(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 420 158**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.05.2005 E 05750620 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2013 EP 1766839**

(54) Título: **Sistema y método para bloquear un inicio de sesión de red no autorizado usando una contraseña robada**

(30) Prioridad:

15.07.2004 US 892584
11.03.2005 US 77948

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.08.2013

(73) Titular/es:

ANAKAM, INC. (100.0%)
9171 Town Centre Drive Suite 460
San Diego, CA 92122 , US

(72) Inventor/es:

CAMAISA, ALLAN y
SAMUELSSON, JONAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método para bloquear un inicio de sesión de red no autorizado usando una contraseña robada.

I. Campo de la Invención

La presente invención se refiere, en general, a la prevención de un inicio de sesión de red no autorizado usando una contraseña robada.

II. Antecedentes de la Invención

Las contraseñas son una manera utilizable desde cualquier lugar para proporcionar un mínimo nivel de autenticación a un usuario de ordenador que trata de acceder a un ordenador en red, tal como un sitio Web. Por ejemplo, la banca en línea requiere que un usuario inicie sesión en un servidor Web de una institución financiera usando un nombre de usuario y una contraseña que han sido proporcionados previamente al usuario por el servidor. De esta manera, sólo un usuario (con suerte, el verdadero dueño de la cuenta) que posee tanto el nombre de usuario como la contraseña puede acceder a la cuenta del usuario.

Como otro ejemplo, algunos servidores Web proporcionan servicios de suscripción. Por ejemplo, los usuarios pueden suscribirse a un sitio Web para recibir publicaciones de noticias, títulos de música, etc. Para garantizar que sólo los usuarios que hayan pagado la cuota de suscripción puedan acceder a los contenidos, se requiere que un usuario que pretende acceder inicie sesión con un nombre de usuario y una contraseña.

En cualquier caso, es posible que una contraseña pueda ser robada y que, consecuentemente, la información destinada únicamente para el propietario legítimo de la contraseña caiga en las manos de un ladrón de contraseñas. Algunas estimaciones para el año 2003 indican que hasta dos millones de estadounidenses han sufrido un asalto de sus cuentas bancarias en línea, con una pérdida promedio de 1.200 dólares para una pérdida total de más de dos mil millones de dólares. Una forma común en la que los ladrones consiguen el acceso es enviando correos electrónicos con aspecto oficial a los clientes del banco, solicitando nombres de usuario y contraseñas de manera que, si las peticiones ilegítimas se cumplen, se usan, a continuación, para iniciar sesión en las cuentas en línea y robarles el dinero. Habiendo reconocido el problema anterior, se proporciona la solución en la presente memoria.

III. Técnica anterior

El documento US 2001/044896 Al (SCHWARTZ GIL [IL] ET AL), 22 de Noviembre de 2001, describe una técnica para autenticar una primera parte a una segunda parte que es aplicable a las transacciones electrónicas. Además de emplear contraseñas personales, y un dispositivo operativo con parámetro de huella dactilar, se emplean dos firmas, una que es característica de la primera parte, y la otra asociada con el ordenador o el dispositivo de comunicación de la primera parte. Las firmas cambian a intervalos aleatorios, en respuesta a solicitudes de cambio realizadas por el dispositivo de la primera parte al dispositivo empleado por la segunda parte. Las firmas cambiadas invalidan las firmas anteriores, y se almacenan en los dispositivos de computación o de comunicación de ambas partes. El procedimiento de cambio autentica el ordenador o el dispositivo de comunicación, y puede autenticar también el propietario de la contraseña.

El documento US 2003/005308 Al (RATHBUN PAUL L [US] ET AL) 2 de Enero de 2003, describe un método y un sistema proporcionados para restringir el acceso de clientes a un sitio Web. Un primer servidor Web recibe un inicio de sesión de cliente y, como respuesta, asigna un cookie al cliente, la cual contiene una credencial de acceso que tiene al menos un atributo basado en el papel de cliente. Un segundo servidor Web aloja el sitio Web seguro, teniendo el sitio Web un fichero de seguridad asociado que contiene al menos un privilegio de acceso basado en el papel de cliente. En respuesta a la solicitud HTTP del cliente en el segundo servidor, la cookie es recuperada, decodificada y las credenciales de acceso se comparan con el al menos un privilegio de acceso basado en el papel de cliente. Si las credenciales de acceso tienen al menos un atributo basado en papel en común con el al menos un acceso basado en el papel de cliente al segundo sitio Web asegurado. El documento US 2004/059951 Al (PINKAS BINYAMIN [US] ET AL), 25 de Marzo de 2004 describe sistemas y métodos proporcionados para la autenticación mediante la combinación de una Prueba de Turing Inversa (Reverse Turing Test, RTT) con protocolos de autenticación de usuarios basados en contraseña para proporcionar una mayor resistencia a los ataques por fuerza bruta. Según una realización de la invención, se proporciona un método para la autenticación de usuarios, en el que el método incluye la recepción de un par nombre de usuario/contraseña asociado con un usuario; la solicitud una o más respuestas de una primera Prueba de Turing Inversa (RTT); y la concesión del acceso al usuario si se recibe una respuesta válida a la primera RTT y el par nombre de usuario/contraseña es válido.

El documento US 6 047 268 A (BARTOLI PAUL D [US] ET AL), 4 de Abril de 2000, describe un método y un

aparato para la autenticación de transacciones realizadas en una red de datos que utiliza una “cookie” que contiene tanto información estática (información que identifica al usuario) como información dinámica (información basada en la transacción). La parte de información dinámica orientada a la transacción comprende un número aleatorio y un número de secuencia, en el que este último realiza un seguimiento del número de transacciones de facturación realizadas por el usuario con el número de cuenta. La cookie, enviada al fichero cookie del usuario tras una transacción previa, es válida para sólo una única transacción nueva. Un servidor de facturación, tras recibir la cookie que contiene las partes de información estática y dinámica, identifica el usuario a partir del número de cuenta en la parte estática y accede desde una base de datos asociada al número aleatorio y al número de secuencia del servidor de facturación enviados por última a ese usuario en la parte dinámica orientada a la transacción. Si la parte dinámica esperada coincide con la parte dinámica recibida, el usuario es autenticado para proceder con la transacción actual.

EXPOSICIÓN DE LA INVENCIÓN

Según la presente invención, en las reivindicaciones adjuntas se exponen un método y un sistema para conceder a un usuario, de manera selectiva, acceso a los datos.

SUMARIO DE LA INVENCIÓN

Un método para conceder a un usuario, de manera selectiva, acceso a los datos incluye, en un servidor Web, la recepción de un nombre de usuario y una contraseña desde un ordenador de usuario. Sin limitaciones, el servidor Web puede ser un servidor de banca en línea o un servidor de suscripción de contenido. Si el nombre y la contraseña de usuario son válidos, se accede a una cookie depositada previamente en el ordenador de usuario y el servidor determina si la cookie es válida. Sólo si la cookie, el nombre de usuario y la contraseña son válidos se concede el acceso a los datos en el ordenador de usuario. De lo contrario, se inicia un procedimiento de validación de usuario.

En realizaciones no limitativas, la cookie incluye al menos una clave de inicio de sesión y un ID de máquina. Si la cookie, el nombre de usuario y la contraseña son válidos y se concede el acceso al ordenador de usuario, una nueva cookie es descargada posteriormente en el ordenador de usuario para su uso durante el siguiente intento de inicio de sesión. La nueva cookie incluye el mismo ID de máquina que la antigua cookie, pero una clave de acceso diferente.

Si se desea, los métodos no limitativos pueden incluir además, antes de iniciar un procedimiento de validación del usuario cuando no se encuentra un cookie válida en el ordenador de usuario, la determinación de si todas las N máquinas asignadas por el servidor al usuario han accedido al servidor, donde N > 1. Si no, el servidor descarga una cookie al ordenador de usuario que está intentando el acceso, en la que esta cookie tiene un ID de máquina único y una clave de inicio de sesión única. A continuación, el servidor concede el acceso al ordenador de usuario, quizás después de una validación exitosa.

Los ejemplos no limitativos del procedimiento de validación pueden incluir el envío de un correo electrónico al usuario, en el que el correo electrónico contiene al menos un hipervínculo a un sitio Web en el que puede obtenerse una nueva cookie que es válida para acceder a los datos. El acceso al sitio Web en el que se encuentra la nueva cookie puede deshabilitarse después de que el usuario hace clic en el hipervínculo. O si no, el procedimiento de validación puede incluir una solicitud al usuario para que llame a un número de teléfono para verificar la información predeterminada, o para que acceda a un sitio Web para verificar en línea una información predeterminada.

En otro aspecto, se describe un sistema para impedir que un ladrón que posee una contraseña de un usuario acceda a la información destinada a ser accedida por el usuario. El sistema incluye al menos un ordenador de usuario asociado con el usuario, y un ordenador servidor que controla el acceso a la información. El ordenador servidor concede el acceso a la información solo tras la recepción de una contraseña válida y la determinación de que una cadena de verificación válida reside en el ordenador de usuario; de lo contrario, el servidor inicia un procedimiento de validación.

En todavía otro aspecto, un sistema de ordenador incluye un servidor Web que tiene medios para enviar un nombre de usuario y una contraseña a un ordenador de usuario, y medios para enviar una cadena de verificación al ordenador de usuario. La cadena de verificación incluye el ID de máquina que es sustancialmente único al ordenador de usuario y una clave de inicio de sesión que es actualizada cada vez que el ordenador de usuario accede al servidor Web. El servidor tiene también medios para, después de enviar la cadena de verificación al ordenador de usuario y en respuesta a un intento de inicio de sesión desde un ordenador de inicio de sesión que puede ser o no el ordenador de usuario, determinar si una contraseña enviada desde el ordenador de inicio de sesión es válida o no, y si la cadena de verificación reside en el ordenador de inicio de sesión. Se proporcionan

medios para, si la contraseña es válida pero la cadena de verificación no reside en el ordenador de inicio de sesión, se deniegue el acceso y, a continuación, se inicie un procedimiento de validación y/o se determine si todas las N máquinas asignadas al usuario han accedido al servidor. Si todas las máquinas asignadas no han accedido al servidor, una cadena de verificación que tiene un ID de máquina que es diferente al ID de máquina del ordenador de usuario y una clave de inicio de sesión que es diferente de la clave de inicio de sesión del ordenador de usuario es descargada al ordenador de inicio de sesión, el cual puede recibir, a continuación, permiso de acceso.

En otra realización, un método para conceder a un usuario, de manera selectiva, acceso a los datos incluye, en un servidor de información, la recepción de un nombre de usuario y una contraseña desde un ordenador de usuario. El método incluye también, si el nombre de usuario y la contraseña son válidos, de manera transparente para el ordenador de usuario, la transferencia de la comunicación del ordenador de usuario a un servidor de autenticación. A continuación, en el servidor de autenticación, se determina si una cookie previamente depositada en el ordenador de usuario incluye un ID de máquina que coincide con un ID de máquina de prueba y una clave de inicio de sesión que coincide con una clave de inicio de sesión de prueba. Si es así, de manera transparente para un usuario del ordenador de usuario, la comunicación del ordenador de usuario es transferida de nuevo al servidor de información y el acceso a los datos es concedido al ordenador de usuario. También se actualiza la clave de acceso. Si la prueba de la cookie falla, sin embargo, el método no concede el acceso del ordenador de usuario a las etapas de autenticación adicionales en ausencia de datos.

En algunas realizaciones, si el ID de máquina no coincide con el ID de máquina de prueba, se ejecutan etapas de autenticación adicionales. En este caso, las etapas de autenticación adicionales pueden incluir el envío de un código PIN a un teléfono inalámbrico asociado con el usuario, y la recepción desde el ordenador de usuario del código PIN desde el usuario obtenido desde el teléfono inalámbrico. O, tal como se ha indicado anteriormente, el código PIN puede ser enviado a una cuenta de correo electrónico del usuario. En otras realizaciones, si el ID de máquina coincide con el ID de máquina de prueba, pero la clave de inicio de sesión no coincide con la clave de inicio de sesión de prueba, no se ejecutan etapas de autenticación adicionales y se deshabilita una cuenta asociada con el usuario.

El servidor de información puede ser, por ejemplo, un servidor de banca en línea, un servidor de comercio electrónico o un servidor VPN.

En otro aspecto, un sistema de autenticación para al menos un ordenador de usuario asociado con un usuario incluye al menos un servidor de información que controla el acceso a la información. El servidor de información recibe los datos de autenticación iniciales desde el ordenador de usuario y si los datos de autenticación iniciales son válidos, de manera transparente para un usuario del ordenador de usuario, transfiere la comunicación a al menos un servidor de autenticación. El servidor de autenticación realiza una autenticación secundaria con el ordenador de usuario y si la autenticación secundaria es válida, de manera transparente para un usuario del ordenador de usuario, es transferida de nuevo al servidor de información para acceder a la información. De lo contrario, una cuenta asociada con el usuario es deshabilitada, y/o se ejecuta una autenticación terciaria, cuya finalización con éxito hace que el servidor de autenticación, de manera transparente para un usuario del ordenador de usuario, transfiera la comunicación de nuevo al servidor de información para acceder a la información.

En todavía otro aspecto, un servidor de autenticación configurado para la comunicación con al menos un ordenador de usuario y al menos un servidor de información incluye medios para la autenticación del ordenador de usuario usando una cookie depositada previamente en el ordenador de usuario. El servidor de autenticación incluye también medios sensibles a los medios de autenticación, para informar al servidor de información para conceder el acceso al ordenador de usuario. El servidor de autenticación incluye además medios sensibles a los medios de autenticación, para transferir la comunicación del ordenador de usuario de nuevo al servidor de información.

Los detalles de la presente invención, en relación a su estructura y funcionamiento, pueden comprenderse mejor con referencia a los dibujos adjuntos, en los que los números de referencia similares se refieren a partes similares, y en los que:

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de bloques de un sistema ejemplar para implementar la presente invención;
La Figura 2 es un diagrama de flujo de la lógica de registro;
La Figura 3 es un diagrama de flujo de la lógica de inicio de sesión subsiguiente;
La Figura 4 es un diagrama de bloques de otro sistema no limitativo;
La Figura 5 es un diagrama de flujo de alto nivel de la lógica usada por el sistema mostrado en la Figura 4;

y
La Figura 6 muestra más detalles de la lógica mostrada en la Figura 5.

DESCRIPCIÓN DETALLADA DE LA REALIZACIÓN PREFERIDA

Con referencia inicialmente a la Figura 1, se muestra un sistema, designado en general con el número de referencia 10, que incluye una pluralidad de ordenadores 12 de usuario (sólo se muestra un único ordenador de usuario en aras de una mayor claridad), cada uno de los cuales puede tener un procesador 14 y un disco y/o un almacenamiento 16 de programa de estado sólido para almacenar el software que conforma la lógica. Además, cada ordenador 12 de usuario puede incluir uno o más dispositivos 18 de entrada, tales como teclados, ratones, dispositivos de reconocimiento de voz, etc., así como uno o más dispositivos 20 de salida, tales como monitores, impresoras, otros ordenadores, etc. La lógica de autenticación ejecutada por el presente sistema y expuesta en la presente memoria puede ser usada en aplicaciones tales como, pero no limitadas a, la banca en línea, el comercio electrónico seguro en línea y el control de acceso VPN.

Tal como se muestra en la Figura 1, el ordenador 12 de usuario se comunica con un servidor 22 Web a través de Internet 24. El servidor 22 tiene un procesador 26 y un disco y/o un almacenamiento 28 de programa de estado sólido para almacenar el software que conforma la lógica, incluida la totalidad o parte de la lógica expuesta más adelante. El servidor 22 puede acceder a una base de datos 30 de información de clientes que contiene la información de inicio de sesión y de registro de los usuarios establecida más adelante, entendiéndose que la base de datos puede estar rellenada previamente con información de usuario acerca de los clientes existentes que elijan iniciar el servicio actual. Además, el servidor 22 puede acceder a una base de datos 32 de información para suministrar a los usuarios una información deseada, por ejemplo, registros de cuentas bancarias, contenido de suscripción, etc. Si se desea, las bases de datos 30, 32 pueden ser implementadas en una única estructura de datos.

Con referencia ahora a la lógica de registro inicial de la Figura 2, que comienza en el bloque 34, el usuario inicia una sesión en el tiempo inicial. Pasando al bloque 36, se establecen un nombre de usuario y una contraseña, por ejemplo, permitiendo al usuario seleccionar un nombre de usuario y una contraseña, o con la concesión, por parte del servidor 22, de un nombre de usuario y una contraseña al usuario. En el bloque 38, si se desea, se puede obtener información adicional del usuario. Dicha información del usuario puede incluir información de facturación e información de validación. La información de validación puede ser confidencial para el usuario con el fin de proteger su cuenta de usuarios externos no deseados que podrían haber robado información de la cuenta del usuario, según una lógica adicional establecida más adelante. Debe entenderse que, de manera alternativa, la información de validación puede ser obtenida previamente desde el usuario de diversas maneras, en línea o fuera de línea.

En el bloque 40, al mismo tiempo que el usuario se registra o posteriormente, en el caso de usuarios que ya están registrados con el servidor para otros propósitos, pero ahora, por primera vez, inician el servicio actual, se envía una cadena de verificación al ordenador del usuario. Preferiblemente, la cadena de verificación es, aunque no necesariamente, una que no requiere interacción con el usuario o con un software especial, tal como una cookie que puede tener un ID de máquina y una clave de inicio de sesión, por ejemplo, una cadena de 4.096 bits con un valor generado aleatoriamente. La cookie puede tener también un ID de usuario que es único para una persona. La cookie no requiere un software de cliente especial y es completamente invisible para el usuario. Tanto el ID de máquina como la clave de inicio de sesión son generados aleatoriamente, almacenados en el servidor, y están asociados con la cuenta de ese usuario. Una vez establecida la cuenta del usuario, el ID de máquina y la clave de inicio de sesión se asocian con la cuenta del usuario. El acceso se concede si toda la información de usuario y la información de la cuenta de usuario son correctas, tal como se muestra en el bloque 42.

Después del registro, la lógica que puede ser implementada por el servidor 22 pasa a la Figura 3 para intentos posteriores por parte del usuario para iniciar sesión en el servidor 26 y acceder a la información del usuario contenida en la base de datos 32 mostrada en la Figura 1. Comenzando con el bloque 44, tras inicios de sesión posteriores, el usuario introduce el nombre de usuario y una contraseña. En el bloque 46 de decisión, el servidor comprueba la validez del nombre de usuario y de la contraseña. Si el nombre de usuario y la contraseña no son correctos, se deniega el acceso del usuario en el bloque 48.

Si en el bloque 46 de decisión, se determina que el nombre de usuario y la contraseña son correctos, la lógica pasa al bloque 50 de decisión, en el que el servidor comprueba el ordenador de usuario para verificar que la cookie correcta esté almacenada en el ordenador del usuario, por ejemplo, comparando la cookie en el ordenador del usuario con los registros de la cookie del servidor. Si el servidor determina que la cookie está presente y es correcta, se concede el acceso a la información del usuario en la base de datos 32 en el bloque 52. A continuación, en el bloque 54, suponiendo que la máquina usada no es una máquina recién introducida, tal como se expone

adicionalmente más adelante en relación al bloque 58, se descarga una nueva clave de acceso transportada en una nueva cookie preferiblemente a través de una conexión SSL cifrada. Esta nueva cookie con la nueva clave de inicio de sesión es usada para el siguiente inicio de sesión de usuario usando la misma máquina. La clave de inicio de sesión en la nueva cookie es diferente de la clave de inicio de sesión de la cookie antigua, pero el ID de máquina se mantiene constante.

Por el contrario, si, en el bloque 50 de decisión, se determina que la cookie en el ordenador de usuario no es correcta, en algunas realizaciones opcionales el servidor 22 pasa al bloque 56 de decisión para determinar si todos los ordenadores que han sido asignados al usuario han accedido o no al servidor 22. En otras palabras, en algunas aplicaciones, tales como la banca en línea, el servidor puede asignar al usuario en el registro, en respuesta a una solicitud del usuario, más de un único ordenador (es decir, para usar “N” ordenadores, N > 1) para acceder a la información en la base de datos 32. Por ejemplo, un cliente de banca en línea podría desear acceder a su cuenta bancaria, tanto desde el ordenador de la oficina como desde un ordenador doméstico. Si todos los "N" ordenadores asignados que han sido asignados al usuario han accedido al servidor 22 y han recibido las cookies, lo que significa que el ordenador usado actualmente tiene un número superior al número autorizado, se deniega el acceso del usuario y la lógica pasa al bloque 57 para desencadenar un procedimiento de validación. Si se desea, para frustrar un ataque de diccionario, pueden permitirse sólo un número limitado de intentos de verificación de inicio de sesión/cookie desde cualquier máquina, después de los cuales la máquina es bloqueada hasta que se produzca una validación exitosa.

En una implementación no limitativa, el procedimiento de validación puede incluir la introducción, por parte del usuario, de información confidencial proporcionada inicialmente en el procedimiento inicial de inicio de sesión. La información de validación puede ser el nombre de soltera de la madre del usuario, el número de la seguridad social del usuario, o alguna otra información que preferiblemente sea personal para el usuario. A continuación, el servidor 22 comprueba la entrada del usuario con la información de validación recopilada en el bloque 38 en la Figura 2. Si se encuentra una coincidencia, la validación es exitosa y se concede el acceso al usuario; de lo contrario, la validación no tiene éxito y se deniega el acceso.

En algunas implementaciones, el procedimiento de validación puede incluir el envío de un correo electrónico al usuario. El correo electrónico puede contener un hipervínculo a un sitio Web en el que puede obtenerse una nueva cookie que es válida para acceder a los datos. Si se desea, el acceso al sitio Web en el que puede obtenerse una nueva cookie puede ser deshabilitado después de que el usuario hace clic una vez en el hipervínculo. O si no, el procedimiento de validación puede incluir una solicitud al usuario para que llame a un número de teléfono para verificar una información predeterminada, o para que acceda a un sitio Web para verificar la información predeterminada en línea. Una vez que la validación es exitosa, el servidor 22 permite el acceso a la información en la base de datos 32. Por el contrario, si el servidor determina en el bloque 56 de decisión que no todas las máquinas que han sido asignadas han accedido al servidor 22, una nueva cookie con un nuevo ID de máquina y una clave de acceso es descargada al nuevo ordenador en el bloque 58. A continuación, la lógica vuelve al bloque 52 para conceder el acceso, en algunas realizaciones sólo después de haber desencadenado la primera validación, tal como se describe en el bloque 57, para asegurar que el usuario correcto está iniciando la sesión.

En el contexto de la adición de una nueva máquina, cuando más de un único ordenador de usuario están autorizados, la nueva máquina puede ser añadida de manera automática en su primer inicio de sesión, según la lógica anterior (suponiendo que se cumplen las condiciones indicadas anteriormente), o el servidor puede preguntar al usuario de la nueva máquina si la nueva máquina debe considerarse como uno de los "N" ordenadores autorizados, de manera temporal o de otra manera. Si el usuario indica que la máquina será sólo temporal (por ejemplo, si el usuario está operando un terminal en un hotel), el usuario podría especificar una fecha de caducidad y/o un número de inicios de sesión después de los cuales se denegaría cualquier acceso a la información de usuario desde esa máquina, o al menos desencadenaría de nuevo el procedimiento de verificación. Esto puede llevarse a cabo haciendo que la cookie se considera “caducada” al final del período. Por ejemplo, en un terminal de una habitación de hotel, un usuario podría especificar una caducidad en la fecha esperada de salida del hotel, o un usuario podría especificar un número de inicios de sesión que se permitirán desde esa máquina antes de que se desencadene de nuevo el procedimiento de verificación. La información de caducidad se almacena en el servidor. Cuando una máquina llega a la fecha de caducidad, el número de nuevas máquinas restantes para ser añadidas a la cuenta del usuario puede actualizarse en una unidad. Por el contrario, no se solicitaría al usuario información sobre el uso temporal al comunicarse con el servidor desde un conjunto básico de ordenadores desde los que el usuario tiene un acceso autorizado permanente. Una o más piezas de la información anterior que es transmitida entre los ordenadores pueden ser encriptadas usando, por ejemplo, un cifrado DES triple.

Las Figuras 4-6 muestran implementaciones preferidas específicas de la lógica y el sistema anteriores. Por motivos de simplicidad, la Figura 4 omite ciertos detalles, tales como los dispositivos de entrada y los dispositivos

de salida. Un sistema 100 preferido puede incluir uno o más ordenadores 102 de usuario que se comunican a través de Internet, por ejemplo, con un servidor 104 de información de una institución financiera. El servidor 104 de información se comunica con un servidor 106 de autenticación. Preferiblemente, ambos servidores 104, 106 están detrás de un cortafuegos 108. Aunque sólo se muestran un único servidor 104 de información y un único servidor 106 de autenticación, debe entenderse que pueden usarse clústeres de servidores. Por ejemplo, pueden usarse clústeres J2EE que usan persistencia de memoria de replicación de sesión, donde los objetos individuales en la sesión Http son serializados en un servidor de respaldo conforme cambian, proporcionando un alto rendimiento y escalabilidad. Además, cuando el servidor 106 de autenticación está detrás del cortafuegos 108, el uso de una Capa de Conexión Segura (Secure Socket Layer, SSL) puede no ser necesario, aunque si se requiere acceso desde una extranet, puede usarse SSL.

En cualquier caso, el propósito del sistema 100 es permitir el acceso controlado del ordenador 102 de usuario a los datos en una base de datos 110 de información sensible, usando la información de autenticación en una base de datos 112 de autenticación. El servidor 104 de información y la base de datos 110 de información sensible pueden ser un servidor/una base de datos convencionales usados, por ejemplo, en una institución financiera, con las excepciones indicadas más adelante. Por el contrario, el servidor 106 de autenticación y la base de datos 112 de autenticación pueden ser complementos según los principios actuales. En cualquier caso, las bases de datos en la presente memoria pueden ser, por ejemplo, servidores SQL, servidores DB2, servidores Oracle o servidores de gama baja, tales como MySQL.

La lógica de una implementación preferida de la lógica se muestra en las Figuras 5 y 6. Aunque puede usarse cualquier arquitectura de software apropiada, en una implementación puede usarse el marco “Struts” orientado a objetos de Apache Software Foundation, en el que las solicitudes del cliente al servidor 104 de información se almacenan en una memoria caché y se pasan a la acción de negocio requerida, tal como se define en el fichero de configuración Struts. A continuación, puede usarse el procedimiento de validación XSD para proporcionar reglas abiertas de validación de datos. La “Vista" es presentada en una única página JSP principal que usa XSL y XML para visualizar las distintas partes de la página. XSLT y XML proporcionan una separación completa entre la presentación, las empresas y las capas de datos. Los detalles adicionales de esta versión particular del diseño J2EE son conocidos en la técnica y se omitirán en aras de la claridad.

La Figura 5 muestra un flujo lógico de alto nivel que puede ser implementado por el sistema 100 mostrado en la Figura 4. Comenzando en el bloque 114, el usuario contacta con el servidor 104 de información usando el ordenador 102’ de usuario. En general, este contacto implica una autenticación inicial, tal como un procedimiento de inicio de sesión que incluye la introducción de un nombre de usuario y una contraseña. Si el procedimiento de inicio de sesión falla en el bloque 116 de decisión, la lógica termina, pero si tiene éxito, la presente invención avanza al bloque 118. La comunicación entre los servidores 104, 105 puede usar los principios SOAP conocidos en la técnica.

En el servidor 106 de autenticación, en el bloque 120 de decisión se determina si la máquina es reconocida (usando el ID de máquina en la cookie descrita anteriormente) y ha sido asegurada previamente por el usuario (usando la clave de inicio de sesión). Esto puede considerarse como un procedimiento de autenticación secundario. Si la prueba es superada, la lógica pasa al bloque 122 para transferir (de manera transparente para el usuario) al usuario de nuevo al servidor 104 de información para un servicio adicional, por ejemplo, para transacciones bancarias en línea. Por otro lado, si la prueba en el bloque 120 de decisión falla, la lógica puede pasar al bloque 124 para realizar una pregunta de seguridad al usuario según los principios establecidos en la presente memoria, cuya pregunta de seguridad podría considerarse como un procedimiento de autenticación terciario. Por ejemplo, un correo electrónico o un mensaje SMS de teléfono inalámbrico pueden ser enviados al usuario, que contienen un código de número de identificación personal (PIN), de un único uso, generado aleatoriamente, que es suministrado por el servidor 106 de autenticación. Este código PIN de un único uso puede ser enviado por el usuario al servidor 106 de autenticación usando el ordenador 102 de usuario, para demostrar que el usuario está autorizado para el acceso.

Si la pregunta de seguridad es superada con éxito en el bloque 126 de decisión, el usuario tiene la opción, en el bloque 128 de asegurar la máquina específica que está siendo usada para un uso futuro y, a continuación, el usuario es redirigido al servidor de información en el bloque 122. De lo contrario, el procedimiento termina sin proporcionar el acceso al usuario.

La Figura 6 muestra partes de una implementación no limitativa detallada de la lógica mostrada en la Figura 5. Comenzando en el bloque 130, el usuario intenta el inicio de sesión descrito anteriormente con el servidor 104 de información. Si esto no tiene éxito en el bloque 132 de decisión, la lógica vuelve al bloque 130, pero tal como se ha descrito anteriormente, cuando el inicio de sesión inicial con el servidor 104 de información es exitoso, la lógica, de

manera transparente para el usuario, es tomada por el servidor 106 de autenticación para determinar, en el bloque 134 de decisión, si el ordenador 102 de usuario tiene cookies deshabilitadas. Si las cookies están deshabilitadas, se devuelve un mensaje de error en el estado 136.

Si el usuario no ha deshabilitado la función de aceptación de cookies, sin embargo, la lógica pasa desde el bloque 134 de decisión al bloque 138 de decisión para determinar si el usuario existe en la base de datos 112 de autenticación tal como se determina, por ejemplo, por el ID de usuario residente en la cookie de autenticación o por el nombre de usuario usado en el bloque 130. En caso contrario, se devuelve un mensaje de error. De lo contrario, la lógica pasa al bloque 138 de decisión para determinar si la cuenta del usuario está habilitada. Esto se hace comprobando un indicador en la base de datos 112 de autenticación que indica si la cuenta del usuario está habilitada o deshabilitada. Si no se ha habilitado ninguna cuenta para el usuario, se devuelve un mensaje de error, pero si no, la lógica pasa desde el bloque 138 de decisión al bloque 140 de decisión para determinar si existe un perfil de usuario.

La expresión "perfil de usuario" hace referencia a un factor asociado con el usuario que indica si se plantea una pregunta de seguridad, y qué tipo de pregunta de seguridad se plantea, al usuario si se requiere una autenticación adicional. En otras palabras, el perfil asociado con un usuario determina qué debe proporcionar el usuario para probar la identidad y, de esta manera, para obtener acceso a la cuenta de usuario. Esta determinación se realiza comprobando si el ID de perfil asociado con el usuario en una tabla de usuarios en la base de datos 112 de autenticación se corresponde a un registro en una tabla de perfiles en la base de datos. Cuando no existe ningún perfil para el usuario, se devuelve un mensaje de error. Cuando existe un perfil, sin embargo, la lógica pasa al bloque 142 de decisión para determinar si la institución servida (por ejemplo, un banco que opera el servidor 104 de información) ha instituido lo que podría entenderse como un protocolo de inicio de sesión "silencioso". Si no se ha implementado este protocolo, la lógica pasa al bloque 144 de decisión donde se bifurca dependiendo del modo de funcionamiento, definido una vez más por la institución. En un modo de "bloqueo", la lógica pasa al bloque 146 de decisión para determinar si se requieren preguntas de autenticación de usuario. Si es así, la lógica pasa al bloque 148 de decisión para determinar si el usuario ha activado las preguntas. La expresión "activación de las preguntas" hace referencia a que el usuario ha proporcionado preguntas de seguridad auto-definidas y respuestas en el pasado (cuya prueba, de esta manera, resulta ser falsa sólo en el primer inicio de sesión), después de lo cual no se pide al usuario que proporcione o responda a preguntas de nuevo, evitando la necesidad de una autenticación terciaria. Si el usuario no ha activado las preguntas, se solicita al usuario que responda a preguntas definidas por la institución en el bloque 150.

Después del bloque 150 o cuando no se requieren las preguntas del usuario, o si se requieren y el usuario las ha activado, la lógica pasa al bloque 152 de decisión donde se determina si el ID de máquina en la cookie del usuario coincide con el ID residente en la base de datos 112 de autenticación. Si el ID de máquina coincide, a continuación, la lógica determina en el bloque 154 de decisión, si la clave de inicio de sesión descrita anteriormente en la cookie coincide con el valor correspondiente en la base de datos 112 de autenticación, y si se encuentra una coincidencia, se genera una nueva clave de inicio de sesión, registrada en el bloque 156, y se constituye una nueva cookie y se envía al usuario según la descripción anterior. A continuación, el usuario es autenticado, por ejemplo, accediendo al servidor 104 de información / la base de datos 110 de información en el bloque 158. El servidor de información recibe una notificación de la autenticación exitosa y la comunicación del ordenador de usuario es transferida de nuevo al servidor de información.

Si la prueba de la clave de inicio de sesión falla en el bloque 154 de decisión, la lógica pasa al bloque 160 de decisión, donde se bifurca dependiendo del modo. En el modo de bloqueo, la cuenta del usuario es deshabilitada en el bloque 162 mediante el establecimiento, de manera apropiada, del indicador indicado anteriormente en la base de datos 112 de autenticación, y se devuelve un mensaje de error. Sin embargo, en el modo de observación se permite al usuario acceder a su cuenta en el bloque 158.

Recuérdese que en el bloque 152 de decisión se realizó una prueba de ID de máquina. Si la prueba falla, la lógica pasa al bloque 164 de decisión, donde se bifurca dependiendo del modo. En el modo de bloqueo, la lógica pasa al bloque 166 para iniciar el segundo factor de autenticación, por ejemplo, la pregunta de seguridad expuesta anteriormente en referencia a la Figura 5. En lugar de invocar el método PIN suministrado por teléfono celular descrito anteriormente, pueden hacerse las preguntas al usuario y las respuestas del usuario pueden compararse con las establecidas en el bloque 150. En cualquier caso, en el bloque 168 de decisión se determina si la pregunta de seguridad ha sido respondida con éxito por el usuario y, si es así, se concede acceso a la cuenta en el bloque 158. Por el contrario, la lógica pasa al bloque 170 de decisión para determinar si se han realizado un número predeterminado de intentos de inicio de sesión, y cuando se supera el valor umbral, la cuenta del usuario es deshabilitada en el bloque 172, y se devuelve un mensaje de error. Sin embargo, en el modo de observación en el bloque 164 de decisión el usuario tiene autorización para acceder a su cuenta en el bloque 158.

Recuérdese que en el bloque 142 de decisión se determina si la función de inicio de sesión "silenciosa" está implementada. Si lo es, la lógica pasa al bloque 174 de decisión para determinar si el usuario, en base a, por ejemplo, el nombre de usuario introducido al iniciar la sesión en el bloque 130, es un usuario que intenta iniciar la sesión por primera vez. Si no, la lógica pasa al bloque 144 de decisión para operar tal como se ha descrito anteriormente. Sin embargo, si el usuario es un usuario que intenta iniciar sesión por primera vez, la lógica pasa al bloque 176 para establecer el ID de máquina estático expuesto anteriormente y, a continuación, al bloque 178 para establecer la clave de inicio de sesión dinámica de una sola vez. A continuación, se concede el acceso en el bloque 158.

De esta manera, en el modo de inicio de sesión silencioso, el usuario, una vez registrado por primera vez con el servidor 104 de información, recibe automáticamente la presente cookie de autenticación (dependiendo de las pruebas exitosas en los bloques 134-140 de decisión), la parte de la clave de acceso que es renovada cada vez que el usuario accede a su cuenta. Con respecto al modo de funcionamiento, en el modo de observación, el usuario recibe acceso a su cuenta, independientemente de las coincidencias de la cookie, mientras que en el modo de bloqueo se habilita una seguridad más alta según la lógica anterior.

REIVINDICACIONES

1. Un método para conceder a un usuario, de manera selectiva, acceso a datos, que comprende:

en un servidor (22, 104) de información, la recepción de un nombre de usuario y una contraseña desde un ordenador (12, 102) de usuario;
si el nombre de usuario y la contraseña son válidos, de manera transparente para el ordenador (12, 102) de usuario, la transferencia de la comunicación del ordenador de usuario a un servidor (106) de autenticación;
en el servidor (106) de autenticación, la determinación de si una cookie depositada previamente en el ordenador (12, 102) de usuario incluye un ID de máquina que coincide con un ID de máquina de prueba y una clave de inicio de sesión coincide con una clave de inicio de sesión de prueba y, si es así, de manera transparente para un usuario del ordenador (12, 102) de usuario, la transferencia de la comunicación del ordenador de usuario de nuevo al servidor (22, 104) de información, la concesión al ordenador (12, 102) de usuario de un acceso a los datos, y la actualización de la clave de acceso, por el contrario, la no concesión al ordenador de usuario de acceso a los datos en ausencia de etapas de autenticación adicionales.

2. Método según la reivindicación 1, en el que si el ID de máquina no coincide con el ID de máquina de prueba, se ejecutan etapas de autenticación adicionales.

3. Método según la reivindicación 1, en el que si el ID de la máquina coincide con el ID de máquina de prueba, pero la clave de inicio de sesión no coincide con la clave de inicio de sesión de prueba, no se ejecutan etapas de autenticación adicionales y una cuenta asociada con el usuario es deshabilitada.

4. Método según la reivindicación 2, en el que las etapas de autenticación adicionales incluyen el envío de un código PIN a un teléfono inalámbrico asociado con el usuario, y la recepción desde el ordenador de usuario el código PIN desde el usuario obtenido desde el teléfono inalámbrico.

5. Método según la reivindicación 1, en el que el servidor (22, 104) de información es un servidor de banca en línea.

6. Método según la reivindicación 1, en el que el servidor (22, 104) de información es un servidor de comercio electrónico.

7. Método según la reivindicación 1, en el que el servidor (22, 104) de información es un servidor VPN.

8. Sistema de autenticación para al menos un ordenador (12, 102) de usuario asociado con un usuario, que comprende un servidor (22, 104) de información y un servidor (106) de autenticación, cada uno configurado para efectuar el método de cualquiera de las reivindicaciones 1 a 7.

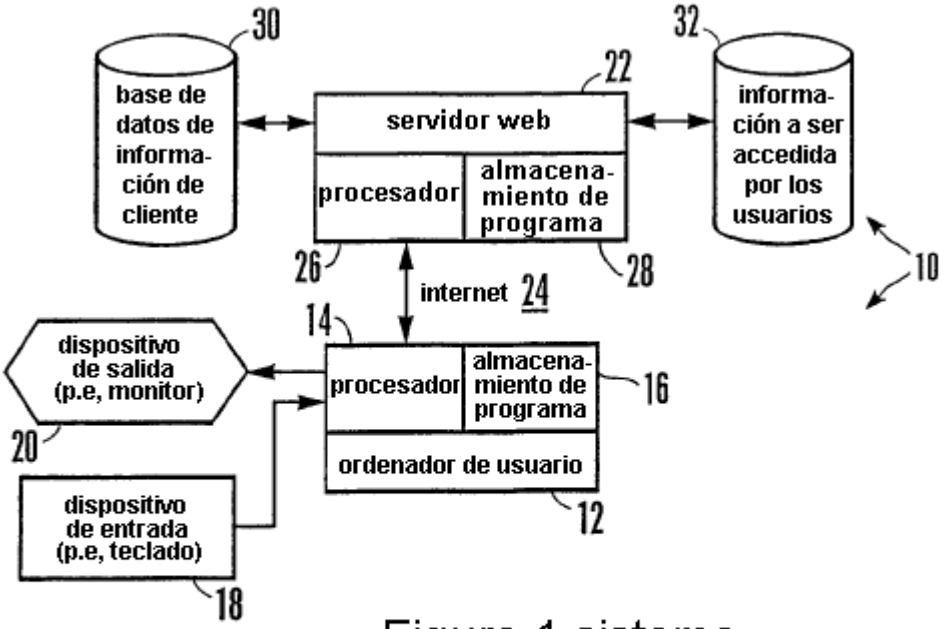
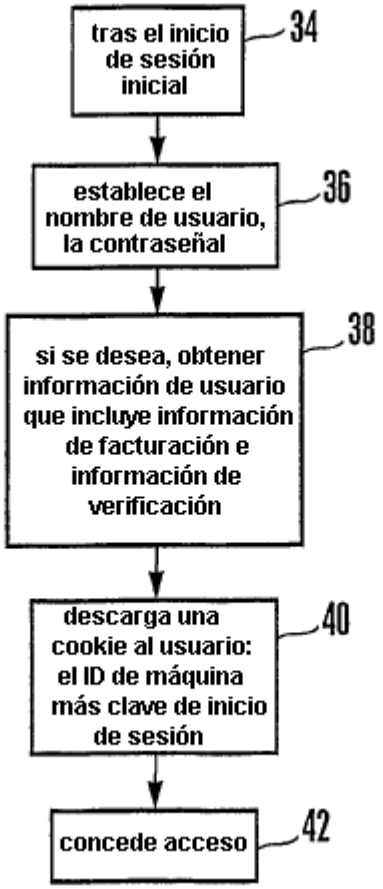


Figura 1 sistema

Figura 2 lógica de registro



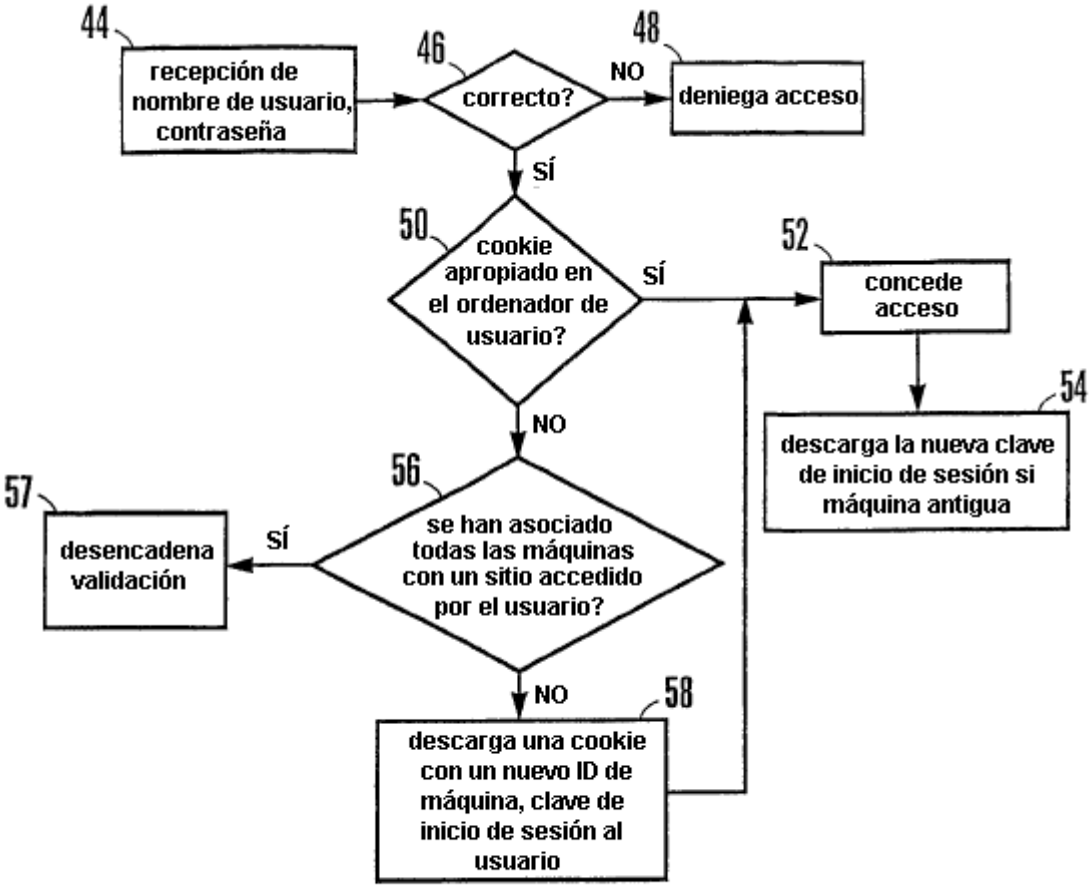


Figura 3 inicios de sesión sub-siguientes

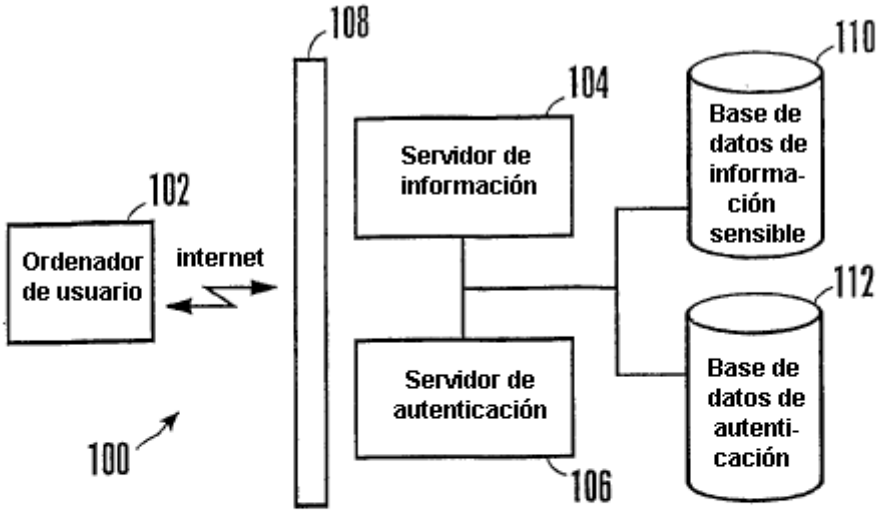
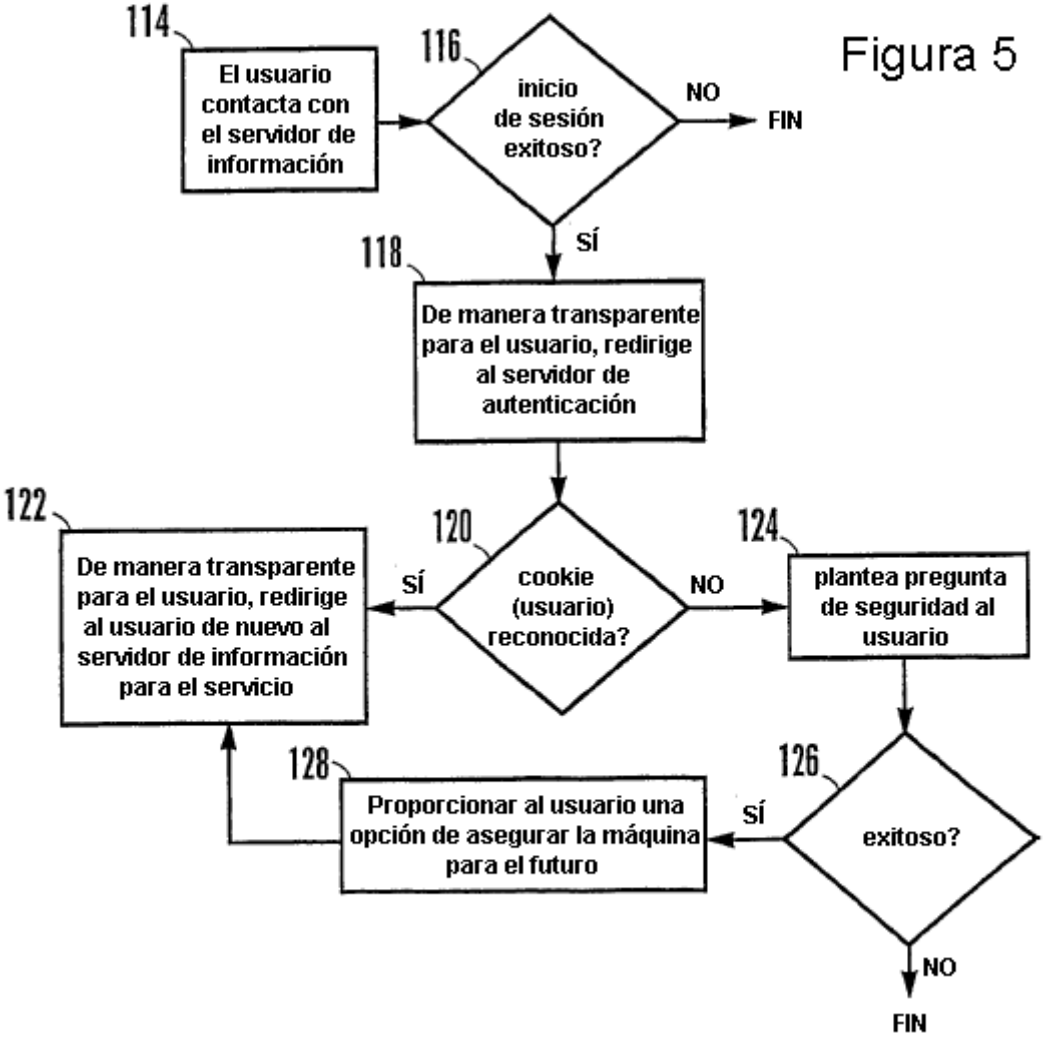


Figura 4

Figura 5



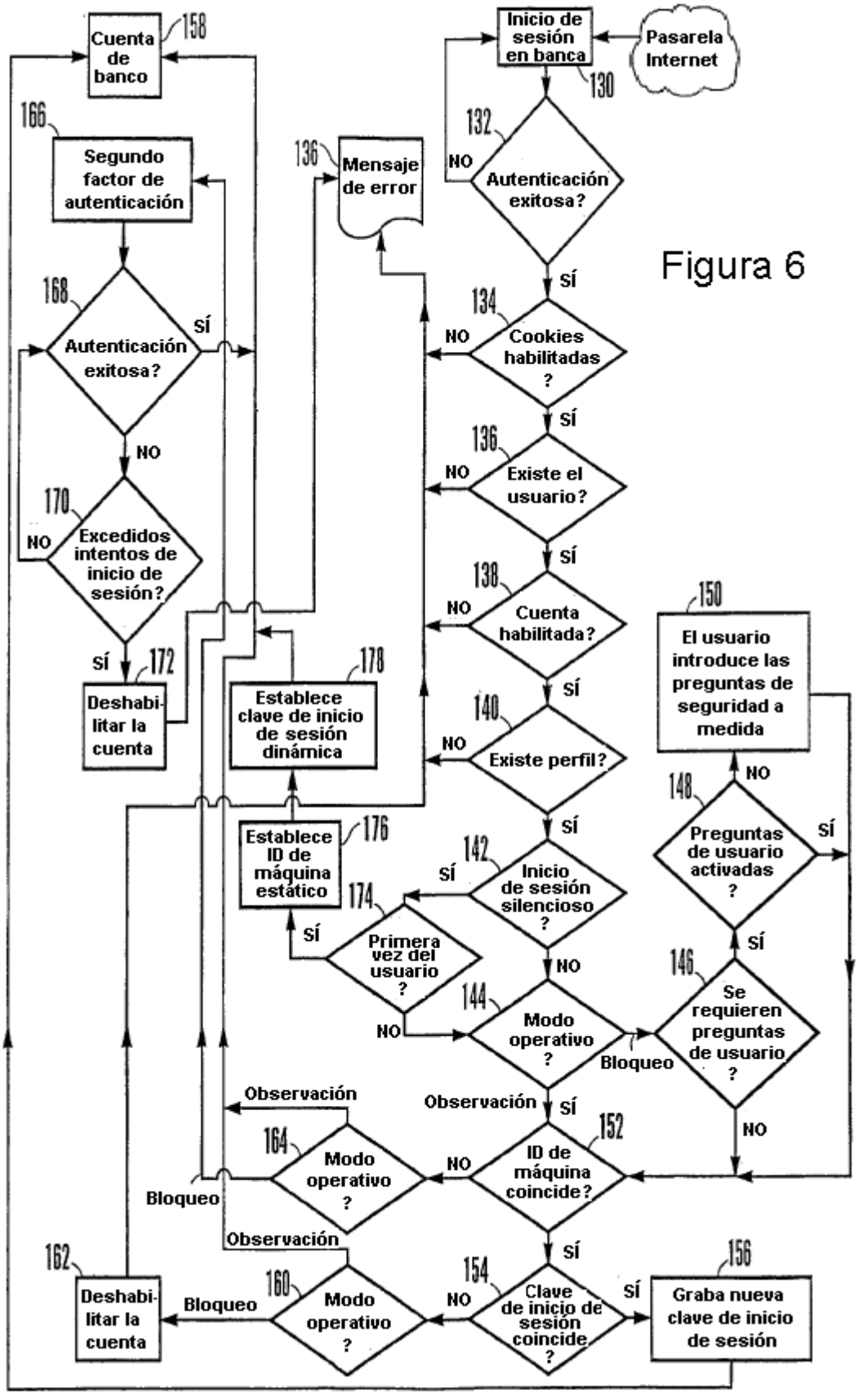

Cuenta de banco
158
Inicio de sesión en banca
Pasarela Internet
130
166
Segundo factor de autenticación
136
Mensaje de error
132
NO
Autenticación exitosa?
SÍ
168
Autenticación exitosa?
SÍ
NO
134
Cookies habilitadas ?
NO
SÍ
136
Existe el usuario?
NO
SÍ
138
Cuenta habilitada?
NO
SÍ
140
Existe perfil?
NO
SÍ
170
NO
Excedidos intentos de inicio de sesión?
SÍ
172
Deshabilitar la cuenta
178
Establece clave de inicio de sesión dinámica
176
Establece ID de máquina estático
142
Inicio de sesión silencioso ?
SÍ
174
Primera vez del usuario ?
SÍ
NO
144
Modo operativo ?
Bloqueo
Observación
Observación
SÍ
152
ID de máquina coincide?
NO
164
Modo operativo ?
Bloqueo
Observación
SÍ
154
Clave de inicio de sesión coincide ?
NO
SÍ
160
Modo operativo ?
Bloqueo
162
Deshabilitar la cuenta
156
Graba nueva clave de inicio de sesión
150
El usuario introduce las preguntas de seguridad a medida
NO
148
Preguntas de usuario activadas ?
SÍ
SÍ
146
Se requieren preguntas de usuario ?
NO

Figura 6