(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 346 825**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08705099 .3**
(96) Fecha de presentación : **17.01.2008**
(97) Número de publicación de la solicitud: **2103073**
(97) Fecha de publicación de la solicitud: **23.09.2009**

(54) Título: **Método y sistema para controlar un programa de aplicación de ordenador.**

(45) Fecha de publicación de la mención BOPI:
20.10.2010

(45) Fecha de la publicación del folleto de la patente:
20.10.2010

(73) Titular/es: **DLB Finance & Consultancy B.V.**
Laakseweg 24
4874 Lv Etten-Leur, NL
HITD Information Technology B.V.

(72) Inventor/es: **Benschop, Dirk, Leonard y**
Benschop, Henderik, Reinout

(74) Agente: **Isern Jara, Jorge**

DESCRIPCIÓN

Método y sistema para controlar un programa de aplicación de ordenador.

Sector de la invención

La invención se refiere al sector de la comunicación electrónica con utilización de uno o varios ordenadores.

Antecedentes de la invención

Con la proliferación de Internet, los sistemas principales pueden proporcionar sus servicios a numerosos sistemas de clientes, de manera que tanto los sistemas principales como los de clientes están distribuidos por todo el mundo. Una vez establecida la conexión apropiada, la información puede pasar libremente entre un sistema principal y un sistema de cliente.

Por ejemplo, en una red convencional distribuida, una serie de sistemas principales o servidores se encuentran en comunicación con una serie de sistemas de cliente con intermedio de una red o conjunto de redes, por ejemplo, Internet. La arquitectura de dicha red distribuida es una fuente de fortaleza (por ejemplo, posibilitando el libre flujo de información entre numerosos sistemas) y una fuente de vulnerabilidad (por ejemplo, creando vulnerabilidad a ataques malintencionados).

Específicamente, cuando un sistema de cliente intenta establecer una conexión, por ejemplo, una conexión TCP (Transmission Control Protocol ("Protocolo de Control de Transmisión")) a un sistema principal, el cliente y el sistema principal intercambian una secuencia de mensajes o paquetes. El enfoque general es aplicable a la totalidad de conexiones TCP: Web, telnet, email y otras. Cuando se ha establecido la conexión, el sistema del cliente puede enviar peticiones al sistema principal, por ejemplo, peticiones de contenidos.

A efectos de impedir o de reducir acciones malintencionadas del sistema de cliente al sistema principal, se conocen habitualmente las llamadas barreras o cortafuegos ("firewalls"). Una barrera es una aplicación específica o software específico que inspecciona el tráfico de la red que pasa por la misma y autoriza o no el paso basándose en una serie de normas.

Existe una serie de clasificaciones de barreras dependiendo del lugar en el que está teniendo lugar la comunicación, el lugar en el que la comunicación es interceptada y el estado que se está localizando. Las barreras por capas de redes, también llamadas filtros de paquetes, funcionan a un nivel relativamente bajo de la pila de protocolos TCP/IF, no permitiendo que pasen los paquetes a través de la barrera, excepto en el caso en que se adapten a un conjunto de normas establecidas. Éstas filtran el tráfico basándose en las características de los paquetes. El administrador de la barrera puede definir las normas; o podrían ser aplicables normas por defecto. Los barreras de redes por capas se subdividen en general en dos subcategorías. Una barrera de estado ("stateful") es una barrera que efectúa el seguimiento del estado de las conexiones de red (tales como flujos TCP, comunicación UDF) que se desplazan por las mismas. La barrera está programada para distinguir paquetes legítimos para diferentes tipos de conexiones. Solamente se permitirán por la barrera los paquetes con un estado de conexión conocido, mientras que otros paquetes serán rechazados. Las barreras sin estado ("stateless") tienen capacidad para el filtrado de paquetes, pero no pueden realizar decisiones más complejas sobre la etapa que han alcanzado las comunicaciones entre sistemas principales.

Las barreras de aplicaciones por capas actúan sobre el nivel de aplicación del apilamiento TCP/IP (es decir, todo el tráfico de navegador o todo el tráfico telnet o ftp), y pueden interceptar todos los paquetes que se desplazan hacia o desde una aplicación. En principio, las barreras de aplicación pueden impedir que llegue a las máquinas protegidas cualquier tráfico externo no deseado. Estas barreras inspeccionan los paquetes buscando contenido impropio. Una barrera XML es un ejemplo de tipos recientes de barrera de aplicación por capas. Un ejemplo de esta barrera es el que da a conocer el documento EP 1 296 252.

El documento WO 02/075547 da a conocer un método de seguridad de aplicación por capas y un sistema para proteger una aplicación contra la realización de solicitudes operativas ilegales o perjudiciales recibidas desde un entorno que suscita desconfianza. El método aplica una o varias conexiones ("pipes") al contenido de una aplicación por capas de una petición operativa para determinar si la petición operativa es ilegal o perjudicial. En uno de los conductos, una ruta de la aplicación está designada como restringida. El destino de una petición operativa es determinado entonces y bloqueado si el destino corresponde a la ruta de aplicación designada.

El documento US 2005/0273857 da a conocer un sistema y metodología para la detección y prevención de intrusiones. Las descripciones de las intrusiones se definen como ataques específicos que pueden ser intentados por tráfico de red malintencionado, indicando las descripciones de intrusión aplicaciones específicas que pueden ser objetivo de ataques individuales. Para una aplicación específica que participa en una comunicación en red, se deriva un subconjunto de las descripciones de intrusión que es aplicable específicamente a dicha aplicación particular. El subconjunto es utilizado para monitorizar tráfico de red destinado a la aplicación particular para detectar un intento de intrusión en la red. Si se detecta una intrusión en la red, los destinos de tráfico de la red para la aplicación particular, que se ha determinad que comprenden ataque, quedan bloqueados.

Las capas de barreras o cortafuegos de la red son desventajosas por el hecho de que se deben disponer y mantener complejos juegos de normas. Por otra parte, las barreras de capas de aplicación son desventajosas por el hecho de que la exploración del contenido de los paquetes requiere una cantidad considerable de recursos y/o puede requerir una cantidad significativa de tiempo.

Existe la necesidad en esta técnica de un sistema de seguridad mejorado capaz, por ejemplo, de ahorrar recursos.

Resumen de la invención

Método implementado mediante ordenador para el control de un programa de aplicación de ordenador en un sistema de ordenador configurado para comunicación electrónica con un cliente, tal como se define en la reivindicación 1.

Se da a conocer asimismo un programa de ordenador para llevar a cabo el método y medios legibles por ordenador que contienen dicho programa de ordenador.

También se da a conocer un sistema de ordenador para controlar un programa de aplicación de ordena-

dor, tal como se define en la reivindicación 15.

La petición de cliente puede comprender, por ejemplo, una instrucción para el programa de aplicación de ordenador.

Se debe observar que el primer conjunto de peticiones permisibles puede comprender una selección de una serie (grande) de peticiones válidas para dicho programa de aplicación de ordenador.

El método y sistema que se proponen combinan una mayor seguridad con una menor aplicación de recursos. De modo general, un programa de aplicación de ordenador es capaz de manejar una serie de peticiones, frecuentemente una cantidad (muy) grande de peticiones. El método y sistema propuestos son capaces de seleccionar solamente las peticiones que son permisibles, dado el estado de aplicación del programa o programas de ordenador. Solamente se ejecutarán las peticiones que se adaptan a las peticiones permisibles para dicho estado, proporcionando un sistema seguro. Por otra parte, el método y sistema no examinan el contenido propiamente dicho, pero hacen el seguimiento de peticiones de la capa de aplicación que se pueden esperar de un cliente en relación con el estado de aplicación del programa o programas de ordenador en un momento determinado. De otra manera, la petición es rechazada o simplemente inmovilizada, pero no es ejecutada. Esta forma de proceder permite una exploración rápida y segura del tráfico. Se constituyen dinámicamente conjuntos de peticiones que corresponden al estado de aplicación aplicable del programa de aplicación del ordenador. El cambio del estado de comunicación del sistema de ordenador u otro sistema de ordenador pueden ser determinados por la ejecución de una petición por el programa de aplicación. La exploración del nivel de aplicación de las peticiones, es decir, por debajo del nivel del contenido real, es rápida pero segura.

Se debe apreciar que el método y al sistema de ordenador pueden encontrarse en comunicación con uno o varios otros sistemas de ordenador que en realidad exploran el programa de aplicación de ordenador. El sistema de ordenador funciona entonces como guardián ("gatekeeper").

Los ejemplos de programas de aplicación incluyen los servidores web, servicios web, servidores de aplicación y en particular bases de datos.

Hay varias formas de informar al sistema de ordenador del juego de peticiones aplicable con peticiones permisibles para un estado de aplicación particular del programa de aplicación de ordenador.

La realización de la reivindicación 2, por otra parte, tiene la ventaja de que el juego de peticiones aplicable es recibido directamente desde el programa de aplicación de ordenador (u otro programa configurado para el estado de aplicación del programa de ordenador al sistema de ordenador).

La realización de la reivindicación 4 posibilita el seguimiento de una serie de clientes conectados al sistema de ordenador por medio de sus conexiones, por ejemplo, tal como una barrera con estado. En particular, el sistema de ordenador monitoriza, por ejemplo, qué cliente está conectado y/o qué peticiones de cliente han sido realizadas por un cliente determinado (estado de conexión). El estado de aplicación del programa de aplicación de ordenador puede ser relacionado con un estado de conexión específico.

La realización de la reivindicación 5 permite distinguir entre clientes malintencionados y no malintencionados. La mayor parte de organizaciones utilizan sistemas de ordenador a los que se hace referencia habitualmente como autorizados ("proxys") que separan una red de área local con respecto a una red de área amplia, tal como Internet. Los llamados autorizados, entre otras funciones, utilizan la traducción de dirección de red (NAT). La cantidad de peticiones realizadas a los autorizados es considerable, pero estas peticiones son muy probablemente no malintencionadas. Al disponer un umbral adecuado (basado, por ejemplo, en el número promedio de peticiones que se puede esperar de una red de área local utilizando datos históricos del número de peticiones de identificación de entrada recibidas desde clientes internos), las peticiones malintencionadas externas pueden ser distinguidas de las peticiones no malintencionadas de la red de área local. La frecuencia de peticiones de clientes internos puede ser estimada en base al número de peticiones de identificación de entrada y al flujo de programa de aplicación, es decir, la secuencia de estados de aplicación del programa de aplicación de ordenador. Un número grande de peticiones de clientes externos puede indicar un ataque. Estas peticiones pueden ser denegadas. Las peticiones de estos clientes pueden ser monitorizadas, rechazadas o analizadas en base a un historial de contactos, comportamiento anterior y/o dominio.

Las realizaciones de las reivindicaciones 6-9 permiten el bloqueo o freno de clientes que, por ejemplo, envían un alto número de peticiones o un alto número de peticiones procedentes del mismo cliente. De modo más general, los clientes malintencionados pueden ser distinguidos con respecto a los clientes no malintencionados, de manera que estos últimos son servidos antes que los primeros aunque sus peticiones lleguen más tarde al sistema de ordenador, si bien estas realizaciones aumentan la seguridad en general, se debe observar que estas realizaciones pueden también ser aplicadas de forma separada con respecto a la invención, tal como se define en las reivindicaciones 1-5.

Si bien el cliente y el sistema de ordenador pueden ser implementados en un dispositivo único, se prefiere la realización de la reivindicación 10.

La cantidad de peticiones posibles es especialmente grande para programas de aplicación de ordenador de base de datos. Las realizaciones de las reivindicaciones 11, 12 son particularmente ventajosas en estos casos.

El sistema de ordenador de la reivindicación 15 puede ser configurado para llevar a cabo el método de las reivindicaciones 1-12.

En particular, el sistema de ordenador comprende además:

- un detector de estado de aplicación configurado para detectar dicho primer estado de aplicación y dicho segundo estado de aplicación;
- un captador de conjunto de peticiones configurado para captar dicho primer juego de peticiones y dicho segundo juego de peticiones, respectivamente, como respuesta a la detección de dicho primer estado de aplicación o dicho segundo estado de aplicación.

Esta realización tiene la ventaja de que el programa de aplicación de ordenador indica solamente su estado de aplicación para un cliente particular (conexión) al sistema de ordenador. El sistema de ordenador puede utilizar el estado indicado para obtener, captar o actualizar el conjunto de peticiones aplica-

bles para este estado del programa de aplicación de ordenador.

En una realización, el sistema de ordenador comprende además un receptor de juego de peticiones, configurado para recibir dicho primer juego de peticiones y dicho segundo juego de peticiones.

En una realización, el receptor de peticiones de cliente está configurado para recibir, como mínimo, una de las peticiones de protocolo de transferencia de hipertexto (HTTP), peticiones de protocolo de transferencia de archivo (FTP), peticiones de protocolo de transferencia de correo simple (SMTP) y peticiones telnet.

En una realización, el sistema de ordenador comprende además un monitor de estado de conexión configurado para determinar un estado de conexión entre dicho cliente y dicho sistema de ordenador, estando configurado dicho sistema de ordenador de manera tal que dicho primer estado de aplicación y un segundo estado de aplicación de dicho programa de aplicación de ordenador están relacionados con dicho estado de conexión.

En una realización, el sistema de ordenador está configurado para mantener una magnitud de umbral de peticiones de capa de aplicación de cliente por unidad de tiempo, y en el que dicho módulo de instrucción está configurado para instruir a dicho programa de aplicación de ordenador para ejecutar dicha petición de capa de aplicación de cliente solamente si la magnitud de peticiones de capa de aplicación de clientes se encuentra por debajo de dicho umbral.

En una realización, dicho sistema de ordenador comprende además:

- un módulo diferenciador configurado para diferenciar entre clientes malintencionados y no malintencionados;

- un módulo de clasificación configurado para clasificar peticiones de capa de aplicación de cliente partiendo de dichos clientes malintencionados y no malintencionados para obtener una cola de peticiones de capa de aplicación de clientes no malintencionados, seguida de dichas peticiones de capa de aplicación de clientes malintencionados;

- de manera que dicho módulo de instrucción está configurado para instruir a dicho programa de aplicación de ordenador para ejecutar en primer lugar dichas peticiones de capa de aplicación de clientes no malintencionados.

En una realización, el sistema de ordenador comprende además un segundo módulo analizador configurado para analizar dichas peticiones de capa de aplicación de clientes malintencionados con respecto a la mencionada cola, después de que dicho módulo de instalación ha instruido a la totalidad de peticiones de capa de aplicación de clientes no malintencionados.

En una realización, el sistema de ordenador comprende además un módulo de almacenamiento para almacenar un historial de contactos de clientes y un módulo de clasificación configurado para clasificar clientes conocidos a partir de dicho historial de contactos con mayor altura en dicha cola que clientes no conocidos a partir de dicho historial de contactos.

En una realización, el módulo diferenciador está configurado para diferenciar dichos clientes malintencionados y no malintencionados en base a, como mínimo, uno de los siguientes criterios: número de peticiones de capa de aplicación de cliente recibidas de clientes, historial de contactos de clientes con dicho sistema de ordenador, tipo de contenido de peticiones de capa de aplicación, contenido de peticiones de capa de aplicación recibidas de dichos clientes.

En una realización, el sistema de ordenador está configurado para recibir dichas peticiones de capa de aplicación de cliente mediante una red de comunicación.

En una realización, el programa de aplicación de ordenador es un programa de aplicación de base de datos, preferentemente instalado en el otro sistema de ordenador mencionado.

En una realización, el sistema de ordenador comprende:

- un receptor configurado para recibir dicho primer juego de peticiones de base de datos permisibles a partir de dicho programa de aplicación de base de datos del otro sistema de ordenador mencionado; y

- dicho módulo de instrucción está configurado para la instrucción de dicho programa de aplicación de base de datos para realizar una operación de base de datos solamente si dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones de base de datos permisibles.

Se pueden combinar dos o varis de estas realizaciones.

A continuación, se describirán realizaciones de la invención de manera más detallada. Se debe observar, no obstante, que estas realizaciones no se deben considerar como limitativas del campo de protección de la presente invención.

Breve descripción de los dibujos

En los dibujos:

Las figuras 1A y 1B consisten en ilustraciones esquemáticas de varias situaciones de utilización del sistema de ordenador, de acuerdo con una realización de la invención;

Las figuras 2A y 2B proporcionan representaciones esquemáticas del sistema, según una realización de la invención; y

Las figuras 3A y 3B muestran etapas de un método, según una realización de la invención.

Descripción detallada de los dibujos

Las figuras 1A y 1B muestran ilustraciones esquemáticas de diferentes situaciones de utilización de un sistema de ordenador (1), de acuerdo con una realización de la invención.

En la figura 1A, los dispositivos de cliente (2A, 2B) están conectados con intermedio de la red (3) al sistema de ordenador (1). El sistema de ordenador (1), no obstante, también puede trabajar por su parte con un cliente directamente y proporcionar un interfaz de usuario para el cliente en una pantalla (4). El sistema de ordenador (1) desarrolla también un programa de aplicación de ordenador, tal como un servidor web o una aplicación de base de datos, al cual se dirigen las peticiones (instrucciones) de los clientes. Los dispositivos de cliente pueden incluir dispositivos inalámbricos móviles (2A), tales como teléfonos, PDA, ordenadores portátiles, etc., que comunican con la red (3) a través de una red (5) de acceso inalámbrico y dispositivos con cables, tales como ordenadores de sobremesa (2B).

En la figura 1B, los dispositivos de clientes (2C, 2D y 2E) están conectados al sistema de ordenador (1) con intermedio de una primera red (3). El sistema de ordenador (1) funciona como guardián de un sistema principal o servidor (6) que desarrolla un pro-

grama de aplicación de ordenador específico al que se dirigen peticiones de los clientes. Se debe disponer una serie de dichos servidores (6). El sistema de ordenador (1) está conectado en comunicación con el sistema principal (6) con intermeid8o de una segunda red (7). El sistema principal (6) tiene acceso a una base de datos (8) y puede desarrollar en particular una aplicación de base de datos utilizando la base de datos (8).

Otras varias situaciones pueden ser previstas por los técnicos en la materia para la aplicación del sistema de ordenador (1) sin salir del alcance de la presente invención.

El programa de aplicación de cliente puede ser instalado y puede funcionar en el sistema de ordenador (1), el sistema principal (6) o bien uno o varios sistemas de ordenador. El programa de aplicación de ordenador tiene una serie de estados de aplicación. Los estados de aplicación pueden representar etapas lógicas en una secuencia específica (predeterminada) de estados para el programa de aplicación. Los estados de aplicación del programa de aplicación de ordenador pueden cambiar después de la ejecución de una petición a dicho programa. Una gran cantidad de peticiones es válida para estos estados de aplicación. No obstante, para cada uno de los estados de aplicación, solamente es permisible un subconjunto específico entre la gran cantidad de peticiones.

Como ejemplo, la activación de un enlace en una página de un sitio web puede devolver otra página web con un nuevo juego de enlaces (cambio del estado de aplicación). De las muchas peticiones posibles al servidor web, solamente la activación de los enlaces en la página web devuelta pertenecen al conjunto de peticiones permisibles para este estado de aplicación.

En la figura 2A, el sistema de ordenador (1) de las figuras 1A y 1B se han mostrado esquemáticamente. El sistema de ordenador (1) comprende un procesador (10), una memoria (11), un adaptador de red (12) para comunicación con uno o varios de los sistemas (2A-2E) con intermedio de las redes (3) (y posiblemente con el sistema principal (6) con intermedio de la segunda red (7)). Se debe observar que normalmente el sistema de ordenador (1) de las figuras 1A y 1B estaría configurado para conectar a más de dos o tres dispositivos de cliente.

El sistema de ordenador (1) puede contener también una base de datos (13) con juegos de peticiones para diferentes estados de aplicación del programa de aplicación desarrollado por el sistema de ordenador (1) en el sistema principal (6). La base de datos (13) puede ser utilizada también por un programa de aplicación de base de datos utilizado en el sistema de ordenador (1).

Las funciones específicas del sistema de ordenador (1) se han mostrado esquemáticamente en la figura 2B y se describirán a continuación de manera más detallada. Se debe observar que las funciones pueden ser principalmente implementadas en forma de partes de código de software de uno o varios programas de ordenador ejecutados en el procesador (10).

El sistema de ordenador (1) comprende un módulo de conexión (20) para establecer conexión con los dispositivos de cliente (2A-2E). El módulo de conexión controla la conexión con los dispositivos de cliente. El módulo de conexión (20) puede estar configurado para determinar un estado de comunicación para el cliente con respecto al sistema de ordenador (1).

El sistema de ordenador (1) comprende un receptor (21) de peticiones de clientes configurado para recibir (y posiblemente procesar) una petición procedente de los dispositivos de cliente (2A-2E) o un cliente interno. La petición de cliente es una petición o instrucción para el programa de aplicación de ordenador instalado en el sistema de ordenador (1) y/o en el sistema principal (6). La petición de cliente puede ser, por ejemplo, una petición http resultado de la activación de un enlace en una página web determinada o una instrucción para una base de datos (8, 13).

El sistema de ordenador (1) puede tener también un módulo analizador (22) configurado para analizar si la petición de cliente recibida por el receptor (21) de peticiones de cliente se adapta a una petición permisible de un conjunto de peticiones que comprende una o varias peticiones permisibles correspondientes a un estado de aplicación del programa de aplicación de ordenador con respecto a ese cliente.

El sistema de ordenador (1) comprende también un módulo de instrucción (23) para instruir el programa de aplicación de ordenador del sistema de ordenador (1) y/o el sistema principal (6), a efectos de ejecutar la petición de cliente solamente si la petición de cliente se adapta a una de las peticione permisibles de dicho juego o conjunto de peticiones.

Desde luego, el receptor (21) de peticiones de cliente puede recibir otras peticiones de cliente. El módulo analizador (22) puede analizar si las otras peticiones de cliente se adaptan a peticiones permisibles de otros correspondientes juegos de peticiones, correspondiendo cada uno de los juegos de peticiones a diferentes estados de aplicación del programa de aplicación del ordenador. El módulo de instrucción (23) puede ordenar al programa de ordenador la ejecución de las otras peticiones solamente si estas peticiones se adaptan a peticiones permisibles del conjunto de peticiones aplicables del estado de aplicación correspondiente.

Existen varias formas de informar al sistema de ordenador (1) del conjunto de peticiones aplicables con peticiones permisibles para un estado de aplicación específico del programa de aplicación de ordenador.

El sistema de ordenador (1) puede comprender, por ejemplo, un detector (24) de estado de aplicación configurado para detectar los estados de aplicación del programa de aplicación de ordenador del sistema de ordenador (1) y/o el sistema principal (6). Si el detector (24) detecta un estado de aplicación del programa, se dispone un captador (25) del juego de peticiones para captar, obtener y/o actualizar el juego de peticiones para dicho estado de aplicación específico. El juego de peticiones puede ser captado, por ejemplo, de la base de datos (13).

No obstante, el juego de peticiones aplicable de peticiones permisibles para un estado específico de aplicación del programa de aplicación de ordenador puede ser recibido también por el captador (26) de juegos de peticiones del sistema de ordenador (1). El conjunto de peticiones puede ser recibido, por ejemplo, desde un programa de aplicación de ordenador que es ejecutado en el sistema de ordenador (1) o el servidor (6), o desde otro programa de ordenador.

El sistema de ordenador (1) puede almacenar también una cantidad umbral de peticiones de cliente. El sistema de ordenador (1) está configurado para mantener una cantidad umbral de peticiones de cliente por unidad de tiempo. El módulo de instrucción

(23) está configurado para la instrucción del programa de aplicación de ordenador a efectos de ejecutar la petición de cliente solamente si la cantidad de peticiones de cliente se encuentra por debajo de dicha magnitud umbral. Esta funcionalidad puede mostrarse ventajosa, por ejemplo, cuando el sistema de ordenador (1) está implementado en un servidor autorizado ("proxy") o cuando muchos clientes comparten una dirección IP pública común.

En una realización alternativa, el sistema de ordenador (1) puede tener también un módulo diferenciador (27) configurado para diferenciar entre clientes malintencionados y no malintencionados. Los clientes malintencionados y no malintencionados pueden ser diferenciados, por ejemplo, en base al número de peticiones de cliente recibidas de los clientes, del historial de contactos de clientes con el sistema de ordenador (1), por el tipo de contenido de peticiones y/o el contenido de peticiones recibidas de dichos clientes. Se dispone un módulo de clasificación (28) que está configurado para clasificar peticiones de clientes a partir de clientes malintencionados y dichos clientes no malintencionados para obtener una cola de peticiones de clientes no malintencionados seguida de las peticiones de clientes malintencionados. El módulo de instrucción (23) está configurado para la instrucción de dicho programa de aplicación de ordenador para ejecutar en primer lugar dichas peticiones de clientes no malintencionados. Las peticiones de clientes malintencionados pueden ser analizadas por otro módulo analizador (29) después de que se hayan manipulado las peticiones legítimas, penalizando, de esta manera, al cliente malicioso. Los resultados pueden ser utilizados, por ejemplo, para actualizar un historial de contactos entre el sistema de ordenador (1) y los clientes maliciosos.

El sistema de ordenador (1) puede tener un módulo de almacenamiento (30) para almacenar un historial de contactos de los clientes. El módulo de clasificación (28) puede estar configurado para clasificar clientes conocidos a partir de dicho historial de contactos en un orden más elevado en la cola que los clientes no conocidos por dicho historial de contactos.

A continuación, se describirá el funcionamiento del sistema de ordenador (1) con referencia a las figuras 3A y 3B. Se supondrá que el sistema de ordenador (1) funciona como guardián para el sistema principal (6) que utiliza un programa de aplicación de base de datos para recuperar datos de la base de datos (8), de acuerdo con la figura 1B.

Un cliente instalado en el dispositivo de cliente (2C) solicita la utilización de un programa de aplicación de ordenador utilizado en el sistema principal (6) con intermedio de la red de comunicación (3).

En la etapa (40), el sistema de ordenador (1) intercepta la petición y establece una conexión utilizando el módulo de conexión (20). El módulo de conexión (20) controla la conexión y las peticiones procedentes del dispositivo de cliente (2C). Una página inicial, por ejemplo, una página html, es presentada al dispositivo de cliente (2C). Se supone en este caso que el sistema de ordenador (1) no explora la petición inicial, si bien puede ser aplicable un estado de aplicación inicial con peticiones permisibles asignadas para iniciar la aplicación de ordenador.

La página inicial del programa de aplicación de ordenador presentada al dispositivo de cliente (2C) permite la realización de una serie de peticiones, por ejemplo, peticiones http GET. Estas peticiones constituyen un primer juego o conjunto de peticiones de peticiones permisibles correspondientes a la página inicial (estado de aplicación) del programa de aplicación de ordenador. Por razones de simplicidad, se supondrá que solamente las peticiones válidas están constituidas en este caso por un conjunto de hipervínculos que pueden ser activados. No obstante, se debe observar que pueden ser posibles otras peticiones o instrucciones, por ejemplo, peticiones http post.

En la etapa (41), se recibe una petición http procedente del dispositivo de cliente (2C), resultado de la activación de un hipervínculo a partir de la página inicial. El módulo de conexión (20) controla que esta petición proceda del dispositivo de cliente (2C) que ha emitido una petición desde la página inicial.

El receptor (26) del juego de peticiones recibe el primer juego de peticiones procedente del programa de aplicación de ordenador, que utiliza en el sistema principal (6), válido para la página inicial. En la etapa (42), el módulo analizador (22) del sistema de ordenador (1) examina si la petición http recibida del dispositivo de cliente (2C) se adapta a una petición permisible del primer juego de peticiones recibido para la página inicial html.

Si la petición http no se adapta a una petición del primer conjunto o juego de peticiones, el módulo de instrucción (23) no dará instrucciones al programa de aplicación de ordenador utilizado en el sistema principal (6) para ejecutar la petición http (etapa (43)). Se debe observar que es posible que una petición que parece válida desde la perspectiva del dispositivo de cliente no sea ejecutada cuando esta petición no forme parte del juego de peticiones aplicable.

En la etapa (44) se llevan a cabo otras acciones en la petición que no se ha ejecutado. Estas acciones incluyen, si bien de forma no limitativa, el descarte de la petición, el análisis de la misma, el almacenamiento de la petición, la extracción de información de la petición para construir un historial de peticiones, etc.

Si el módulo analizador (22) descubre que la petición http del dispositivo de cliente (2C) se adapta a una petición permisible del primer conjunto de peticiones de la página inicial html, el módulo de instrucción (23) da instrucciones al programa de aplicación de ordenador para ejecutar la petición http en la base de datos (8) en la etapa (45). Se observará que también se pueden llevar a cabo otras acciones en estas peticiones ejecutadas.

La ejecución de la petición hace que el programa de aplicación extraiga datos de la base de datos para constituir una nueva página html dependiendo de la petición. La nueva página html es transmitida al dispositivo de cliente (2C).

La nueva página html corresponde a un nuevo estado de aplicación del programa de aplicación de ordenador (etapa 46). El módulo de conexión (20) que mantiene la conexión abierta con el dispositivo de cliente (2C) registra que la nueva página html ha sido transmitida al dispositivo de cliente (2C).

En la etapa 47, se recibe otra petición http procedente del dispositivo de cliente (2C).

Antes o después de haber recibido la petición http, el programa de aplicación de ordenador ha informado al módulo analizador (22) del juego de peticiones correspondiente al nuevo estado de aplicación. Después de la recepción de la petición http adicional, el módulo analizador (22) examina en la etapa (48) si la

petición http adicional se adapta a una petición permisible del juego de peticiones válido para el nuevo estado de aplicación.

Finalmente, dependiendo del resultado del análisis efectuado por el módulo analizador (22), el módulo de instrucción (23) dará instrucciones al programa de aplicación de ordenador para ejecutar la petición (etapa 49) o para no ejecutarla (etapa 50).

Se debe observar que el diagrama de flujo continúa para otras peticiones del dispositivo de cliente (2C).

También se debe observar que el sistema de ordenador (1) mantiene el control del estado de aplicación para cada cliente, por ejemplo, utilizando el módulo de conexión (20) que tiene tablas para cada conexión, de manera tal que el sistema de ordenador (1) está configurado para manipular peticiones procedentes de múltiples clientes, mientras que el estado de aplicación del programa o programas de aplicación de ordenador pueden ser distintos para cada uno de los clientes en un momento determinado de tiempo.

También se debe observar que cada petición recibida de un cliente puede ser analizada de acuerdo con la etapa 44, por ejemplo, por razones estadísticas.

REIVINDICACIONES

1. Método, implementado por ordenador, para el control de un programa de aplicación de ordenador en un sistema de ordenador (1) configurado para comunicación electrónica con un cliente y que tiene acceso a un primer juego de peticiones de una o varias peticiones de capas de aplicación permisibles, que corresponden a un primer estado de aplicación de dicho programa de aplicación de ordenador y un segundo juego de peticiones de una o varias peticiones permisibles de capas de aplicación correspondientes a un segundo estado de aplicación de dicho programa de aplicación de ordenador utilizado en dicho sistema de ordenador u otro sistema de ordenador en relación con dicho cliente, cuyo método comprende las siguientes etapas:

- recibir (41) en dicho sistema de ordenador una petición de capa de aplicación de cliente procedente de dicho cliente para dicho programa de aplicación de ordenador para dicha primera situación de aplicación predeterminada;

caracterizado por

- analizar (42) si dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones permisibles de dicho primer juego de peticiones como respuesta a la recepción de la petición de dicho cliente;

- dar instrucciones (45) a dicho programa de aplicación de ordenador para ejecutar dicha petición de capa de aplicación de cliente solamente si dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones de capa de aplicación permisibles de dicho primer juego de peticiones;

- cambiar (46) dicho primer estado de aplicación a dicho segundo estado de aplicación de dicho programa de aplicación de ordenador como respuesta a la ejecución de dicha petición de capa de aplicación de cliente cuando dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones de capa de aplicación permisibles de dicho primer juego de peticiones, siendo dicho segundo estado de aplicación distinto de dicho primer estado de aplicación;

- recibir (47) otra petición de capa de aplicación de cliente procedente de dicho dispositivo de cliente;

- analizar (48) si dicha petición de capa de aplicación de cliente adicional se adapta a una petición de capa de aplicación permisible de dicho segundo juego de peticiones;

- dar instrucciones (49) a dicho programa de aplicación de ordenador para ejecutar dicha petición de capa de aplicación de cliente adicional solamente si dicha petición de aplicación de cliente adicional se adapta a una de dichas peticiones de capa de aplicación permisibles de dicho segundo juego de peticiones.

2. Método, según la reivindicación 1, en el que, como mínimo, uno de dichos primeros juegos de peticiones o dicho primer estado de aplicación es obtenido a partir de dicho programa de aplicación de ordenador utilizado en dicho sistema de ordenador (1) o los otros sistemas de ordenador mencionados.

3. Método, según la reivindicación 1, en el que dichas peticiones de capa de aplicación comprenden, como mínimo, una petición de protocolo de transferencia de hipertexto (HTTP), petición de protocolo de transferencia de archivo (FTP), petición de protocolo de transferencia de correo simple (SMTP) y peticiones telnet.

4. Método, según una o varias de las reivindicaciones anteriores, que comprende además las siguientes etapas:

- determinar por dicho sistema de ordenador (1) un estado de conexión entre dicho cliente y dicho sistema de ordenador;

- relacionar dicho primer estado de aplicación y segundo estado de aplicación a dicho estado de conexión.

5. Método, según una o varias de las reivindicaciones anteriores, en el que dicho sistema de ordenador (1) mantiene una magnitud umbral de peticiones de capa de aplicación de cliente por unidad de tiempo, comprendiendo el método la etapa de dar instrucciones a dicho programa de aplicaciones de ordenador para ejecutar dichas peticiones de capa de aplicación de cliente solamente si la cantidad de peticiones de capa de aplicación de cliente se encuentra por debajo de dicha magnitud umbral.

6. Método, según una o varias de las reivindicaciones anteriores, que comprende además las siguientes etapas:

- diferenciar entre clientes malintencionados y no malintencionados;

- clasificar las peticiones de capa de aplicación de cliente procedentes de dichos clientes malintencionados y dichos clientes no malintencionados para obtener una cola de peticiones de capa de aplicación de cliente no malintencionados seguida por dichas peticiones de capa de aplicación de clientes malintencionados;

- dar instrucciones a dicho programa de aplicación de ordenador para ejecutar en primer lugar dichas peticiones de clientes no malintencionados.

7. Método, según la reivindicación 6, que comprende además la etapa de analizar dichas peticiones de capa de aplicación de clientes malintencionados desde dicha cola después de haber dado instrucciones a dicho programa de aplicación de ordenador de ejecutar todas las peticiones de capa de aplicación de cliente no malintencionado.

8. Método, según la reivindicación 6 ó 7, en el que dicho sistema de ordenador (1) almacena un historial de contactos de clientes, comprendiendo además la etapa de clasificar los clientes conocidos por dicho historial de contactos en un lugar más elevado de dicha cola que los clientes no conocidos por dicho historial de contactos.

9. Método, según una o varias de las reivindicaciones 6-8, que comprende además la etapa de diferenciar dichos clientes malintencionados y no malintencionados en base, como mínimo, a uno de los siguientes criterios: número de peticiones de capa de aplicación de cliente recibidas de clientes, historial de contactos de clientes con dicho sistema de ordenador, tipo de contenido de peticiones de capa de aplicación, contenido de las peticiones de capa de aplicación recibidas de dichos clientes.

10. Método, según una o varias de las reivindicaciones anteriores, en el que dicho cliente es implementado en un dispositivo de cliente (2A-2E) y dicho sistema de ordenador (1) está conectado, como mínimo, a una red de comunicación (3) para comunicar electrónicamente con dicho dispositivo de cliente, comprendiendo dicho método la etapa de recibir una petición de capa de aplicación de dicho cliente mediante dicha red de comunicación.

11. Método, según una o varias de las reivindica-

ciones anteriores, en el que dicho sistema de ordenador (1) o el otro sistema de ordenador comprende una base de datos (8) y dicho programa de aplicación de ordenador es un programa de aplicación de base de datos.

12. Método, según la reivindicación 11, que comprende además las siguientes etapas:

- recibir dicho primer juego de peticiones de base de datos permisibles desde dicho programa de aplicación de base de datos;
- dar instrucciones de una operación de base de datos de dicho programa de aplicación de la base de datos de la mencionada base de datos (8) solamente si dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones permisibles de la base de datos.

13. Programa de ordenador que comprende partes de código de software adaptadas, una vez instaladas en sistemas electrónicos y ejecutadas por los mismos, para llevar a cabo el método, según las reivindicaciones 1-12.

14. Soporte que contiene el programa de ordenador, según la reivindicación 13.

15. Sistema de ordenador (1) para controlar un programa de aplicación de ordenador en dicho sistema de ordenador o en otro sistema de ordenador, cuyo sistema de ordenador está configurado para su conexión, como mínimo, con un cliente, comprendiendo:

- un receptor (21) de peticiones de cliente configurado para recibir una petición de capa de aplicación de cliente y otra petición de capa de aplicación de cliente dirigida a dicho programa de aplicación de ordenador, comprendiendo, dicho programa de aplicación de ordenador, como mínimo, un primer estado de aplicación y un segundo estado de aplicación, de manera que dicho primer y segundo estados de aplicación son diferentes estados de aplicación que se pueden obtener ejecutando la petición de capa de aplicación del cliente;

caracterizado por un módulo analizador (22) configurado para analizar si dicha petición de capa de aplicación de cliente se adapta a una petición de capa de aplicación permisible de un primer juego de peticiones que comprende una o varias peticiones de capa de aplicación permisibles correspondientes a dicho primer estado de aplicación de dicho programa de aplicación de ordenador en relación con dicho cliente y si dicha petición adicional de capa de aplicación del cliente se adapta a una petición de capa de aplicación permisible de dicho segundo juego de petición de una o varias peticiones de capa de aplicación permisibles correspondientes a dicho segundo estado de aplicación de dicho programa de ordenador en relación con dicho cliente;

- un módulo de instrucciones (23) configurado para dar instrucciones a dicho programa de aplicación de ordenador para ejecutar dicha petición de capa de aplicación de cliente solamente si dicha petición de capa de aplicación de cliente se adapta a una de dichas peticiones de capa de aplicación permisibles de dicho primer juego de peticiones para obtener dicho segundo estado de aplicación y para dar instrucciones a dicho programa de aplicación de ordenador para ejecutar dicha petición adicional de capa de aplicación de cliente solamente cuando dicha petición adicional de capa de aplicación de cliente se adapta a una de dichas peticiones de capa de aplicación permisibles de dicho segundo juego de peticiones.

16. Sistema de ordenador (1), según la reivindicación 15, en el que dicho sistema de ordenador está configurado además para llevar a cabo el método, según cualquiera de las reivindicaciones 2-12.

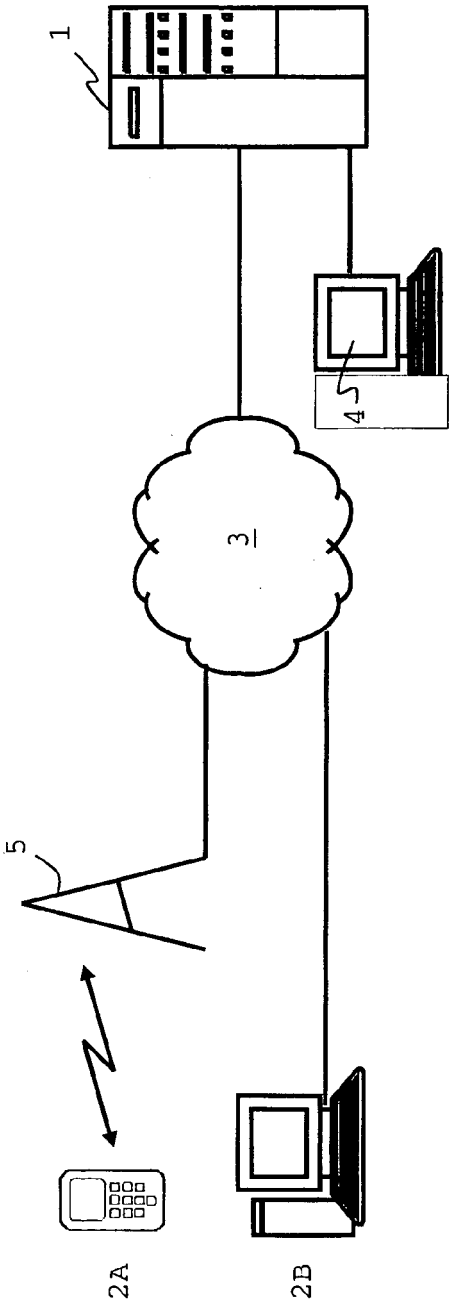

FIG. 1A

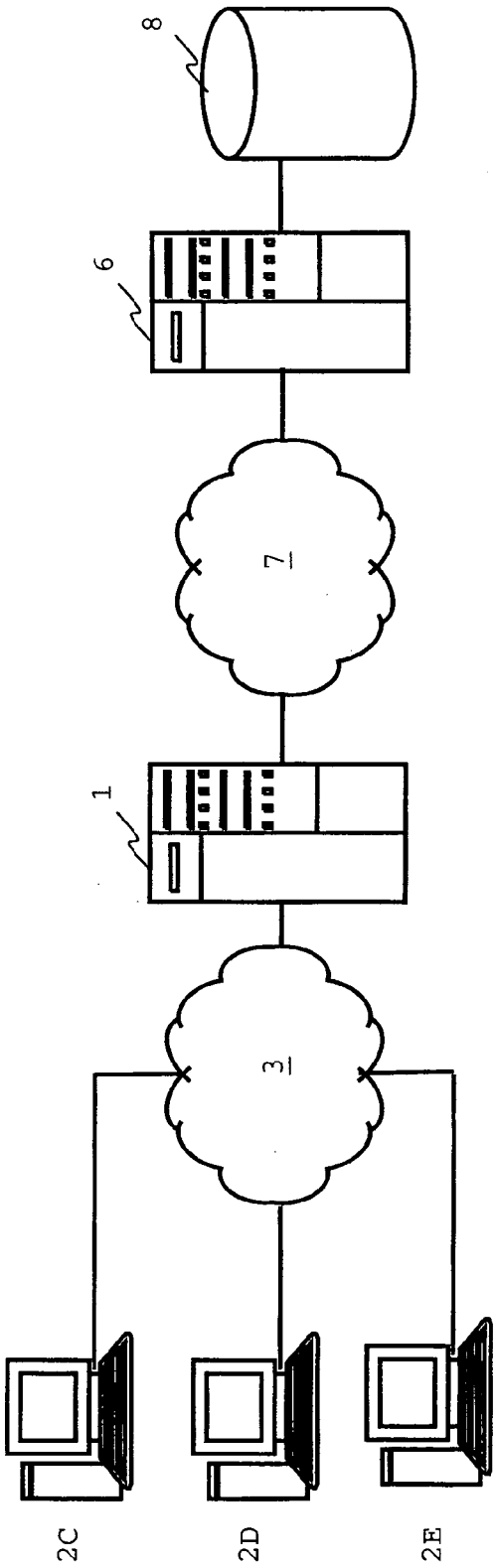

FIG. 1B

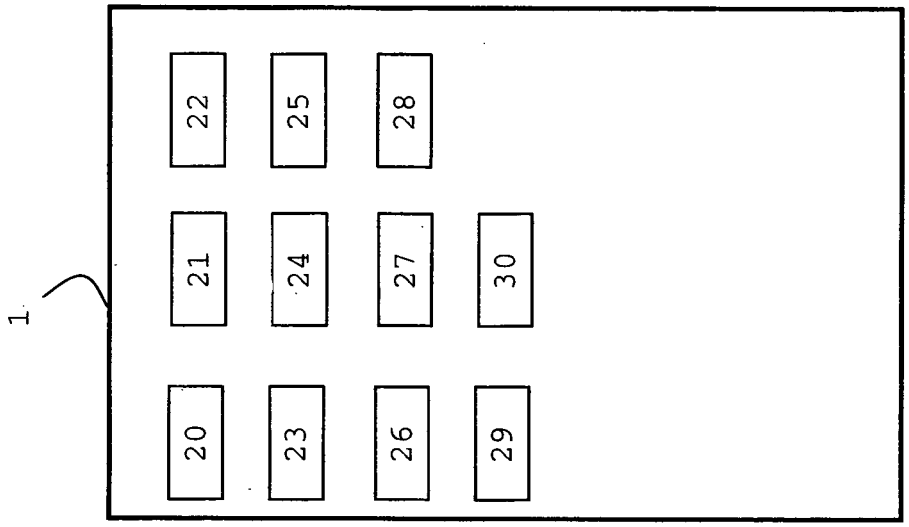

FIG. 2B

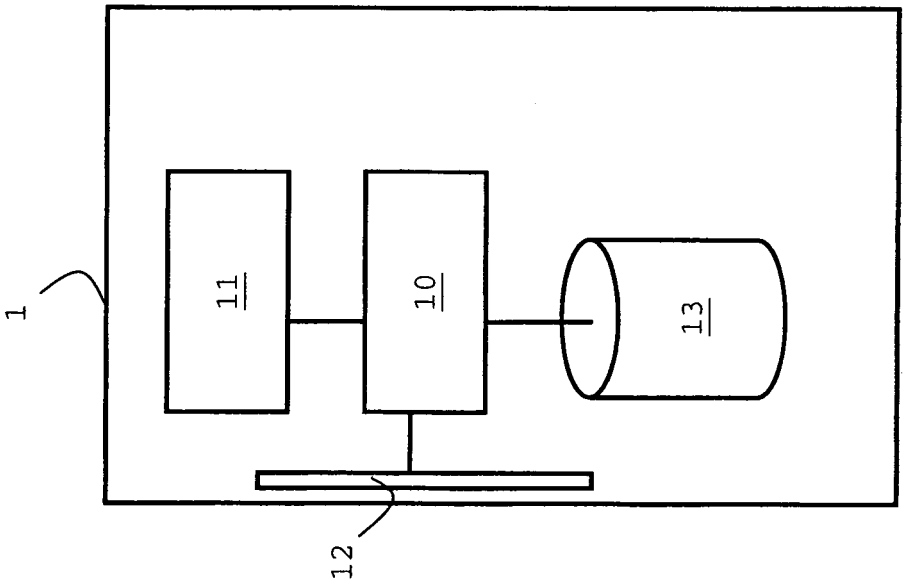

FIG. 2A

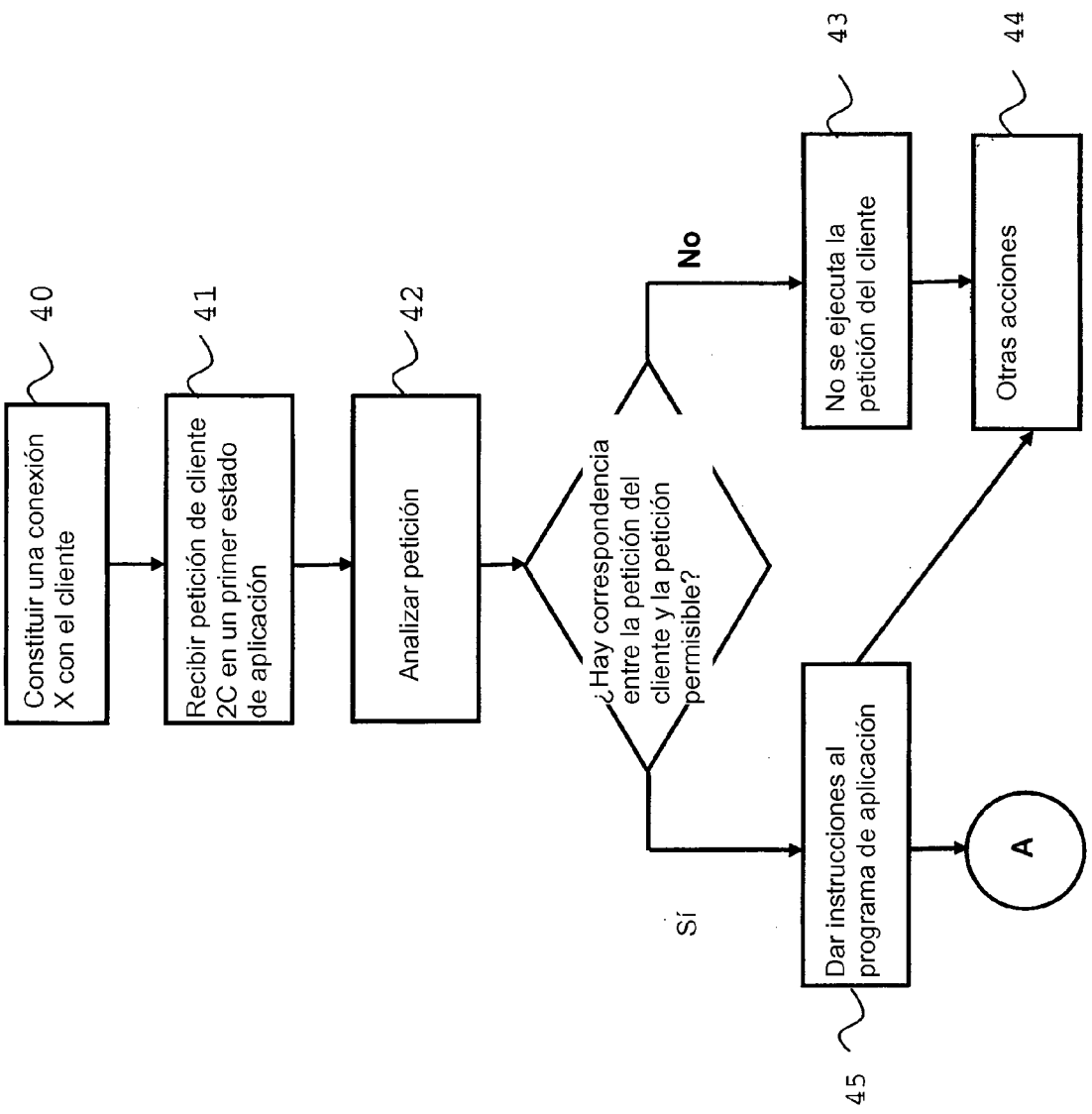
40
Constituir una conexión X con el cliente
41
Recibir petición de cliente 2C en un primer estado de aplicación
42
Analizar petición
¿Hay correspondencia entre la petición del cliente y la petición permisible?
No
Sí
43
No se ejecuta la petición del cliente
44
Otras acciones
45
Dar instrucciones al programa de aplicación
A

FIG. 3A

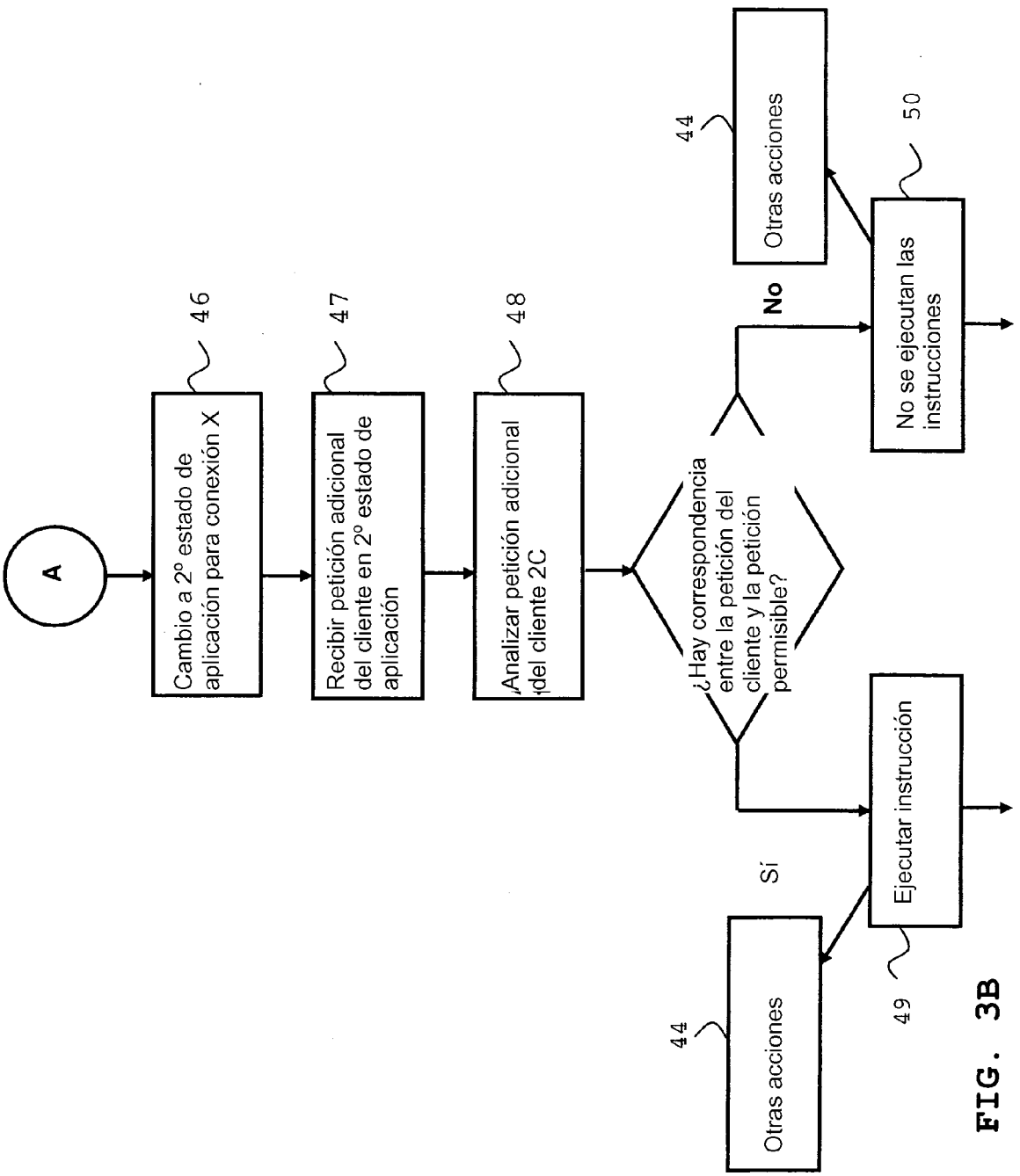
A
Cambio a 2º estado de aplicación para conexión X
46
Recibir petición adicional del cliente en 2º estado de aplicación
47
Analizar petición adicional del cliente 2C
48
¿Hay correspondencia entre la petición del cliente y la petición permisible?
No
Sí
Otras acciones
44
No se ejecutan las instrucciones
50
Ejecutar instrucción
49
Otras acciones
44

FIG. 3B