(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 860**

(51) Int. CI.:

G06F 21/53 (2013.01)
G06F 21/78 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **08.04.2009 PCT/FR2009/050623**

(87) Fecha y número de publicación internacional: **12.11.2009 WO2009136080**

(96) Fecha de presentación y número de la solicitud europea: **08.04.2009 E 09742278 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2274701**

(54) Título: **Sistema y procedimiento de aseguramiento de un ordenador que incluye un micronúcleo**

(30) Prioridad:

08.04.2008 FR 0852336

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2017

(73) Titular/es:

AIRBUS DS SAS (100.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR

(72) Inventor/es:

CLERMONT, NICOLAS;
HAUGUET, FRANCIS y
MEIER, GUILLAUME

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y procedimiento de aseguramiento de un ordenador que incluye un micronúcleo

La presente invención se refiere a un sistema y un procedimiento de aseguramiento de un ordenador que incluye un micronúcleo. Se refiere igualmente a un producto de programa de ordenador que pone en práctica el procedimiento.

Los sistemas operativos clásicos tales como Microsoft Windows, GNU/Linux u otros no se han concebido con unas fuertes restricciones de seguridad. El resultado es una concepción débilmente asegurada en forma de un sistema operativo en dos capas: la primera capa está compuesta por un núcleo ejecutado en un modo privilegiado y la segunda capa por unas aplicaciones que se ejecutan en un modo sin privilegios denominado modo usuario. El núcleo es típicamente un núcleo monolítico, incluso si se elige un enfoque modular para gestionar en particular todos los recursos ofrecidos por el sistema operativo. El núcleo incluye los programas de bajo nivel tal como el planificador, el gestor de procesos, el gestor de memoria así como los controladores de los periféricos y aquellos servicios de alto nivel tales como los sistemas de archivos, las pilas de red, los algoritmos criptográficos, etc.

En consecuencia, el núcleo incluye unos millones de líneas de código con un número proporcional de errores de software y de defectos de seguridad. No puede por tanto verificarse como que está de acuerdo con las especificaciones con los verificadores de código y los sistemas de prueba formales actuales. Además, tienen malas propiedades de aislamiento. De hecho, los procesos de usuario pueden romper el aislamiento de diferentes modos gracias a los tubos, a los ficheros, a la memoria compartida, etc. La gestión de las comunicaciones entre procesos no es fiable. Además, no existe aislamiento en el interior del núcleo, entre subsistemas del núcleo como, por ejemplo, entre los controladores y las pilas de red. De ese modo, un controlador de un componente de hardware defectuoso o corrompido puede poner en peligro todo el sistema.

Según aumentan los riesgos de seguridad, los diseñadores del núcleo han ensayado el aseguramiento de los núcleos existentes añadiendo unos gestores de acceso obligatorio (Mandatory Access Control - MAC) con una pequeña granularidad para implementar el concepto de “Reference Monitor”, o Supervisor de Referencia. De hecho, los sistemas operativos actuales implementan generalmente una Gestión de Acceso Discrecional (Discretionary Access Control - DAC) que no puede resolver el problema genérico de código malicioso, especialmente de los virus. Unos ejemplos de mejora de seguridad del sistema operativo son SELinux, GRSecurity, AppArmor, RSBAC, SEBSD, etc.

Sin embargo, esas implementaciones no cumplen con las condiciones de Supervisor de Referencia porque las funciones de seguridad que forman parte del núcleo no están protegidas y son inutilizables en el interior del dominio del núcleo: no ofrecen ninguna protección entre subsistemas del núcleo. Además, como estos núcleos gestionan el conjunto de los recursos del sistema, es difícil describir una política de seguridad y el resultado es complejo en términos de configuración y de gestión, lo que hace imposible la verificación formal.

Todas estas debilidades no permiten una verificación formal de la protección ofrecida por estos sistemas operativos y generan una cantidad de amenazas de seguridad que limitan el uso de estos sistemas en los entornos que tengan una gran exigencia de seguridad. Además, el espacio de memoria del núcleo está compartido entre todos los procesos, con todos los subsistemas, incluso si estos pertenecen a unos niveles de seguridad diferentes. En consecuencia, los sistemas operativos actuales no ofrecen un entorno sano y asegurado.

Como reacción a la complejidad de los núcleos monolíticos actuales, unos investigadores han propuesto el concepto de micronúcleo que se caracteriza por el desplazamiento de un máximo de servicios al exterior del núcleo, en el espacio de usuario. Estas funcionalidades se proporcionan entonces por pequeños servidores independientes que poseen su propio espacio de direccionamiento.

El micronúcleo se limita así a algunas funciones de base cuya gestión de las comunicaciones entre los servidores se realiza por transferencia de mensajes (IPC-Inter Process Communication). Además de esta gestión, un micronúcleo comprende un controlador de reloj y un planificador.

De ese modo, mientras que un núcleo monolítico tradicional incluye varios millones de líneas de código, un micronúcleo incluye en general menos de 20.000 líneas de código.

Se entiende entonces la atracción de los diseñadores de sistemas asegurados para los micronúcleos puesto que tienen un tamaño que permite mantenerles fácilmente y pueden verificarse formalmente. Pueden certificarse así al nivel más alto, EAL7, de los criterios comunes.

Uno de los micronúcleos más conocidos y utilizados actualmente en diferentes variantes es el micronúcleo L4 concebido e implementado por Jochen Liedtke.

Sin embargo, al lado del micronúcleo en sí, se hace necesario desarrollar los servidores necesarios para que el sistema ofrezca las funcionalidades esperadas de un sistema operativo moderno.

También, para evitar la reescritura completa de un sistema operativo, se ha propuesto utilizar el micronúcleo como base de un hipervisor de virtualización sobre el que se ejecuta uno o varios sistemas operativos tradicionales. En efecto un micronúcleo y el conjunto de los servidores gestores necesarios para la división de los recursos cumplen nativamente la función de hipervisor, a saber la división de los recursos disponibles entre las máquinas virtuales y la emulación de los eventos materiales (no incluyen los controladores de periféricos, solamente unos buses de los sistemas que no pueden compartirse), ofreciendo así una tecnología de virtualización nativa eficaz, denominada de nivel “sistema”.

En este sentido, el proyecto L4 Linux de la Universidad de Dresde (Alemania) ha trasladado el núcleo Linux sobre el micronúcleo L4/Fiasco y su capa de servicios, creando así un LINUX (para) virtualizado que se ejecuta por encima de un hipervisor, en un modo totalmente no privilegiado, en modo usuario.

En términos de seguridad, un sistema de ese tipo se aprovecha de la solidez del micronúcleo. Sin embargo, la seguridad de los servidores depende igualmente de la solidez de las comunicaciones IPC porque es un medio posible de transmisión de datos peligrosos. Ahora bien, por razones de eficacia, la gestión de la seguridad de las comunicaciones se deja tradicionalmente para los servidores, contentándose el micronúcleo con transmitir los mensajes. El micronúcleo puede sin embargo ofrecer un mecanismo de derechos de comunicación; dos tareas no pueden comunicar entre sí más que si poseen los derechos apropiados. En caso contrario, la comunicación se redirige hacia un servidor específico de control de las comunicaciones que autorizará o no la comunicación *on-the-fly*, en función de la política de seguridad.

Además, las arquitecturas de micronúcleo actuales son tales que se “cablea” una política de seguridad en las reglas de acceso del micronúcleo de tal manera que, incluso en un contexto de virtualización con varias máquinas virtuales, todas presentan la misma política de seguridad.

De ese modo, sería particularmente ventajoso tener una arquitectura de micronúcleo asegurado que permita un buen control de los accesos de las máquinas virtuales así como una granularidad y una flexibilidad en la puesta en práctica de una o varias políticas de seguridad sobre un mismo sistema.

El documento de GERNOT HEISER (OPEN KERNEL LABS ET ÁL: “TECHNOLOGY WHITE PAPER. Virtualization for Embedded Systems”, INTERNET CITATION, 27 de noviembre de 2007 (2007-11-27), página 30pp, XP007908697, divulga un procedimiento de aseguramiento de un ordenador que incluye un micronúcleo (“OKL4”) y unos medios de interfaz con al menos un sistema operativo (“OK Linux”).

Según un primer aspecto de la invención, se propone un procedimiento de aseguramiento de un ordenador según la reivindicación 1.

Según otras características y modo de realización, los medios externos incluyen unos medios de almacenamiento de datos criptográficos secretos y porque toda transmisión de datos criptográficos secretos se asegura antes del almacenamiento.

Según un segundo aspecto de la invención, la invención se refiere también a un producto de programa de ordenador según la reivindicación 8.

Según un tercer aspecto, se propone además un ordenador según la reivindicación 9.

La invención se comprenderá mejor con la lectura de la descripción que sigue, dada únicamente a título de ejemplo, y realizada con referencia a los dibujos adjuntos en los que:

- la figura 1 es una vista esquemática de las capas de software de un ordenador que incluye un software de virtualización; y

- la figura 2 es un ordinograma de un procedimiento de aseguramiento según un modo de realización de la invención.

Con referencia a la Figura 1, un ordenador incluye clásicamente por encima del hardware representado simbólicamente por la capa 1, un micronúcleo 3. Este micronúcleo 3 gestiona una parte del hardware directamente, a saber el procesador, los manejadores de memoria, el manejador de interrupciones y el controlador de reloj. Por encima del micronúcleo 3 se ejecutan los diferentes servidores gestores de recursos, simbolizados por la capa 4, teniendo cada uno a su cargo la gestión de un subconjunto de objetos núcleos de un tipo dado. Para alcanzar el nivel de seguridad máximo, se asigna a un servidor gestor un tipo de recursos por dominio de seguridad (por ejemplo un gestor de memoria física por nivel, poseyendo cada una, unas zonas de memoria distintas). Los servidores gestores 4 presentan a unos sistemas operativos virtualizados 7 una interfaz que permite el acceso a los recursos gestionados. Unos controladores de periféricos 5 tienen a su cargo la gestión de un periférico y están íntimamente ligados a un mediador de acceso 11, 11’. El mediador 11’ está encargado de multiplexar los accesos al periférico entre varios sistemas concurrentes, mientras que los mediadores 11 están encargados de aplicar los procesamientos específicos a cada sistema (cifrado,…). Particularmente, los mediadores 11, 11’ presentan un sistema operativo virtualizado 7 a un periférico virtual. El conjunto de las interfaces expuestas por los mediadores

por un lado y los gestores de recursos por otro lado constituyen una “máquina virtual”. Los mediadores 11, 11’ incluyen unas reglas de seguridad definidas en un módulo 13 de gestión de política de seguridad y almacenadas en unos medios de almacenamiento 15.

En esta descripción, se da un sentido amplio al término sistema operativo que comprende un sistema operativo per se tal como el sistema operativo Windows de Microsoft Inc. o el sistema Linux, así como al conjunto de las aplicaciones que se ejecutan en este sistema operativo.

En el modo de realización descrito, el sistema operativo 7 está encerrado en una “jaula” constituida por la máquina virtual y en particular por los mediadores 11, 11’. De ese modo, por ejemplo, cualquier solicitud de presentación del sistema operativo 7 pasa a través de un mediador de presentación. Igualmente, los flujos de red pasan a través de un mediador de red, etc.

Los mediadores 11, 11’ están unidos a los controladores 5 de periféricos correspondientes encargados clásicamente del control del hardware.

El funcionamiento es entonces el siguiente, figura 2.

Cada vez que tiene lugar una transmisión de información entre el sistema operativo 7 y un controlador 5 u otro elemento externo al sistema operativo 7, el mediador 11, 11’ correspondiente intercepta el flujo de información, etapa 20.

Posteriormente, se analiza este flujo, etapa 22, en función de las reglas de acceso predefinidas. Si el flujo está conforme, etapa 24, con estas reglas, se transmite en 26 normalmente a su destinatario.

Si, por el contrario, si este flujo no está conforme con al menos una de las reglas, se anula, etapa 28, es decir que el destinatario no recibe el flujo y el emisor recibe, eventualmente, un mensaje de error de transmisión, o bien se modifica en 30 antes de ser transmitido en 26 al destinatario. La modificación tiene como función hacer válido el flujo con relación a la o las reglas violadas por el flujo en su estado inicial.

Pueden definirse varios tipos de mediadores en función del tipo de filtro y/o del componente de hardware asociado.

Por ejemplo, un primer tipo de mediador se define para los recursos de hardware compartidos por varios sistemas operativos, siendo ejecutado cada uno de dichos sistemas en una “jaula” virtual. Por ejemplo, una máquina posee en general una única tarjeta de red. Es necesario entonces compartir su utilización entre los diferentes sistemas operativos virtualizados para dar a cada uno acceso a la red.

De ese modo, se define un controlador en la capa de virtualización constituida por el micronúcleo y unos servidores gestores y el mediador correspondiente controlan todos los accesos. En el caso de la tarjeta de red, cada sistema operativo recibe su propia dirección MAC a través del mediador. De ese modo, un paquete de datos que entra en la interfaz física es gestionado por el controlador. El mediador de la tarjeta de red actúa como un punto virtual transmitiendo el paquete al sistema operativo adecuado. Es posible igualmente cerciorarse de que los paquetes salientes no son falseados por el sistema operativo, por ejemplo, modificando la dirección MAC de la fuente.

Otro ejemplo se refiere al acceso a los discos. Por ejemplo, si el sistema operativo virtualizado ha recibido como espacio de almacenamiento la primera partición del primer disco, el acceso a las otras particiones será rechazado por el mediador vinculado al controlador de almacenamiento.

De manera clásica, la comunicación entre dos sistemas operativos virtualizados sobre una misma máquina se realiza por intermedio del acceso a la red virtual totalmente gestionado por el software de virtualización. De ese modo cada sistema operativo transmite la información al otro como si el segundo sistema operativo se encontrara en una máquina diferente unida por una red de datos.

Un segundo tipo de mediador se asocia con unos periféricos de red virtuales para cerciorarse de que sólo son posibles unas comunicaciones autorizadas. El mediador juega entonces, siguiendo la política de seguridad establecida, el papel de cortafuegos bloqueando el tráfico no autorizado, o bien, cifra las comunicaciones para transmitirlas a un sistema operativo que funciona con otro nivel de seguridad.

Un tercer tipo de mediador toma a su cargo las funciones criptográficas evitando la exposición de secretos en un entorno no asegurado. De ese modo, es posible evitar confiar a otro sistema operativo no asegurado unas operaciones sensibles.

Por ejemplo, unos datos sensibles que deben almacenarse solamente de manera privada, se transmiten por el sistema operativo al controlador de almacenamiento para que sean escritos sobre el disco duro. El mediador correspondiente intercepta la transmisión de los datos, los cifra con una clave conocida sólo para él y los transmite cifrados al controlador de almacenamiento. De ese modo, la clave de cifrado no se “expone” jamás al sistema operativo no asegurado.

Los mediadores permiten ventajosamente definir un nivel de seguridad para cada sistema operativo.

Como el micronúcleo asociado a los mediadores es mucho menos complejo que un sistema operativo, es más fácil escribir un software de virtualización seguro y que pueda probarse como correcto.

De ese modo, el aislamiento de cada sistema operativo sobre su máquina virtual con el nivel de seguridad adecuado permite obtener un aseguramiento al menos igual al obtenido utilizando unas máquinas separadas.

Además, es posible definir una política de seguridad definiendo las acciones y comunicación autorizadas para cada nivel de seguridad. Esto incluye la atribución de un dispositivo, la autorización de un recurso compartido, las comunicaciones autorizadas, las restricciones para exportar/importar datos del dominio de protección asociado.

Mediante la centralización de la gestión de la política de seguridad en un módulo específico y mediante la descentralización a la altura de cada mediador de la puesta en práctica de estas reglas, es posible así garantizar la obtención de un nivel de seguridad coherente y evolutivo.

En efecto, la política de seguridad se pone en práctica por los mediadores a través de las reglas de seguridad. Es posible por tanto tener unas políticas dinámicas por difusión a los mediadores de nuevas reglas por ejemplo, para contrarrestar un ataque específico, y sin afectar a los otros niveles de seguridad.

Se comprende que una utilización extensiva de los mediadores permite “enjaular” los sistemas operativos virtualizados. En efecto, instalando un mediador en cada punto de conexión, todos los flujos de información, tanto entrante como saliente, son filtrados por los mediadores. De ese modo, como los mediadores son un software seguro que aplica una política de seguridad, un sistema operativo virtualizado no puede hacer nada distinto que lo que se especifica en la política de seguridad. Si no, la operación es rechazada.

Esto permite ejecutar los sistemas operativos sin privilegio particular, en particular sin privilegio de entrada/salida o de instrucciones.

Además, el “enjaulado” es transparente para el sistema operativo virtualizado porque no puede marcar la diferencia entre un flujo procedente del mediador y un flujo procedente de un dispositivo de hardware. Esto permite unos procesamientos adicionales de seguridad sobre los flujos para proteger unos datos del sistema operativo sin implicarle. Por ejemplo, un mediador de antivirus puede escanear el contenido de una llave USB antes de montarla en el sistema operativo.

Los mediadores pueden estar encadenados entre sí lo que permite ventajosamente ejecutar varias operaciones sobre un flujo.

Por ejemplo, para escribir sobre la llave USB, es posible encadenar un mediador antivirus y posteriormente el mediador de cifrado.

De ese modo, es posible obtener ventajosamente una seguridad física protegiendo los datos sensibles que pertenecen a diferentes dominios de seguridad sobre un mismo soporte físico.

Otra ventaja es que la protección se aplica sin tener que modificar o que implicar al sistema operativo, tanto para la protección como para la configuración. De ese modo, el sistema operativo virtualizado se convierte en sin necesidad de configuración para la seguridad, siendo asegurada la configuración de este por las políticas de seguridad puestas en práctica por los mediadores.

El sistema operativo se configura en la inicialización por los mediadores que determinan las reglas de acceso y ponen en práctica la política a lo largo de la ejecución.

En efecto, la política de seguridad puede estructurarse según unas reglas por clase de mediadores, lo que tiene la ventaja de permitir una gran modularidad: la implementación de una clase particular de mediadores puede reemplazarse sin tener que reescribir el conjunto de la política de seguridad, sólo deben reescribirse las reglas relativas a una clase particular. De la misma manera pueden realizarse unas modificaciones dinámicamente, es decir durante el tiempo de ejecución, solamente sobre unos mediadores específicos, que se refieren únicamente a los dominios específicos sin impactar en la protección de las otras interfaces o dominios.

De ese modo, la administración de la plataforma escribe unas reglas de acceso para cada mediador, especificando los clientes autorizados, y los recursos asignados así como las acciones asociadas. Todos los archivos de configuración de los mediadores se reúnen entonces en un único archivo de política de seguridad. Para inicializar un nuevo sistema operativo virtual, o dominio, el cargador comienza por buscar en este archivo los mediadores que tienen este dominio como cliente, posteriormente no autoriza las comunicaciones de este dominio más que con estos mediadores.

El sistema operativo no puede extralimitarse con los mediadores y por tanto la política de seguridad. Posteriormente los mediadores aplican independientemente unos de otros las reglas de acceso definidas para este dominio sobre estos objetos.

Se comprende que pueden realizarse diferentes variantes a partir de esta descripción.

REIVINDICACIONES

1. Procedimiento de aseguramiento de un ordenador que incluye un micronúcleo (3), al menos un sistema operativo (7) virtualizado, una pluralidad de controladores de periférico (5) y al menos un mediador de acceso (11) que filtra el flujo de información asociado a cada controlador de periférico (5) y que presenta a dicho sistema operativo virtualizado un periférico virtual, incluyendo dicho micronúcleo un controlador de reloj, un planificador y un gestor de comunicación entre procesos, al menos una máquina virtual, asociada a cada sistema operativo, que está formada por dicho núcleo, unos gestores de recursos, los controladores de periférico (5) y los mediadores de acceso (11), caracterizado por que el procedimiento incluye, en los mediadores acceso (11), las etapas de:

- interceptar (20) cualquier comunicación entre uno de los controladores de periféricos y dicho sistema operativo virtualizado,

- verificar (24) que la comunicación interceptada está conforme con unas reglas de acceso predefinidas para dicho sistema operativo virtualizado;

- transmitir (26) la comunicación interceptada al destinatario si la comunicación interceptada está conforme con las reglas de acceso predefinidas,

y por que cada sistema operativo virtualizado no está autorizado, en la inicialización, a comunicar más que con los mediadores que tienen ese sistema operativo como cliente.

2. Procedimiento según la reivindicación 1, caracterizado por que en la inicialización de cada sistema operativo, un cargador busca, en un archivo único de política de seguridad que comprende todos los archivos de configuración de los mediadores, los mediadores que tienen dicho sistema operativo como cliente.

3. Procedimiento según la reivindicación 1 o 2, caracterizado por que el ordenador incluye una pluralidad de sistemas operativos virtualizados cada uno aislado sobre su máquina virtual, el procedimiento incluye una etapa de multiplexado, mediante uno de los mediadores de acceso, de los accesos por los sistemas operativos virtualizados a uno de los controladores de periféricos asociado.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado por que unos medios externos incluyen unos medios de almacenamiento de datos criptográficos secretos y por que toda transmisión de datos criptográficos secretos está asegurada antes del almacenamiento.

5. Procedimiento según una de las reivindicaciones 1 a 4 en el que, el micronúcleo y al menos dos controladores de periféricos que forman al menos dos máquinas virtuales en cada una de las cuales se ejecuta un único sistema operativo, al menos un mediador de acceso adicional (11') permite la comunicación entre los sistemas operativos y verifica la conformidad de dichas comunicaciones con relación a unas reglas de seguridad de acceso.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, en el que, para cada sistema operativo, en una etapa previa, se define una política de seguridad en la forma de un juego de reglas de acceso para los mediadores en relación con dicho sistema operativo.

7. Procedimiento según la reivindicación 6, en el que las reglas de acceso asociadas a la política de seguridad de dicho sistema operativo se proporcionan a los mediadores de acceso antes de la inicialización de dicho sistema operativo.

8. Producto de programa de ordenador que comprende unas instrucciones de código de programa grabadas sobre un soporte legible por un ordenador para poner en práctica las etapas del procedimiento según una cualquiera de las reivindicaciones 1 a 7 cuanto dicho programa funciona sobre un ordenador.

9. Ordenador que incluye:

- un micronúcleo (3) que incluye un controlador de reloj, un planificador y un gestor de comunicación entre procesos,

- al menos un sistema operativo virtualizado (7),

- una pluralidad de controladores de periféricos (5);

- unos gestores de recursos,

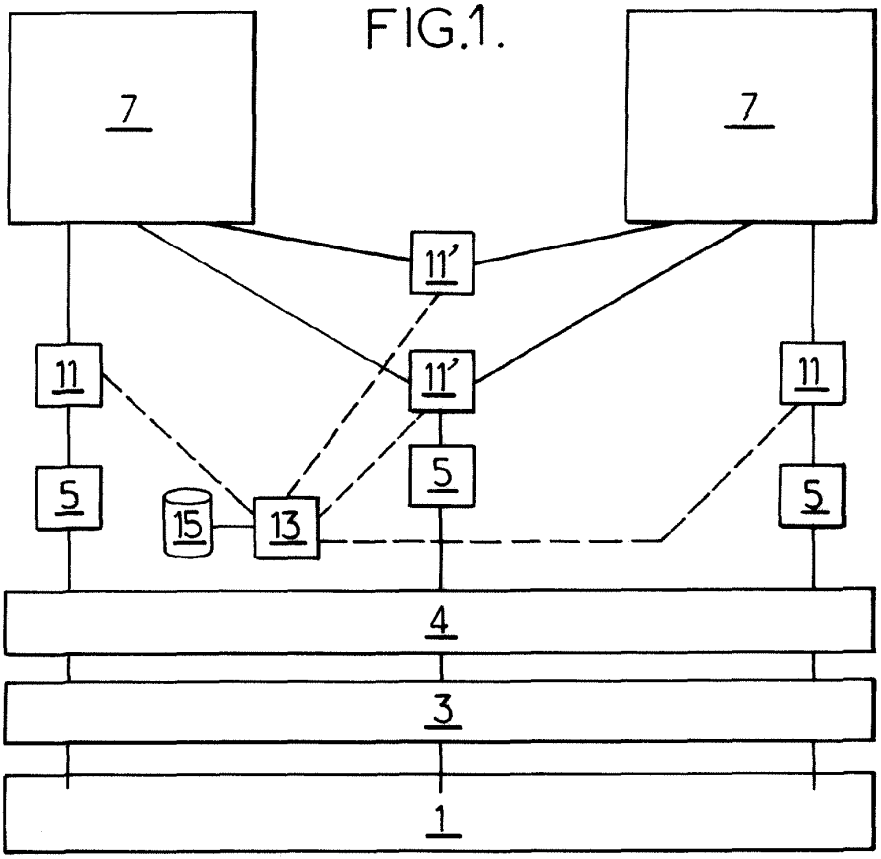
caracterizado por que comprende al menos un mediador de acceso (11) asociado a cada controlador de periférico y acoplado al sistema operativo virtualizado para formar al menos una máquina virtual asociada a cada sistema operativo virtualizado que permite la ejecución de este,

estando adaptado cada uno de los mediadores de acceso (11, 11') para filtrar el flujo de información asociado a cada controlador de periférico (5) y presentando al sistema operativo virtualizado un periférico virtual interceptando

cualquier comunicación entre el controlador de periférico correspondiente y el sistema operativo virtualizado, y no trasmitir dicha comunicación interceptada más que si están validadas unas reglas de seguridad de acceso al controlador de periférico específicas para cada sistema operativo virtualizado por dicha comunicación interceptada, no autorizándose a cada sistema operativo virtualizado a comunicar, en la inicialización, más que con los mediadores que tienen ese sistema operativo como cliente.

10. Ordenador según la reivindicación 9, caracterizado por que en la inicialización de cada sistema operativo, un cargador busca, en un archivo único de política de seguridad que comprende todos los archivos de configuración de los mediadores, los mediadores que tienen dicho sistema operativo como cliente.

FIG.1.


7
7
11'
11
11'
11
5
5
5
15
13
4
3
1

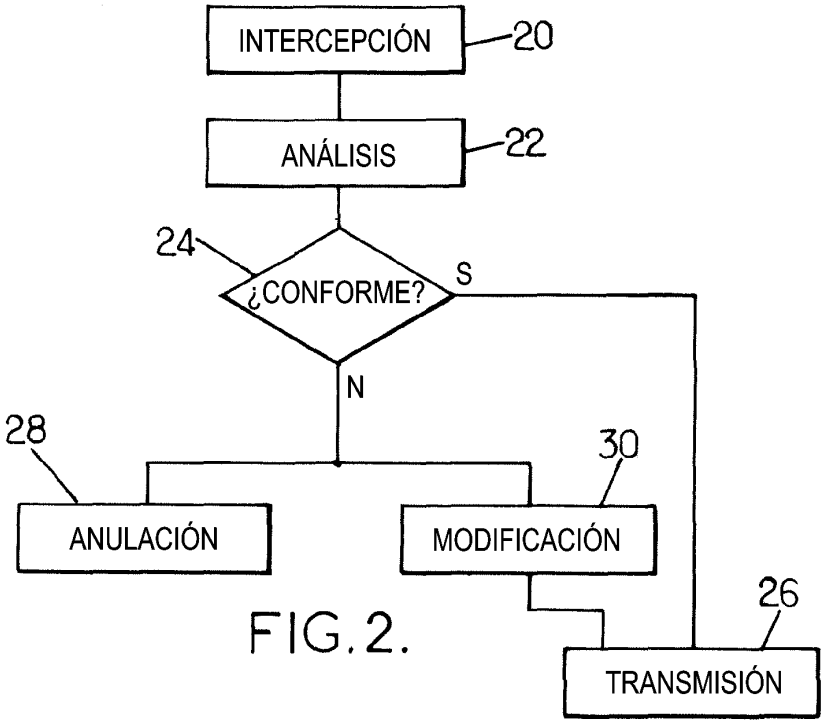

INTERCEPCIÓN
20
ANÁLISIS
22
24
¿CONFORME?
S
N
28
30
ANULACIÓN
MODIFICACIÓN
26
TRANSMISIÓN

FIG.2.