(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 928 482**

(51) Int. CI.:

G06F 21/74 (2013.01)
G06F 21/53 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.06.2016 PCT/EP2016/065342**

(87) Fecha y número de publicación internacional: **05.01.2017 WO17001580**

(96) Fecha de presentación y número de la solicitud europea: **30.06.2016 E 16734348 (2)**

(97) Fecha y número de publicación de la concesión europea: **14.09.2022 EP 3317803**

(54) Título: **Procedimiento y sistema de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados**

(30) Prioridad:

02.07.2015 FR 1556258

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2022

(73) Titular/es:

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

(72) Inventor/es:

SANCHEZ LEIGHTON, VICENTE

(74) Agente/Representante:

PONTI & PARTNERS, S.L.P.

ES 2 928 482 T3

DESCRIPCIÓN

Procedimiento y sistema de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados

[0001] La presente invención se refiere a un procedimiento de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados, incluyendo cada dispositivo programable al menos un procesador de cálculo, y a un sistema de ejecución segura de máquinas virtuales asociado.

[0002] La invención se sitúa en el campo de la ejecución segura de máquinas virtuales, y encuentra una aplicación particular en la ejecución de máquinas virtuales en un sistema centralizado de tratamiento de datos.

[0003] La ejecución segura de determinadas aplicaciones informáticas, denominadas críticas, es un desafío importante, en numerosos contextos industriales y comerciales.

[0004] La ejecución segura de una aplicación informática, que asegura un cierto nivel de seguridad y de robustez frente a diversos ataques de piratería, mediante un conjunto de recursos de hardware, implica una partición en hardware o software de los recursos de hardware para efectuar una separación entre un entorno de ejecución de nivel de seguridad normal o estándar y un entorno de ejecución seguro.

[0005] La separación de software es efectuada, de manera conocida, por un mecanismo de hipervisor o VMM (por «Virtual Machine Monitor», en inglés). Gracias a dicho mecanismo pueden ejecutarse aplicaciones diferentes en entornos memoria aislados unos de otros de la parte de hardware de nivel de seguridad estándar de un procesador.

[0006] Se conocen además arquitecturas de partición de hardware, por ejemplo la arquitectura TrustZone® de la empresa ARM® que suministra un procesador provisto de una parte o enclave de hardware segura, particionada con respecto a una parte de hardware de nivel de seguridad estándar, más baja que el nivel denominado seguro. Esta partición se traduce en la capacidad del procesador de conmutar de un modo normal a un modo seguro para el que se aíslan recursos de hardware físicamente del modo normal. Estos recursos de hardware aislados son, por ejemplo, memoria, recursos de redes o aceleradores criptográficos. Asimismo, el nivel de privilegio y las instrucciones autorizadas para la ejecución por el procesador son distintos según el modo normal o el modo seguro.

[0007] En lo que sigue de la descripción, se hablará respectivamente de parte de hardware de nivel de seguridad estándar y de parte de hardware segura, para designar el conjunto de recursos de hardware implementados en el modo normal y en el modo seguro de dicho procesador. La conmutación del modo normal al modo seguro se lleva a cabo después de una solicitud del modo normal con ayuda de una instrucción específica o durante una interrupción de hardware derivada de uno de los recursos de hardware fijados al modo seguro.

[0008] La consideración de la solicitud como resultado de la conmutación del modo normal al modo seguro es realizada por un firmware de control del procesador (del inglés, que significa «software firme»). Este firmware debe distinguirse del microcódigo del procesador que no es accesible y que define además el juego de instrucciones del procesador.

[0009] Este firmware se ejecuta también en el arranque (o «boot», en inglés) del procesador que se efectúa en modo seguro de tal manera que desde el principio se establece una cadena de confianza. Como resultado de la secuencia de arranque, el firmware inicia el arranque en el mundo normal. El firmware está constituido por secuencias de instrucciones del procesador de los más elevados niveles de privilegio.

[0010] Por ejemplo, en el caso de procesadores de arquitectura ARM v8®, el firmware de control del procesador permite usar una instrucción dada, denominada SMC, por «Secure Monitor Call», que permite que una aplicación ejecutada en la parte de nivel de seguridad estándar del procesador pase parámetros de ejecución para requerir la ejecución de al menos una instrucción, denominada crítica, de esta aplicación por la parte de hardware segura del procesador.

[0011] Existen también otras arquitecturas que suministran funcionalidades similares, tal como SGX® de Intel®, en el contexto en el cual los niveles de privilegios se denominan anillos de protección, o «CPU privilege rings» en inglés.

[0012] Dicha arquitectura asegura la ejecución, denominada así segura, de al menos una instrucción crítica, de una aplicación, en un entorno de ejecución aislado en la parte segura del procesador, denominado Trusted Execution Environment (TEE).

[0013] La aplicación ejecutada en el TEE (a veces llamado «trustlet») está compuesta por varias secuencias de instrucciones, que según el diseño del código (descomposición en varias tareas de ejecución o «threads», en inglés) son ejecutadas en su caso en varios núcleos de procesadores en paralelo dentro de un mismo TEE.

[0014] Cuando varias máquinas virtuales, cada una de las cuales incluye un sistema operativo o SO (en inglés, «Operating System»), ejecutan en un mismo procesador una o varias aplicaciones, se plantea un problema de compartición de la parte de hardware segura del procesador que permita ejecuciones aisladas unas de otras de las aplicaciones de cada una de las máquinas virtuales. En este caso, de hecho, la separación asegurada por el hipervisor en la parte de seguridad estándar del procesador no está asegurada dentro de la parte segura.

[0015] Además, el uso de conjuntos de servidores de almacenamiento y de cálculo, a distancia, por numerosas máquinas virtuales cliente, denominado «cloud computing», es cada vez más habitual. En dicho contexto, numerosas máquinas virtuales pretenden acceder a los recursos de hardware puestos a disposición. En general, estas máquinas virtuales pertenecen a diversos propietarios. El problema de una posibilidad de ejecución segura, y en particular el problema mencionado anteriormente, es crucial en dicho contexto.

[0016] Para resolver este último problema, la solicitud de patente US2009/0204964 A1 propone una plataforma virtual segura distribuida, que implementa una arquitectura con un hipervisor seguro. La arquitectura propone una virtualización lógica de módulos TPM, que son componentes de hardware criptográficos. Las soluciones basadas en estos componentes son vulnerables ante determinados tipos de ataques. De hecho, permiten verificar la integridad de las aplicaciones cargadas para su ejecución, pero no aseguran un aislamiento de hardware de sus ejecuciones. Como alternativa, los módulos de seguridad de hardware, o HSM, por «hardware security modules», en inglés, necesitan unidades de tratamiento dedicadas. Además, estos módulos son costosos.

[0017] El artículo «TEEEI - A Mobile Security Infrastructure for TEE Integration» de Hongfeng Chai y col., publicado en 2014 en IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, describe una infraestructura de ejecución segura que integra múltiples TEE («*trusted execution environment*»).

[0018] El documento US2014/0040886 es una solicitud de patente en el campo de la ejecución segura que usa varias máquinas virtuales.

[0019] La invención tiene como objetivo remediar estos inconvenientes de las soluciones conocidas, proponiendo una solución más segura y menos costosa para la ejecución segura de aplicaciones procedentes de máquinas virtuales múltiples implementadas por una pluralidad de dispositivos programables interconectados.

[0020] Para este fin, la invención propone un procedimiento de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados, incluyendo cada dispositivo programable al menos un procesador de cálculo que incluye uno o varios núcleos, siendo cada dispositivo programable capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales, incluyendo cada procesador una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, de manera que dichas partes de hardware están particionadas.

[0021] Este procedimiento incluye las etapas siguientes:

- memorización de al menos un entorno de ejecución seguro asociado a cada máquina virtual, incluyendo cada entorno de ejecución seguro al menos una instrucción de una aplicación asociada,
- después de una solicitud de ejecución segura de al menos una serie de instrucciones de una aplicación por una máquina virtual solicitante, estando la máquina virtual solicitante implementada en una parte de hardware de ejecución de nivel de seguridad estándar de un procesador, siendo dicha solicitud transmitida a un módulo de control seguro implementado en la parte de hardware segura de dicho procesador,

    • asignación a dicha ejecución segura de al menos una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados, que incluye una transmisión de dicha solicitud de ejecución segura, por dicho módulo de control seguro a otro módulo de control seguro implementado en la parte de hardware segura de otro procesador del conjunto de dispositivos programables interconectados, de manera que cada uno de dichos módulos de control seguro implementa mecanismos de direccionamiento y de encaminamiento de las solicitudes de ejecución segura,
    • carga del entorno de ejecución seguro asociado a dicha máquina virtual solicitante en dicha al menos una parte de hardware segura asignada,
    • uso de la parte de hardware segura asignada para la ejecución segura de dicha serie de instrucciones de la aplicación de la máquina virtual solicitante, siendo el uso de una parte de hardware segura asignado para la ejecución segura de al menos una instrucción de la aplicación de una primera máquina virtual solicitante exclusivo, en un instante dado, de cualquier uso de dicha parte de hardware segura para la ejecución segura de al menos una instrucción de la aplicación de una segunda máquina virtual solicitante.

[0022] Ventajosamente, la invención permite usar sucesivamente partes de hardware seguras de los procesadores de dispositivos programables interconectados, por diversas máquinas virtuales, de manera distribuida, a la vez que se asegura la partición de hardware de las ejecuciones. Además, la invención permite el aprovechamiento de las partes seguras que no son usadas por las aplicaciones situadas en las partes de hardware de nivel de seguridad estándar respectivas dentro de un mismo procesador.

[0023] El procedimiento de ejecución segura de máquinas virtuales según la invención puede presentar una o varias de las características mostradas a continuación, tomadas independientemente o según todas las combinaciones técnicas aceptables.

La parte de hardware segura comprende recursos de memoria y el procedimiento incluye, antes de la carga del entorno de ejecución seguro, una etapa de limpieza de dichos recursos de memoria.

[0024] La parte de hardware segura comprende al menos un periférico, y el procedimiento incluye, antes de la carga del entorno de ejecución seguro, una etapa de limpieza de cada periférico.

[0025] El procedimiento comprende además un cifrado del entorno de ejecución seguro después de la ejecución segura de dicha serie de instrucciones de la aplicación de la máquina virtual solicitante, y una memorización del entorno de ejecución seguro cifrado.

[0026] Después de la solicitud de ejecución segura de al menos una serie de instrucciones de una aplicación, el procedimiento comprende al menos una etapa de evaluación de recursos de hardware necesarios para el entorno de ejecución seguro asociado a dicha máquina virtual solicitante, y de cálculo de un número de partes de hardware seguras que se asignarán para la ejecución de la aplicación segura en el entorno de ejecución seguro asociado.

[0027] Después de la solicitud de ejecución segura de al menos una serie de instrucciones de una aplicación, el procedimiento comprende una etapa de cálculo de una prioridad de secuenciación de ejecución segura de las solicitudes de ejecución.

[0028] La evaluación de recursos de hardware comprende una evaluación de complejidad de cálculo y/o de cantidad de memoria y/o de número de núcleos de ejecución.

[0029] El procedimiento comprende, para una pluralidad de solicitudes de ejecución procedentes de una pluralidad de máquinas virtuales solicitantes, una implementación distribuida de un algoritmo de ordenamiento para el uso de grupos de partes de hardware seguras por los entornos de ejecución seguros asociados a las máquinas virtuales solicitantes.

[0030] El uso de una parte de hardware segura asignada para la ejecución segura de al menos una instrucción de la aplicación de una primera máquina virtual solicitante es exclusivo, en un instante dado, de cualquier uso de dicha parte de hardware segura para la ejecución segura de al menos una instrucción de la aplicación de una segunda máquina virtual solicitante.

[0031] Según otro aspecto, la invención propone un sistema de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados, incluyendo cada dispositivo programable al menos un procesador de cálculo que incluye uno o varios núcleos, siendo cada dispositivo programable capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales, incluyendo cada procesador una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, de manera que dichas partes de hardware están particionadas.

[0032] Cada procesador incluye módulos de firmware de control de dicho procesador y adaptados para:

- memorizar un entorno de ejecución seguro asociado a cada máquina virtual, incluyendo cada entorno de ejecución seguro al menos una instrucción de una aplicación asociada,
- después de una solicitud de ejecución segura de al menos una serie de instrucciones de una aplicación por una máquina virtual solicitante, estando la máquina virtual solicitante implementada en una parte de hardware de ejecución de nivel de seguridad estándar de dicho procesador, siendo dicha solicitud transmitida a un módulo de control seguro implementado en la parte de hardware segura de dicho procesador,

    • asignación a dicha ejecución segura de al menos una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados, que incluye una transmisión de dicha solicitud de ejecución segura, por dicho módulo de control seguro, a otro módulo de control seguro implementado en la parte de hardware segura de otro procesador del conjunto de dispositivos programables interconectados, de manera que cada uno de dichos módulos de control seguro implementa mecanismos de direccionamiento y de encaminamiento de las solicitudes de ejecución segura,
    • carga del entorno de ejecución seguro asociado a dicha máquina virtual solicitante en dicha al menos una parte de hardware segura asignada,
    • uso de la parte de hardware segura asignada para la ejecución segura de dicha serie de instrucciones de la

aplicación de la máquina virtual solicitante, siendo el uso de una parte de hardware segura asignado para la ejecución segura de al menos una instrucción de la aplicación de una primera máquina virtual solicitante exclusivo, en un instante dado, de cualquier uso de dicha parte de hardware segura para la ejecución segura de al menos una instrucción de la aplicación de una segunda máquina virtual solicitante.

[0033] Según una realización, el sistema de ejecución segura de máquinas virtuales incluye recursos de memoria compartidos, y un módulo de cifrado capaz de cifrar el entorno de ejecución seguro después de la ejecución segura de dicha al menos una instrucción de la aplicación de la máquina virtual solicitante, y de salvaguardar el entorno de ejecución seguro cifrado en los recursos de memoria compartidos.

[0034] Según otro aspecto, la invención se refiere a un producto de programa informático que incluye instrucciones de firmware que, cuando son implementadas por uno o varios procesadores de cálculo de dispositivos programables, incluyendo cada procesador de cálculo uno o varios núcleos, siendo cada dispositivo programable capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales, incluyendo cada procesador una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, de manera que dichas partes de hardware están particionadas, implementan un procedimiento tal como se describe brevemente anteriormente.

[0035] Otras características y ventajas de la invención se desprenderán de la descripción que se ofrece a continuación, a modo indicativo y de ninguna forma limitativo, en referencia a las figuras anexas, entre las cuales:

- la figura 1 representa esquemáticamente un sistema centralizado de tratamiento de datos;
- la figura 2 ilustra esquemáticamente una realización de un procesador de un dispositivo programable en una realización de la invención;
- la figura 3 ilustra esquemáticamente una realización con dispositivos programables interconectados;
- la figura 4 es un organigrama de las principales etapas de un procedimiento de ejecución segura de máquinas virtuales según una realización de la invención;
- la figura 5 es un organigrama de implementación de la etapa de asignación distribuida de partes de hardware seguras según una realización de la invención.

[0036] La invención se describirá en su aplicación en un sistema centralizado de tratamiento de datos que incluye conjuntos de dispositivos programables interconectados, que pueden ser usados por una pluralidad de máquinas virtuales cliente.

[0037] No obstante, la invención no se limita a este caso de aplicación, y encuentra una aplicación en cualquier sistema de ejecución de aplicaciones procedentes de una pluralidad de máquinas virtuales.

[0038] La figura 1 ilustra esquemáticamente un sistema centralizado de tratamiento 2, que comprende en el ejemplo dos conjuntos 4, 6 de dispositivos programables 10 interconectados. Cada dispositivo programable 10 comprende dos módulos de interfaz de conexión de red respectivos, denotados por 12 y 14, un primer módulo de interfaz 12 que permite la conexión a una red de comunicación pública 16 y un segundo módulo de interfaz 14 que permite la conexión a una red de administración 18, que permite la implementación de comunicaciones seguras.

[0039] La red de comunicación pública 16 es, por ejemplo, la red cliente de los proveedores del sistema centralizado de tratamiento (o cloud), que permiten que las máquinas virtuales de sus clientes se conecten entre sí y con la red de comunicación de Internet.

[0040] En una aplicación de tratamiento centralizado de datos, cada uno de los dispositivos programables 10 funciona en modo virtualizado, ejecutando varias máquinas virtuales de clientes diferentes. Se habla entonces de ocupación múltiple o «multi-tenancy», en inglés.

[0041] Para permitir una ejecución segura de aplicaciones por estas máquinas virtuales, preferentemente, cada dispositivo programable está equipado con uno o varios procesadores, que tienen uno o varios núcleos de cálculo, y que permiten realizar una ejecución segura en hardware.

[0042] La figura 2 ilustra una realización preferida en la que cada procesador 30 de dispositivo programable incluye dos partes de hardware distintas 32 y 34 que corresponden respectivamente a la parte de hardware de nivel de seguridad estándar y a la parte de hardware segura.

[0043] La parte de hardware 32 es de nivel de seguridad estándar, usado para un funcionamiento clásico. La parte de hardware 34 es una parte de hardware segura, de nivel de seguridad superior en el nivel de seguridad estándar. Estas dos partes están particionadas entre sí, y el acceso a la parte de hardware segura 34 se realiza mediante las solicitudes 33, 35 dedicadas.

[0044] Cada una de las partes de hardware en conexión con su modo de ejecución respectivos implementa varios niveles de privilegio de ejecución: un nivel de privilegio de usuario (inferior) EL_0, y uno o varios niveles de privilegio intermedios (EL_1 y EL_2 en nuestro ejemplo), para la ejecución de un sistema operativo, del hipervisor y finalmente un nivel de privilegio superior (EL_3 en nuestro ejemplo) para el firmware de control en el modo seguro.

[0045] Por ejemplo, en el caso en que el procesador usado tiene una arquitectura ARM v8®, se dispone de un nivel de privilegio de usuario EL_0, en los dos modos, de un nivel de privilegio superior EL_1 en los dos modos, para la ejecución de un sistema operativo, un nivel de privilegio superior EL_2, solo en el modo estándar para el hipervisor y un nivel de privilegio máximo EL_3, solo en el modo seguro.

[0046] Así, las aplicaciones de usuario 36_1 a 36_n son ejecutadas en el nivel de privilegio EL_0, del modo estándar, estando la ejecución soportada por un sistema operativo y un entorno de ejecución.

[0047] En el ejemplo de la figura 2, se consideran varias aplicaciones de usuario APP_1 a APP_n, así como varios sistemas operativos SO_1 a SO_3, en el nivel de privilegio EL_1 del modo estándar, estando cada sistema operativo asociado a una máquina virtual VM_1 a VM_3.

[0048] La ejecución de las aplicaciones APP_1 a APP_n de las diversas máquinas virtuales VM_1 a VM_3 es gestionada por un hipervisor o VMM (por «Virtual Machine Monitor», en inglés), denotado por 38 en la figura 2, en el nivel de privilegio EL_2 del modo estándar.

[0049] La parte de hardware segura 34 es capaz de implementar un entorno de ejecución seguro 40, denominado también TEE por «Trusted Execution Environment», y de ejecutar aplicaciones 42_1 a 42_m de manera particionada y, por tanto, protegida con respecto a posibles intentos de piratería.

[0050] En tal caso se habla de ejecución segura y las aplicaciones 42_1 a 42_m ejecutadas de manera segura también se denominan «trustlets». Un entorno de ejecución seguro 40 comprende asimismo un sistema operativo seguro 44, de nivel de privilegio EL_1.

[0051] Dicho de otro modo, un TEE comprende un sistema operativo y un contexto de ejecución de una o varias aplicaciones para ejecutar.

[0052] La parte de hardware segura 34 comprende un módulo de control seguro 46, de nivel de privilegio EL_3 superior en el nivel de privilegio atribuido al módulo 44, que implementa instrucciones de código firmware de control de la parte de hardware segura.

[0053] Según una realización, el firmware de control implementado por el módulo de control seguro 46 es modificado por la adición de instrucciones de código al objeto de permitir, después de una solicitud de ejecución segura de al menos una instrucción de una aplicación APP_1 a APP_n, de una máquina virtual solicitante, en particular cambiando el contexto memoria visible del entorno de ejecución seguro, un uso distribuido de las partes de hardware seguras de los procesadores de los dispositivos programables interconectados.

[0054] La figura 2 ilustra un único dispositivo programable, pero la figura 3 ilustra dos dispositivos programables interconectados.

[0055] El módulo de control seguro 46 comprende un módulo 50 de recepción y tratamiento de las solicitudes 33, 35 de ejecución segura.

[0056] Por ejemplo, en el ejemplo de la figura 2, se transmite una primera solicitud 33, para una ejecución segura de la aplicación APP_1 en su entorno de ejecución seguro TEE_1, así como una segunda solicitud 35 para una ejecución segura de la aplicación APP_2 en su entorno de ejecución seguro TEE_2.

[0057] El módulo de control seguro 46 comprende también un módulo 52 capaz de realizar una salvaguarda, en una zona de recursos de memoria compartidos 60, de un entorno de ejecución seguro TEE_i asociado a una máquina virtual VM_i.

[0058] Preferentemente, los datos del entorno de ejecución seguro se someten a cifrado antes de la salvaguarda.

[0059] Un módulo 54 de asignación de parte de hardware segura implementa la asignación, para la ejecución segura de una aplicación APP_k en un entorno TEE_i, de al menos una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados.

[0060] Un módulo 56 denominado de asepsia efectúa la limpieza, en particular la puesta a cero, de los recursos de hardware de memoria usados por la parte de hardware segura para la ejecución de instrucciones de código, de manera que evite cualquier posibilidad de piratería debida a ejecuciones sucesivas de instrucciones de código procedentes de máquinas virtuales distintas. Además, otros recursos de hardware, o periféricos, usados para la ejecución de las instrucciones de la aplicación APP_k también se limpian para evitar cualquier riesgo de piratería.

[0061] Un módulo 58 de carga y de ejecución efectúa la carga en memoria de acceso aleatorio RAM del entorno de ejecución seguro TEE_i que corresponde a la solicitud de ejecución recibida, y la ejecución segura de la aplicación APP_k.

[0062] Preferentemente, los recursos de hardware de la parte de hardware segura 34 seleccionada se usan de manera exclusiva para la ejecución de una aplicación dada en un instante dado.

[0063] La figura 3 ilustra esquemáticamente una implementación de la invención en el contexto de interconexión de dos procesadores 30a, 30b de dos dispositivos programables interconectados. Para simplificar la representación, los recursos de memoria compartidos no se han vuelto a ilustrar en la figura 3.

[0064] Cada uno de los procesadores 30a, 30b comprende elementos análogos a los elementos descritos anteriormente para el procesador 30 de la figura 2.

[0065] Como se ilustra en la figura 3, el módulo de control seguro 46a es capaz de transmitir una solicitud 37 de ejecución segura, por medio del módulo de interfaz de red 14a, a un módulo de control 46b de otro procesador, que es capaz de recibirlo por medio del módulo de interfaz de red 14b.

[0066] En el ejemplo, la solicitud 37 es una instrucción de ejecución segura de la aplicación APP_3 en un entorno de ejecución seguro TEE_3 asociado.

[0067] El entorno de ejecución seguro TEE_3 es descifrado, cargado y ejecutado por la parte de hardware segura 34b.

[0068] Los módulos de control seguro 46a, 46b implementan mecanismos de direccionamiento y de encaminamiento de las solicitudes de ejecución segura, siendo cada solicitud de ejecución segura transmitida por una máquina virtual ejecutada por una parte de hardware 32a, 32b de nivel de seguridad estándar.

[0069] Así, los módulos de control seguro respectivos 46a, 46b tal como son suministrados por los fabricantes de procesadores son modificados para permitir un tratamiento de las solicitudes 37 que comprende instrucciones de ejecución por una parte de hardware segura a distancia. Como consecuencia se consigue un funcionamiento distribuido.

[0070] La figura 4 es un organigrama de las principales etapas de un procedimiento de ejecución de máquinas virtuales por un conjunto de dispositivos programables interconectados según una realización de la invención.

[0071] En esta realización, el procedimiento comprende una primera etapa 60 de memorización de al menos un entorno de ejecución seguro, denotada por TEE_i, para cada máquina virtual VM_i que se ejecuta en una de las partes de hardware estándar del conjunto de dispositivos programables del sistema.

[0072] Como se menciona anteriormente, cada TEE_i comprende un sistema operativo seguro y un contexto de ejecución de al menos una aplicación.

[0073] Los TEE_i son memorizados, preferentemente en forma cifrada, en recursos de memoria compartidos por el conjunto de los procesadores interconectados del sistema.

[0074] Preferentemente, solo los módulos de control seguros tienen acceso a estos recursos de memoria compartidos que conforman un espacio de salvaguarda.

[0075] También se memoriza una asociación entre cada entorno de ejecución seguro y la máquina virtual y la aplicación para ejecutar.

[0076] Durante la recepción 62 de al menos una solicitud de ejecución segura de al menos una instrucción *Inst* de una aplicación APP_k por una máquina virtual solicitante VM_j, se implementa una etapa 64 de asignación de al menos una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados.

[0077] A continuación se plantean y se detallan varias realizaciones de esta etapa de asignación.

[0078] Después de la etapa de asignación 64, se implementa una etapa de limpieza 66 de los recursos de memoria y otros periféricos usados por la parte de hardware segura asignada, con el fin de aumentar la seguridad de ejecución de la aplicación para ejecutar y de las aplicaciones ejecutadas previamente. Otros periféricos incluyen, por ejemplo, recursos de redes y aceleradores criptográficos.

[0079] En particular, se implementa un borrado de los recursos de memoria durante la etapa 66 cuando la parte de hardware segura ya está asignada a un TEE_f. Esta etapa está precedida de una salvaguarda cifrada del contexto TEE_f, como se explica a continuación.

[0080] La etapa de limpieza se sigue de una etapa 68 de carga en memoria del entorno de ejecución seguro $TEE_{j,k}$ previamente memorizado, para la máquina virtual VM_j y el contexto de ejecución de la aplicación APP_k. Cuando los entornos de ejecución seguros se salvaguardan en forma cifrada, se aplica un descifrado antes de la carga.

[0081] La etapa de carga 68 se sigue de una etapa 70 de ejecución segura de la instrucción *Inst* de la aplicación APP_k en el $TEE_{j,k}$.

[0082] Debe observarse que en una variante, se asignan varias partes de hardware seguras para la ejecución de la aplicación APP_k, como sucedería, opcionalmente, si la aplicación fuera ejecutada en modo seguro en un procesador de varios núcleos.

[0083] Asimismo, es habitual asignar un conjunto de recursos de memoria, por ejemplo memorias tampón (o «buffers», en inglés), para las ejecuciones implementadas en modo de hardware seguro que servirán para comunicarse con la máquina virtual cliente de este TEE. De esta forma, las aplicaciones seguras remiten los resultados a las aplicaciones estándar.

[0084] Las memorias tampón compartidas son accesibles a la vez por el modo normal y por el modo seguro, pero con derechos de acceso de lectura y de escritura diferentes. Cuando los datos, por ejemplo los TEE, se salvaguardan en forma cifrada, pueden almacenarse en zonas de memoria accesibles por el mundo normal, de nivel de seguridad estándar.

[0085] Cuando una de estas memorias tampón compartidas es modificada por la ejecución de la aplicación APP_k, modificando por consiguiente el contexto asociado al entorno de ejecución seguro $TEE_{j,k}$, el contexto de la máquina virtual VM_j 'cliente' será modificado de forma consecuente para permitir la compartición que habría tenido lugar si el TEE se hubiera quedado en el mismo procesador, en modo síncrono o asíncrono (opción a elegir por el firmware).

[0086] Una vez terminada la ejecución, se implementa una etapa 72 de cifrado y de memorización del entorno de ejecución seguro cifrado.

[0087] La figura 5 es un organigrama de una realización de la etapa 64 de asignación de una o varias partes de hardware seguras para la ejecución segura y distribuida de aplicaciones de máquinas virtuales.

[0088] En esta realización, después de la recepción de una solicitud de ejecución segura de al menos una instrucción o serie de instrucciones *Inst* de una aplicación $AP\text{-}P_k$ por una máquina virtual solicitante VM_j, se implementa una etapa 80 de evaluación de recursos de hardware necesarios para el entorno de ejecución seguro TEE_j asociado a dicha máquina virtual solicitante VM_j. En particular, se evalúa la complejidad de cálculo y/o la cantidad de memoria y/o el número de núcleos de ejecución necesarios para dicha ejecución segura.

[0089] La etapa 80 se sigue de una etapa 82 de asignación de un número de partes de hardware seguras y de recursos de memoria asociados para la ejecución de una instrucción o serie de instrucciones *Inst* de una aplicación $AP\text{- }P_k$ por una máquina virtual solicitante VM_j.

[0090] La etapa 82 se sigue de una etapa 84 de cálculo de prioridad de secuenciación de ejecución por los firmware interconectados de las solicitudes de ejecución que se efectuarán.

[0091] Como variante, la etapa 84 de cálculo de prioridad se efectúa antes de la etapa 82 de asignación de partes de hardware seguras, de manera que las prioridades calculadas se aplican también a la etapa de asignación.

[0092] En el caso de una pluralidad de solicitudes de ejecución procedentes de una pluralidad de máquinas virtuales solicitantes, recibidas sustancialmente en paralelo, la etapa 84 se sigue de una etapa 86 de implementación distribuida de un algoritmo de ordenamiento para el uso de las partes de hardware seguras por los entornos de ejecución seguros TEE_i asociados a las máquinas virtuales solicitantes.

[0093] El número de TEE_i y sus necesidades en núcleos de ejecución es, en determinados casos, superior a los recursos de ejecución de hardware seguros disponibles.

[0094] Se conocen diversos mecanismos de ordenamiento distribuido, y aplicables de forma sencilla por un experto en la materia para el ordenamiento y la distribución de los TEE_i en partes de hardware seguras.

[0095] Por ejemplo, pueden aplicarse mecanismos de turnos o round-robin, o un mecanismo BVT (por «borrowed virtual time»).

[0096] En intervalos regulares o después de una solicitud o con motivo de ciertos sucesos o interrupciones, se implementa un reordenamiento 88, que permite reafectar los TEE_i a otras partes de hardware seguras.

[0097] Preferentemente, la colaboración entre los firmware de control de las partes de hardware seguras de los dispositivos programables, ya se trate del ordenamiento o de la gestión de los sucesos de un entorno de ejecución seguro, es organizada por un mecanismo simplificado de DHT (por «Distributed Hash Table») para la compartición distribuida de las informaciones de asignaciones de las partes de hardware seguras, los sucesos o el tiempo de CPU asignado a cada uno de los TEE_i, como Chord o Kademlia.

[0098] Podrá elegirse un procedimiento de ordenamiento en colaboración entre los citados en la publicación «Scheduling in Distributed Systems», de Dongning Liang y col., accesible en Internet en la dirección siguiente: http://cseweb.ucsd.edu/classes/sp99/cse221/projects/Scheduling.pdf.

[0099] En otra variante menos ventajosa desde el punto de vista de la seguridad y del rendimiento, la invención puede incluir una única red compartida entre cada procesador. En este caso, los firmware de control se comunican de manera cifrada, por ejemplo en VPN, usando la red del mundo no seguro.

REIVINDICACIONES

1. Procedimiento de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados que incluyen, cada uno de ellos, al menos un procesador de cálculo con uno o varios núcleos; y cada dispositivo programable es capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales; cada procesador incluye una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, y dichas partes de hardware están particionadas.

El procedimiento incluye las etapas siguientes:

- memorización (60) de, al menos, un entorno de ejecución seguro, TEEi, asociado a cada máquina virtual, y cada entorno de ejecución seguro incluye, al menos, una instrucción de una aplicación asociada,
- después de una solicitud de ejecución segura de, al menos, una serie de instrucciones de una aplicación por una máquina virtual solicitante, la máquina virtual solicitante se implementa en una parte de hardware (32, 32a) de ejecución de nivel de seguridad estándar de un procesador, y dicha solicitud se transmite a un módulo de control seguro (46, 46a) implementado en la parte de hardware segura (34, 34a) de dicho procesador (30, 30a),

  • asignación (64) a dicha ejecución segura de, al menos, una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados, que incluye una transmisión de dicha solicitud de ejecución segura, por dicho módulo de control seguro (46, 46a) a otro módulo de control seguro (46b) implementado en la parte de hardware segura (34b) de otro procesador (30b) del conjunto de dispositivos programables interconectados, de manera que cada uno de dichos módulos de control seguro (46, 46a, 46b) implementa mecanismos de direccionamiento y de encaminamiento de las solicitudes de ejecución segura,
  • carga (68) del entorno de ejecución seguro, TEEj, asociado a dicha máquina virtual solicitante en, al menos, una parte de hardware segura asignada,
  • uso (70) de la parte de hardware segura asignada para la ejecución segura de dicha serie de instrucciones de la aplicación de la máquina virtual solicitante,

el uso de una parte de hardware segura asignado para la ejecución segura de, al menos, una instrucción de la aplicación de una primera máquina virtual solicitante es exclusivo, en un instante dado, de cualquier uso de dicha parte de hardware segura para la ejecución segura de, al menos, una instrucción de la aplicación de una segunda máquina virtual solicitante.

2. Procedimiento según la reivindicación 1, en el que la parte de hardware segura comprende recursos de memoria, y en el que el procedimiento, antes de la carga del entorno de ejecución seguro, incluye una etapa de limpieza (66) de dichos recursos de memoria.

3. Procedimiento según la reivindicación 2, en el que la parte de hardware segura comprende, al menos un periférico, y en el que el procedimiento, antes de la carga del entorno de ejecución seguro, incluye una etapa de limpieza (66) de cada periférico.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, que comprende además un cifrado (72) del entorno de ejecución seguro después de la ejecución segura de dicha serie de instrucciones de la aplicación de la máquina virtual solicitante, y una memorización (72) del entorno de ejecución seguro cifrado.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que, después de la solicitud de ejecución segura de, al menos, una serie de instrucciones de una aplicación, el procedimiento comprende, al menos, una etapa de evaluación (80) de recursos de hardware necesarios para el entorno de ejecución seguro asociado a dicha máquina virtual solicitante, y de cálculo de un número de partes de hardware seguras que se asignarán para la ejecución de la aplicación segura en el entorno de ejecución seguro asociado.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5 en el que, después de la solicitud de ejecución segura de, al menos, una serie de instrucciones de una aplicación, el procedimiento comprende una etapa de cálculo de una prioridad (84) de secuenciación de ejecución segura de las solicitudes de ejecución.

7. Procedimiento según la reivindicación 5, en el que la evaluación de recursos de hardware comprende una evaluación de complejidad de cálculo y/o de cantidad de memoria y/o de número de núcleos de ejecución.

8. Procedimiento según cualquiera de las reivindicaciones 1 a 7, que comprende, para una pluralidad de solicitudes de ejecución procedentes de una pluralidad de máquinas virtuales solicitantes, una implementación distribuida (86) de un algoritmo de ordenamiento para el uso de grupos de partes de hardware seguras por los entornos de ejecución seguros asociados a las máquinas virtuales solicitantes.

9. Sistema de ejecución segura de máquinas virtuales por un conjunto de dispositivos programables interconectados, y cada dispositivo programable incluye, al menos, un procesador de cálculo con uno o varios núcleos, y cada dispositivo programable es capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales,

cada procesador incluye una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, de manera que dichas partes de hardware están particionadas,
y cada procesador está adaptado para:

- memorización (52) de un entorno de ejecución seguro, TEEi, asociado a cada máquina virtual; cada entorno de ejecución seguro incluye, al menos, una instrucción de una aplicación asociada,
- después de una solicitud de ejecución segura de, al menos, una serie de instrucciones de una aplicación por una máquina virtual solicitante, la máquina virtual solicitante está implementada en una parte de hardware (32, 32a) de ejecución de nivel de seguridad estándar de un procesador (30, 30a), y dicha solicitud es transmitida a un módulo de control seguro (46, 46a) implementado en la parte de hardware segura (34, 34a) de dicho procesador,

• asignación (54) a dicha ejecución segura de, al meno,s una parte de hardware segura disponible perteneciente a uno de los procesadores del conjunto de dispositivos programables interconectados, que incluye una transmisión de dicha solicitud de ejecución segura por dicho módulo de control seguro (46, 46a), a otro módulo de control seguro (46b) implementado en la parte de hardware segura (34b) de otro procesador del conjunto de dispositivos programables interconectados, de manera que cada uno de dichos módulos de control seguro (46, 46a, 46b) implementa mecanismos de direccionamiento y de encaminamiento de las solicitudes de ejecución segura,
• carga (58) del entorno de ejecución seguro, TEEj, asociado a dicha máquina virtual solicitante en, al menos, una parte de hardware segura asignada,
• uso (58) de la parte de hardware segura asignada para la ejecución segura de dicha serie de instrucciones de la aplicación de la máquina virtual solicitante,

el uso de una parte de hardware segura se asigna para la ejecución segura de, al menos, una instrucción de la aplicación de una primera máquina virtual solicitante exclusivo, en un instante dado, de cualquier uso de dicha parte de hardware segura para la ejecución segura de, al menos, una instrucción de la aplicación de una segunda máquina virtual solicitante.

10. Sistema de ejecución segura de máquinas virtuales según la reivindicación 9, que incluye recursos de memoria compartidos, incluido el sistema un módulo de cifrado capaz de cifrar el entorno de ejecución seguro después de la ejecución segura de, al menos, una instrucción de la aplicación de la máquina virtual solicitante, y de salvaguardar el entorno de ejecución seguro cifrado en los recursos de memoria compartidos.

11. Producto de programa informático que incluye instrucciones de *firmware* que, cuando son implementadas por uno o varios procesadores de cálculo de dispositivos programables, cada procesador de cálculo incluye uno o varios núcleos, cada dispositivo programable es capaz de ejecutar de forma simultánea y/o sucesiva aplicaciones de una pluralidad de máquinas virtuales, cada procesador incluye una parte de hardware de ejecución de nivel de seguridad estándar y una parte de hardware segura de nivel de seguridad superior en el nivel de seguridad estándar, y dichas partes de hardware están particionadas e implementan un procedimiento según cualquiera de las reivindicaciones 1 a 8.

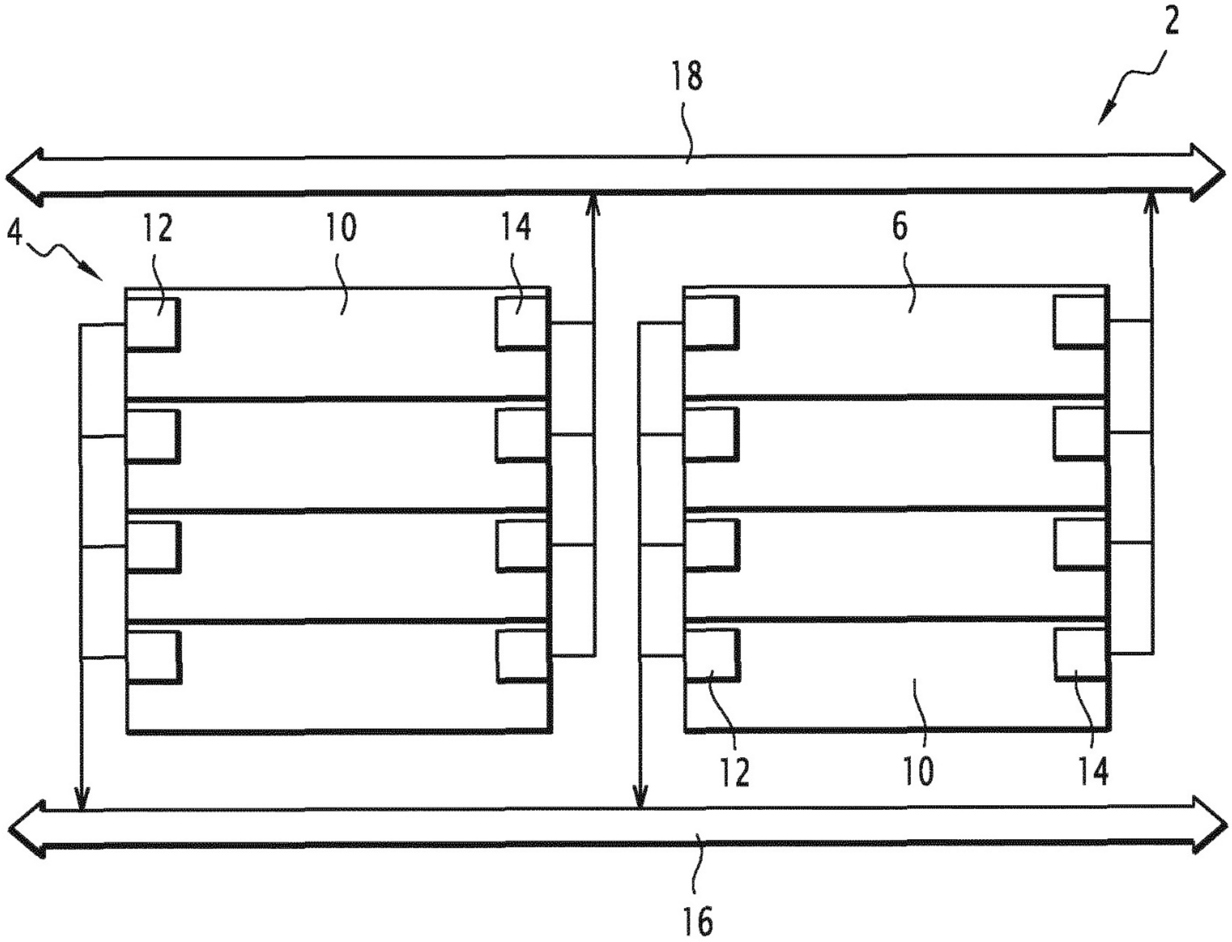
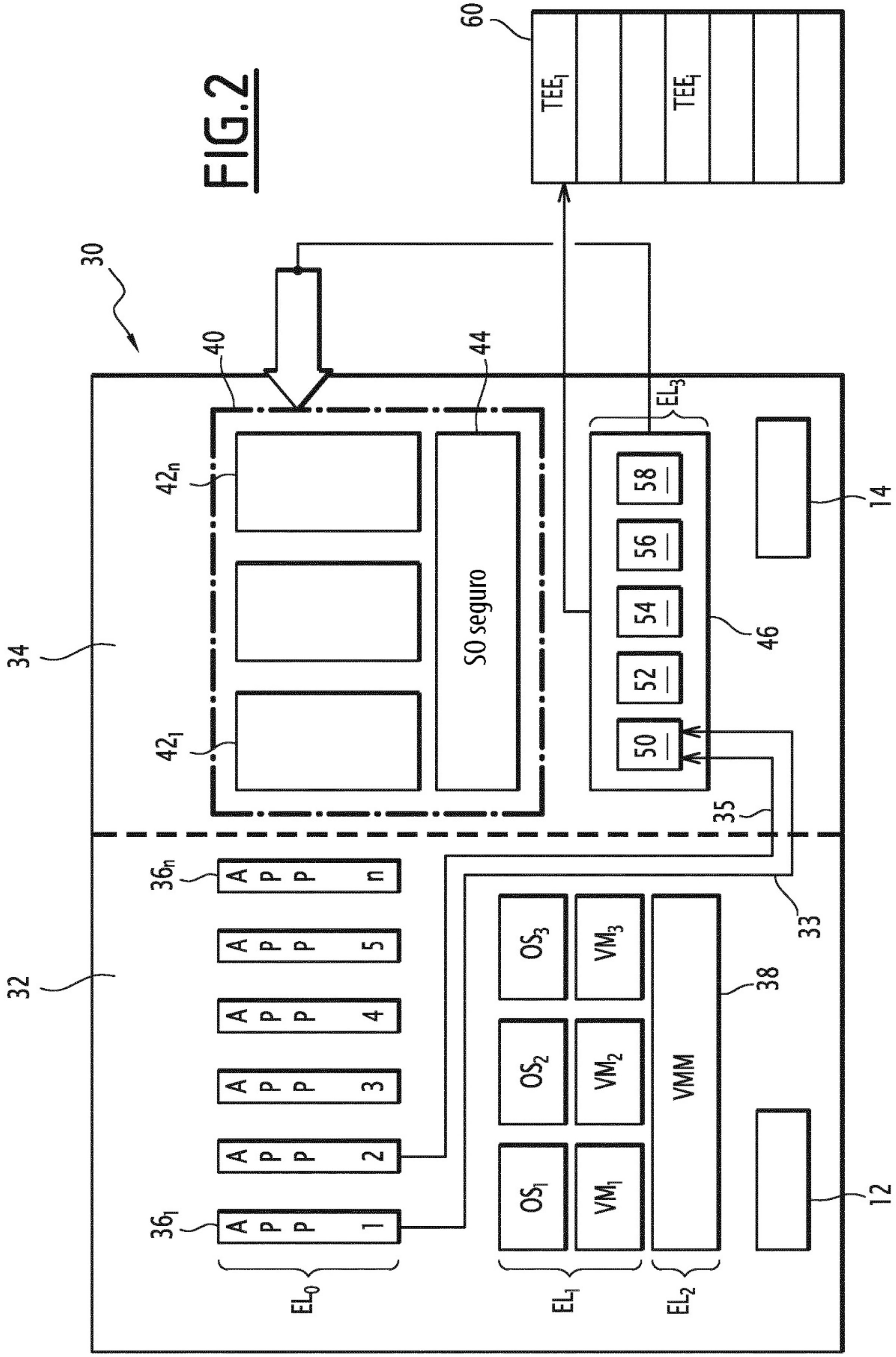


FIG.1

FIG.2


30
34
32
40
44
42_n
42_1
SO seguro
46
50
52
54
56
58
EL_3
14
60
TEE_1
TEE_i
35
33
36_n
36_1
App n
App 5
App 4
App 3
App 2
App 1
OS_3
OS_2
OS_1
VM_3
VM_2
VM_1
VMM
38
12
EL_0
EL_1
EL_2

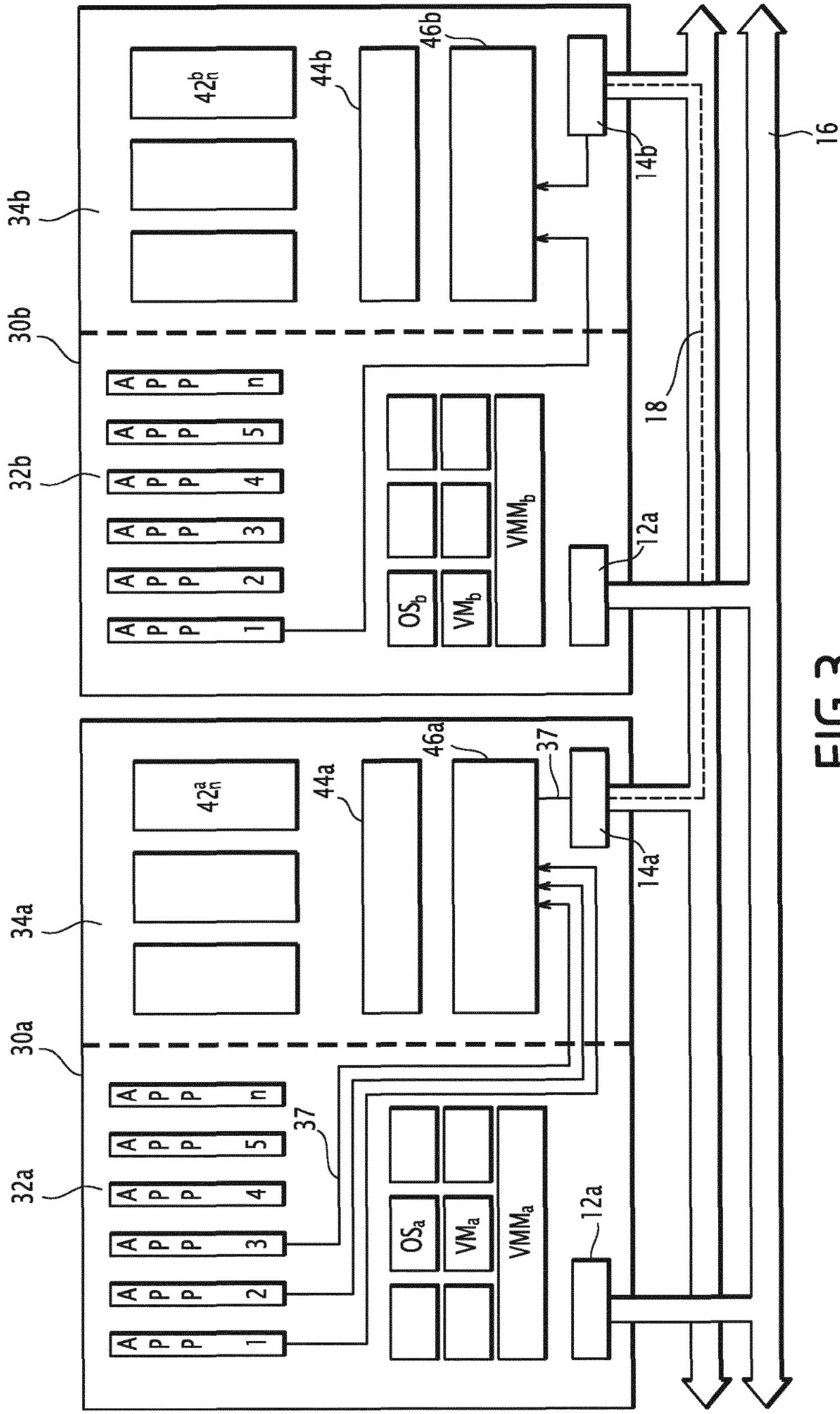

34b
30b
32b
42ⁿᵇ
44b
46b
14b
16
18
12a
App 1
App 2
App 3
App 4
App 5
App n
OSb
VMb
VMMb
34a
30a
32a
42ⁿᵃ
44a
46a
37
14a
37
12a
App 1
App 2
App 3
App 4
App 5
App n
OSa
VMa
VMMa

FIG.3

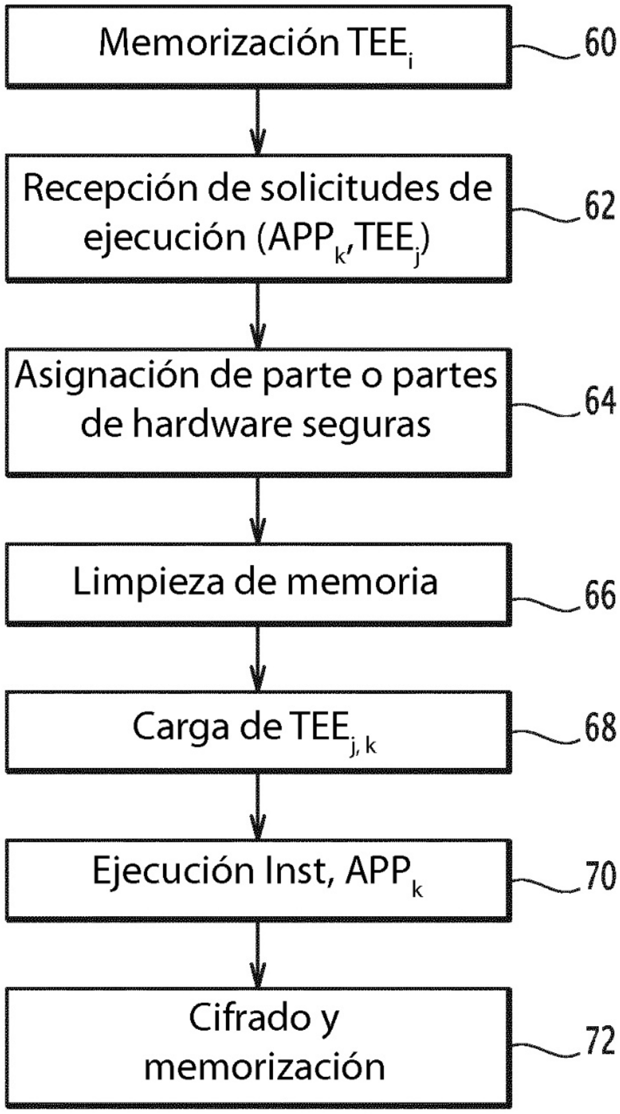

Memorización TEE$_i$
60
Recepción de solicitudes de ejecución (APP$_k$,TEE$_j$)
62
Asignación de parte o partes de hardware seguras
64
Limpieza de memoria
66
Carga de TEE$_{j, k}$
68
Ejecución Inst, APP$_k$
70
Cifrado y memorización
72

FIG.4

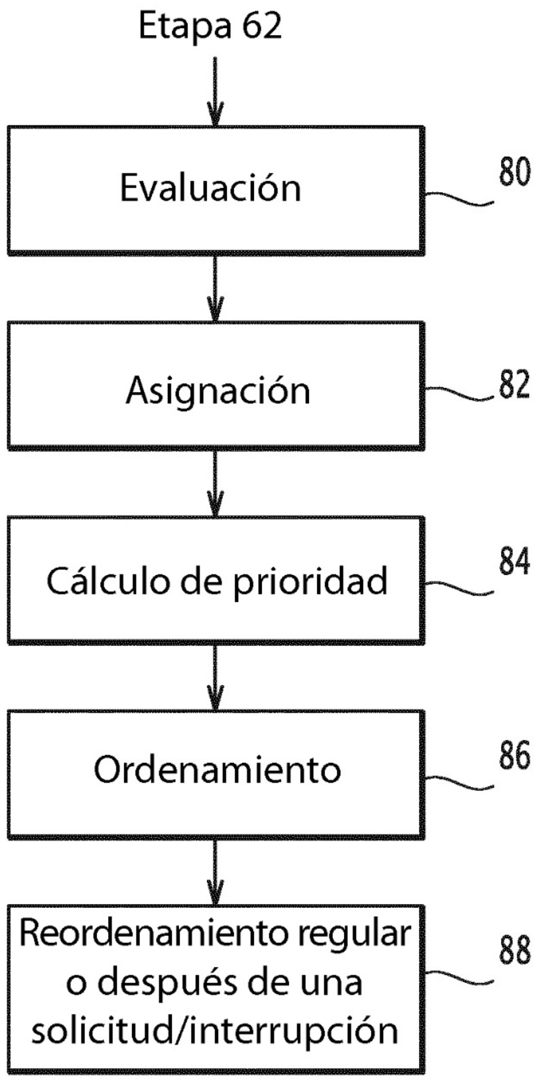

Etapa 62
Evaluación
80
Asignación
82
Cálculo de prioridad
84
Ordenamiento
86
Reordenamiento regular o después de una solicitud/interrupción
88

FIG.5