(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 243**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.10.2013 E 13382396 (3)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 2819371**

(54) Título: **Un método implementado en ordenador para impedir ataques contra sistemas de autorización y productos de programas de ordenador del mismo**

(30) Prioridad:

24.06.2013 EP 13382237

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2020

(73) Titular/es:

TELEFONICA 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 en ordenador para impedir ataques contra sistemas de autorización y productos de programas de ordenador del mismo

Campo de la técnica

La presente invención se dirige, en general, a sistemas de autenticación y autorización y, más particularmente, a un método implementado en ordenador y productos de programa de ordenador para impedir ataques contra los sistemas de autorización en los que se controla el acceso a los diferentes recursos y las acciones definidas para un usuario.

Antecedentes de la invención

En los últimos años, el mercado de la detección de fraudes en la red se ha incrementado considerablemente, de modo que la innovación en los procesos de autenticación y autorización ha llegado a tener gran importancia.

La creciente complejidad de las aplicaciones ha conducido a la adopción de muchas técnicas de seguridad crecientemente sofisticadas. Una de las clasificaciones que se puede proponer para el estudio de estas técnicas de seguridad permite la distinción entre soluciones de autenticación y soluciones de autorización. Las técnicas de autenticación están diseñadas para verificar que una persona es la que reivindica ser. Para añadir más fiabilidad en la verificación de que realmente la persona corresponde a la identidad que está siendo comprobada, se pueden tomar muchos esquemas de autenticación alternativos o se puede extender el número de factores para elaborar esta autenticación.

Hay muchas soluciones diseñadas para reforzar los procesos de autenticación y, por extensión, para fortificar los procesos de autorización. Una vez que los usuarios se han identificado con seguridad, hay esquemas de autorización que permiten flexibilidad y robustez en la asignación de permisos a los usuarios para asegurar un acceso seguro a los recursos del sistema. Sin embargo, hay amenazas que no pueden ser desbaratadas aun adoptando cualquiera de los esquemas existentes para la autenticación/autorización, o la solución es demasiado cara para poder permitírselo. Estas amenazas afectan directamente a la forma en que se realiza el acceso a recursos específicos. Un método para acometer estas amenazas implica el diseño de mecanismos de seguridad completamente nuevos. Estos mecanismos deben garantizar que una vez que se ha verificado la identidad del usuario y se ha comprobado el nivel de autorización a un recurso para este usuario, las acciones realizadas por el usuario de ese recurso no son interceptadas y modificadas por cualquier atacante.

En cualquier modelo de autorización, se incluyen diferentes técnicas que facilitan el acceso a varios recursos del sistema. La información del papel del usuario, los datos de control de acceso proporcionados cuando el usuario es autenticado, son ejemplos de información que se puede usar para determinar a quién dar acceso a qué recursos y cómo ha de garantizarse este acceso. Finalmente, la determinación de qué debería ser accedido por qué usuarios, se especificará para cada aplicación. Por esta razón, a veces será difícil proporcionar un esquema de autorización general. Será necesario definir una lógica específica de la aplicación para determinar qué usuarios pueden acceder y cómo realizarían estos accesos. A partir de esta idea, hay muchas soluciones que proponen esquemas seguros y flexibles para la implementación de la autorización. En todas estas soluciones, la seguridad se debe garantizar mediante la selección correcta del mecanismo de autenticación y una implementación correcta del esquema de autorización seleccionado.

Algunas de las soluciones proporcionan flexibilidad definiendo su propio SDK para fomentar el uso de sus esquemas para autenticación/autorización. Hoy en día, la mayor parte de los SDK se basan en conceptos introducidos por OAuth y no suponen un riesgo por sí mismos. Esto es aplicable al Microsoft Live Connect, Facebook PHP SDK y Windows 8 SDK Authentication Broker. Si existen, las amenazas deberían proceder de un uso deficiente de estos SDK. De hecho, independientemente de las amenazas derivadas de una pobre implementación del esquema elegido, la mayor parte de las amenazas que se pueden definir sobre un sistema de autorización coincide con las amenazas definidas para los sistemas de autenticación. Esta coincidencia tiene que ver con el mal uso de las credenciales usadas para gestionar permisos que garanticen el acceso a los recursos [2], [5].

En [2] se definen cuatro niveles diferentes en términos de las consecuencias de errores de autenticación y autorización y mala utilización de las credenciales. El nivel 1 es el nivel más bajo (el más inseguro) y el nivel 4 es el más alto.

- Nivel 1 - Un atacante puede realizar intentos de registro repetidos suponiendo valores posibles de la autenticación de la prueba (token). Un atacante también es capaz de reproducir mensajes previamente capturados (entre un usuario legítimo y un verificador) para autenticarse como ese usuario al verificador. El NIST recomienda el uso de una autenticación mono o multi-factor sin ninguna demostración de identidad para

proporcionar una protección contra estos ataques de suposición y reproducción en línea.

- Nivel 2 - Un atacante puede escuchar pasivamente el protocolo de autenticación para capturar información que puede usar en un ataque activo posterior para enmascararse como el usuario. El NIST recomienda el uso de una autenticación mono o multi-factor para proporcionar protección contra estos ataques de escuchas a escondidas o espionaje y todos los ataques del nivel 1.
- Nivel 3 - El atacante se coloca a sí mismo entre el usuario y el verificador de modo que puede interceptar y alterar el contenido de los mensajes del protocolo de autenticación. El atacante típicamente imita al verificador para el usuario e imita simultáneamente al usuario para el verificador. La realización de un intercambio activo con ambas partes simultáneamente puede permitir al atacante usar los mensajes de autenticación enviados por una parte legítima para autenticarse con éxito ante la otra. El NIST recomienda el uso de una autenticación multi-factor y el amplio uso de OTP. También sugiere que un token usado para la autenticación sea desbloqueado por el usuario usando una palabra clave o biométrica. La adopción de estas soluciones proporciona protección contra los ataques de imitación del verificador, ataques MitM y ataques del nivel 2.
- Nivel 4 - Un atacante es capaz de situarse a sí mismo entre un usuario y un verificador posteriormente a un intercambio de autenticación con éxito entre estas dos últimas partes. El atacante es capaz de aparentar un usuario para el verificador, o viceversa, para controlar el intercambio de datos de la sesión. Por otro lado, el atacante puede comprometer o explotar en otra manera los tokens de autenticación y puede interceptar todas las comunicaciones de entrada o salida desde el dispositivo (ataques de Man-in-the-device (MitD) o “Persona en el dispositivo” o ataques de Man-in-the-Browser (MitB)). El atacante puede hacer esto infectando el sistema con software maligno. El NIST sugiere el uso de autenticación multi-factor con hardware (tokens de hardware) resistente contra manipulaciones certificado por FIPS-140-2 [4] para obtener protección contra estos ataques de apropiación de la sesión y los ataques del nivel 3.

Para los tres primeros niveles de ataque, los ataques y las soluciones existentes se enfocan ambas en la forma de verificación de la identidad del usuario. En el nivel 4, el NIST propone el uso de soluciones contra la apropiación de la sesión y otros ataques sobre los procesos de autenticación. Esta apropiación de la sesión implica que un atacante se aprovecha del intercambio legítimo de credenciales que un usuario realiza para cumplir con el proceso de autenticación. Una vez que se lleva a cabo esta validación, el atacante se interpone entonces en la comunicación que tiene lugar. Este tipo de ataque se puede implementar de dos maneras: actuando activamente, apropiándose de la conexión y dejando fuera de ella al usuario legítimo, o permaneciendo oculto modificando el contenido de la comunicación transparentemente para el usuario. Cualquiera que sea la implementación de este ataque, es importante observar, que éste es un ataque dirigido a la quiebra del sistema de autorización, dejando intacto, aunque inútil, el sistema de autenticación. Aunque hay alternativas para proteger activamente sistemas frente a esta amenaza, no hay una solución adecuada para mitigar los efectos del ataque una vez que el dispositivo desde el que se requiere el acceso a los recursos, se ha cometido.

El NIST sugiere el empleo de hardware (tokens de hardware) resistente contra manipulaciones certificado por FIPS-140-2 [4]. El uso de estos dispositivos proporciona a los usuarios la capacidad para generar una palabra clave de uso único (palabra clave de una vez, OTP de “one time password”) para probar su identidad en cada transacción. Además, hay implementaciones de hardware de esos tokens que puede generar otras OTP codificadas para contener información sobre cómo concretar una transacción específica.

Se pueden definir diferentes criterios para establecer una comparación entre los esquemas de autenticación/autorización. En [1] los autores sugieren la necesidad de definir los criterios para realizar una comparación efectiva. Estos aspectos son: seguridad, capacidad de uso y complejidad de la implementación (capacidad de despliegue). Este documento presenta un estudio intensivo para instrumentar la comparación a través de la definición de las mediciones. La tabla a continuación resume las mediciones definidas para cada criterio.

Capacidad de uso	Memoria sin esfuerzo Escalable para los usuarios Nada que transportar Sin esfuerzo físico Fácil de aprender Eficiente en el uso Errores infrecuentes Fácil recuperación de una pérdida
Capacidad de despliegue	Accesible Coste por usuario despreciable Compatible con el servidor Compatible con navegador Maduro No propietario

Seguridad	Resistente a la observación física Resistente a la imitación dirigida Resistente a la suposición estrangulada Resistente a la suposición no estrangulada Resistente a la observación interna Resistente a fugas desde otros verificadores Resistente al phishing Resistente al robo Terceras partes no fiables Requiere consenso explícito Desagradable

En el caso del criterio de seguridad, el conjunto de mediciones 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 un cierto número de decisiones. Y estas decisiones definen el escenario de trabajo. Por ejemplo en el caso de OAuth 2.0 [5] los supuestos adoptados son los siguientes:

- El atacante tiene un acceso total a la red entre el cliente y los servidores de autorización del cliente y el servidor de recursos, respectivamente. El atacante puede escuchar a escondidas o espiar 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 involucradas en el protocolo OAuth pueden conspirar para montar un ataque contra la tercera parte. Por ejemplo, el cliente y el servidor de autorización pueden estar bajo el control de un atacante y conspirar para engañar a un usuario para obtener acceso a los recursos.

Atendiendo a las mediciones introducidas anteriormente, es posible determinar qué soluciones correspondientes al nivel de seguridad más alto (nivel 4) tienen un pobre rendimiento en capacidad de despliegue y de uso. Una vez que la evaluación del sistema permite determinar en qué nivel ha de ser desplegado su sistema de autenticación, es necesario evaluar si el usuario se ha autenticado con seguridad y correctamente. Aunque hay algunas herramientas que ayudan en esta tarea [3], [6], los despliegues en el nivel 4 son difíciles de evaluar correctamente. En términos de capacidad de uso, el uso de tokens de hardware resistentes a la manipulación va en contra la adopción de estas soluciones por los usuarios, y se ha comprobado que esta situación conduce a una mala utilización del sistema de credenciales. Estos tokens son caros. Hay dispositivos independientes que el usuario debe custodiar y que pueden emplearse solamente con un proveedor de servicios. Si los usuarios tienen que manejarse con más de un proveedor de servicios que haya adoptado estos tokens de hardware de resistencia a la manipulación, han de tener en custodia tantos tokens como proveedores de servicios tengan.

Adicionalmente, en términos de autorización, en [7] los autores explican que, junto a algunos problemas de seguridad de cada SDK, los desarrolladores que han elegido integrarse con uno de ellos realizan suposiciones que pueden conducir a problemas de seguridad. Esto es debido a que los SDK frecuentemente no están bien documentados y la seguridad casi siempre se rompe procedente de atacantes que hallan formas de violar este sistema de suposiciones en el que confiaron los implementadores.

Junto a estas dificultades, se deben considerar otros problemas para comprender el incremento constante en el fraude que surge del robo de identidades digitales. Por ejemplo, no es posible medir un nivel de seguridad homogéneo en todas las cuentas digitales de usuarios. Es necesaria una solución que pueda igualar el nivel de seguridad de todas las cuentas digitales que un usuario posee. Esta solución debería extender esta seguridad no solamente a los procesos de autenticación, sino también a los procesos de autorización de recursos y a todos los procedimientos relacionados con dichas cuentas.

Por lo tanto, es necesario un enfoque diferente para mejorar la seguridad global en los sistemas de autenticación/autorización, cualquiera que sea el esquema o esquemas adoptados, minimizando el impacto en la capacidad de uso y de despliegue de estos sistemas.

La solicitud de patente US 2009/183247 A1 divulga sistemas y métodos para asegurar el acceso a una red. El acceso a la red se asegura mediante autenticación multi-factor, biometría, cifrado seguro y una variedad de redes inalámbricas normas estándar. La biometría se utiliza en combinación con otros factores de autenticación para crear un esquema de autenticación multi-factor para un acceso de red altamente seguro. Las solicitudes que requieren acceso a recursos de red seguros pueden interceptarse y una página de portal cautiva devuelta para desafiar a un usuario. La información biométrica devuelta en respuesta a la página de portal se usa para autenticar al usuario y determinar los derechos de acceso a la red.

La solicitud de patente US 2004/030932 A1 divulga protocolos de autenticación seguros, particularmente adecuados

para su uso en dispositivos de comunicaciones móviles de autenticación con recursos computacionales limitados. En esta solicitud de patente, un sistema de comunicación basado en la red incluye un dispositivo de cliente y al menos dos servidores. Las primeras y segundas acciones son generadas a partir de una primera palabra clave asociada con el dispositivo de cliente, y almacenada en servidores primero y segundo respectivos. Al enviar información adicional asociada con el dispositivo de cliente al menos a uno de los servidores primero y segundo, cada una de las primeras y segundas acciones tiene la propiedad de que no es posible determinarla únicamente a partir de la correspondencia de la información adicional con la primera palabra clave, los servidores primero y segundo utilizan las acciones primera y segunda respectivas para determinar colectivamente dicha correspondencia de la información adicional con la primera palabra clave.

Referencias:

[1] Bonneau, J., Herley, C., van Oorschot, P. C., y Stajano, F. (mayo de 2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on (págs. 553-567). IEEE.

[2] Burr, W. E., Dodson, D. F., y Polk, W. T. (2006). Electronic authentication guideline. NIST Special Publication, 800, 63.

[3] Dalton, M., Kozyrakis, C., y Zeldovich, N., Nemesis: Preventing Authentication & Access Control Vulnerabilities in Web Application, In Proceedings of the 18th conference on USENIX security symposium, (págs. 267-282) USENIX Association.

[4] Evans, D., Bond, P., Bement, A., Security Requirements for Cryptographic Modules, FIPS PUB 140-2 - FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Recurso en línea: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] McGloin M. y Hunt P. (2013, January) OAuth 2.0 Threat Model and Security Considerations. ISSN: 2070-1721. Recurso en línea: http://tools.ietf.org/pdf/rfc6819.pdf.

[6] Sun, F., Xu, L., y SU,Z. (2011,August) Static detection of Access control vulnerability in web applications. In Proceedings of the 20th USENIX conference on Security (págs. 11-11). USENIX.

[7] Wang, R., Zhou, Y., Chen, S., Qadeer, S., Evans, D., y Gurevich, Y. (2013). Explicating SDKs: Uncovering Assumptions Underlying Secure Authentication and Authorization (Vol. 37). Microsoft Research Technical Report MSR-TR-2013.

Descripción de la invención

Para conseguir lo anterior, la invención proporciona un método y un programa de ordenador según se define en las reivindicaciones 1 y 10, respectivamente. Las realizaciones específicas aparecen definidas en las reivindicaciones dependientes. Esta solución está diseñada para limitar el tiempo en que un atacante puede desarrollar un ataque. Por lo tanto, esta solución supone un límite en los recursos disponibles para que un atacante se organice y ataque. Primero, la invención busca reducir el riesgo de un ataque dirigido a un proceso de autenticación/autorización bloqueando temporalmente el mecanismo de ejecución de la operación. Disminuyendo por lo tanto el periodo de exposición de estos sistemas y, por lo tanto, disminuyendo las oportunidades de éxito de ataques sobre el sistema. Además, un primer servidor o proveedor de servicios puede forzar el uso de una segunda fase de autenticación (usando una infraestructura de OTP) para proveedores de servicios que no proporcionen esta opción en sus procesos de gestión de cuentas o incluso permitan al usuario activarla.

De acuerdo con un primer aspecto se proporciona un método implementado en ordenador para impedir ataques contra sistemas de autorización, que comprende: la recepción por al menos un primer servidor de una solicitud en nombre de un usuario para ser registrado en un servicio de dicho primer servidor; y la autorización de dicha solicitud, por dicho primer servidor, verificando la información de identificación de usuario de dicho usuario.

Al contrario de las propuestas conocidas, y en una forma característica, para que dicha solicitud sea autorizada el método comprende adicionalmente:

- el envío, por dicho primer servidor a un segundo servidor en conexión con un dispositivo de ordenador del usuario con un programa dedicado, de una solicitud acerca de un estado asociado a dicho usuario;
- inicializar un intercambio de credenciales entre dicho primer y segundo servidores para proporcionar una autenticación mutua;
- verificación de dicho estado asociado que ha sido establecido previamente como válido o como inválido por dicho usuario y almacenado en una memoria de dicho segundo servidor;
- envío, en dicho segundo servidor, de dicho estado asociado a dicho primer servidor; y
- el uso por dicho primer servidor de dicho estado asociado recibido para:
    - autorización de dicha solicitud para dicho servicio en nombre de dicho usuario si dicho estado asociado se ha establecido como válido, o
    - rechazo de dicha solicitud para dicho servicio si dicho estado asociado se ha establecido como inválido,

en el que, en caso de que dicha solicitud a ser registrado en un servicio de dicho primer servidor sea autorizada y se realice una solicitud en nombre de dicho usuario para realizar una operación en dicho primer servidor usando al menos una parte de los recursos de dicho primer servidor, el método comprende las siguientes etapas:

- realización, de la verificación del estado de la operación asociada con dicho usuario comprendiendo una solicitud de estado a dicho primer servidor para determinar qué entrada en un esquema corresponde con dicha operación;
- recepción, en dicho segundo servidor desde dicho primer servidor de dicha solicitud sobre un estado de la operación asociado a dicho usuario afectando a dicha entrada;
- inicialización de un intercambio de credenciales entre dichos primer y segundo servidores;
- evaluación, en dicho segundo servidor de un estado de entrada del esquema de estado desde una raíz a dicha entrada;
- envío, por dicho segundo servidor, de un resultado de la evaluación a dicho primer servidor;
- toma de una decisión, por dicho primer servidor, al menos usando dicho resultado recibido para permitir o bloquear dicha solicitud en nombre de dicho usuario para realizar dicha operación.

La solicitud de estado asociada con el usuario comprende el envío de un token de seguridad, siendo generado dicho token de seguridad durante un proceso previo de vinculación de cuentas de usuario. Este token enlaza al usuario con el primer servidor sin desvelar ninguna información personal del usuario al segundo servidor de información. A continuación, el token se almacena con seguridad en una memoria del primer servidor y en una memoria del segundo servidor una vez que el usuario ha configurado la vinculación de la primera y segunda identificaciones de los servidores.

El intercambio de credenciales para asegurar la autenticación mutua entre el primer servidor y el segundo servidor, se realiza, preferiblemente, por medio de un procedimiento de autenticación estándar basado en el intercambio de certificados que define, como resultado, un canal seguro. El intercambio se realiza para verificar que tanto el primer servidor como el segundo servidor son quienes reivindican ser.

El segundo servidor puede mandar una notificación al usuario en caso de que dicha solicitud para ser registrado en un servicio del primer servidor se rechace. Por ejemplo, mediante el envío de un Servicio de Mensajes Cortos (SMS) o un e-mail, de o un mensaje mediante una aplicación de mensajería de teléfono inteligente, o solamente mediante el resalte o notificación en dicho programa dedicado de dicho dispositivo de ordenador del usuario.

Opcionalmente, la etapa de evaluación del estado de entrada del esquema realizada por el segundo servidor puede incluir adicionalmente un segundo factor de autenticación que comprende, si dicho estado de entrada del esquema se establece como válido:

- el envío, por dicho segundo servidor de una OTP al primer servidor dentro del resultado de la solicitud de estado de la operación;
- solicitud, por el primer servidor al usuario, de una OTP que el usuario va a usar como segundo factor temporal;
- envío, por el segundo servidor, de la misma OTP enviada al primer servidor al usuario a través de dicho otro programa dedicado del usuario;
- recuperación, por el usuario, de dicha OTP del segundo factor temporal solicitada a través de dicho programa dedicado, introduciéndola dentro de dicho otro programa dedicado del usuario y enviándola adicionalmente a través de dicho otro programa dedicado del usuario al primer servidor; y
- comprobación, por el primer servidor, de si la OTP recibida desde el segundo servidor y la OTP del segundo factor temporal recibida desde dicho otro programa dedicado del usuario coinciden para permitir o bloquear dicha solicitud en nombre de dicho usuario para realizar dicha operación.

El estado asociado se establece como válido (desbloqueado) o como inválido (bloqueado) un cierto período de tiempo y puede ser modificable por el usuario siempre que éste último lo desee. Por ejemplo, el usuario puede planificar una política de bloqueo/desbloqueo para automatizar la gestión de sus cuentas mantenidas con diferentes servidores usando diferentes criterios: tiempo, geolocalización (diferentes políticas para hogar, trabajo, etc.). Otra posibilidad para la modificación de dicho estado asociado puede ser mediante la delegación del control que dicho usuario tiene sobre sus cuentas a otros usuarios. Esto se puede realizar considerando dos opciones diferentes. En la primera, se usa un mecanismo de control parental de modo que se delega el control de acceso de las cuentas de los hijos (original) al mecanismo de control del padre. En el segundo, una única cuenta permite múltiples bloqueos. En este último caso, la acción de desbloqueo requerirá que los usuarios desbloqueen sus bloqueos simultáneamente. En ambos casos, la delegación se realiza con seguridad manteniendo inalterada la privacidad de cada usuario.

La solicitud para ser registrado en un servicio y/o la solicitud para realizar una operación se puedan registrar para proporcionar estadísticas. De esta forma, el usuario puede obtener estadísticas de uso del sistema que reflejen la actividad del sistema y seguir los intentos de imitación. Estas estadísticas informan sobre cuándo alguien ha

intentado acceder a un servicio con el nombre de usuario del usuario.

La materia objeto descrita en el presente documento se puede implementar en software en combinación con hardware y/o firmware, o una combinación adecuada de ellos. Por ejemplo, la materia objeto descrita en el presente documento se puede implementar en un software ejecutado por un procesador.

De acuerdo con otro aspecto se proporciona un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, una puerta lógica programable en campo (FPGA), un circuito integrado de aplicación específica, un microprocesador, un microcontrolador, o cualquier otra forma de hardware programable.

Las realizaciones de la invención también engloban un producto de programa de ordenador que incluye medios de código de programas adaptados para realizar una segunda autenticación del factor de acuerdo con el método de la reivindicación 6.

La presente invención permite al usuario planificar una política de bloqueo/desbloqueo para automatizar la gestión de cuentas mantenidas con diferentes servidores usando diferentes criterios: tiempo, geolocalización (diferentes políticas para hogar, trabajo, etc.); delegar el control de sus cuentas a otros usuarios del segundo servidor; permitir sistemas de supervisión que permita a los usuarios ser alertados de intentos de robo de la identidad o imitación del usuario no verdadero en solicitudes de ejecución de operaciones, proporcionando una vía de actuación para tomar una acción para controlar la identidad digital; establecer un segundo factor para la autenticación para verificadores que no lo estén proporcionando; establecer una cuenta a ser bloqueada o desbloqueada y cambiarla con efecto inmediato mediante el uso de un control de conmutación; establecer una planificación para validar/invalidar (bloquear/desbloquear) una cuenta con dicha operación automáticamente en base a ajustes de tiempo y fecha. Una vez que se recibe la solicitud de comprobación de estado, el segundo servidor responde en base al estado actual del planificador; mejora el nivel de seguridad de una cuenta de dicha operación configurando un segundo factor de autenticación integrado con el segundo servidor; controla diferentes acciones asociadas con una cuenta, autorizando o prohibiendo la ejecución de las mismas en una forma compatible con el esquema de autorización establecido.

Adicionalmente, la invención permite homogeneizar el nivel de seguridad para todas las diferentes cuentas que tiene un usuario. Permite ofrecer un nivel de seguridad comparable con el nivel 4 definido por el NIST. Esto se realiza para diferentes cuentas que pueden controlarse ahora solamente con un dispositivo e independientemente del esquema de autenticación/autorización definido por cada proveedor de servicios.

La invención no propone ningún esquema de autenticación/autorización nuevo. Realmente, la invención complementa los esquemas existentes con una capa de seguridad extra. Aunque esto puede limitar su capacidad de uso y de despliegue, el diseño de la invención está orientado a minimizar el impacto sobre estos criterios. Como se ha establecido anteriormente, la elección del esquema de autenticación determina el riesgo de seguridad que se está asumiendo para un sistema de autorización. Lo que se propone en este caso es reducir el riesgo tomado con la elección de cualquier mecanismo de autenticación/autorización reduciendo el tiempo en el que este sistema está accesible para ser roto.

Suponiendo que haya una relación entre el éxito y el fallo de un ataque sobre el sistema de autorización y el tiempo en el que este sistema es accesible (tiempo de exposición) es posible la determinación como probabilidad condicional (p (ataque con éxito | expuesto)) el riesgo relativo (RR) satisfaga la siguiente expresión:

$$RR = \frac{p(Ataque\,con\,éxito \mid \text{expuesto})}{p(Ataque\,con\,éxito \mid \text{sin exposición})} > 1 \qquad \text{Ec. 1}$$

En esta expresión, se asume que la probabilidad de éxito de un ataque se relaciona directamente con el tiempo de exposición. Esto es, la exposición continua de un sistema de ordenador, en este caso sistema de autenticación, incrementa la probabilidad de éxito de un ataque a diferencia de un escenario en el que la exposición se limite. De la misma manera se puede evaluar la siguiente expresión:

$$\frac{\frac{p(Ataque\,con\,éxito \mid \text{expuesto})}{p(Ataque\,fallido \mid \text{expuesto})}}{\frac{p(Ataque\,con\,éxito \mid \text{no expuesto})}{p(Ataque\,fallido \mid \text{no expuesto})}} > 1 \qquad \text{Ec. 2}$$

Indicando que hay una mayor probabilidad de un ataque con éxito si existe una exposición continuada del sistema. Es posible también estimar la parte de todos los ataques con éxito que podrían haberse evitado si la exposición se

hubiera evitado (Porcentaje de Riesgo Atribuible, (ARP) de “Attributable Risk Percent”). Esto se calcula con la expresión 3.

$$ARP = \frac{RR - 1}{RR} \qquad \text{Ec. 3}$$

Esta expresión permite la evaluación de la inversión requerida para permitir una solución diseñada para reducir el tiempo que está accesible el proceso de autenticación. La experiencia profesional y el conocimiento técnico de las técnicas de ataque documentadas para romper los sistemas de autenticación/autorización confirman la suposición realizada anteriormente (RR > 1). Por lo tanto, se puede afirmar que ARP > 1 una vez que se adopta el cierre de la cuenta.

Esta reducción en el tiempo de exposición permite la mitigación de los efectos de la mayor parte de las amenazas relacionadas con la fase de autenticación antes de que un usuario pueda acceder a algunos recursos privilegiados. La presente invención permite también la reducción de la exposición de acciones particulares que se pueden tomar después de que el proceso de registro se haya llevado a cabo. Por lo tanto, esta reducción de la exposición supone la limitación del tiempo en el que la acción se puede ejecutar y el establecimiento de un canal que permita el envío de información crítica para asegurar la integridad de esta ejecución de la acción.

La invención engloba las soluciones para las amenazas definidas por el NIST. Pero en este caso, estas soluciones se proporcionan a los usuarios a través de un programa dedicado diseñado para ser ejecutado en un dispositivo móvil, que facilite la interacción con un segundo servidor. Además, este segundo servidor trae la privacidad de las comunicaciones con relación al control de las cuentas del usuario e incorpora toda la información de control que los usuarios han establecido alrededor de las acciones que los proveedores de servicio les han ofrecido.

Breve descripción de los dibujos

Lo anterior y otras ventajas y características se comprenderán más profundamente a partir de la descripción detallada a continuación de las realizaciones, con referencia a los adjuntos, que se deberían considerar en una forma ilustrativa y no limitativa, en los que:

La Figura 1 es una ilustración de la arquitectura general de la presente invención.
La Figura 2 es un diagrama de flujo que ilustra una secuencia de vinculación de cuentas con autorización.
La Figura 3 es un diagrama de flujo que ilustra cómo se puede comprobar un estado de una cuenta de usuario para autenticación.
La Figura 4 muestra el diagrama de flujo que resume la forma en que puede extenderse el proceso introducido en la figura 3 para su generalización, adoptando el proceso de autenticación como otra operación desde el directorio propuesto por el primer servidor.

Descripción detallada de varias realizaciones

Con referencia a la Figura 1, se muestra la arquitectura general de la presente invención. En relación a la Figura 1, se usa un dispositivo informático 100 tal como un teléfono móvil, un teléfono inteligente, una tablet-PC o una PDA entre otros, por dicho usuario para registrarse en un programa dedicado 102 en comunicación con un segundo servidor 200 y para gestionar el estado de cada primer servidor 300 con el que un usuario desea solicitar un servicio.

Con esta nueva propuesta, dicho usuario 100 puede desbloquear dicha operación definida para una cuenta particular creada con dicho primer servidor 300. Tal como se establece a continuación, esta acción puede mejorar el control definido para esta cuenta por la decisión del primer servidor 300. En esta decisión, el primer servidor 300 puede elegir incorporar un nuevo control de seguridad más allá de la opción por defecto de bloqueo/desbloqueo o del segundo factor de autenticación. Este control de seguridad consiste en proporcionar un canal de comunicación desde el usuario 100 al primer servidor 300, a través del segundo servidor 200. El primer servidor 300 puede configurar el sistema para pedir al usuario 100 una información particular relativa a dicha operación a ser realizada. Esta información se puede usar por el segundo servidor 200 para verificar si el usuario 100 es quien realmente está solicitando dicha operación y para confirmar si la operación que ha llegado al primer servidor 300 es exactamente como la que el usuario 100 ha ordenado.

Suponiendo que el primer servidor 300 pudiera desear verificar la integridad de la operación, se puede seleccionar qué parámetros son críticos para asegurar la integridad de la operación. En este caso, es importante que la información solicitada corresponda de modo único con el parámetro crítico de la operación para identificarlo correctamente.

En esta arquitectura, el usuario 100, junto a tener una cuenta en el segundo servidor 200, puede tener múltiples cuentas con diferentes proveedores de servicios. Uno de estos proveedores de servicios es el primer servidor 300.

Una vez que el usuario 100 completa el proceso de registro con estas cuentas tendrá acceso a múltiples operaciones específicas para cada proveedor de servicios. El segundo servidor 200 facilita cómo un primer servidor 300 puede integrar este control dentro de la lógica de sus aplicaciones.

Cuando el primer servidor 300 decide integrar sus servicios, proporcionará la capacidad de enlazar sus cuentas con las cuentas que el usuario 100 tiene en el segundo servidor 200. Cuando dicho usuario 100 decide establecer este enlace, comienza el proceso de vinculación que asegura una privacidad completa para el usuario 100. Una vez que el proceso de vinculación está completo, el usuario 100 puede acceder a la configuración de control de la cuenta con el primer servidor 300 desde un programa dedicado 102 (es decir una aplicación móvil).

Cada vez que los ajustes asociados con una cuenta se cambian en dicha aplicación móvil, esta modificación se propaga inmediatamente al segundo servidor 200 para cambiar el estado de la cuenta a la que puede acceder el primer servidor 300.

El núcleo del segundo servidor implementa la función principal del segundo servidor 200: bloquear o desbloquear dicha cuenta de usuario con el primer servidor 300 y las operaciones proporcionadas por el primer servidor 300. Para hacer esto, el segundo servidor 200 acepta y procesa las solicitudes de comprobación de estado enviadas desde el primer servidor 300. Este segundo servidor 200 también gestiona todos los datos acerca de los enlaces con dicho primer servidor 300 definidos por el usuario 100 y las solicitudes para la vinculación de nuevos bloqueos. La clave es que al usuario 100 nunca se le pregunta por cualquier información privada. Una vez que el usuario 100 crea su cuenta con el segundo servidor 200, puede establecer bloqueos con diferentes proveedores de servicios, como dicho primer servidor 300. Para activar estos bloqueos el segundo servidor 200, de acuerdo con una realización, genera un token. Son necesarios un token único y la definición de canales seguros para completar el proceso de vinculación entre el usuario 100 y el primer servidor 300. Como resultado de este proceso de vinculación, el token criptográfico se envía desde el segundo servidor 200 al primer servidor 300 que tiene que almacenar esta información con sus datos personales del usuario. Posteriormente, este token criptográfico se usará para solicitar el estado de bloqueo correspondiente. El usuario 100 puede modificar el estado de sus bloqueos, mediante la activación o configuración de las diferentes opciones que el segundo servidor 200 proporciona.

En caso de que el usuario 100 haya establecido un bloqueo con el segundo factor para autenticación sobre una cuenta o una acción particular, el segundo servidor 200 incorporará toda la lógica necesaria para la generación y comunicación de la OTP. Cuando el segundo servidor 200 recibe una solicitud desde el primer servidor 300 pidiendo el estado de la cuenta del usuario, se activa un segundo factor de autenticación. Se genera una OTP y se envía al usuario 100. Se envía la misma OTP al primer servidor 300 junto con el estado de la cuenta. Si el estado es ACTIVO y el usuario 100 tiene activado el segundo factor, el primer servidor 300 debería solicitar al usuario introducir la OTP para proseguir con la operación.

Ahora, si el usuario 100 ha establecido un bloqueo sobre una de dichas operaciones con un factor de integridad para verificar que los parámetros de la operación no se han modificado, dicho segundo servidor 200 incorpora la lógica necesaria para obtener la información crítica del usuario 100 y desde el primer servidor 300 y para comprobar si ambas son iguales. El segundo servidor 200 envía el resultado de la comprobación como el estado de la cuenta al primer servidor 300. En caso de falta de coincidencia, el primer servidor 300 puede concluir que un intruso puede estar interceptando la información desde el usuario 100. El primer servidor 300 puede construir entonces mecanismos para eludir el fraude y para elevar alertas de seguridad.

Con referencia a la Figura 2, se ilustra un proceso de vinculación de la cuenta del usuario 100 del segundo servidor 200 con diferentes cuentas para diferentes primeros servidores 300. En la Figura 2, una vez que un usuario 100, usando por ejemplo el programa dedicado 101 tal como un navegador, ha completado el proceso de registro (A-B) con un primer servidor 300 (en este caso particular un banco en línea, una red social, proveedores de tarjetas de créditos, etc.), el usuario 100 decide realizar dicho proceso de vinculación de cuentas. El usuario 100 solicita la vinculación al primer servidor 300 (C) usando el navegador 101. Como respuesta, el primer servidor 300 solicita un token de vinculación (D). El usuario 100 usa entonces el programa dedicado 102 (D') para obtener este token de vinculación desde el segundo servidor 200, después de un proceso de registro previo. El segundo servidor 200 genera un token (por ejemplo como una OTP) (E) y lo envía al programa dedicado del usuario 102 (F). Este token se puede usar para varios procesos de vinculación siempre que sea válida. El usuario obtiene el token (OTP) desde el programa dedicado 102 y la introduce en la página web visualizada en el navegador 101 por el primer servidor 300 (G-G'). El primer servidor 300 envía entonces el token recibido al segundo servidor 200, después de un intercambio previo de credenciales (H). Si la identidad del primer servidor 300 es validada, el segundo servidor 200 almacena el enlace entre el usuario 100 y el primer servidor 300 y genera un nuevo token que identifica este enlace. Este token (ID de cuenta) se envía al primer servidor 300 (I) y allí se almacena para comunicaciones futuras (J). Finalmente, se envía un acuse de recibo de la vinculación al navegador del usuario 101 (K).

Con referencia ahora a la Figura 3 se ilustra cómo se puede comprobar un estado de la cuenta de usuario para autenticación. En la Figura 3, un usuario 100, usando por ejemplo un navegador 101, solicita ser registrado en un

servicio (A) de un primer servidor 300 de modo que una vez que se haya validado (B) la existencia del usuario por dicho primer servidor 300, este último solicitará al segundo servidor 200 el estado de cuentas del usuario (C). Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de que se envíe el resultado de la información del estado de cuentas (D). Con el estado del resultado, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario (E).

En una realización, si el estado de la cuenta es desbloqueado o válido pero el segundo factor de autenticación está activo, dentro de la respuesta de la solicitud de estado, el segundo servidor 200 envía una OTP al primer servidor 300 que ha de emplear para completar la autenticación. El primer servidor 300 solicita entonces al usuario 100 la OTP que va a ser un segundo factor temporal (F). Entonces el segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (G). El usuario 100 recupera la OTP desde programa dedicado 102 y la introduce en el navegador 101 (H) y la envía al primer servidor 300 (I). El primer servidor 300 puede comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (J). Dependiendo de los resultados de esta verificación, el primer servidor realiza el proceso de autenticación (K) y comunica el resultado al usuario través de 101.

Cuando un primer servidor 300 envía una Solicitud de estado (Status_Request), el segundo servidor 200 comprende que alguien, con la información de identificación del servicio apropiada (es decir ID y palabra clave), está tratando de acceder al servicio. Si el estado de la cuenta se establece como bloqueada, o si esta solicitud ha llegado en un momento que no está incluido en el intervalo definido por el usuario 100, el segundo servidor 200 registra este evento como un intento falso. El segundo servidor 200 podría enviar, de acuerdo con una realización, una alerta de este evento al usuario si dicho usuario lo ha configurado así (por ejemplo mediante el envío de un Servicio de Mensajes Cortos (SMS), un e-mail, un mensaje mediante una aplicación de mensajería de teléfono inteligente, mediante un resaltado o notificación en dicho programa dedicado 102 de dicho dispositivo de cálculo del usuario 100, etc.) o solamente actualizar las estadísticas para una revisión posterior. Entonces el segundo servidor 200 vuelve al estado asociado con la cuenta como bloqueada.

Con la intención de mejorar la seguridad de cualquier sistema de autorización, el uso de dicho segundo servidor 200 se propone como una nueva capa que da a los usuarios la oportunidad de controlar el acceso a los recursos y procedimientos asociados con sus cuentas definidas con cualquier primer servidor. Estos recursos y procedimientos se envían con operaciones que dependen de las acciones principales definidas para una cuenta (es decir proceso de registro). Esta dependencia se establece con una jerarquía en la que los cambios en las entradas raíz se propagan a sus hijos.

En esta realización, con referencia a la Figura 4 se muestra el proceso de verificación del estado. Esta operación es propuesta por el primer servidor 300 adjunto a la gestión de cuenta. El usuario 100, usando por ejemplo un navegador 101, solicita, de acuerdo con una realización, ejecutar una operación relacionada con una cuenta (A) en el primer servidor 300. Esta operación puede ser el registro en un servicio particular o ejecutar alguna operación relacionada con los servicios proporcionados por el primer servidor (por ejemplo pago por Internet con una tarjeta de crédito). De ese modo una vez que ha sido validada la existencia del usuario (B) por dicho primer servidor 300, este último realiza la correspondencia de la operación solicitada con la entrada de esquema en la jerarquía definida por esta cuenta de usuario (D) y solicita al segundo servidor 200 este estado de entrada (E).

Entonces el segundo servidor 200 inicializa el intercambio de credenciales antes de evaluar el estado de entrada del esquema desde la raíz a la entrada (F). El estado de la cuenta del usuario se recupera y si está desbloqueada se realiza la misma evaluación con cada etapa hallada hasta alcanzar la entrada del esquema. La información del estado de la entrada del esquema se envía (G) y, con esta información, el primer servidor 300 toma la decisión de permitir o bloquear el acceso del usuario a la operación.

El segundo factor de autenticación se puede activar si el estado de entrada del esquema es válido o está desbloqueado para reforzar el proceso. El segundo servidor 200 envía una OTP al primer servidor 300 dentro de la respuesta de la solicitud de estado. Este primer servidor 300 la emplea para completar la autenticación. El primer servidor 300 solicita al usuario 100 la OTP que va a ser el segundo factor temporal (H). El segundo servidor 200 envía la misma OTP al programa dedicado del usuario 102 (I). El usuario 100 recupera la OTP desde programa dedicado 102 y la introduce en el navegador 101 (J) y la envía al primer servidor 300 (K). Los primeros servidores pueden comprobar si la OTP enviada a través del navegador 101 coincide con la recibida con el estado de la cuenta (L). El primer servidor 300 deniega la operación de ejecución si las OTP no se ajustan.

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

REIVINDICACIONES

1. Un método implementado en ordenador para impedir ataques contra sistemas de autorización, en el que un segundo servidor (200) en conexión con un dispositivo de ordenador de un usuario (100) a través de un segundo programa dedicado (102), instalado en dicho dispositivo de ordenador, se usa para gestionar un estado de las cuentas que tiene el usuario (100) en un primer servidor (300) y un estado de las operaciones definidas para una cuenta particular, estableciéndose dicho estado de cuenta y dicho estado de operación siempre que el usuario (100) quiera, como válido o inválido por el usuario (100) a través del segundo programa dedicado (102) y almacenado en una memoria del segundo servidor (200), y estableciéndose dicho estado de cuenta y dicho estado de operación por el usuario (100) una vez que se ha completado el proceso de vinculación con el segundo servidor (200), asegurando dicho proceso de vinculación la privacidad al usuario (100), comprendiendo el método:

- la recepción por dicho primer servidor (300) del usuario (100) utilizando un primer programa dedicado que incluye un navegador (101), una solicitud de registro en un servicio de dicho primer servidor (300), incluyendo dicha solicitud la provisión de información de identificación que valida la identidad del usuario en el primer servidor (300);
- una vez que se ha validado la existencia del usuario por el primer servidor (300), recibir por dicho segundo servidor (200) desde el primer servidor (300) una solicitud acerca de un estatus referente a una cuenta del usuario (100) en el primer servidor (300);
- en respuesta a la recepción de la solicitud, inicializar un primer intercambio de credenciales entre dicho primer (300) y dicho segundo (200) servidor para proporcionar una autenticación mutua, realizándose el primer intercambio de credenciales a través de un procedimiento de autenticación basado en intercambio de certificados;
- verificación, por dicho segundo servidor (200), de dicho estado de cuenta;
- envío, por dicho segundo servidor (200), de dicho estado de cuenta a dicho primer servidor (300); y
- el uso, por dicho primer servidor (300), de dicho estado de cuenta para:

    - autorización de dicha solicitud de registro de servicio si dicho estado de cuenta se ha establecido como válido, o
    - rechazo de dicha solicitud de registro de servicio si dicho estado de cuenta se ha establecido como inválido,

en el que, en respuesta a que dicha solicitud a ser registrado en un servicio de dicho primer servidor (300) sea autorizada, se realiza una solicitud adicional por el usuario (100) a través de un navegador (101) para realizar una operación relacionada con dicha cuenta en el primer servidor (300), comprendiendo el método además:

- determinación, por el primer servidor (300), de qué entrada en un esquema de jerarquía definido por la cuenta se corresponde con dicha operación solicitada;
- solicitud, por el primer servidor (300), al segundo servidor (200), del estado de operación definido por el usuario (100) sobre dicha entrada;
- inicialización de un segundo intercambio de credenciales entre el primer servidor (300) y el segundo servidor (200);
- evaluación, por el segundo servidor (200), de un estado de entrada del esquema desde una raíz de dicho esquema de jerarquía a dicha entrada;
- envío, por el segundo servidor (200), de un resultado de la evaluación al primer servidor (300); y
- toma de una decisión, por el primer servidor (300), al menos usando dicho resultado recibido para permitir o bloquear dicha operación solicitada.

2. Un método implementado en ordenador de acuerdo con la reivindicación 1, que comprende la notificación, por dicho segundo servidor (200) al usuario (100) en caso de que dicha solicitud para ser registrado en un servicio de dicho primer servidor (300) se rechace.

3. Un método implementado en ordenador de acuerdo con la reivindicación 2, en el que dicha notificación comprende una de entre un envío de un Servicio de Mensajes Cortos (SMS), un envío de un e-mail, un envío de un mensaje mediante una aplicación de mensajería de teléfono inteligente, un resalte o notificación en dicho segundo programa dedicado (102) de dicho dispositivo informático de usuario.

4. Un método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicho estado de cuenta se establece como válido o como inválido un cierto período de tiempo.

5. Un método implementado en ordenador de acuerdo con la reivindicación 1, en el que se usa un segundo factor de autenticación dentro de la respuesta de dicho estado de entrada del esquema si dicho estado de entrada del esquema se establece como válido.

6. Un método implementado en ordenador de acuerdo con la reivindicación 5, en el que dicho segundo factor de

autenticación comprende:

- el envío, por dicho segundo servidor (200) al primer servidor (300), de una palabra clave de un uso (OTP);
- solicitud, por el primer servidor (300) al usuario (100), de una OTP que el usuario (100) va a usar como segundo factor temporal;
- recuperación, por el usuario (100), de dicho segundo factor temporal OTP solicitado a través de dicho segundo programa dedicado (102) y su envío adicional al primer servidor (300); y
- comprobación, por el primer servidor (300), si la OTP recibida desde el segundo servidor (200) y el segundo factor OTP temporal recibido desde el usuario coinciden, para autorizar o rechazar dicha solicitud para dicho servicio.

7. Un método implementado en ordenador de acuerdo con la reivindicación 6, en el que el primer servidor (300) comprende: permitir dicha operación si dichas OTP coinciden, o bloquear dicha operación si dichas OTP no coinciden.

8. Un método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicha etapa de evaluación se realiza para cada etapa hallada hasta alcanzar la entrada del esquema.

9. Un método implementado en ordenador de acuerdo con la reivindicación 1, en el que dicha solicitud para ser registrado en un servicio y/o dicha solicitud para realizar una operación se registran para proporcionar estadísticas.

10. Un programa de ordenador que comprende medios de código de programa de ordenador adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, una puerta lógica programable en campo (FPGA), un circuito integrado de aplicación específica, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

11. Un producto de programa de ordenador de acuerdo con la reivindicación 10, que comprende adicionalmente medios de código de programa adaptados para realizar un segundo factor de autenticación de acuerdo con el método de la reivindicación 6.

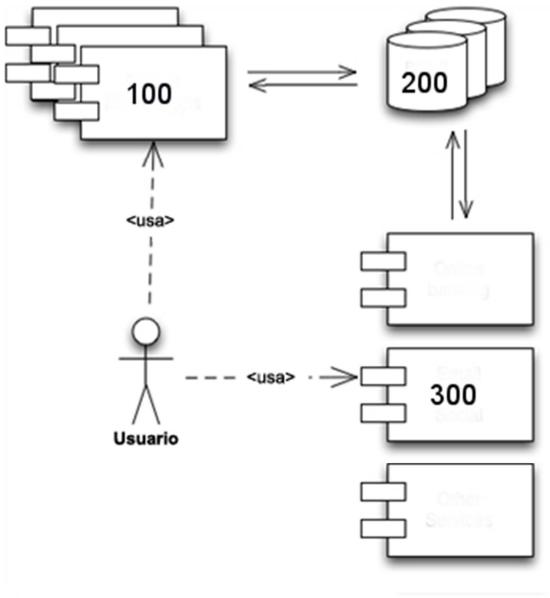

Figura 1

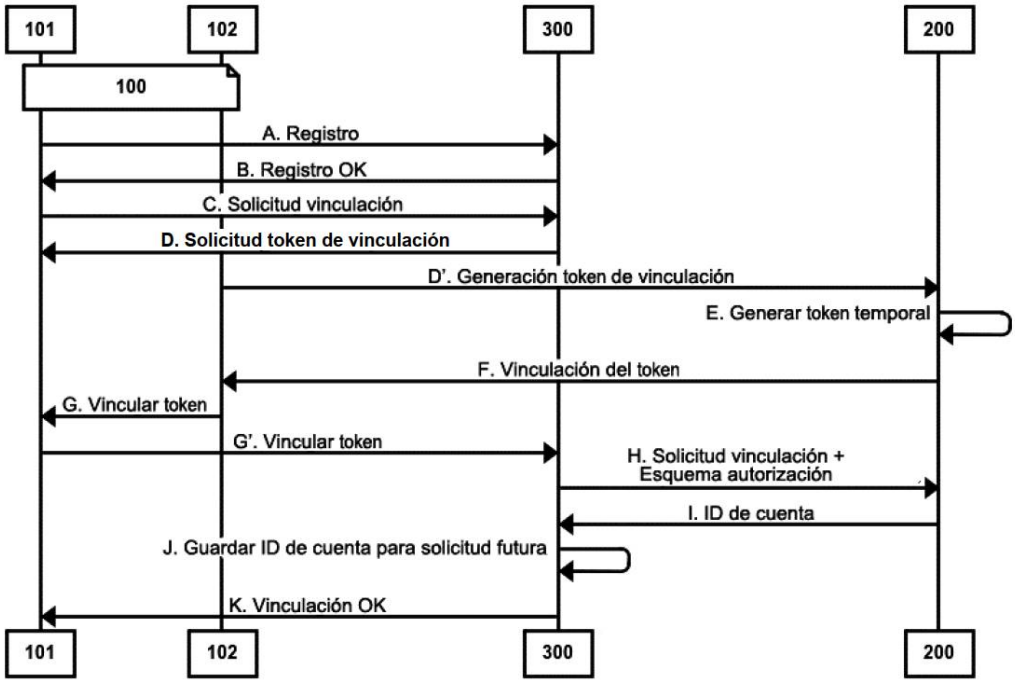

Figura 2

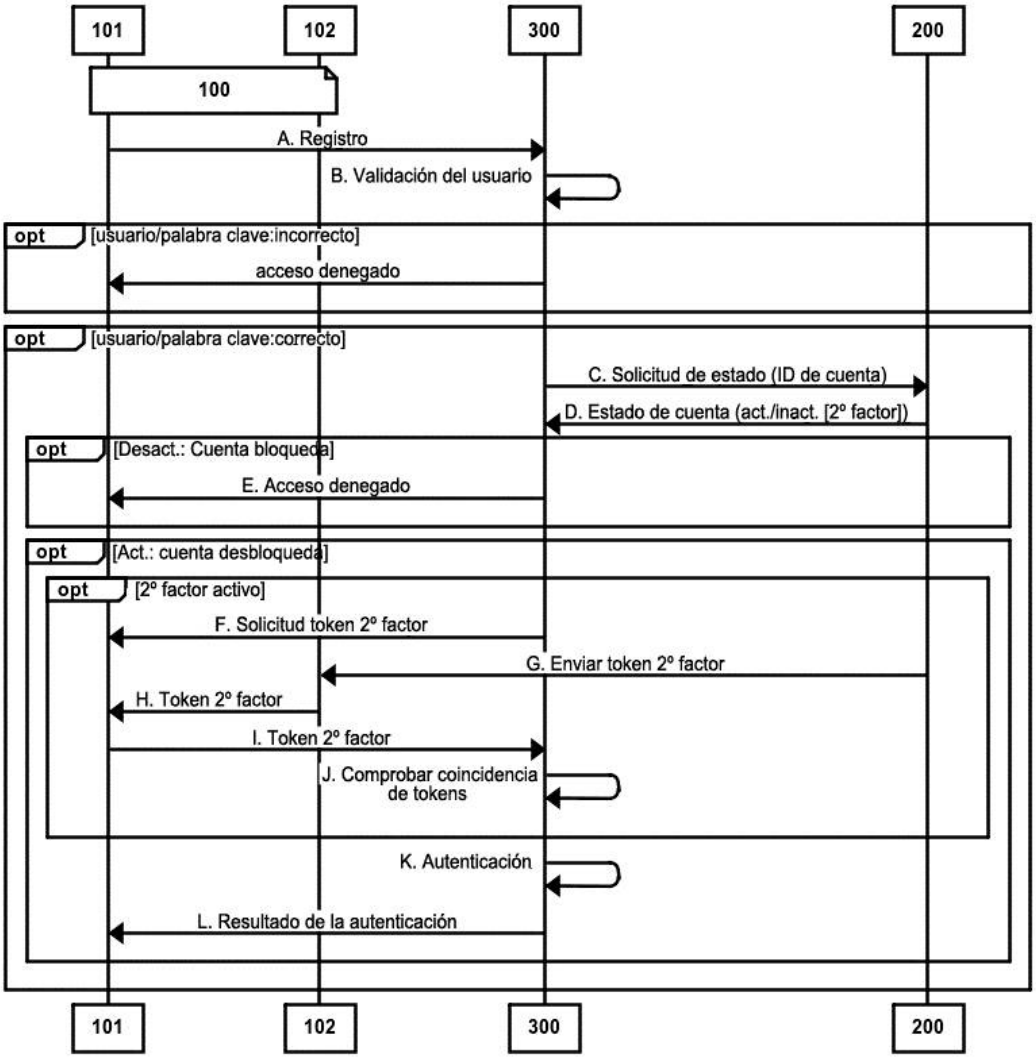
101
102
300
200
100
A. Registro
B. Validación del usuario
opt
[usuario/palabra clave:incorrecto]
acceso denegado
opt
[usuario/palabra clave:correcto]
C. Solicitud de estado (ID de cuenta)
D. Estado de cuenta (act./inact. [2º factor])
opt
[Desact.: Cuenta bloqueda]
E. Acceso denegado
opt
[Act.: cuenta desbloqueda]
opt
[2º factor activo]
F. Solicitud token 2º factor
G. Enviar token 2º factor
H. Token 2º factor
I. Token 2º factor
J. Comprobar coincidencia de tokens
K. Autenticación
L. Resultado de la autenticación
101
102
300
200

Figura 3

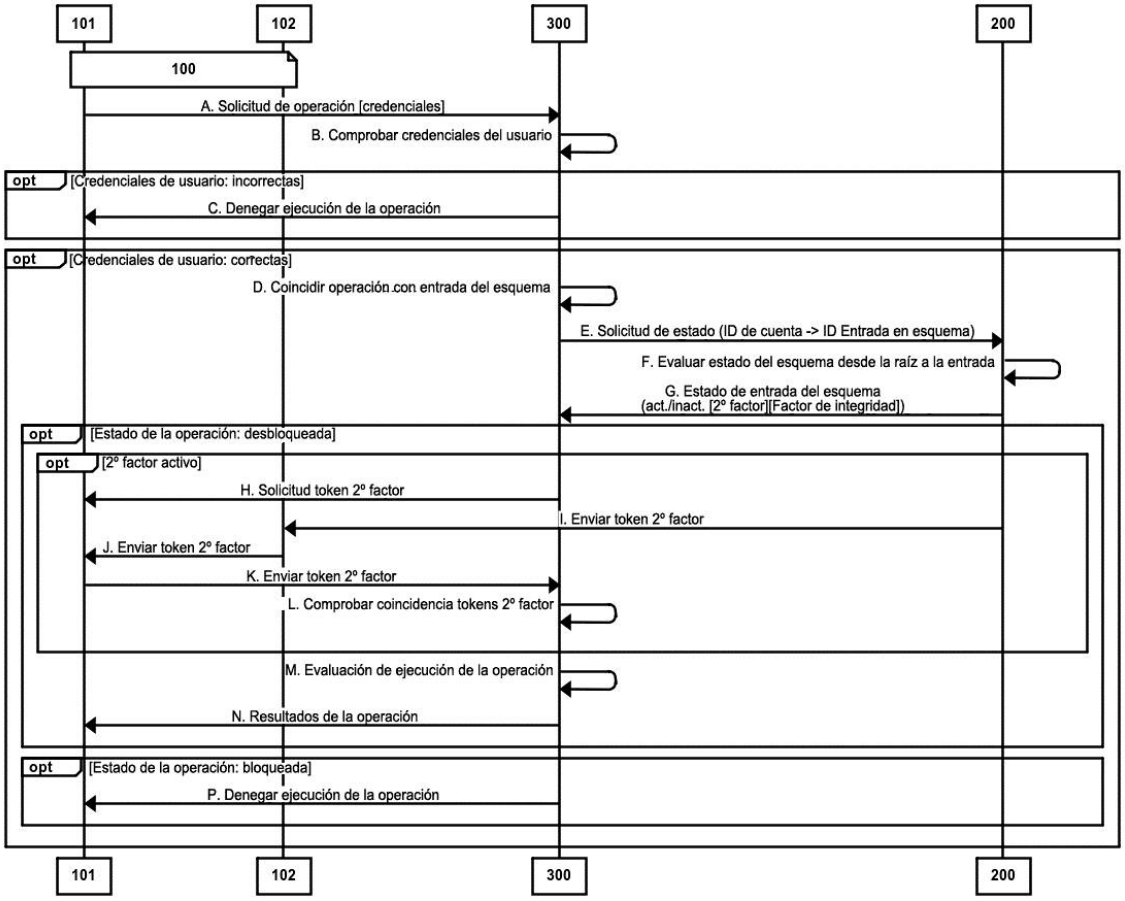
101
102
300
200
100
A. Solicitud de operación [credenciales]
B. Comprobar credenciales del usuario
opt
[Credenciales de usuario: incorrectas]
C. Denegar ejecución de la operación
opt
[Credenciales de usuario: correctas]
D. Coincidir operación con entrada del esquema
E. Solicitud de estado (ID de cuenta -> ID Entrada en esquema)
F. Evaluar estado del esquema desde la raíz a la entrada
G. Estado de entrada del esquema
(act./inact. [2º factor][Factor de integridad])
opt
[Estado de la operación: desbloqueada]
opt
[2º factor activo]
H. Solicitud token 2º factor
I. Enviar token 2º factor
J. Enviar token 2º factor
K. Enviar token 2º factor
L. Comprobar coincidencia tokens 2º factor
M. Evaluación de ejecución de la operación
N. Resultados de la operación
opt
[Estado de la operación: bloqueada]
P. Denegar ejecución de la operación
101
102
300
200

Figura 4