(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 675 160**

(51) Int. CI.:

H04N 21/4627 (2011.01)
H04N 21/4623 (2011.01)
H04N 21/443 (2011.01)
H04N 21/81 (2011.01)
G06F 9/455 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.10.2013 PCT/EP2013/071194**

(87) Fecha y número de publicación internacional: **08.05.2014 WO14067760**

(96) Fecha de presentación y número de la solicitud europea: **10.10.2013 E 13774208 (6)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 2915336**

(54) Título: **Dispositivo de tratamiento de contenidos multimedia que aplica una pluralidad de máquinas virtuales**

(30) Prioridad:

05.11.2012 FR 1260478

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.07.2018

(73) Titular/es:

VIACCESS (100.0%)
Les Collines de l'Arche Tour Opéra C
92057 Paris La Défense, FR

(72) Inventor/es:

SANCHEZ-LEIGHTON, VICENTE

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Dispositivo de tratamiento de contenidos multimedia que aplica una pluralidad de máquinas virtuales

[0001] La presente invención se refiere a un dispositivo de tratamiento de contenidos multimedia, apto para recibir unos contenidos multimedia cifrados, protegidos por un sistema de protección de contenidos y para suministrar dichos contenidos multimedia en forma descifrada a un dispositivo usuario.

[0002] Más generalmente, la invención se sitúa en el campo de la distribución protegida de contenidos multimedia suministrados por un proveedor de contenidos y de unos dispositivos de tratamiento y de visualización de tales contenidos, por ejemplo, los dispositivos de televisión digital enriquecida o «smart TVs» en terminología anglosajona.

[0003] Tales dispositivos de televisión digital enriquecida comprenden clásicamente unos medios de restitución visual y sonora de los contenidos multimedia, de forma típica un televisor, así como un decodificador, ya sea integrado con los medios de restitución o en forma de una caja separada conectada con los medios de restitución. Tal decodificador comprende unos medios de recepción de contenidos multimedia protegidos, por ejemplo, cifrados con la ayuda de una palabra de control, unos medios de aplicación de control de acceso y unos medios de descifrado de los contenidos multimedia recibidos en caso de validación de las condiciones de acceso, unos medios de decodificación y de restitución de los contenidos multimedia recibidos.

[0004] Además, los dispositivos de televisión digital enriquecida recientes presentan igualmente unos medios de conexión a Internet y permiten al usuario descargar y acceder a unos servicios aplicativos de terceros (por ejemplo unos juegos, unos servicios bancarios), que provienen de servidores de terceros que son totalmente independientes del proveedor de contenidos multimedia o del operador que es, por ejemplo, un proveedor de servicios de telecomunicaciones, proveedor del dispositivo de televisión digital enriquecida, que es un intermediario entre el proveedor del contenido y el usuario.

[0005] Actualmente, desde un punto de vista de arquitectura de *software*, el conjunto de los servicios aplicativos y de los servicios relativos a los contenidos multimedia están organizados en una misma pila de *software*, estructurada por encima de un solo sistema operativo. Tal arquitectura de *software* conduce potencialmente a unos problemas de seguridad de los contenidos multimedia y de los datos relativos a los servicios aplicativos de terceros. En efecto, la integración de numerosos servicios, procedentes de fuentes heterogéneas, en una misma pila de *software*, aumenta la probabilidad de errores y de debilidades de *software*, que están en la base de los ataques y el pirateo. En particular, se conoce que cuanto más voluminoso es un *software*, más aumenta la probabilidad de errores.

[0006] Ahora bien, en el campo de la distribución de los contenidos multimedia protegidos, es crucial preservar los derechos de los proveedores de contenido, evitar la recuperación de contenidos descifrados y su restitución o su distribución con excepción de estos derechos. Los servicios relativos a los contenidos multimedia y los contenidos multimedia en sí mismos deben ser protegidos, por tanto.

[0007] Por otro lado, ciertos datos relativos a los servicios aplicativos de terceros deben ser protegidos igualmente, tanto si se trata por ejemplo de datos bancarios como de datos confidenciales en otros campos, que el usuario no desea difundir sin autorización por su parte.

[0008] Así, unos dispositivos de televisión digital enriquecida que permiten a la vez el acceso a unos contenidos multimedia protegidos y el acceso a unos servicios aplicativos que provienen de servidores de terceros diversos presentan fuertes exigencias de seguridad, que no son satisfechas por los dispositivos con arquitectura de *software* con pila de *software* única.

[0009] El documento US2010/263059 A1 describe un dispositivo de tratamiento de contenidos multimedia, de tipo set-top box, que consta de unos módulos de acceso a unos servicios personalizados.

[0010] El documento US2006/0136720 A1 describe un sistema de seguridad informático con varias máquinas virtuales.

[0011] La invención tiene como objeto solucionar este defecto de seguridad de los dispositivos de televisión digital enriquecida del estado de la técnica. A tal efecto, la invención propone un dispositivo de tratamiento de

contenidos multimedia conforme a la reivindicación 1.

[0012] Ventajosamente, la separación en tres grupos de máquinas virtuales controladas por un hipervisor, con un grupo de máquinas virtuales destinado a aplicar todos los servicios de seguridad que tienen un primer nivel de seguridad asociado permite asegurar una mejor seguridad y resistencia a los eventuales ataques que la arquitectura de *software* a una sola pila de *software*. En efecto, los grupos de máquinas virtuales colocados de este modo se ejecutan de manera estrictamente separada y por encima de un hipervisor particularmente compacto, lo que limita claramente, por construcción, los riesgos de ataques.

[0013] Además, ventajosamente, el grupo de máquinas virtuales destinado a aplicar todos los servicios de seguridad asegura un papel de tercero de confianza.

[0014] El dispositivo de tratamiento de contenidos multimedia según la invención puede presentar una o varias de las características siguientes:

- el tercer grupo consta al menos de una máquina virtual que ejecuta un servicio de descifrado multimedia;
- consta además de unos medios de almacenamiento de datos relativos a los servicios aplicados;
- consta de unos medios de acceso a una red de comunicaciones y dichos servicios aplicativos de terceros son descargados por el usuario a través de dicha red de comunicaciones;
- dicho tercer grupo consta de una máquina virtual que ejecuta un servicio de terceros de confianza, apto para comunicar con un servicio aplicado por una máquina virtual del primer grupo o con un servicio aplicado por una máquina virtual del segundo grupo a través de los canales seguros;
- las máquinas virtuales de dicho tercer grupo tienen unos privilegios de ejecución atribuidos por dicho hipervisor superiores a los privilegios de ejecución atribuidos respectivamente a las máquinas virtuales de dicho primer grupo y segundo grupo;
- cada máquina virtual de dicho primer grupo ejecuta un servicio aplicativo de terceros o un agregado de servicios aplicativos de terceros;
- consta de un número predeterminado de procesadores físicos y dicho hipervisor es apto para controlar dichos procesadores físicos.

[0015] Otras características y ventajas de la invención se desprenderán de la descripción que se da a continuación, a título indicativo y en absoluto limitativo, en referencia a las figuras anexas, entre las que:

- la figura 1 representa un sistema de suministro de contenidos multimedia cifrados que comprende un dispositivo de tratamiento de contenidos multimedia según la invención;
- la figura 2 ilustra esquemáticamente un modo de realización de la arquitectura de *software* propuesta, y
- la figura 3 representa esquemáticamente un hipervisor en un modo de realización de la invención.

[0016] El sistema 1 de suministro de contenidos multimedia cifrados de la figura 1 comprende un transmisor 2, gestionado por ejemplo por un proveedor de contenidos o por uno o varios operador(es), que está adaptado para difundir unos contenidos multimedia cifrados con la ayuda de una palabra de control a un conjunto de receptores. Para simplificar, tal receptor único 4 se ilustra en la figura 1.

[0017] En el modo de realización ilustrado en la figura 1, el transmisor 2 está provisto de una antena de transmisión. El transmisor transmite, además de los contenidos multimedia cifrados, unos mensajes de control de los títulos de acceso o ECM (para «Entitlement Control Messages» en inglés) que comprenden una palabra de control adaptada para descifrar los contenidos multimedia cifrados y unos mensajes de gestión de los títulos de acceso o EMM (para «Entitlement Management Messages» en inglés).

[0018] El receptor 4 es de forma típica un dispositivo de tratamiento de contenidos multimedia según la invención, como por ejemplo un dispositivo de televisión digital enriquecida.

[0019] El dispositivo de tratamiento de contenidos multimedia 4 consta de unos medios de restitución de los contenidos multimedia 6, de forma típica una pantalla combinada con unos medios de restitución sonora, unos medios de control clásicos 7, por ejemplo un mando a distancia, que permiten a un usuario controlar diversas funcionalidades ofrecidas por el dispositivo 4, por una parte unas funcionalidades vinculadas a los contenidos multimedia (por ejemplo lectura, cambio de fuente, pausa, retroceso) y, por otra parte, unas funcionalidades vinculadas a la instalación y al uso de otros servicios aplicativos de terceros. El dispositivo 4 consta igualmente de un decodificador 8 provisto de una antena de recepción, apta para recibir unos contenidos multimedia cifrados, para

decodificarlos después de su descifrado y para suministrarlos a continuación a los medios de restitución 6 que forman, con los medios de control 7, un dispositivo usuario en este ejemplo de realización.

[0020] El dispositivo de tratamiento de contenidos multimedia 4 consta igualmente de unos medios 10 de control de los títulos de acceso a los contenidos cifrados, que aplican de manera conocida, los mensajes ECM y EMM recibidos y su tratamiento en función de una suscripción del usuario del dispositivo 4. En un modo de realización, los medios de control 10 que aplican un sistema de acceso condicional tal como se describe en «Functional Model of a Conditional Access System», EBU Review, Technical European Broadcasting Union, Bruxels, BE, N° 266, a 21 de diciembre de 1995.

[0021] Este dispositivo 4 consta igualmente de unos medios de descifrado 12 de los contenidos multimedia recibidos y de medios de desencriptación 12 de los contenidos multimedia recibidos y de medios de desencriptación 14 de las palabras de control encriptadas recibidas a través de los mensajes de control de los títulos de acceso ECM.

[0022] Los medios de descifrado 12 y de desencriptación 14 son unos medios aptos para ejecutar unos servicios de seguridad, que tienen un primer nivel de seguridad, que es el nivel de seguridad más elevado considerado. En particular, esto significa que es importante devolver los servicios de seguridad aplicados por estos medios muy difíciles de piratear por cualquier tipo de ataques.

[0023] Diversos parámetros necesarios para la aplicación de los servicios de seguridad se almacenan en una memoria 16 asociada.

[0024] Los medios de desencriptación 14 y de descifrado 12 se aplican para suministrar unos contenidos multimedia descifrados a partir de los contenidos multimedia recibidos, siendo estos contenidos multimedia descifrados suministrados a continuación al decodificador 8 apto para decodificarlos en tiempo real para suministrar unos contenidos multimedia decodificados, adaptados para ser restituidos en los medios de restitución 6.

[0025] El dispositivo de tratamiento de contenidos multimedia 4 consta además de unos medios de conexión 18 a una red de comunicaciones 20, que es por ejemplo la red Internet.

[0026] Además, unos medios 22 de ejecución de servicios aplicativos están igualmente presentes, teniendo estos servicios aplicativos un nivel de seguridad asociado inferior al primer nivel de seguridad, que necesita, por tanto, una seguridad menor.

[0027] Por ejemplo, unos servicios aplicativos de terceros de nivel de seguridad inferior al primer nivel de seguridad son de forma típica unas aplicaciones de *software* suministradas por unos servidores de terceros y descargadas e instaladas por un usuario del dispositivo de tratamiento de contenidos multimedia 4. Un servidor de terceros 24 es de forma típica totalmente independiente del proveedor u operador que está a cargo del transmisor 2.

[0028] Por ejemplo, un servicio aplicativo de terceros puede ser una aplicación bancaria que permita al usuario consultar sus datos bancarios. Otro servicio aplicativo de terceros es, por ejemplo, una aplicación de juego compatible con los medios de restitución 6 y los medios de control 7 disponibles.

[0029] Unos medios de almacenamiento 26 de los parámetros y datos relativos a los servicios aplicativos de terceros están igualmente presentes.

[0030] En un modo de realización alternativo, el dispositivo de tratamiento 4 que aplica la invención se implementa en la forma de una caja de conexión de tipo *set-top box*, apta para transmitir unos contenidos multimedia descifrados a un dispositivo usuario que tiene unos medios de restitución de los contenidos multimedia, como un televisor. La figura 2 ilustra la arquitectura de *software* que permite implementar los diversos medios aplicados descritos en referencia a la figura 1 según un modo de realización de la invención.

[0031] En este modo de realización, el conjunto de los servicios aplicados por el dispositivo de tratamiento de contenidos multimedia 4 está dividido en tres grupos de máquinas virtuales, señaladas respectivamente como G1, G2 y G3, que están controlados por un hipervisor o VMM (para «Virtual Machine Monitor» en inglés), señalado con 30 en la figura 2.

[0032] Un hipervisor es un mecanismo de *software* conocido que permite crear, en un soporte material

compuesto por uno o varios procesadores, un número cualquiera de procesadores virtuales aislados e independientes y particionar igualmente la memoria (RAM, SRAM, etc.). Un hipervisor se describirá más detalladamente a continuación en referencia a la figura 3.

[0033] El hipervisor 30 controla los grupos de máquinas virtuales G1, G2 y G3 a través de unas instrucciones 31, 32, 33 que atribuyen unos privilegios de ejecución a cada máquina virtual y a cada grupo de máquinas virtuales. Las diferentes máquinas virtuales se ejecutan de manera estrictamente separada incluso si pertenecen a un mismo grupo.

[0034] El primer grupo de máquinas virtuales G1 aplica los medios de ejecución 22 de los servicios aplicativos de terceros, que provienen de servidores de terceros que son controlados por unos proveedores de aplicaciones independientes del o de los operadores proveedores de contenidos multimedia. Los servidores de terceros son accesibles a través de la red de comunicaciones 20 y los servicios aplicativos de terceros son descargados e instalados por el usuario.

[0035] Cada máquina virtual de este primer grupo ejecuta una pila de *software* correspondiente a un conjunto de servicios aplicativos de terceros dado, respectivamente señalados como APP_1, APP_2 y APP_3 en la figura. En el ejemplo ilustrado en la figura 2, una sola máquina virtual se representa en el grupo G1, su pila de *software* está constituida por varios aplicativos de terceros: 34 asociado al servicio APP_1, 35 al servicio APP_2 y 36 al servicio APP_3.

[0036] Como variante, se considera agregar unos servicios aplicativos similares, que tienen unas funcionalidades muy próximas y superpuestas, por razones de rendimiento, en una sola pila de *software*, ejecutada por una máquina virtual. En este caso, una máquina virtual del primer grupo ejecuta un agregado de servicios aplicativos de terceros.

[0037] Por otro lado, un modo de ejecución del procesador virtual del grupo de máquinas virtuales G1 37 específico, que tiene un nivel de privilegio de ejecución elevado, está dedicado a la aplicación de un sistema operativo OS1, por ejemplo, el conjunto Linux completado del conjunto de bibliotecas necesarias para la ejecución de APP1, APP2, APP3, comúnmente llamado *runtime*.

[0038] El segundo grupo de máquinas virtuales G2 está dedicado a las aplicaciones o servicios aplicativos 38 controlados por el operador o uno de los operadores que están a cargo del transmisor 2 de contenidos multimedia cifrados, pero que tienen un nivel de seguridad asociado inferior al primer nivel de seguridad. Los servicios suministrados por el operador se soportan por un sistema operativo OS2, aplicado por un modo privilegiado 39 del procesador virtual.

[0039] El sistema operativo OS2 puede ser diferente del sistema operativo OS1, que permite así cohabitar unos entornos de ejecución heterogéneos.

[0040] Se puede considerar que el nivel de seguridad de estos servicios suministrados por el o los operadores es diferente del nivel de seguridad asociado a los servicios aplicativos de terceros instalados por el usuario, pero es inferior no obstante al nivel de seguridad a la vez del grupo G3 de gestión de la seguridad y al máximo del hipervisor.

[0041] Por ejemplo, estos servicios suministrados por los operadores incluyen el plan de pago de contenidos multimedia, el plan de re-visionado de contenido («replay» en inglés), la recomendación de contenidos, los contenidos sin pago, etc.

[0042] En un modo de realización, los servicios suministrados por un operador son instalados con antelación en el dispositivo de tratamiento de contenidos multimedia 4, durante la puesta a disposición del usuario de este dispositivo. Una actualización de los servicios suministrados por el operador puede ser considerada de igual modo. En este caso, se prevé autentificar al operador, a través de un protocolo de autentificación, por el hipervisor 30, de manera que un servicio aplicativo transmitido por el operador sea instalado por el hipervisor 30 para una ejecución por una máquina virtual del segundo grupo de máquinas virtuales G2.

[0043] Todos los servicios suministrados por el operador y que necesitan un nivel de seguridad elevado igual al primer nivel de seguridad, denominados servicios de seguridad, en particular los servicios aplicados por los medios de control de acceso 10, de descifrado 12 y de desencriptación 14, son ejecutados cada uno por una máquina virtual del tercer grupo de máquinas virtuales G3 o por un proceso de una de sus máquinas virtuales. En

particular, una máquina virtual del grupo G3 suministra un servicio de desencriptación a un servicio de control de acceso, que permite verificar los derechos de acceso del usuario al contenido multimedia.

[0044] El grupo de máquinas virtuales señalado como G3 o grupo de seguridad, ejecuta por otro lado otros servicios de primer nivel de seguridad, como por ejemplo la visualización segura, el almacenamiento seguro, el acceso red segura, la introducción de contraseñas y/o de nombres de usuario, etc.

[0045] Una máquina virtual de este grupo de máquinas virtuales G3 implementa un servicio de vigilancia 40 o control de seguridad, que le permite verificar la conformidad de la ejecución de los servicios aplicados respectivamente por los otros grupos de máquinas virtuales y detener/reiniciar («reboot») las máquinas virtuales referidas si es necesario. En cuanto el comportamiento de una de las máquinas virtuales de los grupos G1 y G2 se aparta o parece apartarse, de los requisitos previos de seguridad declarados por cada uno de estos grupos, el servicio de vigilancia de seguridad 40, podrá tomar, si el contrato de ejecución de uno de los grupos G1 o G2 lo exige, la decisión de detener y relanzar una o el conjunto de las máquinas virtuales del grupo, si su comportamiento sale del marco predefinido, a la manera de los anti-*malwares* o antivirus.

[0046] El grupo de máquinas virtuales G3 implementa igualmente un servicio “de terceros de confianza” 41, que asegura el reparto equitativo de los recursos materiales disponibles: memorias 16, 26, conexiones de red 18, tiempos de ejecución y utilización de los procesadores físicos presentes, en particular de los procesadores especializados tipo GPU.

[0047] Las máquinas virtuales de los otros grupos de máquinas virtuales estarán conectadas a este servicio “de terceros de confianza” 41 a través de los canales seguros 42, 44, permitiéndoles dialogar con el servicio “de terceros de confianza” 41 según un protocolo específico. Un canal de comunicación seguro es un canal cuya utilización no puede poner en peligro directamente el funcionamiento de las máquinas virtuales que lo utilizan. Incluso si una de las máquinas virtuales que utilizan este canal seguro está comprometida, es la presa de los atacantes, el hecho de utilizar este canal no podrá provocar directamente un deterioro de la seguridad de la otra máquina virtual que utiliza el canal. Tales canales seguros son conocidos por el experto en la materia: están construidos principalmente en unos recursos (procesador, memoria, bus) asignados estáticamente y de forma estrictamente limitada. Por supuesto, ningún canal seguro podrá detener unos ataques por canales y deducciones indirectos, pero podrán aminorar la velocidad de la propagación de la amenaza y dar tiempo para una respuesta por parte del grupo de seguridad G3.

[0048] Así, el servicio “de terceros de confianza” 41 asegura, según unas especificaciones preestablecidas, el contrato de seguridad de cada grupo de máquinas, la protección y la integridad de ciertos datos de los grupos G1 y G2 y la estanqueidad relativa a unos ataques o defectos.

[0049] La figura 3 representa de manera esquemática una aplicación en el marco de la arquitectura de procesadores Intel® de un hipervisor 30 que controla dos máquinas virtuales señaladas respectivamente como VM_0 y VM_n.

[0050] El hipervisor 30 está desarrollado en forma de programa de *software*, sobre un soporte material ofrecido por un número n dado de procesadores físicos adaptados. Dos procesadores tales señalados como 50, 52 se ilustran en la figura. El conjunto de procesadores físicos consta de un gestor de memoria virtual llamado MMU (para «Memory Management Unit» en inglés).

[0051] El hipervisor 30 se ejecuta desde la instalación y controla el conjunto de los recursos materiales a fin de reemplazar la explotación de los n procesadores físicos nativos por la de un conjunto de procesadores virtuales o máquinas virtuales.

[0052] De manera clásica, la virtualización de procesador comprende la modificación de los códigos fuentes de los sistemas operativos de los procesadores físicos de tal forma que las instrucciones privilegiadas sean reemplazadas por unos servicios equivalentes suministrados por el hipervisor. Las otras instrucciones son en cuanto a ellas mismas ejecutadas directamente por los procesadores reales. En el marco de la arquitectura Intel® representada por la figura 3, esta modificación de las fuentes no es necesaria ya que los procesadores de esta arquitectura que disponen de la tecnología VT-x simulan de forma material el contexto completo de un procesador virtual con una compatibilidad total.

[0053] Esta funcionalidad es realizada por un módulo 54 que efectúa el control de los procesadores físicos,

en colaboración con un *software* de control y de configuración 56.

[0054] El hipervisor 30 comprende igualmente un módulo 58 de virtualización de la memoria, de los espacios de dirección de memoria y de las entradas-salidas.

[0055] El hipervisor se ejecuta en el modo más privilegiado de los procesadores físicos, los sistemas operativos virtualizados en un modo menos privilegiado que el del hipervisor y las aplicaciones y servicios gestionados por los sistemas operativos virtualizados en un modo incluso menos privilegiado si está disponible, si no en el mismo que el sistema operativo virtualizado, como se ilustra por la superposición de la figura 3.

[0056] En este caso dos módulos señalados respectivamente como 60 y 62 aseguran la planificación de las máquinas virtuales aplicadas.

[0057] Varias aplicaciones de un hipervisor que permiten crear varias máquinas virtuales y gestionar la separación de los espacios de memorias son conocidas en el estado de la técnica. Podemos remitirnos, por ejemplo, al documento WO2006027488 que describe una aplicación ventajosa de un programa hipervisor.

[0058] El documento WO2006027488 describe especialmente la gestión por el hipervisor de los privilegios de ejecución de las máquinas virtuales.

[0059] De preferencia y para obtener los resultados de seguridad esperados, el código binario que comprende las instrucciones que permiten la aplicación del programa hipervisor es muy compacto, por ejemplo, del orden de unas decenas de kilobytes, de manera que se limite estadísticamente la cantidad de errores o bugs.

[0060] De preferencia, y por las mismas razones de seguridad, la ejecución del hipervisor es atómica, por tanto, no puede ser interrumpida y cualquier llamada al hipervisor está por tanto limitada a unos centenares de instrucciones binarias, para no entorpecer la fluidez del conjunto.

[0061] En cada máquina virtual, un sistema operativo respectivo es supervisado por los módulos de control del hipervisor, controlando el sistema operativo la ejecución de las aplicaciones que tienen unos niveles de privilegio menores en modo no virtualizado.

[0062] Por ejemplo, en la ilustración de la figura 3, el hipervisor supervisa el módulo 66 de la máquina virtual VM_0 que aplica un sistema operativo OS que tiene un nivel de privilegio superior al nivel de privilegio de las aplicaciones APP aplicadas en el módulo mencionado 68, por encima del sistema operativo OS. Lo mismo es válido para el sistema operativo 70 aplicado por la máquina virtual VM_n, que tiene un nivel de privilegio superior al nivel de privilegio de las aplicaciones APP del módulo 72.

[0063] Según un modo de realización particular, el hipervisor es apto para dar un nivel de privilegio particular a una de las máquinas virtuales, para permitir por tanto a una de las máquinas virtuales disponer de derechos ampliados con respecto a las otras máquinas virtuales.

[0064] Esta funcionalidad se utiliza de manera ventajosa para la aplicación de las máquinas virtuales del tercer grupo de máquinas virtuales de seguridad señalado como G3 en la figura 2, que permite así especialmente la aplicación de los servicios de vigilancia de seguridad 40 y de terceros de confianza 41, siendo así el grupo G3 apto para arbitrar y para controlar la aplicación de servicios aplicativos ejecutados por una u otra de las demás máquinas virtuales.

[0065] De preferencia, los servicios de seguridad del grupo de máquinas virtuales de seguridad son estáticos y preinstalados para aumentar la seguridad y la resistencia a los eventuales ataques. Estos servicios de seguridad son, no obstante, reiniciables o *rebootables*.

[0066] La comunicación entre las diversas máquinas virtuales se realiza por unos canales de comunicación seguros, como ya se ha descrito más arriba.

[0067] La invención se ha descrito más arriba en un modo de realización en el que los contenidos multimedia son protegidos por un sistema de control de acceso a base de mensajes de control y de gestión de títulos de acceso. Como variante, los contenidos multimedia son protegidos por un sistema de gestión de los derechos DRM (para «Digital Rights Management» por sus siglas en inglés) en el que los derechos asociados a los contenidos multimedia

son gestionados a través de unas licencias.

[0068] Ventajosamente, además del particionamiento apropiado para cada máquina virtual y para cada grupo de máquinas virtuales comunicantes del mismo nivel de seguridad, el grupo de máquinas virtuales destinado a aplicar los servicios de seguridad ejerce además un particionamiento activo: gestionando de manera estricta, equilibrada y preventiva, las bibliotecas de *software* y periféricos divididos entre los demás grupos de máquinas virtuales (el grupo operador, el grupo de aplicaciones de terceros). El grupo de máquinas virtuales de terceros de confianza respeta a la vez las necesidades de seguridad de los servicios de operador y de las aplicaciones de terceros.

REIVINDICACIONES

1. Dispositivo de tratamiento de contenidos multimedia, apto para recibir contenidos multimedia cifrados procedentes de al menos un transmisor gestionado por un operador, protegidos por un sistema de protección de contenidos y para suministrar dichos contenidos multimedia en forma descifrada a un dispositivo usuario, que comprende unos medios (10) de aplicación de control de acceso que autoriza el suministro de dichos contenidos multimedia descifrados a dicho dispositivo usuario, unos medios (10, 12, 14) de ejecución de servicios de seguridad que tienen un primer nivel de seguridad asociado y unos medios (22) de ejecución de servicios que tienen un nivel de seguridad asociado inferior a dicho primer nivel de seguridad, **caracterizado porque** comprende:

- un hipervisor (30) apto para controlar la ejecución de al menos tres grupos de máquinas virtuales (G1, G2, G3), dichos grupos de máquinas virtuales se ejecutan de manera estrictamente separada, entre los que:
- un primer grupo (G1) de máquinas virtuales dedicado a la ejecución de servicios aplicativos de terceros de nivel de seguridad inferior al primer nivel de seguridad, instalados por al menos un usuario, siendo dichos servicios aplicativos de terceros unas aplicaciones cuyo suministro está controlado por al menos un proveedor de aplicaciones, siendo al menos dicho proveedor independiente del operador,
- un segundo grupo (G2) de máquinas virtuales dedicado a la ejecución de servicios controlados por el operador, de nivel de seguridad inferior al primer nivel de seguridad, y
- un tercer grupo (G3) de máquinas virtuales apto para aplicar unos servicios de seguridad de primer nivel de seguridad, que comprenden el suministro de un servicio de desencriptación a un servicio de control de acceso a los contenidos multimedia, estando el usuario del dispositivo autorizado para obtener unos contenidos multimedia descifrados obtenidos a partir de contenidos multimedia cifrados suministrados por el operador bajo el control de una máquina virtual del tercer grupo apto para suministrar dicho servicio de desencriptación, siendo el tercer grupo (G3) de máquinas virtuales además apto para asegurar una función de terceros de confianza, que garantiza un reparto de recursos materiales disponibles, para la ejecución de los servicios de dichos primer y segundo grupo de máquinas virtuales.

2. Dispositivo de tratamiento de contenidos multimedia según la reivindicación 1, **caracterizado porque** dicho tercer grupo consta al menos de una máquina virtual que ejecuta un servicio de descifrado multimedia.

3. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones 1 a 2, **caracterizado porque** consta además de unos medios de almacenamiento de datos relativos a los servicios aplicados.

4. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones 1 a 3, **caracterizado porque** consta de unos medios (18) de acceso a una red de comunicaciones y **porque** dichos servicios aplicativos de terceros son descargados por el usuario a través de dicha red de comunicaciones.

5. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones anteriores, **caracterizado porque** dicho tercer grupo (G3) consta de una máquina virtual que ejecuta un servicio de terceros de confianza (41), apto para comunicar con un servicio aplicado por una máquina virtual del primer grupo o con un servicio aplicado por una máquina virtual del segundo grupo a través de unos canales seguros (42, 44).

6. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones anteriores, **caracterizado porque** las máquinas virtuales de dicho tercer grupo tienen unos privilegios de ejecución atribuidos por dicho hipervisor superiores a los privilegios de ejecución atribuidos respectivamente a las máquinas virtuales de dichos primer grupo y segundo grupo.

7. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones anteriores, **caracterizado porque** cada máquina virtual de dicho primer grupo (G1) ejecuta un servicio aplicativo de tercero o un agregado de servicios aplicativos de terceros.

8. Dispositivo de tratamiento de contenidos multimedia según una de las reivindicaciones anteriores, **caracterizado porque** consta de un número predeterminado de procesadores físicos y **porque** dicho hipervisor es apto para controlar dichos procesadores físicos.

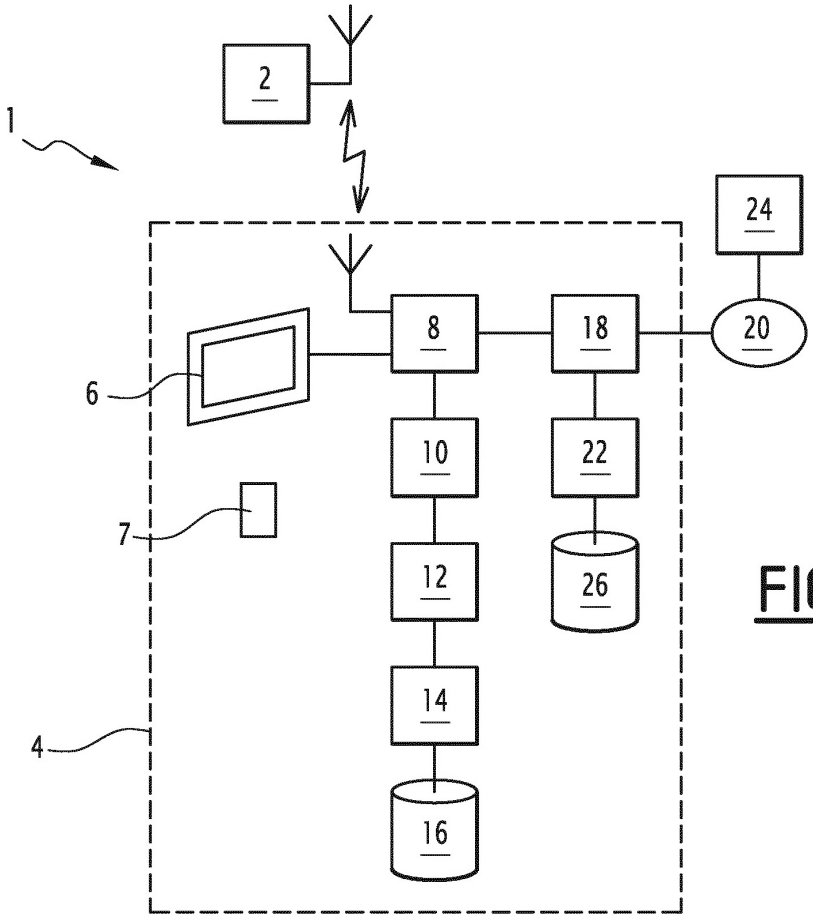
1
2
24
8
18
20
6
10
22
7
12
26
14
4
16

FIG.1

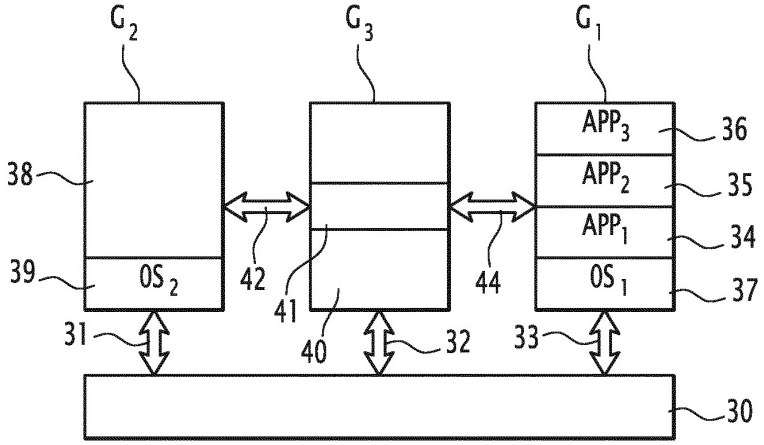
G2
G3
G1
APP3
36
38
APP2
35
APP1
34
39
OS2
42
41
44
OS1
37
31
40
32
33
30

FIG.2

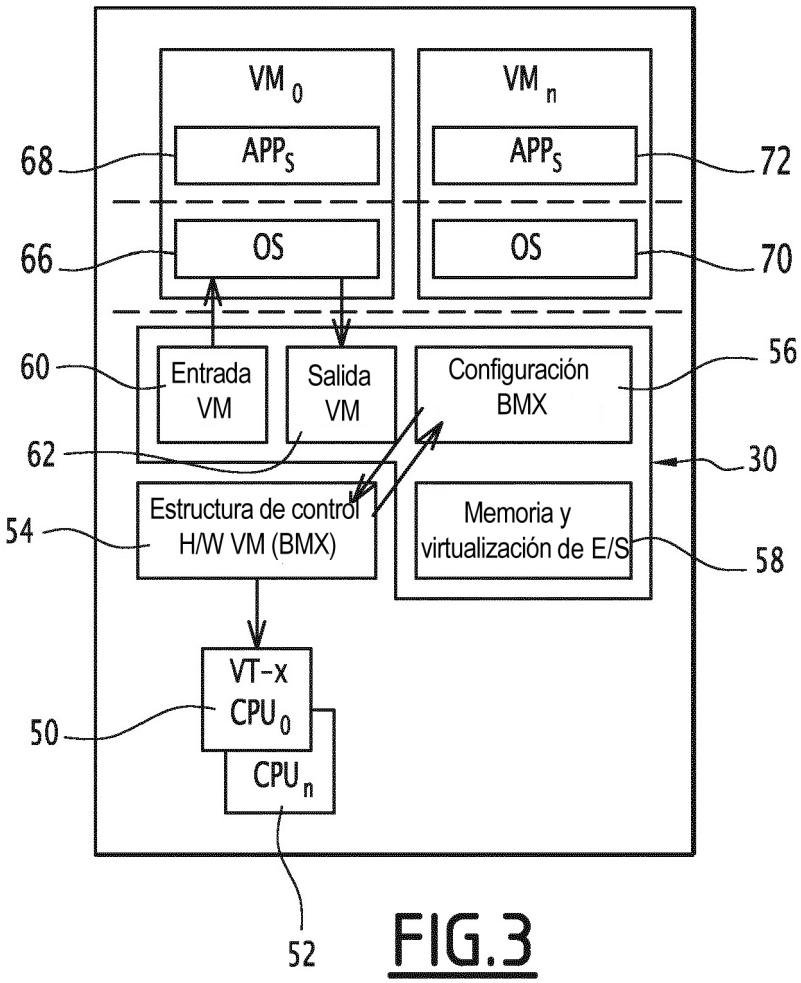
VM 0
VM n
APPS
APPS
OS
OS
Entrada VM
Salida VM
Configuración BMX
Estructura de control H/W VM (BMX)
Memoria y virtualización de E/S
VT-x
CPU 0
CPU n
68
72
66
70
60
56
62
30
54
58
50
52

FIG.3