(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 811 502**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.04.2007 E 07290427 (9)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 1843518**

(54) Título: **Procedimiento de protección de una dirección de correo electrónico, sistema y dispositivos asociados**

(30) Prioridad:

07.04.2006 FR 0603103

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2021

(73) Titular/es:

ORANGE (100.0%)
78 rue Olivier de Serres
75015 Paris, FR

(72) Inventor/es:

GOUTARD, CÉDRIC y
BOUTROUX, ANNE

(74) Agente/Representante:

ISERN JARA, Jorge

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

Procedimiento de protección de una dirección de correo electrónico, sistema y dispositivos asociados

La presente invención se refiere a la protección de direcciones de correo electrónico.

La puesta a disposición de una dirección de correo electrónico, por ejemplo en una red de comunicación tal como Internet, puede dar lugar al envío de múltiples mensajes no deseados a esta dirección. Este fenómeno, que tiende a aumentar, se conoce con los nombres de "correo basura", "correo no deseado" o también "spam".

Para limitar los riesgos de recepción de tales mensajes no deseados, un usuario puede estar interesado en no proporcionar su dirección de correo electrónico durante una comunicación con un servidor de comunicación, por ejemplo, al acceder a un servidor web.

Sin embargo, a pesar de estas precauciones, se constata que muchos servidores web requieren un registro de los usuarios con ayuda de su dirección de correo electrónico, como requisito previo para acceder a su contenido. Ahora bien, a pesar de los marcos legales que existen en ciertos países, las direcciones proporcionadas por los usuarios a menudo son explotadas sin su consentimiento, con fines comerciales en particular.

El correo basura resultante se puede filtrar con relativa eficiencia, a costa de la implementación costosa y restrictiva de medios adecuados, tal como la instalación y la utilización de un software "antispam", por ejemplo.

Otra posibilidad para evitar este correo basura, consiste, para un usuario, en comunicar una dirección de correo electrónico falsa al registrarse en un servidor. Sin embargo, esta técnica consta de ciertos inconvenientes. En efecto, existe un riesgo (bajo) de que la dirección falsa comunicada corresponda efectivamente con la dirección de otro usuario, de modo que el correo basura se dirigirá entonces a este otro usuario. Otro inconveniente, más molesto, es que ninguna información útil podrá ser recibida por el usuario que ha comunicado una dirección de correo electrónico falsa.

El documento EP 1 223527 divulga un mecanismo de distribución de correos electrónicos, que hace uso de una dirección de emisión distinta de la dirección del remitente. Sin embargo, este mecanismo no tiene lugar en el contexto de un procedimiento de registro de usuario en un servidor.

Se pueden encontrar ejemplos y modos de realización de la técnica anterior en el documento WO 00/52900.

Un objetivo de la presente invención es paliar los inconvenientes mencionados anteriormente.

Otro objetivo de la invención es permitir a un usuario recibir mensajes útiles de un servidor remoto, mientras que tiene la posibilidad de controlar el correo basura recibido, por ejemplo, después de un registro en este servidor.

La invención proporciona de este modo un procedimiento de protección de una dirección de correo electrónico de un usuario de acuerdo con la reivindicación 1.

De este modo, el servidor dispone de una dirección de sustitución relacionada con el usuario, con ayuda de la cual puede intercambiar mensajes con el usuario, sin conocer, no obstante, la dirección de correo electrónico real del usuario.

Por lo tanto, el correo basura no puede ser transmitido directamente con destino a la dirección de correo electrónico del usuario. Por lo tanto, esta última está protegida del fenómeno del correo basura.

La sustitución de direcciones también se realiza de forma transparente para el usuario.

Si la dirección de sustitución se utiliza para transmitir a ella correo basura, el usuario tiene, ventajosamente, la posibilidad de invalidar esta dirección, para detener el fenómeno de correo basura relacionado con esta dirección.

De modo ventajoso, la dirección de sustitución tiene en cuenta elementos de contexto, tales como una dirección relacionada con el servidor al que dicho mensaje es enviado. Esta dirección puede ser la del propio servidor o la dirección de una página administrada por este servidor.

De modo ventajoso, la dirección de sustitución se memoriza en correspondencia con la dirección de correo electrónico del usuario, y opcionalmente también con elementos de contexto.

Esta memorización permite recuperar la dirección de correo electrónico del usuario correspondiente a la dirección de sustitución a la que un mensaje es enviado, por ejemplo, por el servidor. A continuación se puede transmitir este mensaje al usuario, con ayuda de la dirección de correo electrónico recuperada.

La invención se define en las reivindicaciones independientes. Realizaciones particulares se presentan en las reivindicaciones dependientes.

Algunas de las realizaciones descritas a continuación no son realizaciones de la invención según las reivindicaciones.

Otras particularidades y ventajas de la presente invención se pondrán de manifiesto en la siguiente descripción de ejemplos de realización no limitativos, con referencia a los dibujos adjuntos, en los que:

- la figura 1 es una representación esquemática de las principales operaciones implementadas en el marco de la invención;
- la figura 2 es una representación esquemática de operaciones implementadas dentro de un sistema de acuerdo con un ejemplo de realización de la invención.

La figura 1 muestra un usuario 1 que utiliza un terminal 2, que puede ser, por ejemplo, un ordenador, un teléfono móvil, un asistente digital personal u otro, provisto de medios para intercambiar mensajes con una entidad remota, ventajosamente por medio de una red de comunicación 4. El usuario 1 tiene que comunicar información relacionada con su dirección de correo electrónico, por ejemplo, en el marco de un procedimiento de registro en un servidor 3.

El servidor 3 es, por ejemplo, un servidor web. En ese caso, el terminal 2 del usuario 1 está provisto además de un navegador web capaz de comunicarse con el servidor 3, por ejemplo por medio de una red de Internet 4. Las interfaces 5 y 6 entre la red 4, por un lado, y el terminal 2 y el servidor 3, por otro lado, pueden ser de todo tipo, por ejemplo, por cable o inalámbricas.

Según la invención, el usuario 1 transmite un mensaje 7 a la atención del servidor 3. Este mensaje 7 contiene una dirección de correo electrónico del usuario, a partir de la cual es capaz de transmitir mensajes a una entidad remota y en la que es capaz de recibir mensajes de una entidad remota.

Este mensaje 7 está destinado al servidor 3 y se transmite por medio de la red 4, por ejemplo, en el marco de un registro del usuario 1 en este servidor 3 o de una página web administrada por este servidor 3. Puede transmitirse a petición del servidor 3. Ventajosamente, asume la forma de un formulario cumplimentado por el usuario 1 con su dirección de correo electrónico. Cuando el servidor 3 es un servidor web en particular, el mensaje 7 comprende, por ejemplo, una solicitud del tipo HTTP (HyperText Transport Protocol).

A continuación, el mensaje 7 es interceptado por un dispositivo o un sistema que tiene lugar, por ejemplo, al menos en parte, en la red 4, aunque también son concebibles otras arquitecturas, pudiendo realizarse ciertas operaciones localmente.

El mensaje 7 es entonces objeto de un análisis de su contenido, a fin de determinar si consta de una dirección de correo electrónico.

En caso afirmativo, entonces se obtiene una dirección de sustitución relacionada con el usuario 1. Esta obtención puede consistir en una creación de una dirección. También puede comprender una búsqueda y una posible identificación de una dirección de sustitución ya creada relacionada con el usuario 1, preferentemente en el mismo contexto, es decir, durante un intercambio previo entre el usuario 1 y servidor 3 o una página web particular administrada por el servidor 3.

La dirección de sustitución obtenida puede, en efecto, depender ventajosamente del servidor 3, o de la página web administrada por este servidor 3, a la que es enviado el mensaje 7, es decir, elementos de contexto en el cual se inscribe la transmisión del mensaje 7. De este modo, a un mismo usuario se le podrán asignar varias direcciones de sustitución distintas cuando se registra en diferentes servidores (o páginas web). Se establece de este modo una correspondencia entre la dirección de sustitución asociada con el usuario y el servicio buscado por el usuario.

Como variante, se podría, por supuesto, considerar asignar la misma dirección de sustitución al usuario 1 independientemente del servidor o la página web en la que el usuario 1 desea registrarse.

Una vez que se ha obtenido la dirección de sustitución, el mensaje 7 se modifica para que la dirección de sustitución reemplace la dirección de correo electrónico real del usuario. Esto se muestra esquemáticamente en la figura 1 mediante la etapa 8, en la que la dirección de correo electrónico A1 del usuario 1 es reemplazada por la dirección de sustitución A2 obtenida previamente.

La dirección de sustitución A2 también se memoriza ventajosamente en correspondencia con la dirección de correo electrónico A1, a fin de establecer un enlace entre la dirección de sustitución A2 y el usuario 1, y ser capaces de este modo de enrutar posteriormente al usuario 1 mensajes que comprenden la dirección de sustitución A2 como la dirección de destino. La memorización se realiza además ventajosamente también en correspondencia con elementos de contexto, tales como la dirección del servidor 3 o de la página web administrada por el servidor 3 en el

que el usuario 1 desea registrarse, por ejemplo.

El mensaje modificado de este modo (mensaje 9) se transmite a continuación al servidor 3. A cambio, se puede transmitir un mensaje de respuesta (no representado). Por lo tanto, el servidor 3 dispone de la solicitud emitida por el usuario 1, pero en la que solo figura la dirección de sustitución relacionada con este usuario, reemplazando a su dirección de correo electrónico real. De este modo, el servidor 3 no tiene conocimiento de la dirección de correo electrónico real del usuario 1. Por lo tanto, se entiende que esta dirección de correo electrónico del usuario 1 no puede ser desviada para enviar a ella mensajes no deseados, es decir, correo basura.

No obstante, el servidor 3 puede transmitir un mensaje 10 a la atención del usuario 1, utilizando su dirección de sustitución. En efecto, la memorización previa de la dirección de sustitución en correspondencia con la dirección de correo electrónico del usuario 1 permite recuperar esta dirección de correo electrónico y, por lo tanto, transmitir al usuario 1, gracias a esta dirección recuperada, el mensaje 10 destinado a él. De este modo, aunque el servidor 3 no conoce la dirección de correo electrónico del usuario 1, puede transmitirle un mensaje 10 utilizando su dirección de sustitución.

De este modo, se entiende que un canal de comunicación está abierto para permitir la transmisión de mensajes desde el servidor 3 al usuario 1. Por supuesto, el usuario 1 siempre puede transmitir mensajes al servidor 3. Cuando estos mensajes emitidos por el usuario 1 contienen la dirección de correo electrónico de este usuario como la dirección de origen, esta se reemplaza ventajosamente por la dirección de sustitución predeterminada antes de la recepción de dichos mensajes en el servidor 3, de modo que este último identifique origen del mensaje transmitido, sin disponer, no obstante, de la dirección de correo electrónico real del usuario 1.

Por lo tanto, se pueden intercambiar mensajes entre el usuario 1 y el servidor 3, sin que se divulgue la dirección de correo electrónico del usuario 1. Además, esta protección de la dirección de correo electrónico del usuario 1 se realiza de manera transparente para este usuario, ya que el reemplazo de la dirección de correo electrónico A1 por una dirección de sustitución A2 se realiza aguas abajo del terminal 2 utilizado por usuario 1. De este modo, el usuario 1 no necesita conocer la dirección de sustitución utilizada en relación con el servidor 3 (o con la página web considerada). Tampoco necesita implementar un mecanismo engorroso para crear, él mismo, una dirección temporal.

De modo ventajoso, se informa al usuario 1 del reemplazo de su dirección de correo electrónico por una dirección de sustitución. Como opción, el usuario 1 podría incluso oponerse a este reemplazo, si desea que su dirección de correo electrónico real sea comunicada al servidor 3.

Puede ser que correo basura sea recibido por el usuario 3 si la dirección de sustitución es utilizada incorrectamente por el propio servidor 3 o por terceros que han tenido acceso a esta información a partir del servidor 3. El usuario 1 tiene entonces la posibilidad de invalidar la dirección de sustitución, de modo que ya no se transmita ningún mensaje que utilice esta dirección de sustitución al usuario 1. De este modo se interrumpe el fenómeno de correo basura proveniente de la dirección de sustitución. Por supuesto, el usuario 1 ya no estará en condiciones de recibir mensajes del servidor 3. Pero esto se puede superar mediante un nuevo registro en este servidor, lo que se traducirá eventualmente en la creación de una nueva dirección de sustitución.

La invalidación de la dirección de sustitución mencionada anteriormente puede asumir varias formas. Comprende ventajosamente una desactivación de la operación que consiste en recuperar la dirección de correo electrónico del usuario 1 memorizada en correspondencia con la dirección de sustitución, cuando se transmite un mensaje 10 con la dirección de sustitución como dirección de destino. Esta desactivación puede resultar, por ejemplo, de la supresión de la correspondencia memorizada entre la dirección de sustitución y la dirección de correo electrónico del usuario, incluso de la supresión de cualquier mención de la dirección de sustitución en la memoria del sistema.

En lo anterior, las operaciones implementadas en el marco de la invención se han descrito de forma general, sin preocuparse por las entidades responsables de esta implementación.

La figura 2 representa, por su parte, un ejemplo de implementación de esta invención. Sin embargo, este modo de realización no es limitativa y, por supuesto, se puede prever otra distribución de roles para la implementación de la invención.

En la figura 2, se encuentra el terminal 2 del usuario 1 por un lado y el servidor web 3 por el otro. El terminal 2 comprende un navegador web 12 capaz de intercambiar solicitudes HTTP con el servidor 3. También comprende un cliente de correo electrónico 13 que coopera con un servidor de correo electrónico 18 para permitir la emisión y recepción de mensajes según una tecnología de correo electrónico clásica.

También se ha representado un sistema 11 en la figura 2 entre el terminal 2 y el servidor 3. Este sistema 11 comprende varios dispositivos que se describirán a continuación.

Al menos algunos de estos dispositivos pueden formar parte de una red de comunicación, tal como una red de

Internet, por medio de la cual el terminal 2 y el servidor 3 pueden comunicarse.

El usuario 1 transmite, a partir de su navegador 12, una solicitud HTTP 20 destinado al servidor web 3. Esta solicitud 20 contiene una dirección de correo electrónico del usuario 1. Puede transmitirse, por ejemplo, a petición del servidor web 3. Esta solicitud puede realizarse en el marco de un registro del usuario 1 en el servidor web 3 o en una página web administrada por este servidor 3. La solicitud 20 puede transmitirse en particular durante la cumplimentación, por el usuario 1, de un formulario proporcionado por el servidor 3.

En la arquitectura ilustrada en la figura 2, la solicitud HTTP 20 emitida por el navegador 12 es interceptada en primer lugar por un enrutador o "conmutador" 14. En la etapa 21, el enrutador 14 redirige la solicitud HTTP a un servidor de caché, también llamado proxy-caché, es decir, un servidor proxy capaz de almacenar y actualizar regularmente páginas web consultadas previamente, a fin de reducir el tiempo de acceso a estas páginas durante una nueva solicitud de consulta.

El proxy-caché 15 analiza entonces la solicitud HTTP recibida. En particular, determina si esta solicitud HTTP es del tipo POST, tal como se define en la especificación técnica RFC 2616 que describe el protocolo HTTP 1.1 y que fue publicada en junio de 1999 por el IETF (Internet Engineering Task Force). En efecto, una solicitud POST es susceptible de contener, en su cuerpo, información proporcionada en un formulario, tal como la dirección de correo electrónico del usuario 1.

Si la solicitud recibida por el proxy-caché 15 es del tipo POST, el proxy-caché puede transmitirla entonces, durante una etapa 22, a un servidor 16 encargado de realizar ciertos procesamientos que se detallarán a continuación. Como variante, el propio proxy-caché 15 podría realizar estos diferentes procesamientos.

De modo ventajoso, el servidor 16 usa el protocolo iCAP (Internet Content Adaptation Protocol) como se describe en particular en la especificación técnica RFC 3507 publicada en abril de 2003 por el IETF. En ese caso, la solicitud POST está encapsulada por el proxy-caché 15 en un flujo iCAP destinado al servidor iCAP 16. Por supuesto, otros protocolos podrían utilizarse como variante.

El servidor iCAP 16 detecta la presencia de una dirección de correo electrónico en el cuerpo de la solicitud recibida. Entonces, posiblemente puede verificar en una base de datos 19, si ya se ha asignado una dirección de sustitución en relación con la dirección de correo electrónico detectada. En efecto, la base de datos 19 memoriza una correspondencia entre cada dirección de correo electrónico y una dirección de sustitución correspondiente que se ha determinado previamente.

Preferentemente, la base de datos 19 almacena además información relacionada con el servidor web, o incluso con la página web, que dio lugar a la creación de dicha dirección de sustitución. De este modo, la base de datos 19 almacena tripletes tales como (dirección de correo electrónico, dirección de sustitución, URL), donde la URL (Uniform Resource Locator) designa la dirección de la página web en la que el usuario 1 se ha registrado previamente. En este último caso, el servidor iCAP 16 permite entonces verificar si ya se ha asignado una dirección de sustitución para el usuario 1 en el mismo contexto, es decir, en relación con la misma URL (etapa 23).

Si el servidor iCAP 16 determina que una dirección de sustitución ya ha sido asignada al usuario 1 preferentemente en el mismo contexto, entonces extrae esta dirección de sustitución de la base de datos 19.

En el caso contrario donde ninguna dirección de sustitución ya se ha asociado con el usuario 1 preferentemente en el mismo contexto, el servidor iCAP 16 genera entonces una dirección de sustitución para este usuario 1. Esta dirección de sustitución es entonces transmitida a la base de datos 19 para ser memorizada en ella en correspondencia con la dirección de correo electrónico del usuario 1, tal como se transmitió en la solicitud 20, y preferentemente también en correspondencia con la URL de la página Web administrada por el servidor web 3, en el que el usuario 1 efectúa un registro (etapa 23).

Una vez obtenida la dirección de sustitución en el servidor iCAP 16, ya sea por extracción de una dirección ya disponible en la base de datos 19, o bien por creación de una nueva dirección, el servidor iCAP 16 reemplaza entonces, en el cuerpo de la solicitud HTTP transmitida desde el navegador web 12, la dirección de correo electrónico del usuario 1 por esta dirección de sustitución. La solicitud modificada de este modo es devuelta por el servidor iCAP 16 al proxy-caché 15 (etapa 24), para poder ser enrutada al servidor web 3 (transmisión 28).

Además, el servidor iCAP 16 informa al servidor de correo electrónico 18 con el que coopera el cliente de correo electrónico 13 del usuario 1, de la determinación de la dirección de sustitución para el usuario 1. El servidor de correo electrónico 18 puede establecer entonces un enlace entre la dirección de correo electrónico real del usuario 1 y dicha dirección de sustitución.

Este enlace o "alias" se puede mantener con ayuda de un puntero que apunta a un campo apropiado de la base de datos 19. Como alternativa, este enlace se puede mantener dentro del propio servidor de correo electrónico 18. En este último caso, el servidor de correo electrónico 18 memoriza entonces la correspondencia entre la dirección de

correo electrónico del usuario 1 y la dirección de sustitución que le ha sido comunicada por el servidor iCAP 16 (etapa 25).

Cabe destacar que el servidor de correo electrónico 18 puede ser administrado a diferentes niveles según las necesidades. Por ejemplo, puede ser un servidor de una empresa a la que pertenece el usuario 1, un proveedor de servicios de Internet al que está suscrito el usuario 1, etc.

De modo ventajoso, el servidor de correo electrónico 18 puede transmitir a continuación un mensaje al cliente de correo electrónico 13 (etapa 26) del usuario 1 para informarle de que la sustitución de dirección se ha realizado. Este mensaje puede contener además información sobre cómo el usuario 1 puede invalidar la dirección de sustitución que se le ha asignado.

De manera clásica, el servidor web 3 puede entonces responder a la solicitud HTTP 20 emitida por el usuario 1, con ayuda de un mensaje de respuesta HTTP (no representado) recibido por el proxy-caché 15 antes de ser enrutado al navegador web 12.

Cabe destacar que las etapas 23 a 25 pueden estar sujetas, cada una o en su conjunto, a una aceptación por parte del usuario 1 (solicitud de confirmación), de modo que este último pueda elegir comunicar al servidor 3 su dirección de correo electrónico real en lugar de una dirección de sustitución.

Al final de las operaciones descritas anteriormente, el servidor web 3 ha recibido, por lo tanto, una solicitud 28 proveniente del usuario 1, pero que contiene una dirección de sustitución como reemplazo de la dirección de correo electrónico real del usuario 1. Por lo tanto, el servidor web 3 no tiene conocimiento de la dirección de correo electrónico real del usuario 1 y, por lo tanto, no puede usarla ni proporcionarla a terceros para transmitir mensajes no deseados al usuario 1, es decir, correo basura.

Por otra parte, se abre entonces un canal de comunicación entre el servidor web 3 y el cliente de correo electrónico 13 por medio del servidor de correo electrónico 18. Este canal de comunicación descendente se denota 27 en la figura 2 y se representa con ayuda de una flecha mixta discontinua. Para comunicarse según este canal 27, el servidor web 3 transmite un mensaje a la atención del usuario 1 utilizando su dirección de sustitución. Este mensaje se recibe en el servidor de correo electrónico 18 que lo analiza y recupera la dirección de correo electrónico del usuario 1 correspondiente a la dirección de sustitución indicada por el servidor 3. El servidor de correo electrónico 18 puede enrutar entonces el mensaje al cliente de correo electrónico 13 del usuario 1 con ayuda de la dirección de correo electrónico recuperada de este modo. Debido a esto, el servidor web 3 puede transmitir normalmente mensajes al usuario 1, sin conocer, no obstante, su dirección de correo electrónico real.

El canal de comunicación 27 también puede utilizarse en sentido ascendente para transmitir mensajes desde el cliente de correo electrónico 13 al servidor web 3, por medio del servidor de correo electrónico 18.

También es posible un mecanismo de invalidación de la dirección de sustitución por iniciativa del usuario 1, en particular para el caso en que el servidor 3 utilizaría o proporcionaría la dirección de sustitución relacionada con el usuario 1 para transmitir a ella correo basura.

La invalidación de la dirección de sustitución puede comprender, por ejemplo, una solicitud del cliente de correo electrónico 13 a la atención del servidor de correo electrónico 18, para que este último suprima el enlace, es decir, el alias, establecido entre la dirección de correo electrónico del usuario 1 y la dirección de sustitución correspondiente.

Si el servidor de correo electrónico 18 conoce este enlace por interrogación de la base de datos 19, la invalidación de la dirección de sustitución puede comprender la ruptura del enlace entre la dirección de correo electrónico del usuario 1 y dicha dirección de sustitución a nivel de esta base de datos 19, por ejemplo, suprimiendo el triplete (dirección de correo electrónico, dirección de sustitución, URL) correspondiente.

La solicitud de invalidación puede ser enviada directamente al servidor de correo electrónico 18 por el cliente de correo electrónico 13. Como variante, esta solicitud puede ser enviada a un servidor web 17 que es responsable de solicitar la invalidación del servidor de correo electrónico. 18. Ventajosamente, el usuario del cliente de correo electrónico 13 conoce la dirección del servidor web 17 después de que se le haya proporcionado un puntero a este servidor 17 con el mensaje 26 mencionado anteriormente. El usuario 1, aunque no tiene acceso a la dirección de sustitución que se le ha asociado, conoce, por lo tanto, la forma de invalidarla.

Cuando la dirección de sustitución ha sido invalidada, el servidor de correo electrónico 18 ya no es capaz de recuperar la dirección de correo electrónico real del usuario 1 al recibir un mensaje destinado a la dirección de sustitución y proveniente por ejemplo del servidor 3 o de un tercero. Debido a esto, el mensaje recibido en el servidor de correo electrónico 18 no se puede enrutar al cliente de correo electrónico 13 del usuario 1. El usuario 1 evita de este modo recibir correo basura vinculado a su registro en el servidor web 3. De este modo, se puede poner fin al fenómeno del correo basura proveniente de una fuente conocida, es decir, por medio de una dirección de sustitución previamente establecida.

Cabe destacar además que, al no ser comunicada la dirección de correo electrónico real del usuario 1 al servidor web 3, por lo tanto, se preserva del fenómeno de correo basura. Esta puede, además, continuar utilizándose normalmente para recibir mensajes de cualquier tercero que haya tenido acceso legítimamente a esta dirección.

Se recuerda que las operaciones descritas anteriormente con referencia a la figura 2 podrían realizarse por un mismo dispositivo o con ayuda de dispositivos distintos de un sistema con una distribución posiblemente diferente de la presentada anteriormente. En particular, al menos algunas de estas operaciones podrían realizarse localmente, a nivel del terminal 2, por ejemplo.

En un modo de realización particular de la invención, al menos algunas de las operaciones descritas anteriormente, por ejemplo las realizadas por el servidor iCAP 16 de la figura 2, podrían efectuarse con ayuda de un programa informático cargado y ejecutado por medios informáticos de un servidor, por ejemplo.

Asimismo, al menos algunas de las operaciones descritas anteriormente con referencia al servidor de correo electrónico 18, en particular aquellas que consisten en recuperar la dirección de correo electrónico del usuario al recibir un mensaje destinado a la dirección de sustitución y en transmitir el mensaje recibido al usuario sobre la base de la dirección de correo electrónico recuperada, podrían efectuarse con ayuda de un programa informático cargado y ejecutado por medios informáticos de un servidor, por ejemplo.

REIVINDICACIONES

1. Procedimiento de protección de una dirección de correo electrónico de un usuario que comprende las siguientes etapas:

- interceptar un mensaje (7:20) enviado por el usuario a un servidor (3), conteniendo dicho mensaje la dirección de correo electrónico del usuario y siendo transmitido en el marco de un procedimiento de registro del usuario en el servidor;
- obtener una dirección de sustitución relacionada con el usuario; y
- transmitir el mensaje (9:28) interceptado al servidor después de reemplazar en él la dirección de correo electrónico del usuario con dicha dirección de sustitución.

2. Procedimiento según la reivindicación 1, que comprende además una memorización de dicha dirección de sustitución en correspondencia con la dirección de correo electrónico del usuario.

3. Procedimiento según la reivindicación 2, que comprende, además, las siguientes etapas, cuando se ha emitido un mensaje destinado a dicha dirección de sustitución:

- recuperar la dirección de correo electrónico del usuario (1) memorizada en correspondencia con dicha dirección de sustitución;
- transmitir al usuario el mensaje destinado a dicha dirección de sustitución, con ayuda de la dirección de correo electrónico recuperada.

4. Procedimiento según la reivindicación 3, en donde, a petición del usuario (1), la etapa que consiste en recuperar la dirección de correo electrónico del usuario memorizada en correspondencia con dicha dirección de sustitución se vuelve inoperante.

5. Sistema adaptado a la implementación del procedimiento de protección de una dirección de correo electrónico de un usuario (1) según una cualquiera de las reivindicaciones 1 a 4, que comprende:

- medios para interceptar un mensaje (7, 20) enviado por el usuario a un servidor (3), conteniendo dicho mensaje la dirección de correo electrónico del usuario y siendo transmitido en el marco de un procedimiento de registro del usuario en el servidor;
- medios para obtener una dirección de sustitución relacionada con el usuario; y
- medios para transmitir el mensaje (9:28) interceptado al servidor después de reemplazar en él la dirección de correo electrónico del usuario con dicha dirección de sustitución.

6. Servidor intermedio (16) adaptado a la implementación del procedimiento de protección de una dirección de correo electrónico de un usuario (1) según una cualquiera de las reivindicaciones 1 a 4, que comprende:

- medios para interceptar un mensaje (20) enviado por el usuario a un servidor (3), conteniendo dicho mensaje la dirección de correo electrónico del usuario y siendo transmitido en el marco de un procedimiento de registro del usuario en el servidor;
- medios para obtener una dirección de sustitución relacionada con el usuario;
- medios para reemplazar, en el mensaje recibido, la dirección de correo electrónico del usuario con dicha dirección de sustitución; y
- medios para entregar el mensaje interceptado, después de dicho reemplazo, para su transmisión al servidor.

7. Producto de programa informático que comprende instrucciones de código para implementar las siguientes etapas, cuando se carga y se ejecuta por medios informáticos de un servidor intermedio (16):

- interceptar un mensaje enviado por un usuario (1) a un servidor (3), conteniendo dicho mensaje la dirección de correo electrónico del usuario y siendo transmitido en el marco de un procedimiento de registro del usuario en el servidor;
- obtener una dirección de sustitución relacionada con el usuario;
- reemplazar, en el mensaje recibido, la dirección de correo electrónico del usuario con dicha dirección de sustitución; y
- entregar el mensaje interceptado, después de dicho reemplazo, para su transmisión al servidor (3).

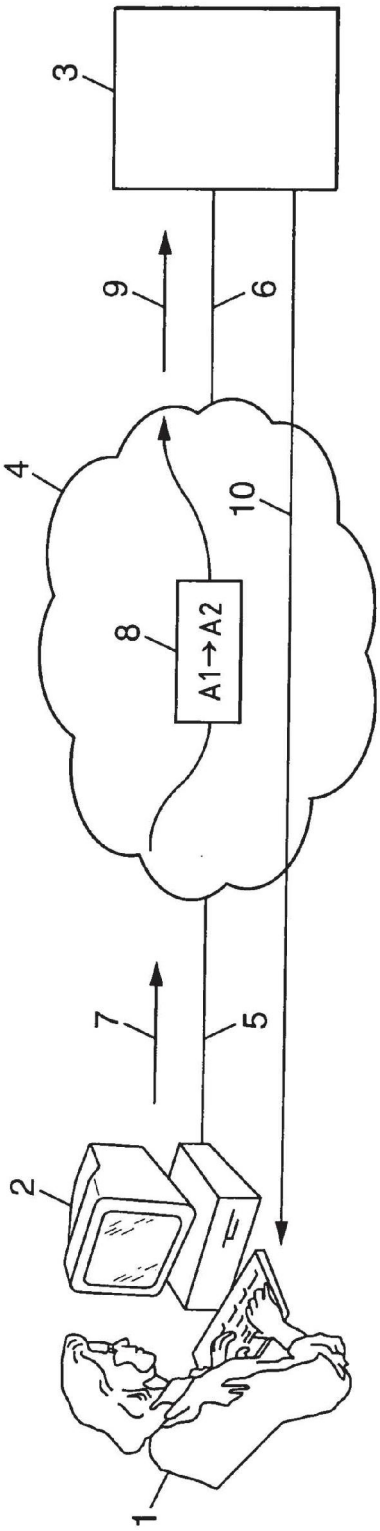

FIG. 1

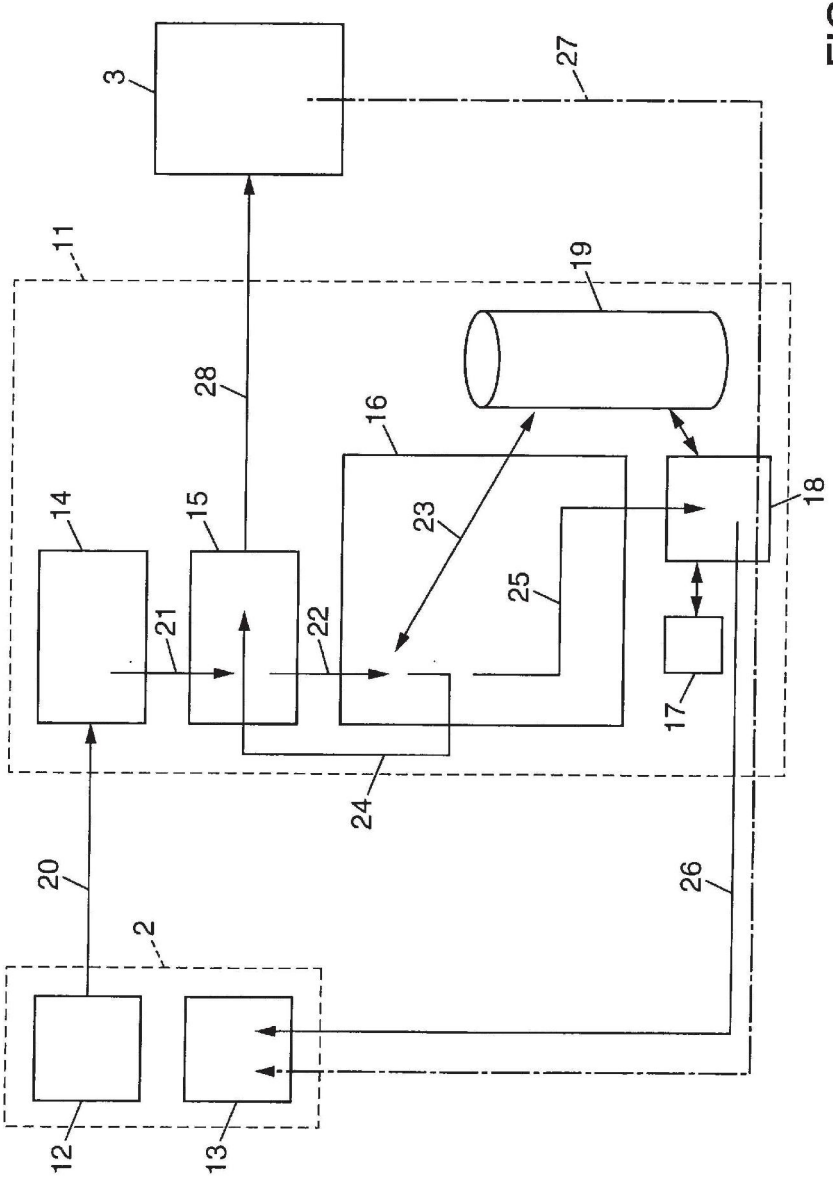

FIG. 2