(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 637**

(51) Int. Cl.:
H04L 12/28 (2006.01)
H04L 12/46 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05105528 .3**
(96) Fecha de presentación : **22.06.2005**
(97) Número de publicación de la solicitud: **1615386**
(97) Fecha de publicación de la solicitud: **11.01.2006**

(54) Título: **Sistema cortafuegos para proteger una comunidad de aparatos, aparato participante del sistema y método para actualización de las reglas de cortafuegos dentro del sistema.**

(30) Prioridad: **09.07.2004 FR 04 51496**

(45) Fecha de publicación de la mención BOPI:
25.05.2011

(45) Fecha de la publicación del folleto de la patente:
25.05.2011

(73) Titular/es: **THOMSON LICENSING**
1-5, rue Jeanne d'Arc
92130 Issy-les-Moulineaux, FR

(72) Inventor/es: **Prigent, Nicolas;**
Heen, Olivier;
Bidan, Christophe;
Courtay, Olivier y
Andreaux, Jean-Pierre

(74) Agente: **Arpe Fernández, Manuel**

DESCRIPCIÓN

Sistema cortafuegos para proteger una comunidad de aparatos, aparato participante del sistema y método para actualización de las reglas de cortafuegos dentro del sistema

La presente invención se refiere a la seguridad de una comunidad de aparatos domésticos interconectables, y más concretamente, a la gestión de la política de normas de cortafuegos que hacen posible el filtrado del tráfico que discurre entre dichos aparatos y la red a la que están conectados.

El Documento US-B1-6212633 (Levy Paul S et al.), de fecha 3 de abril de 2001, describe un cortafuegos distribuido que se utiliza en conjunción con un interfaz de comunicaciones serie con correspondencia de memoria, como el definido por la especificación IEEE 1394, para permitir la transmisión segura de datos entre nodos seleccionados a través del interfaz.

Una red local, y más concretamente una red doméstica, consta de una serie de aparatos (televisores, grabadoras digitales, ordenadores, asistentes personales digitales, etc.) conectados mutuamente en red, y que se autoconfiguran e interactúan de forma transparente para el usuario, para ofrecerle unos servicios mejorados. Algunas de las actuales propuestas de normas para redes domésticas son UPnP, descrita en “UPnPT Device Architecture 1.0”, HAVi, descrita en “HAVi Specification version 1.1” y “rendezvous”, descrita por E. Guttman en “Autoconfiguration for IP networking: Enabling local communication”, IEEE Internet Computing, mayo 2001. Los electrodomésticos que pertenecen al usuario de una familia de usuarios compartirán una y la misma política de seguridad. Estos aparatos son interconectables a través de múltiples redes. Estas redes pueden ser redes cableadas dentro del hogar, como IEEE 1394, IEEE Ethernet y similares. También pueden ser redes inalámbricas, como IEEE 802.11, Bluetooth o similares. Los aparatos también pueden comunicarse a través de Internet, como por ejemplo, un aparato móvil que el usuario transporta consigo a su lugar de trabajo, y que se comunicará con la red de su domicilio a través de la red de la empresa y de Internet.

Estas comunidades deben ser seguras si se desea utilizarlas ampliamente. Concretamente, existen motivos y auténticas oportunidades para atacar los aparatos de un usuario. La primera medida para dotar de seguridad a una comunidad de aparatos domésticos consiste en marcar sus límites, es decir, definir qué aparatos pertenecen a la comunidad.

El segundo paso para dotar de seguridad a estas comunidades domésticas consiste en definir una política de filtrado de las comunicaciones entre aparatos de la comunidad y el mundo exterior, o incluso entre los propios aparatos de la comunidad. Los filtros de este tipo, denominados cortafuegos (firewalls), son muy conocidos. Existen diversos tipos de cortafuegos.

Concretamente, se suele dotar a la red de una empresa de un cortafuegos dispuesto en el enlace entre la red de dicha empresa y el exterior. Específicamente, en este tipo de red, todas las comunicaciones entre la red y el exterior pasan a través de uno o más puntos de conexión bien identificados. En este caso, el cortafuegos es administrado por personal competente, encargado de definir la política de seguridad y de ponerla en práctica.

También se suele equipar a los ordenadores personales directamente conectados a Internet con lo que normalmente se denomina cortafuegos personal. Este cortafuegos es un filtro de software situado en el ordenador, y que filtra el tráfico de la red entre el ordenador y el mundo exterior. Este filtrado se lleva a cabo en función de una política definida por el usuario. A estos efectos, existen herramientas que le permiten expresar esta política de una forma muy sencilla y traducirla en forma de reglas de filtrado de paquetes, en función de los protocolos utilizados, de los servicios utilizados o de la dirección de la comunicación. A pesar de estas herramientas, concebidas para facilitar las tareas del usuario, éste sigue encargado de la gestión de su cortafuegos y de las modificaciones de la política de seguridad de su ordenador.

Para la gestión de la política de cortafuegos en redes que poseen varios puntos de acceso al exterior se ha desarrollado la noción de cortafuegos distribuido. En este tipo de cortafuegos, la política de seguridad se define en un punto de la red que sirve como servidor de políticas, aplicándose en múltiples puntos, normalmente en todos los puntos de acceso a la red. De este modo, la coherencia de la política de cortafuegos se garantiza para toda la red mediante la centralización de las normas de la política y su actualización en un único punto.

Las características de las comunidades de los aparatos domésticos modernos presentan una serie de problemas cuando se trata de protegerlas mediante un cortafuegos, de acuerdo con una de las técnicas mencionadas anteriormente. La utilización de medios de RF, que son compartidos por naturaleza, la comunicación entre aparatos a través de Internet, el desenmascaramiento y el intercambio automático de servicios entre aparatos enfrentados, constituyen otros tantos factores que difuminan los límites físicos de las redes domésticas y la situación de los puntos de acceso entre los aparatos de la red doméstica y el exterior. En dicha comunidad, cada aparato se puede comunicar con aparatos externos a la red, sin que dicha comunicación pase necesariamente a través de un punto de acceso identificado.

Además, los aparatos de la comunidad doméstica son susceptibles de desarrollar defectos, o de ser apagados o transportados por el usuario más allá del alcance de los medios de comunicación del resto de la comunidad. Por lo tanto, está claro que la política de seguridad debe aplicarse, por un lado, a los aparatos transportados fuera de la residencia y aquellos que permanecen en el interior de la residencia. Por lo tanto, no es posible contar con la presencia en la red de un aparato que desempeñe un papel privilegiado que garantice la seguridad de la comunidad. Además, es necesario que la política tenga en cuenta las alteraciones de la comunidad, la adición o la retirada de nuevos aparatos.

La invención permite una gestión distribuida y plenamente centralizada de la política de cortafuegos, implementada a nivel de cada aparato, y que es coherente y se adapta dinámicamente a los cambios que se producen en la red doméstica. Nos referiremos a cortafuegoss ubicuos.

La invención se refiere a un sistema de cortafuegos que permite dotar de seguridad a una comunidad de aparatos interconectables que comparten un conjunto formado al menos por una regla de seguridad global común, y en el que cada aparato de la comunidad posee medios para almacenar una política de seguridad local consistente al menos en unas reglas de seguridad globales, en una lista de miembros de la comunidad y su estado de conexión, así como en una lista de servicios ofrecidos localmente, y en la que una pluralidad de aparatos de la comunidad comprende un filtro de mensajes destinados a y con origen en la red a la cual se encuentran conectados, en la que, considerando que el sistema no comprende medios centralizados, posee en cada aparato de la comunidad local medios para calcular las reglas utilizadas por el filtro, en función de la política de seguridad local.

De acuerdo con una realización específica de la invención, el sistema posee en cada aparato de la comunidad medios de actualización de la política de seguridad local, así como para inicio de un nuevo cálculo de las reglas utilizadas por el filtro.

De acuerdo con una realización específica de la invención, los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las reglas utilizadas por el filtro son al menos uno de los siguientes: el cambio de la dirección de red de un aparato de la comunidad, la adición, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio albergado en uno de los aparatos de la comunidad.

De acuerdo con una realización específica de la invención, los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las normas de cortafuegos utilizadas por el filtro son al menos uno de los siguientes: el cambio de la dirección de red de un aparato de la comunidad, la adición, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio albergado localmente en el aparato.

De acuerdo con una realización específica de la invención, el sistema posee en cada aparato de la comunidad medios para determinar la lista de aparatos externos a la comunidad y que cuentan con acceso privilegiado al menos a un servicio ofrecido por un aparato de la comunidad, estando dicha lista integrada en la política de seguridad local.

La invención también se refiere a un aparato que comprende medios para pertenencia a una comunidad de aparatos interconectables que comparten al menos un conjunto formado, al menos, por una regla de seguridad global común, que poseen medios para almacenar una política de seguridad local consistente al menos en reglas de seguridad globales, en una lista de miembros de la comunidad y su estado de conexión, y en una lista de servicios ofrecidos localmente, incluyendo dicho aparato un cortafuegos que comprende un filtro de los mensajes destinados a y con origen en la red a las que está conectado, de forma que posea medios locales para calcular las reglas de cortafuegos utilizadas por el filtro en función de la política de seguridad local, sin tener que recurrir a medios centralizados.

De acuerdo con una realización específica de la invención, el aparato posee medios para iniciar un nuevo cálculo de las reglas utilizadas por el aparato como en respuesta a los cambios que se producen en la red.

De acuerdo con una realización específica de la invención, los cambios que se tienen en cuenta a la hora de iniciar un nuevo cálculo de las reglas utilizadas por el filtro son, al menos, uno de los siguientes: el cambio de la dirección de red de un aparato de la comunidad, la adición, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio albergado en un aparato de la comunidad.

De acuerdo con una realización específica de la invención, los cambios que se tienen en cuenta a la hora de iniciar un nuevo cálculo de las reglas de cortafuegos utilizadas por el filtro son, al menos, uno de los siguientes: el cambio de la dirección de red de un aparato de la comunidad, la adición, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio albergado localmente en el aparato.

De acuerdo con una realización específica de la invención, el aparato posee medios para determinar la lista de aparatos externos a la comunidad y que gozan de acceso privilegiado, al menos, a un servicio ofrecido por un aparato de la comunidad, estando dicha lista integrada en la política de seguridad local.

La invención también se refiere a un método de actualización de las reglas utilizadas por un cortafuegos consistente en un filtrado de los mensajes destinados a y con origen en la red a la cual se encuentra conectado el aparato que implementa el método, formando dicho aparato parte de una comunidad de aparatos interconectables que comparten un conjunto formado al menos por una regla de seguridad global común, contando el aparato con medios para almacenar una política de seguridad local consistente al menos en reglas de seguridad locales, en una lista de miembros de la comunidad y su estado de conexión, y en una lista de servicios ofrecidos localmente, calculándose dichas reglas en función de la política de seguridad local, que comprende al menos las siguientes etapas:

- la detección de la adición, retirada y exclusión de un aparato de la comunidad;
- la detección de los cambios en la dirección de red de un aparato de la comunidad;
- el inicio de un nuevo cálculo de las reglas en respuesta al cambio en la política de seguridad local.

Adicionalmente, de acuerdo con una realización específica de la invención, el método también incluye una etapa de detección de los cambios de estado de los servicios albergados por un aparato de la comunidad.

De acuerdo con una realización específica de la invención, el inicio de un nuevo cálculo de las reglas de cortafuegos está relacionado con la detección de la adición, retirada y exclusión de un aparato de la comunidad, con la detección del cambio en la dirección IP de un aparato de la comunidad y con el cambio en el estado del servicio.

La invención se comprenderá mejor, y el resto de sus características y ventajas serán evidentes mediante la lectura de la siguiente descripción, la cual hace referencia a las figuras adjuntas, en las cuales:

La figura 1 representa un diagrama general de una comunidad de aparatos domésticos protegidos por la invención.

La figura 2 representa un ejemplo de realización de una arquitectura de un cortafuegos ubicuo.

La figura 3 representa un ejemplo de realización de una arquitectura general de un aparato doméstico que incorpora un cortafuegos ubicuo.

A continuación se describirá un ejemplo de realización de un cortafuegos ubicuo y de la gestión de la política de seguridad que utiliza dicho cortafuegos. El ejemplo de realización se facilita dentro del marco de una comunidad de aparatos domésticos que se comunican a través del protocolo IP ("Internet Protocol [protocolo Internet]"). La especificación del protocolo IP puede encontrarse en la solicitud de comentarios de la RFC, mantenida por la IETF, la Internet Engineering Task Force, con el número 791. No obstante, la persona versada en la materia comprenderá que la invención puede aplicarse a cualquier tipo de red de comunicaciones, independientemente del protocolo utilizado, por ejemplo, IEEE 1394 o similares.

Las limitaciones a las que se ha de hacer frente en la comunidad de aparatos domésticos son las siguientes:

En primer lugar, los aparatos son susceptibles de ser conectados o desconectados en cualquier momento. Por lo tanto, es necesario gestionar la inclusión y la exclusión de estos aparatos en la red.

Los aparatos de la comunidad pueden estar físicamente conectados a aparatos no pertenecientes a la comunidad. Concretamente, en el caso de las comunicaciones inalámbricas, los aparatos conectados a la red física no forman necesariamente parte de la comunidad. Igualmente, cualquier aparato es susceptible de convertirse en un punto de acceso entre la comunidad y el mundo exterior. Por lo tanto, las fronteras físicas de la red que interconecta la comunidad no están claramente definidas.

No todos los aparatos que pertenecen a la comunidad están necesariamente preparados para comunicarse entre sí en cualquier momento. Por ejemplo, un usuario que esté lejos de su domicilio puede hacer que un teléfono móvil se comunique con una agenda digital, de forma que entre ellos constituyan una sub-red desconectada de los aparatos que permanecen en el domicilio. Estos aparatos, desconectados del resto de la red doméstica, deben ser capaces de aplicar la política de seguridad definida para la comunidad. Por lo tanto, la comunidad es susceptible de dividirse en un número arbitrario de particiones que sean temporalmente incapaces de comunicarse entre sí. Igualmente, el entorno y las propiedades de un aparato pueden cambiar a lo largo del tiempo. De este modo, un aparato puede cambiar la dirección IP entre dos conexiones sucesivas a la red.

Además, no es posible contar con la ayuda de un administrador competente que administre la comunidad doméstica, al contrario de lo que sucede en la red de una empresa, por ejemplo. Concretamente, el usuario no suele disfrutar de la competencia o del tiempo necesarios para ahondar en los problemas de personalización de un cortafuegos. No obstante, al mismo tiempo constituye la única autoridad sobre la comunidad. Por lo tanto, es necesario facilitarle un medio sencillo de expresión de la política de seguridad, traduciéndola de forma transparente en reglas de cortafuegos.

La figura 1 muestra un ejemplo de comunidad doméstica. La comunidad doméstica consiste, por una parte, en los aparatos del espacio denominado con la referencia 1.1 y que se encuentran en el domicilio, y en los aparatos ubicados en el espacio 1.3 situado en el exterior de la residencia. Se asumirá que estos dos espacios no pueden comunicarse entre sí. El espacio del domicilio 1.1 contiene por una parte una red cableada que enlaza una televisión 1.5, una grabadora de vídeo digital 1.6 y un decodificador digital 1.7, mientras que un módem ADSL facilita el acceso a Internet 1.4 y un terminal inalámbrico 1.9, que opera, por ejemplo, de acuerdo con uno de los protocolos de la familia 802.11 permite la conexión de un equipo HiFi 1.10 y un ordenador 1.11. La familia de normas 802.11 define una norma de comunicaciones a través de una red inalámbrica normalizada en el documento ANSI/IEEE 802.11-1999 (Reaf. 2003). El ordenador del vecino 1.14, que cuenta con capacidad inalámbrica, puede conectarse físicamente a la red inalámbrica 1.2, aunque no forme parte de la comunidad doméstica. El usuario, cuando se encuentra fuera de su domicilio, puede conectar entre sí, por ejemplo, un organizador digital 1.13 y un teléfono móvil 1.12 mediante una conexión inalámbrica, por ejemplo, de acuerdo con el protocolo Bluetooth, para formar una partición 1.3 de la comunidad. Esta partición se invoca para conectarse de nuevo al resto de la comunidad cuando el usuario regresa a su residencia. El aparato de cortafuegos ubicuo, marcado con la referencia 1.15 está descentralizado en cada aparato, y se encuentra delimitado por el rectángulo gris que aparece en los aparatos de la comunidad.

Para garantizar la seguridad de las comunidades de aparatos domésticos es necesario definir una política de seguridad y los servicios de seguridad que van a permitir llevar a cabo esta política. La política de seguridad de una comunidad doméstica es muy parecida a la que se puede encontrar en la red convencional de una empresa. Se compone de dos partes.

Una primera parte plantea el problema de la pertenencia a la comunidad. Concretamente, el primer problema que ha de resolverse es el de la definición de los límites de la comunidad. Una comunidad doméstica constituirá un dominio de aplicación de una política de seguridad uniforme. Todos los aparatos de una y la misma comunidad compartirán una política de seguridad común y compartirán un elevado nivel mutuo de confianza. Por lo general, se considera que los aparatos de una y la misma comunidad pueden comunicarse libremente entre sí. Este problema se resuelve, por ejemplo, mediante la técnica descrita en el siguiente documento: "Gestion sécurisée de groupes de dispositifs dans un reseau domestique", de Nicolas Prigent y Jean-Pierre Andreux, publicado en los procedimientos del segundo simposio sobre seguridad de la información y tecnologías de comunicaciones (SSTIC 2004). En dicho documento se explica cómo puede el usuario definir fácilmente los aparatos que pertenecen a su comunidad doméstica con la ayuda de una identidad criptográfica demostrable de cada aparato. El usuario puede gestionar la inclusión y la exclusión de los aparatos de la comunidad.

La segunda parte de la política de seguridad de la comunidad pretende gestionar las comunicaciones entre los aparatos de la comunidad y el mundo exterior. Por lo tanto, esto afecta a las comunicaciones entre los aparatos de la comunidad y los aparatos que no pertenecen a la comunidad, pero que son capaces de comunicarse con los aparatos de la comunidad. En este caso se encuentran aparatos accesibles a través de Internet o aparatos que llevan los invitados al domicilio y que se conectan temporalmente a la red doméstica del usuario. Dado que se supone que los aparatos integrados en la comunidad doméstica se ajustan a la política de seguridad, suele admitirse

en general que las comunicaciones iniciadas por los aparatos que forman parte de la comunidad pueden salir de la comunidad con libertad. Por el contrario, las comunicaciones iniciadas por los aparatos externos a la comunidad deben supervisarse, garantizándose su cumplimiento de la política de seguridad. En la práctica, el acceso a los servicios ofrecidos por los aparatos que pertenecen a la comunidad debe haber sido explícitamente autorizado por el usuario a fin de que las solicitudes destinadas a estos servicios sean aceptadas dentro de los límites de la comunidad.

Más exactamente, un servicio en un aparato de la comunidad podrá declararse como público (es decir, que cualquier aparato externo pueda acceder al mismo), restringido (es decir, que el acceso a este servicio por parte del aparato externo está sujeto a una condición) o privado (está prohibido el acceso por parte de un aparato externo). Será entonces necesario verificar el cumplimiento de esta política por parte de las comunicaciones iniciadas por un aparato situado en el exterior de la comunidad.

Es evidente que la política de seguridad descrita constituye un ejemplo y que las reglas definidas de este modo se pueden modificar sin alejarse del marco del ejemplo de realización.

A continuación se describirá un ejemplo de ejecución de esta política de seguridad. Con esta finalidad, definiremos el concepto de cortafuegos ubicuo. Teniendo en cuanta las limitaciones ya descritas, es imposible hacer que un aparato de la comunidad desempeñe un papel específico, debiendo garantizarse la política de seguridad en todos los aparatos, sin presuponer la presencia y la accesibilidad de otro aparato de la comunidad en la red doméstica. Por consiguiente, se definirá un servicio de cortafuegos, denominado ubicuo, a nivel de cada uno de los aparatos de la comunidad.

La figura 2 muestra la arquitectura de este servicio. Está compuesta por una base de conocimiento local, denominada 2.1, que contiene la información relativa a la política, así como la información relativa al actual entorno del aparato. Esta información es utilizada por el núcleo del cortafuegos ubicuo, designado con la referencia 2.5, para generar las normas del cortafuegos. La base de conocimiento local comprende el gestor de política local (GPL), denominado con la referencia 2.2, cuya tarea consiste en adquirir, almacenar y gestionar la información relativa a la política de seguridad, y el módulo de adaptación al entorno (MAE), designado con la referencia 2.3, cuya función consiste en adquirir, almacenar y gestionar la información relativa al entorno del aparato. El módulo de criptografía, designado con la referencia 2.4, se ocupa de las operaciones de autentificación entre el aparato local y el resto de aparatos, así como de las claves posiblemente utilizadas para establecer canales de comunicaciones seguros. Por su parte, el núcleo del cortafuegos ubicuo, denominado con la referencia 2.5, se ocupa de generar las reglas utilizadas por el filtro de mensajes, designado con la referencia 2.6, en base a la información contenida en la base de conocimiento local, y utilizando posiblemente las claves obtenidas del módulo de criptografía. El filtro de mensajes, designado con la referencia 2.6, aplica las reglas obtenidas de esta forma a los mensajes procedentes de, y dirigidos a, la capa de protocolo de la red, en este caso la capa IP. Las aplicaciones, designadas con las referencias 2.8 y 2.9, accederán a la capa de protocolo de la red de una forma transparente, y recibirían los mensajes tras la aplicación del filtro.

El gestor de política local está encargado de la adquisición, el almacenamiento y la gestión de la política de seguridad. Gestiona la información relevante relativa a la política genérica global, que es la misma para todos los aparatos de la comunidad. Un ejemplo de esta política está constituido por las dos reglas siguientes:

- los aparatos pertenecientes a la comunidad doméstica tienen libertad para comunicarse entre sí, de una forma segura o de otro modo.
- se supervisa el acceso por parte de los aparatos externos a la comunidad doméstica a los servicios ofrecidos por los aparatos de la comunidad.

Mediante el uso de esta política general, así como de la información específica que posee en relación con la comunidad doméstica, y concretamente, la lista de aparatos de la comunidad y su estado de conexión, así como la lista de servicios ofrecidos, bien localmente o por la comunidad, y su estado público, restringido o privado, el gestor es capaz de construir su propia visión local de la política de seguridad.

Concretamente, el gestor de política local posee una primera categoría de información relativa a los límites de la comunidad. Esta consiste principalmente en información relativa a los aparatos pertenecientes a la comunidad doméstica y al método que permite su identificación y autentificación. Cada aparato de la comunidad doméstica está dotado de una identidad demostrable, que le permite ser identificado y autentificarse con el resto de aparatos de su red. Denominaremos a una identidad que es fácil de verificar, pero muy difícil de usurpar, una “identidad demostrable”. Por ejemplo, la clave pública de un par de claves privada/pública se puede utilizar como una identidad demostrable; un aparato que pretenda ser identificado mediante su clave pública puede aceptar un desafío utilizando su clave privada, y es capaz de descifrar por sí solo un mensaje que ha sido cifrado con su clave pública. Además, al utilizar sus respectivas identidades demostrables, dos aparatos pueden crear un canal de comunicaciones seguro, lo que posiblemente les permite instalar claves simétricas de sesión, utilizando un protocolo de acuerdo relativo a las claves, por ejemplo. Estas claves de sesión punto a punto pueden servir para posteriores autentificaciones y para asegurar las comunicaciones (autenticidad y confidencialidad) entre los dos aparatos.

Existen numerosos métodos conocidos para garantizar de forma digna de confianza la pertenencia de un aparato a una comunidad, incluyendo el ya citado documento “Gestión segura de grupos de aparatos en una red doméstica”.

El gestor de política local posee una segunda categoría de información relativa a las comunicaciones que están autorizadas a saltarse los límites de la comunidad doméstica. En esta categoría se encuentra, en primer lugar, la lista de servicios públicos ofrecidos por el aparato, como por ejemplo, servidores públicos HTTP. También se encuentra aquí la lista de servicios restringidos. Por lo tanto, sólo puede accederse a dichos servicios en determinadas condiciones. Para cada uno de estos servicios, el gestor posee información relativa a las condiciones que deben cumplirse para acceder a este servicio. Un ejemplo de dicha información podría ser un nombre de

usuario y una contraseña con el método de autentificación utilizado, el conocimiento de un elemento informativo criptográfico particular, una lista de aparatos explícitamente autorizados, un dominio cuyos aparatos estén autorizados o cualquier otra condición. Existen diversas fuentes de información para el gestor de la política local. Estas pueden ser el usuario o una fuente legítima de política de seguridad, tal como otro aparato de la comunidad doméstica.

Algunas modificaciones producidas en la política local son compartidas por los diversos aparatos de la comunidad. Estas modificaciones pueden ser de diversos tipos. Por una parte, el usuario puede añadir, eliminar o excluir un aparato de la comunidad. Puede efectuarse la adición desde un aparato de la comunidad conectado al nuevo aparato, en el que el usuario indicará que el nuevo aparato debería considerarse parte integrante de la comunidad. La eliminación de un aparato puede efectuarse en el aparato que el usuario desea excluir de la comunidad, o desde cualquier otro aparato perteneciente a la misma. La exclusión se refiere al procedimiento mediante el que un usuario indicará la comunidad que un aparato al que ha dejado de tener acceso debe dejar de considerarse como un integrante de la comunidad. Los mecanismos que permiten su implementación se describen en el ya citado documento “Gestión segura de grupos de aparatos en una red doméstica”. Por lo tanto, estas modificaciones serán tenidas en cuenta por todos los aparatos de la comunidad en cuanto tienen la posibilidad de comunicarse.

Otro tipo de cambio de política es el cambio de estado de un servicio en un aparato de la comunidad. En este caso se puede pensar en dos soluciones. La primera consiste en afirmar que tan sólo la lista de servicios albergada en un aparato forma parte de la política local de dicho aparato. Teniendo esto en cuenta no es necesario transmitir al resto de los aparatos un cambio de estado de un servicio que se produce en un aparato. La consecuencia de esta solución es que el bloqueo de una solicitud no autorizada de un servicio albergado en un aparato dado será posible tan sólo en ese mismo aparato. Por lo tanto, el resto de los aparatos de la red que desconozcan el estado de los servicios transmitirán la petición sin que sean capaces de verificar su cumplimiento de la política de seguridad. La segunda solución consiste en transmitir la información relativa al estado de los servicios a todos los aparatos de la comunidad. En este caso, cualquier cambio en el estado de un servicio de un aparato se transmitirá automáticamente a todos los aparatos conectados de la comunidad. Se efectuará una actualización de los aparatos no conectados en el momento de producirse el cambio cuando se lleve a cabo la siguiente conexión. Esta solución permite bloquear una solicitud no conforme con las reglas tan pronto como llega al primer aparato de la comunidad. El cambio en el estado de un servicio efectuado por el usuario sólo puede autorizarse en el aparato que alberga el servicio. En este caso, no pueden producirse conflictos de política durante la conexión de dos particiones de la comunidad, ya que el estado definido en la partición que alberga el servicio se considera siempre como el estado correcto que ha de transmitirse a los aparatos de la otra partición. En el caso de que el usuario esté autorizado a modificar el estado de un servicio desde cualquier aparato de la comunidad, puede darse el caso de que se encuentren conectadas dos particiones de la comunidad que tengan un estado diferente para un servicio dado. Este tipo de conflicto puede resolverse, bien teniendo en cuenta el calendario del último cambio de estado, o solicitando el arbitraje del usuario para confirmar la opción seleccionada entre los dos estados.

Por su parte, el módulo de adaptación al entorno es el responsable de la gestión de la asociación entre la identidad de los aparatos y la dirección de red, en este caso, IP, que éstos poseen en un momento dado. Concretamente, esta información es indispensable cuando se desea enviar un mensaje a un aparato que en otro caso sólo se conoce a través de su identidad demostrable. Este módulo también mantiene la asociación entre las direcciones y las identidades de los aparatos privilegiados que cuentan con acceso a la comunidad, es decir, los aparatos que, aunque no formen parte de la comunidad, disfrutarán de un acceso privilegiado a determinados servicios de la comunidad. Una de las múltiples soluciones para que este módulo sea capaz de adquirir y actualizar las asociaciones entre las identidades de los aparatos y su dirección en la red consiste, para cada aparato, en transmitir periódicamente su dirección e identidad a través de la red. Cuando el módulo de adaptación al entorno recibe un mensaje de este tipo, puede verificar que esta identidad es legítima, a fin de combatir una posible usurpación. Este módulo es el que también se encarga de transmitir los mensajes periódicos de anuncio de tal forma que los MAEs de las otras aplicaciones también puedan actualizarse a sí mismos.

Por su parte, el módulo de datos criptográficos tendrá al menos dos funciones principales. Por una parte, se encargará de la gestión de la identidad demostrable del aparato. Por otra parte, también servirá para construir canales seguros de comunicaciones. Concretamente, dado que no es posible impedir que un aparato externo y potencialmente malévolo pueda acceder físicamente a la red, puede resultar útil asegurar las comunicaciones entre los aparatos de la comunidad. Por lo tanto, es posible crear una red privada virtual que agrupe los aparatos de la comunidad doméstica. Teniendo en cuenta las erráticas propiedades de la conexión dentro de la red doméstica, el establecimiento de un canal seguro de comunicaciones no debe requerir la presencia de más de dos aparatos en la comunidad. En función del conocimiento local que tiene de la comunidad, cada aparato puede garantizar la seguridad punto a punto de las comunicaciones con los otros aparatos. Por razones de rendimiento, se fomenta la utilización de la criptografía simétrica, pero es evidente que también se puede utilizar la criptografía asimétrica. La utilización de la criptografía simétrica requiere la instalación simétrica de claves punto a punto en los aparatos. Por razones de facilidad de utilización, no es posible pedir al usuario que defina e introduzca estas claves simétricas en los aparatos. Además, esto sería contraproducente a nivel de seguridad: de hecho, existe un riesgo de que el usuario pueda seleccionar unas claves débiles. La instalación de las claves puede efectuarse, por ejemplo, utilizando el protocolo STS (“Estación a Estación”) definido en el documento “Authentication and Authenticated key exchanges”. *Design Codes and Cryptography*, 2: 107-125, 1992, de W. Diffie, P. van Oorschot y M. Wiener. Por lo tanto, las claves se instalan de una forma incondicional sin la intervención del usuario, que desconoce las claves utilizadas. Esto permite obtener un adecuado nivel de seguridad y una buena ergonomía del sistema. Otra ventaja de este sistema de claves punto a punto es su resistencia a la corrupción de un aparato. Concretamente, si un

atacante fuese a tomar el control de un aparato, las comunicaciones entre el resto de las aplicaciones no se verían comprometidas por el hecho de que las claves son estrictamente punto a punto entre cada par de aparatos de la comunidad. Además, el sistema opera tan pronto como se encuentran presentes dos aparatos en la comunidad doméstica. Las limitadas dimensiones de una comunidad doméstica y la gestión completamente distribuida de las claves implican que el número de claves que han de ser gestionadas por cada aparato aumenta linealmente con el tamaño de la comunidad y sigue siendo razonable.

El núcleo del cortafuegos se encarga de generar las reglas de cortafuegos que serán utilizadas por el filtro. Esta generación se efectúa a partir de las reglas de la política, de la forma siguiente:

En primer lugar, el núcleo del cortafuegos establecerá las reglas que autorizan las comunicaciones necesarias para el funcionamiento del cortafuegos ubicuo. Esto afecta a los mensajes intercambiados entre los MAEs para anunciar y detectar los aparatos con los que es posible comunicarse, así como los mensajes intercambiados por los módulos de criptografía para permitir la autentificación y el intercambio de claves punto a punto en caso de que se instalen canales de comunicaciones seguras. Estos mensajes entre los módulos criptográficos, aunque no son indispensables para el funcionamiento de un cortafuegos ubicuo, son necesarios para establecer un elevado nivel de seguridad dentro de la comunidad doméstica. También es necesario autorizar los mensajes entre las bases de conocimiento locales, así como, posiblemente, aquellos que resulten útiles para obtener una dirección de red, como una solicitud DCHP o similares. Todas estas comunicaciones se autorizan sin que se les dote de seguridad (encriptadas o autentificadas) a nivel del filtro.

En segundo lugar, el núcleo del cortafuegos establecerá las reglas que permiten la comunicación entre aparatos de la comunidad. Cualquier mensaje con origen en una dirección identificada por el módulo de adaptación al entorno como perteneciente a la comunidad, es posible que se descifre y que se verifique su autenticidad, en virtud de la identidad demostrable de la fuente conocida, o la clave o claves simétricas instaladas por el módulo criptográfico. Si se instala la autentificación, el mensaje se aceptará si la autentificación es correcta, denegándose en caso contrario. Si no se instala la autentificación, el mensaje se aceptará.

Igualmente, en el caso de cualquier mensaje destinado a un aparato de la comunidad, será posible llevar a cabo su cifrado y su autentificación basándose en la identidad demostrable del destino, o en la clave o claves simétricas instaladas por el módulo de criptografía, despachándose a continuación.

El núcleo del cortafuegos también definirá las reglas que rigen las comunicaciones pertenecientes a los servicios privilegiados. Las reglas deben llevar a cabo las comprobaciones de verificación de las condiciones de acceso. Por ejemplo, si la política indica que un aparato que posee una identidad demostrable de este tipo puede acceder a un servicio privilegiado determinado, podrá utilizarse entonces el MAE para verificar la dirección IP correspondiente a esta identidad demostrable, para generar la regla que autoriza las solicitudes destinadas a este servicio y con origen en esta dirección. También es posible utilizar las propiedades del grupo seguro de protocolos IP IPsec para filtrar las solicitudes enviadas a un servicio que se ha cifrado mediante una clave secreta compartida. La especificación del grupo de protocolos IPsec puede encontrarse en la RFCs, solicitud de comentarios, mantenida por la IETF Internet Engineering Task Force, con el número 2401, y la descripción de una parte de los protocolos de los que se compone, AH, ESP e IKE, respectivamente, con los números 2402, 2406 y 2409. Por otra parte, los servicios cuyo acceso se ha hecho seguro mediante un método de autentificación de alto nivel se declararán como servicios públicos, y en este caso, la autentificación se llevará a cabo a nivel de servicio. En este caso, puede citarse el acceso a un servidor HTTP accesible a través de un nombre de usuario y una contraseña.

En este caso, no se pueden efectuar las comprobaciones al nivel de la capa de protocolos de la red.

Igualmente, el núcleo del cortafuegos generará las reglas que autorizan las comunicaciones relativas a los servicios públicos, independientemente del origen de los mensajes.

Por último, el núcleo del cortafuegos generará las reglas que prohíben cualquier conexión de entrada, a excepción de las explícitamente autorizadas por una de las anteriores reglas y que autorizan cualquier conexión de salida. Específicamente, y por defecto, todos los servicios se consideran como privados.

Estas reglas se generan nuevamente con cada modificación de la política de seguridad, o cuando se modifica el entorno de la aplicación. Estas modificaciones pueden proceder de la modificación de la topología, es decir, de la adición o eliminación de uno o más aparatos de la red. En este caso, puede comentarse que la eliminación de un aparato de la red, es decir, la pérdida de conectividad de un aparato que no abandona la comunidad no requiere generar nuevamente las reglas de cortafuegos, y tan sólo un retorno de la conectividad, en la medida en que no se haya modificado su dirección IP. En este caso, los eventos que requieren una nueva generación de las reglas de cortafuegos tan sólo son el cambio de una dirección IP de un aparato de la comunidad, o de un aparato autorizado a acceder a un servicio privilegiado, o la eliminación, la adición y la exclusión de un aparato de la comunidad. Esta modificación también puede proceder de la modificación de la política relativa a un servicio disponible a nivel de la comunidad. Como ya hemos visto, esta modificación puede gestionarse totalmente de manera local en el aparato que alberga el servicio, que tan sólo tendrá que generar un nuevo conjunto de reglas, o dicha modificación puede transmitirse por el ámbito de la comunidad y precisar que se genere de nuevo en todos los aparatos de la comunidad. Dado que esta generación es totalmente automatizada se dispone en cualquier momento en el aparato de un conjunto de reglas de cortafuegos coherente con la política de seguridad de la cual tiene conocimiento.

El usuario es la única autoridad dentro de la comunidad. Por lo tanto, él es el único que define el estado, bien público o restringido, de los servicios ofrecidos por los aparatos que posee. Para ello, tendrá que autentificarse en el aparato que alberga el servicio cuyo estado desea modificar. La forma de autentificarse en el aparato dependerá del aparato, y no es necesariamente uniforme dentro de la comunidad. Puede conllevar un código que se introduce en un teléfono móvil, una contraseña en un televisor, y similares. Una vez autentificado como autoridad en el aparato, se presenta al usuario una lista de servicios ofrecidos por el aparato, y puede modificar el estado de los mismos.

También puede especificar, para los servicios restringidos, la condición de acceso como secreto compartido a utilizar, por ejemplo.

La figura 3 muestra un ejemplo de la arquitectura general de un aparato, designado con la referencia 3.1, y que forma parte de un aparato de cortafuegos. Dicho aparato comprende un interfaz de red, designado con la referencia 3.6, para conectar el aparato a la red indicada con la referencia 3.7. También comprende una memoria permanente, indicada con la referencia 3.5, pensada para almacenar los programas necesarios para la ejecución del cortafuegos de acuerdo con la arquitectura de la figura 2. Estos programas se cargarán en la memoria de acceso aleatorio, indicada con la referencia 3.2. Todos estos elementos se interconectarán mediante un bus de comunicaciones indicado con la referencia 3.4. Es evidente para cualquier persona versada en la materia que esta arquitectura puede variar en cuanto a la disposición de estos medios, y que tan sólo es un ejemplo de la arquitectura de un aparato que puede implementar un cortafuegos ubicuo.

De este modo, hemos definido un cortafuegos ubicuo, que opera en todos los aparatos de la una comunidad de aparatos domésticos. Dicho cortafuegos ejecutará una política de seguridad coherente y uniforme en todo el ámbito de la comunidad, protegiendo a ésta mediante el filtrado de las comunicaciones. Este cortafuegos está totalmente distribuido en todos los aparatos, y ninguno de los aparatos desempeña ninguna función específica en este modo de funcionamiento. Esta política altera dinámicamente y se adapta automáticamente a las alteraciones de la conectividad dentro de la comunidad. El usuario puede modificar esta política fácilmente, sin tener que averiguar los detalles de la implementación del cortafuegos. Será evidente para la persona versada en la materia que la invención podrá llevarse a cabo dentro de un entorno de red que se ajuste a diversos protocolos de comunicaciones, incluyendo los que no se basan en una IP, y que la modificación de las reglas de la política de seguridad aplicadas, o la modificación de la división funcional de la arquitectura presentada para el cortafuegos ubicuo no se aleja del marco de la invención.

REIVINDICACIONES

1. Sistema de cortafuegos (11.15) que permite dotar de seguridad a una comunidad de aparatos interconectables (1.5, - 1.13) que comparten un conjunto formado al menos por una regla de seguridad global común, teniendo cada aparato (1.5, - 1.13) de la comunidad (1.1, - 1.3) medios (2.1) para almacenar una política de seguridad local consistente al menos en reglas de seguridad globales, en una lista de miembros de la comunidad (1.1, - 1.3), así como su estado de conexión, y una lista de servicios ofrecidos localmente, incluyendo una pluralidad de aparatos (1.5, - 1.13) de la comunidad (1.1, - 1.3) un filtro (2.6) para mensajes destinados a y con origen en la red a la que están conectados,

caracterizado porque el sistema no comprende medios centralizados, y porque posee en cada aparato (1.5, - 1.13) de la comunidad (1.1, - 1.3) medios locales para cálculo de reglas (2.5) utilizadas por el filtro (2.6) en función de la política de seguridad local.

2. Sistema de acuerdo con la reivindicación 1, que posee en cada aparato de la comunidad medios (2.2) para actualización de la política de seguridad local y para inicio de un nuevo cálculo de las reglas utilizadas por el filtro.

3. Sistema de acuerdo con la reivindicación 2, que posee medios (2.3) para iniciar un nuevo cálculo de las reglas utilizadas por el filtro en respuesta a cambios acaecidos en la red.

4. Sistema de acuerdo con la reivindicación 3, en el que los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las reglas utilizadas por el filtro son al menos uno de los siguientes: el cambio en la dirección de red de un aparato de la comunidad, la inclusión, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio ofrecido por la comunidad.

5. Sistema de acuerdo con la reivindicación 3, en el que los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las reglas de cortafuegos utilizadas por el filtro son, al menos, uno de los siguientes: el cambio en la dirección de red de un aparato de la comunidad, la inclusión, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio ofrecido localmente en el aparato que alberga el servicio.

6. Sistema de acuerdo con la reivindicación 1, que posee en cada aparato de la comunidad medios para determinar una lista de aparatos externos a la comunidad que gozan de acceso privilegiado al menos a un servicio ofrecido por un aparato de la comunidad, estando integrada dicha lista en la política de seguridad local.

7. Aparato (1.5, - 1.13) que comprende medios de pertenencia a una comunidad (1.1, - 1.3) de aparatos interconectables (1.5, - 1.13) que comparte un conjunto formado, al menos, por una regla de seguridad global común, que posee medios (2.1) para almacenar una política de seguridad local consistente al menos en reglas globales de seguridad, una lista de miembros de la comunidad (1.1, - 1.3), así como su estado de conexión y una lista de servicios ofrecidos localmente, teniendo dicho aparato (1.5, - 1.13) un cortafuegos (1.15) que comprende un filtro (2.6) de mensajes destinados a y con origen en la red a la que se encuentra conectado,

caracterizado porque posee medios locales, (2.5) para cálculo de reglas de cortafuegos utilizadas por el filtro (2.6) en función de la política de seguridad local, sin necesidad de recurrir a medios centralizados.

8. Aparato de acuerdo con la reivindicación 7, que posee medios (2.2) para actualizar la política de seguridad local y para iniciar automáticamente un nuevo cálculo de las reglas utilizadas por el filtro.

9. Aparato de acuerdo con la reivindicación 8, que posee medios (2.3) para iniciar un nuevo cálculo de las reglas utilizadas por el filtro, en respuesta a cambios acaecidos en la red.

10. Aparato de acuerdo con la reivindicación 9, en el que los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las reglas utilizadas por el filtro son al menos uno de los siguientes: el cambio en la dirección de red de un aparato de la comunidad, la inclusión, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio ofrecido por la comunidad.

11. Aparato de acuerdo con la reivindicación 9, en el que los cambios que se tienen en cuenta para iniciar un nuevo cálculo de las reglas de cortafuegos utilizadas por el filtro son, al menos, uno de los siguientes: el cambio en la dirección de red de un aparato de la comunidad, la inclusión, retirada o exclusión de un aparato de la comunidad y el cambio de estado de un servicio ofrecido localmente por el aparato que alberga el servicio.

12. Aparato de acuerdo con la reivindicación 7, que posee medios para determinar una lista de aparatos externos a la comunidad y que gozan de acceso privilegiado, al menos, a un servicio ofrecido por un aparato de la comunidad, estando dicha lista integrada en la política de seguridad local.

13. Método de actualización de reglas utilizadas por un cortafuegos (1.15) consistente en un filtro (2.6) de mensajes destinados a y con origen en la red a la cual se encuentra conectado un aparato (1.5-1.3) que implementa dicho método, formando dicho aparato (1.5-1.13) parte de una comunidad (1.1-1.3) de aparatos interconectables (1.5-1.13) que comparten un conjunto formado al menos por una regla de seguridad global común, contando el aparato con medios para almacenar una política de seguridad local consistente, al menos, en reglas de seguridad locales, en una lista de miembros de la comunidad (1.1-1.3) y su estado de conexión, y en una lista de servicios ofrecidos localmente, calculándose dichas reglas en función de la política de seguridad local, que comprende al menos las siguientes etapas:

- la detección de la adición, retirada y exclusión de un aparato (1.5-1.13) de la comunidad (1.1-1.3);
- la detección de los cambios en la dirección de red de un aparato (1.5-1.13) de la comunidad (1.1-1.3);
- el inicio de un nuevo cálculo de las reglas en respuesta al cambio en la política de seguridad local.

14. Método de acuerdo con la reivindicación 13, que adicionalmente incluye una etapa de detección de los cambios de estado de los servicios ofrecidos localmente en el aparato que alberga los servicios.

15. Método de acuerdo con la reivindicación 13, que adicionalmente incluye una etapa de detección de los cambios de estado de los servicios ofrecidos por la comunidad.

16. Método de acuerdo con la reivindicación 14 o 15, en el que el inicio de un nuevo cálculo de las reglas de cortafuegos se encuentra relacionado con la detección de la adición, retirada y exclusión de un aparato de la

comunidad, con la detección del cambio en la dirección IP de un aparato de la comunidad y con el cambio de estado de un servicio.

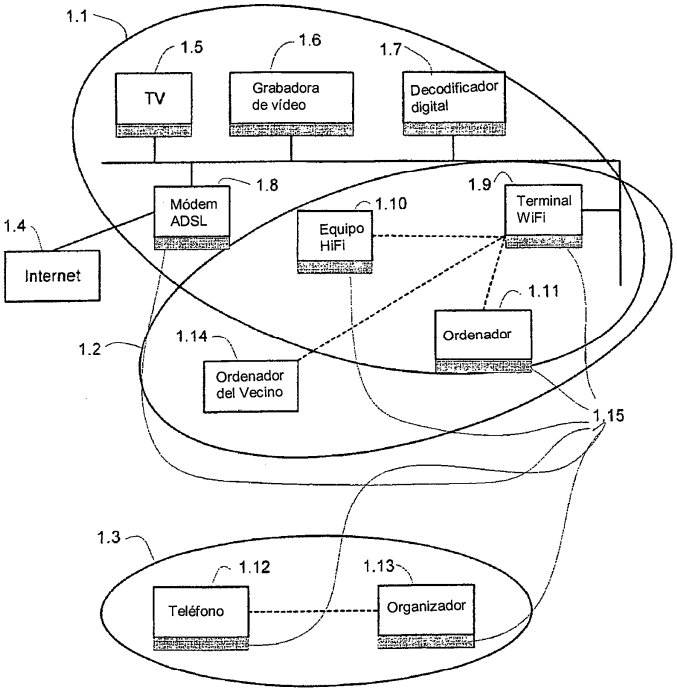
1.1
1.5
1.6
1.7
TV
Grabadora de vídeo
Decodificador digital
1.8
1.9
Módem ADSL
1.10
Equipo HiFi
Terminal WiFi
1.4
Internet
1.11
Ordenador
1.14
1.2
Ordenador del Vecino
1.15
1.3
1.12
1.13
Teléfono
Organizador

Fig. 1

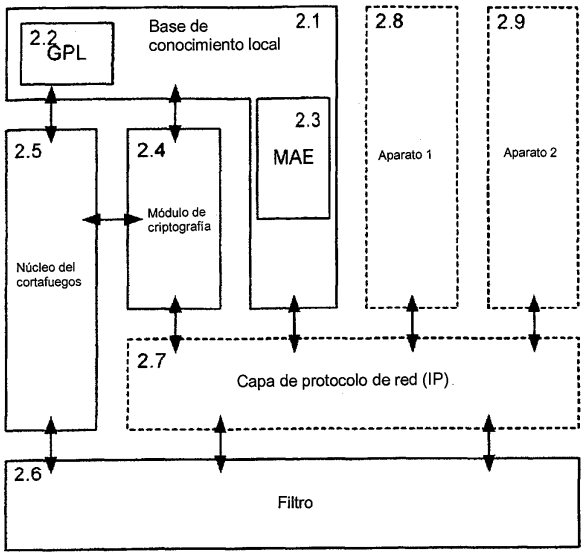
2.2
GPL
Base de
conocimiento local
2.1
2.8
2.9
2.3
MAE
Aparato 1
Aparato 2
2.5
2.4
Módulo de
criptografía
Núcleo del
cortafuegos
2.7
Capa de protocolo de red (IP)
2.6
Filtro

Fig. 2

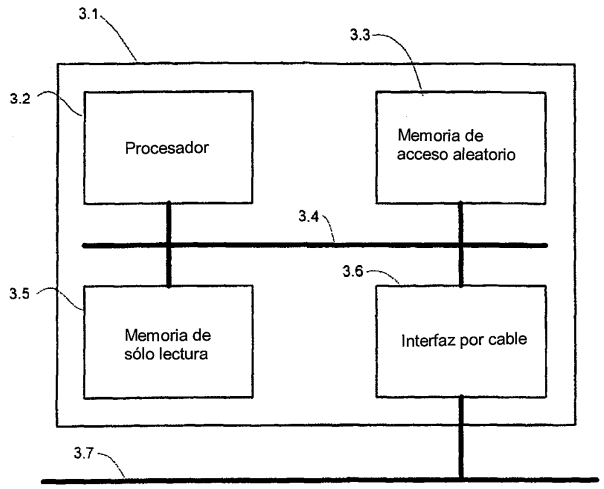
3.1
3.3
3.2
Procesador
Memoria de acceso aleatorio
3.4
3.6
3.5
Memoria de sólo lectura
Interfaz por cable
3.7

Fig. 3

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citado en la descripción

• US 6212633 B1 **[0002]**

Bibliografía de patentes citada en la descripción

• **W. Diffie, P. van Oorschot ; M. Wiener.** Authentication and authenticated key exchanges. Design Codes and Cryptography, 1992, vol. 2, 107-125 **[0051]**