(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 374 275**

(51) Int. CI.:
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04779292 .4**
(96) Fecha de presentación: **26.07.2004**
(97) Número de publicación de la solicitud: **1609045**
(97) Fecha de publicación de la solicitud: **28.12.2005**

(54) Título: **APLICACIÓN PARA HABILITAR LA INTEGRACIÓN DE TECNOLOGÍAS ANTI-CORREO BASURA.**

(30) Prioridad:
12.11.2003 US 706368

(45) Fecha de publicación de la mención BOPI:
15.02.2012

(45) Fecha de la publicación del folleto de la patente:
15.02.2012

(73) Titular/es:
MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052, US

(72) Inventor/es:
MCMILLAN, Bruce, A.;
WALLACE, Andrew, J.;
KOORLAND, Neil, K.;
WANG, Qiang;
ATWELL, Simon, P. y
NEELY, Samuel, J.

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Aplicación para habilitar la integración de tecnologías anti-correo basura

Campo de la invención

La presente invención se refiere, en general, a la mensajería electrónica y, más específicamente, se refiere al filtrado de correo electrónico no deseado.

Antecedentes de la invención

La mensajería electrónica, en particular, el correo electrónico ("e-mail") transportado por Internet, está volviéndose rápidamente no solamente penetrante en la sociedad sino también, dada su informalidad, facilidad de uso y bajo coste, en un procedimiento preferido de comunicación para muchos individuos y organizaciones.

Desafortunadamente, los destinatarios del correo electrónico están siendo sometidos, en forma creciente, a envíos masivos de correo no solicitado. Con el crecimiento del comercio basado en Internet, una amplia y creciente variedad de mercaderes electrónicos están enviando repetidamente correo no solicitado, publicitando sus productos y servicios a un universo en expansión continua de destinatarios de correo electrónico. La mayoría de los consumidores que encargan productos o que tratan de otra forma con un comerciante por Internet esperan y, de hecho, reciben regularmente tales peticiones de esos comerciantes.

Sin embargo, los usuarios del correo electrónico están expandiendo continuamente sus listas de distribución para llegar a un número creciente de destinatarios. Por ejemplo, los destinatarios que simplemente proporcionan sus direcciones de correo electrónico en respuesta a solicitudes de apariencia tal vez inocua de información de visitantes, generadas por diversas sedes de la red, a menudo reciben correo no solicitado y, muy a su pesar, hallan que han sido incluidos en listas de distribución electrónica. Esto ocurre sin el conocimiento, y no digamos el consentimiento, de los destinatarios. Además, un emisor de correo electrónico diseminará a menudo su lista de distribución, ya sea por venta, alquiler con opción a venta, u otro, a otro emisor de correo electrónico, para su uso, y así sucesivamente con subsiguientes emisores de correo electrónico. En consecuencia, a lo largo del tiempo, los destinatarios de correo electrónico se hallan a menudo bombardeados por correo no solicitado, resultante de distintas listas de distribución mantenidas por una amplia y creciente variedad de emisores masivos de correo electrónico. Un individuo puede fácilmente recibir cientos, e incluso miles, de muestras de correo electrónico no solicitado en el curso de un año. Los individuos en las listas de distribución electrónica pueden esperar recibir un número considerablemente mayor de mensajes no solicitados durante un periodo de tiempo mucho más breve.

Además, si bien muchos mensajes de correo electrónico no solicitados son benignos, tales como ofertas de suministros de oficina o informáticos con descuentos, cotizaciones de tasas hipotecarias, o invitaciones para asistir a conferencias de un tipo u otro, otros, tales como los de contenido pornográfico, incendiario y abusivo, son ofensivos para sus destinatarios. Estos mensajes no solicitados se conocen como correo "basura" o como "spam". La carga de correo electrónico del correo basura puede ser equivalente a la carga generada por el correo electrónico legítimo.

De forma similar a la tarea de gestionar el correo postal basura, un destinatario de correo electrónico debe cribar su correo entrante para eliminar el correo basura. La industria informático reconoció este problema y ha desarrollado técnicas para automatizar la eliminación del correo basura. Por ejemplo, una técnica es la de las listas de dominio. Los destinatarios de correo electrónico se abonan a listas de dominio, que identifican y se niegan a aceptar correo usando una regla definida basada en un conjunto de características. Desafortunadamente, la opción de si un mensaje dado de correo electrónico es correo basura o no depende en grado sumo del destinatario específico y del contenido efectivo del mensaje. Lo que puede ser correo basura para un destinatario puede no ser correo basura para otro, lo que limita la funcionalidad de las listas de dominio. Adicionalmente, un emisor de correo electrónico (es decir, un generador de correo basura) preparará un mensaje de modo tal que su verdadero contenido no sea evidente a partir de su línea de Asunto y que sólo pueda discernirse al leer el cuerpo del mensaje.

Otra técnica desarrollada se conoce como una lista de agujeros negros. La lista de agujeros negros es una lista de direcciones conocidas de correo basura desde las cuales se envía correo basura. La dirección del remitente de correo electrónico se coteja con la lista de agujeros negros. Si la dirección está en la lista, el mensaje de correo electrónico no se acepta. Los generadores de correo basura simplemente cambian su dirección para eludir esta técnica. También se han desarrollado otras técnicas. Ninguna de las técnicas es efectiva en un 100%. Las innovaciones por parte de los servidores de correo electrónico para evitar el correo basura son afrontadas por innovaciones por parte de los creadores de correo basura para vencer a las innovaciones.

El documento US 6.161.130 se refiere a una técnica que, mediante un clasificador probabilístico, y para un usuario dado, detecta mensajes de correo electrónico que es probable que este usuario considere como "basura". Un generador construye un vector de características de N elementos para el mensaje entrante. Los datos para este vector de

características se aplican entonces como entrada a un clasificador. El clasificador genera una probabilidad de clasificación de que este mensaje específico sea correo basura. Un comparador compara esta probabilidad para el mensaje de entrada con respecto a una probabilidad de umbral predeterminado asociada al correo basura. Si la probabilidad de clasificación es mayor o igual que el umbral, entonces el mensaje de entrada se indica como correo basura.

Breve resumen de la invención

La presente invención proporciona una aplicación que permite que se desplieguen múltiples soluciones de detección de correo basura, para operar juntas de manera gestionable y racional, y permite que se creen y se desplieguen nuevas innovaciones sobre un modelo de despliegue rápido.

Se presenta un procedimiento que determina si un mensaje de correo electrónico es correo basura, usando módulos anti-correo basura. El procedimiento invoca a uno de los módulos anti-correo basura y recibe un nivel de confianza de correo basura desde el módulo anti-correo basura. Puede aplicarse un factor de afinación al nivel de confianza de correo basura para crear un nivel afinado de confianza de correo basura. El nivel más alto de confianza de correo basura se compara con al menos un umbral. Si el nivel más alto de confianza de correo basura es mayor que el umbral, se invoca una acción asociada a dicho(s) umbral(es).

En una realización, se usa una pluralidad de umbrales, que incluyen un umbral máximo, y el nivel más alto de confianza de correo basura se compara con cada umbral. Si el nivel más alto de confianza de correo basura es mayor que uno o más de los umbrales, se invoca la acción asociada al umbral que ha sido superado y que está más cerca del umbral máximo.

Las acciones invocadas incluyen interrumpir una conexión si el nivel más alto de confianza de correo basura supera un primer nivel de umbral, devolver un mensaje de falta de entrega a un remitente si el nivel más alto de confianza de correo basura supera un segundo nivel de umbral y está por debajo del primer nivel de umbral, entregar el mensaje a una carpeta de correo basura si el nivel más alto de confianza de correo basura supera un tercer nivel de umbral y está por debajo del segundo nivel de umbral, y enviar el nivel más alto de confianza de correo basura al cliente para permitir que el cliente realice acciones personalizadas por cada usuario.

Las características y ventajas adicionales de la invención resultarán evidentes a partir de la siguiente descripción detallada de realizaciones ilustrativas, que continúa con referencia a los dibujos adjuntos.

Breve descripción de los dibujos

Si bien las reivindicaciones adjuntas exponen las características de la presente invención con especificidad, la invención, junto con sus objetos y ventajas, puede entenderse mejor a partir de la siguiente descripción detallada, considerada conjuntamente con los dibujos adjuntos, de los cuales:

la FIG. 1 es un diagrama en bloques que ilustra en general un sistema informático ejemplar en el cual reside la presente invención;

la FIG. 2 es un diagrama en bloques que ilustra en general la aplicación de la presente invención en un sistema que usa una pila de protocolos del SMTP;

la FIG. 3 es un diagrama en bloques que ilustra ejemplos de módulos anti-correo basura usados según la presente invención; y

la FIG. 4 es un diagrama de flujo que ilustra el proceso de integración de módulos anti-correo basura y de determinación de si un mensaje es correo basura.

Descripción detallada de la invención

Pasando a los dibujos, en los cuales los números iguales de referencia se refieren a elementos iguales, se ilustra la invención como implementada en una aplicación informático adecuado. Aunque no se requiere, la invención se describirá en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutadas por un ordenador personal. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas específicas o implementan tipos específicos de datos abstractos. Además, los expertos en la técnica apreciarán que la invención puede ponerse en práctica con otras configuraciones de sistemas informáticos, incluyendo los dispositivos de mano, los sistemas multiprocesadores, los equipos electrónicos de consumo basados en microprocesadores o programables, los ordenadores personales en red, los miniordenadores, los ordenadores centrales, y similares. La invención también puede ponerse en práctica en aplicaciones informáticos distribuidos, donde las tareas son realizadas por dispositivos de procesamiento remoto que están enlazados a través de una red de comunicaciones. En una aplicación informático distribuido, los módulos de programa pueden situarse en dispositivos de almacenamiento de memoria tanto local como remota.

La FIG. 1 ilustra un ejemplo de una aplicación 100 de un sistema informático adecuado sobre el cual puede implementarse la invención. La aplicación 100 de sistema informático es sólo un ejemplo de una aplicación informático adecuado y no está concebido para sugerir ninguna limitación en cuanto al alcance del uso o la funcionalidad de la invención. Tampoco debería interpretarse la aplicación informático 100 como que presenta ninguna dependencia o requisito referido a cualquier componente, o combinación de los mismos, ilustrado(s) en la aplicación operativo ejemplar 100.

La invención es operativa con otras numerosas aplicaciones o configuraciones de sistemas informáticos de propósito general o de propósito especial. Los ejemplos de sistemas, aplicaciones y / o configuraciones informáticos bien conocidos, que pueden ser adecuados para su uso con la invención incluyen, pero no se limitan a: ordenadores personales, ordenadores servidores, dispositivos de mano o portátiles, dispositivos de tableta, sistemas multiprocesadores, sistemas basados en microprocesadores, equipos de sobremesa, sistemas electrónicos programables de consumo, ordenadores personales en red, miniordenadores, ordenadores centrales, aplicaciones informáticos distribuidos que incluyen a cualquiera de los sistemas o dispositivos anteriores, y similares.

La invención puede describirse en el contexto general de las instrucciones ejecutables por ordenador, tales como los módulos de programa, ejecutados por un ordenador. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas específicas o implementan tipos específicos de datos abstractos. La invención también puede ponerse en práctica en aplicaciones informáticos distribuidos donde las tareas son realizadas por dispositivos de procesamiento remoto que están enlazados a través de una red de comunicaciones. En una aplicación informático distribuido, los módulos de programa pueden situarse en medios de almacenamiento de ordenadores locales y / o remotos, que incluyen dispositivos de almacenamiento de memoria.

Con referencia a la FIG. 1, un sistema ejemplar para implementar la invención incluye un dispositivo informático de propósito general en forma de un ordenador 110. Los componentes del ordenador 110 pueden incluir, pero no se limitan a, una unidad 120 de procesamiento, una memoria 130 del sistema y un bus 121 del sistema que acopla diversos componentes del sistema, incluso la memoria del sistema con la unidad 120 de procesamiento. El bus 121 del sistema puede ser cualquiera de diversos tipos de estructuras de bus, incluso un bus de memoria o controlador de memoria, un bus periférico y un bus local que usa cualquiera entre una gran variedad de arquitecturas de bus. A modo de ejemplo, y no de limitación, tales arquitecturas incluyen el bus de Arquitectura Industrial Estándar (ISA), el bus de Arquitectura de Micro Canal (MCA), el bus ISA Mejorado (EISA), el bus local de la Asociación de Estándares de Electrónica de Vídeo (VESA) y el bus de Interconexión de Componentes Periféricos (PCI), también conocido como el bus Entresuelo.

El ordenador 110 incluye habitualmente una gran variedad de medios legibles por ordenador. Los medios legibles por ordenador pueden ser medios disponibles cualesquiera a los que pueda acceder el ordenador 110, e incluyen medios tanto volátiles como no volátiles, y medios extraíbles y no extraíbles. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender medios de almacenamiento de ordenador y medios de comunicación. Los medios de almacenamiento de ordenador incluyen medios volátiles y no volátiles, extraíbles y no extraíbles, implementados en cualquier procedimiento o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento de ordenador incluyen, pero no se limitan a, memoria RAM, ROM, EEPROM, flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico en disco, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y a la que pueda acceder el ordenador 110. Los medios de comunicación realizan habitualmente instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, tal como una onda portadora u otro mecanismo de transporte, e incluyen cualquier medio de entrega de información. El término “señal de datos modulada” significa una señal que tiene una o más de sus características fijada o cambiada de modo tal como para codificar información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados tales como una red cableada o conexión directamente cableada, y medios inalámbricos tales como medios acústicos, de frecuencia de radio, infrarrojos y otros medios inalámbricos. Las combinaciones de cualquiera de los anteriores también deberían incluirse dentro del alcance de los medios legibles por ordenador.

La memoria 130 del sistema incluye medios de almacenamiento de ordenador en forma de memoria volátil y / o no volátil, tal como memoria de sólo lectura (ROM) 131 y memoria de acceso aleatorio (RAM) 132. Un sistema básico 133 de entrada / salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del ordenador 110, tal como durante el arranque, se almacena habitualmente en la memoria ROM 131. La memoria RAM 132 contiene habitualmente datos y / o módulos de programa que son inmediatamente accesibles a y / o actualmente objeto de operaciones por parte de la unidad 120 de procesamiento. A modo de ejemplo, y no de limitación, la FIG. 1 ilustra el sistema operativo 134, los programas 135 de aplicación, otros módulos 136 de programa y datos 137 de programa.

El ordenador 110 también puede incluir otros medios de almacenamiento de ordenador extraíbles / no extraíbles, volátiles / no volátiles. A modo de ejemplo solamente, la FIG. 1 ilustra un controlador 141 de disco rígido que lee de, o escribe en,

medios magnéticos no extraíbles y no volátiles, un controlador 151 de disco magnético que lee de, o escribe en, un disco magnético 152 extraíble, no volátil y un controlador 155 de disco óptico que lee de, y escribe en, un disco óptico 156 extraíble, no volátil, tal como un CD ROM u otro medio óptico. Otros medios de almacenamiento de ordenador extraíbles / no extraíbles, volátiles / no volátiles, que pueden usarse en la aplicación operativo ejemplar, incluyen, pero no se limitan a, casetes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cinta de vídeo digital, memoria RAM de estado sólido, memoria ROM de estado sólido, y similares. El controlador 141 de disco rígido está habitualmente conectado con el bus 121 de sistema a través de una interfaz de memoria no extraíble, tal como la interfaz 140, y el controlador 151 de disco magnético y el controlador 155 de disco óptico están habitualmente conectados con el bus 121 del sistema por una interfaz de memoria extraíble, tal como la interfaz 150.

Los controladores y sus medios asociados de almacenamiento en ordenador, expuestos anteriormente e ilustrados en la FIG. 1, proporcionan el almacenamiento de instrucciones, estructuras de datos y módulos de programa legibles por ordenador, y otros datos para el ordenador 110. En la FIG. 1, por ejemplo, el controlador 141 de disco rígido se ilustra albergando el sistema operativo 144, los programa 145 de aplicación, otros módulos 146 de programa y los datos 147 de programa. Obsérvese que estos componentes pueden bien ser los mismos, o bien distintos, que el sistema operativo 134, los programas 135 de aplicación, otros módulos 136 de programa y los datos 137 de programa. El sistema operativo 144, los programas 145 de aplicación, otros módulos 146 de programa y los datos 147 de programa reciben aquí distintos números para ilustrar que, como mínimo, son copias distintas. Un usuario puede ingresar comandos e información en el ordenador 110 a través de dispositivos de entrada tales como un teclado 162, un dispositivo puntero 161, usualmente denominado un ratón, una bola de rastreo o panel táctil, un micrófono 163 y una tableta o digitalizador electrónico 164. Otros dispositivos de entrada (no mostrados) pueden incluir una palanca de juegos, un panel de juegos, una antena satelital, un escáner, o similares. Estos y otros dispositivos de entrada están a menudo conectados con la unidad 120 de procesamiento a través de una interfaz 160 de entrada de usuario que está acoplada con el bus del sistema, pero pueden estar conectados por otras estructuras de interfaz y de bus, tales como un puerto paralelo, un puerto de juegos o un bus universal en serie (USB). Un monitor 191 u otro tipo de dispositivo visor también está conectado con el bus 121 del sistema mediante una interfaz, tal como una interfaz 190 de vídeo. El monitor 191 también puede integrarse con un panel de pantalla táctil o similar. Obsérvese que el monitor y / o el panel de pantalla táctil puede estar físicamente acoplado con una carcasa en la cual está incorporado el dispositivo informático 110, tal como en un ordenador personal de tipo tableta. Además, los ordenadores tales como el dispositivo informático 110 también pueden incluir otros dispositivos periféricos de salida tales como los altavoces 197 y la impresora 196, que pueden conectarse a través de una interfaz periférica 194 de salida, o similar.

El ordenador 110 puede funcionar en una aplicación en red, usando conexiones lógicas con uno o más ordenadores remotos, tal como un ordenador remoto 180. El ordenador remoto 180 puede ser un ordenador personal, un servidor, un encaminador, un ordenador personal en red, un dispositivo a la par u otro nodo común de red, y habitualmente incluye muchos de, o todos, los elementos descritos anteriormente con respecto al ordenador 110, aunque sólo un dispositivo 181 de almacenamiento de memoria ha sido ilustrado en la FIG. 1. Las conexiones lógicas ilustradas en la FIG. 1 incluyen una red de área local (LAN) 171 y una red de área amplia (WAN) 173, pero también pueden incluir a otras redes. Tales aplicaciones de red son usuales en oficinas, redes de ordenadores de ámbito empresarial, intranets e Internet. Por ejemplo, el sistema informático 110 puede comprender la máquina de origen desde la cual se están migrando los datos, y el ordenador remoto 180 puede comprender la máquina de destino. Obsérvese, sin embargo, que las máquinas de origen y de destino no necesitan estar conectadas por una red o por otros medios cualesquiera, sino que, en cambio, los datos pueden migrarse mediante cualquier medio capaz de ser escrito por la plataforma de origen y leído por la plataforma, o plataformas, de destino.

Cuando se usa en una aplicación de redes LAN, el ordenador 110 se conecta con la LAN 171 a través de una interfaz o adaptador 170 de red. Cuando se usa en una aplicación de red WAN, el ordenador 170 incluye habitualmente un módem 172 u otro medio para establecer comunicaciones por la WAN 173, tal como Internet. El módem 172, que puede ser interno o externo, puede estar conectado con el bus 121 del sistema mediante la interfaz 160 de entrada de usuario, u otro mecanismo adecuado. En una aplicación en red, los módulos de programa ilustrados con respecto al ordenador 110, o partes del mismo, pueden almacenarse en el dispositivo remoto de almacenamiento de memoria. A modo de ejemplo, y no de limitación, la FIG. 1 ilustra los programas 185 de aplicación remota como residentes en el dispositivo 181 de memoria. Se apreciará que las conexiones de red mostradas son ejemplares y que pueden usarse otros medios para establecer un enlace de comunicaciones entre los ordenadores.

En la descripción siguiente, se describirá la invención con referencia a actos y representaciones simbólicas de operaciones que son llevadas a cabo por uno o más ordenadores, a menos que se indique lo contrario. Así pues, se entenderá que tales actos y operaciones, que se mencionan a veces como ejecutadas por ordenador, incluyen la manipulación, por parte de la unidad procesadora del ordenador, de las señales eléctricas que representan los datos en forma estructurada. Esta manipulación transforma los datos o los mantiene en ubicaciones en el sistema de memoria del ordenador, que reconfigura o altera de otro modo el funcionamiento del ordenador en una forma bien conocida por los expertos en la técnica. Las estructuras de datos donde se mantienen los datos son ubicaciones físicas de la memoria que tienen propiedades

específicas definidas por el formato de los datos. Sin embargo, si bien la invención se describe en el contexto precedente, no está concebido como limitador, ya que los expertos en la técnica apreciarán que varios actos y el funcionamiento descrito a continuación también pueden implementarse en hardware.

El Protocolo Sencillo de Transferencia de Correo (SMTP), con un servidor de Exchange, se usará para describir la invención. Exchange es un servidor de correo electrónico producido por la Corporación Microsoft. El SMTP es el protocolo predominante de correo electrónico usado en Internet. Si bien se usarán SMTP y Exchange, la invención puede usarse con otros protocolos de transferencia y servidores de correo. El SMTP es un protocolo de comunicación del Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP) que define los formatos de mensajes usados para la transferencia de correo desde un servidor de correo electrónico, tal como Exchange, mediante Internet, a otro servidor de correo electrónico. Según el SMTP, un mensaje de correo electrónico se envía habitualmente de la siguiente manera. Un usuario ejecuta un programa de correo electrónico para crear un mensaje de correo electrónico, y el programa de correo electrónico coloca el texto del mensaje y la información de control en una cola de mensajes salientes. La cola se implementa habitualmente como una colección de ficheros accesibles desde el servidor de correo electrónico.

El servidor de Exchange establece una conexión del Protocolo de Control de Transmisión (TCP) con el puerto reservado del SMTP en el servidor de correo electrónico de destino y usa el SMTP para transferir el mensaje por Internet. La sesión del SMTP entre los servidores remitentes y receptores da como resultado que el mensaje se transfiera desde una cola en el anfitrión remitente a una cola en el anfitrión receptor, por etapas. Las etapas varían desde la provisión por parte del servidor remitente de la dirección de IP de la conexión que se está estableciendo, hasta la recepción de todas las cabeceras de mensaje y contenidos de mensaje. Cuando se completa la transferencia del mensaje, el servidor receptor cierra la conexión del TCP usado por el SMTP, el anfitrión remitente quita el mensaje de su cola de correo, y el destinatario usa su programa de correo electrónico configurado para leer el mensaje en la cola de correo.

Pasando ahora a la FIG. 2, la pila 200 del SMTP se ejecuta dentro del servidor de información de Internet (IIS) 202, que es software servidor de red vendido por la Corporación Microsoft, instalado en el servidor 204. El IIS 202 se comunica, mediante el SMTP, con otros servidores 206 de Exchange, o servidores del SMTP (no mostrados), en Internet. El IIS 202 tiene una base de datos 208 que se usa para almacenar mensajes salientes o entrantes. Cuando se establece una conexión con el protocolo 200 del SMTP para un mensaje entrante, un suceso es activado y recibido por la aplicación 210. La aplicación 210 intercepta el mensaje y lo pasa a uno o más filtros 212. El filtro 212 analiza el mensaje, determina un nivel de confianza que tiene el filtro 212 en cuanto a si el mensaje es correo basura, y envía el nivel de confianza al entorno 210. La aplicación 210 decide, en base al nivel de confianza, si quiere invocar a otro filtro 212, o a una acción 214. La acción 214 incluye interrumpir la conexión, enviar el mensaje al transporte 216 de Exchange y borrar el mensaje. El transporte 216 de Exchange encamina el mensaje. Determina si el mensaje ha de entregarse a un buzón en el servidor 204 o si debe ir, mediante el SMTP 200, a otro servidor 206.

Pasando ahora a la FIG. 3, los filtros 212 consisten en diversos tipos de tecnologías de detección de anti-correo basura. Por ejemplo, los tipos de filtros 212 pueden ser un módulo 300 de lista de agujeros negros en tiempo real, un módulo no lineal 302, una API 304 antivirus que los módulos antivirus 306 usan para comunicarse con el servidor 204 de Exchange, un módulo 308 de lista de dominio y otros filtros 310 que usan sus propias reglas para determinar si un mensaje es correo basura. Por ejemplo, los otros filtros pueden ser de clasificación de textos, de coincidencia de palabras clave, etc.

El módulo 300 de lista de agujeros negros en tiempo real compara la dirección de IP del remitente del mensaje con una lista conocida de direcciones de correo basura. Si la dirección de IP está en la lista conocida, el servidor 204 de Exchange no acepta el correo. El módulo 302 no lineal normaliza los niveles de confianza del filtro 212 usando funciones tales como una curva en forma de s, una función Bayesiana, y similares, que fuerzan la separación entre el correo basura y los mensajes legítimos. Por ejemplo, si un filtro 212 devuelve un nivel de confianza del 95%, el módulo no lineal 302 puede ajustar el nivel de confianza al 96%, mientras que un nivel de confianza del 40% puede ser ajustado hasta un nivel de confianza del 30%. El módulo 308 de lista de dominio rechaza el correo durante el intercambio del protocolo SMTP entre el remitente y el servidor de Exchange, en base a la información disponible. incluyendo la dirección de correo y / o dominio de los remitentes, el destinatario, o destinatarios, del correo y las características del cuerpo efectivo del mensaje, tal como el identificador de mensaje, la fecha, el asunto y el tipo y nombre de anexos.

La aplicación 210 gestiona la invocación de uno o más de los filtros anti-correo basura 212, normaliza los resultados de cada invocación, evalúa el resultado normalizado y aplica alguna acción sobre el resultado. La aplicación 210 se despliega, muy habitualmente, en los servidores 204 en el borde de una red (es decir, los servidores de correo que son los primeros en recibir mensajes de correo electrónico desde Internet). Algunas de las tecnologías usadas, tales como la clasificación de textos, pueden utilizarse para usos distintos, tal como la identificación de la importancia o la sensibilidad de un mensaje. Como resultado de esto, la aplicación también puede desplegarse útilmente en servidores internos. La aplicación 210 puede usarse únicamente como una biblioteca de utilidades que son invocadas por implementaciones autónomas existentes de detección de correo basura, para ayudar a la migración desde las implementaciones autónomas o, más preferiblemente, como un envoltorio que proporciona una abstracción del mecanismo subyacente de sucesos (descrito

más adelante) que se usa para invocar a los filtros anti-correo basura 212. La realización del envoltorio permite que los filtros anti-correo basura 212 desarrollados para el correo electrónico también se usen para otras soluciones de mensajería, tales como la Mensajería Instantánea, la determinación de mensajes de acoso, etc. En cualquier caso, la aplicación se entrega como una biblioteca que se enlaza con la tecnología anti-correo basura en tiempo de configuración o de ejecución.

La arquitectura de una pila 200 del SMTP en Exchange es tal que los sucesos son activados por (es decir, originados desde) la pila 200 hacia sumideros de sucesos, que se implementan habitualmente como objetos COM. Cuando se despliega una nueva tecnología anti-correo basura, implementa un objeto COM que se registra en el sistema de sucesos del protocolo en tiempo de instalación. El código de registro es entregado por la aplicación 210. La instalación dla aplicación 210 incluye la instalación del software en el servidor en cuestión, el registro del sumidero de sucesos, la habilitación o inhabilitación de técnicas específicas para el servidor específico, mediante una consola de administrador del sistema, y el establecimiento de las estrategias de evaluación y de acción a seguir cuando se recibe correo basura. La habilitación / inhabilitación de una técnica específica mejora la gestionabilidad dla aplicación 210, al permitir que todos los servidores en una red contengan idénticos códigos binarios del software.

Pasando ahora a la FIG. 4, se ilustra el proceso de integrar los módulos anti-correo basura 212 y de determinar si un mensaje es correo basura. En tiempo de ejecución, cuando se abre una conexión con la pila 200 del SMTP (y a ella apunta a continuación), se activa un suceso (etapa 400). Un sistema de despacho de sucesos inspecciona la lista de registros e invoca al correspondiente objeto. La invocación llega al entorno 210, bien directamente cuando está actuando como un envoltorio, o bien indirectamente cuando está siendo llamada como una función de biblioteca (etapa 402). En ambos casos, la aplicación 210 examina su propia configuración para determinar cuál de las tecnologías anti-correo basura 300-310 en las cuales ha sido registrado ha sido “habilitada” o “inhabilitada” por el Administrador del Sistema. Se enumeran las tecnologías anti-correo basura que han sido habilitadas, y se fija en cero un resumen de los niveles de confianza de correo basura (etapa 404).

Si el específico filtro anti-correo basura 212 está “habilitado”, la aplicación 210 obtiene aquella información que esté disponible para que la examine el filtro anti-correo basura 212, y envía la información al filtro 212 (etapa 406). La magnitud y el tipo de información disponible cambiarán según la etapa del protocolo en la cual se invoque al filtro 212. Por ejemplo, la primera vez que se invoque puede haber solamente información acerca de la dirección de IP de la conexión que se está estableciendo. En la última llamada antes de que el mensaje sea aceptado por el sistema, estarán disponibles todas las cabeceras y contenidos de mensaje. Si la aplicación 210 es capaz de descifrar el contenido codificado del mensaje, la aplicación 210 descifrará el contenido codificado del mensaje en una forma más directamente utilizable por el filtro anti-correo basura 212. Cuando la aplicación se implementa como un envoltorio, esta información está automáticamente disponible. Cuando se implementa como una biblioteca, la información solamente estará disponible si es específicamente solicitada por el filtro anti-correo basura 212. Independientemente de la forma dla aplicación (es decir, envoltorio o biblioteca), las funciones utilitarias tales como el descifrado del contenido del mensaje son invocadas pasivamente por el filtro anti-correo basura para reducir la carga de la CPU: En una realización, la aplicación 210 también proporciona una búsqueda de direcciones de destinatario en el mensaje, que el filtro 212 puede usar como parte de su evaluación de una pieza de correo como correo basura.

Al completar su evaluación, el filtro 212 devuelve al entorno 210, bien por valor o referencia de retorno (o llamando a la biblioteca dla aplicación), una evaluación de la confianza que la solución tiene en cuanto a que el específico mensaje de correo es correo basura (etapa 408). La aplicación 210 espera habitualmente una respuesta en la gama entre 0 y 100%, donde 0% representa, claramente, la ausencia de correo basura y 100% representa claramente el correo basura. En una realización, el porcentaje se indica como un número entre 0 y 1.000. Para asimilar las diversas tecnologías anti-correo basura 300-310 que usan distintas medidas, la aplicación 210 proporciona un factor de ajuste o afinación a aplicar a los resultados de cada filtro individual 212 invocado para crear un nivel normalizado o afinado de confianza de correo basura (etapa 410). El factor de ajuste o afinación es configurado por el administrador del servidor 204. Esto constituye la normalización que la aplicación debe realizar a fin de comparar los resultados de distintos filtros 212. Este número normalizado se denominará el nivel de confianza de correo basura. El nivel de confianza de correo basura se suma al resumen de niveles de confianza de correo basura (etapa 412). La aplicación 210 almacenará el nivel calculado de confianza de correo basura como una suma variable, bien en el mismo mensaje para su preservación, y / o en memoria para mayores prestaciones. Los resultados de la evaluación de soluciones sucesivas se suman al resumen de niveles de confianza de correo basura.

La normalización (es decir, la aplicación del factor de ajuste) puede implementarse en una gran variedad de formas. Por ejemplo, una forma de normalizar los resultados es confiar igualmente en los resultados de cada filtro 212 y simplemente sumar los resultados (p. ej., 0,5 + 0,7 + 0,8 + ... = resumen). Otra forma es aplicar un ajuste para cada uno. Por ejemplo, si al administrador le gusta la forma en que un filtro específico detecta el correo basura, el administrador ajustaría el nivel de confianza de correo basura de ese filtro con un número relativamente alto (p. ej., 0,9). De manera similar, si hay un filtro sobre el cual el administrador no se siente muy seguro, el administrador ajusta el nivel de confianza de correo basura de

ese filtro con un número relativamente bajo (p. ej., 0,3). Otro ejemplo de un factor de ajuste es usar una normalización no lineal del nivel de confianza, usando una curva ponderada tal como una curva en forma de s. Por ejemplo, si un filtro 212 devuelve un nivel de confianza de correo basura del 95%, el factor de ajuste lo ajusta más alto, por ejemplo, al 96%. Si el nivel de confianza de correo basura está en el medio de la gama (p. ej., entre 50 y 55%), se aplica un ajuste más radical para ajustarlo más hacia abajo (p. ej., entre 30 y 35%).

La aplicación 210 proporciona al administrador la capacidad de fijar varios umbrales que permiten al administrador definir distintas acciones a aplicar sobre un mensaje, en base al máximo umbral superado por el resumen de los niveles de confianza de correo basura. Las acciones pueden ser evitar que el mensaje sea entregado hasta que se tenga una idea mejor de si el mensaje es o no correo basura, interrumpir la conexión, enviar un mensaje de no entrega al remitente, borrar el mensaje, pasarlo a otro filtro 212 en base al resumen de niveles de confianza de correo basura, enviar el mensaje al destinatario, etc. Un conjunto por omisión de umbrales y de las correspondientes acciones se proporciona en la aplicación 210.

El resumen de los niveles ajustados de confianza de correo basura se compara con el umbral máximo fijado por el administrador (etapa 414). Si el resumen de los niveles de confianza de correo basura supera el umbral máximo, se aplica la acción configurada para el umbral máximo (etapa 416). Si el resumen de niveles de confianza de correo basura no supera el nivel máximo de umbral y si hay más filtros 212 que pueden usarse para evaluar el mensaje (etapa 418), se repiten las etapas 404 a 416 hasta que bien el umbral máximo haya sido superado, o bien se haya recibido el final del mensaje (etapa 420). Si no se ha recibido el final del mensaje, la pila 200 del SMTP avanza al estado de aceptación del próximo mensaje (422) y se repiten las etapas 406 a 420 para el próximo estado de aceptación de mensaje. Si se ha recibido el final del mensaje y todos los filtros habilitados han analizado el mensaje, se compara el resumen de los niveles de confianza de correo basura con los umbrales restantes, en orden descendente desde el umbral máximo hasta el umbral mínimo (etapa 424), hasta que el resumen de los niveles de confianza de correo basura supere un umbral (426). Si el resumen de los niveles de confianza de correo basura supera un umbral, se aplica la acción configurada para ese umbral.

En resumen, después de que un filtro 212 ha completado su análisis, la aplicación 210 evalúa el resumen de los niveles de confianza de correo basura con respecto a un conjunto de umbrales definidos por el administrador. Si el resumen de los niveles de confianza de correo basura es mayor que el mayor umbral fijado por el administrador, entonces se aplica la acción especificada para el mayor umbral con respecto al mensaje. En caso contrario, se usan filtros subsiguientes para evaluar el mensaje, hasta que bien se supera el umbral máximo, o bien todos los filtros han evaluado el mensaje. Después de que todos los filtros han evaluado el mensaje, el resumen de los niveles de confianza de correo basura se compara con todos los umbrales, y se selecciona el umbral coincidente. Se aplica entonces la acción asociada a ese umbral. Por ejemplo, si el resumen de los niveles de confianza de correo basura supera un umbral de nivel de confianza del 99%, la conexión del mensaje puede interrumpirse silenciosamente. Si el resumen de los niveles de confianza de correo basura supera un umbral de nivel de confianza del 70%, un informe de no entrega puede ser devuelto al remitente. Si el resumen de los niveles de confianza de correo basura supera un umbral de nivel de confianza del 40%, el mensaje puede entregarse a una carpeta de “correo basura” en el buzón del usuario. Si el resumen de los niveles de confianza de correo basura no supera ninguno de los umbrales (etapa 428), el mensaje puede considerarse legítimo y entregarse a la bandeja de entrada del usuario.

El nivel de confianza de correo basura para un mensaje se propaga por el mensaje cuando se envía entre servidores en una organización (y entre organizaciones). Esto admite un enfoque gradual para la gestión de distintos niveles de correo basura. Por ejemplo, los servidores de pasarela (es decir, servidores en los puntos de entrada de una organización) en una organización pueden realizar acciones destructivas, tales como rechazar o borrar correo basura con altos valores del nivel de confianza de correo basura. Alternativamente, los servidores de pasarela archivan los mensajes con un alto nivel de confianza de correo basura, de modo que los administradores puedan comprobar los mensajes para verificar el funcionamiento de los filtros anti-correo basura 212. Los servidores de trastienda pueden realizar acciones menos destructivas para valores inferiores del nivel de confianza de correo basura, tales como llevar el mensaje a una carpeta especial de correo basura.

En algunos casos, es difícil determinar un factor razonable de ajuste entre distintas soluciones anti-correo basura, a fin de determinar un nivel final normalizado de confianza de correo basura. En estos casos, el algoritmo por omisión para combinar los valores del nivel de confianza de correo basura de múltiples filtros anti-correo basura 212 es tomar el mayor nivel de confianza de correo basura devuelto (después de que haya sido ajustado en la gama normalizada, tal como entre 0 y 9) como el nivel final de confianza de correo basura para el mensaje. En esta realización, los filtros anti-correo basura 212 se invocan y cada sumidero anti-correo basura devuelve un nivel de confianza de correo basura. Se determina el mayor nivel de confianza de correo basura y se compara con los umbrales, según lo descrito anteriormente. Obsérvese que este algoritmo implica que la solución anti-correo basura más agresiva ganará siempre, y tiene el efecto de que según se añaden más filtros anti-correo basura, menos correo correo basura tiende a colarse. Obsérvese que es posible que un filtro anti-correo basura 212 pueda ser demasiado agresivo y determinar que mensajes legítimos son correo basura, con más frecuencia que otros filtros anti-correo basura 212. En tal situación, el nivel de confianza de correo basura del filtro

anti-correo basura que es demasiado agresivo se inhabilita, o se ajusta, de modo tal que se reduzca el número de mensajes legítimos clasificados como correo basura.

En todos los puntos, las acciones aplicadas para un mensaje específico pueden registrarse o añadirse a una tabla de rastreo de mensajes, según el nivel de información que el administrador escoge registrar. Un conjunto por omisión de acciones está disponible para el administrador con la aplicación 210. Pueden añadirse acciones adicionales, proporcionando código de ejecución de acciones adicionales, de manera similar a la usada para desplegar nuevos filtros anti-correo basura.

Cualquier mensaje aceptado para su entrega a un buzón por la aplicación 210 tendrá el resumen de niveles de confianza de correo basura de ese mensaje almacenado en el mismo, en una propiedad bien conocida. Un agente de entrega que procese el mensaje puede escoger evaluar esta propiedad como parte de su propia lógica. Un cliente que ve el mensaje, o una tabla de tales mensajes, puede escoger enumerar los mensajes en orden ascendiente o descendiente del resumen de niveles de confianza de correo basura, como ayuda para identificar aquellos mensajes que pueden haber sido mal calculados.

Puede verse que se ha descrito una plataforma que permite que el correo basura y los virus puedan ser detectados y gestionados en el borde de la frontera de red, usando una gran variedad de filtros y tecnologías anti-correo basura, existentes y futuras, La plataforma permite que las soluciones y tecnologías interactúen y sean gestionadas de manera racional, proporcionando por ello la capacidad de desplegar una rápida innovación en el lado del servidor, en la aplicación bélico de la detección de correo basura.

A la vista de las muchas realizaciones posibles a las cuales pueden aplicarse los principios de esta invención, debería reconocerse que la realización descrita en el presente documento con respecto a las figuras de los dibujos está concebida para ser solamente ilustrativa, y no debería tomarse como limitadora del alcance de la invención. Por ejemplo, aquellos expertos en la técnica reconocerán que los elementos de la realización ilustrada mostrada en software pueden implementarse en hardware, y viceversa, o que la realización ilustrada puede modificarse en su disposición y detalle sin apartarse de la invención. Por lo tanto, la invención, según lo descrito en el presente documento, contempla todas esas realizaciones como incluidas dentro del alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para determinar si un mensaje es correo basura en un sistema con una pluralidad de módulos anti-correo basura, que comprende las etapas de:

invocar a una pluralidad de la pluralidad de módulos anti-correo basura (212);

recibir un nivel de confianza de correo basura de cada uno entre la pluralidad de la pluralidad de módulos anti-correo basura (212);

determinar un mayor nivel de confianza de correo basura a partir de los niveles de confianza de correo basura;

comparar el mayor nivel de confianza de correo basura con al menos un umbral; y

invocar una acción (214) asociada a dicho(s) umbral(es) si el mayor nivel de confianza de correo basura es mayor que dicho(s) umbral(es),

en el que la etapa de invocar la acción (214) incluye:

interrumpir la conexión usada para transferir el mensaje si el mayor nivel de confianza de correo basura supera un primer nivel de umbral;

devolver un mensaje de no entrega a un remitente si el mayor nivel de confianza de correo basura supera un segundo nivel de umbral y está por debajo del primer nivel de umbral;

entregar el mensaje a una carpeta de correo basura si el mayor nivel de confianza de correo basura supera un tercer nivel de umbral y está por debajo del segundo nivel de umbral.

2. El procedimiento de la reivindicación 1, que comprende adicionalmente la etapa de aplicar un factor de afinación a al menos un nivel de confianza de correo basura, para crear al menos un nivel afinado de confianza de correo basura, y en el cual la etapa de determinar un mayor nivel de confianza de correo basura comprende la etapa de determinar el mayor de dicho(s) nivel(es) afinado(s) de confianza de correo basura entre los niveles de confianza de correo basura a los que se aplicó el factor de afinación.

3. El procedimiento de la reivindicación 2, en el cual la etapa de aplicar un factor de afinación comprende afinar dicho(s) nivel(es) de confianza de correo basura con el nivel de confianza de un usuario en el módulo anti-correo basura asociado a dicho(s) nivel(es) de confianza de correo basura.

4. El procedimiento de la reivindicación 1, que comprende adicionalmente la etapa de ajustar cada nivel de confianza de correo basura en una gama normalizada.

5. El procedimiento de la reivindicación 4, en el cual la gama normalizada está entre 0 y 9.

6. El procedimiento de la reivindicación 1, que comprende adicionalmente la etapa de añadir el nivel de confianza de correo basura al mensaje.

7. El procedimiento de la reivindicación 1, en el cual dicho(s) umbral(es) comprende(n) una pluralidad de umbrales, que incluye un umbral máximo y un umbral mínimo, comprendiendo adicionalmente el procedimiento las etapas de:

comparar el mayor nivel de confianza de correo basura con cada uno entre la pluralidad de umbrales;

determinar si el mayor nivel de confianza de correo basura es mayor que al menos uno entre la pluralidad de umbrales;

si el mayor nivel de confianza de correo basura es mayor que al menos uno entre la pluralidad de umbrales:

comparar el mayor nivel de confianza de correo basura con los umbrales, en orden

desde el umbral máximo hasta el umbral mínimo, hasta que el mayor nivel de confianza de correo basura supere un umbral, y aplicar la acción configurada para ese umbral.

8. El procedimiento de la reivindicación 1, en el cual la etapa de invocar la acción (214) incluye invocar uno entre borrar el mensaje, enviar una notificación de no envío, archivar el mensaje y pasar el mensaje con el mayor nivel de confianza de correo basura a un cliente.

9. El procedimiento de la reivindicación 1, en el cual el primer umbral es un nivel de confianza de correo basura del noventa y nueve por ciento, el segundo umbral es un nivel de confianza de correo basura del setenta por ciento y el tercer nivel de

umbral es un nivel de confianza de correo basura del cuarenta por ciento.

10. El procedimiento de la reivindicación 1, que comprende adicionalmente la etapa de registrar la acción (214) aplicada con el mensaje.

11. Un medio legible por ordenador con instrucciones ejecutables por ordenador, para determinar si un mensaje es correo basura, en un sistema con una pluralidad de módulos anti-correo basura (212), comprendiendo las instrucciones las etapas de:

recibir un nivel de confianza de correo basura desde cada uno entre una pluralidad de la pluralidad de módulos anti-correo basura (212);

determinar un mayor nivel de confianza de correo basura;

comparar el mayor nivel de confianza de correo basura con al menos un umbral; y

invocar una acción (214) asociada a dicho(s) umbral(es) si el mayor nivel de confianza de correo basura es mayor que dicho(s) umbral(es),

en el que la etapa de invocar la acción (214) incluye:

interrumpir la conexión usada para transferir el mensaje si el mayor nivel de confianza de correo basura supera un primer nivel de umbral;

devolver un mensaje de no entrega a un remitente si el mayor nivel de confianza de correo basura supera un segundo nivel de umbral y está por debajo del primer nivel de umbral;

entregar el mensaje a una carpeta de correo basura si el mayor nivel de confianza de correo basura supera un tercer nivel de umbral y está por debajo del segundo nivel de umbral.

12. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar la etapa de aplicar un factor de afinación a al menos un nivel de confianza de correo basura, para crear al menos un nivel afinado de confianza de correo basura, y en el cual la etapa de determinar un mayor nivel de confianza de correo basura comprende la etapa de determinar el mayor de dicho(s) nivel(es) afinado(s) de confianza de correo basura entre los niveles de confianza de correo basura a los que se aplicó el factor de afinación.

13. El medio legible por ordenador de la reivindicación 12, en el cual la etapa de aplicar un factor de afinación comprende afinar dicho(s) nivel(es) de confianza de correo basura con un nivel de confianza de un usuario en el módulo anti-correo basura asociado a dicho(s) nivel(es) de confianza de correo basura.

14. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar la etapa de ajustar cada nivel de confianza de correo basura en una gama normalizada.

15. El medio legible por ordenador de la reivindicación 14, en el cual la gama normalizada está entre 0 y 9.

16. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar la etapa de añadir el nivel de confianza de correo basura al mensaje.

17. El medio legible por ordenador de la reivindicación 11, en el cual dicho(s) umbral(es) comprende(n) una pluralidad de umbrales que incluyen un umbral máximo y un umbral mínimo, teniendo el medio legible por ordenador instrucciones adicionales ejecutables por ordenador, para realizar las etapas de:

comparar el mayor nivel de confianza de correo basura con cada uno entre la pluralidad de umbrales;

determinar si el mayor nivel de confianza de correo basura es mayor que al menos uno entre la pluralidad de umbrales;

si el mayor nivel de confianza de correo basura es mayor que al menos uno entre la pluralidad de umbrales:

comparar el mayor nivel de confianza de correo basura con los umbrales, en orden

desde el umbral máximo hasta el umbral mínimo, hasta que el mayor nivel de confianza de correo basura supere un umbral, y aplicar la acción configurada para ese umbral.

18. El medio legible por ordenador de la reivindicación 11, en el cual la etapa de invocar la acción (214) incluye invocar a uno entre borrar el mensaje, enviar una notificación de no entrega, archivar el mensaje y pasar el mensaje con el mayor nivel de confianza de correo basura a un cliente.

19. El medio legible por ordenador de la reivindicación 11, en el cual el primer umbral es un nivel de confianza de correo basura del noventa y nueve por ciento, el segundo umbral es un nivel de confianza de correo basura del setenta por ciento y el tercer nivel de umbral es un nivel de confianza de correo basura del cuarenta por ciento.

20. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar las etapas de registrar la acción (214) aplicada con el mensaje.

21. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar las etapas de invocar a la pluralidad de la pluralidad de módulos anti-correo basura (212).

22. El medio legible por ordenador de la reivindicación 21, en el cual la etapa de invocar a la pluralidad de la pluralidad de módulos anti-correo basura (212) incluye la etapa de proporcionar las direcciones de los destinatarios de un mensaje de correo.

23. El medio legible por ordenador de la reivindicación 11, con instrucciones adicionales ejecutables por ordenador, para realizar la etapa que comprende descifrar un contenido codificado del mensaje.

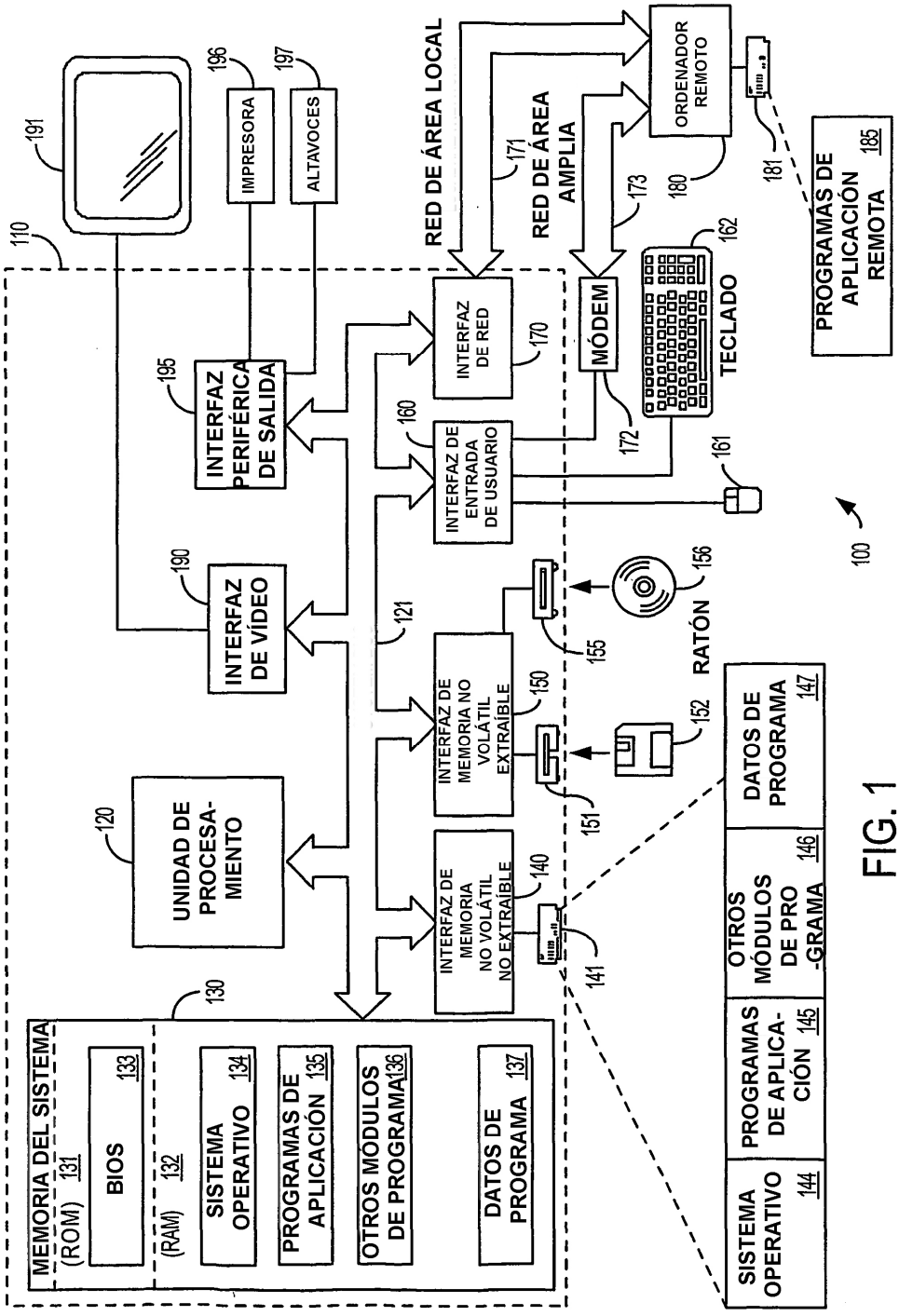
110
191
196
IMPRESORA
197
ALTAVOCES
RED DE ÁREA LOCAL
RED DE ÁREA AMPLIA
ORDENADOR REMOTO
180
181
PROGRAMAS DE APLICACIÓN REMOTA
185
171
173
162
TECLADO
INTERFAZ PERIFÉRICA DE SALIDA
195
INTERFAZ DE RED
170
MÓDEM
172
160
INTERFAZ DE ENTRADA DE USUARIO
161
190
INTERFAZ DE VÍDEO
121
156
RATÓN
155
150
INTERFAZ DE MEMORIA NO VOLÁTIL EXTRAÍBLE
152
151
120
UNIDAD DE PROCESA-MIENTO
140
INTERFAZ DE MEMORIA NO VOLÁTIL NO EXTRAÍBLE
141
130
MEMORIA DEL SISTEMA
(ROM) 131
BIOS 133
(RAM) 132
SISTEMA OPERATIVO 134
PROGRAMAS DE APLICACIÓN 135
OTROS MÓDULOS DE PROGRAMA 136
DATOS DE PROGRAMA 137
SISTEMA OPERATIVO 144
PROGRAMAS DE APLICA-CIÓN 145
OTROS MÓDULOS DE PRO -GRAMA 146
DATOS DE PROGRAMA 147
100

FIG. 1

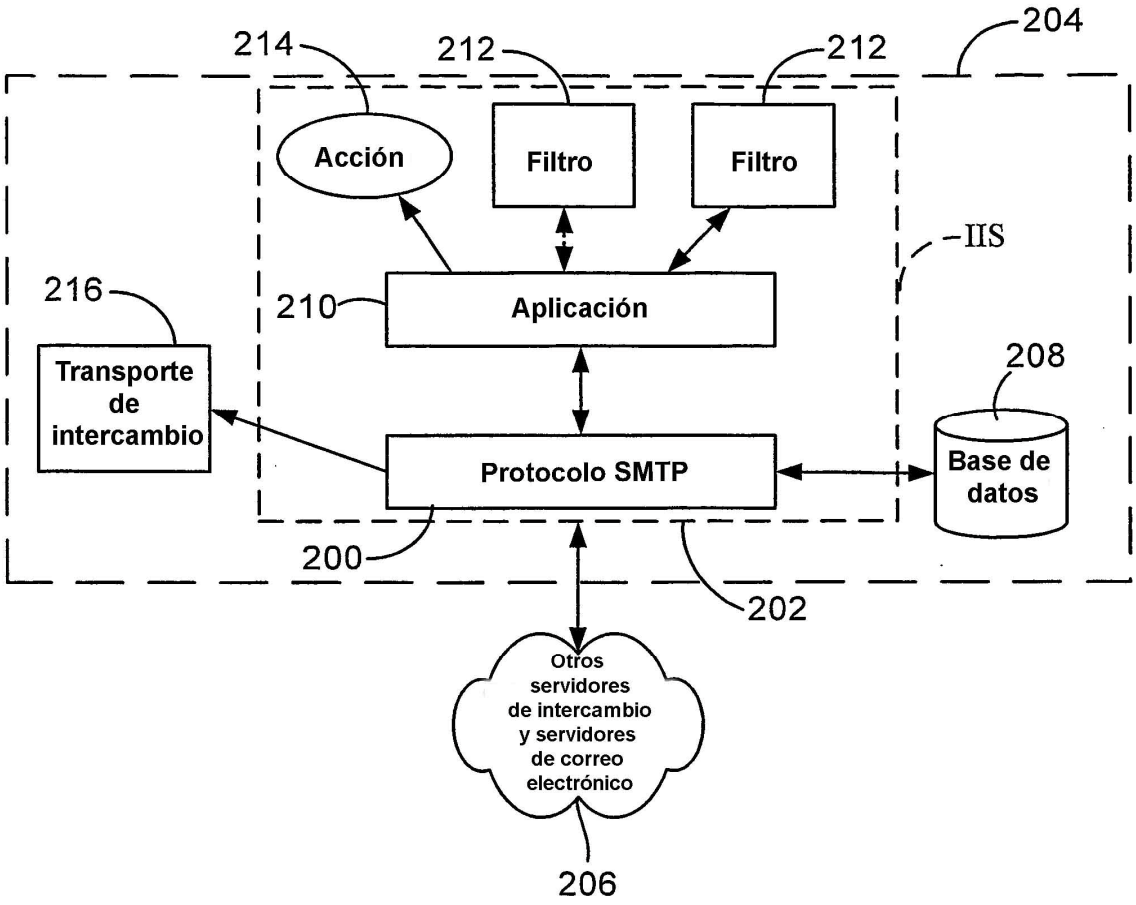
214
212
212
204
Acción
Filtro
Filtro
IIS
216
210
Aplicación
208
Transporte de intercambio
Protocolo SMTP
Base de datos
200
202
Otros servidores de intercambio y servidores de correo electrónico
206

FIG. 2

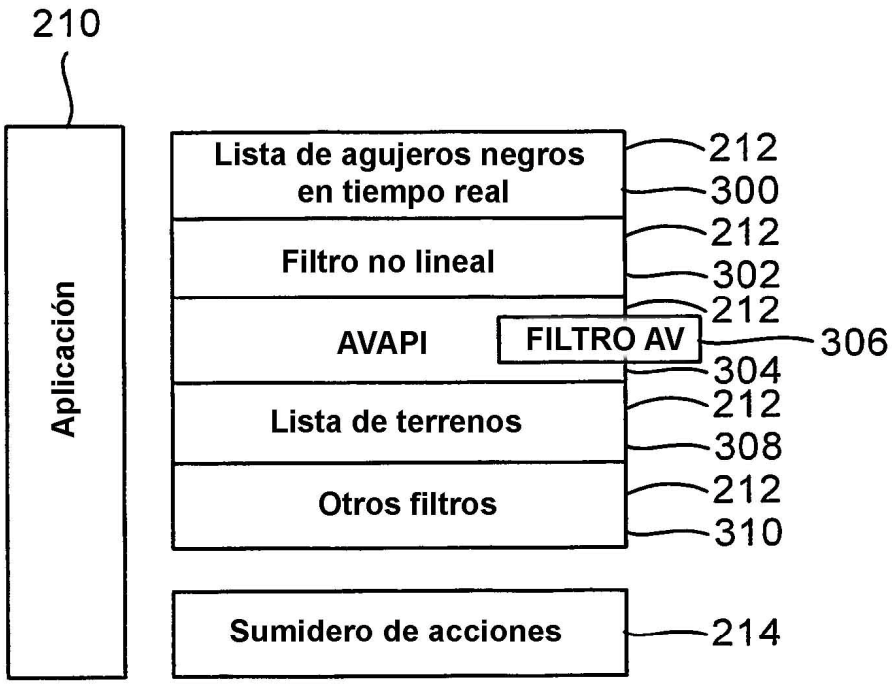
210
Aplicación
Lista de agujeros negros en tiempo real
212
300
Filtro no lineal
212
302
AVAPI
FILTRO AV
212
306
304
Lista de terrenos
212
308
Otros filtros
212
310
Sumidero de acciones
214

FIG. 3

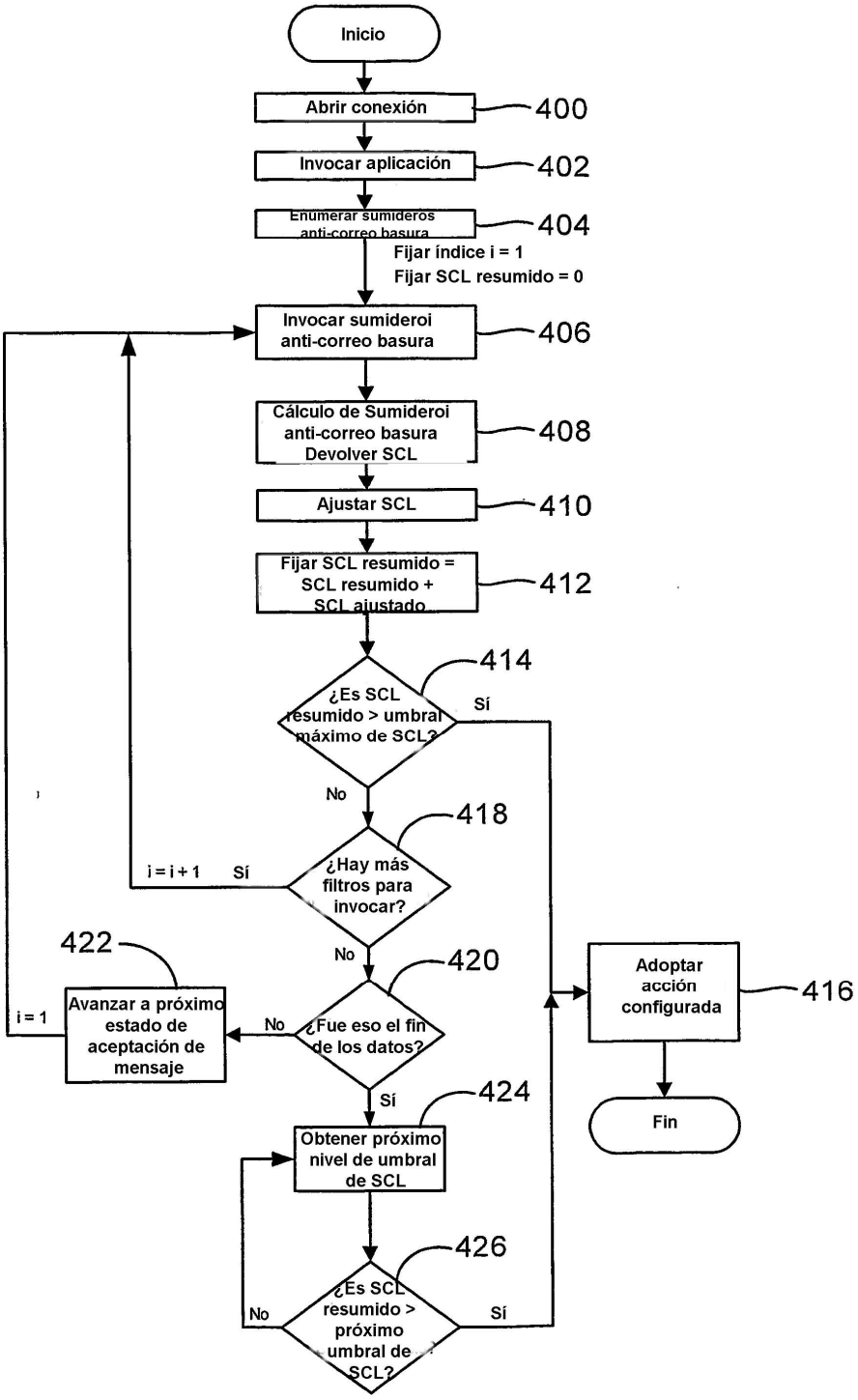
Inicio
Abrir conexión
400
Invocar aplicación
402
Enumerar sumideros anti-correo basura
404
Fijar índice i = 1
Fijar SCL resumido = 0
Invocar sumideroi anti-correo basura
406
Cálculo de Sumideroi anti-correo basura Devolver SCL
408
Ajustar SCL
410
Fijar SCL resumido = SCL resumido + SCL ajustado
412
414
¿Es SCL resumido > umbral máximo de SCL?
Sí
No
418
¿Hay más filtros para invocar?
i = i + 1
Sí
No
420
¿Fue eso el fin de los datos?
422
Avanzar a próximo estado de aceptación de mensaje
i = 1
No
Sí
424
Obtener próximo nivel de umbral de SCL
426
¿Es SCL resumido > próximo umbral de SCL?
No
Sí
Adoptar acción configurada
416
Fin

FIG. 4