(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 373 647**

(51) Int. Cl.:
H04N 7/16 (2006.01)
H04N 5/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03709351 .5**
(96) Fecha de presentación : **27.02.2003**
(97) Número de publicación de la solicitud: **1479232**
(97) Fecha de publicación de la solicitud: **24.11.2004**

(54) Título: **Método y dispositivo para la obtención de un objeto de perfil de seguridad jerárquica.**

(30) Prioridad: **27.02.2002 US 360100 P**

(45) Fecha de publicación de la mención BOPI:
07.02.2012

(45) Fecha de la publicación del folleto de la patente:
07.02.2012

(73) Titular/es: **OPENTV, Inc.**
275 Sacramento Street
San Francisco, California 94111, US

(72) Inventor/es: **Kidd, Taylor, W.**

(74) Agente: **Tomás Gil, Tesifonte Enrique**

DESCRIPCIÓN

Método y dispositivo para la obtención de un objeto de perfil de seguridad jerárquica.

Antecedentes de la invención

Campo de la invención

Esta invención se refiere a la seguridad en la televisión interactiva y, más particularmente, a la gestión de perfil de seguridad jerárquico para programas, servicios y otras aplicaciones transmitidas en un entorno de televisión interactiva.

Descripción de las técnicas relacionadas

Las últimas formas de comunicación de transmisión televisiva incluyen la posibilidad de televisión interactiva en la que no sólo la entidad emisora envía sus programas al espectador, sino que el espectador puede enviar también información de vuelta a la fuente emisora o emisor. El contenido de la entidad emisora incluye típicamente programas de red y anuncios publicitarios, al igual que páginas web, programas interactivos de televisión, gráficos y texto, y otros elementos. Sin restricción, el espectador puede al mismo tiempo pedir información a la entidad de emisora o enviar datos vía el dispositivo televisivo. Los usuarios o espectadores pueden interactuar con los sistemas de varias maneras, incluyendo, por ejemplo, pidiendo productos o servicios anunciados, chateando con otros espectadores, solicitando información especializada en relación a programas particulares, o navegando a través de páginas de información.

El documento WO 99/66714 se refiere a un sistema donde las restricciones de seguridad están condicionadas por el estado/contexto actual de un dispositivo de recepción. Una política de seguridad puede definir además las condiciones que se pueden controlar, al mismo tiempo que se intenta una función de protección.

En términos generales, en un extremo de esta corriente de comunicación de teledifusión está el receptor decodificador integrado (IRD) del cliente, tal como un decodificador (STB), que recibe el contenido transmitido desde un servidor o cabecera de red. La cabecera de red, generalmente un operador de red en un entorno de televisión interactiva, recoge las señales de varias redes (p. ej. CNN, ESPN, etc.) y las transmite a sus clientes (p. ej. STBs) con una variedad de contenido adicional incluidos los servicios de comercio electrónico y los programas interactivos. El STB se conecta al aparato de televisión y se sitúa típicamente encima de éste. Este IRD opera programas informáticos denominados en este caso como software personalizado que controla el flujo de programas transmitidos, programas interactivos y tráfico de Internet transmitidos desde la cabecera de red del servidor al igual que los datos enviados o recibidos por el espectador a la cabecera de red vía el IRD. El IRD está configurado generalmente para manejar el flujo bidireccional de datos. En un entorno interactivo algunos programas proveen para comunicaciones estrictamente unidireccionales, otros programas proveen para comunicaciones de dos direcciones, y otros programas proporcionan programas opcionales modulares a través de los cuales el espectador puede obtener información adicional sobre un punto de interés. Debido a la integración de muchos formatos de medios diferentes, el IRD también puede ser capaz de reconocer los diferentes formatos de medios del contenido, tal como la diferencia entre la forma y el protocolo de una página web, y la de un anuncio de televisión.

Además, debido al hecho de que cada tipo de comunicación para cada programa tiene su propio nivel de interacción y/o su propio protocolo, puede ser deseable requerir un nivel particular de seguridad para identificar el nivel permitido de interacción para un programa y mantener la integridad de la comunicación. Debido a la naturaleza interactiva del medio, es deseable definir una política de seguridad para regular el tipo de acceso disponible para un espectador y el nivel al que los programas del espectador emitidos en el IRD pueden interactuar con otras entidades, tal como el servidor de cabecera de red, otros clientes y con cualquier otra.

En el pasado, ni la política de seguridad estaba fijada, es decir, conectada directamente al IRD, ni el servidor de cabecera de red formulado y provisto de una política de seguridad para el control de acceso a programas (p. ej., tal como una declaración XML en un fichero asociado a cada programa descargado del servidor al IRD del cliente). La política de seguridad relacionada con los programas emitidos en el IRD se definió típicamente por un módulo de diseño de política. Un administrador de seguridad, un programa emitido en el IRD, moderaba entonces los servicios que realizaba el IRD en relación a la política de seguridad proporcionada.

Existen diferentes paradigmas de políticas de seguridad en el estado de la técnica. Un ejemplo de tal paradigma, el API de JAVA para TV, incluye la arquitectura de la plataforma de seguridad de JAVA 2, que define una estructura que consiste en APIs relacionados con la seguridad para la ejecución de una política de seguridad en un entorno de ejecución de JAVA. El API de JAVA para TV no dicta un modelo o política particular de seguridad, pero usa la arquitectura de seguridad del equipo de desarrollo de JAVA (JDK) 1.2 para expresar las políticas de seguridad proporcionadas por el entorno de la aplicación. Esta solución proporciona a los arquitectos, así como a los operadores de red y a las organizaciones de normalización, la libertad de redefinir sus modelos de seguridad como futura necesidad de cambio. La arquitectura de seguridad de la plataforma de JAVA 2 no asigna por mandato un formato para la política de seguridad, aunque si proporciona una implementación de ejemplo o por defecto. Esta implementación de ejemplo proporciona una amplia política de seguridad del sistema y un fichero específico de política del usuario. En el entorno

de la televisión digital, la plataforma multimedia del hogar (MHP) de la emisión de vídeo digital (DVB) y la *Digital Televisión Application Software Environment* (DASE) del Comité de Sistemas de Televisión Avanzada (ATSc, de sus siglas en inglés) están basados ambos en tecnología JAVA para TV.

Otro ejemplo de un paradigma de implementación de una política de seguridad del estado de la técnica puede encontrarse en las especificaciones 1.0 y 1.1 de la plataforma multimedia del hogar (MHP) (que son instalaciones específicas de la arquitectura de la plataforma de seguridad de JAVA 2 tratada anteriormente). La política de acceso a recursos para MHP se deriva de los derechos de acceso solicitados por la entidad emisora o cabecera de red y de los derechos de acceso concedidos por el usuario. Este método define un formato para una política de seguridad en una base por aplicación vía un "fichero de petición de permiso". El fichero de petición de permiso define aquellos recursos a los que puede acceder la aplicación asociada.

Otro método para designar permisos de seguridad es la *Digital TV Application Software Environment* (DASE). La especificación del nivel 1 de DASE define dos ficheros de política, siendo uno un fichero de permisos de la entidad emisora y el otro aplicado específicamente a las aplicaciones individuales. El fichero de permisos de la entidad emisora se aplica a todas las aplicaciones descargadas ejecutadas y define típicamente aquellas operaciones que la entidad emisora permitirá que ejecute una aplicación. El fichero de permiso de la aplicación define específicamente qué recursos pueden solicitar acceso a qué aplicaciones. La política de seguridad actual implementada por el IRD es la intersección entre la entidad emisora y los ficheros de permiso de la aplicación. El perfil de seguridad global consiste en la política de la entidad emisora y en la política específica asociada a la aplicación. Este método proporciona una implementación de seguridad de dos niveles donde ambos ficheros se transmiten y son asociados específicamente a cada aplicación individual o programa por el administrador de seguridad.

En el entorno de la televisión interactiva, la anchura de banda de comunicación y la capacidad de procesamiento están limitados en el cliente típico. Además, hay numerosos diferentes tipos de aplicaciones, cada uno de estos tipos requiriendo potencialmente su propio conjunto de permisos de seguridad. Así, hay una necesidad de un método y un dispositivo eficaz y flexible para la implementación de una política de seguridad que habilita políticas de seguridad personalizadas para aplicaciones diferentes.

Resumen de la invención

Según la presente invención se proporciona un método para especificar y administrar una política de seguridad jerárquica en un sistema de televisión interactiva, comprendiendo dicho método: formulación de una política de seguridad para aplicaciones que se pueden ejecutar en un dispositivo de cliente del sistema de proceso de datos, donde la formulación de dicha política comprende (i) la identificación de una pluralidad de dichas clases a las que pueden corresponder dichas aplicaciones, (ii) la asignación a cada una de dichas clases de restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través de la que la aplicación dada se ejecuta, y (iii) la organización de las clases en una jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase, creando un objeto de programa de seguridad jerárquica (HSPO, de sus siglas en inglés) que representa dicha política de seguridad, donde el HSPO incluye un nodo para cada clase de la pluralidad de clases, donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica, que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos que definen una clase de aplicaciones y un conjunto de restricciones y/o privilegios correspondientes que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del cual la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores por lo que las restricciones y/o privilegios de los nodos antecesores se agregan a los del nodo de sucesión, transmitiendo el HSPO desde un servidor a un dispositivo de cliente, almacenando el HSPO transmitido en un dispositivo de cliente, en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente: determinando una primera clase de la pluralidad de clases a la que pertenece la primera aplicación, identificando una o más clases y los nodos correspondientes definidos por el HSPO que abarcan la primera clase, identificando restricciones y/o privilegios definidos por los nodos identificados correspondientes, formulando un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definidos por los nodos correspondientes, asignando el conjunto de restricciones y/o privilegios a la primera aplicación, y ejecutando el conjunto de restricciones y/o privilegios en la primera aplicación.

Según otro aspecto, se proporcionan también uno o más medios legibles por ordenador que comprenden instrucciones de programa para especificar y administrar una política de seguridad jerárquica en un sistema de televisión interactivo, donde las instrucciones de programa son ejecutables para: crear un objeto de programa de seguridad jerárquica (HSPO) que representa una política de seguridad para aplicaciones que se pueden ejecutar en un dispositivo de cliente del sistema de proceso de datos, donde el HSPO incluye un nodo para cada clase de la pluralidad de clases a las que pueden corresponder dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del cual la aplicación dada se ejecuta, donde las clases se organizan en una jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase, donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica

que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos que definen una clase de aplicaciones y su correspondiente conjunto de restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del que la aplicación dada se ejecuta, donde los nodos se estructuran en las superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores, transmitir el HSPO de un servidor a un dispositivo de cliente, almacenar el HSPO transmitido en un dispositivo de cliente, en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente: determinación de una primera clase de la pluralidad de clases a la que pertenece la primera aplicación, identificación de una o más clases y los nodos correspondientes definidos por el HSPO, que abarcan la primera clase, identificación de restricciones y/o privilegios definidos por los correspondientes nodos identificados, formulación de un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios está definido por los nodos correspondientes, asignación del conjunto de restricciones y/o privilegios a la primera aplicación, y ejecución del conjunto de restricciones y/o privilegios en la primera aplicación.

Según otro aspecto se proporciona un sistema de televisión interactiva para especificar y administrar una política de seguridad jerárquica, comprendiendo dicho sistema: un servidor configurado para: crear un objeto de programa de seguridad jerárquica (HSPO) que representa una política de seguridad para aplicaciones que se pueden ejecutar en un dispositivo de cliente del sistema, donde el HSPO incluye un nodo para cada clase de una pluralidad de clases a las que pueden corresponder dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del que se ejecuta la aplicación dada, donde las clases se organizan en una jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase, donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos que definen una clase de aplicaciones y su correspondiente conjunto de restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de los nodos antecesores, transmitir el HSPO, un dispositivo de cliente configurado para: recibir el HSPO transmitido, almacenar el HSPO transmitido en el dispositivo de cliente, en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente: determinación de una primera clase de la pluralidad de las clases a la que pertenece la primera aplicación, identificación de una o más clases y los nodos correspondientes definidos por el HSPO que abarcan la primera clase, identificación de restricciones y/o privilegios definidos por los nodos identificados correspondientes, formulación de un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definida por los nodos correspondientes, asignación del conjunto de restricciones y/o privilegios a la primera aplicación, y ejecución del conjunto de restricciones y/o privilegios en la primera aplicación.

Según otro aspecto más, se proporciona un dispositivo para uso en un sistema de televisión interactiva, comprendiendo el dispositivo: un receptor configurado para recibir un objeto de programa de seguridad jerárquica (HSPO) que representa una política de seguridad para aplicaciones que se pueden ejecutar en el dispositivo, donde el HSPO incluye un nodo para cada clase de una pluralidad de clases a las que pueden corresponder dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos del dispositivo a través del que se ejecuta la aplicación dada, donde las clases se organizan en una jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase, donde los nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos que definen una clase de aplicaciones y un conjunto correspondiente de restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos del dispositivo a través del que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores, el almacenamiento se configura para almacenar el HSPO, donde en respuesta a la detección de ejecución de una primera aplicación el dispositivo es configurado para: determinar una primera clase de la pluralidad de clases a la que pertenece la primera aplicación, identificación de una o más clases y los nodos correspondientes definidos por el HSPO que abarcan la primera clase, identificación de restricciones y/o privilegios definidos por los nodos identificados correspondientes, formular un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definida por los nodos correspondientes, asignar el conjunto de restricciones y/o privilegios a la primera aplicación, y ejecutar el conjunto de restricciones y/o privilegios a la primera aplicación.

Se describe una política de seguridad de la entidad emisora que puede ser impuesta por un módulo de diseño de política sobre una clase de entidades en un entorno de televisión interactiva. Se define una política general para una clase de entidades. También puede definirse una política específica para cualquier subclase de entidades, tal como el grupo de anuncios o programas. Se puede definir una política específica para cualquier entidad dada, tal como un programa de televisión específico como una excepción a una clase. Así, el objeto del programa de seguridad jerárquica aquí descrito, puede ser más eficaz y más general que las especificaciones de seguridad conocidas que definen la seguridad y los permisos de seguridad por separado en un fichero proporcionado con cada aplicación individual.

Breve descripción de los dibujos

La figura 1 es un diagrama que ilustra una forma de realización de la distribución de aplicaciones de televisión interactiva, programas de televisión e información de un sistema, desde un servidor fuente de cabecera de red a un cliente.

La figura 2 ilustra una forma de realización de una plataforma de servicio de servidor de cabecera de red y la comunicación de cliente.

La figura 3 es un diagrama que ilustra una forma de realización de un objeto de perfil de seguridad jerárquica.

La figura 4 ilustra una forma de realización de una política de seguridad como aplicada a una aplicación.

Mientras la invención es susceptible de varias modificaciones y formas alternativas, se muestran como ejemplo formas de realización específicas de la misma en los dibujos y serán descritas aquí en detalle. Debe entenderse, no obstante, que los dibujos y su descripción detallada no se destinan a limitar la invención a la forma particular descrita, al contrario, la intención es cubrir todas las modificaciones, equivalentes y alternativas comprendidas dentro del espíritu y alcance de la presente invención tal y como se define en las reivindicaciones anexas.

Descripción detallada

En una estructura de programa típica para televisión interactiva, la presentación de programas de red y aplicaciones interactivas y eventos se controlan por ordenador. Los programas de televisión y los anuncios son ejemplos específicos de aplicaciones de datos y de ordenador. Los propios programas de televisión están típicamente codificados en formato MPEG. Además, la entidad emisora puede insertar también programas informáticos en la corriente transmitida para ser descargados al cliente IRD, a través de los cuales el espectador puede interactuar con la aplicación y/o tomar decisiones de visionado. Suponiendo que el cliente IRD puede ejecutar un programa transmitido, la red debe considerar el riesgo de sabotaje y ambos, daños mal intencionados y no intencionados. Es preciso estar atento para no transmitir ni permitir la transmisión involuntariamente de un virus de TV o de ordenador. Cada programa o aplicación insertada tiene diferentes niveles de interacción requerida o permitida con el espectador y el cliente alojador (es decir, el IRD). Generalmente es preferible desactivar las capacidades que pueden no ser necesitadas o deseadas durante una ejecución de la aplicación, pero que, de otra manera si se permite, podría ser perjudicial para las comunicaciones o para la integridad del entorno y datos operativos en ambos, el servidor de cabecera de red y/o el cliente.

En una forma de realización, un servidor transmite las restricciones o los permisos de seguridad a un cliente receptor (p. ej., el STB) que el servidor desea imponer al cliente transmitiendo un objeto de política de seguridad jerárquica (HSPO) al cliente. El HSPO proporciona una estructura de herencia de seguridad. En una forma de realización, el HSPO puede ser un objeto (p. ej., un único fichero), pero puede estar distribuido alternativamente por muchos de estos objetos. En una forma de realización, el HSPO puede estar programado como un árbol con una raíz. La raíz del árbol de HSPO contiene las restricciones y excepciones de seguridad más generales y universales, tales como las restricciones de seguridad para la cabecera de red, que están impuestas por ejemplo, en todas las redes y contenidos transmitidos por el servidor. La sucesiva ramificación de los nodos fuera de la raíz del HSPO contiene requisitos de seguridad más específicos, aumentando el nivel de especificidad con el aumento de la distancia u "orden" a los nodos de la raíz.

Cada nodo del árbol de HSPO representa una clase o subclase de aplicaciones y las restricciones adicionales, o privilegios adicionales, que el receptor del cliente impone o atribuye a entidades tales como aplicaciones en la clase o subclase correspondiente. El conjunto final de restricciones/privilegios que es impuesto/concedido a una aplicación dada, se deriva (típicamente por un administrador de seguridad con un receptor IRD) de este HSPO al seguir un procedimiento definido para combinar los nodos apropiados del árbol de HSPO junto con cualquiera de las restricciones adicionales impuestas por el cliente (es decir, el IRD). Así, una aplicación hereda los atributos de seguridad de la clase a la que ésta pertenece y todos los atributos de seguridad de los nodos predecesores en el árbol de HSPO. Por ejemplo, en una forma de realización, el nodo más bajo del árbol que corresponde a la aplicación se identifica, y se forma una unión de todas las restricciones/privilegios de los nodos antecesores de este nodo. Ésta se prueba como eficaz ya que la implementación de una nueva aplicación, deliberadamente, requiere la especificación de un conjunto más pequeño de requisitos de seguridad en el momento de la implementación. Es decir, sólo las excepciones a la política de seguridad existente necesitan ser especificadas para un grupo de aplicaciones o una aplicación individual. Por consiguiente, los tipos arbitrarios de aplicaciones pueden tener un conjunto uniforme de requisitos de seguridad impuestos automáticamente.

Los nodos que se ramifican del nodo de raíz de HSPO pueden representar una red o una clase de aplicaciones tales como anuncios o programas de red, y los nodos subordinados a estos nodos segmentan estas clases de seguridad en más subclases. Generalmente, el nivel de seguridad en un nivel de clase es más o menos restrictivo que en su superclase. Los niveles de seguridad pueden variar también en el mismo nivel de clase.

Volviendo ahora a la figura 1, se muestra un diagrama que ilustra una forma de realización de una arquitectura para la transmisión o distribución de aplicaciones de televisión interactivas, programas de televisión (audio y vídeo) e

información de sistema (p. ej., números de servicios, nombres de servicios, nombres de eventos, horarios de eventos) incluyendo el HSPO de un servidor fuente de cabecera de red a un espectador STB. El HSPO se puede transmitir o teletransmitir una vez o periódicamente a los clientes. Alternativamente el HSPO puede ser programado en la memoria del cliente por el fabricante, descargado de Internet, instalado vía un medio legible por ordenador, o recibido vía una conexión igual a igual (PTP, por sus siglas en inglés) o por correo electrónico. El sistema incluye un servidor de cabecera de red 20, que se puede acoplar con un dispositivo de vídeo y audio (no mostrado) que alimenta un vídeo particular con audio asociado a la cabecera de red. La señal interactiva de audio-vídeo contiene programas de televisión o contenido similar de audio-vídeo, al igual que otras señales asociadas a contenido interactivo, tales como señales de control, información de sistema, HSPO y aplicaciones interactivas. La información de vídeo se puede digitalizar en la cabecera de red 20 y transmitir vía un transmisor a un sistema receptor de cliente 24. La información transmitida por el servidor de cabecera de red 20 se transmite al sistema receptor 24 de varias maneras. Por ejemplo, la información transmitida se puede enviar al sistema receptor 24 vía una señal transmitida tal como una transmisión por satélite. La estación de recepción 24 está configurada también para recibir señales vía un canal de módem, cable u ondas terrestres. El sistema receptor de cliente 24 puede comprender, por ejemplo, una televisión 26 conectada a un decodificador 28, un miniordenador portátil o un teléfono móvil (no mostrado). Si se usa la transmisión por satélite, el STB 28 puede incluir una antena de recepción 30 para recibir información de un satélite 32. La antena 30 de la estación de recepción pasa la señal de televisión interactiva al cliente (p. ej., STB 28), que ejecuta las funciones de procesamiento de la estación de recepción 24. Una vez que la información se recibe a través de la antena de recepción 30, se puede procesar por el cliente (p. ej. STB 28) y visualizar en el aparato 26. De esta manera, el audio, el vídeo y los datos interactivos se pueden recibir y procesar por el STB 28. Las señales transmitidas vía los canales de emisión o de módem incorporan varios módulos que comprenden componentes de una aplicación interactiva. Los módulos contienen cualquier tipo de datos tales como código de aplicación, datos brutos o información gráfica, por ejemplo.

La información de sistema proporcionada al decodificador 28 incluye también una lista de servicios (p. ej. CNN, MTV, ESPN) a disposición de un espectador, nombres de eventos (p. ej. Dateline, Star Trek) y un horario de los eventos (p. ej., hora/fecha de inicio y duración). La pasarela de servicio 246 proporciona un enlace de comunicación entre el cliente (p. ej., el STB 28) y la plataforma de servicio (servidor de cabecera de red) 50 de la figura 2.

El uso de un objeto de política de seguridad jerárquica (HSPO) para imponer las restricciones o permisos de seguridad en un cliente receptor (p. ej., el STB 28 de la figura 1) puede ser útil en cualquier sistema de computación distribuido con un servidor para determinar una política de seguridad para uno o más dispositivos de cliente. En una forma de realización, el sistema de computación distribuido comprende un sistema de televisión interactiva, como se describe a continuación conjuntamente con la descripción de la figura 2.

Volviendo ahora a la figura 2, se muestra una ilustración de una forma de realización de un entorno de una plataforma de servicio (SP) de un servidor de cabecera de red 50 desde el cual se puede formular y teletransmitir el módulo de diseño de política y el HSPO. Se indica, no obstante, que el módulo de diseño de política puede residir alternativamente en un STB tal como el STB 28 de la figura 1. Los servicios 200 pueden proporcionar compras, chat y otros servicios a través de un enlace de comunicación tal como Internet u otra red o canales de comunicación accesibles a un operador de red. El SP 50 comunica sucesivamente con un cliente 212 vía uno o más enlaces de comunicación 211. El cliente 212 puede ser un STB, un asistente digital, un teléfono móvil, o cualquier otro dispositivo de comunicación capaz de comunicarse con el SP 50 a través del enlace de comunicación 210. Al usar el SP 50, el operador de red puede acceder a los servicios 200. Las funciones de negocio 206, que comprende el administrador de servicio 238, interactúan con el administrador carrusel 254 para recuperar el contenido de un servicio 200. El carrusel comprende una corriente de repetición de teletransmisión de datos de audio/vídeo/interactivos a clientes del SP 50. El administrador carrusel 254, el administrador de transacción 242 y el administrador de servicio 238 controlan la inserción y supresión de contenido del carrusel de teletransmisión.

En una forma de realización, la creación del HSPO y la funcionalidad del módulo de diseño de política pueden existir en el administrador de servicio 238. En una forma de realización alternativa, la funcionalidad del módulo de diseño de política del HSPO se puede localizar en el cliente. El contenido de servicio se puede recuperar y convertir en un formato adecuado para el SP por el H2O 248. Por ejemplo, el H2O 248 se puede configurar para convertir el contenido HTML en contenido legible por el cliente SP. El contenido convertido es formateado en una carrusel de datos y multiplexado por la cinta continua abierta 256 para la emisión al cliente 212. El cliente 212 interactúa con los servicios y, si es necesario y permitido por el HSPO, se comunica con el SP 50 y los servicios 200. La comunicación de red punto a punto (PTP) entre el STB y el SP va a través de la pasarela de servicio (SGW) 246.

Volviendo ahora a la figura 3, se muestra un diagrama con estructura de árbol de una forma de realización de un objeto de perfil de seguridad jerárquica (HSPO). El HSPO 300 puede ser un HSPO para una red de emisión ejemplar NBS. La cabecera de red formula el HSPO 300 para el NBS y lo transmite a todos sus telespectadores/receptores o clientes/STBs. La política de raíz NBS 302 divide sus aplicaciones en 3 grupos o clases: "política de aplicación OTV" 310, "política de anuncios" 312 y "política de aplicación HTML" 314. Una cuarta clase puede existir implícitamente y por defecto, y consiste en todas aquellas aplicaciones no incluidas en las otras tres clases definidas explícitamente. En la forma de realización ilustrada de la figura 3, la clase "política de aplicación OTV" 310 contiene entradas para dos aplicaciones, "política de aplicación del tiempo" 316 y "política de aplicación de La isla de Gilligan" 318. La clase "política de anuncios" 312 incluye una "política de aplicación Coca Cola™" 320. La clase "política de aplicación HTML" 314 está además subdividida en la política de aplicación de la guía electrónica de programas (EPG) 322 bajo la cual la entidad de emisión define las restricciones adicionales especiales para la aplicación "política de guía de TV" 324.

En términos generales, las políticas de seguridad en el nivel NBS 302 se deben aplicar a todos los elementos de la misma clase y de las clases subordinadas. Así, para el nivel de red NBS 302 que estaría por debajo del nivel de la cabecera de red, la política de seguridad establecida por el módulo de diseño de política se define por el NBS. A este nivel, se impone un grado alto de seguridad. Típicamente, cada nivel de grupo de tipo de aplicación impone una seguridad diferente basada en los requisitos de seguridad específicamente deseados y seleccionados para cada grupo. Por ejemplo, debido a su naturaleza fiable, a las aplicaciones de la clase "política de aplicación OTV" 310, que en una forma de realización están escritas en código "C", se les permite una política de seguridad menos restrictiva que a aquellas de la clase "política de anuncios" 312. Esto se debe a que las aplicaciones de OTV vienen de una fuente fiable y se consideran menos arriesgadas. Así, las aplicaciones de OTV pueden estar provistas de un conjunto más permisivo, menos restrictivo de restricciones de seguridad. De forma similar, las aplicaciones en el mismo nivel de clase pueden tener niveles de seguridad que difieren. Por ejemplo, a la aplicación "política de aplicación del tiempo" 316 se le permiten más habilidades, debido a su carácter fiable de una fuente conocida, que a la aplicación "política de aplicación de La isla de Gilligan" 318, que puede originarse de una fuente sindicada externa y por ello se considera menos fiable.

En este ejemplo, se asume que el receptor/cliente STB ya tiene una copia del HSPO 300 bien transmitido previamente desde la cabecera de red, descargado de Internet o programado en la memoria del cliente. Cuando la estación de TV pide que el receptor arranque la aplicación asociada con, por ejemplo, el anuncio de "Coca Cola™", el receptor IRD debe determinar primero qué restricciones de seguridad impone sobre la aplicación. El IRD/receptor coge aquellas restricciones definidas por el nivel máximo o política "raíz" 302, por ejemplo, "sin control del ciclo de vida", añade cualquier restricción adicional definida por la política "de anuncios" 312, por ejemplo "sin acceso al módem", y finalmente incluye las restricciones definidas específicamente para la "política de aplicación Coca Cola™" 320, por ejemplo "sin cookies." La política de seguridad resultante de la entidad de emisión para la aplicación "Coca Cola™" podría, por ejemplo, ser la unión de estas políticas definidas en el HSPO: "sin control del ciclo de vida, sin acceso al módem, sin cookies", es decir, el nodo hereda los atributos de seguridad de su clase y todos los nodos precedentes del árbol de HSPO.

Como se muestra en la figura 4, la política de seguridad real 405 implementada impuesta a cualquier aplicación comprende una combinación de características heredadas de aquellas definidas por el HSPO 401, cualquier política que acompañe a la misma aplicación 402, y cualquier política definida en el IRD 403 (p. ej., por el espectador).

Volviendo a la figura 3, como otra ilustración, el IRD/receptor puede computar una política de seguridad aplicada a una aplicación asociada con un anuncio de "Ford" de forma similar. No obstante, aunque "Ford" está contenida en la clase "política de anuncios" 312, no hay nodo de política "Ford" bajo el nodo "anuncios". En este caso, el anuncio de Ford sólo tendría las restricciones de la entidad de emisión especificadas por los nodos "raíz" 302 y "anuncios" 312, a saber "sin control del ciclo de vida, sin acceso al módem." Nuevamente, estas restricciones se combinarán luego con cualquier información de acceso proporcionada con el anuncio de "Ford" y se obtendrán del mismo IRD para crear la política resultante obligatoria en la aplicación como se ha descrito anteriormente conjuntamente con la descripción de la figura 4.

La utilización de las restricciones de seguridad del HSPO puede prevenir la necesidad de transmitir un conjunto de restricciones de seguridad de la entidad de emisión con cada programa de teletransmisión. El HSPO puede ser más eficaz, ya que un HSPO necesita ser transmitido sólo una vez, o programado en un STB de cliente. A partir de entonces, sólo las excepciones al HSPO establecido pueden precisar ser transmitidas para una aplicación. Una vez se establece una excepción en el HSPO, se vuelve parte del árbol de HSPO y no necesita ser transmitida nuevamente.

Las restricciones de seguridad del HSPO pueden ser útiles para prevenir la teletransmisión o descarga de programas a un cliente desde un servidor de cabecera de red al realizar acciones consideradas arriesgadas por ese servidor, tal como contraer un virus por interacción con el mundo exterior (es decir, Internet, correo electrónico u otros programas internos o externos al cliente (p. ej., el STB)).

Las restricciones de seguridad del HSPO pueden deshabilitar también las capacidades o el acceso a lugares de memoria y datos, lo que puede ocurrir inesperadamente debido a un error de programación. El HSPO también puede permitir el acceso o denegar el acceso a datos encriptados y/o protegidos.

En una forma de realización, cada nivel de una estructura de HSPO se puede especificar por una entidad diferente. Por ejemplo, en el nivel más alto, una cabecera de red define una restricción de seguridad de nivel máximo, tal como "sin ejecución JAVASCRIPT" durante un programa. Además, una cadena (p. ej., HBO, NBC, ABC, CBS, ESPN, etc.) puede añadir restricciones de seguridad adicionales al programa, (p. ej., sin acceso al módem al siguiente nivel de nodo de red en el HSPO). En el siguiente nivel de nodo de HSPO, un productor de programa puede especificar una restricción de seguridad adicional para el programa. En el siguiente nivel, un productor publicitario puede especificar una restricción de seguridad adicional para el programa o incluso una política más permisiva para el programa que la heredada de la estructura jerárquica del HSPO y así sucesivamente.

Dependiendo del HSPO existente y de la política de seguridad, puede aceptarse una política de anuncios más permisiva o no. En una forma de realización, un objeto de seguridad de nivel inferior puede anular una restricción de seguridad heredada de un nodo de HSPO de un nivel más alto.

Se observa que aunque las formas de realización descritas anteriormente, han sido descritas como si residieran en un entorno de televisión interactiva, se contempla que otras formas de realización puedan residir en y/u operar en cualquier sistema informático distribuido incluyendo un servidor y un dispositivo de cliente. El dispositivo de cliente puede ser un ordenador portátil, un teléfono móvil, un asistente personal digital o cualquier dispositivo capaz de recibir y/o transmitir una señal electrónica. El servidor puede ser cualquier dispositivo capaz de transmitir y/o recibir una señal electrónica. Además, las formas de realización descritas anteriormente se pueden implementar como un conjunto de instrucciones conducido vía un medio portador tal como una señal de emisión, o en un medio legible por ordenador, comprendiendo ROM, RAM, CD ROM, Flash o cualquier otro medio legible por ordenador, por ahora conocido o desconocido, de manera que cuando es ejecutado causa la implementación en el ordenador de las formas de realización descritas anteriormente.

Aunque las formas de realización anteriores han sido descritas con una cantidad considerable de detalles, numerosas variaciones y modificaciones se harán aparentes a aquellos expertos en la técnica una vez la descripción anterior sea apreciada completamente. Se pretende que las siguientes reivindicaciones sean interpretadas para abarcar todas esas variaciones y modificaciones.

REIVINDICACIONES

1. Método para especificar y administrar una política de seguridad jerárquica en un sistema de televisión interactiva, comprendiendo dicho método:

formulación de una política de seguridad para aplicaciones que pueden ejecutarse en un dispositivo de cliente del sistema de televisión, donde la formulación de dicha política comprende

(i) identificación de una pluralidad de clases a las que pueden corresponder dichas aplicaciones,

(ii) asignación a cada una de dichas clases de restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente a través del cual se ejecuta la aplicación dada, y

(iii) organización de las clases en un jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase,

creación de un objeto de programa de seguridad jerárquica (HSPO) (300) que representa dicha política de seguridad, donde el HSPO incluye un nodo para cada clase de la pluralidad de clases, donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos (302, 310, 312, 316 ...) que definen una clase de aplicaciones y un conjunto correspondiente de restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente en el que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores, de modo que las restricciones y/o privilegios de nodos antecesores se agregan a los del nodo de sucesión,

transmisión del HSPO (300) de un servidor (206) a un dispositivo de cliente (212),

almacenamiento del HSPO transmitido en un dispositivo de cliente,

en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente:

determinación de una primera clase de la pluralidad de clases a la que pertenece la primera aplicación,

identificación de una o más clases y nodos correspondientes definidos por el HSPO que abarcan la primera clase,

identificación de restricciones y/o privilegios definidos por los correspondientes nodos identificados,

formulación de un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definida por los nodos correspondientes,

asignación del conjunto de restricciones y/o privilegios a la primera aplicación, y ejecución del conjunto de restricciones y/o privilegios en la primera aplicación.

2. Uno o más medios legibles por ordenador comprendiendo instrucciones de programa para especificar y administrar una política de seguridad jerárquica en un sistema de televisión interactivo, donde las instrucciones de programa son ejecutables para:

crear un objeto de programa de seguridad jerárquica (HSPO) (300) que representa una política de seguridad para aplicaciones que se pueden ejecutar en un dispositivo de cliente del sistema de televisión, donde el HSPO incluye un nodo para cada clase de la pluralidad de clases a las que corresponden dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que una aplicación dada tiene en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente en el que la aplicación dada se ejecuta, donde las clases se organizan en una jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada, representa una subclase de la superclase,

donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos (302, 310, 312, 316 ...) que definen una clase de aplicaciones y un conjunto correspondiente de restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente en el que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores,

transmitir el HSPO (300) desde un servidor (206) a un dispositivo de cliente (212),

almacenar el HSPO transmitido en un dispositivo de cliente,

en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente:

determinar una primera clase de la pluralidad de clases a la que pertenece la primera aplicación,

identificar una o más clases y nodos correspondientes definidos por el HSPO que abarcan la primera clase,

identificar restricciones y/o privilegios definidos por los correspondientes nodos identificados,

formular un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios viene definido por los nodos correspondientes,

asignar el conjunto de restricciones y/o privilegios a la primera aplicación, y

ejecutar el conjunto de restricciones y/o privilegios en la primera aplicación.

3. Método según la reivindicación 1 o medios legibles por ordenador según la reivindicación 2, donde dicho HSPO se descarga a un dispositivo de cliente vía una red de ordenador (211).

4. Método según la reivindicación 1 o medios legibles por ordenador según la reivindicación 2, donde el HSPO se recibe en un dispositivo de cliente, y donde las instrucciones de programa son además ejecutables para programar un HSPO predeterminado en el dispositivo del cliente.

5. Método según la reivindicación 1 o medios legibles por ordenador según la reivindicación 2, donde el HSPO define una segunda clase de restricciones y/o privilegios, siendo dicha segunda clase una superclase de la primera clase, y donde el conjunto de restricciones y/o privilegios comprende una unión de la primera clase de restricciones y/o privilegios y la segunda clase de restricciones y/o privilegios.

6. Método o medios legibles por ordenador según la reivindicación 5, donde la primera clase comprende una clase publicitaria y la segunda clase comprende una clase de red.

7. Método o medios legibles por ordenador según la reivindicación 5, donde las clases de HSPO se definen por un módulo de diseño de política de seguridad (238) localizado bien en el servidor o en un dispositivo de cliente que recibe el HSPO transmitido.

8. Sistema de televisión interactivo para especificar y administrar una política de seguridad jerárquica, comprendiendo dicho sistema:

un servidor (206) configurado para:

crear un objeto de programa de seguridad jerárquica (HSPO) (300) que representa una política de seguridad para aplicaciones que se pueden ejecutar en un dispositivo de cliente del sistema, donde el HSPO incluye un nodo para cada clase de una pluralidad de clases a las que corresponden dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente en el que la aplicación dada se ejecuta, donde las clases se organizan en un jerarquía con dos o más niveles, comprendiendo la jerarquía superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase,

donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos (302, 310, 312, 316 ...) que definen una clase de aplicaciones y un conjunto correspondiente de restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos de un dispositivo de cliente en el que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores,

transmitir el HSPO (300),

un dispositivo de cliente (212) configurado para:

recibir el HSPO transmitido,

almacenar el HSPO transmitido en el dispositivo de cliente,

en respuesta a la detección de ejecución de una primera aplicación en el dispositivo de cliente:

determinar una primera clase de la pluralidad de clases a la que pertenece la primera aplicación,

identificar una o más clases y los nodos correspondientes definidos por el HSPO que abarcan la primera clase,

identificar restricciones y/o privilegios definidos por los nodos identificados correspondientes,

formular un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definida por los nodos correspondientes,

asignar el conjunto de restricciones y/o privilegios a la primera aplicación, y

ejecutar el conjunto de restricciones y/o privilegios en la primera aplicación.

9. Dispositivo (212) para uso en un sistema de televisión interactivo, comprendiendo el dispositivo:

receptor configurado para recibir un objeto de programa de seguridad jerárquica (HSPO) (300) que representa una política de seguridad para aplicaciones que se pueden ejecutar en el dispositivo, donde el HSPO incluye un nodo para cada clase de una pluralidad de clases a los que pueden corresponder dichas aplicaciones, siendo asignadas a cada una de dichas clases restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos del dispositivo en el que la aplicación dada se ejecuta, donde las clases se organizan en una jerarquía con dos o más niveles, comprendiendo la superclases y subclases, donde una subclase de una superclase dada representa una subclase de la superclase,

donde dichos nodos se organizan como una estructura de herencia de seguridad jerárquica que corresponde a dicha jerarquía, incluyendo cada nivel de la estructura uno o más nodos (302, 310, 312, 316 ...) que definen una clase de aplicaciones y un conjunto correspondiente de restricciones y/o privilegios que tiene una aplicación dada en la clase correspondiente para acceder a uno o más recursos del dispositivo en el que la aplicación dada se ejecuta, donde los nodos se estructuran en superrelaciones y/o relaciones subordinadas de nodo con otros nodos, y donde los nodos se configuran para heredar las restricciones y/o privilegios de nodos antecesores,

almacén configurado para almacenar el HSPO,

donde en respuesta a la detección de ejecución de una primera aplicación, el dispositivo es configurado para:

determinar una primera clase de la pluralidad de clases a la que pertenece la primera aplicación,

identificar una o más clases y los nodos correspondientes definidos por el HSPO que abarca la primera clase,

identificar restricciones y/o privilegios definidos por los nodos identificados correspondientes,

formular un conjunto de restricciones y/o privilegios, donde dicho conjunto de restricciones y/o privilegios comprende una unión de restricciones y/o privilegios definida por los nodos correspondientes,

asignar el conjunto de restricciones y/o privilegios a la primera aplicación, y ejecutar el conjunto de restricciones y/o privilegios en la primera aplicación.

10. Dispositivo según la reivindicación 9, donde el HSPO se recibe vía una red de ordenador (211).

11. Sistema según la reivindicación 8 o dispositivo según la reivindicación 9, donde el HSPO define una segunda clase de restricciones y/o privilegios, siendo dicha segunda clase una superclase de la primera clase, y donde el conjunto de restricciones y/o privilegios comprende una unión de la primera clase de restricciones y/o privilegios y la segunda clase de restricciones y/o privilegios.

12. Sistema o dispositivo según la reivindicación 11, donde la primera clase comprende una clase publicitaria y la segunda clase comprende una clase de red.

13. Sistema o dispositivo según la reivindicación 11, donde las clases de HSPO se definen por un módulo de diseño de política de seguridad (238) localizado bien en el servidor o en un dispositivo de cliente que recibe el HSPO transmitido.

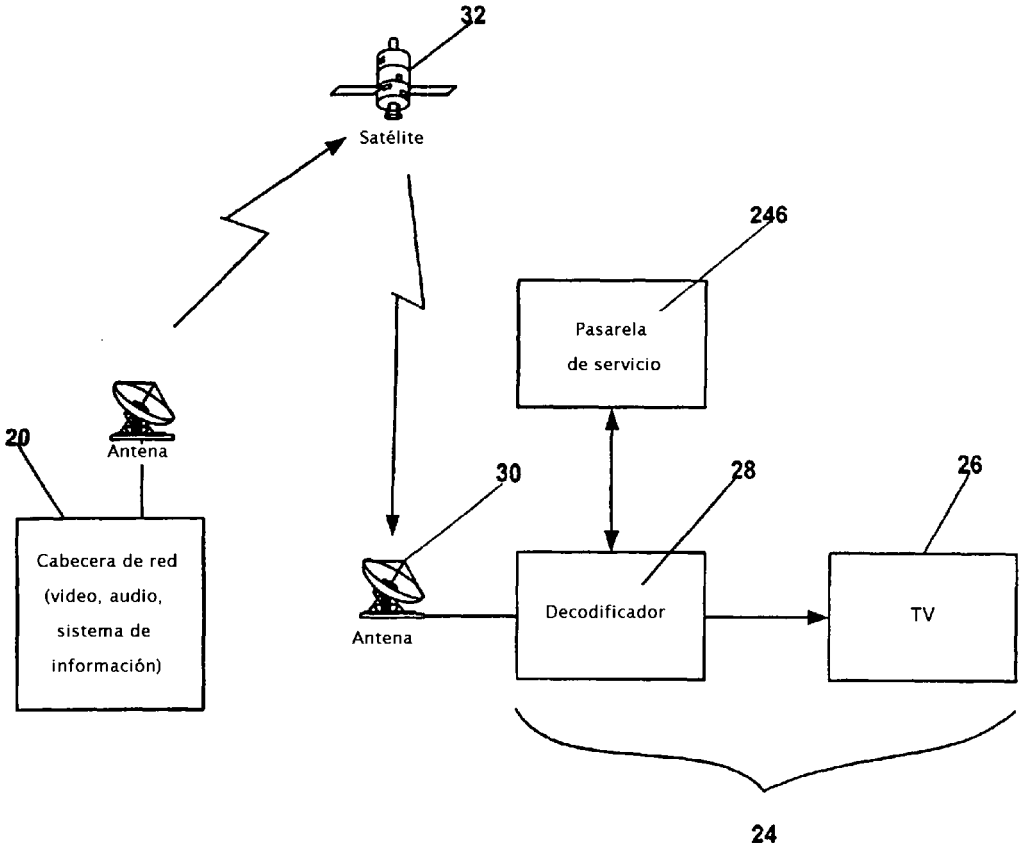
32
Satélite
246
Pasarela
de servicio
20
Antena
Cabecera de red
(vídeo, audio,
sistema de
información)
30
Antena
28
Decodificador
26
TV
24

Figura 1

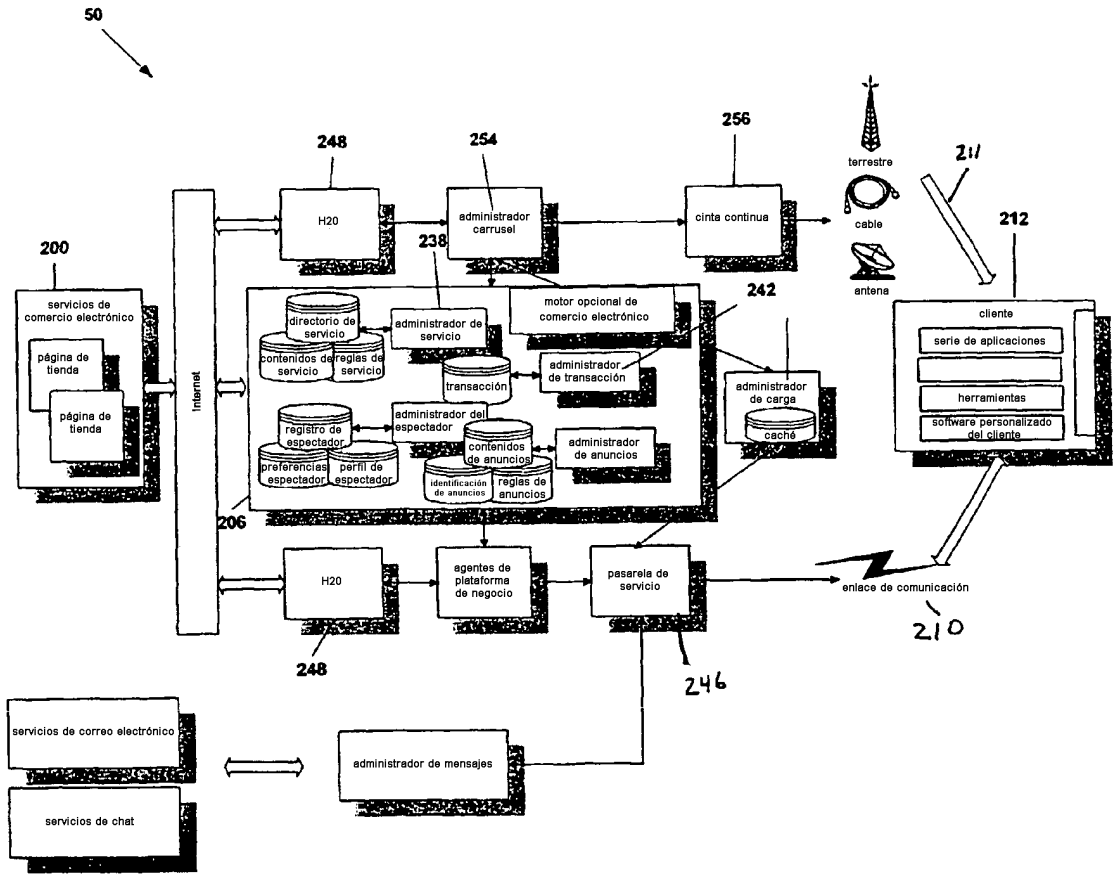
50
248
254
256
terrestre
211
cable
212
200
238
antena
servicios de comercio electrónico
página de tienda
página de tienda
Internet
H20
administrador carrusel
cinta continua
motor opcional de comercio electrónico
242
cliente
serie de aplicaciones
herramientas
software personalizado del cliente
directorio de servicio
administrador de servicio
contenidos de servicio
reglas de servicio
transacción
administrador de transacción
administrador de carga
caché
registro de espectador
administrador del espectador
contenidos de anuncios
administrador de anuncios
preferencias espectador
perfil de espectador
identificación de anuncios
reglas de anuncios
206
H20
agentes de plataforma de negocio
pasarela de servicio
enlace de comunicación
210
248
246
servicios de correo electrónico
servicios de chat
administrador de mensajes

Figura 2

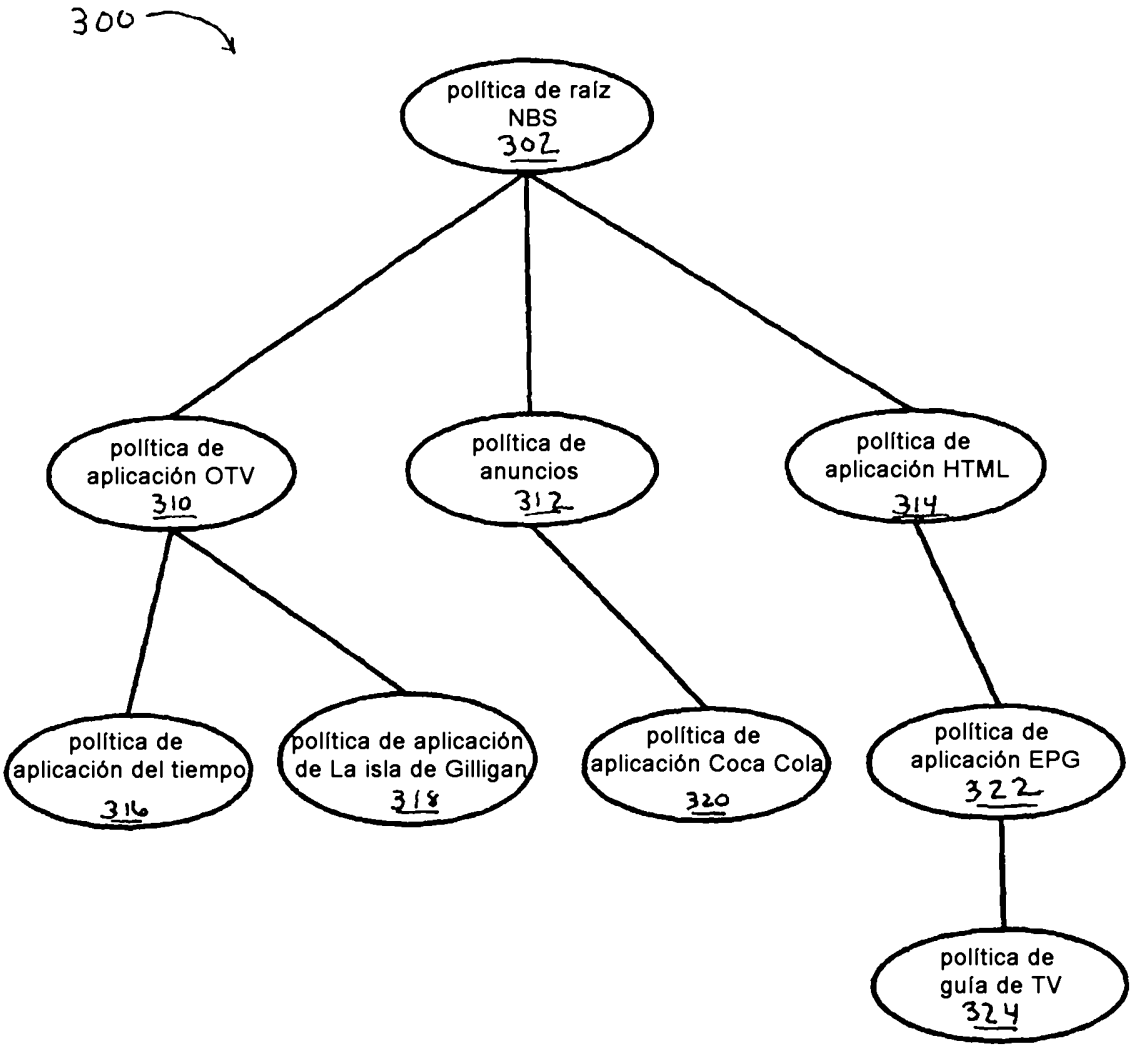
300
política de raíz NBS 302
política de aplicación OTV 310
política de anuncios 312
política de aplicación HTML 314
política de aplicación del tiempo 316
política de aplicación de La isla de Gilligan 318
política de aplicación Coca Cola 320
política de aplicación EPG 322
política de guía de TV 324

Figura 3

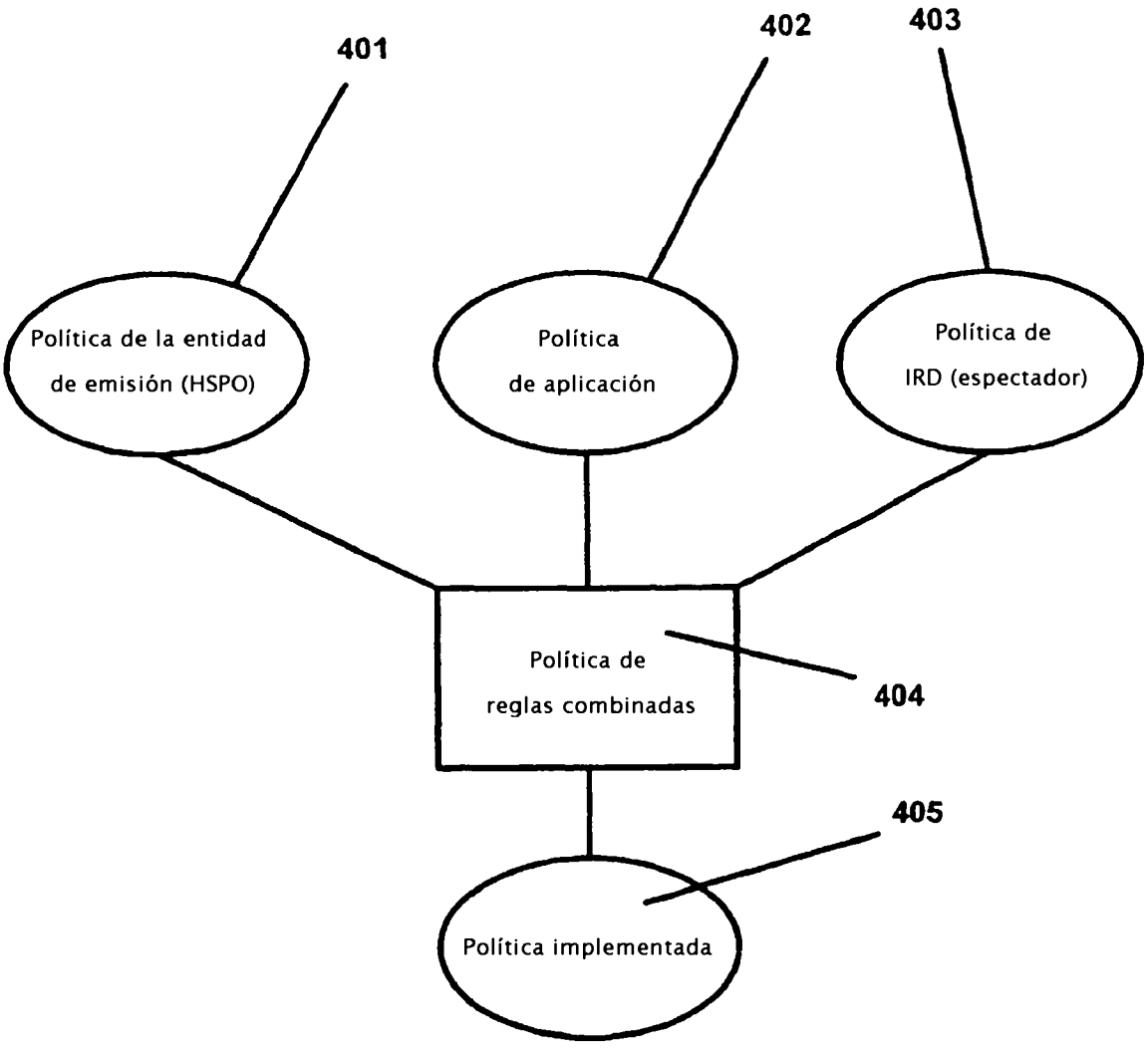
401
402
403
Política de la entidad de emisión (HSPO)
Política de aplicación
Política de IRD (espectador)
Política de reglas combinadas
404
405
Política implementada

Figura 4