(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 525**

(51) Int. CI.:

***H04L 29/06*** (2006.01)
***H04L 29/08*** (2006.01)
***G06F 9/46*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.12.2009 PCT/FR2009/052687**

(87) Fecha y número de publicación internacional: **08.07.2010 WO10076523**

(96) Fecha de presentación y número de la solicitud europea: **23.12.2009 E 09806106 (2)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 2380328**

(54) Título: **Servidor de pasarela con micronúcleo**

(30) Prioridad:

**30.12.2008 FR 0859143**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**25.02.2020**

(73) Titular/es:

**CASSIDIAN CYBERSECURITY SAS (100.0%)**
**1 Boulevard Jean Moulin, ZAC de la Clef Saint Pierre**
**78990 Elancourt, FR**

(72) Inventor/es:

**MEIER, GUILLAUME;**
**CHALAND, MARC;**
**CLERMONT, NICOLAS y**
**HAUGUET, FRANCIS**

(74) Agente/Representante:

**ELZABURU, S.L.P**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Servidor de pasarela con micronúcleo

La presente invención hace referencia a un servidor de pasarela provisto de un micronúcleo. Asimismo, hace referencia a un procedimiento de transmisión de datos entre redes a través de un servidor de pasarela de este tipo.

Los sistemas operativos convencionales, tales como Microsoft Windows o GNU/Linux, no han sido diseñado con grandes restricciones de seguridad. El resultado es un diseño con poca seguridad en forma de un sistema operativo que utiliza capas operativas que se pueden representar según diversos modelos, tales como el modelo de interconexión de sistemas abiertos (OSI – Open Systems Interconnection, en inglés).

En el marco de un servidor de pasarela 17 (figura 1), denominado también mandatario o “proxy”, en inglés, esta representación se puede llevar a cabo de manera simple en tres niveles:

- Un primer nivel 16 de control comprende un núcleo que gestiona las operaciones realizadas por las aplicaciones del sistema operativo, en particular, asignando recursos a estas aplicaciones y controlando las comunicaciones entre estos recursos. El núcleo es, habitualmente, un núcleo monolítico, aunque se puede elegir un enfoque modular para gestionar de manera específica cada recurso ofrecido por el sistema operativo.

Un núcleo monolítico de este tipo incluye software de bajo nivel, tal como el programador, el gestor de procesos, el gestor de memoria, así como los controladores de los dispositivos periféricos, y algunos servicios de alto nivel, tales como sistemas de archivos y algoritmos criptográficos o de filtrado.

- Un segundo nivel 14 de comunicación comprende las aplicaciones de software, en particular, que forman las pilas de protocolos necesarias para emitir o recibir datos a través de una red de telecomunicación utilizando un protocolo de comunicación.

En una pila de protocolos, cada capa resuelve un cierto número de problemas relativos a la transmisión de datos, y proporciona servicios bien definidos a las capas superiores del primer nivel 16. Estas capas altas están más cerca del usuario y gestionan datos más abstractos, utilizando los servicios de las capas inferiores que formatean estos datos para que puedan ser emitidos en un medio físico.

- Un tercer nivel 12 de rendimiento de medios realizan la interfaz del servidor 17 con una red exterior 10 u 11. Este nivel 12, habitualmente, cumple con el protocolo de Ethernet que implementa una capa física y una subcapa de software, a saber, la capa de control de acceso a medios (MAC – Media Access Control, en inglés) del modelo OSI.

Una pasarela 17 de este tipo puede tener una función de filtrado destinada a garantizar la transmisión de datos 13 recibidos, por ejemplo, de una red insegura 10, tal como la red de Internet, hacia una red sensible 11. En este caso, estos datos 13 son tratados:

- Mediante el nivel de 12 de Ethernet del servidor de pasarela 17, para permitir su tratamiento en el servidor, y, a continuación,

- mediante el nivel 14 de comunicación, que comprende una pila de protocolos TCP/IP, siglas de “protocolo de control de la transmisión” y “protocolo de internet” (“Transmission Control Protocol” / “Internet Protocol, en inglés), para generar los datos, transmitidos según los protocolos de transporte, según protocolos de aplicación y, después, finalmente,

- mediante el nivel 16 de control, que lleva a cabo servicios de filtrado de alto nivel que permiten, por ejemplo, desencriptar los datos antes de su transmisión a la red sensible 11.

El documento US5828893 describe un sistema con dos servidores de pasarela cuyas capas de aplicación se comunican a través de una red dedicada segura. El documento “Future Directions in the Evolution of the L4 Microkernel” de K. Elphinstone, Actas del taller de NICTA sobre verificación de OS, páginas 1-17, 2004, describe un micronúcleo, un controlador de IPC y una memoria compartida, adecuados para gestionar comunicaciones.

La presente invención resulta de la constatación de que un servidor de este tipo, y el procedimiento requerido para su puesta en práctica, presentan inconvenientes. En particular, presentan problemas específicos propios de la complejidad de un núcleo monolítico y de la arquitectura de un sistema informático que no permite una verificación formal de la vulnerabilidad de un servidor de pasarela.

De manera más precisa, ningún mecanismo puede probar que los datos procedentes de 10 pasan sucesivamente por todas las etapas del filtrado realizadas por los niveles 12, 14 y 16. Por lo tanto, se puede producir un mal funcionamiento 15, voluntario o accidental en uno de estos niveles 12 o 14 y provocar que se evite el nivel 16 de control.

A título de ejemplo, un mal funcionamiento 15 de este tipo se representa en el nivel de comunicación 14, por ejemplo, en la capa propia de la pila TCP/IP. En este caso, este mal funcionamiento 15 transmite datos provenientes de la red 10 a la red 11 sin la transmisión previa de estos últimos en el nivel 16 de control.

Por lo tanto, es posible acceder a la red 11 con independencia de las reglas de transmisión que deben ser aplicadas por el nivel 16 de control, lo que representa un fallo del servidor 17 difícilmente aceptable.

Para dar respuesta a este problema, la presente invención hace referencia a un servidor de pasarela provisto de un primer subsistema que comprende un nivel de medios, un nivel de comunicación y un nivel de control, comprendiendo, asimismo, este servidor, un micronúcleo y un controlador de IPC que gestionan comunicaciones entre los recursos del servidor asignados al primer subsistema, caracterizado por que comprende:

- un segundo subsistema, que comprende un segundo nivel de medios, un segundo nivel de comunicación y un segundo nivel de control, de tal manera que el micronúcleo y el controlador de IPC gestionan asimismo comunicaciones entre los recursos del servidor asignados a este segundo subsistema, y

- una memoria compartida en lectura y en escritura, establecida bajo el control del micronúcleo y del controlador de IPC, entre el nivel de control del primer subsistema y el nivel de control del segundo subsistema.

Un servidor de pasarela de este tipo da respuesta al problema de la ausencia de las funciones de control para transmisiones debidas a un mal funcionamiento, provocadas o accidentales, del nivel de medios y/o del nivel de comunicación de un servidor de pasarela.

De hecho, un mal funcionamiento de este tipo no puede conducir a la transmisión de datos entre redes en un servidor según la invención, pudiendo transmitir datos el nivel de control entre estas redes únicamente a través de la memoria compartida.

Por consiguiente, un servidor de este tipo presenta numerosas ventajas. Por una parte, permite dar respuesta a un defecto de reglas de seguridad claramente establecidas en la red sensible, puesto que estas reglas pueden ser implementadas por su nivel de control.

Asimismo, permite prevenir un ataque proveniente de una red no sensible y dirigido a evitar el nivel de seguridad de un servidor de pasarela evitando su nivel de control.

Un servidor según la invención permite, de este modo, proteger una red sensible de agresiones externas, voluntarias o no. De esta manera permite garantizar una política de seguridad entre redes de diferentes sensibilidades, por ejemplo, entre una red no segura y una red sensible.

En una realización, cada subsistema comprende medios para codificar información, recibida en una solicitud según un protocolo de comunicación de red, en una estructura binaria según un protocolo de comunicación entre los niveles de control del primer subsistema y del segundo subsistema.

En este caso, cada subsistema puede comprender medios para codificar la información en una estructura binaria tras el tratamiento de aquella en el nivel de comunicación y, a continuación, en el nivel de control de este subsistema.

Según una realización, el servidor comprende medios para identificar, en función de la naturaleza de la solicitud, datos característicos de la solicitud que deben ser codificados en la estructura binaria.

En una realización, el servidor comprende medios para asociar la solicitud revisada con una solicitud predefinida en una lista limitada de solicitudes autorizadas.

Según una realización, el micronúcleo comprende medios para asociar cada aplicación puesta en práctica mediante un subsistema al control de un recurso del servidor.

En una realización, el servidor comprende medios para limitar las comunicaciones de tal manera que ni el nivel de medios ni el nivel de comunicación de un subsistema se puedan comunicar directamente con el nivel de medios o el nivel de comunicación del otro subsistema sin la mediación de los niveles de control de los subsistemas.

Según una realización, el servidor comprende medios para analizar la sintaxis y la validez de los protocolos filtrados por cada capa utilizada en el servidor.

La invención hace referencia, asimismo, a un procedimiento de control de un servidor de pasarela provisto de un primer subsistema que comprende un nivel de medios, un nivel de comunicación y un nivel de control, comprendiendo, asimismo, este servidor un micronúcleo y un controlador de IPC que gestiona las comunicaciones entre los recursos del servidor asignados al primer subsistema, caracterizado por que el servidor está provisto, asimismo, de un segundo subsistema, que comprende un segundo nivel de medios, un segundo nivel de comunicación y un segundo nivel de control, de tal manera que el micronúcleo y el controlador de IPC gestionan, asimismo, comunicaciones entre los recursos del servidor asignados a este segundo subsistema, se utiliza una

memoria compartida en lectura y en escritura, establecida bajo el control del micronúcleo, para transmitir solicitudes entre el nivel de control del primer subsistema y el nivel de control del segundo subsistema utilizando un servidor según una de las realizaciones anteriores.

Finalmente, la invención hace referencia, asimismo, a un producto de programa informático que comprende instrucciones de código de programa registradas en un medio legible por ordenador para llevar a cabo un procedimiento según la invención cuando dicho programa es ejecutado en un ordenador.

La invención se comprenderá con la lectura de la siguiente descripción, dada únicamente a título ilustrativo y no limitativo, y realizada haciendo referencia a los dibujos adjuntos, en los que:

- la figura 1, ya descrita, es una vista esquemática del funcionamiento de un servidor de pasarela según la técnica anterior;
- la figura 2 es una vista esquemática del funcionamiento de un servidor de pasarela según la invención, y
- la figura 3 representa el tratamiento de una solicitud de HTTP por parte de un servidor según la invención.

Haciendo referencia a la figura 2, un servidor de pasarela 27 según la invención comprende dos niveles de medios 22 y 32, dos niveles de comunicación 24 y 34 y dos niveles de control 26 y 36.

Sin embargo, se implementa un solo micronúcleo 38 para realizar algunas funciones básicas, tal como la gestión de las comunicaciones entre los recursos del servidor, en particular, mediante transferencia de mensaje IPC para “Inter Process Communication”, en inglés.

Además de esta gestión, un micronúcleo de segunda generación comprende un controlador de reloj y un programador, para que dicho micronúcleo contenga menos de 20.000 líneas de código.

Comparativamente, un núcleo monolítico comprende millones de líneas de código, con un riesgo proporcional de errores y fallos de seguridad. Difícilmente se puede verificar que cumple con las especificaciones de los verificadores de código y de los sistemas de prueba formal actuales.

Además, los núcleos monolíticos tienen malas propiedades de aislamiento. De hecho, los procesos del usuario pueden romper el aislamiento de diferentes formas, gracias a los tubos, a los archivos, a la memoria compartida, etc. La gestión de las comunicaciones entre procesos no es confiable.

De hecho, tal como se indicó anteriormente, no existe aislamiento, en el interior de un núcleo monolítico, entre subsistemas del núcleo, tal como, por ejemplo, entre los controladores y las pilas de la red. De este modo, un controlador de un componente de hardware defectuoso o dañado puede poner en peligro todo el sistema.

La utilización de micronúcleos llamados de segunda generación resuelve el problema de un fallo en el nivel de control. Estos micronúcleos tienen un tamaño que les permite ser fácilmente mantenidos y verificados formalmente, por ejemplo, para certificarlos a un nivel alto, tal como el nivel 7 del estándar internacional EAL, “Evaluation Assurance Level” en inglés.

A título de ejemplo, los micronúcleos de segunda generación más conocidos, y actualmente utilizados en diferentes variantes, están basados en una aplicación de programación o API, “Application Programming Interface” en inglés común - L4 diseñada bajo la dirección de Jochen Liedtke.

De este modo, un servidor de pasarela equipado con dicho micronúcleo permite responder a la complejidad y vulnerabilidad de los núcleos monolíticos. En términos de seguridad, dicho sistema aprovecha la solidez del micronúcleo.

Sin embargo, la seguridad de los servidores depende, asimismo, de la solidez de las comunicaciones IPC, ya que representan un medio posible de transmisión de datos peligrosos. Ahora bien, por razones de eficacia, la gestión de la seguridad de las comunicaciones se deja tradicionalmente al nivel de los servidores, contentándose el micronúcleo con transmitir los mensajes.

Es por lo que, en esta realización, el micronúcleo 38 comprende un controlador de IPC 25 que proporciona un mecanismo de derechos de comunicación de tal manera que dos aplicaciones solo se pueden comunicar entre sí si el controlador 25 reconoce que estas aplicaciones poseen los derechos apropiados.

De hecho, el micronúcleo considera cada aplicación, por ejemplo, de servicios o de controladores, como el sujeto de los criterios de seguridad que le fueron proporcionados de antemano.

A partir de estos criterios, el micronúcleo 38 puede asignar recursos del sistema a las aplicaciones que gestiona según una regla establecida en su inicio, mientras que su controlador de IPC 25 asigna o niega derechos de comunicación entre estas aplicaciones.

En otras palabras, el micronúcleo 38 identifica, por una parte, recursos para asignar, tales como la memoria, las entradas y salidas, privilegios para niveles de gestión de - y, por otra parte, comunicaciones pendientes de autorización del controlador de IPC 25.

De este modo, cuando una aplicación requiere una comunicación IPC entre diferentes elementos, el controlador de IPC 25 determina a partir de esta lista si la aplicación solicitante tiene derecho a comunicarse con la aplicación de destino.

El controlador de IPC 25 realiza, por consiguiente, la función de controlador de IPC para, por ejemplo, emitir derechos de comunicación a aplicaciones particulares bajo demanda. De manera similar, este controlador de IPC puede detectar intentos de violación de los criterios de seguridad y proporcionar una auditoría sobre el potencial de violación.

En esta realización, el micronúcleo 38 tiene, asimismo, la función de mantener para cada aplicación las comunicaciones previamente autorizadas.

Una estructura de este tipo permite un control preciso sobre la utilización de los recursos, mientras que, de manera simultánea, cada aplicación es asociada con el control de un recurso, es decir, de un componente o mecanismo de hardware, lo que refuerza el control para bloquear la propagación de un ataque o de un error.

En el servidor 27, el tratamiento de datos utiliza, por consiguiente, dos subsistemas, a saber:

- por una parte, un subsistema, formado por el nivel 22 de medios, el nivel 24 de comunicación y el nivel 26 de control, conectado a la red 20 no segura, por ejemplo, la red de Internet, y
- por otra parte, un subsistema seguro, formado por el nivel 32 de medios, el nivel 34 de comunicación y el nivel 36 de control conectado a la red sensible 21, por ejemplo, una red de aviónica, una intranet de defensa y/o un nodo central de comunicación.

De hecho, cada subsistema gestiona un flujo de datos, por ejemplo, al nivel de su interfaz de red o de su pila de protocolos, utilizando sus propios recursos físicos que están aislados del otro subsistema, excepto entre su nivel de control, tal como se describe más adelante.

De este modo, el micronúcleo 38 y su controlador de IPC 25 permiten comunicaciones del nivel 22, respectivamente 32, de medios con el nivel 24, respectivamente 34, de comunicación, pudiendo comunicarse el último nivel solo con el nivel de control 26, respectivamente 36.

De este modo, suponiendo que un ataque o un error de la red 20 logró infiltrarse a través de un fallo en una de las capas del nivel de medios 22 y/o el nivel de comunicación 24, por ejemplo, en la aplicación de un controlador y/o de la pila de protocolos, los datos no pueden ser transmitidos a la red sensible 21 sin su tratamiento por parte de los niveles 26 y 36 de control.

Por otra parte, la arquitectura del servidor permite realizar un filtrado profundo de la red, utilizando este filtrado un análisis de la sintaxis y de la validez de los protocolos filtrados por cada capa del servidor, por ejemplo: Ethernet, IP, TCP, nivel de aplicación.

Por ello, una solicitud enviada por el subsistema no seguro es transformada, durante su tratamiento progresivo por el nivel de comunicación 24 y después por el nivel de control 26, de una solicitud en una estructura binaria simple claramente definida.

Una transformación de este tipo está representada en la figura 3, que ilustra la descomposición de una solicitud de protocolo HTTP en datos binarios que codifican la información transmitida mediante esta instrucción HTTP.

De manera más precisa, estos datos comprenden una instrucción “Get”, una dirección URL, la versión del protocolo HTTP utilizado y los formatos de archivo tenidos en cuenta por un software de exploración, o navegador.

Estos datos binarios, representados en forma de tabla en aras de la claridad, son transmitidos a continuación al nivel 36 de control del subsistema seguro por medio de una memoria compartida 29 entre los dos subsistemas.

A este efecto, se utiliza un protocolo definido de manera limitativa. Un protocolo de este tipo define el conjunto de las solicitudes que pueden ser emitidas por el nivel 26 de control de la red no segura, de tal manera que los campos de datos requeridos para estas solicitudes pueden, por una parte, estar predeterminados y, por otra parte, ser rellenados con datos binarios que codifican la información identificada en la solicitud recibida.

De este modo, las solicitudes transmitidas por la red 20 no segura a través del servidor de pasarela 27 son tratadas por el subsistema no seguro para extraer estas últimas de los datos característicos de las solicitudes, siendo transmitidos estos datos característicos al subsistema seguro a través del nivel de control 26 de este subsistema no seguro.

A continuación, el subsistema seguro reescribe la solicitud según su nivel 34 de comunicación, por ejemplo, según un protocolo HTTP, en base a datos característicos previamente extraídos. A continuación, esta solicitud es transmitida a través del nivel 32 de comunicación al servidor de destino, que puede ser forzado, por lo tanto, de manera válida y segura.

Un formateado de los datos de este tipo se representa en la figura 3 a partir de los datos binarios obtenidos anteriormente a partir de una solicitud HTTP.

A cambio, la respuesta del servidor de destino es recibida por el nivel de medios 32, y, después, 34 de comunicación, a fin de alcanzar el nivel 36 de control.

Este nivel 36 de control puede transmitir, por lo tanto, los datos binarios, obtenidos a partir de la respuesta, a través de la memoria compartida 29, para que esta última la transmita al solicitante a través de los niveles 26, 24 y después 22 del subsistema no seguro.

Parece que un servidor de pasarela según la invención no pretende bloquear errores y/o ataques, sino limitar sus consecuencias en la red sensible, puesto que el conjunto de las solicitudes emitidas en la red sensible por este servidor son solicitudes validadas mediante su reescritura, no correspondiéndose estas solicitudes validadas exactamente con la solicitud inicial. La arquitectura del servidor garantiza, de este modo, la seguridad de la pasarela.

En resumen, cada subsistema actúa como una esclusa, no pudiendo comunicarse con el otro subsistema más que a través de una memoria en la que están registrados datos binarios que codifican la información identificada en una solicitud recibida en la entrada de uno de los subsistemas en campos predefinidos.

De esta manera, los subsistemas no se comunican más que a través de su nivel de control, particularmente confiable por la presencia de un micronúcleo, y por medio de datos cuyo rango está limitado al campo predefinido.

La presente invención es susceptible de numerosas variantes. En particular, la siguiente descripción de la invención realizada anteriormente presenta un micronúcleo 38 que comprende el controlador de IPC 25 pero, en función de las variantes y criterios utilizados para definir un micronúcleo, este controlador de IPC 25 puede estar localizado fuera del micronúcleo 38.

**REIVINDICACIONES**

1. Servidor de pasarela (27), caracterizado por que comprende:

- un primer subsistema (22, 24, 26), con un nivel de medios (22), un nivel (24) de comunicación y un nivel (26) de control,
- un segundo subsistema (32, 34, 36), con un segundo nivel de medios (32), un segundo nivel (34) de comunicación y un segundo nivel (36) de control,
- un micronúcleo (38) y un controlador (25) de IPC ("*Inter Process Communication*", en inglés) adaptado para gestionar comunicaciones entre los recursos del servidor asignados al primer subsistema, por una parte, y para gestionar, asimismo, comunicaciones entre los recursos del servidor asignados al segundo subsistema, por otra parte, y
- una memoria (29) compartida en lectura y en escritura, establecida bajo el control del micronúcleo y del controlador de IPC, para la transmisión de solicitudes entre el nivel de control del primer subsistema y el nivel de control del segundo subsistema.

2. Servidor según la reivindicación 1, en el que cada uno de los primer y segundo subsistemas comprende medios para codificar información, recibida en una solicitud según un protocolo de comunicación de red, en una estructura binaria según un protocolo de comunicación entre el nivel de control del primer (26) subsistema y el nivel de control del segundo (36) subsistema.

3. Servidor según la reivindicación 2, en el que cada uno de los primer y segundo subsistemas (22, 24, 26; 32, 34, 36) comprende medios para codificar la información en una estructura binaria después del tratamiento de dicha información en el nivel de comunicación (24; 34) y, después, en el nivel (26; 36) de control del subsistema.

4. Servidor según la reivindicación 2 o 3, que comprende, además, medios para identificar, en función de la naturaleza de la solicitud, datos característicos de la solicitud que deben ser codificados en la estructura binaria.

5. Servidor según la reivindicación 2, que comprende, además, medios para asociar la solicitud recibida con una solicitud predefinida en una lista limitada de solicitudes autorizadas.

6. Servidor según una cualquiera de las reivindicaciones anteriores, en el que el micronúcleo (38) comprende medios para asociar cada aplicación puesta en práctica por un subsistema (22, 24, 26; 32, 34, 36) al control de un recurso del servidor.

7. Servidor según una cualquiera de las reivindicaciones anteriores, que comprende, además, medios para limitar las comunicaciones, de tal manera que ni el nivel de medios (22) ni el nivel de comunicación (24) de uno de los primer y segundo subsistemas se puedan comunicar directamente con el nivel de medios (32) o el nivel de comunicación (34), respectivamente, del otro de dichos primer y segundo subsistemas sin la mediación de los niveles de control (26, 36) de dichos primer y segundo subsistemas.

8. Servidor según una de las reivindicaciones anteriores, que comprende, además, medios para analizar la sintaxis y la validez de los protocolos filtrados por cada capa utilizada en el servidor.

9. Procedimiento de control de un servidor de pasarela (27), que comprende un primer subsistema con un nivel de medios (22), un nivel (24) de comunicación y un nivel (26) de control, así como, además, un segundo subsistema (32, 34, 36) con un segundo nivel de medios (32), un segundo nivel (34) de comunicación y un segundo nivel (36) de control, comprendiendo este servidor (27), asimismo, un micronúcleo (38) y un controlador (25) de IPC ("Inter Process Communication", en inglés) que gestiona comunicaciones entre los recursos del servidor asignados al primer subsistema, por una parte, y que gestiona, asimismo, comunicaciones entre los recursos del servidor asignados al segundo subsistema, por otra parte, procedimiento en el que se utiliza la memoria (29) del servidor compartida en lectura y en escritura, establecida bajo el control del micronúcleo y del controlador de IPC, para transmitir solicitudes entre el nivel de control del primer subsistema y el nivel de control del segundo subsistema con la ayuda de los medios de un servidor según una de las reivindicaciones anteriores.

10. Producto de programa informático, que comprende instrucciones de código de programa registradas en un medio legible por ordenador, para llevar a cabo el procedimiento según la reivindicación 9 cuando el programa está siendo ejecutado en un ordenador.

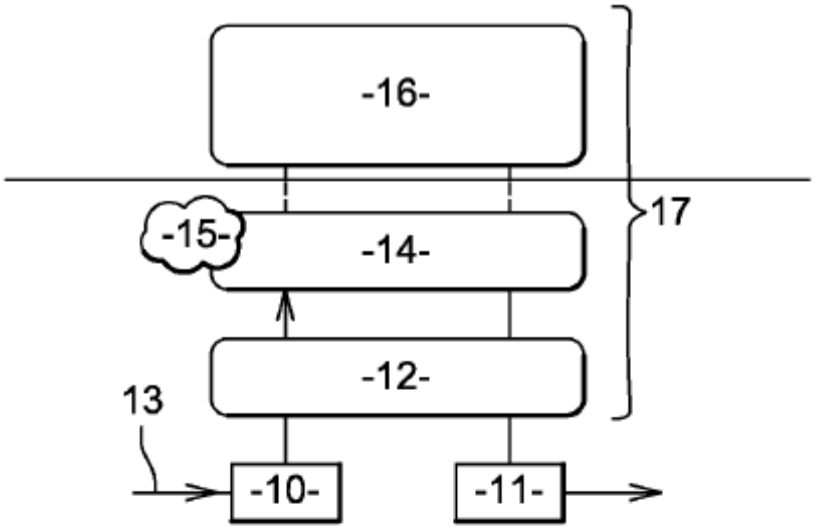


Fig. 1

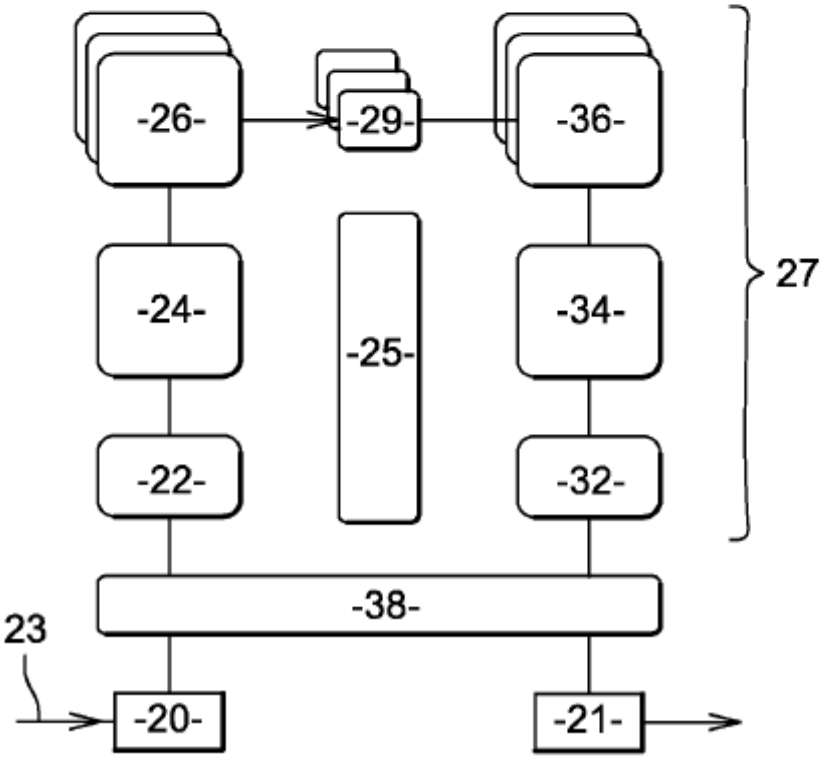


Fig. 2

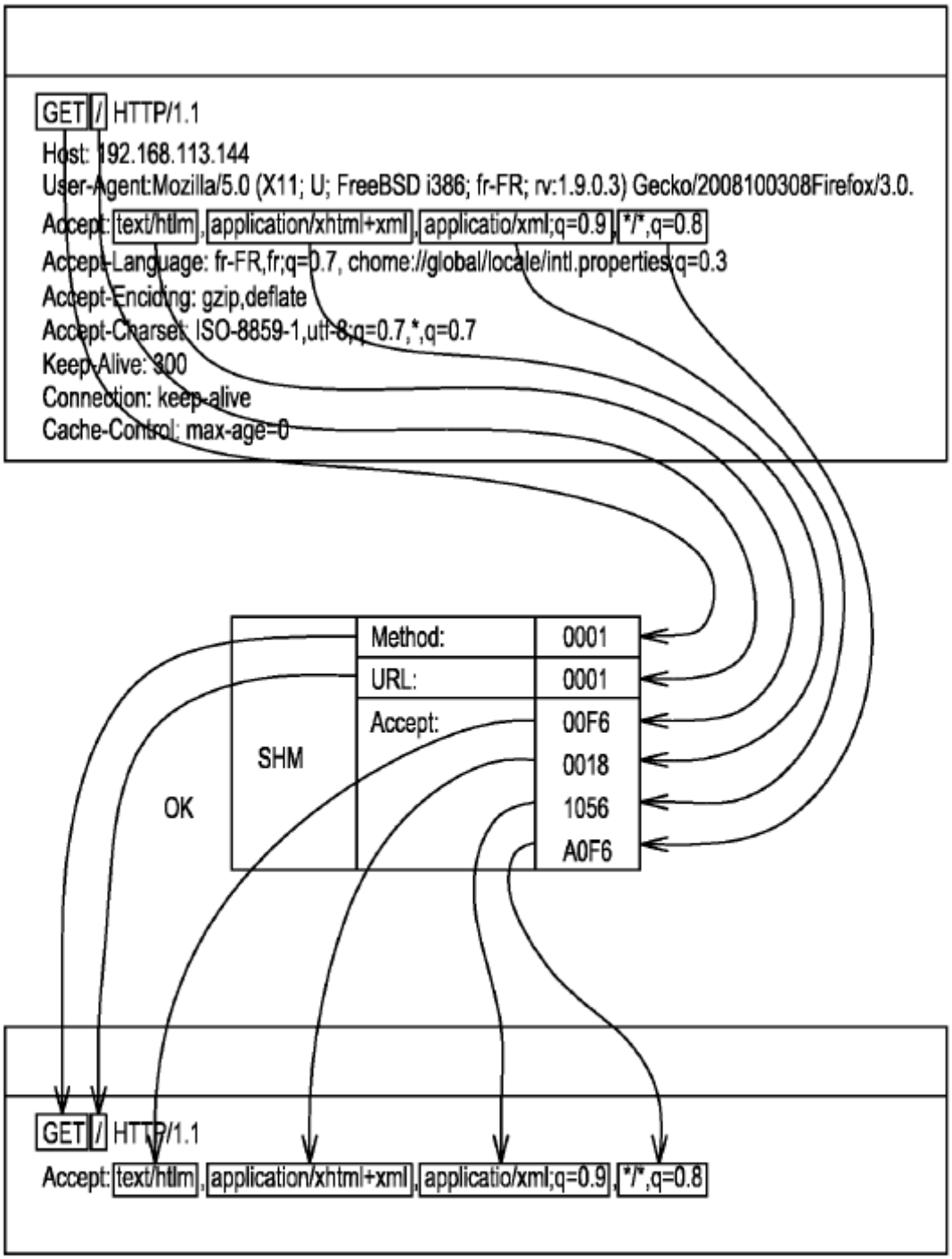
GET / HTTP/1.1
Host: 192.168.113.144
User-Agent:Mozilla/5.0 (X11; U; FreeBSD i386; fr-FR; rv:1.9.0.3) Gecko/2008100308Firefox/3.0.
Accept: text/html, application/xhtml+xml, applicatio/xml;q=0.9, */*,q=0.8
Accept-Language: fr-FR,fr;q=0.7, chome://global/locale/intl.properties;q=0.3
Accept-Enciding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*,q=0.7
Keep-Alive: 300
Connection: keep-alive
Cache-Control: max-age=0
Method:
0001
URL:
0001
Accept:
00F6
0018
1056
A0F6
SHM
OK
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, applicatio/xml;q=0.9, */*,q=0.8

**Fig. 3**