(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 484 141**

(51) Int. CI.:

H04W 12/12 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.04.2010 E 10717601 (8)**

(97) Fecha y número de publicación de la concesión europea: **23.04.2014 EP 2425647**

(54) Título: **Gestión de solicitudes de servicio no deseadas en una red**

(30) Prioridad:

27.04.2009 EP 09005814

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.08.2014

(73) Titular/es:

KONINKLIJKE KPN N.V. (50.0%)
Maanplein 55
2516 CK The Hague, NL y
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST -NATUURWETENSCHAPPELIJK ONDERZOEK TNO (50.0%)

(72) Inventor/es:

LAARAKKERS, JEROEN;
MULLER, FRANK y
HARTOG, TIM

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Gestión de solicitudes de servicio no deseadas en una red

Campo de la invención

La invención se refiere a la gestión de solicitudes de servicio no deseadas en una red y, en particular, aunque no exclusivamente, a un método y un sistema para gestionar solicitudes de servicio no deseadas en una red, a una función de verificación de usuario, a un terminal que se usará en un sistema de este tipo y a un producto de programa informático para ejecutar el método.

Antecedentes de la invención

Los dispositivos móviles de nueva generación, tales como los teléfonos inteligentes, proporcionan funcionalidades computacionales mejoradas mediante conexiones de red abiertas. Tales dispositivos móviles pueden, por ejemplo, recibir correo electrónico, compartir software entre sí a través de conexiones de corto alcance, descargar y ejecutar software desde Internet, hacer llamadas automáticas y funcionar mediante control remoto. Por tanto, de manera similar a un ordenador personal, los dispositivos móviles, y en particular los componentes de software involucrados en el establecimiento de una conexión entre el dispositivo móvil y la red, son vulnerables a ataques por parte de código malicioso (*malware*). Normalmente, el *malware* intenta conseguir un uso indebido de un dispositivo móvil o simplemente interferir en el uso legítimo de un dispositivo móvil. Una tarjeta de chip que posiblemente esté presente en el dispositivo móvil, por ejemplo un (U)SIM, no ofrece protección contra esta vulnerabilidad.

Un tipo de *malware* se denomina marcador. Los marcadores son elementos de código malicioso que pueden establecer llamadas de manera ilegal en el dispositivo móvil infectado. Tales marcadores usan habitualmente información de autenticación del (U)SIM del dispositivo móvil para obtener acceso a la red como si la conexión fuera establecida legítimamente por el usuario móvil. Tras el procedimiento de autenticación, el marcador empieza a realizar llamadas a, por ejemplo, números de tarificación especial caros (normalmente no detectados por el usuario del dispositivo móvil infectado), dando lugar a importantes riesgos financieros tanto para el usuario móvil como para el operador móvil.

Se han tomado medidas para eliminar o al menos reducir los efectos no deseados de este tipo de *malware*. Una medida conocida es la introducción de un filtro en la red. Tales filtros se describen en los documentos WO 2007/041157 y US 2005/0060399. Un filtro que reside en una estación base supervisa las llamadas transmitidas desde un dispositivo móvil y bloquea llamadas que están presentes en una lista negra. El operador de red y/o el usuario móvil pueden añadir solicitudes de servicio a la lista negra, las cuales deberían ser excluidas explícitamente por el filtro.

Un problema relacionado con el uso de este tipo de filtro es la gestión de la lista de solicitudes de servicio excluidas. En el lado del operador hay tres problemas. El primero es que para bloquear todas las solicitudes de servicio no deseadas, el tamaño de la lista negra necesaria puede llegar a ser muy grande y prácticamente inmanejable. El segundo problema es que se requiere una búsqueda constante de servicios maliciosos para mantener la lista negra actualizada. El tercer problema es que la identificación de solicitudes sospechosas requiere analizar las solicitudes de servicio de cada usuario individual de dispositivo móvil. Por tanto, tales análisis requieren una gran cantidad de recursos en la red. En el lado del usuario móvil, un problema reside en el hecho de que las solicitudes de servicio no deseadas del dispositivo móvil pasan normalmente desapercibidas por el usuario y solo se detectan tras la facturación, es decir, después de que el daño ya esté hecho. Otro problema para el usuario puede ser que el operador incluya en la lista negra servicios que el usuario desee usar.

El documento US 2008/0196099 da a conocer un método de filtrado de URL (localizadores uniformes de recursos) en aplicaciones IM (mensajería instantánea). En caso de que un mensaje IM contenga un URL, este URL se comprueba con una lista negra de URL conocidos maliciosos. Si el URL no está en la lista negra se presenta al emisor un desafío para confirmar que el emisor es un usuario real y no un programa (*malware*). Este método protege a los destinatarios contra la recepción de mensajes IM con URL maliciosos. Además, el sistema puede configurarse para mantener una “lista de permitidos” o “lista blanca” de URL conocidos no maliciosos. De esta manera, un mensaje IM que contiene un URL de la “lista blanca” puede reenviarse al destinatario sin presentar un desafío al emisor.

Este método no es deseable ni desde el punto de vista de la seguridad ni desde el punto de vista de los usuarios cuando se aplica en el contexto de un teléfono móvil. Desde la perspectiva de la seguridad, el método del documento US 2008/0196099 no ofrece ninguna solución al problema en cuestión ya que no es el contenido de la comunicación lo que supone una amenaza, sino el destino de la comunicación, por ejemplo números de tarifa especial para llamadas o mensajes de texto (SMS). Por lo tanto, el método descrito trata de proteger al destinatario pero no al emisor. Además, este método supone una molestia para el emisor, ya que el emisor recibirá desafíos por cada mensaje IM que contenga un URL que no esté en la lista negra (o lista blanca). Cuando el emisor responde (con éxito) al desafío, el mensaje IM que incluye el URL se reenviará, pero la lista blanca no se actualiza conforme a

la acción del emisor. Esto significa que el emisor recibirá un desafío para el mismo URL una y otra vez.

Los problemas de la técnica anterior pueden resumirse de la siguiente forma:

- el tamaño de la lista negra puede llegar a ser inmanejable, ya que todos los servicios sospechosos deben introducirse en la lista negra;
- las listas blancas no se generan automáticamente;
- la detección de *malware* no incluye una prueba en el servicio particular;
- no se rechazan solicitudes de servicio relacionadas con nuevos destinos maliciosos, por lo que se requiere un esfuerzo constante por parte del operador de red o del usuario para mantener actualizada la lista negra;
- se importuna múltiples veces al usuario cuando lleva a cabo solicitudes de servicio idénticas;
- existe la posibilidad de que un operador de red incluya en la lista negra servicios que un usuario desea usar.

Por tanto, existe la necesidad en la técnica de un método sencillo que gestione de manera eficaz solicitudes de servicio no deseadas y que evite el uso indebido.

Sumario de la invención

La invención está definida por las reivindicaciones independientes.

Un objeto de la invención es reducir o eliminar al menos uno de los inconvenientes conocidos de la técnica anterior y proporcionar en un primer aspecto de la invención un método y un sistema para gestionar solicitudes de servicio no deseadas enviadas desde al menos un terminal (dispositivo de comunicaciones móviles) a una red, donde la red puede comprender un nodo de red para almacenar información de servicios de confianza. El método puede comprender al menos una de las siguientes etapas: recibir, a través de la red, una solicitud de servicio procedente de un terminal, comprendiendo la solicitud información de solicitud de servicio; y/o enviar, preferentemente a través de un canal de comunicación seguro, una solicitud de verificación de usuario para solicitar al usuario que verifique el servicio solicitado por el terminal si al menos parte de la información de solicitud de servicio no está presente en la información de servicios de confianza. La información de servicios de confianza contiene al menos uno de entre el tipo de servicio (SMS, MMS, llamada, mensajería instantánea, vídeo, etc.) y el destino (por ejemplo, la dirección, el número de teléfono) del servicio solicitado, y si el tipo y/o el destino están permitidos o no. En una realización de la invención, la información de servicios de confianza incluidos se rellena con las solicitudes subsiguientes, posiblemente complementada mediante la introducción independiente de información de servicios de confianza. En otra realización de la invención, la lista con la información de servicios de confianza se rellena introduciendo de manera independiente la información de servicios de confianza. El usuario puede ser un usuario que esté usando en un momento dado el terminal o un usuario que sea dueño del terminal o al que se le haya asignado la tarea de ejecutar la verificación de la solicitud de servicio.

El método y sistema impiden de manera eficaz el daño causado por un *malware* al verificar con el usuario si la solicitud de servicio en cuestión es una solicitud legítima. Este efecto se consigue manteniendo dinámicamente una información de servicios de confianza (por ejemplo, en forma de una lista blanca) de servicios permitidos en la red y verificando para cada solicitud de servicio que el servicio está incluido en la información de servicios de confianza antes de permitir el servicio. Cuando el servicio no está incluido, la red solicitará dinámicamente al usuario, de manera segura, que verifique si debe establecerse la solicitud. Mediante este método, el usuario puede reconocer las solicitudes que origina un *malware* y el usuario puede rechazar el establecimiento de tales servicios.

En una realización, el método comprende además al menos una de las siguientes etapas: recibir, preferentemente a través de un canal de comunicación seguro, una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario, indicando la información de verificación si el usuario acepta o rechaza la solicitud de servicio; y/o añadir al menos parte de la información de solicitud de servicio a la información de servicios de confianza si la información de verificación proporciona una indicación de que se permite el servicio solicitado. La red establece por tanto automáticamente un diálogo con el usuario para la verificación del servicio. Si el usuario permite el servicio, la información de servicios de confianza se actualiza dinámicamente.

En otra realización, el método puede comprender además al menos una de las siguientes etapas: establecer un canal de comunicación cifrado, usando preferentemente una clave segura almacenada en un módulo de identidad del terminal, entre dicho terminal y dicha red; enviar al terminal la solicitud de verificación de usuario a través de dicho canal de comunicación cifrado; y/o recibir a través del canal de comunicación cifrado una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario que indica si el usuario acepta o rechaza la solicitud de servicio. El diálogo de usuario puede establecerse usando un

canal de comunicación cifrado usando la clave privada almacenada en el módulo de identidad del terminal.

En otra realización adicional, el terminal puede comprender al menos uno de los siguientes elementos: un módulo de identidad, una o más interfaces de entrada/salida y/o al menos un componente de hardware de confianza. Dicho componente de hardware de confianza puede configurarse para establecer una o más trayectorias de comunicación de confianza entre dicho componente de hardware de confianza y el módulo de identidad y/o la una o más interfaces de entrada/salida. Usando uno o más componentes de hardware de confianza en el terminal puede conseguirse una o más trayectorias de comunicación de confianza en el terminal, impidiendo así que un *malware* interfiera en el diálogo de verificación de usuario entre el usuario y la red.

En una variante, el método puede comprender además al menos una de las siguientes etapas: establecer un canal de comunicación adicional diferente del canal de comunicación a través del cual la red recibe la solicitud de servicio; enviar al terminal la solicitud de verificación de usuario a través del canal seguro; y/o recibir a través del canal de comunicación adicional una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación que indica si el abonado permite o rechaza la solicitud de servicio. En otra variante adicional, el canal de comunicación adicional puede ser proporcionado por un servicio de mensajería, preferentemente un servicio de mensajes cortos o un servicio USSD.

En una variante adicional, la solicitud de verificación puede comprender una prueba configurada para determinar si el usuario es una persona o no, preferentemente una prueba de Turing inversa, más preferentemente un *Captcha*, y donde la respuesta de verificación comprende información que indica si la prueba tuvo éxito o no.

En otra variante adicional, la red puede comprender al menos un nodo de red de provisión de servicios. Dicho nodo de red de provisión de servicios puede comprender un registro de posiciones de visitantes (VLR) que comprende información de servicios de confianza. Dicho nodo de red puede comprender además una función de verificación de usuario para enviar al terminal, en respuesta a una solicitud de servicio procedente de un terminal, una solicitud de verificación de usuario si al menos parte de la información de solicitud de servicio no está incluida en la información de servicios de confianza. En una variante, la red puede comprender un registro de posiciones base (HLR), donde dicho registro de posiciones base comprende información de servicios de confianza de dicho terminal. El método puede comprender además la etapa de transmitir información de servicios de confianza desde dicho registro de posiciones base a dicho registro de posiciones de visitantes. Tras el registro de un terminal en la red, el VLR del nodo de red de provisión de servicios que da servicio al terminal puede recuperar la información de servicios de confianza del registro de posiciones base HLR de la red local del terminal. Asimismo, la información de servicios de confianza del HLR puede actualizarse transmitiendo al HLR servicios de confianza verificados por el usuario y añadidos a la información de servicios de confianza del VLR.

En otro aspecto, la invención puede referirse a un sistema para gestionar solicitudes de servicio no deseadas enviadas desde al menos un terminal a una red. El sistema puede comprender al menos una de las siguientes características: uno o más terminales para establecer un canal de comunicación con la red; un nodo de red de provisión de servicios configurado para recibir una solicitud de servicio, que comprende información de solicitud de servicio, procedente de al menos uno de dichos terminales, y/o una base de datos de servicios de confianza conectada a dicho nodo de red de provisión de servicios; en el que dicho nodo de red de provisión de servicios está configurado para enviar, preferentemente a través de un canal de comunicación seguro, una solicitud de verificación de usuario para solicitar al usuario que verifique el servicio solicitado por el terminal si al menos parte de la información de solicitud de servicio no está incluida en la información de servicios de confianza.

En un aspecto adicional, la invención puede referirse a una función de verificación de usuario para su uso en un sistema como el descrito anteriormente, donde la función de verificación de usuario puede comprender al menos una de las siguientes características: medios para recibir una solicitud de servicio procedente de un terminal, comprendiendo dicha solicitud de servicio información de solicitud de servicio; medios para comprobar si al menos parte de dicha información de solicitud de servicio está comprendida en una base de datos de servicios de confianza; y/o medios para establecer un diálogo seguro entre el usuario del terminal y la red si al menos parte de la información de solicitud de servicio no está incluida en la información de servicios de confianza.

En otro aspecto adicional, la invención puede referirse a un terminal para su uso en un sistema como el descrito anteriormente. El terminal puede comprender al menos una de las siguientes características: un cliente de verificación de usuario para establecer, en respuesta a una solicitud de verificación de usuario procedente del nodo de red de provisión de servicios, un diálogo seguro entre el usuario del terminal y la red; un módulo de identidad para proporcionar una clave privada para establecer un canal de comunicación seguro para dicho diálogo; un elemento de entrada para recibir información de diálogo del usuario; un elemento de salida para transmitir información de diálogo al usuario; y/o un componente de hardware de confianza para establecer, usando preferentemente una norma informática de confianza, una o más trayectorias de comunicación de confianza entre dicho cliente de verificación de usuario, módulo de identidad, elemento de entrada y/o elemento de salida.

La invención también puede referirse a un producto de programa informático que comprende fragmentos de código de software configurados para, cuando se ejecutan en la memoria de un ordenador, preferentemente un ordenador

ubicado en uno o más nodos de red, ejecutar las etapas de método según cualquiera de las reivindicaciones de método descritas anteriormente.

La invención se ilustrará en mayor detalle con referencia a los dibujos adjuntos, que muestran de manera esquemática realizaciones según la invención. Debe entenderse que la invención no está limitada de ninguna manera a estas realizaciones específicas.

Breve descripción de los dibujos

La figura 1 muestra una representación esquemática de un sistema de comunicaciones según una realización de la invención.

La figura 2 muestra un diagrama de flujo de un método según una realización de la invención.

La figura 3 muestra un terminal para su uso con un método según una realización de la invención.

Descripción detallada

La figura 1 ilustra una representación esquemática de un sistema de comunicaciones 100 según una realización de la invención. El sistema puede comprender un terminal 102 conectado a una red de comunicaciones 104. En una realización, la red puede ser una red móvil de tipo 2G (por ejemplo, GSM) que comprende una estación transceptora base (BTS) 106 que sirve como un nodo de acceso. La BTS puede conectarse, a través de un controlador de estación base (BSC) 108, a un centro de conmutación móvil (MSC) 110 de, por ejemplo, una red visitante (VN). Además, el MSC puede estar conectado a registro de posiciones de visitantes (VLR) 112, que es una base de datos que almacena datos relacionados con los usuarios y que lleva a cabo funciones de seguridad. El MSC puede estar conectado además al registro de posiciones base (HRL) 114, que comprende un centro de autenticación (AuC) 116. El HLR/AUC puede estar ubicado en la red local (HN), donde el usuario del terminal 102 tiene una suscripción con el operador de red. El HLR almacena datos relacionados con los usuarios, por ejemplo datos relacionados con suscripciones, y actúa conjuntamente con el MSC/VLR 110 para mantener un seguimiento de la ubicación del terminal. El centro de autenticación (AuC) comprende (entre otras cosas) algoritmos para el cálculo de parámetros de autenticación usados en el procedimiento de autenticación. Para cada abonado, el AuC almacena una clave de autenticación secreta K que también está almacenada en un módulo de identidad asociado, por ejemplo una tarjeta (U)SIM o similar, ubicado en el terminal.

Una base de datos de servicios de confianza (TS) 118 que comprende información de servicios de confianza, por ejemplo una o más listas de confianza de identificadores de servicio permitidos y/o no permitidos (por ejemplo, números de teléfono) asociados a un abonado, puede estar conectada a o ser parte del HLR. La lista de la base de datos TS puede ser actualizada por el HLR del abonado y/o por la función de verificación de servicio 120. La función de verificación de servicio está configurada para acceder a la base de datos TS y para establecer, en respuesta a una solicitud de servicio procedente del terminal, un canal de comunicación seguro con el terminal de usuario.

La función de verificación de servicio puede implementarse en forma de un componente de hardware funcional o como un producto de programa informático ejecutado en el MSC u otro elemento de red diferente conectado al MSC. Como alternativa, la función puede ser una función distribuida que requiere dos o más elementos de red que comprenden uno o más productos de programa de software, que cuando se ejecutan proporcionan la funcionalidad de verificación de llamada. Una explicación más detallada de la función de verificación de llamada se proporcionará posteriormente en relación con la figura 2.

Otras redes diferentes a una red GSM, como la ilustrada en la figura 1, pueden usarse. Por ejemplo, en una realización, la red puede ser una red móvil de tipo 3G (UMTS) que comprende elementos de red 3G. En ese caso, la red puede comprender una estación base de radio (RBS) 106 conectada, a través de un controlador de red de radio (RNC) 108, a un nodo de soporte GPRS de servicio (SGSN) 110. El SGSN está conectado además a un VLR 112 y a un AuC/HLR 114, 116 de manera similar a la red de tipo 2G descrita anteriormente. En una realización adicional, la red de comunicaciones 104 puede comprender elementos de red basados en IMS en forma de un conjunto de funciones de control de llamadas/sesiones (CSCF), tal como una CSCF de *proxy* (P-CSCF), una CSCF de interrogación (I-CSCF), una CSCF de servicio (S-CSCF) y un servidor de abonado local (HSS). Variantes adicionales incluyen elementos de red LTE 3GPP o SAE 3GPP.

El terminal 102 puede ser un ordenador personal o un dispositivo móvil, tal como un teléfono inteligente, un asistente digital personal (PDA), un ordenador portátil o cualquier otro dispositivo de comunicaciones móviles que pueda proporcionar servicios a través de una o más redes móviles (2G, 2.5G, 3G, 4G, NG, WiMax, etc.). El terminal comprende un módulo de radio 122, un sistema operativo (OS) 124 y un módulo de identidad 120.

El módulo de radio 122 actúa como punto de conexión hacia servicios de red inalámbricos y comprende para tal fin al menos una interfaz aérea que comprende un receptor de RF conectado a una o más antenas. La figura 1 muestra una implementación a modo de ejemplo en la que la tarjeta de radio 122 proporciona contacto por radio con la

estación base 106. La interfaz de RF del módulo de radio puede recibir y/o transmitir señales de RF según varias tecnologías inalámbricas (por ejemplo, TDMA para servicios GSM, W-CDMA para servicios UMTS, IEEE 802.11 usada para servicios WiFi, *Bluetooth*, DECT, etc.).

El sistema operativo (OS) 124 del terminal puede comprender un núcleo (*kernel*) que gestiona los recursos del dispositivo móvil, por ejemplo, la unidad central de procesamiento (CPU), una memoria para almacenar instrucciones de programa 130 y datos, y dispositivos de entrada/salida (E/S) tales como el módulo de radio 122, un dispositivo de visualización 134 y un teclado 132. Además, el OS comprende habitualmente una o más interfaces de programación de aplicaciones (API) a través de las cuales programas de aplicación 128 pueden acceder a servicios ofrecidos por el OS, por ejemplo una API de red de radio para establecer una conexión de radio con una red móvil.

El módulo de identidad 126, que normalmente puede extraerse, puede ser una UICC (tarjeta de circuito integrado universal) para su uso en dispositivos móviles adecuados para servicios de red de tipo 2G (GSM) o servicios de red de tipo 3G (UMTS). Para ese fin, la UICC puede comprender un módulo de identidad de abonado (SIM), que comprende aplicaciones SIM, y/o un módulo de identidad de abonado UMTS (USIM), que comprende aplicaciones USIM. Debe entenderse que el módulo de identidad no está limitado a aplicaciones SIM y/o USIM. En realizaciones adicionales, el módulo de identidad puede ser un SIM de subsistema multimedia IP (ISIM) para la autenticación y el acceso a servicios basados en IMS según una AKA basada en IMS predeterminada como, por ejemplo, la descrita en la especificación técnica TS 33.203 del ETSI, o un SIM basado en un protocolo de autenticación extensible (EAP) para la autenticación y el acceso a una red según una AKA basada en EAP predeterminada como la descrita, por ejemplo, en la especificación RFC4187.

El módulo de identidad puede comprender un procesador, uno o más componentes de memoria, por ejemplo, una ROM, una RAM y/o una EEPROM y/o un circuito de E/S. Con fines de autenticación, la UICC comprende una clave secreta K de autenticación de servicio-abonado y uno o más algoritmos para calcular una respuesta que comprende uno o más parámetros de autenticación tras la recepción de un desafío aleatorio.

Para acceder a la red, el terminal lleva a cabo en primer lugar un procedimiento de autenticación como el definido por una de las disposiciones de autenticación y clave (AKA) de la norma de telecomunicaciones usada por la red. La AKA GSM es un procedimiento de autenticación de tipo desafío-respuesta que implica enviar un número aleatorio RAND al SIM del terminal. El SIM genera una respuesta RES que se envía a la red, la cual compara la respuesta con una respuesta esperada calculada por la red. Como parte de la AKA GSM, se establece una clave de cifrado simétrica CK entre el terminal móvil y la red de servicio para cifrar datos a través de la interfaz aérea GSM. La AKA GSM se describe en detalle en las normas GSM 02.09 y GSM 03.20 del ETSI, las cuales se incorporan en este documento mediante referencia.

En el procedimiento de autenticación UMTS estándar se llevan a cabo etapas similares a las de la AKA GSM. Sin embargo, con el fin de mejorar la seguridad, la red también se autentica a sí misma con respecto al terminal. En el esquema UMTS, el AuC/HLR genera un número aleatorio RAND y determina un vector de autenticación (AV) {AUTN, RAND, XRES, CK, IK}. Posteriormente, el SGSN/VLR reenvía el RAND y el AUTN al terminal. El USIM del terminal determina, basándose en el RAND y el AUTN, una respuesta RES, la cual se envía posteriormente a la red y se compara con una respuesta esperada determinada por la red. De manera similar a la AKA GSM, una clave de cifrado CK y una clave de integridad IK se establecen durante la AKA UMTS, las cuales se usan para el cifrado y la protección de la integridad de los datos enviados a través de la interfaz aérea entre el terminal móvil y la red de servicio. La AKA UMTS se describe en detalle en la especificación técnica TS 33.102 del ETSI, la cual se incorpora en este documento mediante referencia.

La figura 2 ilustra un diagrama de flujo del establecimiento de una llamada de origen en una red GSM según una realización de la invención. Durante el proceso de autenticación descrito anteriormente, datos de registro de abonado, incluyendo la identidad del abonado (IMSI), datos de autenticación, el número de teléfono del abonado, una lista de servicios permitidos, la dirección HLR del abonado e información de servicios de confianza, que comprende, entre otras cosas, una lista blanca y/o una lista negra, pueden transferirse desde el HLR al MSC/VLR (etapa 202). Tras una autenticación con éxito, el terminal puede acceder a un servicio de red enviando al MSC/VLR, a través de la BSS, una solicitud de servicio, por ejemplo una solicitud para establecer una llamada que comprende el número de red digital de servicios integrados del abonado móvil (MSISDN) (etapa 204).

En respuesta, el MSC comprueba con el VLR si el terminal tiene permiso para acceder al servicio solicitado. Además, la función de verificación de servicio del MSC comprueba si la información de la solicitud de servicio, en particular el MSISDN, está presente en la información de servicios de confianza (por ejemplo, en forma de una lista de números de teléfono de confianza). La lista puede comprobarse accediendo al VLR conectado al MSC (etapas 206 y 208). Si se encuentra una correspondencia, el MSC solicita a la BSS que asigne recursos para la llamada y que encamine la llamada hacia el destinatario (no mostrado), a través del GMSC, una pasarela que conecta la red móvil con una red PSTN fija.

Si el número no está presente en la lista de números permitidos, la función de verificación de servicio MSC puede iniciar un diálogo con el terminal de origen para solicitar al usuario del terminal que verifique si la llamada puede

permitirse o no. Para ello, puede establecerse un canal de comunicación seguro entre el terminal y la red, el cual es robusto frente a los ataques de un *malware*. Ejemplos de tales canales de comunicación seguros se describirán posteriormente en mayor detalle.

Usando un canal de comunicación seguro, la función de verificación de servicio del MSC/VLR puede enviar una solicitud de verificación de usuario al terminal de usuario. La solicitud de verificación de usuario puede iniciar un diálogo con el usuario del terminal en el que se pide al usuario que verifique si hay que establecer o no el servicio solicitado (etapa 210). En respuesta a la solicitud de verificación de usuario, un mensaje de respuesta de usuario se envía a la función de verificación de servicio del MSC (etapa 212). Si la respuesta de usuario indica que el usuario ha aceptado la llamada, la lista de servicios de confianza se actualiza añadiendo el número a la información de servicios de confianza de la base de datos TS (etapas 214 y 216). Tras el diálogo de verificación de llamada con el usuario, el MSC asigna recursos para el servicio solicitado, por ejemplo una llamada, y encima la solicitud de servicio hacia el terminal llamado a través del GMSC y una o más redes de comunicaciones, por ejemplo la red telefónica pública conmutada (PSTN) (etapa 218). Si el mensaje de respuesta indica que el usuario no acepta la llamada, el MSC (no mostrado) rechaza la llamada.

Por tanto, a diferencia del establecimiento convencional de una llamada de origen, la invención ofrece un control estricto sobre el servicio enviado por el terminal a la red al comprobar si la información de la solicitud de servicio está presente en una lista blanca. Usando la lista blanca puede bloquearse de manera eficaz solicitudes de servicio de origen generadas por un *malware*. Además, la invención permite que la lista blanca se genere de manera interactiva y dinámica. Una vez que la lista ha alcanzado un determinado tamaño, el uso de lista blanca generada por la característica de verificación de llamadas da como resultado que los operarios de la red sepan con mayor seguridad que las llamadas registradas son realmente llamadas legítimas.

El canal de comunicación entre el terminal y la red debe ser seguro en el sentido de que no permita que un *malware* interfiera. En una realización, el canal de comunicación seguro puede ser un canal de radio cifrado que usa la clave de cifrado CK establecida entre el terminal móvil y la red de servicio durante el procedimiento de autenticación conforme a la AKA GSM o la AKA UMTS. En este esquema, el MSC/VLR puede enviar una solicitud de verificación de usuario cifrada 210 a un terminal puede modificarse para impedir que un *malware* interfiera en el diálogo entre el usuario y la red. Una realización a modo de ejemplo de un terminal 300 de este tipo se muestra en mayor detalle en la figura 3. En esta realización, el terminal comprende una aplicación de verificación de usuario 302 (cliente) que se ejecuta en el OS 304 del terminal. El terminal comprende además uno o más componentes de hardware de confianza 306 (THC) para establecer una o más trayectorias de comunicación de confianza 308 a 316 entre el cliente de verificación de usuario 302, un módulo de identidad 318 (por ejemplo, (U)SIM), una memoria 320 y/o una o más interfaces de E/S, tales como un elemento de entrada 322 (teclado, micrófono, etc.) y un elemento de salida 324 (dispositivo de visualización, altavoz, etc.).

La solicitud de verificación de usuario puede iniciar la ejecución del cliente de verificación de usuario, que está configurado para comunicarse de manera segura con el (U)SIM para el cifrado y descifrado de datos y con el teclado y las interfaces de visualización 322, 324 del terminal para la interacción con el usuario.

El THC puede ser un dispositivo resistente a las manipulaciones indebidas configurado para llevar a cabo múltiples funciones de seguridad, incluyendo una ratificación local y/o remota, un almacenamiento de datos seguro y funciones de E/S seguras. Estas funciones pueden usarse para establecer trayectorias de comunicación de confianza en el terminal. El THC puede implementarse según una norma de plataforma informática de confianza predefinida, por ejemplo la plataforma informática de confianza (TCP) definida en la especificación “Módulo De confianza Móvil (MTM)”, versión 1.0, rev. 1, 12 de junio de 2007, publicada por Trusted Computer Group (TCG) o la plataforma de hardware Tecnología de Ejecución de Confianza (TXT) de Intel.

El THC puede verificar la integridad del cliente de verificación de usuario usando la función de ratificación local y/o remota. Tras haberse aprobado la integridad, el THC puede establecer una o más trayectorias de comunicación de confianza en el terminal, como se muestra en la figura 3. Usando estas trayectorias de confianza, la aplicación de verificación de usuario establece un diálogo seguro con el usuario, permitiendo al usuario aceptar o rechazar la solicitud de servicio. La respuesta del usuario (es decir, datos introducidos con el teclado) se envía, a través de la interfaz de radio 326 y el canal de radio cifrado, a la función de verificación de servicio del MSC/VLR.

En otra realización, el canal de comunicación puede establecerse usando una tarjeta SIM adicional, que está registrada en la red. Tal terminal de doble SIM permite que la solicitud de servicio se envíe a la red usando un canal establecido según el primer SIM y que la respuesta del usuario a un cuadro de diálogo para la aceptación o el rechazo de una solicitud de servicio se envíe a través de un canal de comunicación cifrado usando el segundo SIM. Esta realización se basa en que el *malware* no tiene constancia de una segunda tarjeta SIM y, por tanto, ofrece menos seguridad en comparación con el uso de un canal de comunicación cifrado en combinación con un THC.

En otra realización, el canal seguro puede establecerse como un canal de comunicación diferente en la misma infraestructura. Por ejemplo, en respuesta a la recepción de una solicitud de servicio procedente de un terminal, la red envía un mensaje, por ejemplo en forma de un mensaje SMS, EMS, MMS o USSD, al usuario del terminal y el

usuario envía la respuesta a la red usando el mismo canal de comunicación diferente.

En una variante adicional, el diálogo de validación de servicio entre el terminal y la red puede comprender la etapa de enviar una prueba, preferentemente basada en texto, gráficos y/o sonido, que permita determinar si el usuario es una persona o no. La respuesta a la prueba se envía a la red, donde una respuesta correcta corresponde a la aceptación de la solicitud de servicio por parte del usuario del terminal. Preferentemente, la prueba es una prueba de Turing inversa (por ejemplo, un *Captcha* o similar). Una prueba de Turing inversa puede permitir que el diálogo tenga lugar usando una infraestructura habitual y posiblemente insegura. Sin embargo, para una mayor seguridad, el diálogo que usa la prueba de Turing inversa puede combinarse fácilmente con un canal de comunicación cifrado y/o diferente, como se ha descrito anteriormente.

La funcionalidad de la base de datos de servicios de confianza (TS) puede mejorarse incluyendo una lista adicional de números no deseados (es decir, una lista negra). Cuando la red, por ejemplo el MSC, recibe una solicitud de servicio, comprobará si el número marcado en la solicitud está presente en la lista negra o en la lista blanca. Si está presente en la lista negra, la llamada puede rechazarse automáticamente sin ningún diálogo adicional con el terminal. La lista negra puede actualizarse de manera similar a lo descrito anteriormente en relación con la lista de servicios de confianza (una lista blanca).

En una realización, después de que el usuario haya rechazado la solicitud de servicio, el número puede añadirse a la lista negra. Esto puede realizarse automáticamente en respuesta al rechazo del usuario o, como alternativa, esto puede presentarse en un cuadro de diálogo como una opción para el usuario durante el diálogo de validación de llamada. Seleccionar la opción de la lista negra dará como resultado que la lista negra se actualice en la base de datos TS con el rechazo. Tal actualización de la lista negra y/o de la lista blanca puede tener lugar cuando se produce la comunicación entre el MSC/VLR y el HLR, por ejemplo en el momento en que un MSC/VLR informa al HLR de que un abonado está en el área cubierta por el VLR, tras un periodo de tiempo predeterminado de inactividad del abonado, tras lo cual el terminal cancelará su registro en el MSC/VLR de servicio. Además, tal actualización puede ser en tiempo real, es decir, inmediatamente después del diálogo de verificación de usuario o en el momento en que el registro de abonado se borra del VLR.

Además, el operador de red puede proporcionar al usuario acceso (indirecto) a las listas de la base de datos TS, por ejemplo a través de una conexión de Internet segura, para permitir que el usuario realice cambios en la lista.

Debe entenderse que cualquier característica descrita en relación con cualquier realización puede usarse sola o en combinación con otras características descritas, y también puede usarse en combinación con una o más características de cualquier otra realización, o en cualquier combinación de cualquier otra realización. Además, también pueden utilizarse equivalencias y modificaciones no descritas anteriormente sin apartarse del alcance de la invención, que está definida en las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Método para gestionar al menos una solicitud de servicio enviada desde al menos un terminal a una red, comprendiendo la red un nodo de red para almacenar información de servicios de confianza, que comprende las siguientes etapas:

- la red recibe una solicitud de servicio procedente de un terminal, comprendiendo la solicitud información de solicitud de servicio;

- se envia una solicitud de verificación de usuario para solicitar a un usuario que verifique el servicio solicitado por el terminal si al menos parte de la información de solicitud de servicio no está presente en la información de servicios de confianza;

- se recibe una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario, indicando la información de verificación si el usuario acepta o rechaza la solicitud de servicio;

- se añade al menos parte de la información de solicitud de servicio a la información de servicios de confianza si la información de verificación proporciona una indicación de que se permite el servicio solicitado.

2.- Método según la reivindicación 1, comprendiendo además el método al menos una de las siguientes etapas:

enviar la solicitud de verificación de usuario a través de un canal de comunicación seguro; y

recibir la respuesta de verificación de usuario a través de un canal seguro.

3.- Método según la reivindicación 2, en el que una solicitud de verificación de usuario se envía a través de un canal seguro y una respuesta de verificación de usuario se recibe a través del mismo canal seguro.

4.- Método según la reivindicación 1, comprendiendo además el método la etapa de:

añadir al menos parte de la información de solicitud de servicio a la información de servicios de confianza si la información de verificación proporciona una indicación de que no se permite el servicio solicitado.

5.- Método según la reivindicación 1, comprendiendo además el método las etapas de:

- establecer un canal de comunicación cifrado entre dicho terminal y dicha red;

- enviar la solicitud de verificación de usuario a través de dicho canal de comunicación cifrado al terminal;

- recibir a través del canal de comunicación cifrado una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario que indica si el usuario acepta o rechaza la solicitud de servicio.

6.- Método según la reivindicación 5, en el que el terminal comprende un módulo de identidad, una o más interfaces de entrada/salida y al menos un componente de hardware de confianza, estando configurado dicho componente de hardware de confianza para establecer una o más trayectorias de comunicación de confianza entre dicho componente de hardware de confianza y el módulo de identidad y/o la una o más interfaces de entrada/salida.

7.- Método según la reivindicación 5, comprendiendo el método además las etapas de:

- establecer un canal de comunicación adicional que es diferente del canal de comunicación a través del cual la red recibe la solicitud de servicio;

- enviar al terminal la solicitud de verificación de usuario a través del canal seguro; y,

- recibir a través del canal de comunicación adicional una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación que indica si el abonado permite o rechaza la solicitud de servicio.

8.- Método según la reivindicación 6, en el que el canal de comunicación seguro es proporcionado por un servicio de mensajería, preferentemente un servicio de mensajes cortos o un servicio USSD.

9.- Método según cualquiera de las reivindicaciones 1 a 8, en el que la solicitud de verificación comprende una prueba configurada para determinar si el usuario es una persona o no, preferentemente una prueba de Turing inversa, más preferentemente un *Captcha*, y en el que la respuesta de verificación comprende información que indica si la prueba ha tenido éxito o no.

10.- Método según cualquiera de las reivindicaciones 1 a 9, en el que dicha red comprende un nodo de red de provisión de servicios, comprendiendo dicho nodo de red de provisión de servicios un registro de posiciones de visitantes (VLR) que comprende información de servicios de confianza, comprendiendo además dicho nodo de red una función de verificación de usuario para enviar al terminal, en respuesta a una solicitud de servicio procedente de un terminal, una solicitud de verificación de usuario si al menos parte de la información de solicitud de servicio no está presente en la información de servicios de confianza.

11.- Método según la reivindicación 10, en el que la red comprende además un registro de posiciones base (HLR), comprendiendo dicho registro de posiciones base información de servicios de confianza de dicho terminal, comprendiendo además dicho método la etapa de:

transmitir información de servicios de confianza desde dicho registro de posiciones base a dicho registro de posiciones de visitantes.

12.- Un sistema para gestionar al menos una solicitud de servicio enviada desde al menos un terminal a una red, comprendiendo el sistema:

- uno o más terminales para establecer un canal de comunicación con la red,

- un nodo de red de provisión de servicios configurado para recibir una solicitud de servicio, que comprende información de solicitud de servicio, procedente de al menos uno de dichos terminales,

- una base de datos de servicios de confianza conectada a dicho nodo de red de provisión de servicios;

en el que dicho nodo de red de provisión de servicios está configurado para:

- enviar una solicitud de verificación de usuario para solicitar a un usuario que verifique el servicio solicitado por el terminal si al menos parte de la información de solicitud de servicio no está presente en la información de servicios de confianza,

- recibir una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario, indicando la información de verificación si el usuario acepta o rechaza la solicitud de servicio,

- añadir al menos parte de la información de solicitud de servicio a la información de servicios de confianza si la información de verificación proporciona una indicación de que se permite el servicio solicitado.

13.- Una función de verificación de usuario para su uso en un sistema según la reivindicación 12, comprendiendo la función de verificación de usuario:

- medios para recibir una solicitud de servicio procedente de un terminal, comprendiendo dicha solicitud de servicio información de solicitud de servicio;

- medios para comprobar si al menos parte de dicha información de solicitud de servicio está comprendida en una base de datos de servicios de confianza;

- medios para establecer un diálogo seguro entre el usuario del terminal o entre otro usuario, relacionado con el terminal, y la red si al menos parte de la información de solicitud de servicio no está presente en la información de servicios de confianza; y

- medios para añadir al menos parte de la información de solicitud de servicio a la información de servicios de confianza si el diálogo seguro proporciona una indicación de que se permite el servicio solicitado.

14.- Un producto de programa informático que comprende fragmentos de código de software configurados para, cuando se ejecutan en la memoria de un ordenador, ejecutar una función de verificación de servicio con respecto a una solicitud de servicio que comprende información de solicitud de servicio, enviada desde al menos un terminal a una red, estando configurados los fragmentos de código de software para:

- enviar una solicitud de verificación de usuario para solicitar a un usuario que verifique el servicio solicitado por el terminal si al menos parte de la información de solicitud de servicio no está presente como información de servicios de confianza;

- recibir una respuesta de verificación de usuario, comprendiendo la respuesta información de verificación proporcionada por el usuario, indicando la información de verificación si el usuario acepta o rechaza la solicitud de servicio;

- añadir al menos parte de la información de solicitud de servicio a la información de servicios de confianza si la información de verificación proporciona una indicación de que se permite el servicio solicitado.

15.- Un producto de programa informático según la reivindicación 14, en el que la función de verificación de servicio está implementada en forma de un componente de hardware funcional o como un producto de programa informático ejecutado en el MSC u otro elemento de red diferente conectado al MSC, o es una función distribuida que implica dos o más elementos de red que comprenden uno o más productos de programa de software.

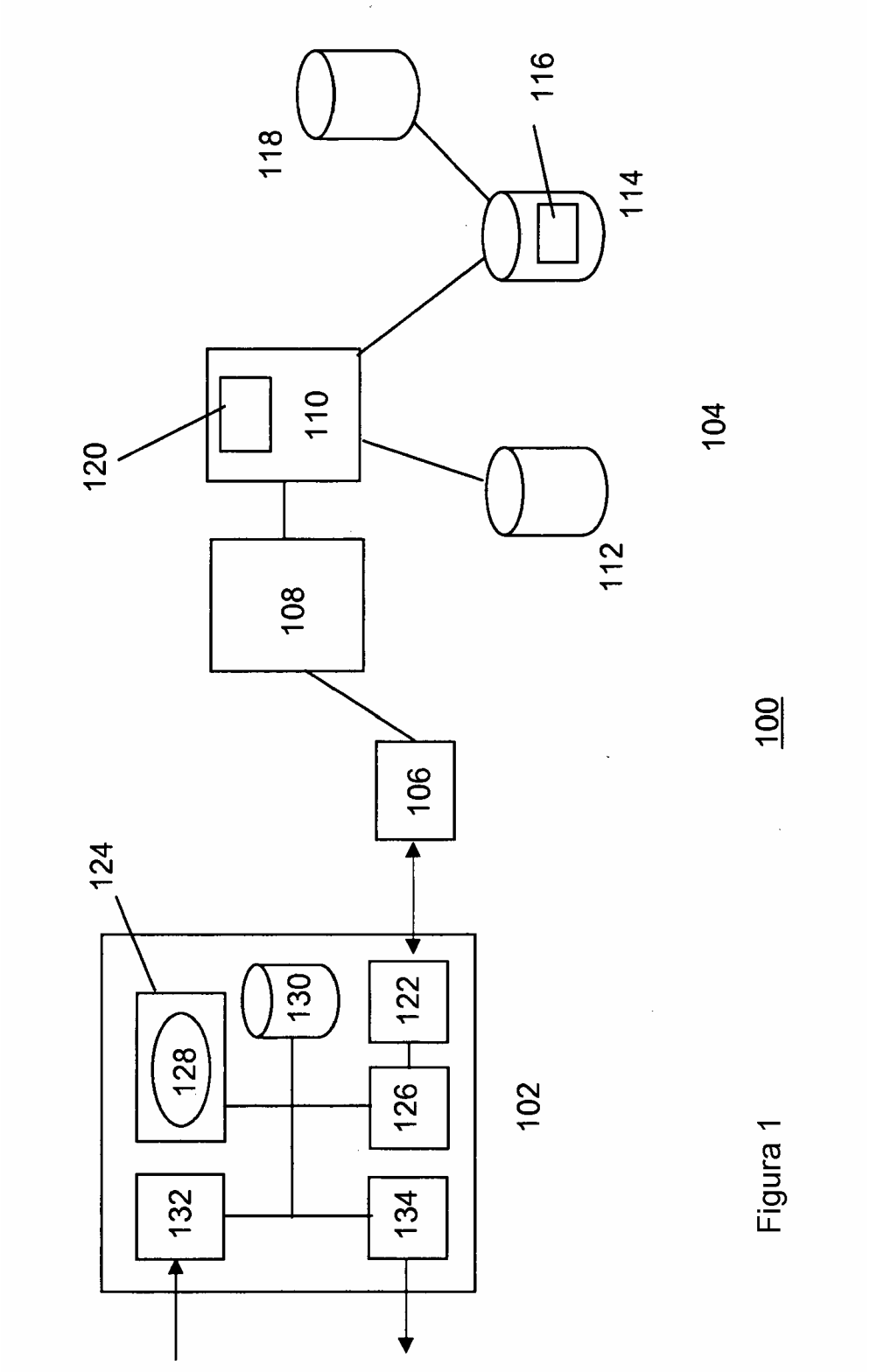
118
116
114
120
110
104
112
108
106
100
124
130
122
128
126
102
132
134

Figura 1

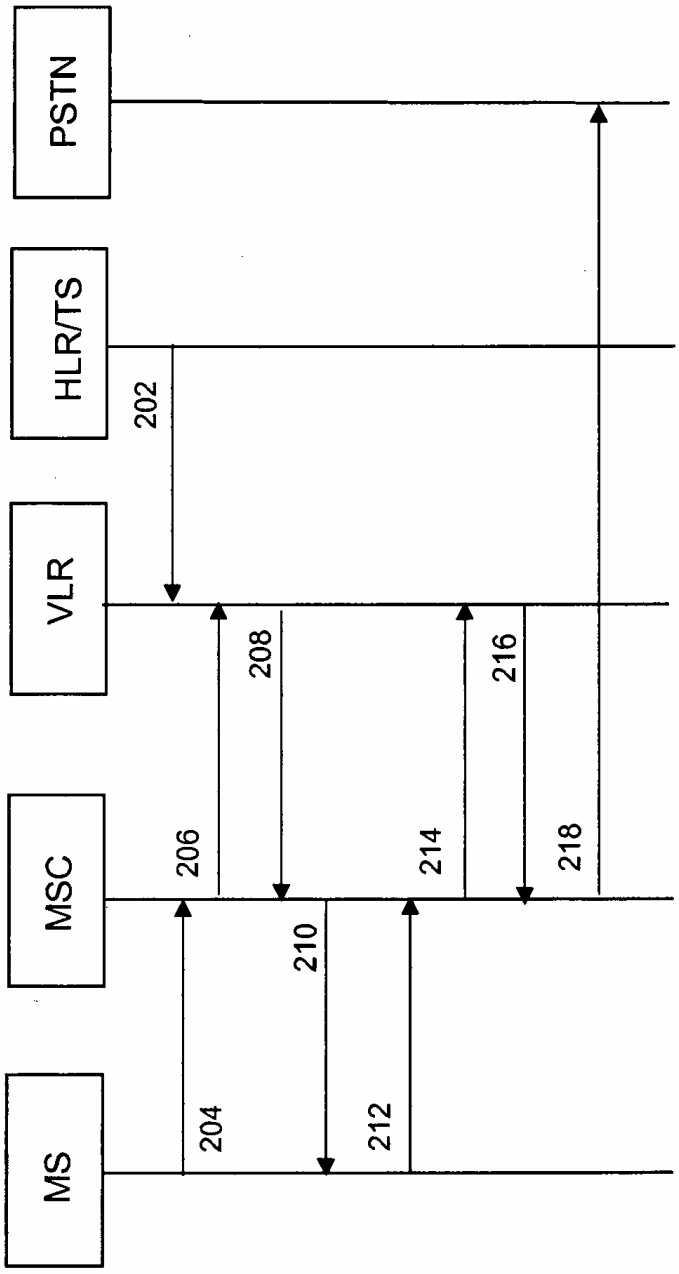

Figura 2

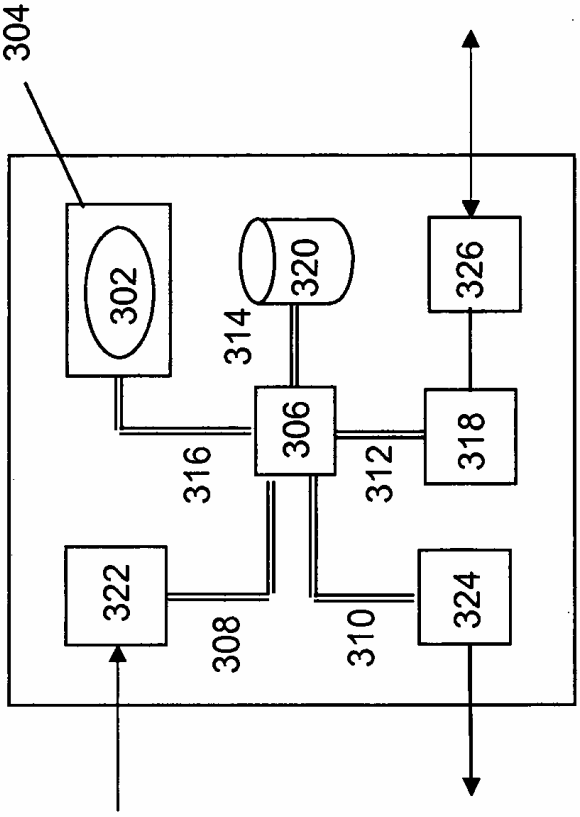

Figura 3