance de las reivindicaciones o las secciones tituladas.

Entorno de operación ejemplar

Antes de describir las herramientas en detalle, se proporciona el siguiente análisis de un entorno de operación ejemplar para ayudar al lector a entender algunas maneras en las que pueden emplearse diversos aspectos inventivos de las herramientas. El entorno descrito a continuación constituye solamente un ejemplo y no se pretende para limitar la aplicación de las herramientas a un entorno de operación particular cualquiera. Pueden usarse otros entornos sin alejarse del alcance de la materia objeto reivindicada. Por ejemplo, aunque las siguientes secciones describen realizaciones con un agente de protección, pueden utilizarse también múltiples agentes de protección. En algunos casos, estos agentes de protección pueden ejecutarse independientemente y en cooperación. En tales casos, los agentes de protección típicamente pueden únicamente acceder a memoria en su respectiva partición. Adicionalmente, las técnicas descritas a continuación pueden utilizarse de manera concurrente. Es decir, diferentes agentes de protección pueden utilizar diferentes técnicas dentro de un mismo entorno de operación.

Volviendo al ejemplo actual, la Figura 1 ilustra un entorno de operación ejemplar de este tipo en general en 100. Este entorno incluye un dispositivo 102 informático, que por sí mismo incluye uno o más procesadores 104 así como el medio 106 legible por ordenador. El medio 106 legible por ordenador incluye un monitor 108 de máquina virtual (por ejemplo, un hipervisor), que puede posibilitar la virtualización del uno o más procesadores en múltiples procesadores virtuales. El monitor 108 de máquina virtual puede posibilitar también múltiples particiones virtuales. Uno o más

procesadores pueden estar asociados con cada partición, y estos procesadores virtuales se planifican en los procesadores físicos disponibles. Como se ilustra, en algunas realizaciones el monitor de máquina virtual puede posibilitar una primera partición 110 virtual y una segunda partición 112 virtual. Como se analiza en detalle a continuación, estas particiones pueden servir para separar funciones de sistema operativo de servicios de agente de protección.

También como se ilustra, el medio 106 legible por ordenador incluye adicionalmente un sistema operativo (SO) 114 así como una o más aplicaciones 116 de usuario. El sistema 114 operativo proporciona servicios 118 de sistema operativo a las aplicaciones 116 de usuario, permitiendo por lo tanto que las aplicaciones se ejecuten en el dispositivo informático. Además, uno o más recursos 120 de sistema operativo residen en el sistema operativo. Recursos ejemplares incluyen una tabla de despacho de servicio de sistema (SSDT), una tabla de despacho de interrupción (IDT), una tabla de descriptor global (GDT), y similares. También como se ilustra, el sistema operativo puede incluir software maligno 122 (es decir, código con intención maliciosa), que puede haberse cargado en el dispositivo informático en las maneras anteriormente analizadas o de otra manera. Uno o más agentes de protección, analizados a continuación, pueden detectar cambios realizados a los recursos del sistema operativo por el software maligno y, en respuesta a la detección, tomar una acción defensiva. Si el agente hace una determinación de este tipo, a continuación el agente de protección puede apagar el sistema operativo y/o el dispositivo informático o puede tomar otra acción contrarrestante.

Habiendo analizado la estructura del dispositivo informático, la atención ahora gira a modos de privilegio variables presentes en el uno o más procesadores 104 físicos subyacentes. El modo 124 de privilegio de monitor de máquina virtual representa el modo más privilegiado ilustrado en la figura 1. Este modo de privilegio tiene acceso a todos o sustancialmente todos los recursos y memoria del dispositivo. A partir del modo 124 de privilegio de monitor de máquina virtual, el monitor de máquina virtual puede planificar los procesadores y puede permitir acceso a áreas de memoria para cada partición virtual. Mientras que un sistema operativo que se ejecuta en una partición puede creer que controla todos los recursos de un procesador físico, en realidad únicamente controla una porción como se determina por el monitor de máquina virtual.

Menos privilegiado que el modo de privilegio de monitor de máquina virtual, el modo 126 de privilegio de sistema operativo tiene acceso a todos los recursos 120 del sistema operativo y a la mayoría o a toda la memoria de sistema operativo. Este modo de privilegio, sin embargo, no tiene acceso a ningún recurso o memoria asociada con otra partición, tal como la segunda partición 112 virtual. Sin embargo, puesto que este modo de privilegio en general tiene acceso a toda la memoria de sistema operativo, en ocasiones se denomina como el "Modo privilegiado". "Anillo 0", "Modo de Supervisor", o "Modo de núcleo" pueden describir también este modo de privilegio. Como se ha analizado anteriormente, una aplicación de usuario que opera en el modo 126 de privilegio de sistema operativo generalmente puede ejecutar la mayoría de las instrucciones proporcionadas por el procesador, con la excepción de aquellas instrucciones reservadas para modo de monitor de máquina virtual.

Este modo de privilegio de sistema operativo está en contraste con el modo 128 de privilegio de usuario, en ocasiones denominado como "Modo no privilegiado", "Anillo 3", o simplemente "Modo de usuario". También como se ha analizado anteriormente, la aplicación de usuario puede no acceder o modificar cierta memoria asociada con el sistema operativo cuando opera desde el modo 128 de privilegio de usuario. En general, las aplicaciones de usuario de dispositivo informático operan en este modo de privilegio de usuario cuando realizan operaciones básicas.

Además de los modos anteriormente analizados, la figura 1 también ilustra un modo 130 de privilegio de segunda partición virtual y un modo 132 de privilegio de agente de protección. Como se analiza en detalle a continuación, el modo 132 de privilegio de agente de protección puede tener acceso a una porción de memoria que el modo de privilegio de sistema operativo no tiene, aunque en general no tiene tanto acceso a memoria como el modo de privilegio de monitor de máquina virtual. Como tal, este modo de privilegio puede estar más privilegiado que el modo de privilegio de sistema operativo pero menos privilegiado que el modo de privilegio de monitor de máquina virtual.

También como se analiza en detalle a continuación, el modo de privilegio de la segunda partición virtual en general tiene acceso a memoria asociada con la segunda partición 112 virtual. Además, este modo puede tener acceso a la primera partición virtual. Tal acceso adicional puede permitir, por ejemplo, a un agente de protección que reside en la segunda partición virtual explorar memoria asociada con la primera partición virtual y su correspondiente sistema operativo. Este modo en general no tiene acceso al monitor de máquina virtual, y por lo tanto está menos privilegiado que el modo de privilegio de monitor de máquina virtual. Sin embargo, el modo de privilegio de la segunda partición virtual aún tiene acceso a una porción de memoria que el modo de privilegio de sistema operativo no tiene.

Mientras tanto, la figura 2 ilustra los derechos 200 de memoria del dispositivo informático. Esta figura por lo tanto representa la cantidad de memoria accesible por los módulos de la figura 1. Como se ilustra, el monitor 108 de máquina virtual que opera en modo 124 de privilegio de monitor de máquina virtual tiene la mayoría de los derechos de memoria de todos los módulos ilustrados. De hecho, el monitor de máquina virtual reside en, y en solitario tiene acceso a, una porción de memoria 202. A continuación, el agente 204 de protección (por ejemplo, cualquiera de los agentes de protección ilustrados en la figura 1) opera en modo 132 de privilegio de agente de protección y tiene acceso a toda la memoria distinta de la porción 202 que corresponde al monitor de máquina virtual. El agente de protección, sin embargo, tiene acceso a una porción 206 de memoria, que es la porción de memoria en la que reside

el mismo el agente de protección.

El sistema 114 operativo, mientras tanto, opera en el modo 126 de privilegio de sistema operativo y tiene acceso a toda la memoria distinta de la porción 202 y la porción 206. Aunque el sistema operativo puede no tener acceso a la porción 206 de memoria asociada con el agente de protección, el sistema operativo y su modo de privilegio asociado no tienen acceso a una porción 208 de memoria. Esta porción 208 de memoria en ocasiones es conocida como memoria de núcleo o el componente de nivel más inferior de un sistema operativo y en general contiene los recursos mostrados en la figura 1. Incluso si el software maligno se carga y opera en la porción 208 de memoria, sin embargo, el software maligno no puede acceder a la porción 206 de memoria asociada con el agente de protección.

Finalmente, la figura 2 ilustra que las aplicaciones 116 de usuario únicamente tienen acceso a una porción 210 de memoria. Estas aplicaciones de usuario y el correspondiente modo de privilegio de usuario no tienen acceso a la porción 208 de memoria asociada con el componente de nivel más inferior del sistema operativo. Con este entorno de operación en mente, las siguientes cuatro secciones describen en detalle maneras ejemplares que un agente de protección puede hacerse inalterable o inaccesible del modo de privilegio de sistema operativo.

Agentes de protección autónomos

La siguiente sección describe herramientas que pueden determinar, desde memoria inaccesible por una entidad que opera en un modo de privilegio de sistema operativo, si uno o más recursos de sistema operativo han sido modificados. Como tal, las herramientas pueden permitir que un agente de protección resida en una localización distinta de la localización de la misma memoria de sistema operativo. Más particularmente, las siguientes sub-secciones describen cómo pueden residir los agentes de protección en un monitor de máquina virtual o en una partición virtual autónoma.

Agentes de protección de monitor de máquina virtual

Esta sub-sección describe cómo un agente 134 de protección puede residir en el mismo monitor de máquina virtual, como ilustra la figura 1. Puesto que el modo de privilegio de sistema operativo no puede acceder al monitor de máquina virtual, esta localización protege el agente de protección de cualquier software maligno localizado en la memoria de sistema operativo. Para operar desde esta localización, el agente de protección recibe una identificación del uno o más recursos 120 de sistema operativo que el agente 134 de protección puede monitorizar. Esta identificación puede recibirse mediante el identificador 136 de recurso. Como se ilustra, el sistema operativo puede proporcionar esta información al monitor de máquina virtual a través de llamadas de Interfaz de Programación de Aplicación (API), o el sistema operativo puede proporcionar la información en forma de un manifiesto 138. Como se ha analizado anteriormente, estos recursos pueden incluir la SSDT, IDT y GDT.

Una vez que ha recibido la identificación de recursos, el agente 134 de protección amplía los servicios 140 de agente de protección al sistema 114 operativo. Estos servicios de agente de protección generalmente comprenden determinar si cualquiera de los recursos identificados han sido modificados. Si se realiza una determinación de este tipo, el agente de protección o monitor de máquina virtual puede, por ejemplo, apagar el sistema operativo. Los servicios de agente de protección pueden incluir también aplicar invariancia frente a cualesquiera recursos marcados como inmodificables (por ejemplo, "de solo lectura").

Emplear una técnica de este tipo empieza con la carga e inicialización del monitor de máquina virtual, que puede alojar uno o más sistemas operativos. En este ejemplo, el monitor de máquina virtual aloja el único sistema 114 operativo, que por sí mismo empieza la inicialización después de que carga el monitor de máquina virtual. Durante la inicialización del sistema operativo, la porción 208 de memoria asociada con el componente de nivel más inferior del sistema operativo (por ejemplo, el núcleo) se carga en primer lugar. Algunos o todos los recursos 120 de sistema operativo (por ejemplo, la SSDT, GDT, IDT) generalmente ocupan esta porción 208 de memoria.

Antes o mientras el sistema operativo se inicializa, el agente 134 de protección puede empezar a ejecutarse desde dentro del monitor de máquina virtual. Como se ha analizado anteriormente, el agente de protección generalmente recibe una identificación de un conjunto de uno o más recursos de sistema operativo y determina si uno o más de los recursos identificados han sido modificados. Obsérvese que cada recurso identificado a menudo comprende múltiples componentes en múltiples localizaciones, cada una de las cuales el agente de protección puede monitorizar para proteger completamente todo el recurso. Por ejemplo, si el manifiesto identifica una SSDT como un recurso a monitorizarse y protegerse, el agente de protección no únicamente protege la tabla real sino también otros componentes de la SSDT. Por ejemplo, el agente de protección puede también monitorizar y explorar el registro que apunta a la localización de la tabla. Adicionalmente, el agente de protección puede también monitorizar las estructuras de datos de traducción de memoria (por ejemplo, tablas de página) que traducen la dirección virtual de la SSDT a una dirección física. Si el agente de protección falla al hacer esto, entonces el código malicioso puede crear otra tabla con diferentes mapeos de tabla de página (es decir, omitir la propia SSDT).

Además de la identificación, el agente de protección puede recibir también un atributo de protección que instruye al agente de protección sobre cómo proteger un recurso correspondiente. Por ejemplo, el agente de protección puede recibir una identificación de un recurso de SSDT, así como un correspondiente atributo de protección de "solo lectura". El agente de protección por lo tanto aprende que la SSDT debería permanecer en solo lectura y, como tal,

no debería modificarse. "Iniciar solo lectura" es otro posible atributo de protección, que instruye al agente de protección que el correspondiente recurso puede escribirse una vez durante la inicialización, pero después de tal tiempo el recurso debería permanecer como de solo lectura.

El agente de protección puede recibir esta identificación de los recursos y atributos de protección de recurso en un número de maneras, tanto de manera positiva como pasiva. Por ejemplo, el sistema operativo puede proporcionar un manifiesto firmado digitalmente que identifica los recursos que puede monitorizar el agente de protección. Este manifiesto firmado digitalmente puede identificar los recursos en una multitud de maneras, tal como por nombre (por ejemplo, SSDT, IDT, GDT, etc.) o por dirección, que mapea recursos a correspondientes localizaciones en la porción 208 de memoria. En los últimos casos, el manifiesto puede identificar una dirección física de invitado del recurso, dirección virtual de invitado o dirección física de sistema. Obsérvese que en algunos casos, una dirección física de invitado puede mapearse a una dirección física de sistema real para descubrir la localización física real del correspondiente componente de recurso.

Después de que el monitor de máquina virtual o el agente de protección reciben el manifiesto, estos componentes pueden determinar si el manifiesto ha sido manipulado o modificado. Si el monitor de máquina virtual o el agente de protección hacen una determinación de este tipo, el monitor de máquina virtual o el agente de protección pueden optar por fallar el inicio del sistema operativo. Además, la encriptación asociada con la lista de recursos puede invalidarse, protegiendo por lo tanto su seguridad.

Además o como alternativa al manifiesto, el agente de protección puede recibir identificación de recurso y de atributo de protección mediante una o más llamadas de interfaz de programación de aplicación (API) en el monitor de máquina virtual (por ejemplo, "hiperllamadas"). A medida que el sistema operativo se inicializa, el sistema operativo (y tal vez el componente de nivel más inferior del sistema 208 operativo) puede hacer hiperllamadas en el monitor de máquina virtual que informan al agente de protección de ciertos recursos que pueden monitorizarse y protegerse. Estas hiperllamadas pueden identificar los recursos pertinentes en las mismas maneras anteriormente analizadas. También como se ha analizado anteriormente, estas hiperllamadas pueden identificar también atributos de protección de los recursos.

En las realizaciones que utilizan un manifiesto firmado digitalmente, así como una o más hiperllamadas, el agente de protección puede explorar en primer lugar los recursos identificados en el manifiesto antes o mientras se arranca el sistema operativo. Después de esta exploración inicial, el sistema operativo puede a continuación hacer hiperllamadas en el monitor de máquina virtual que instruyen al agente de protección a determinar si las páginas identificadas de hiperllamada han sido modificadas. El manifiesto por lo tanto identifica recursos a explorar tras cada arranque de sistema operativo, mientras que las hiperllamadas identifican recursos a explorar dinámicamente tras su respectiva inicialización.

Habiendo identificado los recursos a monitorizarse, el agente de protección a continuación determina si los recursos han sido modificados o no (por ejemplo, todas las porciones de la SSDT anteriormente analizada). El agente de protección puede aplicar también una invariancia frente a los recursos identificados. Por ejemplo, el agente de protección puede asegurar que cualquier recurso designado como "de solo lectura" no cambie a "escribible".

Para monitorizar y proteger los recursos de esta manera, la ejecución de código en el monitor de máquina virtual puede emplear un gestor de intercepción de monitor de máquina virtual (por ejemplo, el gestor 146 de la figura 1). Si se instruye así, este gestor de intercepción puede registrar intercepciones en los diversos componentes de los recursos identificados. Debido a este registro, el agente de protección en el monitor de máquina virtual puede ahora recibir intercepciones si se realizan intentos para acceder o modificar estos recursos identificados. Como tal, el agente de protección puede inspeccionar y explorar los diversos componentes de recursos identificados. También puede bloquear de manera activa intentos para modificar estos recursos.

En algunas realizaciones, el agente de protección explora los recursos y determina un estado inicial de los recursos para su uso al comparar los resultados de exploraciones futuras. En otras realizaciones, el agente de protección ya tiene conocimiento de un estado inicial de los recursos para comparar los resultados de exploraciones futuras. En cualquier caso, el agente de protección puede calcular un valor de troceo o de suma de comprobación de este estado inicial. Después de este cálculo, el agente de protección explora los recursos antes, después o mientras se arranca el sistema operativo. Después de la exploración, el agente de protección calcula un troceo o suma de comprobación de los resultados y compara este al valor de troceo o de suma de comprobación del estado inicial. Si son iguales, el agente de protección determina que los correspondientes recursos no han sido modificados. Por supuesto, el agente de protección puede omitir los valores de troceo o de suma de comprobación y comparar directamente en su lugar el estado inicial a la exploración.

Si los valores son diferentes, sin embargo, el agente de protección y/o el monitor de máquina virtual pueden tomar una o más acciones de respuesta. En primer lugar, el mismo agente de protección puede apagar el sistema operativo o modo de privilegio de sistema operativo, o puede instruir al monitor de máquina virtual para hacer eso. De nuevo, puesto que el agente de protección reside en el monitor de máquina virtual y puesto que el monitor de máquina virtual aloja el sistema operativo, estos dos componentes pueden hacer esto apagando el sistema operativo. Adicionalmente, puesto que el agente de protección reside en el monitor de máquina virtual, el apagado

del sistema operativo no puede manipularse desde incluso el modo de privilegio de sistema operativo.

Además de apagar el sistema operativo, el agente de protección y/o monitor de máquina virtual pueden advertir en primer lugar al sistema operativo del apagado inminente. Un canal de comunicación entre el monitor de máquina virtual y el sistema operativo puede permitir una comunicación de este tipo. Como alternativa, el agente de protección y/o el monitor de máquina virtual pueden escribir una advertencia a una localización de memoria o señalizar un evento que el sistema operativo monitoriza.

Sin importar si se ha proporcionado o no una advertencia, el apagado del sistema operativo puede ser abrupto o elegante. En el primer caso, el monitor de máquina virtual puede simplemente desconectar el sistema operativo inmediatamente después del aprendizaje de los valores de troceo o de suma de comprobación dispares. En el último caso, el monitor de máquina virtual puede permitir al sistema operativo una cierta cantidad de tiempo para apagarse a sí mismo de manera limpia. En este tiempo, el sistema operativo puede cerrar, por ejemplo, cualquier fichero abierto y evacuar cualquier dato correspondiente. El sistema operativo puede también liberar recursos asignados. Adicionalmente, el apagado puede utilizar ambos enfoques. Por ejemplo, si el monitor de máquina virtual aloja múltiples particiones, puede apagar inmediatamente la partición con los valores de troceo o de suma de comprobación dispares mientras permite que las otras particiones tiempo se apaguen de manera limpia. En cualquier caso, la manera de apagado puede ser configurable por política y puede ser ajustable.

Además de un apagado y advertencia correspondiente, el agente de protección y/o monitor de máquina virtual pueden tomar acciones post-arranque en respuesta a una modificación no permitida de un recurso identificado. Por ejemplo, el monitor de máquina virtual y/o el agente de protección pueden notificar, tras reinicio del sistema operativo, al sistema operativo de la modificación de recurso. En respuesta, el sistema operativo puede realizar una exploración de antivirus para detectar si algún software maligno no reside de hecho en la memoria de sistema operativo, tal como la porción 208 (por ejemplo, el núcleo). Adicionalmente, el monitor de máquina virtual puede arrancar el sistema operativo en un modo seguro, o el sistema operativo puede elegir por sí mismo arrancar en el modo seguro. También en respuesta a la notificación, el sistema operativo puede identificarse a sí mismo como que ha sido atacado y, como tal, puede no permitirse a sí mismo acceder a alguna red a la que está acoplado.

Agentes de protección de partición virtual

En lugar de residir en el mismo monitor de máquina virtual, un agente de protección (por ejemplo, el agente 142 de protección de la figura 1) puede residir en una partición virtual separada (por ejemplo, la segunda partición 112 virtual de la figura 1). En estas realizaciones, esta partición separada actúa como un delegado confiable del monitor de máquina virtual. El agente 142 de protección por lo tanto es inaccesible del modo de privilegio de sistema operativo. Como se ha analizado anteriormente, el monitor 108 de máquina virtual proporciona una virtualización de este tipo del dispositivo 102 informático. Mientras que el monitor de máquina virtual puede virtualizar el dispositivo informático en cualquier número de particiones, la figura 1 ilustra una primera partición que aloja el sistema operativo y una segunda partición que aloja el agente de protección. La segunda partición virtual en la que reside el agente de protección puede ser, en algunos casos, una partición de seguridad especializada cuya función principal o única es ejecutar el agente de protección. En otras realizaciones, esta segunda partición virtual puede realizar funciones adicionales, tales como alojar otro sistema operativo.

El agente 142 de protección que reside en la segunda partición virtual puede realizar muchas o todas las mismas funciones como se han descrito anteriormente con respecto al agente 134 de protección que reside en el monitor de máquina virtual. Es decir, el agente 142 de protección puede recibir de manera positiva o pasiva una identificación de uno o más recursos 120 de sistema operativo. En respuesta a la identificación, el agente de protección puede de nuevo ampliar los servicios 140 del agente de protección, que en general comprenden determinar si uno o más de los recursos identificados han sido modificados o no y, en caso afirmativo, tomar acción de respuesta. Estos servicios pueden incluir también aplicar invariancia de recursos especificados. El agente 142 de protección puede realizar estas funciones mediante técnicas similares a aquellas anteriormente descritas.

Como se ilustra, el agente 142 de protección es accesible desde el modo 130 de privilegio de la segunda partición virtual, pero inaccesible desde el modo 126 de privilegio de sistema operativo. Como tal, la arquitectura resultante permite protección del agente de protección a sí mismo desde cualquier software maligno localizado en el sistema operativo, incluso si el software maligno reside en la porción 208 de memoria asociada con el componente de nivel más inferior del sistema operativo.

Modos de privilegio de agente de protección autónomo

Esta sección describe herramientas que pueden hacer una porción de memoria de sistema operativo asociada con un agente de protección inalterable o inaccesible desde un modo de privilegio de sistema operativo, mientras aún permite que esta porción de memoria resida físicamente en un espacio de memoria física de sistema operativo. Estas herramientas por lo tanto crean un modo de privilegio de agente de protección autónomo que tiene acceso a la porción de memoria asociada con el agente de protección así como al resto de la memoria que es accesible en el modo de privilegio de sistema operativo. Este modo de privilegio por lo tanto es más privilegiado que el modo de privilegio de sistema operativo.

La primera sub-sección describe herramientas que pueden crear el modo de privilegio de agente de protección solicitando que un monitor de máquina virtual proteja una porción de memoria asociada con el agente de protección. La segunda sub-sección, mientras tanto, describe herramientas que permiten la creación del modo de privilegio de agente de protección mediante virtualización de un procesador físico en múltiples procesadores virtuales, incluyendo un procesador virtual especializado para ejecutar el agente de protección.

Solicitudes de protección a un monitor de máquina virtual

Esta sub-sección describe cómo un agente de protección puede solicitar a un monitor de máquina virtual que proteja memoria asociada con el agente de protección y, como tal, al mismo agente de protección. Esta protección da como resultado un agente 144 de protección que opera en el modo 132 de privilegio de agente de protección, como se ilustra en la figura 1. Como se ilustra, el agente 144 de protección puede residir inicialmente en el modo de privilegio de sistema operativo, antes de desplazarse al modo de privilegio de agente de protección. Cuando se opera en este último modo de privilegio, el agente de protección es en general impermeable a los ataques de entidades que operan con el modo 126 de privilegio de sistema operativo.

Cuando opera en el modo 132 de privilegio de agente de protección, una entidad tiene ligeramente más privilegios que si opera en el modo 126 de privilegio de sistema operativo, pero aún menos privilegios que en el modo 124 de privilegio de monitor de máquina virtual. Como ilustra la figura 2, un agente de protección que opera en este modo de privilegio tiene acceso a toda la memoria asociada con el sistema operativo, además de la misma porción 206 de memoria asociada con el agente de protección. El monitor 108 de máquina virtual aplica la accesibilidad de protección de agente añadida.

Las Figuras 3 y 4 ilustran una manera ejemplar de crear este modo de privilegio de agente de protección. La Figura 3 representa toda o sustancialmente toda la memoria 300 del dispositivo informático. La memoria 300 de dispositivo informático incluye una porción de memoria 302 asociada con el modo de privilegio de sistema operativo (por ejemplo, el núcleo) y una porción de memoria 304 asociada con el modo de privilegio de usuario. La porción de memoria 302 también incluye, como se ilustra, una porción 306 de memoria asociada con el agente 144 de protección así como una porción de memoria 308 en la que se cargan los controladores.

Como ilustra la figura 4, un procedimiento 400 de creación del modo 132 de privilegio de agente de protección comienza en el acto 1 mediante la inicialización de la porción de memoria 302 (por ejemplo, el núcleo). En el acto 2, la porción 306 de memoria o el mismo agente 144 de protección llama al monitor 108 de máquina virtual para solicitar que el monitor de máquina virtual proteja la porción de memoria asociada con el agente de protección. Al solicitar esto, el agente de protección o la memoria correspondiente pide que no se permita que el código que se ejecuta en el modo de privilegio de sistema operativo modifique o toque de otra manera esta porción 306 de memoria. El agente de protección puede verificar también por sí mismo (por ejemplo, por una firma digital) al monitor 108 de máquina virtual. Esta porción de memoria, o el mismo agente de protección, puede solicitar también que el monitor de máquina virtual establezca un temporizador y ejecute el agente de protección cuando el temporizador se agota. El acto 3 representa el monitor de máquina virtual que protege la memoria de entidades que operan en el modo de privilegio de sistema operativo y establecer un temporizador en respuesta a la solicitud. Obsérvese que puesto que esta porción 306 de memoria asociada con el agente de protección ahora es inalterable y/o inaccesible del modo de privilegio de sistema operativo, el agente de protección ahora reside en el modo de privilegio de agente de protección.

En el acto 4, se cargan los controladores en la porción de memoria 308. Obsérvese que la solicitud del acto 2 y la correspondiente protección del acto 3 en general tienen lugar antes de que los controladores se carguen en memoria, ya que el software maligno puede existir en forma de un controlador. Como se analiza en la sección "Uso ejemplar de las herramientas" a continuación, los autores de software maligno a menudo engañan a los usuarios para que instalen controladores maliciosos en un dispositivo informático. Si uno o más controladores maliciosos se cargan de hecho en memoria antes de que la porción 306 de memoria esté protegida, entonces los controladores maliciosos pueden potencialmente parchear la solicitud para la misma protección. Tal parcheo impediría de esta manera la ejecución periódica del agente de protección mediante el monitor de máquina virtual y, por lo tanto, la creación del modo de privilegio de agente de protección. Solicitando que el monitor de máquina virtual establezca un temporizador desde el principio, sin embargo, este procedimiento asegura que el código en el modo de privilegio de sistema operativo no puede desactivar de esta manera la ejecución periódica del agente de protección.

El acto 5, mientras tanto, probablemente tiene lugar algún tiempo después de que se hayan cargado los controladores. Como se ilustra, el acto 5 representa la expiración del temporizador de monitor de máquina virtual y, por lo tanto, la ejecución del agente de protección. Cuando se ejecuta, el agente 144 de protección realiza funciones similares o idénticas a aquellas analizadas en las secciones anteriores. También como se ha analizado anteriormente, el agente de protección puede tomar acciones en respuesta a una determinación de que se han modificado uno o más recursos identificados. El agente de protección puede tomar también tal acción en respuesta a un acceso intentado o modificación del agente de protección, o su correspondiente memoria, de entidades que operan en el modo de privilegio de sistema operativo.

El acto 6 representa el agente de protección que notifica al monitor de máquina virtual cuando el agente de protección finaliza la ejecución. Finalmente, el acto 7 representa la repetición de los actos 3, 5 y 6. Como tal, el monitor de máquina virtual puede resetear su temporizador y ejecutar el agente de protección a intervalos periódicos, tal como cada 100 milisegundos (ms).

Estableciendo un temporizador frente a fallos en el monitor de máquina virtual, el procedimiento 400 elimina de esta manera la capacidad del código de sistema operativo para manipular con la porción de memoria asociada con el agente de protección. Como tal, este procedimiento asegura que el agente de protección continuará ejecutándose y no se parcheará por el software maligno que actúa en el modo de privilegio de sistema operativo. En su lugar, el agente de protección se ejecutará en un modo de privilegio autónomo mientras aún reside en memoria física asignada al sistema operativo.

Procesadores virtuales de agente de protección

Esta sub-sección describe cómo un monitor de máquina virtual puede crear un modo de privilegio de agente de protección planificando un procesador virtual para ejecutar el agente 144 de protección. La Figura 5 ilustra una arquitectura 500 que incluye el monitor 108 de máquina virtual que virtualiza el dispositivo 102 informático en dos particiones, incluyendo cada una un sistema operativo. Como se ilustra, el dispositivo informático en este ejemplo incluye dos procesadores 104(a) y 104(b) reales, después de los cuales cada uno de los procesadores virtuales puede planificar múltiples procesadores virtuales. También como se ilustra, el monitor de máquina virtual crea una primera partición 502 virtual y una segunda partición 504 virtual. La primera partición virtual incluye un primer procesador 506 virtual para ejecutar un primer sistema operativo. De manera similar, la segunda partición virtual incluye un segundo procesador 508 virtual para ejecutar un segundo sistema operativo. En este caso, sin embargo, el monitor de máquina virtual también incluye un procesador 510 virtual de agente de protección para ejecutar un agente de protección, tal como el agente 144 de protección de la figura 1.

Para crear la arquitectura 500, el monitor de máquina virtual en primer lugar se carga e inicializa. Como se ilustra en la figura 6, el monitor de máquina virtual a continuación virtualiza los diversos procesadores virtuales y, al hacer esto, asigna el ancho de banda 600 de procesador real. Para comenzar esta virtualización y asignación, el monitor de máquina virtual virtualiza el primer procesador virtual en el primer procesador real. En el ejemplo actual, esta virtualización se hace en una base uno a uno como se ilustra por la figura 6. Es decir, únicamente este único procesador 506 virtual corresponde al procesador 104(a) real y, como tal, el monitor de máquina virtual asigna todo el ancho de banda del procesador real a este procesador virtual. El monitor de máquina virtual a continuación virtualiza el segundo procesador 508 virtual en el segundo procesador 104(b) real. En lugar de una base uno a uno, sin embargo, el monitor de máquina virtual retiene alguna porción del ancho de banda del segundo procesador real. El monitor de máquina virtual a continuación virtualiza el procesador 510 virtual de agente de protección en este ancho de banda restante del segundo procesador 104(b) real, como se ilustra por la figura 6.

Cada procesador virtual que opera en el segundo procesador real en general actúa en una base por segmentos de tiempo. Es decir, el segundo procesador virtual puede operar en el segundo procesador real durante alguna cantidad de tiempo, antes de que se suspenda la operación del segundo procesador virtual. En este punto, el segundo procesador real conmuta a la operación del procesador virtual de agente de protección durante alguna otra cantidad de tiempo. Por ejemplo, el segundo procesador virtual puede operar en el segundo procesador real durante 90 ms, punto en el cual la operación de este segundo procesador virtual se suspende y la operación del procesador virtual de agente de protección comienza durante 10 ms. El procesador virtual de agente de protección en general es transparente para ambas particiones de sistema operativo y tanto para el primer como el segundo procesadores virtuales. Como tal, ambos sistemas operativos creen que sus procesadores virtuales correspondientes corresponden a un procesador real respectivo.

Además de asignar el ancho de banda de procesador real, el monitor de máquina virtual también gestiona la porción de memoria que puede acceder cada procesador virtual. En el ejemplo actual, el primer procesador virtual puede acceder a toda la memoria asociada con el primer sistema operativo. El segundo procesador virtual, mientras tanto, puede acceder a toda la memoria asociada con el segundo sistema operativo, distinta de la porción de memoria asociada con el agente de protección. El procesador virtual de agente de protección en solitario tiene acceso a la porción de memoria asociada con el agente de protección, además de la memoria asignada al segundo sistema operativo.

Adicionalmente, el primer y segundo procesadores virtuales únicamente tienen la capacidad de modificar su memoria asociada. Como tal, ninguno de los procesadores virtuales que operan sus respectivos sistemas operativos puede modificar la porción de memoria asociada con el agente de protección. El procesador virtual de agente de protección, sin embargo, puede modificar la memoria asociada con el agente de protección y, en algunas realizaciones, la memoria asociada con el segundo procesador virtual también.

Mediante su naturaleza programada, el procesador virtual de agente de protección ejecutará periódicamente el agente de protección. Aunque en algunos casos el procesador virtual de agente de protección puede ejecutar otras aplicaciones, el ejemplo actual ilustra un procesador virtual de agente de protección especializado. Como tal, este procesador virtual en general únicamente sirve para ejecutar periódicamente el agente de protección. De nuevo, el

agente de protección puede realizar funciones similares o idénticas, en maneras similares o idénticas, como los agentes de protección anteriormente descritos.

Planificando un procesador virtual de agente de protección especializado, el monitor de máquina virtual asegura que el agente de protección ejecutará periódicamente el control de este procesador y en un modo de privilegio de agente de protección autónomo. Adicionalmente, puesto que únicamente este procesador virtual de agente de protección tiene acceso a la porción de memoria asociada con el agente de protección, el monitor de máquina virtual protege esta memoria de código en un sistema operativo. Por lo tanto, el software maligno que opera en un modo de privilegio de sistema operativo no puede parchearse a través del agente de protección y evitar que el agente de protección se ejecute. Como tal, esta técnica esencialmente elimina una capacidad del sistema operativo para manipular el agente de protección.

Uso ejemplar de las herramientas

Habiendo descrito previamente las herramientas que pueden asegurar la protección de un agente de protección, la siguiente sección describe solamente un ejemplo de estas herramientas en la operación. En primer lugar, imagínese que un usuario de ordenador navega por Internet y, mientras está navegando por un cierto sitio web, aparece un cuadro de diálogo con intención maliciosa en la pantalla del usuario. El cuadro de diálogo solicita permiso del usuario para instalar alguna clase de software maligno en el ordenador del usuario. Aunque esta solicitud puede ser directa, imagínese que el cuadro de diálogo disfraza la solicitud como es típicamente el caso. El cuadro de diálogo puede, por ejemplo, informar de manera falsa al usuario de que él o ella ganó un regalo. Al informar así, el cuadro de diálogo instruye de manera maliciosa a que el usuario haga clic el botón de "OK" en el cuadro de diálogo para recibir el regalo. Imagínese que el usuario de hecho selecciona el botón de OK y que el usuario elige continuar las operaciones solicitadas a pesar de una o más advertencias de software (por ejemplo, una aplicación de antivirus) que se ejecuta en el dispositivo informático.

En este punto, el dispositivo informático comienza la instalación de un controlador que contiene el software maligno. Como se cumple en general con los controladores, se concede acceso a este controlador malicioso a un modo de privilegio de sistema operativo y se carga en memoria asociada con este modo de privilegio (por ejemplo, el núcleo). Una vez cargado en el núcleo, el controlador malicioso y su software maligno adjunto esencialmente tienen acceso de carta blanca a la memoria y al sistema operativo del ordenador. Desafortunadamente para el usuario, imagínese que este software maligno incluye un registrador de teclas que registra las pulsaciones de tecla de un usuario. Imagínese ahora que el usuario navega a su sitio web del banco y firma en su cuenta bancaria. Debido a su capacidad para registrar pulsaciones de teclas, el registrador de teclas aprende la contraseña de la cuenta bancaria del usuario y envía esta contraseña a través de la Internet al autor del controlador malicioso.

Para hacer la situación peor, imagínese que el software maligno es un "encubridor de inicio"- o software maligno que intenta ocultar de manera activa un agente de protección y el software de antivirus del usuario. En sistemas convencionales, un agente de protección reside en el núcleo (es decir, en memoria a la que el controlador malicioso tiene acceso). Por lo tanto, en estos sistemas convencionales el software maligno tiene acceso al agente de protección y puede intentar ocultarse a sí mismo del agente de protección. Si es satisfactorio, el software maligno parecería que no existe para el agente de protección en el núcleo. Por lo tanto, cuando el software de antivirus del usuario llama al agente de protección y solicita una lista de todas las aplicaciones presentes en la memoria del ordenador, el software maligno estaría ausente. Esta ausencia hace que el software de antivirus sea impotente de conocer y eliminar el software maligno. Adicionalmente, el software maligno puede parchear a través del agente de protección, evitando de esta manera que el agente de protección se ejecute en absoluto. Como tal, el agente de protección puede fallar al avisar si el software maligno modifica cualesquiera recursos de sistema operativo.

En lugar de residir en el núcleo como en sistemas convencionales, sin embargo, imagínese que el agente de protección en el dispositivo informático del usuario reside en memoria o se ejecuta en un modo que es inaccesible del modo de privilegio de sistema operativo. Por lo tanto, cuando el controlador malicioso se carga en el núcleo, no tiene acceso a la memoria en la que reside el agente de protección o el modo en el que se ejecuta el agente de protección. Por lo tanto, el controlador y su software maligno adjunto no tienen acceso al mismo agente de protección. El software maligno por lo tanto no puede ocultarse a sí mismo del agente de protección y, por lo tanto, el software de antivirus también. Por lo tanto, cuando el software de antivirus pide al agente de protección una lista de todas las aplicaciones presentes en la memoria del ordenador, la lista devuelta incluye el software maligno. El software de antivirus a continuación reconoce este código como software maligno y en consecuencia lo elimina del dispositivo informático del usuario. Adicionalmente, el agente de protección puede notificar por sí mismo si el software maligno modifica recursos de sistema operativo y, en respuesta, puede apagar el dispositivo informático del usuario.

Por lo tanto, residiendo en memoria o ejecutando en un modo que es inaccesible del modo de privilegio de sistema operativo, las realizaciones descritas en el presente documento evitan que el software maligno se oculte a sí mismo desde o parcheándose a través del agente de protección. En el ejemplo anterior, el dispositivo informático del usuario puede eliminar por lo tanto el software maligno de la máquina o, en algunos casos, apagar el sistema cuando el software maligno modifica recursos importantes. En cualquier caso, estas realizaciones sirven para reducir la efectividad del software maligno en su deseo de provocar daño.

Otras realizaciones de las herramientas

Las secciones anteriores describen unos pocos ejemplos particulares donde un agente de protección se hace inalterable o inaccesible del modo de privilegio de sistema operativo. En esta sección, se describen otras realizaciones de las herramientas, tal como añadir un modo de privilegio a un procesador que no está presente en un procesador subyacente.

Estas realizaciones ejemplares se describen como parte de los procedimientos 700 a 1100 de las figuras 7 a 11. Estos procedimientos, así como procedimientos ejemplares descritos o ilustrados con referencia a las figuras 1 a 6, pueden implementarse en cualquier hardware, software, firmware, o combinación de los mismos adecuada; en el caso de software y firmware, estos procedimientos representan conjuntos de operaciones implementadas como instrucciones ejecutables por ordenador almacenadas en medio legible por ordenador y ejecutables por uno o más procesadores. Estas realizaciones de las herramientas descritas en esta sección no se pretenden para limitar el alcance de las herramientas o las reivindicaciones.

Con referencia a la figura 7, el bloque 702 recibe una política de cumplimiento que identifica uno o más recursos de sistema operativo. Esta política de cumplimiento, que puede comprender datos encriptados, puede recibirse mediante un manifiesto firmado digitalmente o exponiendo una interfaz de programa de aplicación (API) al sistema operativo (por ejemplo, una hiperllamada). El bloque 704 identifica, de la memoria inaccesible desde una entidad que opera en un modo de privilegio de sistema operativo, uno o más recursos de sistema operativo. Los recursos ejemplares incluyen una tabla de despacho de servicio de sistema (SSDT), una tabla de despacho de interrupción (IDT), y/o una tabla de descriptor global (GDT). Como se ha descrito anteriormente, esta identificación puede tener lugar en un monitor de máquina virtual (por ejemplo, por el agente 134 de protección de la figura 1) o en una partición virtual separada (por ejemplo, por el agente 142 de protección de la figura 1).

El bloque 706, mientras tanto, representa la determinación de si alguno de los recursos identificados ha sido modificado. De nuevo, esto puede tener lugar en un monitor de máquina virtual o en una partición separada. Si el bloque 706 determina que uno o más de los recursos identificados de hecho han sido modificados, a continuación el bloque 708 termina el sistema operativo en respuesta a esta determinación. Finalmente, el bloque 710 notifica al sistema operativo de una operación ilegal tras reinicio del sistema operativo.

La Figura 8 ilustra un procedimiento 800 para permitir que un agente de protección se ejecute en un monitor de máquina virtual. El bloque 802 modifica un gestor de intercepción de monitor de máquina virtual efectivo para permitir la recepción de una indicación que una página de memoria o registro asociado con un recurso de sistema operativo ha sido modificado. Este recurso puede comprender uno de los recursos descritos con referencia a la figura 7, o puede ser otro recurso de sistema operativo. En cualquier caso, el bloque 804 recibe una política de cumplimiento que identifica el recurso de sistema operativo y posiblemente uno o más otros recursos de sistema operativo. De nuevo, esta identificación puede hacerse mediante las técnicas anteriormente analizadas. Como se ha descrito anteriormente, un atributo de protección (por ejemplo, "solo lectura" o "iniciar solo lectura") del recurso puede acompañar la identificación del recurso. El bloque 806, mientras tanto, representa la recepción de una indicación de que la página de memoria o el registro asociado con el recurso de sistema operativo ha sido de hecho modificado. En respuesta, el bloque 808 apaga un modo de privilegio de sistema operativo eficaz para apagar un sistema operativo asociado con el recurso de sistema operativo. En algunos casos, el monitor 108 de máquina virtual de la figura 1 puede conseguir este apagado del modo de privilegio de sistema operativo.

A continuación, la figura 9 describe un procedimiento 900 ejemplar para crear un modo de privilegio de agente de protección, tal como el modo 132 de privilegio de agente de protección ilustrado en la figura 1. El bloque 902 recibe una solicitud de que un rango de memoria particular puede hacerse inalterable o inaccesible de un modo de privilegio de sistema operativo. De nuevo, un monitor de máquina virtual puede recibir esta solicitud, que puede originarse desde el mismo rango de memoria o desde un agente de protección que reside con el rango de memoria. El bloque 904 protege el rango de memoria y establece un temporizador para ejecutar periódicamente el agente de protección que reside con el rango de memoria. De nuevo, un monitor de máquina virtual puede establecer un temporizador de este tipo, que puede ordenar al monitor de máquina virtual que ejecute el agente de protección a intervalos regulares.

Mientras tanto, el bloque 906 recibe una política de cumplimiento que describe un recurso de sistema operativo. De nuevo, la política de cumplimiento y recurso descritos pueden ser similares o idénticos a aquellos anteriormente analizados. El bloque 908 ejecuta el agente de protección, que puede conseguirse por el monitor de máquina virtual. El bloque 910 decisión cuestiona si el recurso de sistema operativo ha sido modificado. El agente de protección puede hacer esta determinación funcionando en las maneras anteriormente descritas en detalle. Si el bloque 910 de hecho determina que ha tenido lugar una modificación, a continuación el bloque 912 apaga el sistema operativo. Si, sin embargo, no se realiza una determinación de este tipo, entonces el bloque 914 recibe una notificación de que el agente de protección ha finalizado la ejecución. En algunos casos y como se ha descrito anteriormente, el mismo agente de protección puede notificar de esta manera al monitor de máquina virtual. El bloque 916, mientras tanto, representa la realización de ciclos entre ejecutar el agente de protección y no ejecutar el agente de protección. Finalmente, obsérvese que aunque el agente de protección no se ejecuta, el monitor de máquina virtual puede apagar el sistema operativo en respuesta a un acceso intentado, desde una entidad que opera en el modo de

privilegio de sistema operativo, del rango de memoria asociada con el agente de protección.

La Figura 10 ilustra otro procedimiento 1000 ejemplar para crear un modo de privilegio de agente de protección, tal como el modo 132 de privilegio de agente de protección ilustrado en la figura 1. El bloque 1002 virtualiza un procesador informático real en múltiples procesadores informáticos virtuales. Estos procesadores virtuales pueden comprender uno o más procesadores virtuales de sistema operativo teniendo cada uno un privilegio para modificar su propia memoria de sistema operativo y usar una porción de un ancho de banda de procesamiento de los procesadores reales, como se ilustra en la figura 6. Los procesadores virtuales pueden incluir también al menos un procesador virtual de agente de protección que tiene un privilegio para modificar su propia memoria de agente de protección y usar una porción diferente del ancho de banda de procesamiento de los procesadores reales. Aunque todos los procesadores virtuales pueden planificarse por el monitor de máquina virtual, el procesador virtual de agente de protección puede ser transparente para los procesadores virtuales de sistema operativo. En algunos casos, los procesadores virtuales de sistema operativo no pueden modificar la memoria asignada al procesador virtual de agente de protección. Adicionalmente, el procesador virtual de agente de protección puede ser un procesador especializado cuyo único fin y primario es provocar que se ejecute el agente de protección, como se ha analizado anteriormente.

A continuación, el bloque 1004 provoca que el procesador virtual de agente de protección ejecute un agente de protección, que puede ser eficaz para determinar si una porción de dicha memoria de sistema operativo ha sido modificada o no. El bloque 1006, mientras tanto, recibe una indicación de que una porción de la memoria de sistema operativo ha sido modificada.

En respuesta, el bloque 1008 apaga un correspondiente sistema operativo.

Finalmente, la figura 11 representa un procedimiento 1100 para añadir un modo de privilegio a un procesador informático real. El bloque 1102 representa la determinación, identificación o clasificación de uno o más modos de privilegio presentes en un procesador físico subyacente. Estos modos de privilegio se definen en general por el mismo procesador físico subyacente. A cualquier velocidad, el bloque 1104 añade un modo de privilegio que no está presente en el procesador físico subyacente. En algunos casos, el modo de privilegio añadido puede modificar una porción de memoria del dispositivo informático que es diferente de una porción de memoria que puede modificarse por el uno o más modos de privilegio presentes. El modo de privilegio añadido también puede añadir y ejecutar instrucciones que no existían previamente o que no eran ejecutables en el procesador subyacente.

Adicionalmente, el uno o más modos de privilegio presentes en el procesador físico subyacente pueden incluir un modo de privilegio de usuario y un modo de privilegio de sistema operativo. En estas realizaciones, el modo de privilegio añadido puede ser más privilegiado tanto que el modo de usuario privilegiado como el modo de privilegio de sistema operativo, más privilegiado que el modo de privilegio de usuario pero menos privilegiado que el modo de privilegio de sistema operativo, o menos privilegiado que tanto los modos de privilegio de usuario como de sistema operativo. Finalmente, obsérvese que un caso de la adición del modo de privilegio puede comprender añadir un modo de privilegio de agente de protección (por ejemplo, el modo 132 de privilegio de agente de protección ilustrado en la figura 1) en una multitud de maneras anteriormente analizadas. Por ejemplo, un agente de protección o su rango de memoria asociado puede solicitar que el rango de memoria pueda hacerse inaccesible de entidades que operan en el modo de privilegio de sistema operativo. Un monitor de máquina virtual puede también crear este modo de privilegio planificando un procesador virtual de agente de protección para ejecutar el agente de protección.

Conclusión

Las herramientas anteriormente descritas pueden hacer a un agente de protección no modificable o inaccesible de un modo de privilegio de sistema operativo, ya sea posibilitando que el agente de protección resida en una localización que es inaccesible del modo de privilegio de sistema operativo, o creando un modo de privilegio de agente de protección. Aunque las herramientas se han descrito en lenguaje específico a características estructurales y/o actos metodológicos, se ha de entender que las herramientas definidas en las reivindicaciones adjuntas no están necesariamente limitadas a las características específicas o actos descritos. En su lugar, las características específicas y actos se desvelan como formas ejemplares de implementar las herramientas.

REIVINDICACIONES

1. Uno o más medios legibles por ordenador que tienen instrucciones legibles por ordenador en los mismos que, cuando se ejecutan por un dispositivo (102) informático, provocan que el dispositivo (102) informático realice actos que comprenden:

recibir (902), en un monitor (108) de máquina virtual que opera en un modo (124) de privilegio de monitor de máquina virtual, una solicitud desde un agente de protección de que un rango de memoria (206, 306) puede hacerse inalterable desde o inaccesible desde un modo (126) de privilegio de sistema operativo, residiendo el agente de protección en el rango de memoria (206, 306);
hacer (904), por el monitor de máquina virtual, el rango de memoria (206, 306) inalterable desde o inaccesible desde el modo (126) de privilegio de sistema operativo y establecer, por el monitor de máquina virtual, un temporizador para ejecutar el agente de protección; y
ejecutar (908), cuando se agota el temporizador, el agente (144) de protección que opera en un modo (132) de privilegio de agente de protección;
en el que el modo (132) de privilegio de agente de protección es más privilegiado que el modo (126) de privilegio de sistema operativo pero menos privilegiado que el modo (124) de privilegio de monitor de máquina virtual.

2. El medio de la reivindicación 1, en el que el temporizador ordena al monitor (108) de máquina virtual ejecutar el agente (144) de protección a intervalos regulares.

3. El medio de la reivindicación 1, en el que el agente (144) de protección está configurado para recibir (906) una política de cumplimiento que describe uno o más recursos (120) accesibles desde el modo (126) de privilegio de sistema operativo y, en respuesta a la recepción de la política de cumplimiento, determinar (910) si uno o más del uno o más recursos (120) han sido modificados.

4. El medio de la reivindicación 3, que comprende adicionalmente apagar (912) un sistema (114) operativo asociado con el modo (126) de privilegio de sistema operativo en respuesta a una determinación por el agente (144) de protección de que uno o más del uno o más recursos (120) han sido modificados.

5. El medio de la reivindicación 3, en el que el uno o más recursos (120) incluyen una tabla de despacho de servicio de sistema SSDT, una tabla de despacho de interrupción IDT, o una tabla de descriptor global GDT.

6. El medio de la reivindicación 1, que comprende adicionalmente recibir (914), en el monitor (108) de máquina virtual y después de la ejecución (908) del agente (144) de protección, una notificación de que el agente (144) de protección ha finalizado la ejecución.

7. El medio de la reivindicación 1, que comprende adicionalmente:

apagar un sistema (114) operativo asociado con el modo (126) de privilegio de sistema operativo en respuesta a un intento de acceso, desde el modo (126) de privilegio de sistema operativo, del rango de memoria (206, 306) o el agente (144) de protección; y/o
realizar ciclos (916) entre la ejecución (908) del agente (144) de protección y la no ejecución del agente (144) de protección, de manera que al menos cuando se ejecuta el agente (144) de protección es inalterable o inaccesible desde el modo (126) de privilegio de sistema operativo.

8. Un procedimiento que comprende:

recibir (902), en un monitor (108) de máquina virtual que opera en un modo (124) de privilegio de monitor de máquina virtual, una solicitud desde un agente de protección de que un rango de memoria (206, 306) puede hacerse inalterable desde o inaccesible desde un modo (126) de privilegio de sistema operativo, residiendo el agente de protección en el rango de memoria (206, 306);
hacer (904), por el monitor de máquina virtual, el rango de memoria (206, 306) inalterable desde o inaccesible desde el modo (126) de privilegio de sistema operativo y establecer, por el monitor de máquina virtual, un temporizador para ejecutar el agente de protección; y
ejecutar (908), cuando se agota el temporizador, el agente (144) de protección que opera en un modo (132) de privilegio de agente de protección;
en el que el modo (132) de privilegio de agente de protección es más privilegiado que el modo (126) de privilegio de sistema operativo pero menos privilegiado que el modo (124) de privilegio de monitor de máquina virtual.

9. El procedimiento de la reivindicación 8, en el que el temporizador ordena que el monitor (108) de máquina virtual ejecute el agente (144) de protección a intervalos regulares.

10. El procedimiento de la reivindicación 8, en el que el agente (144) de protección está configurado para recibir (906) una política de cumplimiento que describe uno o más recursos (120) accesibles desde el modo (126) de privilegio de sistema operativo y, en respuesta a la recepción de la política de cumplimiento, determinar (910) si uno o más del uno o más recursos (120) han sido modificados.

11. El procedimiento de la reivindicación 10, que comprende adicionalmente apagar (912) un sistema (114) operativo asociado con el modo (126) de privilegio de sistema operativo en respuesta a una determinación por el agente (144) de protección de que uno o más del uno o más recursos (120) han sido modificados.

12. El procedimiento de la reivindicación 10, en el que el uno o más recursos (120) incluyen una tabla de despacho de servicio de sistema SSDT, una tabla de despacho de interrupción IDT, o una tabla de descriptor global GDT.

13. El procedimiento de la reivindicación 8, que comprende adicionalmente recibir (914), en el monitor (108) de máquina virtual y después de la ejecución (908) del agente (144) de protección, una notificación de que el agente (144) de protección ha finalizado la ejecución.

14. El procedimiento de la reivindicación 8, que comprende adicionalmente:

apagar un sistema (114) operativo asociado con el modo (126) de privilegio de sistema operativo en respuesta a un intento de acceso , desde el modo (126) de privilegio de sistema operativo, del rango de memoria (206, 306) o el agente (144) de protección; y/o
realizar ciclos (916) entre la ejecución (908) del agente (144) de protección y la no ejecución del agente (144) de protección, de manera que al menos cuando se ejecuta el agente (144) de protección es inalterable o inaccesible desde el modo (126) de privilegio de sistema operativo.

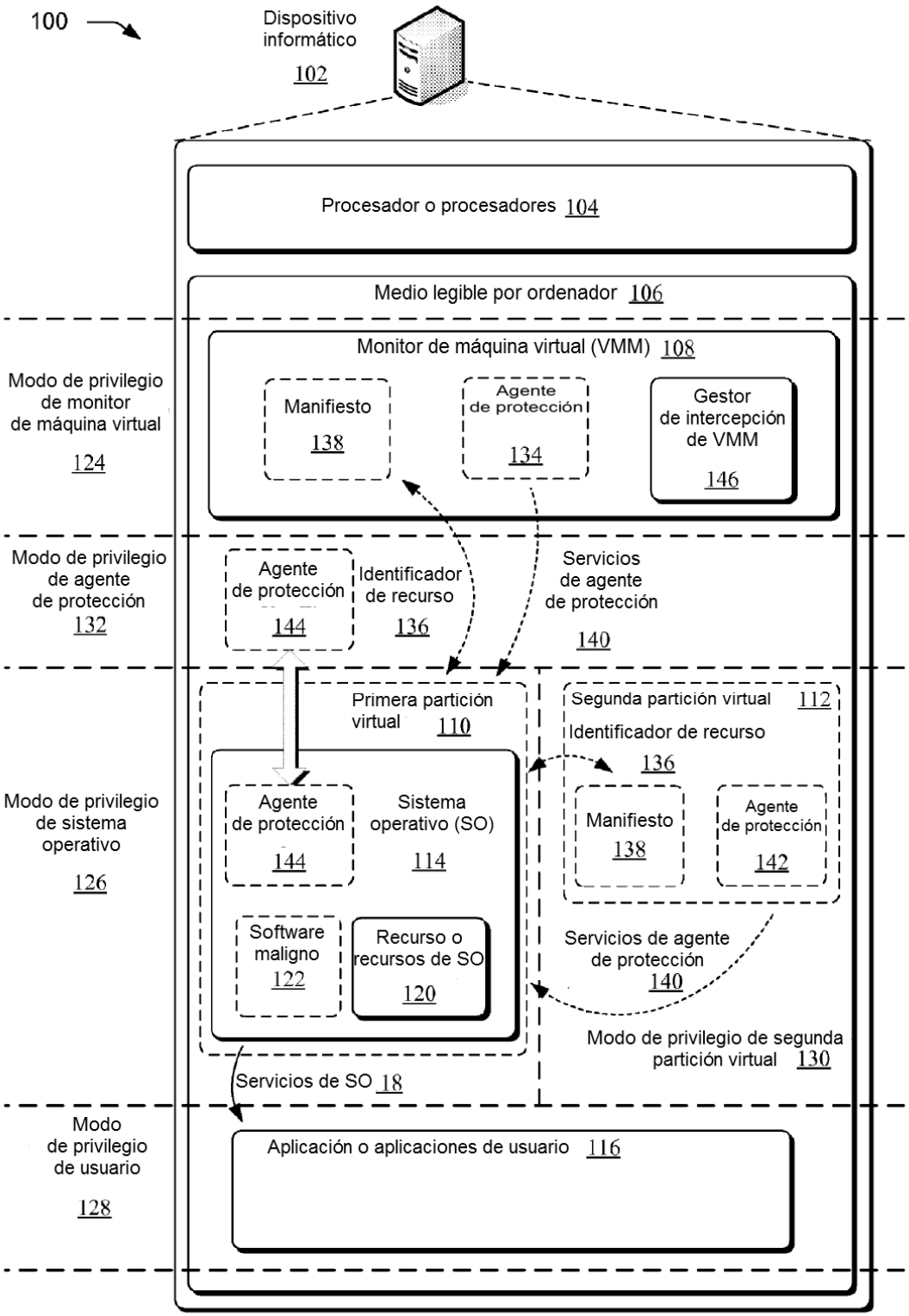
100
Dispositivo informático
102
Procesador o procesadores 104
Medio legible por ordenador 106
Monitor de máquina virtual (VMM) 108
Manifiesto
138
Agente de protección
134
Gestor de intercepción de VMM
146
Modo de privilegio de monitor de máquina virtual
124
Modo de privilegio de agente de protección
132
Agente de protección
144
Identificador de recurso
136
Servicios de agente de protección
140
Primera partición virtual
110
Segunda partición virtual
112
Identificador de recurso
136
Modo de privilegio de sistema operativo
126
Agente de protección
144
Sistema operativo (SO)
114
Manifiesto
138
Agente de protección
142
Software maligno
122
Recurso o recursos de SO
120
Servicios de agente de protección
140
Modo de privilegio de segunda partición virtual
130
Servicios de SO 18
Modo de privilegio de usuario
128
Aplicación o aplicaciones de usuario
116

FIG. 1

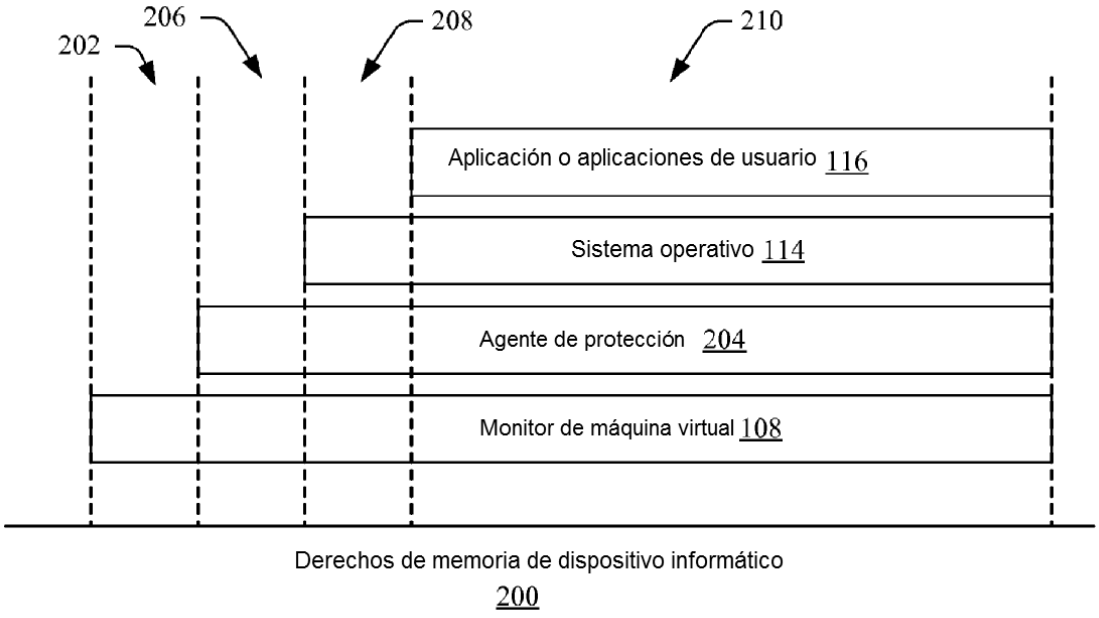
206
208
210
202
Aplicación o aplicaciones de usuario 116
Sistema operativo 114
Agente de protección 204
Monitor de máquina virtual 108
Derechos de memoria de dispositivo informático
200

FIG. 2

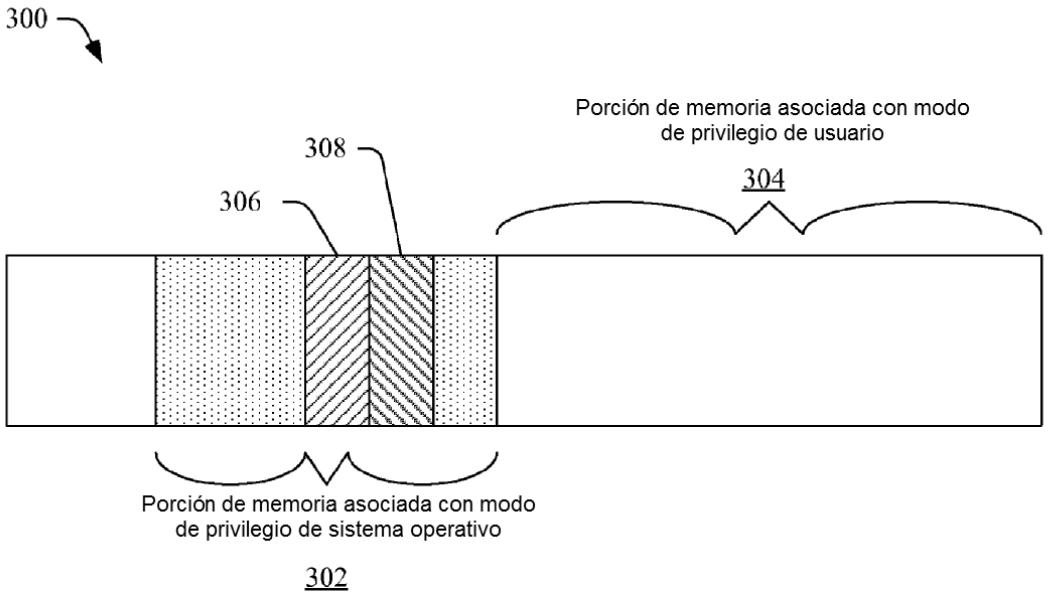
300
Porción de memoria asociada con modo de privilegio de usuario
308
304
306
Porción de memoria asociada con modo de privilegio de sistema operativo
302

FIG. 3

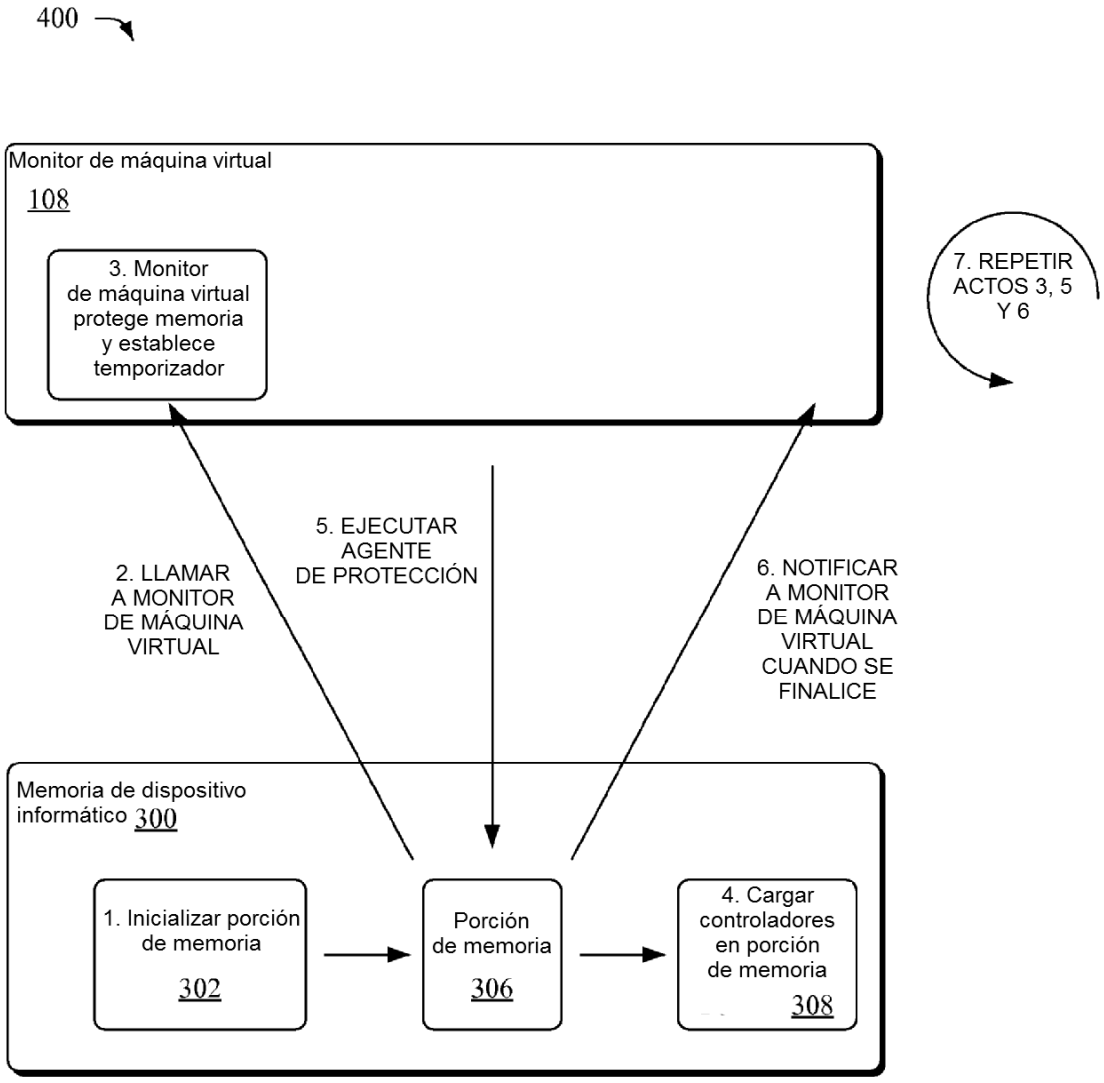
400
Monitor de máquina virtual
108
3. Monitor de máquina virtual protege memoria y establece temporizador
7. REPETIR ACTOS 3, 5 Y 6
2. LLAMAR A MONITOR DE MÁQUINA VIRTUAL
5. EJECUTAR AGENTE DE PROTECCIÓN
6. NOTIFICAR A MONITOR DE MÁQUINA VIRTUAL CUANDO SE FINALICE
Memoria de dispositivo informático 300
1. Inicializar porción de memoria 302
Porción de memoria 306
4. Cargar controladores en porción de memoria 308

FIG. 4

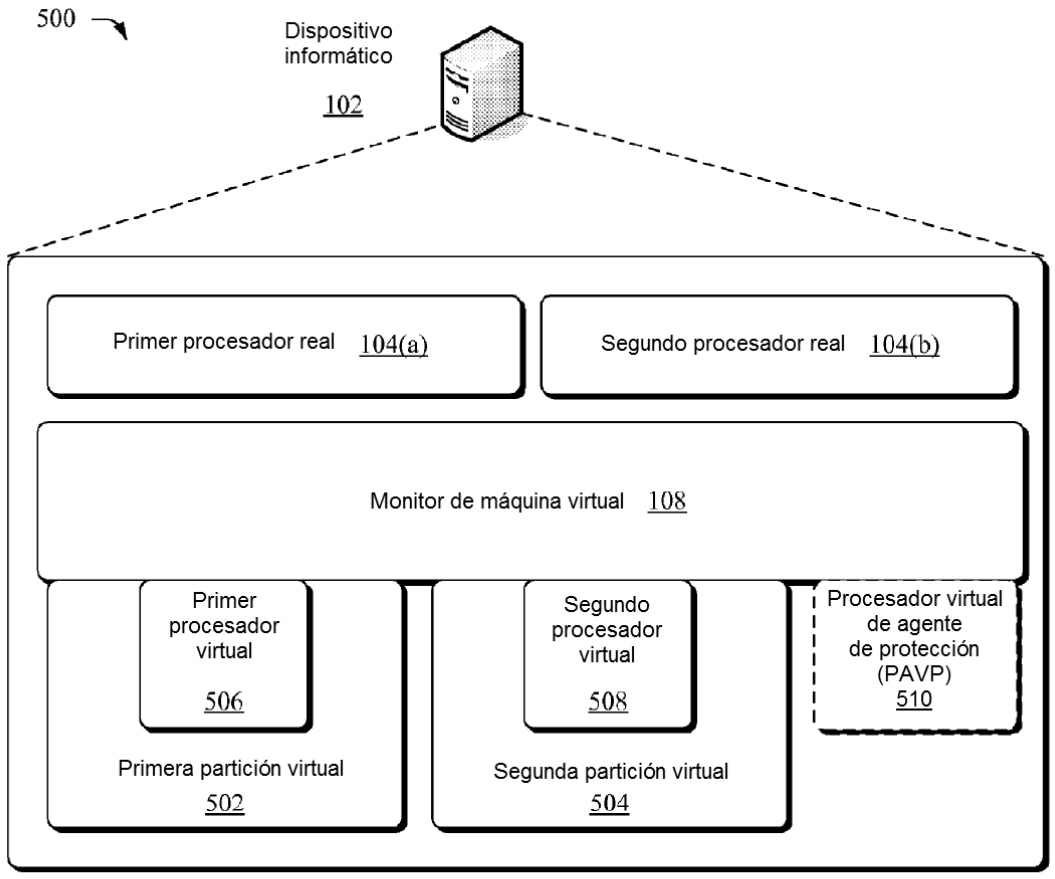
500
Dispositivo informático
102
Primer procesador real 104(a)
Segundo procesador real 104(b)
Monitor de máquina virtual 108
Primer procesador virtual 506
Segundo procesador virtual 508
Procesador virtual de agente de protección (PAVP) 510
Primera partición virtual 502
Segunda partición virtual 504

FIG. 5

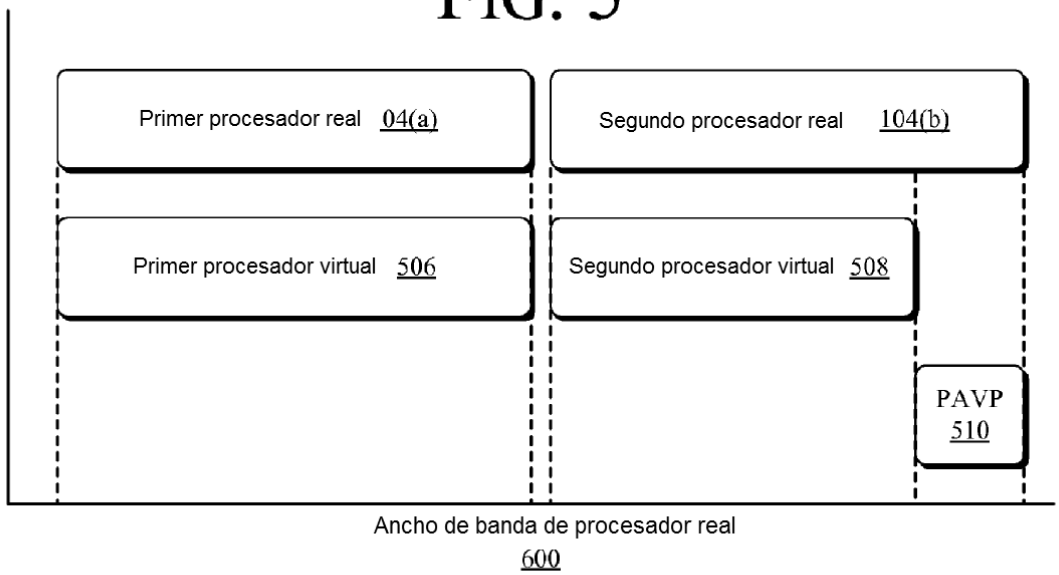
Primer procesador real 04(a)
Segundo procesador real 104(b)
Primer procesador virtual 506
Segundo procesador virtual 508
PAVP 510
Ancho de banda de procesador real 600

FIG. 6

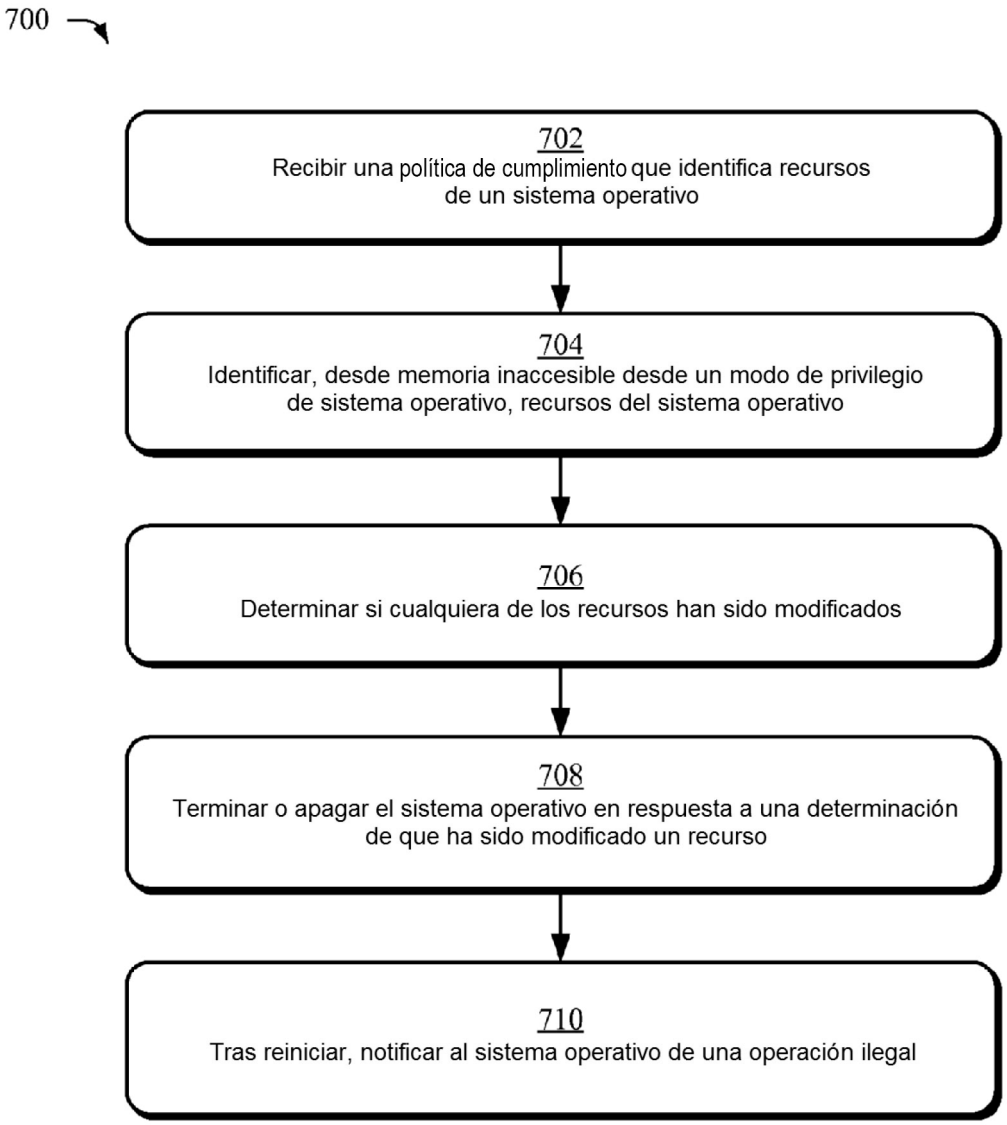
700
702
Recibir una política de cumplimiento que identifica recursos de un sistema operativo
704
Identificar, desde memoria inaccesible desde un modo de privilegio de sistema operativo, recursos del sistema operativo
706
Determinar si cualquiera de los recursos han sido modificados
708
Terminar o apagar el sistema operativo en respuesta a una determinación de que ha sido modificado un recurso
710
Tras reiniciar, notificar al sistema operativo de una operación ilegal

FIG. 7

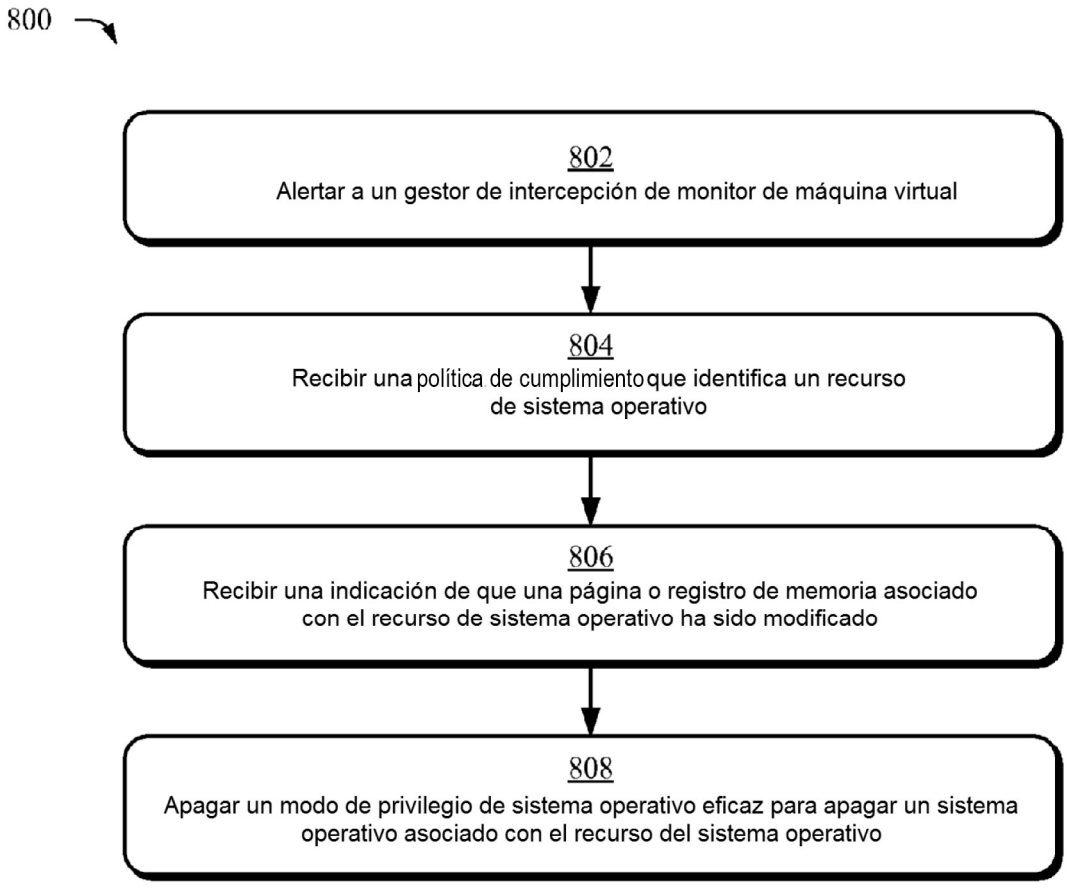
800
802
Alertar a un gestor de intercepción de monitor de máquina virtual
804
Recibir una política de cumplimiento que identifica un recurso de sistema operativo
806
Recibir una indicación de que una página o registro de memoria asociado con el recurso de sistema operativo ha sido modificado
808
Apagar un modo de privilegio de sistema operativo eficaz para apagar un sistema operativo asociado con el recurso del sistema operativo

FIG. 8

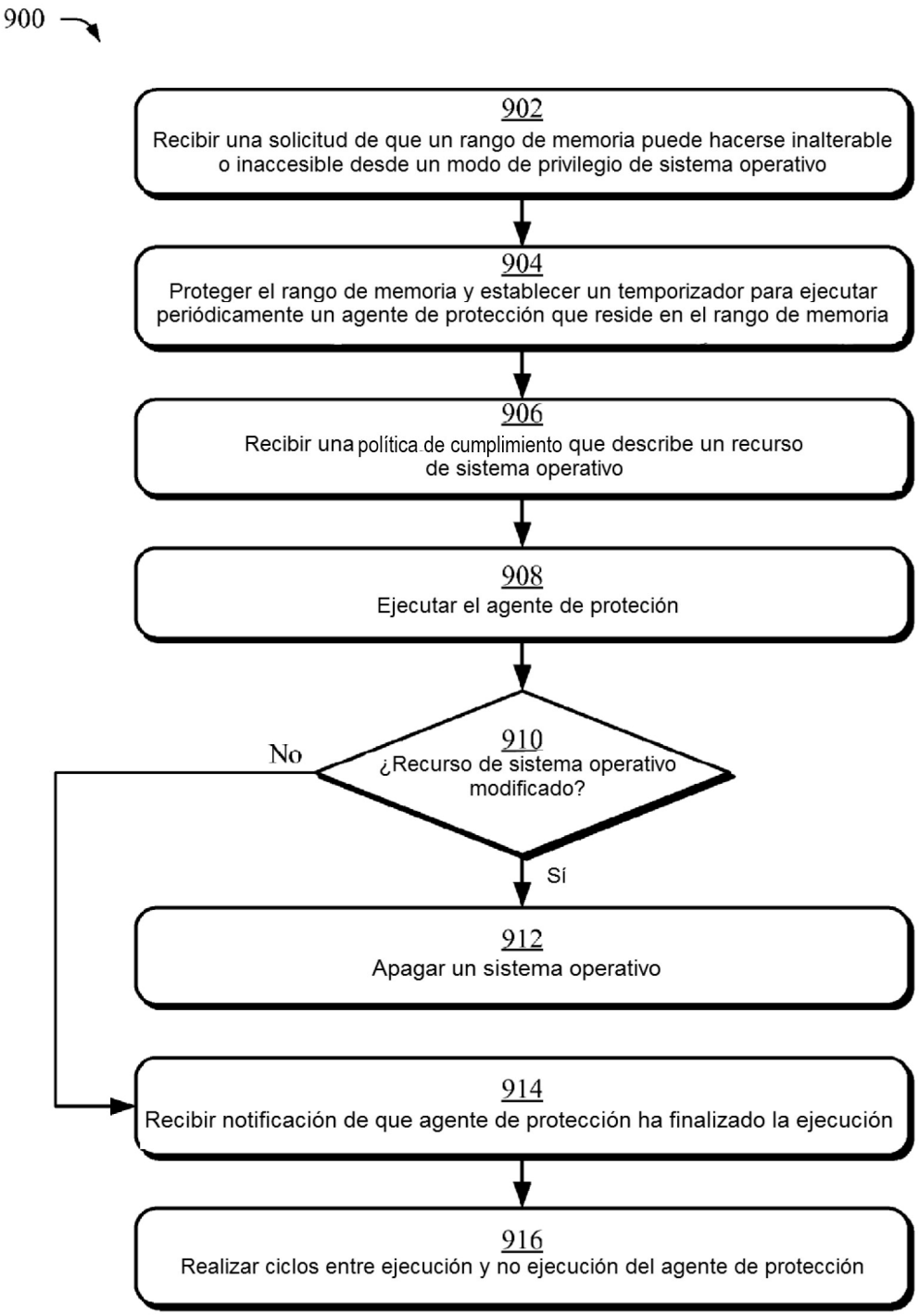
900
902
Recibir una solicitud de que un rango de memoria puede hacerse inalterable o inaccesible desde un modo de privilegio de sistema operativo
904
Proteger el rango de memoria y establecer un temporizador para ejecutar periódicamente un agente de protección que reside en el rango de memoria
906
Recibir una política de cumplimiento que describe un recurso de sistema operativo
908
Ejecutar el agente de proteción
910
¿Recurso de sistema operativo modificado?
No
Sí
912
Apagar un sistema operativo
914
Recibir notificación de que agente de protección ha finalizado la ejecución
916
Realizar ciclos entre ejecución y no ejecución del agente de protección

FIG. 9

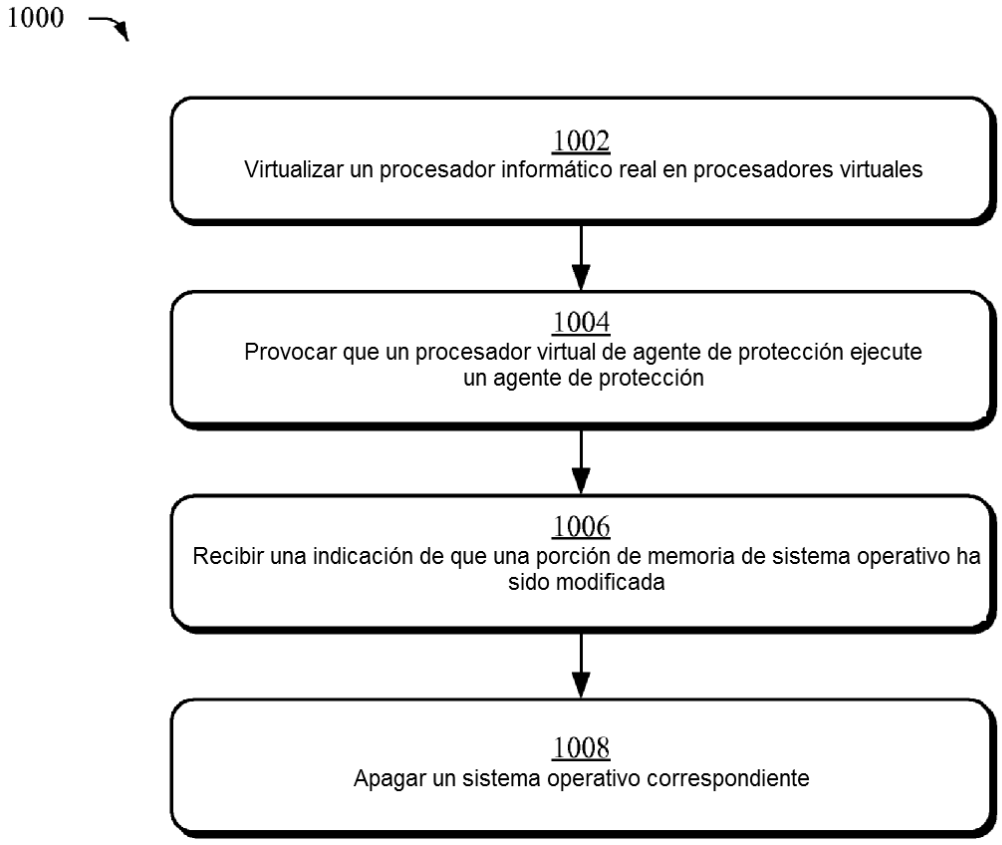
1000
1002
Virtualizar un procesador informático real en procesadores virtuales
1004
Provocar que un procesador virtual de agente de protección ejecute un agente de protección
1006
Recibir una indicación de que una porción de memoria de sistema operativo ha sido modificada
1008
Apagar un sistema operativo correspondiente

FIG. 10

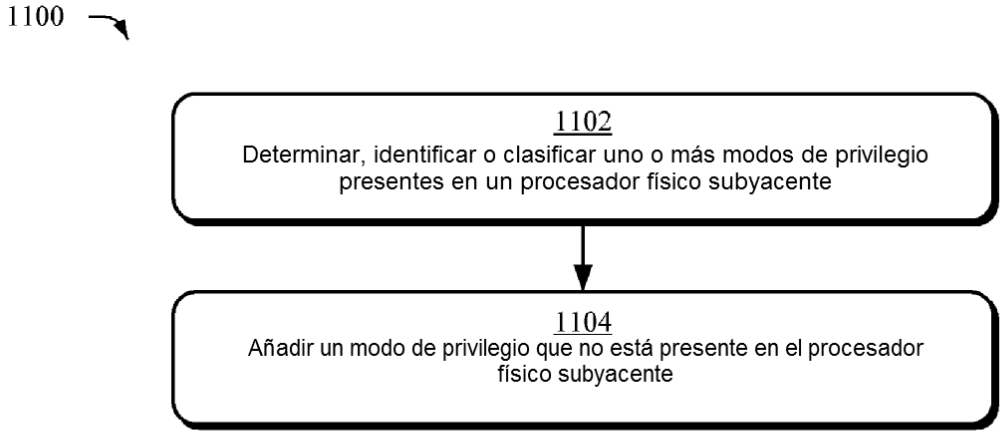
1100
1102
Determinar, identificar o clasificar uno o más modos de privilegio presentes en un procesador físico subyacente
1104
Añadir un modo de privilegio que no está presente en el procesador físico subyacente

FIG. 11