(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 669 276**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.03.2014 E 14159374 (9)**

(97) Fecha y número de publicación de la concesión europea: **02.05.2018 EP 2779572**

(54) Título: **Sistema y método para controlar intentos de autenticación**

(30) Prioridad:

14.03.2013 US 201313827201

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.05.2018

(73) Titular/es:

PALANTIR TECHNOLOGIES, INC. (100.0%)
100 Hamilton Avenue Suite 300
Palo Alto, California 94301, US

(72) Inventor/es:

CASTELLUCCI, RYAN;
GETTINGS, NATHAN y
BELKNAP, GEOFF

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Sistema y método para controlar intentos de autenticación

Campo de la invención

La presente descripción se refiere en general a la seguridad del sistema informático y, más específicamente, a un sistema y método para monitorizar intentos de autenticación.

Descripción de la técnica relacionada

Los usuarios remotos pueden normalmente acceder a una red de área local (LAN) a través de un servicio de red privada virtual (VPN). Para acceder a la LAN, un usuario remoto generalmente se autentica con el servicio VPN al proporcionar una combinación única de nombre de usuario y contraseña. Una vez autenticado, el usuario puede acceder a la LAN como si el usuario fuera local en la LAN. Más específicamente, un usuario que accede a la LAN a través del servicio VPN tiene la autoridad para ver y modificar activos dentro de la LAN, como documentos y correos electrónicos, como si el usuario fuera local de la LAN.

Típicamente, cada intento de autenticación realizado por un usuario para acceder a la LAN se registra. Los auditores pueden ver los registros de autenticación para identificar y abordar la actividad de autenticación sospechosa. Sin embargo, tal auditoría no ocurre en tiempo real. Por lo tanto, es posible que las actividades sospechosas no se solucionen a tiempo, lo que da como resultado un compromiso de seguridad de la LAN. Además, la actividad que puede parecer sospechosa para un auditor a menudo es una actividad legítima en nombre de los usuarios que intentan acceder a la LAN. Sin embargo, debido a que los registros de autenticación no indican ningún contexto relacionado con los intentos de autenticación, se requiere que un auditor investigue cada intento de autenticación que parezca sospechoso. Dichas investigaciones consumen mucho tiempo y pueden distraer a los auditores de investigar actividades sospechosas que tienen verdaderamente naturaleza maliciosa.

Como lo anterior ilustra, lo que se necesita en la técnica es un mecanismo más robusto y eficiente para rastrear y monitorear los intentos de inicio de sesión en un entorno seguro.

Se hace referencia a Ashraf Anonymous “Proteja su cuenta de Google (Gmail) habilitando las notificaciones de SMS (mensajes de texto) para actividades sospechosas [Sugerencia]” de http://dottech.org/94405/how-to-setup-text-messagesms- google-notification-for-sospechos-activity /.

Resumen de la invención

Los aspectos de la invención se proporcionan mediante las reivindicaciones adjuntas a la misma.

Una realización de la invención es un método implementado por ordenador para notificar a los usuarios cuando se realizan intentos para iniciar sesión en un entorno seguro. El método incluye las etapas para determinar que un usuario ha realizado un intento de autenticación y determinar que se ha realizado un intento de autenticación con credenciales pertenecientes a un usuario, determinar que una notificación que indique que se ha realizado el intento de autenticación debe transmitirse al usuario, y transmitir la notificación al usuario.

Una ventaja del enfoque/mecanismo divulgado es que, debido a que un usuario es notificado cada vez que el usuario supuestamente realiza un intento de autenticación, el usuario puede alertar a las partes relevantes si recibe una notificación que no se correlaciona con su actividad de autenticación. Tal mecanismo de notificación permite la alerta en tiempo real de actividades sospechosas, que luego pueden abordarse rápidamente.

Breve descripción de las figuras

De modo que la manera en que las características citadas de la presente invención se pueden entender en detalle, puede tenerse una descripción más particular de la invención, brevemente resumida anteriormente, con referencia a las realizaciones, algunas de las cuales se ilustran en los dibujos adjuntos. Sin embargo, debe observarse que los dibujos adjuntos ilustran solo realizaciones típicas de esta invención y, por lo tanto, no deben considerarse limitativos de su alcance, ya que la invención puede admitir otras realizaciones igualmente efectivas.

La figura 1 ilustra un sistema configurado para seguir los intentos de autenticación de usuario en un entorno seguro, de acuerdo con una realización de la invención;

La Figura 2 ilustra una vista más detallada del motor de notificación de la Figura 1, de acuerdo con una realización de la invención;

La Figura 3 es un diagrama de flujo de las etapas del método para notificar a los usuarios de intentos de autenticación en un entorno seguro, de acuerdo con una realización de la invención; y

La Figura 4 es un sistema ejemplar configurado para implementar uno o más aspectos de la invención.

Descripción de realizaciones de ejemplo

La figura 1 ilustra un sistema 100 configurado para rastrear intentos de autenticación de usuario en un entorno seguro, de acuerdo con una realización de la invención. Como se muestra, el sistema 100 incluye, sin limitación, el motor 102 de autenticación, el motor 104 de notificación y la base de datos 106 de usuario.

El motor 102 de autenticación es un motor de software que permite a los usuarios del sistema 100 autenticarse y acceder al sistema 100 de una manera segura. En una realización, el motor 102 de autenticación proporciona un servicio de red privada virtual (VPN). Una vez autenticado, un usuario puede acceder a cualquier servicio o activo disponible en el sistema 100. En una realización, cada intento de autenticación, exitoso o no, realizado por un usuario es registrado por el motor 102 de autenticación en un registro de autenticación. Tal registro puede escribirse en una unidad de memoria para su persistencia y puede ser accedido por los usuarios del sistema 100 o por diferentes módulos de software del sistema 100.

El motor 104 de notificación supervisa los intentos de autenticación supuestamente realizados por usuarios particulares y luego notifica a los usuarios de los intentos para que los usuarios puedan verificar que los intentos de autenticación fueron válidos. Para cada intento de autenticación, el motor 104 de notificación determina la identificación del usuario asociada con la autenticación intentada en base a la información especificada por el motor 102 de autenticación. El motor 104 de notificación accede entonces a la base 106 de datos del usuario para identificar al usuario particular asociado con la identificación del usuario. En base a un grupo de reglas de notificación, el motor 104 de notificación determina entonces si se debe enviar una notificación que indique que se ha realizado el intento de autenticación al usuario asociado con la identificación del usuario. Si se debe enviar una notificación, el motor 104 de notificación transmite una notificación al usuario. Se describen detalles más específicos relacionados con el funcionamiento del motor 104 de notificación junto con la Figura 2 a continuación.

La figura 2 ilustra una vista más detallada del motor 104 de notificación de la figura 1, de acuerdo con una realización de la invención. Como se muestra, el motor 104 de notificación incluye, sin limitación, un módulo 202 de supervisión de inicio de sesión, un módulo 204 de notificación basado en reglas y reglas 206 de notificación.

En funcionamiento, el módulo de monitorización de inicio de sesión 202 accede periódicamente al motor 102 de autenticación para identificar cualquier nuevo intento de autenticación que puedan haber realizado los usuarios del sistema 100. En una realización, el motor 104 de notificación solicita dicha información del motor 102 de autenticación a través de un protocolo de comunicación previamente identificado entre el motor 102 de autenticación y el motor 105 de notificación. En otra realización, el motor 104 de notificación supervisa los inicios de sesión leyendo un registro de autenticación mantenido por el motor 102 de autenticación que especifica cada intento de autenticación realizado por los usuarios.

Cuando el módulo 202 de inicio de sesión identifica un nuevo intento de autenticación, el módulo 202 de supervisión de inicio de sesión informa al módulo 204 de notificación basado en reglas del nuevo intento de autenticación. En respuesta, el módulo 204 de notificación basado en reglas determina las credenciales, es decir, la identificación del usuario, con la que se realizó el intento de autenticación. En una realización, el módulo 204 de notificación basado en reglas extrae la identificación del usuario de la información recuperada del motor 102 de autenticación. El módulo 204 de notificación basado en reglas identifica luego qué usuarios, si los hay, del sistema 100 deberían ser notificados del intento de autenticación. Tal determinación se basa en las reglas 206 de notificación.

Las reglas 206 de notificación incluyen reglas diferentes que son evaluadas por el módulo 204 de notificación basado en reglas para determinar si deben transmitirse las notificaciones de un intento de autenticación y, en caso afirmativo, a qué usuarios deben transmitirse tales notificaciones. Un ejemplo de una regla incluida en las reglas 206 de notificación es una lista blanca que especifica una lista de usuarios, en el que no es necesario notificar a cada usuario de la lista cuando el usuario realiza un intento de autenticación en el sistema 100.

De manera similar, una lista blanca podría basarse en una lista de redes informáticas (por ejemplo, identificadas por dirección IP o nombre de dominio) a partir de la cual los intentos de acceso no deberían dar como resultado una notificación. En otro escenario, una regla podría especificar que solo se envíe un mensaje de notificación para acceder a intentos desde una ubicación particular, incluso si se realizan múltiples intentos durante el transcurso de un día.

Otro ejemplo de una regla incluida en las reglas 206 de notificación es una regla configurable que especifica si las notificaciones solo deben transmitirse si un intento de autenticación fue exitoso. Otro ejemplo de una regla incluida en las reglas 206 de notificación es la regla de notificación multiusuario que especifica una lista de usuarios de alto riesgo, donde, si se realiza un intento de autenticación utilizando las credenciales de un usuario de alto riesgo, se incluye una lista de usuarios adicionales. los usuarios especificados por la regla deben ser notificados. Otro ejemplo de una regla incluida en las reglas 206 de notificación es una regla basada en la ubicación que especifica una distancia umbral entre una ubicación desde la cual se realizó un intento de autenticación anterior usando las credenciales y una ubicación desde la cual se realizó el intento de autenticación actual que debería desencadenar la transmisión de una notificación al usuario.

Todavía otro ejemplo de una regla incluida en las reglas 206 de notificación es una regla basada en el tiempo que especifica un período de tiempo en un día durante el cual las notificaciones no se deben transmitir al usuario. Cualquier otra regla que dicte la transmisión de notificación a los usuarios cuando se realiza un intento de autenticación está dentro del alcance de la presente invención. Otra regla podría basarse en un análisis de un patrón de intentos de inicio de sesión, como una regla de notificación que evalúa la latencia entre dos intentos de acceso. Por ejemplo, si un inicio de sesión actual se originó desde una dirección IP en California, mientras que un intento de acceso anterior se originó desde una Dirección IP en Nueva York, una regla podría evaluar el tiempo entre los dos intentos. En tal caso, se esperaría cierta latencia de red del solicitante (suponiendo que ambos intentos fueran legítimos). Por lo tanto, si la regla determina que el tiempo entre los intentos de acceso no excedió una cantidad esperada (posiblemente porque la solicitud se enruta a través de varios proxies), entonces la regla podría desencadenar un mensaje de notificación. Las reglas más sofisticadas podrían basarse en el aprendizaje automático o técnicas de agrupamiento que desarrollen patrones de intentos de acceso esperados para un usuario o clase de usuarios determinados.

En una realización, las reglas 206 de notificación son configurables de manera que un administrador del sistema del sistema 100 puede agregar, eliminar, habilitar y deshabilitar reglas. En una realización, los usuarios del sistema 100 se dividen en diferentes grupos. En dicha realización, para un intento de autenticación realizado usando una credencial que pertenece a un usuario particular, el motor 204 de notificación basado en reglas evalúa solo un subgrupo predeterminado de las reglas 206 de notificación asociadas con el grupo al que pertenece el usuario.

En funcionamiento, para cada nuevo intento de autenticación, el módulo 204 de notificación basado en reglas identifica el grupo de reglas relevantes incluidas en las reglas 206 de notificación que deberían evaluarse para determinar qué usuarios del sistema 100, si los hubiere, deberían ser notificados del intento de autenticación. El módulo 204 de notificación basado en reglas luego evalúa cada regla en el grupo de reglas relevantes. En una realización, el módulo 204 de notificación basado en reglas determina que la notificación debe transmitirse solo si se cumple cada regla en el grupo de reglas relevantes. En una realización alternativa, el módulo 204 de notificación basado en reglas determina que la notificación se debe transmitir incluso si se cumple alguna de las reglas en las reglas relevantes del grupo relevante.

Para evaluar una regla particular, el módulo 204 de notificación basado en reglas determina si la regla particular se satisface, necesitando así la transmisión de una notificación al menos al usuario asociado con las credenciales con las que se realizó el intento de autenticación. Por ejemplo, para la regla basada en la ubicación discutida anteriormente, el módulo 204 de notificación basado en reglas determina si la diferencia entre la ubicación de un intento de autenticación anterior y la ubicación del intento de autenticación actual es mayor que la distancia umbral especificada en la ubicación basada en regla. Si la distancia es mayor que la distancia umbral, entonces el módulo 204 de notificación basado en reglas determina que se debe transmitir una notificación. Como otro ejemplo, para la regla de notificación multiusuario, el módulo 204 de notificación basado en reglas determina si el usuario cuyas credenciales se usaron para hacer el intento de inicio de sesión se incluye en la lista de usuarios de alto riesgo. Si el usuario está incluido en la lista de usuarios de alto riesgo, el módulo 204 de notificación basado en reglas determina que se debe transmitir una notificación al usuario, así como a cada uno de los usuarios adicionales incluidos en la lista de usuarios adicionales especificados por la regla.

Una vez que el módulo 204 de notificación basado en reglas determina que las notificaciones del intento de autenticación deben ser transmitidas y los usuarios que se va a notificar son identificados, el módulo 204 de notificaciones basado en reglas accede a la base 106 de datos del usuario para recuperar un identificador diferente asociado con cada usuario a ser notificado. En una realización, el identificador de notificación asociado con un usuario particular es una dirección de correo electrónico del usuario al que se va a transmitir la notificación. En otra realización, el identificador de notificación asociado con un usuario particular es un número de teléfono del usuario al que se va a transmitir la notificación a través de un sistema de mensajes cortos (SMS). Las notificaciones se transmiten a cada usuario para que se le notifique mediante el identificador de notificación asociado. Además, la notificación en sí misma puede proporcionarle a un usuario (u otra persona) una variedad de información. Por ejemplo, además de notificar al usuario del intento de acceso en sí, un mensaje de notificación podría indicar la ubicación del intento de acceso como parte de la notificación enviada al usuario. Es decir, el mensaje podría indicar que un intento de acceso se originó desde una ubicación particular. Por ejemplo, una ubicación geográfica de un intento de acceso podría correlacionarse con una dirección IP de origen de una solicitud de conexión VPN. Además, la notificación podría indicar qué regla (o reglas) dio como resultado que se envíe un mensaje de notificación dado, por ejemplo, “estás recibiendo esta notificación según la siguiente regla de notificación”. Por supuesto, la cantidad de información también se puede adaptar al identificador de notificación. Por ejemplo, un correo electrónico podría incluir una descripción detallada del intento de acceso que activó el mensaje de notificación. Al mismo tiempo, un mensaje SMS al mismo usuario podría simplemente proporcionar una alerta en cuanto a la ocurrencia de un intento de acceso que desencadena el mensaje SMS, dejándolo al destinatario para obtener más detalles de otra fuente.

La figura 3 es un diagrama de flujo de las etapas del método para notificar a los usuarios de inicios de sesión realizados en un entorno seguro, de acuerdo con una realización de la invención. Aunque las etapas del método se describen junto con el sistema para las Figuras 1 y 2, los expertos en la técnica entenderán que cualquier sistema configurado para realizar las etapas del método, en cualquier orden, está dentro del alcance de la invención.

Un método 300 comienza en la etapa 302, en el que el módulo 202 de supervisión de inicio de sesión supervisa el motor 102 de autenticación para identificar cualquier nuevo intento de autenticación realizado por los usuarios del sistema 100.

En la etapa 304, si no se ha realizado un nuevo intento de autenticación hecho, entonces el método 300 vuelve a la etapa 302. Sin embargo, si se ha realizado un nuevo intento de autenticación, entonces el método 300 pasa a la etapa 306.

En la etapa 306, el módulo 204 de notificación basado en reglas determina las credenciales (identificación del usuario) con las que se realizó el intento de autenticación. En una realización, el módulo 204 de notificación basado en reglas extrae la identificación del usuario de la información recuperada del motor 102 de autenticación. En la etapa 308, el módulo 204 de notificación basado en reglas identifica un grupo de reglas relevantes incluidas en las reglas 206 de notificación que deberían evaluarse para determinar qué usuarios del sistema 100, en caso de haberlos, deberían ser notificados del intento de autenticación. En una realización, el grupo de reglas relevantes se determina basándose en un grupo particular al que pertenece el usuario, en el que cada grupo de usuarios se asocia con un grupo de reglas relevantes incluidas en las reglas 206 de notificación.

En la etapa 310, el módulo 204 de notificación basado en reglas evalúa a continuación cada regla en el grupo de reglas relevantes. De nuevo, para evaluar una regla particular, el módulo 204 de notificación basado en reglas determina si la regla particular se satisface, por lo que se necesita la transmisión de una notificación al menos al usuario que realizó el intento de autenticación. En la etapa 312, el módulo 204 de notificación basado en reglas determina si debe transmitirse una notificación que indique que se ha realizado el intento de autenticación. Si es así, entonces el método avanza a la etapa 314. En el paso 314, el módulo 204 de notificación basado en reglas accede a la base 106 de datos de usuario para recuperar un identificador de notificación asociado con un usuario que se va a notificar. La notificación se transmite luego al usuario a través del identificador de notificación asociado.

La figura 4 es un sistema 400 ejemplar configurado para implementar uno o más aspectos de la invención. Como se muestra, el sistema 400 incluye, sin limitación, una memoria 402 del sistema, una memoria 404 externa, una unidad de procesamiento 406 central (CPU), un dispositivo 410 de entrada y un dispositivo 412 de visualización. La memoria 402 del sistema incluye el motor 104 de notificación previamente descrito aquí. La memoria 402 del sistema es un espacio de memoria, normalmente una memoria de acceso aleatorio (RAM), que almacena temporalmente programas de software que se ejecutan dentro del sistema 400 en cualquier momento dado. La CPU 406 ejecuta una secuencia de instrucciones almacenadas asociadas y/o transmitidas desde los diversos elementos en el sistema 400 informático. La memoria 404 externa es un dispositivo de almacenamiento, por ejemplo, un disco duro, para almacenar datos asociados con el motor 104 de notificación. El dispositivo 410 de entrada es un dispositivo de entrada controlado por el usuario final, por ejemplo, un mouse o teclado, que permite a un usuario manipular diversos aspectos del motor 104 de notificación. El dispositivo 412 de visualización puede ser un tubo de rayos catódicos (CRT), una pantalla de cristal líquido (LCD) o cualquier otro tipo de dispositivo de visualización.

Una estrategia/mecanismo revelado de ventaja es que, debido a que se notifica a un usuario cada vez que el usuario supuestamente realiza un intento de autenticación, el usuario puede alertar a las partes pertinentes si recibe una notificación que no se correlaciona con su actividad de autenticación. Tal mecanismo de notificación permite la alerta en tiempo real de actividades sospechosas, que luego pueden abordarse rápidamente. Además, el mecanismo de notificación proporciona un contexto adicional a los auditores cuando se investigan los registros de autenticación, lo que resulta en investigaciones más eficientes. Más específicamente, si, después de recibir una notificación, un usuario indica que un intento de autenticación, que parece ser sospechoso, fue legítimo, entonces el auditor no necesariamente tiene que perder tiempo investigando ese intento de autenticación.

Una realización de la invención puede implementarse como un producto de programa para uso con un sistema informático. El(los) programa(s) del producto del programa definen las funciones de las realizaciones (que incluyen los métodos descritos en este documento) y puede estar contenido en una variedad de medios de almacenamiento legibles por ordenador. Los medios ilustrativos de almacenamiento computarizables incluyen, pero no están limitados a: (i) medios de almacenamiento no grabables (por ejemplo, dispositivos de memoria de solo lectura dentro de un ordenador como discos de CD-ROM legibles por una unidad de CD-ROM, memoria flash, chips ROM) o cualquier tipo de memoria semiconductora no volátil de estado sólido) en la que la información se almacena permanentemente; y (ii) medios de almacenamiento de escritura (por ejemplo, disquetes dentro de una unidad de disquete o unidad de disco duro o cualquier tipo de memoria de semiconductor de acceso en rand de estado sólido) en la que se almacena información alterable.

La invención se ha descrito anteriormente con referencia a realizaciones específicas. Los expertos en la técnica, sin embargo, comprenderán que se pueden realizar diversas modificaciones y cambios sin apartarse del alcance de la invención tal como se establece en las reivindicaciones adjuntas. La descripción y los dibujos anteriores son, por consiguiente, a considerar en un sentido ilustrativo más que restrictivo. Por lo tanto, el alcance de las realizaciones de la presente invención se establece en las reivindicaciones que siguen.

REIVINDICACIONES

1. Un método implementado por ordenador para notificar a los usuarios cuando se intenta iniciar sesión en un entorno seguro, el método comprende:

determinar (304) que se ha realizado un intento de autenticación con credenciales que pertenecen a un usuario;

determinar (312) que se debe transmitir al usuario una notificación que indique que se ha realizado el intento de autenticación; y

transmitir (314) la notificación al usuario,

en el que determinar que la notificación debe transmitirse comprende evaluar un grupo de reglas (206) de notificación para determinar si se cumple al menos una de las reglas de notificación y en el que una primera regla de notificación en el grupo de las reglas de notificación especifica una lista de usuarios a los que las notificaciones no deben transmitirse, y la evaluación de la primera regla de notificación comprende determinar si el usuario está incluido en la lista de usuarios.

2. El método de la reivindicación 1, en el que una primera regla de notificación en el grupo de reglas de notificación especifica una distancia umbral, y la evaluación de la primera regla de notificación comprende determinar si una distancia entre una ubicación desde la cual se realizó un intento de autenticación previa con las credenciales el usuario y una ubicación desde la cual se realizó el intento de autenticación están por debajo de la distancia umbral.

3. El método de la reivindicación 1 o 2, en el que una primera regla de notificación en el grupo de reglas de notificación especifica un período de tiempo en un día durante el cual las notificaciones no deberían transmitirse, y la evaluación de la primera regla de notificación comprende determinar si una hora actual no cae dentro del período de tiempo.

4. El método de cualquier reivindicación precedente, en el que determinar que el intento de autenticación se ha realizado comprende acceder a un registro de inicio de sesión mantenido por un servicio (102) de autenticación, en el que el registro de inicio de sesión indica al menos el intento de autenticación.

5. El método de cualquier reivindicación precedente, que transmite la notificación al usuario comprende recuperar un identificador de notificación asociado con el usuario desde un repositorio (106) de información de usuario y transmitir la notificación al usuario a través del identificador de notificación, en el que el identificador de notificación comprende un número de teléfono asociado con el usuario y la transmisión de la notificación al usuario comprende además la transmisión de un mensaje corto al número de teléfono a través de un sistema de mensajes cortos.

6. El método de cualquier reivindicación precedente, que comprende además determinar que el usuario pertenece a una primera categoría que incluye usuarios de alto riesgo, y transmitir la notificación a un usuario adicional.

7. Un programa de ordenador, opcionalmente almacenado en un medio (402) legible por ordenador, que comprende instrucciones que, cuando son ejecutadas por un procesador (406), hacen que el procesador notifique a los usuarios cuando se intenta iniciar sesión en un entorno seguro, realizando las etapas de cualquiera de las reivindicaciones 1 a 6.

8. Un sistema informático, que comprende una memoria (402) y un procesador (402) acoplado a la memoria y configurado para realizar las etapas de cualquiera de las reivindicaciones 1 a 6.

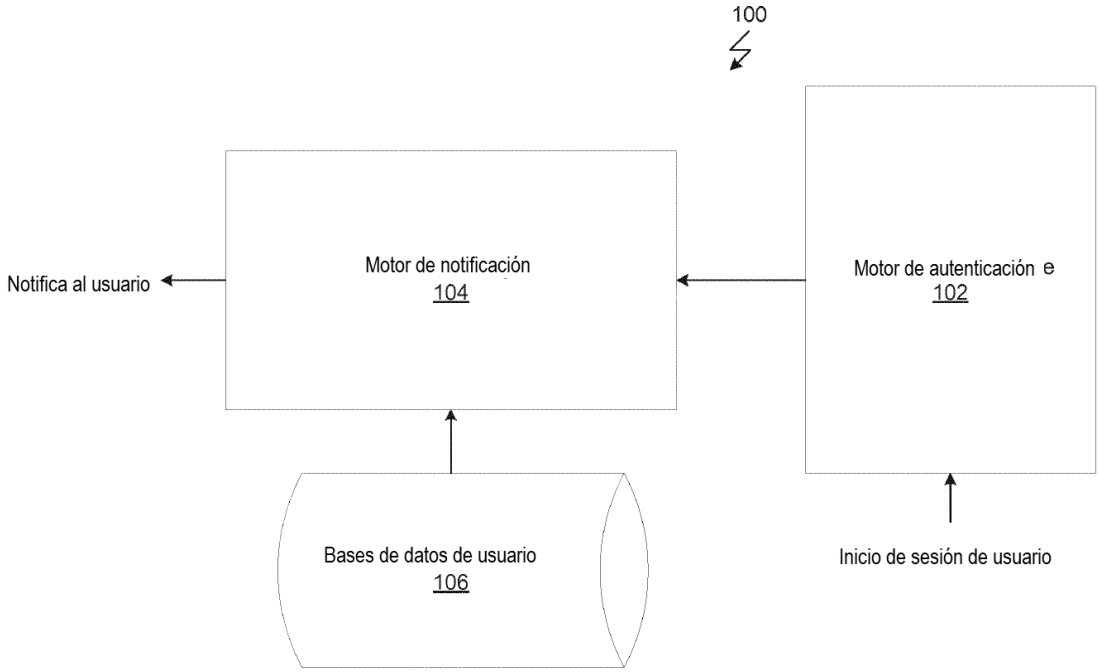
100
Motor de notificación
104
Motor de autenticación e
102
Notifica al usuario
Bases de datos de usuario
106
Inicio de sesión de usuario

FIGURA 1

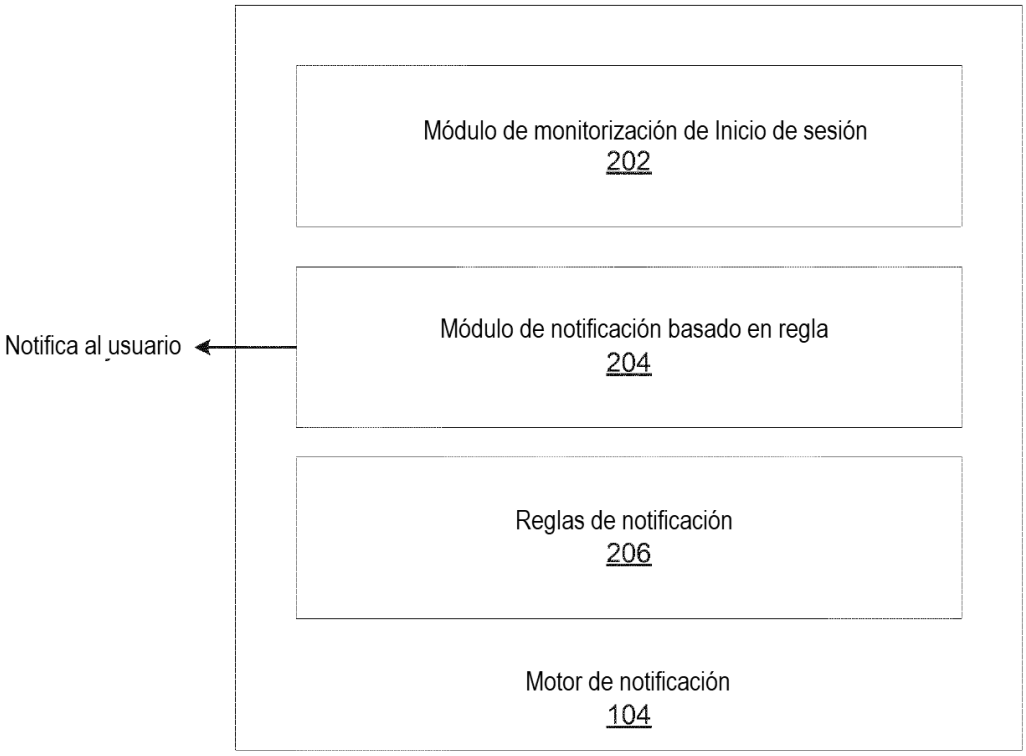
Módulo de monitorización de Inicio de sesión
202
Módulo de notificación basado en regla
204
Notifica al usuario
Reglas de notificación
206
Motor de notificación
104

FIGURA 2

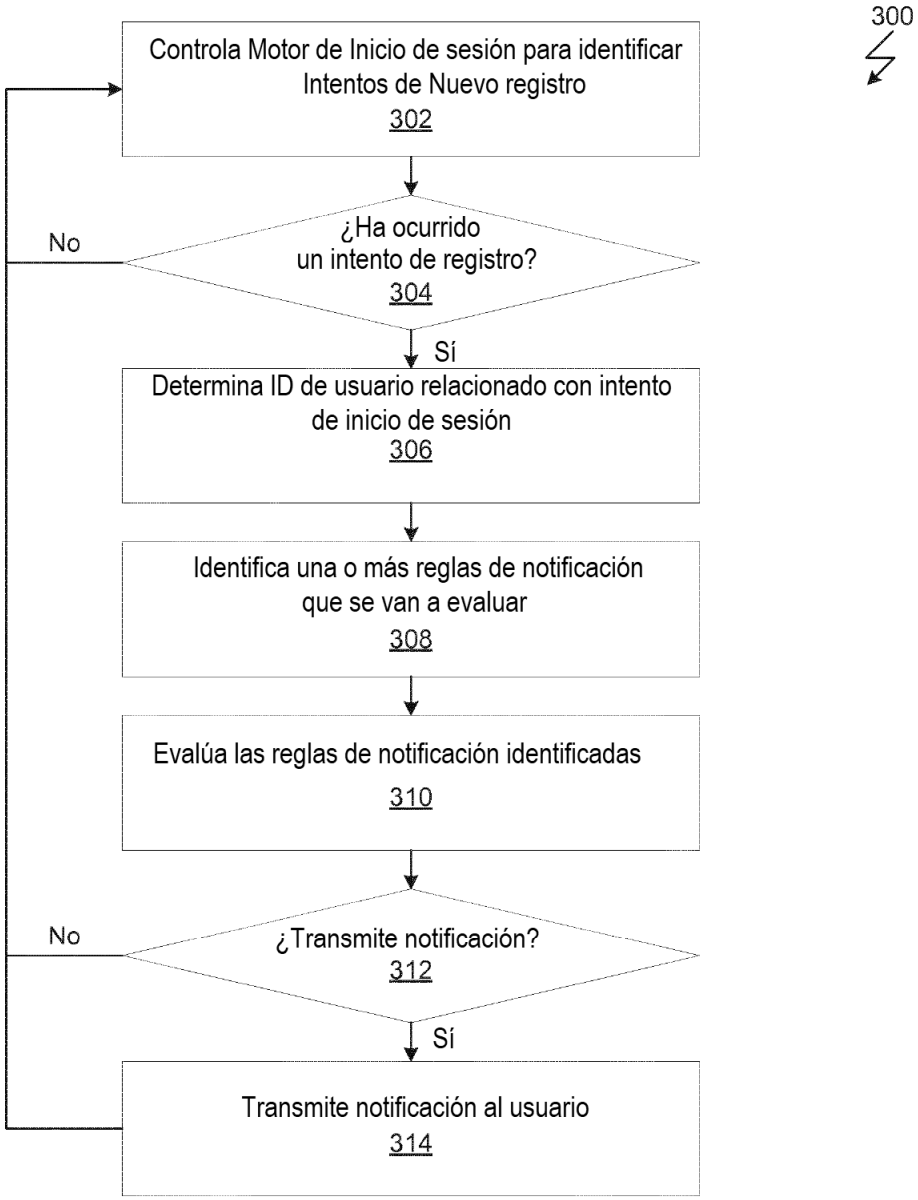
300
Controla Motor de Inicio de sesión para identificar Intentos de Nuevo registro
302
¿Ha ocurrido un intento de registro?
304
No
Sí
Determina ID de usuario relacionado con intento de inicio de sesión
306
Identifica una o más reglas de notificación que se van a evaluar
308
Evalúa las reglas de notificación identificadas
310
¿Transmite notificación?
312
No
Sí
Transmite notificación al usuario
314

FIGURA 3

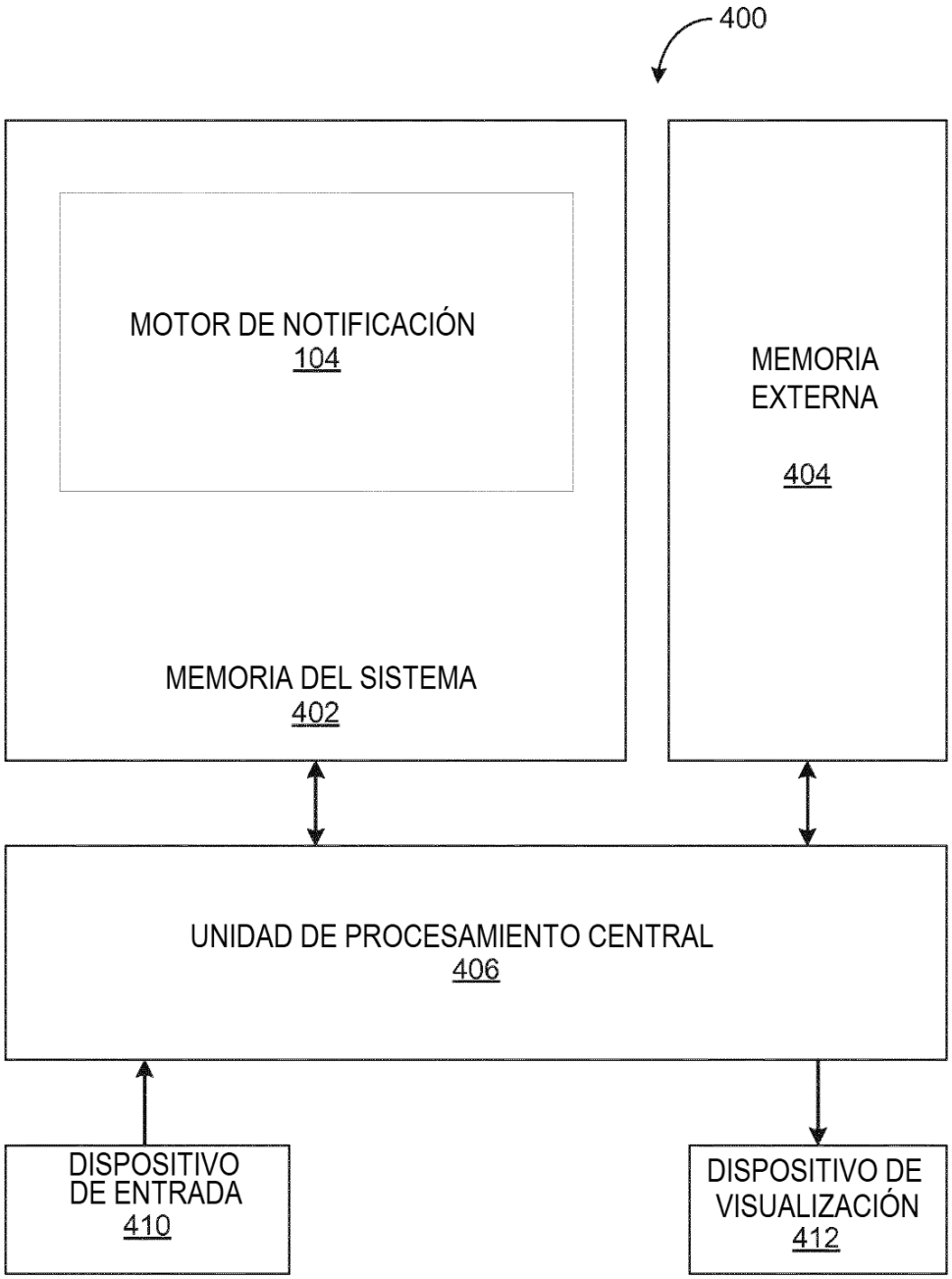
400
MOTOR DE NOTIFICACIÓN
104
MEMORIA DEL SISTEMA
402
MEMORIA
EXTERNA
404
UNIDAD DE PROCESAMIENTO CENTRAL
406
DISPOSITIVO
DE ENTRADA
410
DISPOSITIVO DE
VISUALIZACIÓN
412

FIGURA 4