(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 548 178**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 9/455 (2006.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.11.2010 E 10793009 (1)**

(97) Fecha y número de publicación de la concesión europea: **01.07.2015 EP 2502399**

(54) Título: **Procedimiento y dispositivos para la securización de la conexión de un terminal a una red informática**

(30) Prioridad:

19.11.2009 FR 0958182

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.10.2015

(73) Titular/es:

SAAD, CLÉMENT (100.0%)
1 Traverse de l'Artimon
34970 Lattes, FR

(72) Inventor/es:

SAAD, CLÉMENT

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Procedimiento y dispositivos para la securización de la conexión de un terminal a una red informática.

Campo técnico

La presente invención se sitúa en el campo de las comunicaciones y de la informática.

La invención se refiere más particularmente a la conexión de un terminal a una red de comunicación de tipo informático y a la securización de los datos que transitan por una conexión del tipo mencionado.

La invención encontrará una aplicación particular, aunque en ningún caso limitativa, en la securización y la regulación de flujos de datos que entran o salen hacia o desde un terminal, tal como un ordenador, recíprocamente desde o hacia una red de comunicación, en particular informática, tal como internet, a través de una conexión con dicha red.

Estado de la técnica anterior

Tal como es sabido, un terminal se conecta a una red informática a través de por lo menos una interfaz de comunicación. Por medio de esta interfaz, transitan flujos de datos entrantes desde dicha red hacia dicho terminal y salientes desde dicho terminal hacia dicha red.

Un inconveniente principal de los flujos de datos, en particular recibidos por dicho terminal, reside en los problemas de seguridad creados. En efecto, dichos datos recibidos pueden ser peligrosos, en particular los que comprenden un programa o datos maliciosos (“malware”) por ejemplo, de manera no exhaustiva: un virus, un gusano informático, un troyano, una puerta trasera (“backdoor”), un programa espía, un bulo (“hoax”), correo basura, suplantación de identidad (“phishing”) o similares. Por lo tanto, existe una necesidad absoluta de proteger dicho terminal contra la recepción de datos maliciosos del tipo mencionado a través de la securización de su conexión y del filtrado de los datos recibidos.

Por otro lado, la conexión con dicha red puede provocar defectos de seguridad o accesos a portales virtuales no deseados, por ejemplo, sitios de internet de orden personal a los cuales accede un usuario desde un terminal profesional. Se debe contemplar por lo tanto una restricción del acceso de dicho terminal hacia dicha red.

Para ello, existen muchas soluciones, en forma tangible o de software, generalmente dedicadas a uno u otro caso.

Una solución generalizada consiste en un cortafuegos o *firewall* que limita las intrusiones hacia dicho terminal bloqueando ciertos puertos de comunicación con dicha red y filtrando los flujos de datos. Un firewall puede ser un software, instalado en dicho terminal o un servidor que actúe como pasarela con dicha red, o tangible.

Otra solución, totalmente de software, consiste en aplicaciones denominadas “anti-virus”. Se trata de aplicaciones instaladas en dicho terminal, o en un servidor que actúa como pasarela, y que permiten filtrar los datos una vez recibidos.

Dichas soluciones, aunque están adaptadas para terminales de tipo puesto fijo, generan problemas de puesta en práctica en el ámbito de los terminales móviles, de tipo ordenador portátil, susceptibles de conectarse desde diferentes emplazamientos geográficos. Por lo tanto, no se pueden contemplar las soluciones puestas en práctica por un servidor o un hardware anexo físico (tal como un cortafuegos o un encaminador).

Una solución alternativa conocida consiste en unos dispositivos amovibles, aptos para conectarse a dicho terminal y que permiten configurar para cada terminal parámetros de conexión particulares y que integran programas anti-virus u otros.

Un ejemplo de un dispositivo amovible del tipo mencionado se describe por medio del documento WO 02/095543 referente a la securización, por cifrado, de los datos, en particular de los paquetes que forman dichos flujos. Aunque una solución de este tipo mejora la seguridad de la transferencia de los datos, no impide en modo alguno la transmisión, incluso cifrada, de programas o datos maliciosos.

En el documento WO 2007/069245 se describe otra solución referente a un dispositivo amovible provisto de medios de conexión con un terminal y que actúa como pasarela de forma que filtra los flujos de datos procedentes de dicha red. Para ello, este intermediario integra unos programas ejecutados en dicho terminal desde el dispositivo, aunque también a nivel de hardware para desviar la conexión con dicha red con el fin de que la misma transite por dicho dispositivo amovible.

Un dispositivo de este tipo está limitado al nivel de hardware, en relación con dicho terminal. En efecto, adolece del inconveniente de ser específico de cada tipo de conexión, por cables o no, con dicha red. Además, es específico del sistema operativo que funciona en dicho terminal, dado que actúa en las capas del núcleo de dicho sistema.

Se conoce también el documento US 2006/112342 A1, que describe un procedimiento según el preámbulo de la reivindicación 1.

Exposición de la invención

La invención tiene como objetivo paliar los inconvenientes del estado de la técnica al proponer una solución totalmente aplicativa, es decir que se puede implementar en una forma de software, que permite securizar la conexión de un terminal a una red de comunicación. En particular, la invención permite filtrar los flujos de datos por medio de aplicaciones dedicadas y configurar restricciones de acceso de un usuario a dicha red.

De forma ventajosa, el tratamiento de los flujos resulta posible a través de una reproducción virtual de las interfaces de conexión de dicho ordenador y convirtiendo éstas últimas en indisponibles.

Para ello, la presente invención se refiere a un procedimiento de securización de la conexión de un terminal a una red de comunicación, en particular de tipo informático, en el que dicho terminal está conectado a dicha red a través de por lo menos una interfaz de comunicación de forma que emite y recibe por lo menos un flujo de datos, según la reivindicación 1.

El procedimiento según la invención puede comprender además unas etapas:

- de atribución de una dirección física a la interfaz virtual idéntica a la dirección física de la interfaz de comunicación;

- de atribución de una dirección MAC (Control de Acceso al Medio o *Media Access Control* en inglés) a la interfaz virtual, idéntica a la dirección MAC de la interfaz de comunicación;

- de asignación a la interfaz de comunicación de una dirección IP incompatible con la red;

- de creación de una interfaz nueva a nivel de dicho terminal apta para recibir el flujo controlado;

El procedimiento según la invención puede comprender además, en calidad de control del flujo de datos a nivel de la pasarela, por lo menos cualquiera de las siguientes etapas: protección, filtrado, tratamiento de dicho flujo de datos.

La pasarela virtual puede comprender una máquina virtual.

Esta máquina virtual puede comprender un sistema operativo diferente al del terminal, o un sistema operativo idéntico o similar al del terminal.

Según otros aspectos, se propone:

- un dispositivo de programa de ordenador que comprende instrucciones para ejecutar las etapas del procedimiento según la invención, siendo dicho programa de ordenador apto para ser ejecutado en el terminal;

- un dispositivo de almacenamiento masivo que comprende un programa de ordenador, caracterizado por que es apto para conectarse al terminal de tal manera que se permite la ejecución de dicho programa de ordenador en dicho terminal;

- un dispositivo de almacenamiento masivo que comprende cualquiera de los siguientes dispositivos: llave USB, tarjeta de memoria, disco duro, o cualquier otro soporte físico o virtual.

Según otros modos de realización, el procedimiento según la invención puede consistir en:

- crear una pasarela virtual de control aplicativo de dicho flujo de datos;

- crear una interfaz virtual a nivel de dicha pasarela por duplicación de dicha interfaz de comunicación;

- convertir en indisponible dicha interfaz de comunicación con respecto a dicha red de manera que dicho flujo sea redirigido hacia dicha interfaz virtual;

- controlar dicho flujo a nivel de dicha pasarela y a continuación encaminarlo (o transferirlo), controlado, hacia dicho terminal.

Dicha duplicación puede consistir en la creación de un puente entre dicha interfaz de comunicación y dicha interfaz virtual nueva.

De forma ventajosa, dicho procedimiento puede consistir en convertir en indisponible dicha interfaz de comunicación modificando la interfaz con la red por asignación de una dirección incompatible con dicha red.

Además, el encaminamiento puede consistir en crear una interfaz nueva a nivel de dicho terminal con el fin de transmitirle dicho flujo controlado.

En particular, dicho control aplicativo puede consistir en un conjunto de módulos de protección, de filtro y de tratamiento de dicho flujo de datos.

Preferentemente, dicha pasarela virtual puede estar constituida por una imagen virtual ejecutada a partir de una máquina virtual.

De esta manera, la invención bloquea las interfaces existentes de un terminal, convirtiéndolas en inaccesibles y duplica estas interfaces de manera virtual con el fin de sustituir por ellas las interfaces bloqueadas. Por lo tanto, esta última recibe los flujos de datos en lugar y en calidad de dicho terminal, y efectúa un tratamiento sobre estos flujos para reenviarlos tratados hacia dicho terminal.

De manera ventajosa, las interfaces virtuales presentan, desde el punto de vista de la red, unas características sustancialmente idénticas a las correspondientes de las interfaces de comunicación del terminal que reproducen. En particular, pueden presentar la misma dirección física o dirección MAC, y por lo tanto pueden sustituir completamente las interfaces de comunicación del terminal.

Esta sustitución de las interfaces de comunicación del terminal por las interfaces virtuales a nivel de la dirección física, que se corresponde con una toma de control por parte de la pasarela virtual de las interfaces de comunicación del terminal a nivel de la capa de enlace (según la terminología clásica de los protocolos TCP/IP), permite obtener con el procedimiento según la invención una eficacia de protección óptima, claramente superior a la de procedimientos de la técnica anterior basados simplemente en la utilización de máquinas virtuales para securizar aplicaciones de red. Efectivamente, en los procedimientos conocidos de la técnica anterior, las interfaces de comunicación simplemente se reparten entre el terminal y una o varias máquinas virtuales por medio de una aplicación de encaminamiento que es de hecho un programa ejecutado a nivel del sistema operativo del terminal. De aquí se deriva un riesgo de fallo de seguridad entre las interfaces de comunicación y la pasarela virtual, el cual no existe en el procedimiento según la invención.

Además, al ser la invención completamente aplicativa, es decir que se puede realizar en forma de software, la misma se libera de las restricciones vinculadas al hardware y se puede introducir en cualquier tipo de soporte.

Descripción de las figuras y modos de realización

Otras características y ventajas de la invención se pondrán de manifiesto a partir de la descripción detallada que se ofrece a continuación de los modos de realización no limitativos de la invención, en referencia a la figura 1 adjunta que representa una vista esquematizada de un ejemplo de arquitectura en cuyo seno se pone en práctica el procedimiento de securización según la invención.

La presente invención se refiere a la securización de la conexión de un terminal 1 a una red de comunicación 2.

Se observará que el terminal 1 y la red 2 pueden ser de cualquier tipo, en particular de tipo informático. En este caso, el terminal 1 puede ser un ordenador, mientras que la red 2 puede ser de forma ventajosa una intranet o internet.

De forma general, el terminal 1 está conectado a la red 2 a través de por lo menos una interfaz de comunicación, preferentemente varias interfaces distintas.

En el ejemplo de arquitectura visible en la figura, el terminal 1 comprende dos interfaces de comunicación 3 y 4 conectadas a la red 2. En particular, la conexión se efectúa a través de un encaminador 5, que actúa como pasarela con el resto de la red 2, en particular internet.

A este respecto, el encaminador 5 comprende una parametrización de la red a nivel local, en particular entre el encaminador 5 y el terminal 1. Más particularmente, el encaminador 5 puede comprender unos parámetros de tipo direccionamiento de las interfaces 3 y 4 de dicho terminal 1.

Se observará que, según el modo preferido de realización, este direccionamiento puede consistir en la asignación de direcciones IP (de “Internet Protocol”) y/o de máscara de subred, de forma automática (por ejemplo a través del

protocolo de asignación de red DHCP de “Dynamic Host Configuration Protocol”) o manual por medio de un administrador de dicho encaminador 5.

Así, básicamente, a cada interfaz 3, 4 se le asigna inicialmente una dirección IP que le permite conectarse a la red 2 por el desvío del encaminador 5. Por lo tanto, estando configurado así inicialmente, el terminal 1 se conecta a la red 2 de manera que emite y recibe por lo menos un flujo de datos, en particular un flujo por la interfaz 3 y 4.

Esta conexión inicial se representa en la figura con la forma de dos flujos de datos sombreados y de puntos entre el terminal 1 y el encaminador 5.

De forma ventajosa, la presente invención consiste en crear una pasarela virtual 6 con capacidad de garantizar la securización y la regulación del o de los flujos de datos. La pasarela 6 puede consistir en una imagen virtual, de software, construida y configurada a partir de las características del terminal 1.

A este respecto, es posible introducir en el seno de esta imagen virtual un sistema operativo similar o diferente al correspondiente que actúa en el terminal 1. En el caso de un sistema diferente, los riesgos de ejecución de programas de software maliciosos o de ataques por un tercero, se verán en particular disminuidos.

En particular, la imagen virtual se ejecuta a partir o en forma de una máquina virtual instalada en el terminal 1 o que se ejecuta a partir de un soporte distinto. En cualquiera de los dos casos, se puede asignar una parte de la memoria del terminal 1 para esta ejecución.

Resulta por ejemplo ventajoso crear una pasarela virtual 6 que comprenda una máquina virtual que funcione bajo un sistema operativo Linux, para implementarla en un terminal 1 que funcione con un sistema operativo de tipo diferente, como por ejemplo Microsoft® Windows®.

De esta manera, la pasarela virtual 6 se puede configurar, en particular vinculándole la totalidad de las interfaces 3, 4 del terminal 1, especialmente puenteándolas. Se puede realizar entonces una copia de seguridad del estado de la imagen de la pasarela virtual 6 para restaurarla durante una próxima ejecución.

Además, la invención prevé que cada flujo de datos se redirija hacia la pasarela 6 con el fin de controlarlo.

De forma ventajosa, este control del flujo después de su redireccionamiento hacia la pasarela 6 se efectúa de manera aplicativa, en particular interviene únicamente a través de programas de software de la capa aplicativa (en el sentido en que es ejecutado por aplicaciones de software). Por lo tanto, la invención es portátil y compatible, en particular se puede adaptar a cualquier sistema operativo, y también puede prescindir de cualquier tipo de soporte. Así, la misma se puede instalar directamente en el terminal 1, o en un dispositivo tangible provisto de medios de interacción con el terminal 1, tal como una memoria masiva equipada con una conectividad normalizada, como por ejemplo una llave equipada con conectividad USB (de “Universal Serial Bus”).

De forma más precisa, el control aplicativo consiste en un conjunto 7 de módulos de protección, de filtro y de tratamiento de dicho flujo de datos.

Dichos módulos pueden ser, de manera no exhaustiva, un cortafuegos, un antivirus, un anti-espía, un anti-correo basura, un proxy, un filtro de direccionamiento (tal como un URL de “Uniform Resource Locator”), un sistema de detección y de prevención de intrusiones (IDPS), un sistema de prevención de usurpación de identidades físicas (MAC), una red privada virtual (RPV), una securización y regulación de ciertos tipos de flujo, especialmente la voz por red IP (VoIP de “Voice over Internet Protocol”).

Después del tratamiento, los flujos de datos filtrados y por lo tanto limpios, son reenviados hacia el terminal 1. Ocurre lo mismo en sentido inverso para solicitudes de acceso a portales virtuales autorizados o no en función de la configuración de un módulo.

Para permitir el tránsito de los flujos de datos a través de la pasarela virtual 6, la invención prevé el cortocircuito o bloqueo del camino de conexión existente entre el terminal 1 y la red 2, específicamente el encaminador 5.

Por un lado, la invención procura sustituir las interfaces de comunicación 3, 4 existentes a nivel del terminal 1 por interfaces virtuales 30, 40 a nivel de la pasarela 6.

La creación de cada interfaz virtual 30 (o 40) a nivel de la pasarela 6 se efectúa por duplicación de la interfaz de comunicación correspondiente 3 (o recíprocamente 4).

Preferentemente, esta duplicación consiste en la creación de un puente entre la interfaz de comunicación 3 (o 4) y la interfaz virtual nueva 30 (o 40). En otras palabras, las interfaces de comunicación 3, 4 y las interfaces virtuales nuevas 30, 40 se “puentean”.

Esta duplicación comprende la duplicación de la dirección física (o dirección MAC para Control de acceso al soporte o en inglés *Media Access Control*), de tal manera que la interfaz virtual 30 (o 40) tenga, desde el punto de vista de la red 2 o del encaminador 5, la misma dirección MAC que la interfaz de comunicación 3 (o 4).

La creación de la interfaz virtual 30 (o 40) implica por lo tanto una toma de control de la interfaz de comunicación 3 (o 4) a nivel de la capa de enlace, lo cual permite obtener una seguridad óptima.

Por otro lado, la invención prevé convertir en indisponible la interfaz de comunicación 3, 4 con respecto a la red 2. Para ello, la invención modifica la interfaz con la red 2 por asignación de una dirección incompatible con la red 2. En otras palabras, la invención cambia la configuración de red inicial del terminal 1. A cada interfaz de comunicación 3, 4 se le asigna una dirección IP no válida en la red 2, no encaminable por el encaminador 5.

Por lo tanto, el flujo de datos es redirigido automáticamente hacia la interfaz virtual 30, 40. En efecto, la duplicación de las interfaces mantiene los parámetros válidos de la configuración inicial (incluyendo las direcciones físicas o MAC) y los lleva a nivel de la pasarela virtual 6 que se conecta entonces automáticamente a dicha red 2, en particular el encaminador 5, en lugar del terminal 1.

Así, los flujos de datos transitan por la pasarela 6 y pueden ser controlados y a continuación encaminados (o dirigidos) después del tratamiento hacia el terminal 1.

Se observará que varios flujos que entran a nivel de la pasarela 6 pueden ser controlados y a continuación reenviados en forma de un único flujo hacia el terminal 1.

A este respecto, el encaminamiento consiste en crear una interfaz nueva 8 a nivel del terminal 1 con el fin de transmitirle el flujo controlado desde la pasarela virtual 6.

De manera más precisa, se crea una interfaz 80 virtual complementaria de encaminamiento, de modo que se cree una conexión, por un lado, con la interfaz 8 y, por otro lado, con las otras interfaces virtuales 30 y 40. La conexión entre las interfaces virtuales 30, 40 y la interfaz complementaria 80 transita por los módulos de control 7 con el fin de llevar a cabo el tratamiento sobre los flujos de datos.

Así, los flujos llegan limpios al nivel del terminal 1 por medio de la pasarela virtual 6.

La invención permite que el terminal 1 reciba flujos de datos desde la red 2 pero redirigiéndolos hacia la pasarela 6 antes de poder acceder a su contenido.

Evidentemente, la invención no se limita a los ejemplos ilustrados y descritos anteriormente que pueden presentar variantes y modificaciones sin apartarse por ello del alcance de la invención.

REIVINDICACIONES

1. Procedimiento de securización de la conexión de un terminal (1) a una red (2) de comunicación, en particular de tipo informático, en el que dicho terminal (1) se conecta a dicha red (2) a través de por lo menos una interfaz de comunicación (3, 4) de manera que emita y reciba por lo menos un flujo de datos, que comprende unas etapas de:

- creación de una pasarela virtual (6) de control de dicho flujo de datos que comprende una máquina virtual implementada en dicho terminal (1),
- creación de una interfaz virtual (30, 40) a nivel de dicha pasarela (6) por duplicación de dicha interfaz de comunicación (3, 4),
- control de dicho flujo de datos a nivel de dicha pasarela (6) y encaminamiento del flujo de datos controlado hacia dicho terminal (1),
- configuración de dicha interfaz de comunicación (3, 4) para convertirla en indisponible con respecto a dicha red (2), de manera que dicho flujo de datos sea redirigido hacia dicha interfaz virtual (30, 40),

caracterizado por que comprende además una etapa de asignación a la interfaz de comunicación (3, 4) de una dirección incompatible con dicha red (2), de tal manera que dicha interfaz de comunicación (3, 4) se convierte en indisponible con respecto a dicha red (2).

2. Procedimiento de securización según la reivindicación 1, caracterizado por que consiste en:

- crear una pasarela virtual (6) de control aplicativo de dicho flujo de datos,
- crear una interfaz virtual (30, 40) a nivel de dicha pasarela (6) por duplicación de dicha interfaz de comunicación (3, 4),
- convertir en indisponible dicha interfaz de comunicación (3, 4) con respecto a dicha red (2) de manera que dicho flujo sea redirigido hacia dicha interfaz virtual (30, 40),
- controlar dicho flujo a nivel de dicha pasarela (6) y a continuación encaminarlo, (controlarlo), hacia dicho terminal (1).

3. Procedimiento de securización según una de las reivindicaciones 1 o 2, caracterizado por que dicha duplicación comprende además una etapa de creación de un puente entre dicha interfaz de comunicación (3, 4) y dicha interfaz virtual (30, 40).

4. Procedimiento según cualquiera de las reivindicaciones anteriores, caracterizado por que comprende además una etapa de atribución de una dirección física a la interfaz virtual (30, 40) idéntica a la dirección física de la interfaz de comunicación (3, 4).

5. Procedimiento según cualquiera de las reivindicaciones anteriores, caracterizado por que comprende además una etapa de atribución de una dirección MAC a la interfaz virtual (30, 40) idéntica a la dirección MAC de la interfaz de comunicación (3, 4).

6. Procedimiento según la reivindicación 6, caracterizado por que comprende además una etapa de asignación a la interfaz de comunicación (3, 4) de una dirección IP incompatible con la red (2).

7. Procedimiento de securización según cualquiera de las reivindicaciones anteriores, caracterizado por que comprende además una etapa de creación de una nueva interfaz (8) a nivel de dicho terminal (1) apta para recibir el flujo controlado.

8. Procedimiento de securización según cualquiera de las reivindicaciones anteriores, caracterizado por que comprende además, en calidad de control del flujo de datos a nivel de la pasarela (6), por lo menos cualquiera de las siguientes etapas: protección, filtrado, tratamiento de dicho flujo de datos.

9. Procedimiento de securización según cualquiera de las reivindicaciones anteriores, caracterizado por que la pasarela virtual (6) comprende una máquina virtual.

10. Procedimiento de securización según la reivindicación 10, caracterizado por que la máquina virtual comprende un sistema operativo diferente del correspondiente del terminal (1).

11. Dispositivo de programa de ordenador, caracterizado por que comprende instrucciones para ejecutar las etapas del procedimiento según cualquiera de las reivindicaciones anteriores, y por que es apto para ser ejecutado en el terminal (1).

12. Dispositivo de almacenamiento masivo que comprende un programa de ordenador según la reivindicación 11, caracterizado por que es apto para conectarse al terminal (1) de tal manera que permita la ejecución de dicho programa de ordenador en dicho terminal (1).

13. Dispositivo de almacenamiento masivo según la reivindicación 12, caracterizado por que comprende cualquiera de los siguientes dispositivos: llave USB, tarjeta de memoria, disco duro.

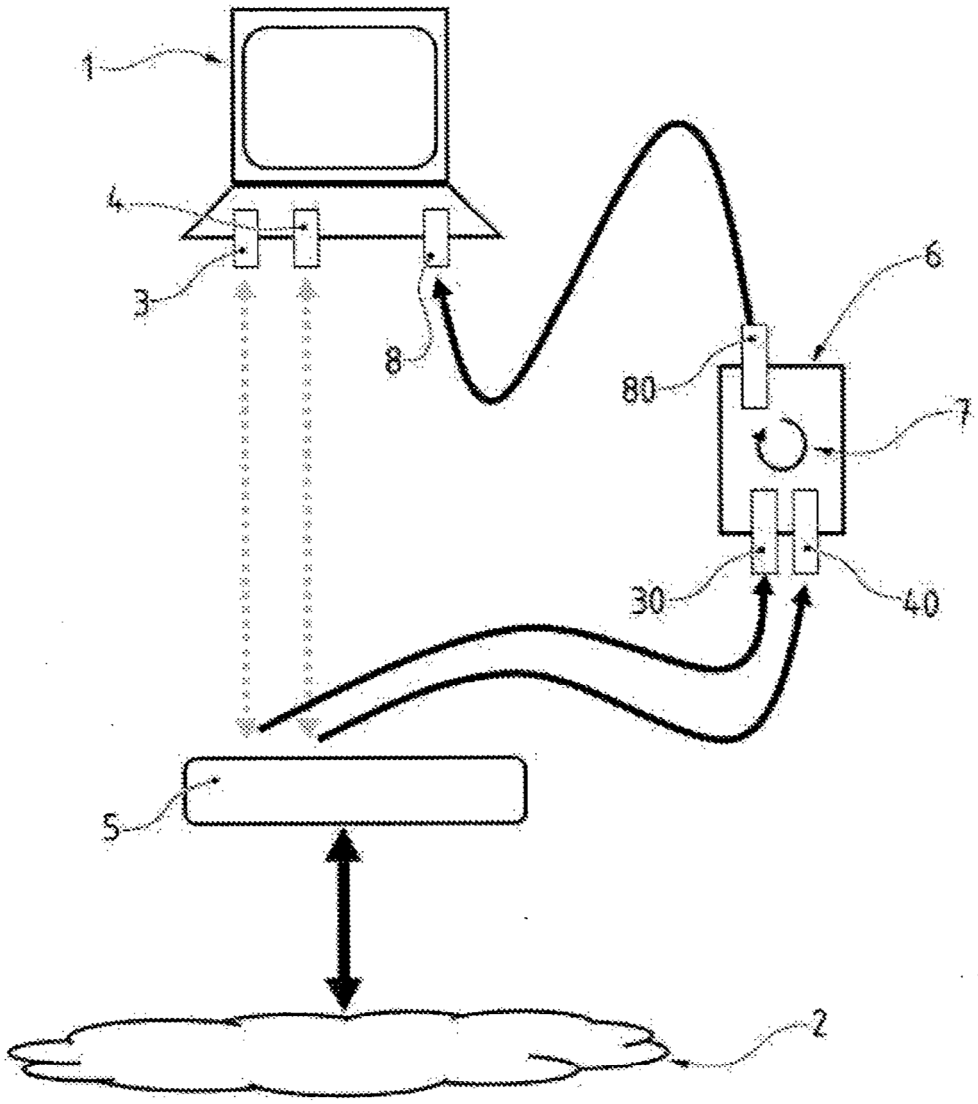

Figura 1