(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 701 613**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.06.2013 E 13382237 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 2819370**

(54) Título: **Un método implementado por ordenador para evitar ataques contra la autenticación de usuario y productos de programas informáticos del mismo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2019

(73) Titular/es:

TELEFÓNICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Via 28
28013 Madrid, ES

(72) Inventor/es:

ALONSO CEBRIÁN, JOSÉ MARÍA;
BARROSO BERRUETA, DAVID;
PALAZÓN ROMERO, JOSÉ MARÍA y
GUZMÁN SACRISTÁN, ANTONIO

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Un método implementado por ordenador para evitar ataques contra la autenticación de usuario y productos de programas informáticos del mismo

Campo de la técnica

La presente invención se refiere, en general, a sistemas de autenticación y más particularmente a un método implementado por ordenador y a productos de programas informáticos para evitar ataques contra la autenticación de usuario que mejoran la seguridad general de un sistema de autenticación, minimizando el impacto en la facilidad de uso y la capacidad de despliegue de estos sistemas.

Antecedentes de la invención

En los últimos años, el mercado de la detección del fraude en web ha aumentado considerablemente, por lo que la innovación en los métodos de autenticación se ha vuelto de gran importancia.

Los sistemas de control de acceso generales proporcionan métodos para la autenticación, autorización y auditoría (o contabilidad). El proceso de autorización es distinto del de autenticación. Mientras que la autenticación es el proceso de verificar que "eres quien dices ser", la autorización es el proceso de verificar que "se te permite hacer lo que estás tratando de hacer". La autenticación y la autorización se combinan a menudo en una sola operación, por lo que el acceso se concede basándose en una autenticación satisfactoria. Los autenticadores se basan comúnmente en al menos uno de los siguientes cuatro factores: algo que sabes, algo que tienes, algo que eres y donde estás.

La arquitectura de seguridad vulnerable en muchas aplicaciones informáticas conduce al problema común de ataques de piratería informática de autenticación. Los ataques de autenticación se dirigen y tratan de aprovechar el proceso de autenticación que un sistema basado en ordenador usa para verificar la identidad de un usuario, servicio o aplicación. La Fundación para el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) ha publicado una amplia lista de amenazas a los métodos de autenticación que muestran una serie de trucos, técnicas y tecnologías que existen para robar contraseñas, atacar sistemas de contraseñas y eludir la seguridad de autenticación. De acuerdo con Burr, W. E. et al. [1] esta lista de amenazas del proceso de autenticación puede estructurarse en las siguientes categorías:

Tabla 1: Categorías de ataques sobre el proceso de autenticación (NIST)

Adivinación en línea	Un atacante realiza repetidas pruebas de inicio de sesión adivinando los posibles valores del autenticador de testigos.
Suplantación de identidad	Se seduce a un usuario para interactuar con un verificador falso y se le engaña para que revele su testigo secreto, datos personales sensibles o valores de autenticador que pueden usarse para enmascararse como el abonado frente al verificador.
Redireccionamiento malicioso	Un usuario que está intentando conectarse a un verificador legítimo, se le encamina a la página web de un atacante a través de la manipulación del servicio de nombres de dominio o las tablas de encaminamiento.
Escuchas informática	Un atacante escucha de forma pasiva el protocolo de autenticación para capturar la información que puede usarse en un ataque activo posterior para enmascararse como el usuario.
Reproducción	Un atacante es capaz de reproducir mensajes capturados previamente (entre un usuario legítimo y un verificador) para autenticarse como ese usuario frente al verificador.
Secuestro de sesión	Un atacante es capaz de insertarse a sí mismo entre un usuario y un verificador después de un intercambio de autenticación satisfactorio entre las dos últimas partes. El atacante puede hacerse pasar por un usuario frente al verificador/RP o viceversa para controlar el intercambio de datos de la sesión.
Hombre en el Medio (MitM)	El atacante se posiciona entre el usuario y el verificador de forma que pueda interceptar y alterar el contenido de los mensajes del protocolo de autenticación. El atacante suplanta, normalmente, al verificador para frente al usuario y suplanta al mismo tiempo al usuario frente al verificador. Llevar al mismo tiempo un intercambio activo con ambas partes puede permitir que el atacante use los mensajes de autenticación enviados por una parte legítima para autenticar satisfactoriamente a la otra.
Denegación de servicio	El atacante abruma al verificador inundándole con una gran cantidad de tráfico a través del protocolo de autenticación.
Código malicioso	El atacante podría comprometer o, de otra manera, explotar testigos de autenticación y podría interceptar todas las comunicaciones de entrada y salida del dispositivo (Hombre en el Dispositivo) (MitD) u Hombre en el Navegador) (MitB)).

Es posible implementar una variedad de contramedidas para los ataques de autenticación descritos anteriormente.

Esta invención propone un nuevo enfoque contra algunos ataques de autenticación que es una autenticación agnóstica, completamente independiente de cualquier procedimiento de autenticación.

Existen alternativas distintas para fortalecer los esquemas de autenticación existentes. La seguridad en el intercambio de información se implementa, en general, con SSL/TLS o EVC/SSL. Pero la forma en que se selecciona esta información para asociarse a una identidad de usuario puede ser muy diferente para esquemas de autenticación diferentes. Por lo tanto, es fundamental realizar un estudio en profundidad de tales esquemas para revelar sus deficiencias. Puede afirmarse que en la actualidad en la mayoría de los sistemas predominan los esquemas basados en dos factores.

Por ejemplo, Bonneau J. et. al. [2] propone la siguiente definición de las categorías de procedimientos de autenticación:

- Esquema tradicional. En este esquema de seguridad se depende del usuario. El usuario debe crear una contraseña sólida y asegurarse de que no se comprometa fácilmente.
- Basado en intermediario. Los esquemas basados en intermediario se basan en la definición de un servicio entre el cliente y el servidor (hombre en el medio), que gestiona el proceso de autenticación usando una contraseña de un solo uso.
- Inscripción única federada. Permiten sitios web para delegar la identificación de sus usuarios a un servidor de identidad de confianza que gestiona todo el proceso de autenticación.
- Gráfica. Estos esquemas buscan explotar la capacidad humana de reconocer imágenes para eliminar la necesidad de una contraseña.
- Cognitiva. Estos esquemas se basan en el desafío/respuesta. El usuario debe demostrar su conocimiento de un secreto sin tener que revelarlo. Normalmente, el servidor espera que un usuario sea capaz de realizar un resumen criptográfico del secreto junto con un número aleatorio generado por el servidor.
- Testigo de papel. Se utiliza un almacenamiento físico (papel) de un conjunto de contraseñas indexadas. El esquema de autenticación supone que el servidor pide al usuario la clave correspondiente a un índice específico.
- Criptografía visual. Bastante similar al testigo de papel, pero con un sistema de almacenamiento de claves complejas que potencia las características de la pantalla usada por el cliente y la forma en que los humanos perciben los colores.
- Testigos de hardware. Los secretos se almacenan en un módulo de hardware que los usuarios deben mantener con ellos. Se basan en los mismos principios que los esquemas cognitivos, pero la respuesta al desafío que envía el servidor se proporciona mediante el testigo de hardware del usuario.
- Basado en un teléfono. Es un esquema basado en un testigo, pero en lugar de utilizar un hardware específico para el almacenamiento y cálculo de la clave, se usa el teléfono como almacenamiento de claves y el procesador del teléfono como sustituto del hardware criptográfico específico.
- Biométrico. Estos esquemas evitan el uso de la contraseña, basando la autenticación del usuario en algo que los define, no algo que se tiene o algo que se sabe.
- Recuperación. Estos esquemas son complementarios de cualquier esquema de autenticación basado en contraseñas. Y permiten la recuperación más fácil de la información necesaria para la autenticación en caso de pérdida.

Es digno de tenerse en cuenta que algunos de los esquemas de autenticación no pertenecen a una sola categoría y que la mayoría de las instituciones usan al menos dos o más de estos esquemas, como es el caso en el producto autenticador de Google (un sistema de autenticación de segundo factor basado en una aplicación móvil o mensajería SMS).

Se pueden definir criterios diferentes para establecer una comparación entre los esquemas de autenticación. En [2], los autores sugieren la necesidad de definir tres criterios para realizar una comparación eficaz. Estos aspectos son: seguridad, facilidad de uso y complejidad en la implementación (capacidad de despliegue). [2] presenta un estudio intensivo para instrumentar la comparación a través de la definición de métricas. La Tabla 2 resume las métricas definidas para cada criterio.

Tabla 2: Métricas de diseño para esquemas de autenticación

Facilidad de uso	Sin esfuerzo de memoria Escalable para usuarios Nada que llevar Sin esfuerzo físico Fácil de aprender Eficiente de usar Errores poco frecuentes Fácil recuperación de pérdida

Capacidad de despliegue	Accesible Insignificante coste por usuario Compatible con servidor Compatible con explorador Maduro No propietario Resistente a la observación física Resistente a la suplantación dirigida
Seguridad	Resistente a la adivinación estrangulada Resistente a la adivinación no estrangulada Resistente a la observación Interna Resistente a fugas de otros Verificadores Resistente a suplantación de identidad Resistente al robo Sin tercera parte confiable Requiere consentimiento explícito No enlazable

En el caso del criterio de seguridad, el conjunto de métricas propuesto resume todos los aspectos que se estiman normalmente en la definición de un modelo de amenaza. En la definición de estos modelos es necesario adoptar una serie de decisiones, definiendo estas decisiones el escenario de trabajo. Por ejemplo, en el caso de OAuth 2.0 [3] las suposiciones adoptadas son las siguientes:

- El atacante tiene acceso total a la red entre el cliente y los servidores de autorización y el cliente y el servidor de recursos, respectivamente. El atacante puede escuchar a escondidas cualquier comunicación entre esas partes. No se supone que tiene acceso a la comunicación entre el servidor de autorización y el servidor de recursos.
- Un atacante tiene recursos ilimitados para organizar un ataque.
- Dos de las tres partes implicadas en el protocolo OAuth pueden conspirar para montar un ataque contra el tercero. Por ejemplo, el cliente y el servidor de autorización podrían estar bajo el control de un atacante y conspirar para engañar a un usuario para obtener acceso a los recursos.

Por otra parte, las contraseñas tienen una alta aceptación de los clientes, se basan en un secreto compartido y hay que tener una diferente para cada proveedor de servicios. El problema es que las contraseñas se confían a la memoria del usuario y el cumplimiento de las buenas prácticas de contraseña. Sin embargo, la evidencia anecdótica muestra que una proporción significativa de clientes no seguirá las buenas prácticas de contraseña y los ataques normalmente trabajan obteniendo la contraseña. Esta es una brecha grave de seguridad ya que el atacante es capaz de operar como el cliente hasta que se descubre la brecha.

Los testigos de hardware se consideran, en general, para soportar una seguridad más fuerte, pero todavía son susceptibles a los ataques de códigos maliciosos que pueden incitar al testigo para una petición de autenticación. Las personas con información privilegiada autorizadas podrían abusar también de sus privilegios y ser capaces de obtener las claves criptográficas almacenadas. Los testigos de software tienen costes más bajos que los testigos de hardware, pero la desventaja es que son viables los ataques de copia.

Todos los sistemas de contraseña de un solo uso necesitan usarse junto con las protecciones del canal de comunicación. Como no se soporta la autenticación mutua, son posibles los ataques de suplantación del verificador. Esto significa que existe una cierta exposición a los ataques de suplantación de identidad, aunque el potencial de éxito con tales ataques está mucho más limitado que con los sistemas de contraseña. La exposición a los ataques de copia depende del producto.

Cuando se usan protecciones del canal de comunicación, incluso los esquemas de autenticación basados en biométrica siguen siendo susceptibles a ataques que copian los datos biométricos. Tales ataques pueden llegar a ser más populares si la biometría se usa más ampliamente. Debido a que los datos biométricos son datos personales, la privacidad es un problema con respecto al almacenamiento, uso y transferencia de datos biométricos.

En [1] se definen cuatro niveles diferentes en términos de las consecuencias de los errores de autenticación y el mal uso de las credenciales. El nivel 1 es el nivel más bajo (el más inseguro) y el nivel 4 es el más alto. A partir de la Tabla 1, puede hacerse la siguiente correspondencia.

- Nivel 1 - Protección contra la adivinación en línea y ataques de reproducción. NIST recomienda utilizar una autenticación única o de múltiples factores sin prueba de identidad.
- Nivel 2 - Protección contra escuchas informáticas y todos los ataques del nivel 1. NIST recomienda una autenticación única o de múltiples factores.
- Nivel 3 - Protección contra la suplantación del verificador, ataques MitM y ataques del nivel 2. NIST recomienda

una autenticación de múltiples factores y un amplio uso de OTP. También sugiere un testigo usado para la autenticación para desbloquearse por el usuario usando una contraseña o biométrica.

- Nivel 4 - Protección contra el secuestro de sesión y los ataques del nivel 3. NIST sugiere emplear la autenticación de múltiples factores con el hardware resistente a la manipulación certificado por FIPS-140-2 (testigos de hardware).

Atendiendo a las métricas presentadas anteriormente, es posible determinar que soluciones que corresponden al nivel de seguridad más alto (nivel 4) tienen bajo rendimiento en la capacidad de despliegue y en la facilidad de uso. Una vez que la evaluación de un sistema permite determinar en qué nivel tiene que desplegarse su sistema de autenticación, se necesita evaluar si los usuarios se autentican de manera segura y correcta. Aunque existen algunas herramientas que ayudan en esta tarea, como las presentadas por Dalton, M. et. al. [3] o por Sun, F. et. al. [4], los despliegues en el nivel 4 son difíciles de evaluar correctamente. En términos de facilidad de uso, el uso de testigos de hardware resistentes a la manipulación va en contra de la adopción de estas soluciones por los usuarios, y se ha demostrado que esta situación conduce a una mala utilización de los sistemas de credenciales. Se necesita un enfoque diferente que mejore la seguridad general en los sistemas de autenticación, cualquiera que sea el esquema o esquemas (múltiples factores) adoptados, que minimice el impacto en la facilidad de uso y en la capacidad de despliegue de estos sistemas.

La petición de patente internacional WO 02/095554 A2 se refiere a autenticación usando biométrica. En esta solicitud de patente internacional, se asocia un alías para un individuo con un conjunto de referencia de datos biométricos del individuo y, en una ubicación separada del conjunto de referencia de datos biométricos, se almacena información que asocial al individuo con el alias. Esta invención puede operar con una petición de autenticación que solicita autenticación de un usuario identificado mediante el alias, junto con un conjunto candidato de datos biométricos del usuario y confirmar la autenticación del usuario como el individuo registrado; la autenticación se concede si el conjunto candidato de datos biométricos coindice suficientemente con el conjunto de referencia de biométricos.

La solicitud de patente de Estados Unidos US 2006/130140 A1 divulga un sistema y método para proteger un servidor contra ataques de denegación de servicio proporcionando un servidor de autenticación de intermediario que tiene una tabla de historial de peticiones de autenticación; manteniendo en la tabla peticiones de autenticación recientes a un segundo servidor, incluyendo ID de usuario y momento de cada petición de autenticación reciente; recibiendo una petición de autenticación posterior en el servidor de autenticación de intermediario; y determinando si reenviar la petición de autenticación posterior al segundo servidor basándose en una regla o reglas de filtrado predefinidas y el ID de usuario y momento de petición de autenticación en la tabla de historial de petición de autenticación.

Referencias

[1] Burr, WE, Dodson, DF, y Polk, WT (2006). Electronic authentication guideline. NIST Special Publication, 800, 63.

[2] Bonneau, J., Herley, C., van Oorschot, PC, y Stajano, F. (Mayo 2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), Simposio IEEE 2012 en (páginas 553-567). IEEE.

[3] Michael Dalton, Christos Kozyrakis y Nickolai Zeldovich, Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Application, en las Actas de la 18ª Conferencia en el simposio de seguridad USENIX, (páginas 267-282) Asociación USENIX.

[4] Sun F., Xu, L., y SU, Z. (Agosto 2011) Static detection of Access control vulnerability in web applications. En las actas de la 20ª conferencia USENIX en Seguridad (páginas 11-11). USENIX.

Descripción de la invención

Para lograr lo anterior, la invención proporciona una solución diseñada para limitar el tiempo de exposición en el que puede hacerse un ataque de autenticación en nombre de un usuario. Por lo tanto, suponiendo un límite de los recursos disponibles para realizar dicho ataque, que ahora, al menos en términos de tiempo, puede considerarse no infinito.

Para tal fin, la invención proporciona en un primer aspecto, un método implementado por ordenador para evitar los ataques contra la autenticación de usuario, que comprende recibir, un primer servidor, una petición en nombre de un usuario para iniciar sesión en un servicio de dicho primer servidor, y autenticar dicha petición, dicho primer servidor, verificando la información de identificación de usuario de dicho usuario.

El método implementado por ordenador del primer aspecto comprende, al contrario de las propuestas conocidas, y de una manera característica, usar un segundo servidor en conexión con un dispositivo informático de usuario con un programa especializado que comprende: recibir desde dicho primer servidor una petición acerca de un estado

asociado a dicho usuario, es decir, a la cuenta de usuario con el primer servidor; inicializar un intercambio de credenciales entre dichos primer y segundo servidores para proporcionar autenticación mutua; verificar dicho estado asociado que se ha establecido previamente como válido o como no válido por dicho usuario y almacenado en una memoria de dicho segundo servidor; y enviar dicho estado asociado a dicho primer servidor. Además, el método implementado por ordenador usa dicho primer servidor para: registrar dicha petición en nombre de dicho usuario si dicho estado asociado se establece como válido o rechazar dicho registro si dicho estado asociado se establece como no válido.

El estado asociado establecido como válido o como no válido puede modificarse por dicho usuario cuando este lo requiera. Por ejemplo, el usuario puede planificar una política de bloqueo/desbloqueo para automatizar la gestión de sus cuentas mantenidas en diferentes servidores usando diferentes criterios: momento, geolocalización (diferentes políticas para el hogar, el trabajo, etc.). Otra posibilidad para modificar dicho estado asociado puede ser delegando el control que dicho usuario tiene de sus cuentas a otros usuarios. Esto puede hacerse considerando dos opciones diferentes. En la primera, se usa un mecanismo de control parental de forma que se delega el control de acceso (original) de las cuentas de los niños a dicho mecanismo de control parental. En el segundo, una sola cuenta permite múltiples bloqueos. En este último caso, la acción de desbloqueo requerirá que múltiples usuarios desbloqueen sus bloqueos simultáneamente. En ambos casos, la delegación se realiza manteniendo sin cambios de forma segura la privacidad de cada usuario.

La petición del estado asociado a dicho usuario comprende el envío de un testigo de seguridad, generándose dicho testigo de seguridad durante el proceso de emparejamiento de las cuentas de usuario previo. Este testigo vincula al usuario con dicho primer servidor sin la divulgación de ninguna información personal de dicho usuario a dicho segundo servidor de información. A continuación, el testigo se almacena de forma segura en una memoria de dicho primer servidor y en una memoria de dicho segundo servidor una vez que el usuario ha configurado el emparejamiento de dichas identificaciones de los servidores primero y segundo.

El intercambio de credenciales para garantizar la autenticación mutua entre el primer servidor y el segundo servidor se realiza, preferentemente, a través de un procedimiento de autenticación convencional basándose en los intercambios de los certificados que definen, como consecuencia, un canal seguro. Como se dijo anteriormente, dicho intercambio se realiza para verificar que tanto el primer servidor como el segundo servidor son quienes dicen ser.

Además, en una realización preferida, la etapa de envío de dicho estado asociado a dicho primer servidor puede incluir el envío de un identificador único para dicho usuario, por ejemplo, el envío de una contraseña de un solo uso (OTP), de modo que puede activarse un segundo factor de autenticación para dicho primer servidor o varios servidores que no proporcionan esta opción en sus procesos de inicio de sesión.

La petición recibida puede grabarse para proporcionar estadísticas a través de dicho dispositivo informático de usuario. De esta manera, el usuario puede obtener estadísticas de uso del sistema que reflejan la actividad del sistema y rastrear los intentos de suplantación. Estas estadísticas informan sobre cuándo alguien ha intentado acceder a un servicio con el nombre de usuario del usuario.

El segundo servidor puede notificar a dicho usuario, en otra realización, si se ha producido dicho registro de rechazo. Por ejemplo, mediante el envío de un servicio de mensajes cortos (SMS), de un correo electrónico, de o un mensaje mediante una aplicación de mensajería de un teléfono inteligente, o simplemente por el resaltado o proposición en un programa especializado de dicho dispositivo informático de usuario.

La invención proporciona en un segundo aspecto, un producto de programa informático que puede cargarse en un segundo servidor para evitar ataques contra la autenticación de usuario, comprendiendo varios módulos de software que se ejecutan en dicho segundo servidor para ejecutar las etapas de: recepción desde un primer servidor de una petición acerca de un estado asociado a dicho usuario; inicialización de un intercambio de credenciales entre dichos primer y segundo servidor para proporcionar una autenticación mutua; verificación de dicho estado asociado, estando dicho estado asociado establecido previamente como válido o como no válido por un usuario desde un programa especializado de un dispositivo informático de usuario, tal como un teléfono móvil, un teléfono inteligente, un PC de tableta o un PDA entre cualquier otro dispositivo informático de características similares, en comunicación con dicho segundo servidor y estando almacenado en uno de dichos varios módulos de software; y envío de dicho estado asociado a dicho primer servidor.

El producto de programa informático puede incluir, en una realización preferida, un módulo de software de autenticación de segundo factor para enviar un identificador único a dicho segundo servidor y a dicho primer servidor.

La presente invención no propone ningún nuevo esquema de autenticación. De hecho, la intención es complementar los esquemas mostrados anteriormente para aumentar su seguridad. Aunque esto puede limitar su facilidad de uso y

la capacidad de despliegue, el segundo diseño del servidor está orientado para reducir al mínimo el impacto sobre estos criterios. La elección del esquema de autenticación determina el riesgo de seguridad que se asume para un sistema. Lo que se propone en este documento es reducir el riesgo tomado con la elección del mecanismo de autenticación reduciendo el tiempo en el que este sistema es accesible para que pueda romperse.

En la Tabla 1 se ha presentado una clasificación completa de ataques de autenticación. Las cinco primeras categorías incluyen ataques que tienen la intención de capturar una contraseña de usuario para realizar un ataque posterior. La adivinación en línea incluso requiere un acceso constante al proceso de autenticación. En los siguientes cuatro ataques, una vez que se captura y se rompe la contraseña, el atacante tiene que solicitar el proceso de autenticación, haciéndose pasar por el usuario legítimo. Este proceso consume mucho tiempo y supone que el atacante interactúa directamente con el sistema de autenticación. Esto significa que la invención propuesta optimiza el proceso de autenticación, independientemente del esquema de autenticación elegido. Además, con dicho segundo factor de autenticación, la invención otorga protección contra la suplantación y los ataques MitM, incluso a los servicios que se han implementado únicamente con protección contra ataques de adivinación en línea, escucha informática o reproducción. Y esto se hace sin aumentar la complejidad de la implementación de los sistemas de autenticación y sin un deterioro significativo de la facilidad de uso de la solución. Por lo tanto, esta solución permite homogeneizar los niveles de seguridad de las diferentes cuentas de un usuario.

Es posible establecer ciertas comparaciones con las soluciones de autenticación basadas en un intermediario, con soluciones de inscripción única federada o, incluso, con soluciones basadas en un teléfono. Sin embargo, en ningún caso la presente invención reemplaza a ningún servidor de autenticación. Con esta solución, cualquier esquema de autenticación se reforzaría reduciendo el tiempo de exposición y, si es necesario, se ampliaría su funcionalidad permitiendo un segundo factor de autenticación, si así lo solicita el usuario.

Es cierto que hay una cierta similitud con las soluciones móviles que se proporcionan como una alternativa al uso de los testigos de hardware. Sin embargo, la necesidad de tener el teléfono o dispositivo informático a mano en todos los procesos de autenticación se atenúa en la presente invención. Una vez que el usuario ha desbloqueado el proceso de inicio de sesión en diferentes servidores éstos permanecerán desbloqueados hasta que el usuario los vuelva a bloquear. Una vez que el usuario configura un período de tiempo en que el servicio debe estar bloqueado, el usuario podría acceder a su cuenta siempre que lo haga fuera de este período. No será necesario que el usuario tenga el teléfono a mano para completar el inicio de sesión en el sistema a menos que sus roles exijan un segundo factor de autenticación.

Los recursos de los sistemas de control de acceso son otra comparación que se puede establecer. Estos sistemas actúan normalmente como un "gestor de autorización" que permite a los usuarios coordinar la protección de los recursos que posee el usuario definiendo las políticas asociadas con cada recurso. De esta manera, el usuario controla cómo hacer la compartición de estos recursos con terceros. En el caso particular de la UMA se propone un esquema que facilita la centralización de estas políticas. La UMA también facilita la integración con OpenID y OAuth, compartiendo una serie de procesos básicos y complementa las funciones disponibles de los usuarios para la delegación de la autenticación y la autorización. Una de estas funciones básicas es la autorización desde una identidad autenticada. Es decir, es necesario establecer previamente mecanismos de autorización para autentificar a los usuarios. La presente invención surge, en este punto, como una solución que complementa el proceso de autenticación antes de la autorización. Reduce el riesgo de robo de identidad y se propone como una capa que soporta estos sistemas de autenticación.

Breve descripción de los dibujos

Las anteriores y otras ventajas y características se comprenderán más plenamente a partir de la siguiente descripción detallada de las realizaciones, con referencia a las adjuntas, que deben considerarse de una manera ilustrativa y no limitante, en los que:

La Figura 1 es una ilustración de la arquitectura general de la presente invención.
La Figura 2 es una ilustración del esquema general del mecanismo de bloqueo de la presente invención, de acuerdo con una realización.
La Figura 3 es una realización de cómo funciona la presente invención para realizar un emparejamiento de una cuenta.

Descripción detallada de varias realizaciones

En referencia a la Figura 1 se muestra la arquitectura general de la presente invención. Con respecto a la Figura 1, un dispositivo informático 100 de usuario tal como un teléfono móvil, un teléfono inteligente, un PC de tableta o un PDA entre cualquier otro, se usa por dicho usuario para iniciar sesión en un programa especializado 101 en comunicación con un segundo servidor 200 y para gestionar el estado de cada primer servidor 300 con los que un usuario desea solicitar un servicio.

De acuerdo con algunas realizaciones, el usuario, por medio de dicho dispositivo informático 100 de usuario, puede configurar las cuentas que tiene con varios servidores 300 con opciones diferentes. Por ejemplo, el usuario puede fijar una planificación para bloquear/desbloquear cada cuenta. Es posible planificar que será el estado del servicio para cada día y cada hora en una semana o para períodos de tiempo en un año. Además, el usuario puede mejorar también el nivel de seguridad de un servicio; no sólo reduciendo el tiempo de exposición, sino configurando un segundo factor de autenticación o incluso puede delegar el control de sus cuentas a otros usuarios usando dicho programa especializado 101. Esta delegación se realiza de manera segura y manteniendo la privacidad de cada usuario sin cambios. Únicamente se necesita un ID de identificación. Por último, el usuario puede obtener las estadísticas de cada cuenta de uso del sistema que reflejan la actividad del sistema y rastrear los intentos de suplantación.

Una interfaz de usuario define un interfaz 201 entre los usuarios y el segundo servidor 200. También define y controla el intercambio de credenciales entre los usuarios y el segundo servidor 200 para construir un canal seguro. Una vez que se define este canal, esta interfaz 201 concede la capacidad de crear nuevos bloqueos en el segundo servidor 200. A través de esta interfaz 201 es posible recuperar la configuración de la cuenta de usuario desde el segundo servidor 200. Permite que el usuario pueda modificar esta configuración y pueda obtener las estadísticas de sus cuentas. También facilita la gestión de un identificador único (tal como, una OTP) para construir dicha autenticación basada en segundo factor.

Un gestor 202 de cuentas de usuario almacena los datos de la cuenta de usuario e implementa el mecanismo de autenticación para identificar y validar al usuario. El mecanismo básico propone un nombre de usuario y/o un esquema de contraseña, pero la invención está diseñada para integrar múltiples factores de autenticación como la geolocalización, perfiles de preferencias de usuario, biometría, etc.

Un primer gestor 205 de servicios de servidor almacena la información acerca de la comunicación con dicho primer servidor o varios servidores 300. Gestiona los certificados usados para conceder un intercambio seguro entre el segundo servidor 200 y el primer servidor o varios servidores 300. Se han implementado varias maneras de obtener estos certificados, por ejemplo, el segundo servidor 200 puede generar un certificado válido para un primer servidor 300 o el primer servidor 300 puede aportar un certificado público que el segundo servidor 200 podría validar.

Un módulo 203 de autenticación de segundo factor, en el caso de que el usuario haya configurado un bloqueo con un segundo de autenticación, de acuerdo con una realización preferida, incorporará toda la lógica necesaria para la generación y la emisión de una OTP-por-Proposición, una OTP-por-SMS o una OTP-por-mail. Cuando el segundo servidor 200 recibe una petición desde el primer servidor 300 preguntando por el estado de la cuenta de usuario, se desencadena un segundo factor de autenticación. Por ejemplo, se genera y se envía una OTP al usuario. La misma OTP se envía al primer servidor 300 junto con el estado de la cuenta. Si el estado está ACTIVO y el usuario ha activado el segundo factor, el primer servidor 300 espera a que el usuario introduzca la OTP para proceder con el inicio de sesión. Este módulo 203 permite elevar el nivel de seguridad de una organización a un nivel 3 de acuerdo con [1] como se ha indicado anteriormente.

Un núcleo bloqueador de cuenta 204 implementa la función principal del segundo servidor 200, es decir, bloquear o desbloquear una cuenta de usuario con un primer servidor 300. Para hacer esto, este módulo 204 acepta y procesa las peticiones de estado enviadas desde el primer servidor 300. Este módulo 204 también gestiona todos los datos acerca de las cuentas con dichos otros varios servidores 300 definidas por los usuarios y las peticiones de emparejamiento de nuevos bloqueos. La clave es que al usuario no se le pide ninguna información privada. Una vez que el usuario crea su cuenta con dicho programa especializado 101, el usuario puede establecer bloqueos con varios servidores 300 diferentes.

Para activar estos bloqueos, el segundo servidor 200 puede generar un testigo. Este testigo y la definición de canales seguros se usan en el proceso de emparejamiento entre el usuario y el primer servidor 300. Como resultado de este proceso de emparejamiento, un testigo, que puede encriptarse con fines de protección, se envía al primer servidor 300 quien tiene que almacenar esta información con los datos personales de sus usuarios. Más tarde, este testigo se usará para solicitar el estado de bloqueo correspondiente.

Una primera interfaz de servidor define una interfaz 206 entre el segundo servidor 200 y el primer servidor o varios servidores 300. Define y controla el intercambio de credenciales entre el segundo servidor 200 y dichos servidores 300 para construir un canal seguro. Una vez que se define este canal, esta interfaz 206 concede la capacidad de crear nuevos bloqueos. Define un canal para recibir y enviar la información relativa al estado de los bloqueos. También define la forma en que un primer servidor 300 puede enviar cualquier información adicional para mejorar las estadísticas ofrecidas a los usuarios (geolocalización desde donde se ha hecho el intento de inicio de sesión, IP desde donde se ha hecho el intento de inicio de sesión, si el usuario tenía la contraseña correcta, etc.).

En referencia ahora a la Figura 2, un usuario solicita, de acuerdo con una realización, iniciar sesión en un servicio

(A) de un primer servidor 300 así que una vez que se ha validado (B) la existencia del usuario por dicho primer servidor 300, este último exige al segundo servidor 200 los estados (C) de la cuenta de usuario. A continuación, el segundo servidor 200 inicia el intercambio de credenciales (D y E) antes de enviar la información del estado de la cuenta (F). Con el estado el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario (G).

Cuando un primer servidor 300 envía una petición de estado, el segundo servidor 200 entiende que alguien, con la información de identificación de servicio apropiada (por ejemplo, ID y contraseña), está tratando de acceder al servicio. Si el estado de la cuenta se establece como bloqueado, o si esta petición ha llegado en un momento en que no está incluido en el intervalo definido por el usuario, el segundo servidor 200 registra este evento como un intento falso. El segundo servidor 200 podría enviar una alerta de este evento al usuario si dicho usuario lo ha configurado de este modo (por ejemplo, enviando un servicio de mensajes cortos (SMS), un correo electrónico, un mensaje de una aplicación de mensajería de teléfono inteligente, mediante un resaltado o proposición en dicho programa 101 especializado de dicho dispositivo informático 100 de usuario, etc.) o simplemente actualizar las estadísticas para una revisión posterior. A continuación, el segundo servidor 200 devuelve el estado asociado con la cuenta como bloqueada.

Como una realización ejemplar para ilustrar el uso de esta invención, se considera un usuario que había bloqueado el uso de su tarjeta de crédito. Este usuario había configurado también, por medio de dicho programa o de la aplicación del dispositivo informático, recibir todas las alertas de intento de inicio de sesión fallido como un SMS en su dispositivo informático (es decir, un teléfono móvil). Por otro lado, una vez que el segundo servidor, o también llamado bloqueador de cuenta, notifica al primer servidor o al proveedor del servicio (en este caso el que emitió la tarjeta de crédito) que el usuario legítimo de la cuenta había bloqueado el servicio, puede a su vez empezar con acciones inmediatas para preservar sus activos contra los intentos de fraude (mediante límites de crédito, supervisión de este servicio, etc.).

En otra realización, en referencia a la Figura 3 se muestra el proceso de emparejamiento de la cuenta de usuario del segundo servidor 200 con las diferentes cuentas de los diferentes primeros servidores 300. En la Figura 3, una vez que un usuario, usando, por ejemplo, un navegador 100, ha completado el proceso de inicio de sesión (A-B) con un primer servidor (en este caso específico, un banco en línea, una red social, un proveedor de tarjetas de crédito, etc.), el usuario decide realizar dicho proceso de emparejamiento de las cuentas. El usuario solicita el emparejamiento con el primer servidor 300 (C). Como respuesta, el primer servidor 300 pide un testigo de emparejamiento (D). A continuación, el usuario usa el programa especializado 101 (D') para obtener este testigo de emparejamiento del segundo servidor 200 (E), después de un proceso de inicio de sesión anterior. El segundo servidor 200 genera un testigo (por ejemplo, una OTP) y lo envía al programa especializado 101 (F) del usuario. Este testigo puede usarse para varios procesos de emparejamiento, mientras sea válido. El usuario obtiene el testigo (OTP) del programa especializado 101 y lo introduce en la página web que se muestra en el navegador 100 mediante el primer servidor 300 (G-G'). A continuación, el primer servidor 300 envía el testigo recibido al segundo servidor 200, después de un intercambio (H) de credenciales previo. Si se valida la identidad del primer servidor 300, el segundo servidor 200 almacena el enlace entre el usuario y el primer servidor 300 y genera un nuevo testigo que identifica este enlace. Este testigo (usuario/primer servidor) se envía al primer servidor y allí se almacena para comunicaciones (I) futuras. Finalmente, se envían unos acuses de recibo emparejados al navegador 100 (J) del usuario.

La presente invención, sería útil también para autorizar operaciones tales como transacciones para un pago electrónico, entre muchos otros ejemplos. En este caso particular, el método y el sistema propuestos se ampliarían. Por ejemplo, el primer servidor 300 en vez de recibir una petición en nombre de un usuario para iniciar sesión en un primer servicio de un servidor, recibirá una petición para realizar una operación en el mismo, en el que dicha petición será autorizada por el primer servidor 300. A continuación, después de que el segundo servidor 200 ejecute sus tareas comunes (es decir, el inicio de intercambio de credenciales, la verificación del estado asociado, etc.), como se han ejecutado en las realizaciones anteriores, el primer servidor 300 podría autorizar dicha petición o rechazarla, dependiendo del estado asociado proporcionado por el usuario, proporcionando por tanto un mecanismo más seguro para las operaciones de autorización.

El alcance de la presente invención se define en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un método implementado por ordenador para evitar ataques contra la autenticación de usuario, comprendiendo el método:

- recibir, mediante un primer servidor (300), desde un usuario, una petición para iniciar sesión en un servicio de dicho primer servidor (300); incluyendo dicha petición la provisión de información de identificación que valida la identidad del usuario en el primer servidor (300); y
- autenticar mediante dicho primer servidor (300), dicha información de identificación de dicho usuario para autorizar dicha petición de inicio de sesión de servicio,

Caracterizado porque el método comprende

- usar un segundo servidor (200), en conexión con un dispositivo informático (100) del usuario a través de un programa especializado (101) instalado en el dispositivo informático de usuario (100), para gestionar un estado de las cuentas que tiene el usuario en el primer servidor (300),

en el que dicho estado de cuentas se establece como válido o como no válido por el usuario a través del programa especializado (101) y almacena en una memoria del segundo servidor (200), después de que se define un canal seguro entre el segundo servidor (200) y el dispositivo informático (100), y en el que dicho canal seguro se define después de que se hace un intercambio de credenciales entre el segundo servidor (200) y el usuario;

- recibir, mediante el segundo servidor (200), desde dicho primer servidor (300) una petición acerca de un estado con respecto a una cuenta del usuario en el primer servidor (300);
- en respuesta a la recepción de la petición, inicializar, mediante el segundo servidor (200), un intercambio de credenciales con el primer servidor (300) para proporcionar autenticación mutua, realizándose el intercambio de credenciales a través de un procedimiento de autenticación basándose en intercambio de los certificados entre el primer servidor (300) y el segundo servidor (200);
- verificar, mediante el segundo servidor (200), dicho estado de cuenta; y
- enviar, mediante el segundo servidor (200), dicho estado de cuenta al primer servidor (300), usando este el estado de cuenta recibido para autorizar dicha petición de inicio de sesión de servicio si dicho estado de cuenta está establecido como válido o rechazar dicha petición de inicio de sesión de servicio si dicho estado de cuenta está establecido como no válido.

2. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que dicha petición acerca del estado de cuenta comprende el envío de un testigo de seguridad, generándose dicho testigo de seguridad durante un proceso anterior de emparejamiento de las cuentas de usuario.

3. Un método implementado por ordenador de acuerdo con la reivindicación 2, que comprende además almacenar dicho testigo de seguridad generado en dicha memoria y en una memoria de dicho primer servidor (300).

4. Un método implementado por ordenador de acuerdo con la reivindicación 3, en el que dicho testigo de seguridad se envía encriptado a dicho primer servidor (300).

5. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que la etapa de envío de dicho estado de cuenta a dicho primer servidor (300) incluye el envío de un identificador único para dicho usuario.

6. Un método implementado por ordenador de acuerdo con la reivindicación 1, que comprende notificar a dicho usuario si se rechaza dicha petición para iniciar sesión en un servicio de dicho primer servidor (300).

7. Un método implementado por ordenador de acuerdo con la reivindicación 6, en el que dicha notificación comprende uno de un envío de un servicio de mensajes cortos (SMS), un envío de un correo electrónico, un envío de un mensaje mediante una aplicación de mensajería de teléfono inteligente, un resaltado o proposición en dicho programa especializado de dicho dispositivo informático de usuario.

8. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que dicha petición recibida se registra para proporcionar estadísticas a través de dicho dispositivo informático de usuario.

9. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que dicho estado de cuenta establecido como válido o como no válido es modificable.

10. Un método implementado por ordenador de acuerdo con la reivindicación 1, en el que dicho estado de cuenta se establece como válido o como no válido durante un cierto período de tiempo.

11. Un producto de programa informático que comprende instrucciones que, cuando el programa se ejecuta por un ordenador, provocan que el ordenador efectúe las etapas de:

- gestión y almacenamiento de un estado de las cuentas que tiene el usuario en un primer servidor (300), recibiéndose dicho estado desde un programa especializado (101) instalado en un dispositivo informático (100) del usuario y estableciéndose el estado como válido o no válido por el usuario a través del programa especializado (101);
- recepción desde un primer servidor (300) de una petición acerca de un estado con respecto a una cuenta del usuario en el primer servidor (300);
- inicialización de un intercambio de credenciales con el primer servidor (300) para proporcionar autenticación mutua, realizándose el intercambio de credenciales a través de un procedimiento de autenticación basado en intercambio de los certificados entre el primer servidor (300) y el segundo servidor (200);
- verificación de dicho estado de cuenta; y
- envío de dicho estado de cuenta a dicho primer servidor (300), permitiendo de esta forma que el primer servidor (300) use el estado de cuenta recibido para autorizar o rechazar que el usuario inicie sesión en un servicio del primer servidor (300).

12. Un producto de programa informático de acuerdo con la reivindicación 11, que comprende además un módulo (203) de software de autenticación de segundo factor para enviar un identificador único a dicho segundo servidor (200) y a dicho primer servidor (300).

13. Un producto de programa informático de acuerdo con la reivindicación 11, en el que dicho dispositivo informático (100) de usuario es un teléfono móvil, un teléfono inteligente, un PC de tableta o un PDA.

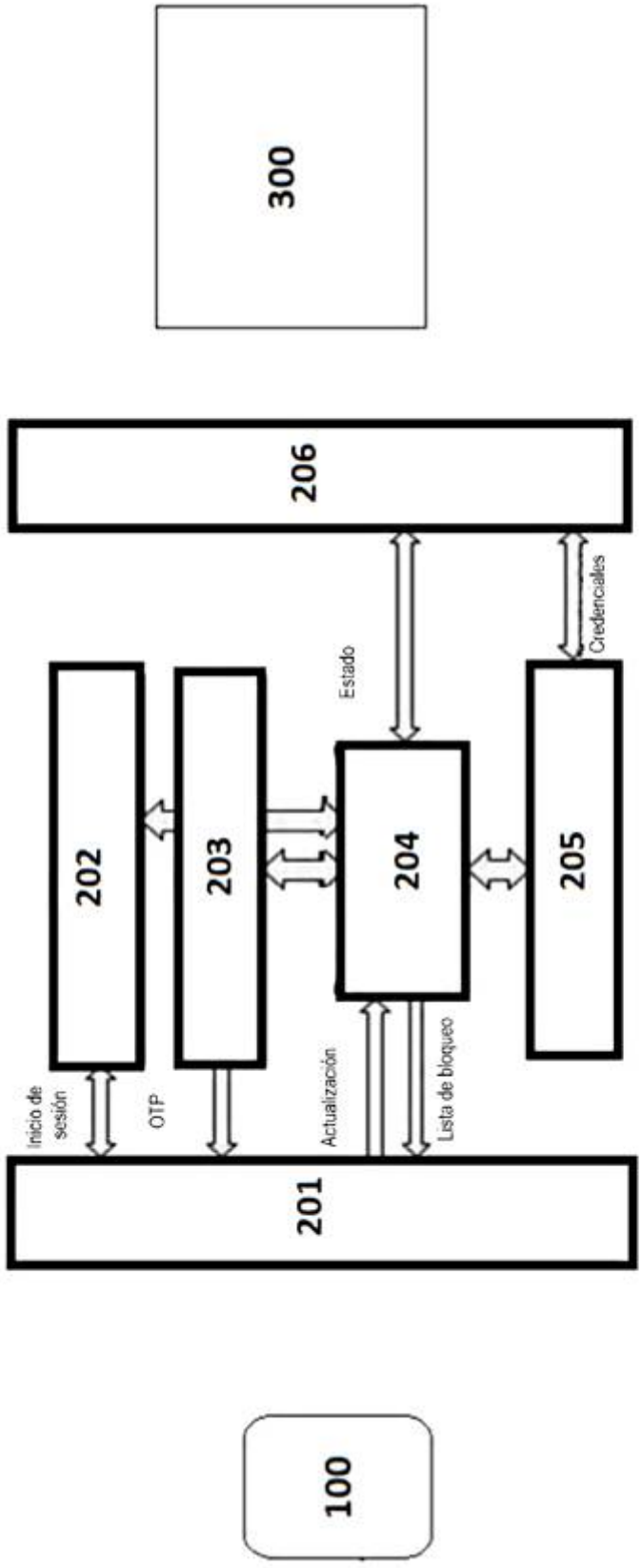
300
206
Credenciales
Estado
202
203
204
205
200
Inicio de sesión
OTP
Actualización
Lista de bloqueo
201
100

Fig. 1

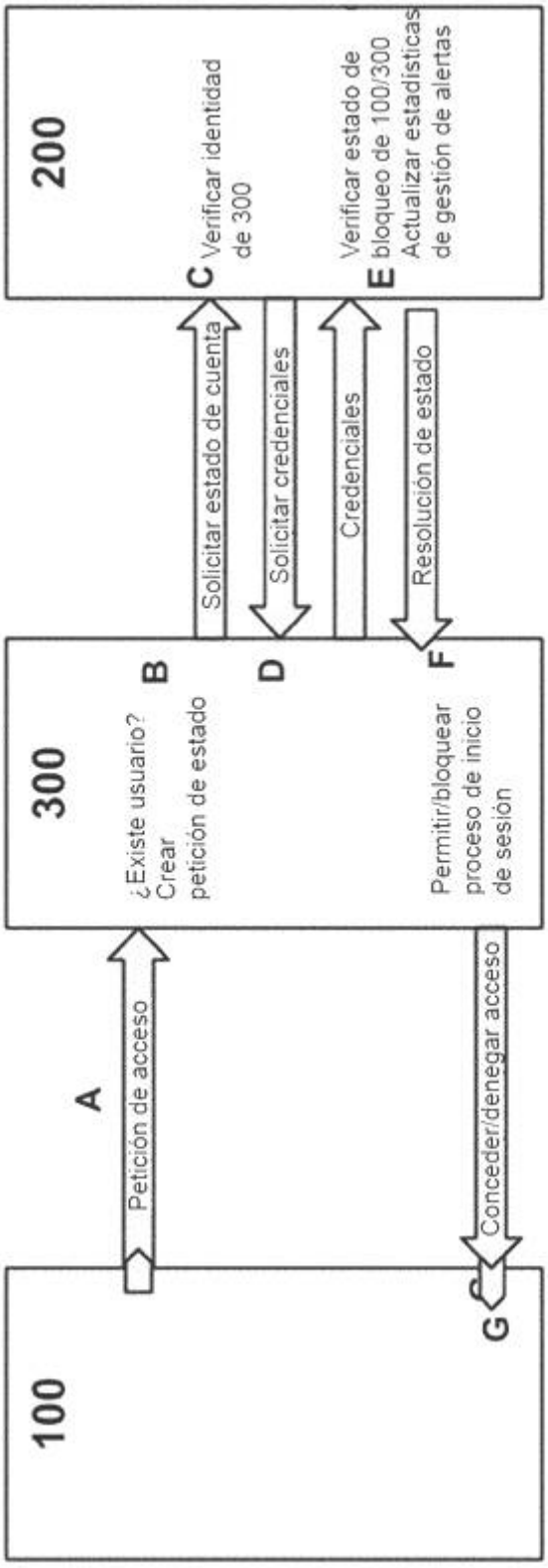
100
200
300
A
Petición de acceso
B
¿Existe usuario?
Crear
petición de estado
C
Verificar identidad
de 300
D
Solicitar credenciales
E
Verificar estado de
bloqueo de 100/300
Actualizar estadísticas
de gestión de alertas
F
Permitir/bloquear
proceso de inicio
de sesión
G
Conceder/denegar acceso
Solicitar estado de cuenta
Credenciales
Resolución de estado

Fig. 2

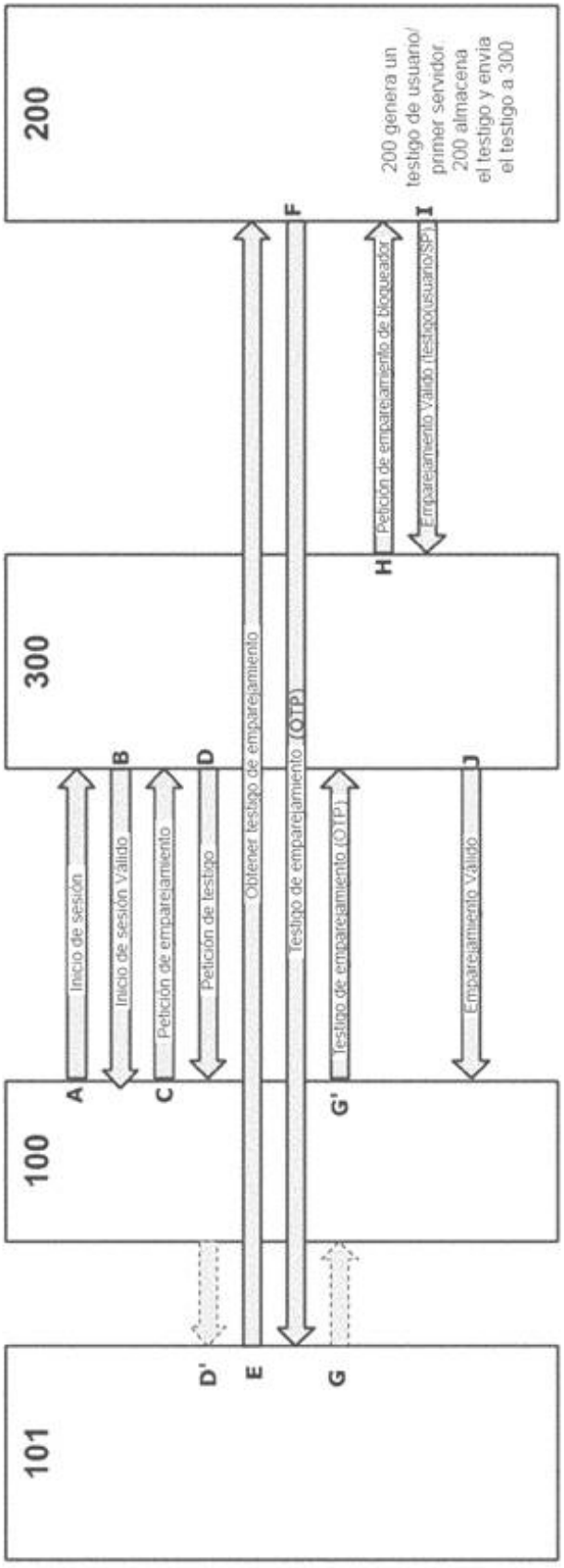
200
300
100
101
200 genera un testigo de usuario/ primer servidor 200 almacena el testigo y envia el testigo a 300
Inicio de sesión
Inicio de sesión Válido
Petición de emparejamiento
Petición de testigo
Obtener testigo de emparejamiento
Testigo de emparejamiento (OTP)
Testigo de emparejamiento (OTP)
Emparejamiento Válido
Petición de emparejamiento de bloqueador
Emparejamiento Válido (testigousuario/SP)
A
B
C
D
D'
E
F
G
G'
H
I
J

Fig. 3