(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 674**

(51) Int. CI.:

G06F 21/85 (2013.01)
H04L 12/713 (2013.01)
G06F 21/53 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.12.2014 E 14200267 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2018 EP 2889803**

(54) Título: **Equipo de seguridad para la compartimentación entre un primer y segundo dominios, que comprende un componente de controlador**

(30) Prioridad:

24.12.2013 FR 1303074
24.12.2013 FR 1303075

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2018

(73) Titular/es:

THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR

(72) Inventor/es:

LACROIX, JEAN-MARC;
CURO, FRANCK;
RAGOT, DOMINIQUE;
THIERRY, PHILIPPE y
GERMAIN, FABIEN

(74) Agente/Representante:

SALVA FERRER, Joan

DESCRIPCIÓN

Equipo de seguridad para la compartimentación entre un primer y segundo dominios, que comprende un componente de controlador

[0001] La presente invención se refiere a un equipo de seguridad para la compartimentación entre un primer y segundo dominios, que comprende: una capa de hardware, que comprende un medio de cálculo, un medio de memorización, y un primer y segundo medios de interfaz con dichos primer y segundo dominios; una capa de virtualización de la capa de hardware, que comprende un núcleo y un hipervisor; y una capa de aplicación que comprende: un primer componente de interfaz, para intercambiar datos con el primer dominio; un segundo componente de interfaz para intercambiar datos con el segundo dominio; y un componente de seguridad que forma una celda de intercambio de datos entre el primer y segundo componentes.

[0002] En el campo de la seguridad de los sistemas de información, el documento FR 2008 006839 o incluso el documento US 7 607 167 B1 divulgan, respectivamente, un equipo de seguridad del tipo mencionado anteriormente adecuado para realizar la compartimentación entre el primer y segundo dominios. El documento DE 10 2012 105 068 A1 describe un sistema similar, basado en máquinas virtuales y que vincula varios controladores de interfaz aislados a través de una partición de control. En cada dominio, se implementa un controlador de interfaz virtual. Ventajosamente, tal equipo de seguridad constituye una puerta de enlace entre un primer dominio que presenta un nivel de seguridad "bajo" y un segundo dominio que presenta un nivel de seguridad "alto".

[0003] La capa de aplicación del equipo de seguridad del documento FR 2008 006839 B1 comprende un primer y segundo componentes de interfaz y un componente de seguridad.

[0004] El primer componente de interfaz está dedicado a gestionar el intercambio de paquetes de datos con el primer dominio. Comprende, en particular, los controladores necesarios para la comunicación con el primer dominio, a través de una primera interfaz de entrada/salida de la capa física del equipo de seguridad.

[0005] Cuando se ejecuta, el primer componente de interfaz sitúa los paquetes de datos recibidos desde el primer dominio en un primer espacio de almacenamiento de entrada de la memoria del equipo de seguridad. El primer componente de interfaz lee los paquetes de datos de un primer espacio de almacenamiento de salida de la memoria y los transmite al primer dominio.

[0006] De manera similar, el segundo componente de interfaz está dedicado a la gestión de intercambios de datos con el segundo dominio. Comprende, en particular, los controladores necesarios para la comunicación con el segundo dominio, a través de la segunda interfaz. Cuando se ejecuta, el segundo componente de interfaz accede a un segundo espacio de almacenamiento de salida de memoria y transmite los paquetes leídos al segundo dominio. El segundo componente de interfaz coloca los paquetes recibidos desde el segundo dominio en un segundo espacio de almacenamiento de entrada.

[0007] El componente de seguridad forma una celda en el intercambio de paquetes de datos entre el primer y segundo componentes de interfaz. Cuando se ejecuta, el componente de seguridad lee los paquetes de datos del primer espacio de almacenamiento de entrada, los procesa y coloca los paquetes procesados en el segundo espacio de almacenamiento de salida. De forma similar, el componente de seguridad lee los paquetes de datos del segundo espacio de almacenamiento de entrada, los procesa y coloca los paquetes procesados en el primer espacio de almacenamiento de salida.

[0008] Una partición espacial (es decir, el hecho de que los espacios de almacenamiento de entrada y salida de un canal de circulación del flujo de datos de un dominio a otro corresponden a espacios diferentes y predeterminados por la memoria) y una partición temporal (es decir, el hecho de que los componentes se ejecutan sucesivamente y por separado unos de otros por el procesador del equipo de seguridad, restringiéndose el tiempo de ejecución de un componente), garantizan la compartimentación entre el primer y segundo dominios.

[0009] Sin embargo, si el componente de seguridad puede certificarse en términos de seguridad operativa, no sucede lo mismo con el primer y segundo componentes de interfaz.

[0010] De hecho, si bien el componente de seguridad es un componente de aplicación que integra solo un programa de aplicación específico para acceder directamente a los recursos de hardware, un componente de interfaz es un componente del sistema operativo que integra un sistema operativo (SO para "sistema operativo"), tal

como el sistema LINUX, y posiblemente uno o más programas de aplicación, que son específicos para acceder a los recursos de hardware, pero solamente a través del sistema operativo.

[0011] Por lo tanto, un componente del sistema operativo es rico, en el sentido de que se implementan por defecto muchas funcionalidades. El programa de aplicación utiliza algunas de las funcionalidades disponibles, simplemente llamando a las funciones correspondientes. En particular, un componente de interfaz usa los controladores de periféricos nativos del sistema operativo.

[0012] Además, un sistema operativo es un programa complejo, que comprende unos cientos de miles de líneas de código. Es un programa que evoluciona regularmente a medida que se lanzan nuevas versiones. En el caso del sistema LINUX, el programa es actualizado por una comunidad cuyos miembros no se conocen.

[0013] Por lo tanto, no es posible evaluar y, por lo tanto, certificar un sistema operativo. Como resultado, no es posible certificar un componente del sistema operativo.

[0014] Por lo tanto, debido a que el sistema operativo contiene, un componente de sistema operativo y, en particular, un componente de interfaz tiene vulnerabilidades de seguridad.

[0015] Al aprovechar estas vulnerabilidades de seguridad, es posible eludir la compartimentación hecha por el componente de seguridad.

[0016] Por lo tanto, la invención tiene el propósito de superar este problema.

[0017] Para este fin, el objeto de la invención es un equipo de seguridad del tipo mencionado anteriormente, en el que al menos un componente de interfaz entre el primer y segundo componentes de interfaz está asociado con un componente complementario de controlador de interfaz, el núcleo realiza una partición espacial de manera que solo el componente de controlador tiene acceso exclusivo a un espacio de almacenamiento del medio de memorización asignado al medio de interfaz correspondiente, y el componente de controlador y el componente de interfaz intercambian datos a través de un espacio de memoria compartida del medio de memorización.

[0018] Al proporcionar al componente de seguridad un componente de controlador del tipo componente de aplicación y limitando los puertos de salida del componente de interfaz del tipo componente de sistema operativo, se eliminan los fallos de seguridad asociados con los controladores nativos del sistema operativo del componente de la interfaz.

[0019] De acuerdo con realizaciones particulares, el equipo comprende una o más de las siguientes características:

- el componente de interfaz y el componente de controlador asociado se ejecutan juntos en la misma partición temporal.
- el componente de interfaz y el componente de controlador asociado se ejecutan por separado en dos particiones temporales.
- el núcleo de la capa de virtualización es un núcleo de separación.
- el componente de seguridad realiza un intercambio de datos del tipo diodo, medio criptográfico o filtro.
- el componente de seguridad realiza un intercambio de datos de tipo diodo entre un espacio de almacenamiento de entrada en el lado del primer dominio y un espacio de almacenamiento de salida en el lado del segundo dominio.
- el primer componente de interfaz está asociado con un primer componente de controlador y el segundo componente de interfaz está asociado con un segundo componente de controlador.
- cada componente de controlador implementa aplicaciones de servicio, en particular de control del flujo de datos que pasa a través del componente de controlador, o un medio de interfaz de entrada/salida.

[0020] La invención se comprenderá mejor tras leer la siguiente descripción de una realización, dada únicamente a modo de ejemplo ilustrativo y no limitativo, y con referencia a los dibujos adjuntos, en los que:

- la Figura 1 es una vista esquemática de un equipo de seguridad según la invención;
- la Figura 2 es un gráfico temporal que muestra la ejecución de los diversos componentes del equipo de seguridad de la Figura 1.

[0021] En la Figura 1 se representa un equipo de seguridad 10 que establece una compartimentación en el

intercambio de paquetes de datos entre un primer y segundo dominios 1 y 2.

[0022] En el presente documento, el término "dominio" debe tomarse en sentido amplio: puede ser uno o más equipos informáticos diferentes conectados al equipo de seguridad considerado, a través de un enlace de comunicación adecuado. También puede tratarse de un programa asociado a una partición y ejecutado en el equipo de seguridad considerado. Sin embargo, la invención se aplica a un equipo de seguridad en comunicación a través de al menos una interfaz adaptada a otro equipo, constituyendo un dominio.

[0023] En la realización descrita en detalle en el presente documento, el primer y segundo dominios son redes conectadas al equipo de seguridad por enlaces de comunicación que cumplen con el protocolo ETHERNET. Sin embargo, los principios de arquitectura descritos en el presente documento no están limitados a un tipo particular de protocolo, y los expertos en la técnica pueden prever muchas variantes de realización alternativas.

[0024] El primer dominio 1 tiene un nivel de seguridad "bajo", más débil que el nivel de seguridad "alto" del segundo dominio 2.

[0025] Esto justifica la implementación, por el componente de seguridad 10, de una política de seguridad asimétrica entre paquetes de datos que fluyen desde el primer dominio al segundo dominio y los que fluyen desde el segundo dominio hasta el primer dominio.

[0026] En la realización descrita en el presente documento en detalle, el componente de seguridad 10 tiene una función de diodo, que autoriza la transmisión de paquetes de datos desde un emisor del primer dominio 1 a un receptor del segundo dominio 2, y que prohíbe, en operación nominal, cualquier intercambio de paquetes de datos desde el segundo dominio 2 al primer dominio 1.

[0027] El equipo de seguridad 10 comprende una capa de hardware 20, una capa de virtualización 30 y una capa de aplicación 38.

[0028] La capa de hardware 20 comprende un medio de cálculo, que comprende un procesador y un mecanismo de hardware para compartimentar la memoria, llamada MMU (Unidad de Gestión de Memoria), y un medio de memorización, que comprende una memoria, que es una memoria del sistema (RAM).

[0029] La capa de hardware 20 también comprende unos medios de interfaz de entrada/salida. Por ejemplo, el equipo de seguridad comprende una primera interfaz 21, del tipo ETHERNET, para la conexión al primer dominio 1 y una segunda interfaz 22, del tipo ETHERNET, para la conexión al segundo dominio 2.

[0030] La capa física 20 comprende finalmente un bus físico de comunicación entre los medios de cálculo, de memorización y de interfaz.

[0031] La capa de virtualización 30 hace posible virtualizar la capa física 20. Comprende un núcleo y un hipervisor.

[0032] De una manera conocida *per se*, el núcleo es del tipo núcleo de separación. Permite, en función de la MMU, la partición espacial de la memoria y la asignación ("mapeo") a un componente de la capa de aplicación, de un espacio específico de la memoria RAM del sistema.

[0033] De una manera también conocida *per se*, el hipervisor garantiza la partición temporal, asignando una fracción del tiempo de uso del medio de cálculo a cada componente o grupo de componentes de la capa de aplicación, y esto de acuerdo con un plan de programación definido durante la configuración del equipo de seguridad.

[0034] La capa de aplicación 38 comprende una pluralidad de componentes de software.

[0035] Un primer tipo de componente de software, la denominada aplicación, integra solamente un programa de aplicación Appli, específico para acceder directamente a los recursos de hardware.

[0036] Un segundo tipo de componente de software, el denominado sistema operativo, integra un sistema operativo SO, tal como el sistema LINUX, y posiblemente uno o más programas de aplicación Appli, específicos para acceder a los recursos de hardware a los que autorizó el hipervisor, solamente a través del sistema operativo.

[0037] En la realización mostrada en la Figura 1, la capa de aplicación 38 comprende un primer compartimento 40, que comprende un primer componente de controlador 41 y un primer componente de interfaz 42, un componente de seguridad 50, y un segundo compartimento 60, que comprende un segundo componente de controlador 61 y un segundo componente de interfaz 62.

[0038] Si el primer y segundo componentes de interfaz, 42 y 62, son componentes del sistema operativo, el primer y segundo componentes de controlador 41 y 61 y el componente de seguridad 50 son componentes de aplicación.

[0039] Un compartimento se divide funcionalmente entre un componente de controlador y un componente de interfaz.

[0040] Gracias a la partición espacial realizada por el núcleo de separación, el componente de interfaz no tiene acceso al espacio de la memoria reservada para la interfaz de entrada/salida de la capa de hardware. Solo el componente de controlador tiene acceso exclusivo al espacio de la memoria de la interfaz de entrada/salida de la capa de hardware.

[0041] Además, se define un canal de comunicación, a priori bidireccional, entre el componente de interfaz y el componente de controlador.

[0042] Por lo tanto, en la comunicación de enlace descendente, una función del componente de interfaz, llamada por un controlador nativo del sistema operativo de este componente, no escribe un dato en el espacio de la memoria de la interfaz de entrada/salida, sino en un espacio de memoria compartida con el componente del controlador. Éste lee los datos escritos en el espacio de memoria compartida e inicia una función correspondiente para escribir en el espacio de la memoria de la interfaz de entrada/salida.

[0043] Una descripción similar podría hacerse en la comunicación de enlace ascendente. El componente de controlador llama a una función que requiere la lectura de datos escritos en el espacio de memoria de la interfaz de entrada/salida y escribe los datos correspondientes en el espacio de la memoria compartida con el componente de interfaz. Éste llama a la función correspondiente del controlador nativo y lee los datos ubicados en el espacio de memoria compartida.

[0044] Ventajosamente, el componente de controlador puede, además de la aplicación de controlador AppliP, enriquecerse con una aplicación de servicio Appli, permitiendo, por ejemplo, el dominio de las operaciones de control del periférico conectado a la interfaz en cuestión, o incluso dominar el perfil del flujo de datos, ascendentes o descendentes, que fluye a través del componente de controlador.

[0045] Por lo tanto, el primer compartimento 40 está dedicado al intercambio de paquetes de datos con el primer dominio 1. Al ejecutarse por el medio de cálculo, el primer compartimento 40 escribe los paquetes de datos procedentes del primer dominio 1 en un espacio de almacenamiento de entrada 51 de la memoria de la capa física 20.

[0046] Específicamente, el primer compartimiento 40 comprende un primer componente de controlador 41 y un primer componente de interfaz 42. La partición espacial proporciona acceso para el primer componente de interfaz 42 a la primera interfaz 21 a través del componente de controlador 41 solamente, usando el espacio de memoria compartida 44. Por lo tanto, se define un canal de comunicación exclusivo entre el componente de interfaz 42 y el componente de controlador 41.

[0047] De manera similar, el segundo compartimento 60 está dedicado al intercambio de paquetes de datos con el segundo dominio 2. Al ejecutarse por el medio de cálculo, el segundo compartimento 60 lee los paquetes de datos de un espacio de almacenamiento de salida 52 de la memoria de la capa física 20 y los transmite al segundo dominio 2.

[0048] Específicamente, el segundo compartimiento 60 comprende un segundo componente de controlador 61 y un segundo componente de interfaz 62. La partición espacial proporciona acceso para el segundo componente de interfaz 62 a la segunda interfaz 22 a través del componente de controlador 61 solamente, usando el espacio de memoria compartida 64. Por lo tanto, se define un canal de comunicación exclusivo entre el componente de interfaz 62 y el componente de controlador 61.

[0049] El componente de seguridad forma una celda de intercambio de paquetes de datos entre el primer y

segundo compartimentos 40 y 60.

[0050] En la realización descrita en el presente documento en detalle, el componente de seguridad que es del tipo diodo es adecuado para leer un paquete de datos ubicado en el espacio de almacenamiento de entrada 51 y para escribirlo en el espacio de almacenamiento de salida 52.

[0051] En la Figura 2, el encadenamiento temporal de la ejecución de los diferentes componentes o grupo de componentes del equipo de seguridad 10 se muestra durante el transcurso de una trama T1, y la siguiente trama T2. Las tramas tienen una duración D constante predeterminada.

[0052] Cabe señalar que la programación de la ejecución de los componentes es idéntica de una trama a otra. Esta programación temporal se define mediante una partición de inicialización ejecutada una vez al inicio del componente de seguridad. La partición de inicialización no se muestra en la Figura 1.

[0053] Se ejecutan sucesivamente, en una primera partición temporal, los primeros componentes de controlador y de interfaz, 41 y 42, en una segunda partición temporal, el componente de seguridad 50 y, en una tercera partición temporal, los segundos componentes de controlador y de, 61 y 62.

[0054] Como alternativa, la ejecución del componente de controlador y la del controlador de interfaz de un mismo compartimiento se pueden dividir temporalmente entre sí.

[0055] Como alternativa, el componente de seguridad realiza otro tipo de compartimentación entre el primer y segundo dominio.

[0056] En aún otra variante, independiente de las anteriores, solo el compartimento de intercambio de datos con el dominio cuyo nivel de seguridad es el más bajo está funcionalmente dividido como se acaba de presentar, siendo el otro compartimento de conformidad con un componente interfaz de la técnica anterior.

[0057] En aún otra variante, los compartimentos 40, 60 y el componente de seguridad 50 pueden ejecutarse de forma programada en varios procesadores de cálculo en paralelo, desde el momento en que dos dominios se ejecutan en el mismo procesador de cálculo, su programación se descompondrá estrictamente, como se describe en las variantes anteriores.

[0058] Por lo tanto, el experto encontrará que el componente de controlador es un componente del tipo "PROXY", capaz de actuar en nombre del componente de interfaz.

[0059] El componente de controlador que es un componente de la aplicación puede ser certificado.

[0060] Se evitan los accesos del componente de interfaz a la capa de hardware.

[0061] Al inhibir de esta manera el acceso a los canales ocultos del sistema operativo de un componente rico, se mejora la seguridad operativa del equipo de seguridad.

REIVINDICACIONES

1. Equipo de seguridad (10) para la compartimentación entre el primer y el segundo dominios (1, 2), que comprende:

- una capa de hardware (20), que comprende un medio de cálculo, un medio de memorización, y un primer y segundo medios de interfaz (21, 22) con dichos primer y segundo dominios;
- una capa de virtualización (30) de la capa de hardware, que comprende un núcleo y un hipervisor;
- una capa de aplicación (38) que comprende:
- un primer componente de interfaz (42) para intercambiar datos con el primer dominio, siendo el primer componente de interfaz (42) del tipo componente del sistema operativo que integra un sistema operativo enriquecido, en el sentido de que se implementan por defecto numerosas funcionalidades y que no es posible certificarlo, comprendiendo el sistema operativo en particular un controlador nativo;
- un segundo componente de interfaz (62) para intercambiar datos con el segundo dominio, siendo el segundo componente de interfaz (62) del tipo componente del sistema operativo que integra un sistema operativo enriquecido, en el sentido de que se implementan por defecto numerosas funcionalidades y que no es posible certificarlo, comprendiendo el sistema operativo en particular un controlador nativo;
- un componente de seguridad (50) que forma una celda de intercambio de datos entre el primer y el segundo componentes,

caracterizado porque al menos un componente de interfaz entre el primer y segundo componentes de interfaz está asociado con un componente de controlador (41, 61), siendo el componente de controlador del tipo componente de aplicación que es posible certificar, realizando el núcleo una partición espacial tal que solo el componente de controlador tiene acceso exclusivo a un espacio de almacenamiento del medio de memorización asignado al medio de interfaz correspondiente (21, 22),y el componente de controlador (41, 61) y el componente de interfaz intercambian datos por medio de un espacio de memoria compartida (44, 64) del medio de memorización, siendo el componente de controlador (41, 61) un componente de tipo "PROXY" capaz de actuar por cuenta del componente de interfaz,
de tal manera que, en una primera dirección de intercambio de datos, una función del componente de interfaz, llamado por el controlador nativo del sistema operativo, escribe un dato en el espacio de memoria compartida con el componente del controlador y el componente del controlador lee los datos escritos en el espacio de memoria compartida y lanza una función correspondiente para escribir en el espacio de almacenamiento del medio de memorización asignado al medio de interfaz correspondiente (21, 22); y en una segunda dirección de intercambio de datos, el componente de controlador apela una función que requiere la lectura de datos escritos en el espacio de almacenamiento del medio de memorización asignado al medio de interfaz correspondiente (21, 22) y escribe el dato correspondiente en el espacio de memoria compartida con el componente de interfaz, y el componente de interfaz llama a la función correspondiente del controlador nativo y lee el dato ubicado en el espacio de memoria compartida, y **por que** el componente de controlador (41, 61) implementa aplicaciones de servicio para controlar el flujo de datos que pasa a través del componente de controlador.

2. Equipo de seguridad según la reivindicación 1, **caracterizado porque** el componente de interfaz (42, 62) y el componente de controlador asociado (41, 61) se ejecutan juntos en la misma partición temporal.

3. Equipo de seguridad según la reivindicación 1, **caracterizado porque** el componente de interfaz (42, 62) y el componente de controlador asociado (41, 61) se ejecutan por separado en dos particiones temporales.

4. Equipo de seguridad según una cualquiera de las reivindicaciones 1 a 3, **caracterizado porque** el núcleo de la capa de virtualización (30) es un núcleo de separación.

5. Equipo de seguridad según una cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** el componente de seguridad (50) realiza un intercambio de datos del tipo de diodo, medios criptográficos o filtro.

6. Equipo de seguridad según una cualquiera de las reivindicaciones 1 a 5, **caracterizado porque** el componente de seguridad (50) realiza un intercambio de datos de tipo diodo entre un espacio de almacenamiento de entrada (51) en el lado del primer dominio (1) y un espacio de almacenamiento de salida (52) en el lado del segundo dominio (2).

7. Equipo de seguridad según una cualquiera de las reivindicaciones 1 a 6, **caracterizado por que** el primer componente de interfaz está asociado con un primer componente de controlador y el segundo componente

de interfaz está asociado con un segundo componente de controlador.

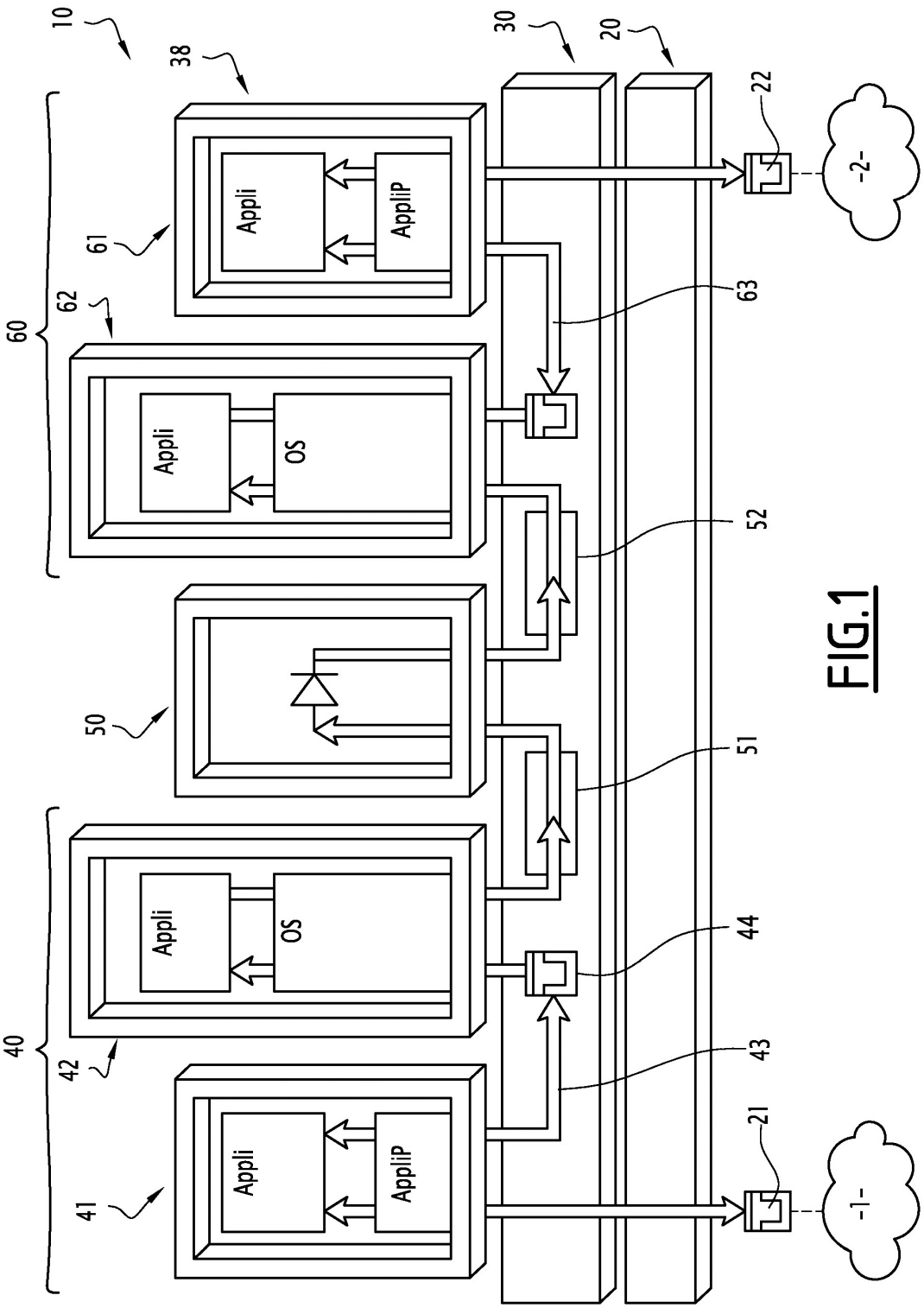
10
38
30
20
22
-2-
61
Appli
AppliP
63
62
60
Appli
OS
52
50
51
Appli
OS
44
40
42
43
41
Appli
AppliP
21
-1-

FIG.1

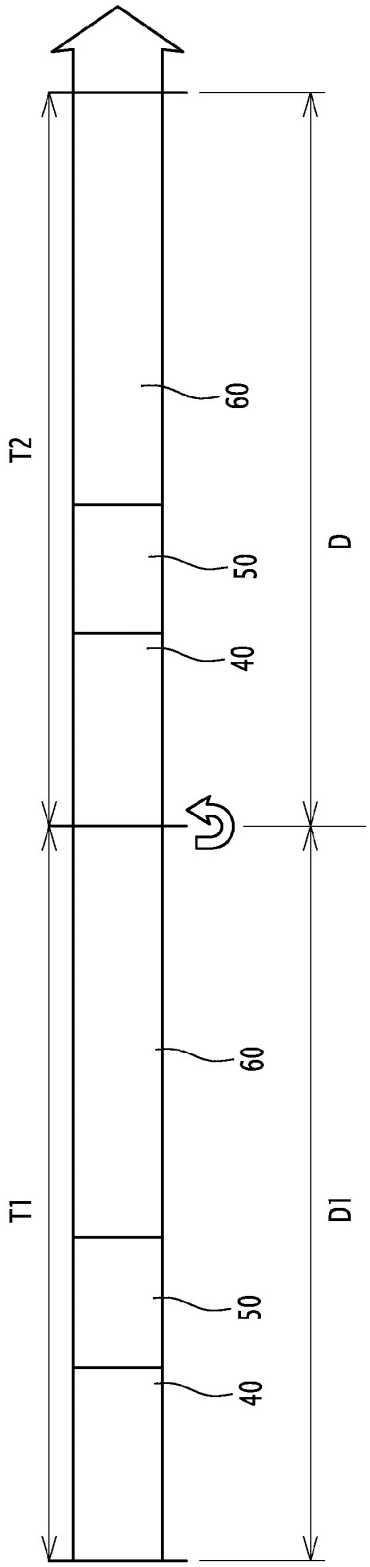

FIG.2