(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 338**

(51) Int. CI.:
H04L 29/06 (2006.01)
G06F 21/00 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02013985 .3**
(96) Fecha de presentación: **25.06.2002**
(97) Número de publicación de la solicitud: **1278350**
(97) Fecha de publicación de la solicitud: **22.01.2003**

(54) Título: **Autenticación de credenciales para usuarios móviles**

(30) Prioridad:
28.06.2001 US 894607

(45) Fecha de publicación de la mención BOPI:
12.11.2012

(45) Fecha de la publicación del folleto de la patente:
12.11.2012

(73) Titular/es:
MICROSOFT CORPORATION (100.0%)
ONE MICROSOFT WAY
REDMOND, WA 98052, US

(72) Inventor/es:
FISHMAN, NEIL S. y
KRAMER, MICHAEL

(74) Agente/Representante:
CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Autenticación de credenciales para usuarios móviles

Antecedentes de la invención

1. El campo de la invención

La presente invención se refiere a credenciales de autenticación. Más específicamente, la presente invención se refiere a procedimientos, sistemas y productos de programa de ordenador para autenticar a un cliente móvil, que pueden tener un sistema de entrada optimizado para la entrada numérica.

2. Antecedentes y técnica relacionada

El contenido almacenado en las redes es protegido a menudo por un buen número de razones. Por ejemplo, el contenido puede incluir tecnología de propiedad industrial que proporciona a una empresa una ventaja competitiva. Muchos empleadores consideran al menos alguna parte de su información de personal como privada o confidencial. Puede ser importante proteger cierto contenido vital, tal como pedidos de clientes, contra la corrupción o la pérdida. Ya sea que la motivación sea asegurar la confidencialidad o la privacidad, impedir la corrupción o pérdida de contenido, o asegurar información sensible, el acceso a las redes de ordenadores está usualmente gobernado mediante credenciales de autenticación, tales como un nombre de usuario y una contraseña, para un sistema o dominio específico.

Sin embargo, las credenciales de autenticación para una red de ordenadores pueden quedar comprometidas de un buen número de maneras, incluyendo los ataques de fuerza bruta, la monitorización del tráfico de red y la obtención de acceso a sistemas de terceros que almacenan credenciales de autenticación. En un ataque de fuerza bruta, un gran número de potenciales credenciales de autenticación, tal vez todas las combinaciones posibles, se presentan a una red de ordenadores. Por ejemplo, un PIN (Número de Identificación Personal) de cuatro dígitos podría ser descubierto presentando los números entre 0000 y 9999. Aunque la presentación de diez mil números puede parecer una tarea significativa, para los ordenadores la carga es mínima, a lo sumo.

Una defensa usual ante los ataques de fuerza bruta es aumentar el número de posibilidades que deben presentarse. Cada dígito añadido aumenta el número de selecciones potenciales en un factor de diez. Si se dispone de letras además de números, cada carácter representa un factor de treinta y seis. La inclusión de letras mayúsculas y minúsculas aumenta el peso de cada carácter hasta sesenta y dos. Para una máxima protección, puede añadirse puntuación a los números y letras, llegando a unas familiares ciento y una posibles elecciones para cada carácter. (Los teclados ingleses habituales vendidos en los Estados Unidos se describen como teclados 101, lo que indica el número de caracteres imprimibles que disponen de soporte). Incluso si no se permiten algunos caracteres, con alrededor de cien opciones para cada uno de los cuatro caracteres, el número de combinaciones distintas se aproxima a los 100 millones, una mejora significativa con respecto a las diez mil combinaciones ofrecidas por un PIN de cuatro dígitos.

Debido a que las combinaciones arbitrarias de números, letras y puntuación son difíciles de recordar, las palabras, las fechas, los acrónimos y similares pueden ayudar a lograr que las credenciales de autenticación sean familiares. Los atacantes explotan esta debilidad empleando un tipo de ataque de fuerza bruta, conocido habitualmente como un ataque de diccionario. No hay ninguna necesidad de probar todas las combinaciones de letras o números; en cambio, solamente se presentan combinaciones que tengan sentido, tales como palabras, acrónimos o fechas. La limitación del ataque a un “diccionario” puede llevar a reducir nuestra mejora de 100 millones a la gama de diez o veinte mil, e incluso menos si se consideran solamente palabras relativamente comunes.

Para reducir la amenaza planteada por los ataques de diccionario, los administradores de redes pueden imponer políticas con respecto a las credenciales de autenticación. Por ejemplo, puede requerirse que las contraseñas incluyan al menos una letra mayúscula, al menos una letra minúscula, al menos un número y al menos un signo de puntuación. Además, puede imponerse una cierta longitud, tal como cinco, seis, siete u ocho caracteres. Debido a que las contraseñas largas son más difíciles de recordar, la especificación de mucho más de ocho caracteres puede ser contraindicada, porque las contraseñas se escribirán en lugar de ser memorizadas, admitiendo que queden comprometidas las credenciales de autenticación si la contraseña escrita es descubierta alguna vez. Por ejemplo, una ocurrencia demasiado común en un contexto financiero es almacenar un PIN con su correspondiente tarjeta de carga o débito. Cualquier valor del PIN está prácticamente perdido si el PIN debe escribirse para ser recordado. Existen cuestiones similares en otros entornos, en particular con respecto al acceso a redes de ordenadores.

Recientemente, ha habido una demanda creciente de acceso a redes de ordenadores, y al contenido que puedan ofrecer, usando clientes móviles. Debido a su tamaño conveniente y a su utilidad, los teléfonos están entre los clientes móviles más extensamente utilizados. Sin embargo, algunos clientes móviles, tales como los teléfonos, tienen sistemas de entrada que están optimizadas para la entrada numérica. Si bien puede disponerse de letras y de puntuación, a menudo es bastante engorroso para la mayoría de los usuarios ingresar caracteres cualesquiera que no sean números.

Como se ha descrito anteriormente, admitir credenciales de autenticación que solamente contengan dígitos hace a una red de ordenadores vulnerable a los ataques de fuerza bruta.

Además, pueden estar implicados terceros en la provisión de acceso móvil al contenido. Por ejemplo, los teléfonos pueden conectarse con un servidor del protocolo de aplicaciones inalámbricas ("WAP") al alcanzar una red o servidor de contenidos deseados. En muchas circunstancias, el servidor de WAP y la red estarán totalmente desvinculados. Las empresas pueden ser reacias o incapaces para asumir el gasto de ofrecer acceso móvil a su red, mientras que los portadores telefónicos podrán usar servidores de WAP como una fuente de ingresos, mediante el tiempo de conexión aumentado.

Los servidores intermedios representan un riesgo de seguridad, porque los protocolos inalámbricos pueden no proveer conexiones seguras de extremo a extremo. Las conexiones seguras pueden limitarse a cada salto, tal como una conexión segura entre un teléfono y un servidor de WAP, y una conexión segura entre el servidor de WAP y la red a la que se está accediendo. Como resultado, el servidor de WAP contendrá contenido no cifrado. Por ejemplo, el teléfono puede ingresar credenciales de autenticación que son cifradas durante el tránsito al servidor de WAP. El servidor de WAP descifra las credenciales de autenticación en base al protocolo seguro usado al comunicarse con la red. Si el servidor de WAP queda comprometido, un atacante puede ser capaz de adquirir credenciales de autenticación que permitan el acceso a cualquier red a la que hayan accedido los clientes móviles. Además, para reducir la cantidad de información que debe ser recordada, los clientes móviles pueden usar las mismas credenciales de autenticación para otras redes que no brindan acceso móvil, haciendo a esas otras redes asimismo vulnerables al ataque.

Aunque pueda ser improbable que quede comprometido un servidor intermedio, el problema para la red es que el riesgo puede ser difícil de cuantificar. Las medidas de seguridad en el servidor intermedio son determinadas, implementadas, monitorizadas y controladas por quienquiera que sea responsable del servidor intermedio. Para algunas redes, el riesgo proveniente de credenciales numéricas de autenticación, acoplado con la incertidumbre en cuanto a la extensión de la seguridad proporcionada por un servidor intermedio, será demasiado grande, y el acceso móvil se prohibirá.

El documento US6067623 describe el control del acceso de clientes a recursos de empresa, a través de un servidor de nivel medio. Las autorizaciones de recursos de empresa se mantienen en un servidor de nivel medio. Los usuarios se autentican ante el servidor, haciendo que correlacione y transforme la autorización de acceso del cliente en credenciales de recursos de empresa. Se accede a los recursos de empresa después de la autorización, usando las credenciales transformadas.

El documento W00103402 se refiere a un procedimiento y sistema de autenticación para identificar a un abonado de una primera red en una segunda red, en donde una dirección de la segunda red está adjudicada al abonado. La información acerca de una correlación entre la dirección de la segunda red y una identidad de abonado es generada y transmitida a la segunda red. Por ello, se proporciona una conexión de servidor de autenticación entre la primera red y la segunda red, de modo que la identidad del abonado pueda ser entregada a la segunda red. De esta manera, una plataforma de VAS (Sistema de validación) de la segunda red puede recibir la dirección de la segunda red y la identidad de abonado del abonado, de modo que un abonado que acceda a los servicios de la plataforma de VAS pueda ser identificado con fines de facturación y / o direccionamiento.

El documento W00046963 describe una pasarela que tiene una pila, con una capa de adaptación del portador y un cliente de HTTP. La pasarela puede ser conectada, por un enlace de HTTP, con un servidor de origen y, por una interfaz de portador, con una red móvil. También puede ser conectada, por un enlace de HTTP, con un servidor de WTA (aplicaciones de telefonía inalámbrica). Un administrador de contexto es un usuario en la pila y da soporte a interfaces para permitir el acceso a entidades externas de manera versátil. Un administrador de sucesos captura sucesos, incluso sucesos de facturación, y escribe en un registro de sucesos y un registro de facturación. Una entidad de gestión proporciona el control global y fija configuraciones para el administrador de sucesos.

El documento W00022794 describe un sistema para ingresar una o más configuraciones, un ordenador servidor, un cliente y un procedimiento de ingresar una o más configuraciones a un cliente, para acceder a un ordenador servidor conectado con una red de telecomunicación inalámbrica. El sistema comprende un cliente, un ordenador servidor y una red de telecomunicación inalámbrica. El cliente está dispuesto para recibir una entrada de una o más configuraciones. El ordenador servidor tiene medios de inicialización que dan al cliente acceso a dicho servidor, en donde los medios de inicialización comprenden información acerca de la(s) configuración(es) a ingresar en el cliente. La red de telecomunicación inalámbrica está conectada con el servidor, y está dispuesta para establecer una conexión inalámbrica entre el cliente y la red de telecomunicación, tras la recepción de una solicitud desde el cliente. La solicitud comprende medios de identificación que identifican al cliente. La red también comprende un medio de memoria, que está dispuesto para identificar a los medios de identificación provenientes del cliente.

El documento "Seguridad para acceso remoto y aplicaciones móviles", de HOOGENBOOM M. y STEEMERS P., ORDENADORES Y SEGURIDAD, EDITORES CIENTÍFICOS ELSEVIER, AMSTERDAM, Vol. 19, Nº 2, febrero de

2000, páginas 149 a 163, describe la autenticación para el acceso remoto. Los usuarios son autenticados ante una base de datos de usuarios antes de permitir el acceso. Después de marcar el número del servidor de acceso remoto, el usuario proporciona el nombre de usuario y la contraseña para quedar autenticado. Durante la autenticación, la seguridad es proporcionada por el cifrado del nombre de usuario y la contraseña. Esta seguridad es ofrecida por la Seguridad de Capa de Transporte, TLS. La autenticación usando criptografía de clave pública podría comprender el envío de un mensaje aleatorio al receptor, cifrando el receptor el mensaje aleatorio con su clave privada y enviando la respuesta, y recibiendo el remitente la respuesta y verificándola con respecto al mensaje originalmente enviado.

El documento US5586260 se refiere a la autenticación de un cliente para un servidor cuando el cliente y el servidor tienen distintos mecanismos de seguridad. Un sistema intermediario, conocido como una pasarela de autenticación, proporciona la autenticación del cliente usando el mecanismo de seguridad del cliente, y la personificación del cliente en una llamada a un servidor al que el cliente desea acceder. El cliente se conecta a la pasarela de autenticación y proporciona un nombre de usuario y una contraseña. Luego, la pasarela de autenticación obtiene y guarda las credenciales de seguridad para el cliente, devolviendo una clave de acceso al cliente. Cuando el cliente desea llamar al servidor, el cliente llama a la pasarela de autenticación, que actúa como un servidor agente, y pasa la clave de acceso, que se usa luego para extraer las credenciales de seguridad y para personificar al cliente en una llamada al servidor. Cualquier argumento de salida resultante de la llamada al servidor se devuelve al cliente a través de la pasarela de autenticación.

Resumen de la invención

Estos y otros problemas son superados por la presente invención, que se orienta hacia la autenticación en base a credenciales relativamente débiles, tales como contraseñas con pocos caracteres o contraseñas con selecciones limitadas para cada carácter. Por ejemplo, un cliente puede tener un sistema de entrada optimizado para la entrada numérica y, por lo tanto, usar solamente contraseñas numéricas, mientras que otro cliente puede usar contraseñas relativamente cortas. En general, la presente invención puede ser usada para correlacionar un conjunto de credenciales de autenticación con otro conjunto de credenciales de autenticación. Una pasarela recibe credenciales de autenticación del cliente y usa un filtro de autenticación para correlacionar las credenciales de autenticación según criterios pre-establecidos. El filtro de autenticación puede cambiar el nombre del dominio, el nombre de usuario, o ambos. Por ejemplo, un nombre de dominio puede ser reemplazado por otro, o puede añadirse un sufijo al nombre de usuario. Luego, las credenciales de autenticación correlacionadas se envían a la red que incluye al servidor de contenido al que se está accediendo. Todo privilegio de acceso concedido al cliente se basa en las credenciales de autenticación correlacionadas.

La pasarela admite credenciales de autenticación que sean específicas para el acceso del cliente a través de la pasarela, sin revelar información acerca de la red con la cual se conectan los clientes. Si las credenciales de un cliente están comprometidas, los intentos de autenticarse con las credenciales que no impliquen a la pasarela fallarán, porque el nombre de dominio especificado, el nombre de usuario, o ambos, no existen en la red. Además, la pasarela puede configurarse para aceptar conexiones solamente desde servidores de terceros conocidos. Como resultado, cualquier credencial de autenticación que pueda ser descubierta por un atacante está limitada al uso en un contexto de pasarela.

Definiendo credenciales de autenticación que sean específicas para el acceso del cliente a través de la pasarela, los administradores de redes pueden equilibrar un nivel adecuado de permisos de acceso con el nivel aumentado de riesgo que resulta de las credenciales débiles, tales como las contraseñas numéricas. En lugar de conceder el mismo nivel de acceso que un usuario disfrutaría usando otras credenciales de autenticación, tal como al autenticarse ante un ordenador de oficina, por una conexión de red interna, las credenciales de autenticación de pasarela pueden ser restringidas para garantizar una exposición mínima si quedan comprometidas. Por ejemplo, las credenciales de autenticación de pasarela pueden ser limitadas a los recursos de red de un único usuario, tales como la cuenta de correo electrónico del usuario, un directorio de conexión por omisión, etc., mientras que otras credenciales de autenticación podrían permitir al usuario el acceso a un gran número de recursos de red que están usualmente compartidas entre un cierto número de usuarios, incluyendo a servidores, directorios, bases de datos, etc.

La pasarela también facilita la gestión de credenciales de autenticación de pasarela. Los nombres de dominio y / o los nombres de usuario pueden ser actualizados sin imponer aprietos a los clientes. Por ejemplo, si parece que un dominio ha quedado comprometido, puede crearse un nuevo dominio, o pueden crearse nuevas cuentas en un dominio, y actualizarse la pasarela en consecuencia. Las credenciales de autenticación de pasarela pueden estar asociadas a otras credenciales de autenticación, para identificar recursos potenciales a los que los clientes puedan acceder, con permisos de acceso específicos concedidos según convenga. En otras palabras, las credenciales de autenticación de pasarela no concederían permisos mayores que los proporcionados en las otras credenciales de autenticación.

Una relación de confianza puede ser establecida entre diversas credenciales de autenticación y los correspondientes dominios. La relación de confianza define áreas específicas de confianza. Por ejemplo, un dominio puede confiar en las credenciales de autenticación en otro dominio para privilegios de acceso delegados, pero no para otros privilegios, más sensibles, tales como los privilegios de administrador. La definición de una relación de confianza ofrece un nivel

adicional de control sobre los privilegios de acceso móvil, porque impide que las credenciales de autenticación móvil prevalezcan sobre otras calificaciones de autenticación.

Características y ventajas adicionales de la invención se estipularán en la descripción que sigue y, en parte, serán obvias a partir de la descripción, o bien pueden ser aprendidas en la práctica de la invención. Las características y ventajas de la invención pueden ser realizadas y obtenidas por medio de los instrumentos y combinaciones específicamente señalados en las reivindicaciones adjuntas. Estas, y otras, características de la presente invención, devendrán más completamente evidentes a partir de la siguiente descripción y las reivindicaciones adjuntas, o bien pueden ser aprendidas en la práctica de la invención, según se estipula a continuación.

Breve descripción de los dibujos

A fin de describir la manera en que pueden obtenerse las ventajas y características precitadas, y otras, de la invención, se presentará una descripción más específica de la invención, descrita brevemente en lo anterior, por referencia a realizaciones específicas de la misma, que se ilustran en los dibujos adjuntos. En el entendimiento de que estos dibujos ilustran solamente realizaciones típicas de la invención y, por lo tanto, no han de considerarse como limitadores de su alcance, se describirá y explicará la invención con especificaciones y detalles adicionales, mediante el uso de los dibujos adjuntos, en los cuales:

la Figura 1 ilustra un sistema ejemplar que proporciona un entorno operativo adecuado para la presente invención;

la Figura 2 es un diagrama en bloques que muestra una red con dominios separados para credenciales de autenticación móviles y otras;

la Figura 3 es un diagrama en bloques que muestra una red con un único dominio para credenciales de autenticación móviles y otras; y

la Figura 4 ilustra un procedimiento ejemplar para autenticar un cliente móvil mediante una pasarela móvil.

Descripción detallada de la invención

La presente invención se extiende a procedimientos, sistemas y productos de programa de ordenador para autenticar clientes. Una pasarela correlaciona credenciales de autenticación recibidas desde un cliente y envía las credenciales de autenticación correlacionadas a una red que incluye los recursos a los que el cliente desea acceder. Las credenciales de autenticación identifican a un cliente específico y determinan los recursos a los que el cliente está autorizado a acceder, incluso los tipos de acceso permitidos.

Las credenciales de autenticación a menudo incluyen un nombre de usuario y una contraseña para uno o más dominios. Otros tipos de información, incluso atributos biométricos (p. ej., huellas dactilares) y claves de hardware (p. ej., tarjetas inteligentes), pueden ser usadas igualmente. La presente invención no está limitada a ningún tipo específico de credenciales de autenticación. Las credenciales de autenticación se aplican usualmente a un grupo o colección de uno o más recursos, a menudo denominado un dominio. Los dominios facilitan la administración de recursos permitiendo que los recursos sean gestionados como una unidad individual, con reglas y procedimientos comunes. Más en general, el término “dominio” describe un agrupamiento lógico de recursos, en el cual el agrupamiento puede ser independiente de cómo están interconectados los recursos. Una red individual puede tener uno o más dominios y un dominio individual puede incluir una o más redes.

En ocasiones, las credenciales de autenticación pueden ser descritas como débiles o cortas. Según se usan en esta solicitud, sin embargo, débil y corto deberían interpretarse como términos comparativos, antes que absolutos. Las credenciales de autenticación débiles y / o cortas son débiles y / o cortas solamente en cuanto a que credenciales de autenticación más fuertes, y / o más largas, sean posibles y puedan ser deseables. Por ejemplo, una contraseña de cuatro dígitos es débil y corta en comparación a una contraseña de cinco dígitos. De manera similar, una contraseña de cinco dígitos es débil, aunque no corta, en comparación con una contraseña alfanumérica de cinco caracteres. En su sentido más general, la presente invención implica sustituir un conjunto de credenciales de autenticación en lugar de otro. Los ejemplos específicos expuestos más adelante identifican meramente entornos o realizaciones ejemplares para poner en práctica la presente invención, y no deberían ser interpretados como necesariamente limitadores de su alcance.

El término “cliente” puede ser usado para describir individuos, dispositivos, ordenadores, sistemas, etc., ya sea solos o en combinación, que acceden a recursos de ordenador. El término “servidor” describe a un proveedor de recursos de ordenador, y asimismo incluye dispositivos, ordenadores, sistemas, etc. Según las circunstancias, un servidor en una configuración puede ser un cliente en otra, y análogamente, un cliente en una configuración puede ser un servidor en otros momentos. El término red describe recursos interconectados, y abarca una amplia gama de configuraciones, incluso un recurso individual, tal como un ordenador, sistema de almacenamiento, impresora, servidor de ficheros, etc., que admite conexiones con clientes, y / o cualquier otro recurso.

A cada uno de los términos precedentes debería acordársele la más amplia interpretación posible. Los expertos en la tecnología pueden reconocer que, en un contexto específico, ciertos términos pueden adquirir un significado más específico, o alternativo. Debería observarse, por lo tanto, que la siguiente descripción detallada se ofrece para presentar implementaciones ejemplares, y no está concebida para limitar el alcance de la presente invención. Las realizaciones de la presente invención pueden comprender un ordenador de propósito especial o de propósito general, incluso hardware diverso de ordenador, según se expone en mayor detalle más adelante.

Las realizaciones dentro del alcance de la presente invención también incluyen medios legibles por ordenador para transportar, o tener, instrucciones o estructuras de datos legibles por ordenador almacenadas en los mismos. Tales medios legibles por ordenador pueden ser cualquier medio disponible al que pueda acceder un ordenador de propósito general o de propósito especial. A modo de ejemplo, y no de limitación, tales medios legibles por ordenador pueden comprender memorias RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda ser usado para llevar o almacenar medios deseados de código de programa, en forma de instrucciones o estructuras de datos ejecutables por ordenador, y a los que pueda acceder un ordenador de propósito general o de propósito especial. Cuando la información se transfiere o se suministra por una red u otra conexión de comunicaciones (ya sea cableada, inalámbrica, o una combinación de cableada e inalámbrica) a un ordenador, el ordenador visualiza debidamente la conexión como un medio legible por ordenador. De esta manera, cualquier conexión de ese tipo se denomina adecuadamente un medio legible por ordenador. Las combinaciones de lo precedente también deberían ser incluidas dentro del alcance de los medios legibles por ordenador. Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que hacen que un ordenador de propósito general, un ordenador de propósito especial, o un dispositivo de procesamiento de propósito especial realicen una cierta función o grupo de funciones.

La Figura 1 y la siguiente exposición están concebidas para proporcionar una descripción breve y general de un entorno informático adecuado en el cual pueda implementarse la invención. Aunque no se requiere, la invención se describirá en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutadas por ordenadores en entornos de red. 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. Las instrucciones ejecutables por ordenador, las estructuras de datos asociadas y los módulos de programa representan ejemplos del medio de código de programa para ejecutar etapas de los procedimientos revelados en el presente documento. La secuencia específica de tales instrucciones ejecutables, o estructuras de datos asociadas, representan ejemplos de actos correspondientes para implementar las funciones descritas en tales etapas.

Los expertos en la tecnología apreciarán que la invención puede ser puesta en práctica en entornos informáticos en red, con muchos tipos de configuraciones de sistemas de ordenador, incluso ordenadores personales, dispositivos de mano, sistemas multiprocesadores, electrónica de consumo, basada en microprocesadores o programable, PC en red, miniordenadores, ordenadores centrales y similares. La invención también puede ser puesta en práctica en entornos informáticos distribuidos, donde las tareas son llevadas a cabo por dispositivos de procesamiento locales y remotos que están enlazados (bien por enlaces cableados, bien por enlaces inalámbricos o bien por una combinación de enlaces cableados o inalámbricos) a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programa pueden estar situados en dispositivos de almacenamiento de memoria tanto local como remota.

Con referencia a la Figura 1, un sistema ejemplar para implementar la invención incluye un dispositivo informático de propósito general en forma de un ordenador convencional 20, que incluye una unidad 21 de procesamiento, una memoria 22 de sistema y un bus 23 de sistema que acopla diversos componentes de sistema, incluso la memoria 22 de sistema con la unidad 21 de procesamiento. El bus 23 del sistema puede ser cualquiera de varios tipos de estructuras de bus, incluso un bus de memoria o controlador de memoria, un bus periférico y un bus local que use cualquiera entre una gran variedad de arquitecturas de bus. La memoria del sistema incluye memoria de sólo lectura (ROM) 24 y memoria de acceso aleatorio (RAM) 25. Un sistema de entrada / salida básica (BIOS) 26, que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del ordenador 20, tal como durante el arranque, puede ser almacenado en la memoria ROM 24.

El ordenador 20 también puede incluir un controlador 27 de disco rígido magnético para leer de, y escribir en, un disco rígido magnético 39, un controlador 28 de disco magnético para leer de, o escribir en, un disco magnético extraíble 29, y un controlador 30 de disco óptico para leer de, o escribir en, el disco óptico extraíble 31, tal como un CD-ROM u otros medios ópticos. El controlador 27 de disco rígido magnético, el controlador 28 de disco magnético y el controlador 30 de disco óptico están respectivamente conectados con el bus 23 del sistema por una interfaz 32 de controlador de disco rígido, una interfaz 33 de controlador de disco magnético y una interfaz 34 de controlador óptico. Los controladores y sus medios asociados legibles por ordenador proporcionan el almacenamiento no volátil de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador 20. Aunque el entorno ejemplar descrito en el presente documento emplea un disco rígido magnético 39, un disco magnético extraíble 29 y un disco óptico extraíble 31, pueden usarse otros tipos de medios legibles por ordenador para almacenar datos, incluso casetes magnéticos, tarjetas de memoria flash, discos de vídeo digital, cartuchos Bernoulli,

memorias RAM, memorias ROM y similares.

Los medios de código de programa que comprenden uno o más módulos de programa pueden almacenarse en el disco rígido 39, el disco magnético 29, el disco óptico 31, la memoria ROM 24 o la memoria RAM 25, incluso un sistema operativo 35, uno o más programas 36 de aplicación, otros módulos 37 de programa y datos 38 de programa. Un usuario puede ingresar comandos e información en el ordenador 20 mediante el teclado 40, el dispositivo 42 de puntero u otros dispositivos de entrada (no mostrados), tales como un micrófono, una palanca de juegos, un panel de juegos, una antena de plato satelital, un escáner o similares. Estos y otros dispositivos de entrada están a menudo conectados con la unidad 21 de procesamiento a través de una interfaz 46 de puerto en serie acoplada al bus 23 del sistema. Alternativamente, los dispositivos de entrada pueden estar conectados por otras interfaces, tales como un puerto paralelo, un puerto de juegos o un bus universal en serie (USB). Un monitor 47, u otro dispositivo de visualización, también está conectado con el bus 23 del sistema mediante una interfaz, tal como el adaptador 48 de vídeo. Además del monitor, los ordenadores personales incluyen habitualmente otros dispositivos de salida periféricos (no mostrados), tales como altavoces e impresoras.

El ordenador 20 puede funcionar en un entorno en red, usando conexiones lógicas con uno o más ordenadores remotos, tales como los ordenadores remotos 49a y 49b. Cada uno de los ordenadores remotos 49a y 49b puede ser otro ordenador personal, un servidor, un encaminador, un PC de red, un dispositivo a la par u otro nodo de red común, y habitualmente incluyen muchos de, o todos, los elementos descritos anteriormente con respecto al ordenador 20, aunque solamente los dispositivos 50a y 50b de almacenamiento de memoria, y sus programas 36a y 36b de aplicación asociados, han sido ilustrados en la Figura 1. Las conexiones lógicas ilustradas en la Figura 1 incluyen una red de área local (LAN) 51 y una red de área amplia (WAN) 52, que se presentan aquí a modo de ejemplo y no de limitación. Tales entornos en red son proverbiales en redes de ordenadores de toda una oficina o de toda una empresa, las intranets e Internet.

Cuando se usa en un entorno de red LAN, el ordenador 20 está conectado con la red local 51 a través de una interfaz o adaptador 53 de red. Cuando se usa en un entorno de red WAN, el ordenador 20 puede incluir un módem 54, un enlace inalámbrico u otro medio para establecer comunicaciones por la red 52 de área amplia, tal como Internet. El módem 54, que puede ser interno o externo, está conectado con el bus 23 del sistema mediante la interfaz 46 de puerto en serie. En un entorno en red, los módulos de programa ilustrados con respecto al ordenador 20, o partes de los mismos, pueden ser almacenados en el dispositivo remoto de almacenamiento de memoria. Se apreciará que las conexiones de red mostradas son ejemplares y que pueden usarse otros medios de establecimiento de comunicaciones por la red 52 de área amplia.

El diagrama en bloques de la Figura 2 muestra la red 210 con dominios individuales, el dominio móvil 240 y otro(s) dominio(s) 230, para gestionar, respectivamente, credenciales de autenticación, móviles y otras. El dominio móvil 240 puede ser reconocido, en general, por la red 210, o bien puede ser usado solamente al proporcionar acceso al servidor 220 de contenido. Otro(s) dominio(s) 230 incluye(n) el nombre 232 de usuario, que identifica a Neil como un usuario, con una contraseña 234 de valor A1(b)c5. (Obsérvese que el uso de caracteres mayúsculos y minúsculos, números y puntuación provee una defensa significativa contra los ataques de fuerza bruta). El dominio móvil 240 incluye el nombre 242 de usuario, que identifica a Neil-m como un usuario, con una contraseña numérica 244 de valor 1234. Según lo indicado por las referencias 212 y 214, tanto Neil como Neil-m tienen permisos de acceso para el servidor 220 de contenido.

Debido a que el dominio móvil 240 es independiente de otro(s) dominio(s) 230, no es necesario que el nombre 242 de usuario y el nombre 232 de usuario sean distintos. Bien los nombres de usuario independientes, o bien los nombres de dominio independientes, son suficientes para proporcionar credenciales de autenticación que sean específicas para un cliente móvil. En la práctica, la administración de los dos dominios puede simplificarse si los nombres de usuario son compartidos. Por ejemplo, una relación de confianza puede establecerse entre los dos dominios. La extensión de la relación de confianza entre los dominios depende de las circunstancias de una implementación específica, pero los dominios móviles serían fiables con respecto a algún nivel mínimo de permisos de acceso, tales como los permisos delegados en un contexto de correo electrónico. Los distintos nombres de usuario, sin embargo, asisten más adelante para distinguir entre los comentarios referidos a otro(s) dominio(s) 230 y los comentarios que se refieren al dominio móvil 240. Los nombres distintos de usuario, Neil y Neil-m, por lo tanto, se conservarán a lo largo de la exposición restante de la Figura 2, con fines de claridad. Obsérvese que la Figura 3 centra la atención en el uso de un único dominio con distintos nombres de usuario.

Para dar cuenta del riesgo aumentado asociado a los clientes móviles, los permisos de acceso concedidos a través del dominio móvil 240 están limitados en comparación con los concedidos por otro(s) dominio(s) 230. Por ejemplo, si el servidor 220 de contenido proporciona recursos de correo electrónico, Neil puede tener todos los derechos de acceso para una cuenta específica de correo electrónico, mientras que a Neil-m pueden concederse solamente ciertos privilegios delegados de acceso. Además, Neil también puede tener privilegios de acceso a otros recursos que son parte de otro(s) dominio(s) 230, mientras que los privilegios de acceso de Neil-m se extienden solamente al servidor

220 de contenido.

Los privilegios de acceso pueden aplicarse a uno o a múltiples clientes. Por ejemplo, el dueño o administrador de un recurso puede tener un conjunto de privilegios de acceso, ciertos agrupamientos o dominios pueden tener otro conjunto de privilegios de acceso y todos los otros pueden tener un conjunto por omisión de privilegios de acceso. Los expertos en la tecnología reconocerán que existe una gran variedad de esquemas para especificar privilegios de acceso, y que otros pueden ser desarrollados en el futuro. Debería observarse que la presente invención no está limitada a ninguna forma específica de privilegios de acceso. En cambio, la presente invención reconoce que puede ser deseable proporcionar privilegios de acceso independientes para clientes móviles, y proporciona la tecnología relevante para hacerlo, independientemente de los privilegios de acceso de la implementación subyacente.

Si las credenciales de autenticación asociadas a Neil-m quedaran comprometidas, solamente los recursos disponibles a un único cliente móvil serían accesibles. Para los recursos del correo electrónico, esto probablemente incluiría solamente el buzón del cliente móvil. Por el contrario, quedando comprometidas las credenciales de autenticación asociadas a Neil, es probable que produzcan privilegios de acceso mucho más amplios para recursos de la red 210 que están probablemente compartidos por diversos clientes.

Alternativamente, el dominio móvil 240 puede ser una base de datos de credenciales administrada por separado, que se usa solamente al proporcionar acceso al servidor 220 de contenido. En este caso, el dominio móvil 240 no es un dominio en el mismo sentido en que otro(s) dominio(s) 230 es (son) un dominio. La base de datos de credenciales administrada por separado no podría ser usada para el acceso directo de recursos que sean parte de la red 210. En cambio, el servidor 220 de contenido puede ser configurado para verificar las credenciales de autenticación incluidas dentro de esta base de datos de credenciales. Una vez verificada, una cuenta compartida en un dominio, tal como otro(s) dominio(s) 230, sería usada al acceder al servidor 220 de contenido. Como antes, si las credenciales de autenticación para Neil-m quedaran comprometidas, solamente los recursos disponibles para un único cliente móvil estarían en peligro, tal como el buzón del cliente. Sin embargo, si la cuenta compartida hubiera quedado comprometida, los recursos asociados a todos los clientes móviles estarían en peligro.

Pasando ahora al flujo de credenciales de autenticación desde cualquiera de los diversos clientes móviles hasta la red 210, el teléfono 280 proporciona credenciales de autenticación al servidor 270 de WAP, por la conexión 296. Aunque se muestra un nombre de usuario textual (Neil) en la Figura 2, el nombre de usuario se almacena usualmente en el teléfono, por lo que no necesita ser ingresado cada vez que se hace una solicitud de contenido. La conexión 296 puede ser cifrada, usando un protocolo tal como el de seguridad de capa de transporte inalámbrico (“WTLS”), para proteger el contenido intercambiado entre el teléfono 280 y el servidor 270 de WAP. El servidor 270 de WAP descifra las credenciales de autenticación y las envía a la pasarela móvil 250 por la conexión 294. Como la conexión 296, la conexión 294 puede cifrar las credenciales de autenticación usando un protocolo tal como el de la capa de zócalos seguros (“SSL”). Habitualmente, el servidor 270 de WAP funciona como un traductor de protocolos entre los protocolos inalámbricos de los clientes móviles y los protocolos de línea de cable usados en la comunicación con la pasarela móvil 250. Las credenciales de autenticación están expuestas a un ataque en el servidor de WAP porque, al menos por un tiempo, no están cifradas. Además, debido a que es probable que las credenciales de autenticación incluyan partes numéricas relativamente cortas, tales como una contraseña o PIN numéricos, las credenciales de autenticación son vulnerables a ataques de fuerza bruta.

La pasarela móvil 250 incluye un filtro 260 de autenticación que se usa al correlacionar las credenciales de autenticación recibidas. El filtro 260 de autenticación incluye dos componentes, el identificador 266 de dominio y el modificador 262 de nombre de usuario. El identificador 266 de dominio especifica el dominio que la red 210 usará al procesar las credenciales de autenticación. En la Figura 2, el identificador de dominio es Móvil. El cambio de un nombre de dominio, de acuerdo al identificador 266 de dominio, incluye sustituir un dominio por otro (reemplazar un dominio especificado por un cliente móvil por el identificador 266 de dominio), alterar un nombre de dominio (hacer un cambio en un dominio especificado por un cliente móvil) y añadir un dominio donde ninguno estuviera especificado (añadir el identificador 266 de dominio allí donde un cliente móvil no especificara un dominio), etc. El modificador 262 de nombre de usuario incluye un cuadro 262a de nombre de usuario y un sufijo 262b. El cuadro 262a de nombre de usuario es simplemente un receptáculo para todos los nombres de usuario, mientras que la pasarela móvil añade el sufijo 262b a los nombres de usuario. La pasarela móvil 250 envía a la red 210 credenciales de autenticación correlacionadas por la conexión 292, usando el cifrado según convenga.

La red 210 procesa las credenciales de autenticación que recibe según lo descrito anteriormente. Obsérvese que la pasarela móvil 250 tanto identifica un dominio móvil 240 individual como añade un sufijo de nombre de usuario. Si el nombre de usuario Neil y la contraseña 1234 son ingresados en el teléfono 280, la pasarela móvil cambia el nombre de usuario a Neil-m y envía las credenciales de autenticación al dominio móvil 240 para su procesamiento. Debido a que un nombre de usuario Neil-m, con una contraseña de valor 1234, ya existe en el dominio móvil 240, al teléfono 280 se concederán los privilegios de acceso que están asociados a Neil-m. Usualmente, solamente se necesita un dominio móvil independiente, tal como el dominio móvil 240, o un sufijo de nombre de usuario, para proporcionar credenciales

de autenticación que sean específicas para un cliente móvil.

El diagrama en bloques de la Figura 3 muestra una red con un único dominio, el dominio corporativo 330, para credenciales de autenticación, tanto móviles como otras. Un nombre 332 de usuario de valor Mike, con una contraseña 334 de valor X9(y)z3, está definido en el dominio corporativo 330 para determinar privilegios de acceso a los recursos, tal como el servidor 320 de contenido, de la red 310. Un cliente móvil, con un nombre 342 de usuario de valor Mike-m y una contraseña 344 de valor 5678, también está definido en el dominio corporativo 330. Obsérvese que la presente invención no requiere que se añada ningún sufijo específico a los nombres de usuario. Además, la presente invención no necesariamente requiere cambiar los nombres de usuario añadiendo un sufijo. Los nombres de usuario pueden ser cambiados añadiendo un prefijo, insertando caracteres en el medio de un nombre de usuario, reemplazando todo, o una parte de, un nombre de usuario por otra parte o nombre de usuario, borrando caracteres de un nombre de usuario, etc.

De manera similar a la descripción con referencia a la Figura 2, y pasando ahora al flujo de credenciales de autenticación desde cualquiera de diversos clientes móviles a la red 310, el teléfono 380 proporciona credenciales de autenticación al servidor 370 de WAP por la conexión 396, usando WLTS. El servidor 370 de WAP descifra las credenciales de autenticación recibidas por la conexión 396 y re-cifra las credenciales de autenticación para la conexión 394 de SSL. En la pasarela móvil 350, el filtro 360 de autenticación añade el sufijo 362b a los nombres 362a de usuario, según lo indicado por la referencia 362. La pasarela móvil 350 establece el dominio aplicable 366, para las credenciales de autenticación recibidas, como el Corporativo.

Si el nombre de usuario Mike, y la contraseña 5678, son ingresadas en el teléfono 380, la pasarela móvil cambia el nombre de usuario a Mike-m y envía las credenciales de autenticación al dominio corporativo 330 para su procesamiento. Debido a que un nombre de usuario Mike-m, con una contraseña de valor 5678, existe en el dominio corporativo 330, al teléfono 380 se concederán los privilegios de acceso que están asociados a Mike-m. Aquí, solamente un dominio único, tal como el dominio corporativo 330, se necesita para proporcionar credenciales de autenticación que sean específicas para un cliente móvil.

Un inconveniente para la implementación del dominio único es que las políticas y procedimientos para las credenciales de autenticación se establecen a menudo por cada dominio. Es decir, el dominio corporativo 330 puede establecerse para requerir al menos una letra mayúscula, al menos una letra minúscula, un número y un signo de puntuación, en todas las contraseñas. Por tener a Mike-m en el dominio corporativo 330, la contraseña 344 estaría sujeta a estos requisitos y, por lo tanto, una contraseña totalmente numérica, tal como 5678, no puede ser admitida.

También debería observarse que el filtro 360 de autenticación es capaz de hacer todos aquellos cambios en las credenciales de autenticación que sean adecuados para el tipo y formato de las credenciales de autenticación implementadas por la red 310, el servidor 320 de contenido y / o el dominio corporativo 330. Como muestra la referencia 312, el servidor 320 de contenido depende del dominio corporativo 330 para determinar privilegios de acceso. Una implementación específica de las credenciales de autenticación, sin embargo, no está necesariamente limitada por la presente invención. Todo cambio que haga la pasarela móvil 350 solamente necesita ser adecuada para las credenciales de autenticación que son esperadas por la red 310, el servidor 320 de contenido y / o el dominio corporativo 330. Allí donde una base de datos de credenciales de autenticación, administrada por separado, proporcione acceso a recursos, la correlación realizada por una pasarela móvil puede ser específica para la base independiente de datos de credenciales, incluso aunque esas correlaciones no fueran adecuadas para la red 310 o para dominios asociados cualesquiera.

Pasando ahora a la Figura 4, se ilustra un procedimiento ejemplar para autenticar un cliente móvil a través de una pasarela móvil. Una etapa para alterar (410) las credenciales de autenticación puede incluir los actos de definir (412) un filtro de autenticación y de correlacionar (414) credenciales de autenticación recibidas cualesquiera. La correlación puede incluir cambiar el nombre de dominio, el nombre de usuario, o modificar de otro modo las credenciales de autenticación. Un nombre de dominio puede ser reemplazado por otro y los nombres de usuario pueden tener un sufijo añadido.

Una etapa para identificar (420) un cliente móvil puede incluir los actos de recibir (422) credenciales de autenticación desde un cliente móvil y de enviar (424) las credenciales de autenticación correlacionadas a una red que proporciona los recursos que serán solicitados por el cliente móvil. Las etapas de alterar (410) las credenciales de autenticación y de identificar (420) un cliente móvil están entrelazadas para indicar que los actos asociados a las etapas no se efectúan necesariamente en ningún orden específico. Una etapa para acceder (430) a contenido proporcionado por la red puede incluir los actos de recibir (432) una solicitud de contenido, enviar (434) la solicitud a la red, recibir (436) el contenido solicitado y enviar (438) el contenido solicitado al cliente móvil.

REIVINDICACIONES

1. Un procedimiento de acceso a contenido por parte de un cliente, para su uso en un sistema informatizado que incluye uno o más clientes que acceden a una pasarela y a un servidor de contenido, en el cual un servidor del protocolo de aplicaciones inalámbricas, WAP, está situado entre dicho(s) cliente(s) y la pasarela, en el cual el servidor de contenido es parte de una red y en el cual la pasarela está conectada con la red, en el cual el acceso al servidor de contenido requiere credenciales de autenticación, en el cual la pasarela realiza el procedimiento de:

definir (412) un filtro de autenticación que correlaciona las credenciales de autenticación recibidas desde los clientes según criterios pre-establecidos, como credenciales de autenticación correlacionadas;

recibir (422) credenciales de autenticación desde un cliente mediante el servidor de WAP, en donde las credenciales de autenticación son aceptadas solamente desde el servidor de WAP;

correlacionar (414) las credenciales de autenticación recibidas en base a criterios pre-establecidos;

enviar (424) las credenciales de autenticación correlacionadas a la red, en donde los privilegios de acceso están basados en las credenciales de autenticación correlacionadas;

recibir (432) una solicitud de contenido disponible en el servidor de contenido;

enviar (434) la solicitud a la red;

recibir (436) el contenido solicitado desde la red; y

enviar (438) el contenido recibido al cliente.

2. El procedimiento según la reivindicación 1, en el cual el acto de correlacionar (414) las credenciales de autenticación recibidas incluye cambiar un nombre de dominio que es parte de las credenciales de autenticación recibidas.

3. El procedimiento según la reivindicación 2, en el cual el acto de correlacionar (414) las credenciales de autenticación recibidas incluye reemplazar el nombre de dominio, que es parte de las credenciales de autenticación recibidas, por otro nombre de dominio.

4. El procedimiento según la reivindicación 1, en el cual el acto de correlacionar (414) las credenciales de autenticación recibidas incluye cambiar un nombre de usuario que es parte de las credenciales de autenticación recibidas.

5. El procedimiento según la reivindicación 4, en el cual el acto de correlacionar (414) las credenciales de autenticación recibidas incluye añadir un sufijo al nombre de usuario.

6. El procedimiento según la reivindicación 4, en el cual el acto de correlacionar (414) las credenciales de autenticación recibidas incluye añadir un prefijo al nombre de usuario.

7. Un medio legible por ordenador para almacenar un producto de programa de ordenador que comprende instrucciones que, cuando son ejecutadas en un ordenador, hacen que el ordenador realice un procedimiento según cualquiera de las reivindicaciones 1 a 6.

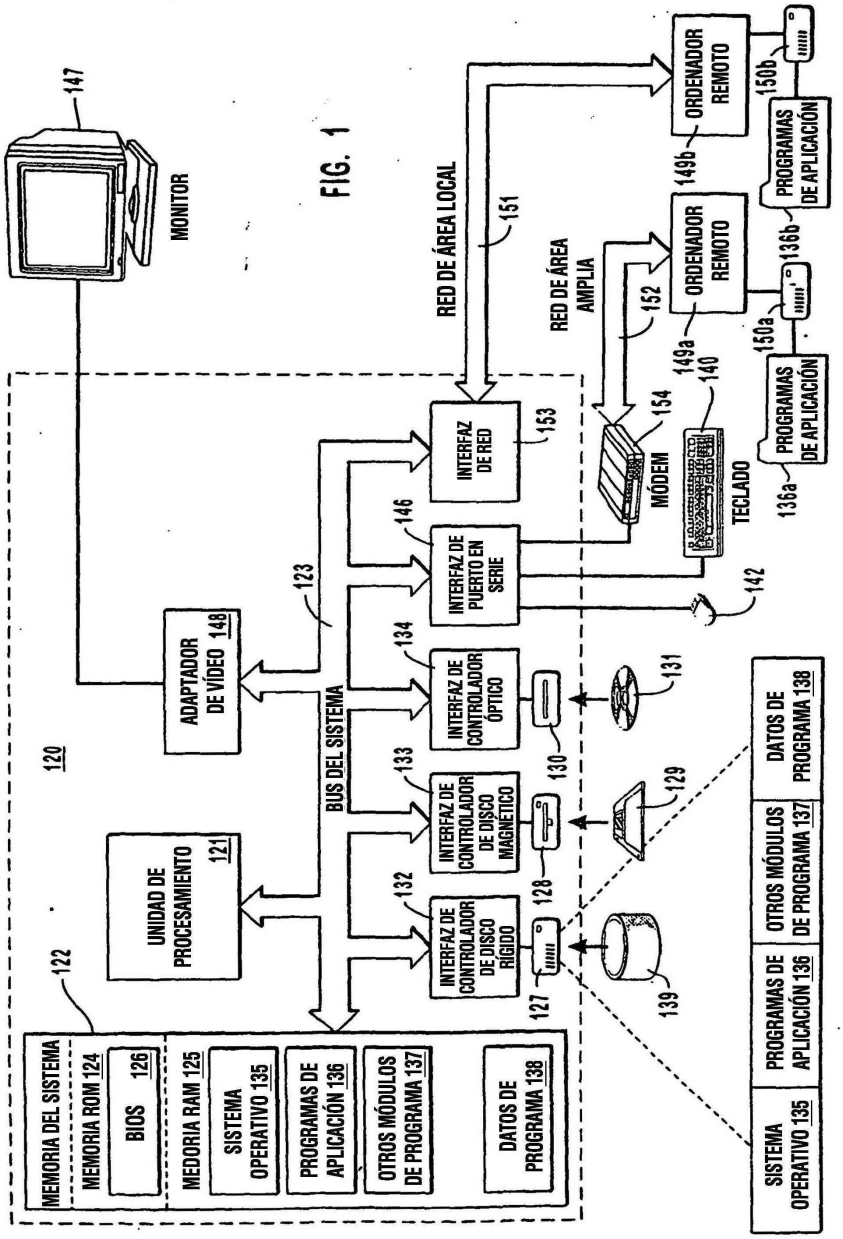
147
MONITOR
120
122
MEMORIA DEL SISTEMA
MEMORIA ROM 124
BIOS 126
MEDORIA RAM 125
SISTEMA OPERATIVO 135
PROGRAMAS DE APLICACIÓN 136
OTROS MÓDULOS DE PROGRAMA 137
DATOS DE PROGRAMA 138
UNIDAD DE PROCESAMIENTO 121
ADAPTADOR DE VÍDEO 148
BUS DEL SISTEMA
123
INTERFAZ DE CONTROLADOR DE DISCO RÍGIDO
INTERFAZ DE CONTROLADOR DE DISCO MAGNÉTICO
INTERFAZ DE CONTROLADOR ÓPTICO
INTERFAZ DE PUERTO EN SERIE
INTERFAZ DE RED
132
133
134
146
153
127
128
130
131
129
139
142
TECLADO
140
MÓDEM
154
RED DE ÁREA AMPLIA
152
RED DE ÁREA LOCAL
151
ORDENADOR REMOTO
149a
ORDENADOR REMOTO
149b
PROGRAMAS DE APLICACIÓN
136a
PROGRAMAS DE APLICACIÓN
136b
150a
150b
SISTEMA OPERATIVO 135
PROGRAMAS DE APLICACIÓN 136
OTROS MÓDULOS DE PROGRAMA 137
DATOS DE PROGRAMA 138

FIG. 1

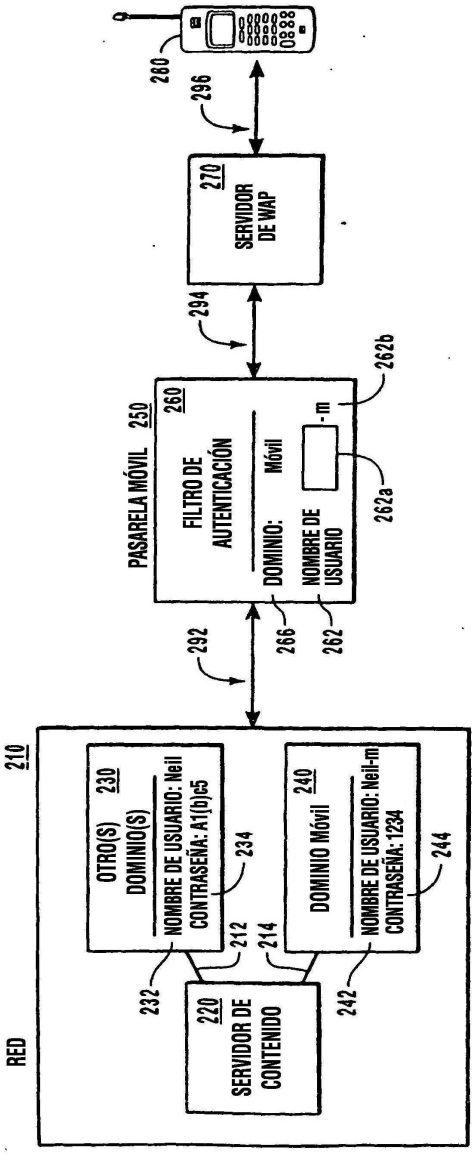
280
296
270
SERVIDOR DE WAP
294
PASARELA MÓVIL 250
260
FILTRO DE AUTENTICACIÓN
DOMINIO: Móvil
NOMBRE DE USUARIO -m
262b
262a
266
262
292
210
RED
OTRO(S) DOMINIO(S) 230
NOMBRE DE USUARIO: Neil
CONTRASEÑA: A1(b)p5
234
DOMINIO Móvil 240
NOMBRE DE USUARIO: Neil-m
CONTRASEÑA: 1234
244
212
214
232
242
220
SERVIDOR DE CONTENIDO

FIG. 2

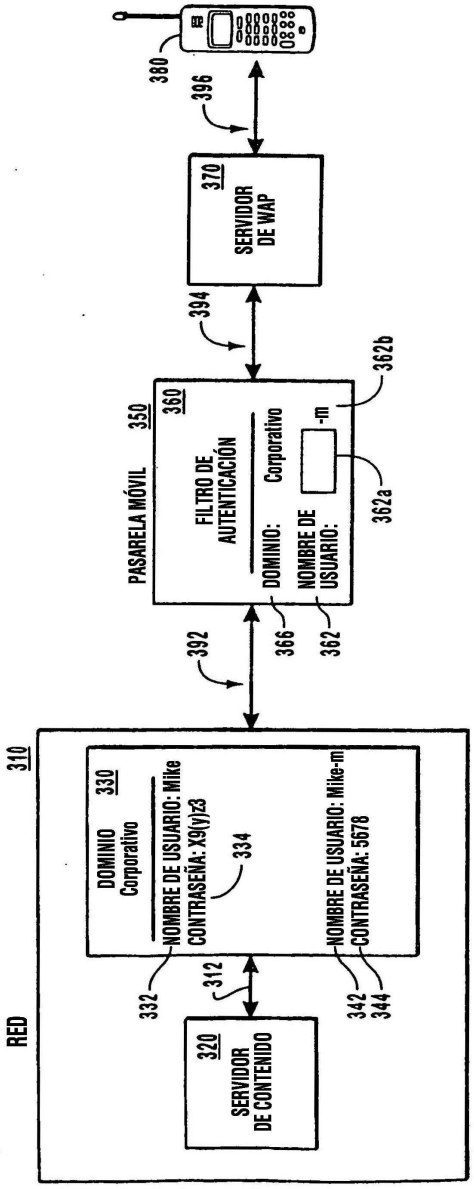
380
396
370
SERVIDOR DE WAP
394
362b
360
PASARELA MÓVIL 350
FILTRO DE AUTENTICACIÓN
DOMINIO: Corporativo
-m
NOMBRE DE USUARIO:
362a
392
366
362
310
RED
DOMINIO 330
Corporativo
NOMBRE DE USUARIO: Mike
CONTRASEÑA: X9(y)z3
334
NOMBRE DE USUARIO: Mike-m
CONTRASEÑA: 5678
332
312
342
344
320
SERVIDOR DE CONTENIDO

FIG. 3

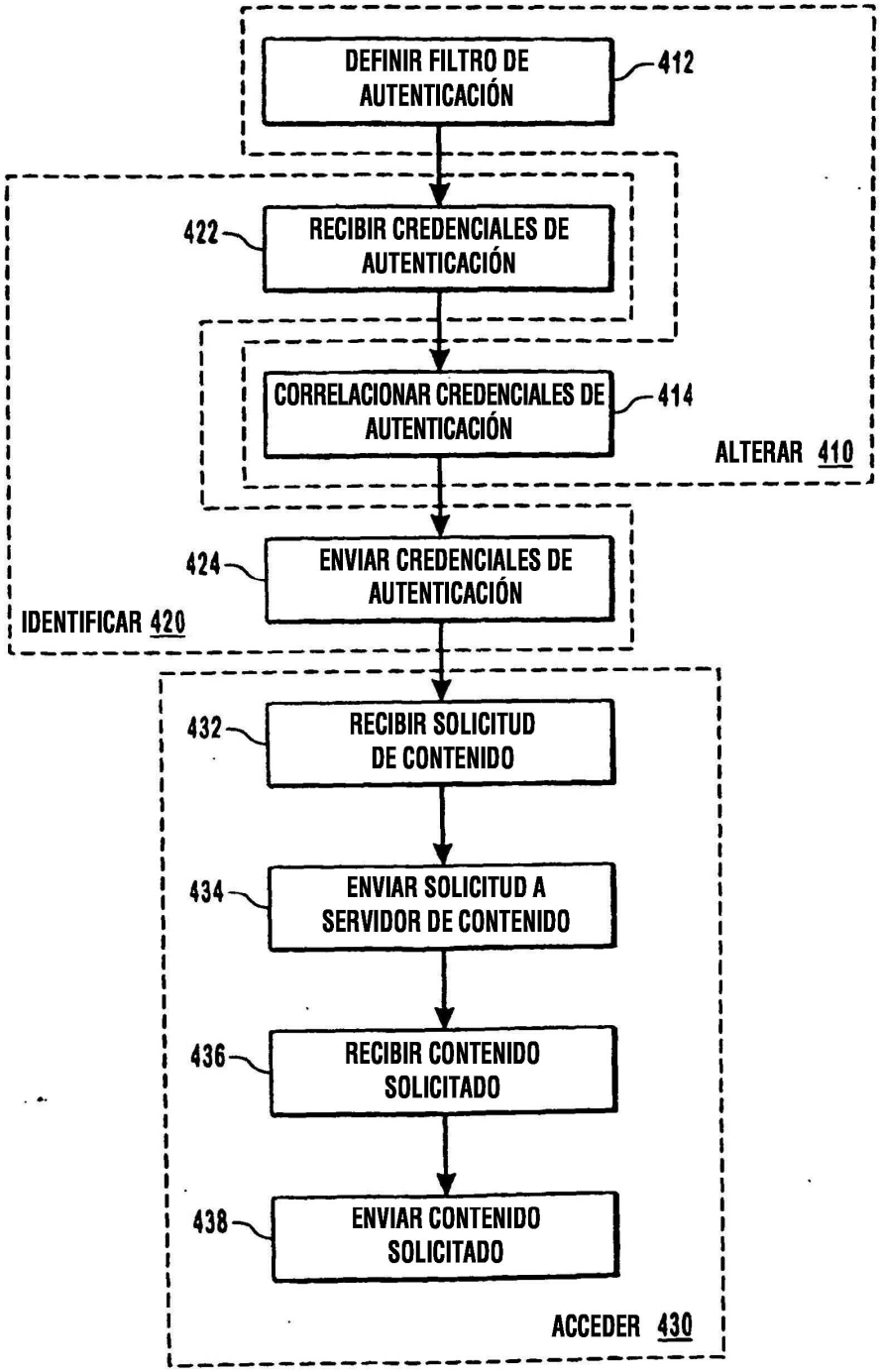
DEFINIR FILTRO DE AUTENTICACIÓN
412
422
RECIBIR CREDENCIALES DE AUTENTICACIÓN
CORRELACIONAR CREDENCIALES DE AUTENTICACIÓN
414
ALTERAR 410
424
ENVIAR CREDENCIALES DE AUTENTICACIÓN
IDENTIFICAR 420
432
RECIBIR SOLICITUD DE CONTENIDO
434
ENVIAR SOLICITUD A SERVIDOR DE CONTENIDO
436
RECIBIR CONTENIDO SOLICITADO
438
ENVIAR CONTENIDO SOLICITADO
ACCEDER 430

FIG. 4