(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 719 538**

(51) Int. CI.:

G06F 21/41 (2013.01)
H04L 29/06 (2006.01)
G06F 21/44 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.03.2016 PCT/FR2016/050482**

(87) Fecha y número de publicación internacional: **09.09.2016 WO16139427**

(96) Fecha de presentación y número de la solicitud europea: **03.03.2016 E 16714996 (2)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2019 EP 3265948**

(54) Título: **Transferencia segura de información de autenticación**

(30) Prioridad:

03.03.2015 FR 1551784

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.07.2019

(73) Titular/es:

WALLIX (100.0%)
250 Bis Rue du Faubourg Saint-Honoré
75008 Paris, FR

(72) Inventor/es:

ADDA, SERGE y
ZHOU, RAPHAËL

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Transferencia segura de información de autenticación

Campo de la invención

La presente invención se refiere al campo de los servidores de aplicación, y más particularmente de los procedimientos y sistemas de acceso a recursos aplicativos alojados en uno o varios servidores, por un usuario.

Estado de la técnica

Se conoce en particular en el estado de la técnica la solicitud de patente internacional WO 2014064686 que describe un sistema y procedimiento de autenticación segura basada en una pasarela intermediaria. Este documento divulga un sistema y un procedimiento de autenticación segura que facilita la mejora de la seguridad de una autenticación entre un cliente y un destino por medio de un módulo de autenticación novedoso en una pasarela intermediaria. Según la invención, el cliente puede conectarse a la pasarela intermediaria por medio de un protocolo nativo y proporciona informaciones de identificación de usuario a la pasarela intermediaria.

La invención facilita la conexión entre el cliente y el destino de modo que es inútil, para el usuario, estar en posesión de las informaciones de identificación de acceso de destino. La pasarela intermediaria puede conectarse eventualmente a un sistema de gestión de acceso privilegiado que puede proporcionar y/o almacenar informaciones de identificación de acceso de destino. Las informaciones de identificación de acceso de destino proporcionadas por la pasarela intermediaria facilitan la prevención contra un fallo en la seguridad del cliente que expone las informaciones de identificación de acceso de destino.

Inconvenientes de la técnica anterior

La solución propuesta por la solicitud WO2014064686 no se refiere explícitamente a un procedimiento de acceso seguro a aplicaciones sino solamente a recursos de infraestructura tales como un servidor o un enrutador. Esta solicitud se refiere al acceso a un destino, que corresponde expresamente a un servidor y no a una aplicación alojada por un servidor.

Solución aportada por la invención

El objeto de la presente invención no es solamente asegurar el acceso a un servidor, sino más precisamente asegurar el acceso a aplicaciones alojadas en un servidor, con el fin de permitir por ejemplo el uso en una cuenta compartida por varios usuarios manteniendo la imputabilidad de las acciones operadas bajo esta cuenta.

Para este propósito, la invención se refiere según su acepción más general a un procedimiento de conexión segura a una aplicación ejecutada en un servidor desde un equipo informático cliente, por un usuario que no dispone de los datos de autenticación de la cuenta declarada en dicha aplicación, comprendiendo dicha cuenta al menos una identidad ID_{proxy}, aplicación y datos de autenticación asociados, implementando un proxy [pasarela intermediaria] que comprende una memoria para el registro, para cada usuario declarado por una cuenta primaria que comprende al menos una identidad $ID_{usuario,}$ de la lista de los destinos $D_{recursos,\ cuentas}$ a la que tiene acceso, comprendiendo el procedimiento las etapas siguientes:

- apertura por el usuario de una conexión a un proxy por medio de un protocolo de administración nativo multicanal [SSH, RDP o ICA,...], con una primera identidad $ID_{usuario}$ para la apertura de una sesión multicanal primaria
- definición simultánea [en los parámetros de conexión] o secuencial [selección después de apertura de la conexión de entre una lista propuesta por el proxy] de la aplicación (destino).
- conexión del proxy al servidor de alojamiento de dicha aplicación seleccionada por medio del mismo protocolo de administración nativo multicanal [SSH, RDP o ICA,...] con una segunda identidad $ID_{proxy,\ servidor}$ para abrir una sesión multicanal secundaria
- registro temporal de una información $I_{relé}$ correspondiente al enlace entre dicha sesión primaria y dicha sesión secundaria
- ejecución en el servidor de un código informático [script, en español, secuencia de comandos] que abre un canal entre dicho servidor y dicho proxy, en el marco de dicha sesión secundaria,
- envío por dicho código en dicho canal de una petición que solicita, para dicha aplicación y dicha cuenta, los datos de autenticación [password, en español, contraseña]
- en respuesta a esta petición, transmisión por el proxy de estos datos de autenticación si el destino definido por dicha aplicación y dicha cuenta pertenece a la lista de los destinos $D_{recursos,\ cuentas}$ registrados para dicho usuario
- y ejecución de dicha aplicación y transmisión a dicha aplicación por dicho código de los datos usuarios o notificación de error si la cuenta no pertenece a dicha lista.

Una de las ventajas de este procedimiento es que luego la aplicación puede usarse gracias a la misma conexión que la que ha servido para el acceso a la pasarela.

Ventajosamente, el procedimiento incluye además una etapa de selección de un servidor de aplicación de entre una pluralidad de servidor que aloja la misma aplicación.

Según un modo de implementación particular, dicho código informático se registra en el servidor de aplicación.

Preferentemente, dicho código informático se registra por el proxy en dicho servidor de aplicación con un nombre de uso único.

Según una variante, dicho código informático registrado en el servidor de aplicación contiene un testigo de uso único transmitido con dicha petición.

Preferentemente, la aplicación puede usarse por dos usuarios diferentes que tienen como identidades $ID_{usuario\ A}$ e $ID_{usuario\ B}$. Para ello, cada una de las sesiones secundarias se ejecuta con una identidad diferente ($ID_{proxy,servidor\ A}$ e $ID_{proxy,servidor\ B}$). Estas identidades se eligen automáticamente por el proxy de entre las identidades configuradas de modo que nunca haya al mismo tiempo dos sesiones secundarias con la misma identidad.

Descripción detallada de un ejemplo no limitativo de realización

La presente invención se comprenderá mejor con la lectura de la descripción que sigue, en referencia con unos ejemplos no limitativos de realización, ilustrados por los dibujos adjuntos en los que:

- la figura 1 representa un esquema de la arquitectura funcional de la invención
- la figura 2 representa un esquema de la arquitectura funcional de una variante de realización de la invención
- la figura 3 representa una vista esquemática de los datos intercambiados entre los diferentes recursos informáticos.

Arquitectura funcional

El usuario es un administrador de recursos de un sistema de información (SI) (servidores, aplicaciones, enrutadores...) que dispone de derechos limitados de administrador, para un conjunto de recursos de los que se encarga.

Dispone de un terminal (100) que comunica con la pasarela intermediaria (300) (o “pasarela de administración”) por la mediación de un canal (201) de una conexión (200) según un protocolo por ejemplo SSH (“secure shell”, en español, intérprete de órdenes seguro) o RDP (“remote desktop protocol”, en español, protocolo de escritorio remoto).

La conexión conlleva la creación de una sesión primaria (301) en la pasarela (300).

El usuario se identifica mediante identificadores digitales que le son propios, y que definen sus derechos, así como la imputación de las acciones que efectúa.

La pasarela (300) incluye una base de datos (302) en la que se registran los identificadores de los usuarios autorizados así como los derechos asociados, que definen los destinos (cuentas y equipos) en los que el usuario tiene derecho de actuar.

Durante la conexión, dos modos de selección del recurso son posibles:

- según el primer modo, el usuario precisa, durante la conexión, el destino al que quiere acceder. En este caso la pasarela verifica si el usuario identificado por su identificador dispone de las autorizaciones necesarias para acceder a este destino, en función de las informaciones registradas en la base de datos (302).
- Según el segundo modo, la pasarela transmite al usuario la lista de los destinos que corresponden a los datos registrados en la base de datos (302) en relación con el identificador transmitido, para permitir al usuario seleccionar uno de los destinos propuestos.

La etapa siguiente consiste en abrir una conexión (400), generalmente con el mismo protocolo SSH o RDP, o incluso con un segundo protocolo con la cuenta asociada al destino seleccionado. Esta conexión abre una sesión secundaria (501) en el destino.

Cuando el destino es una aplicación (504), la pasarela (300) elige el servidor (500) adecuado para la ejecución de dicha aplicación. Para este propósito, la base de datos (302) comprende una lista de las aplicaciones y de los servidores que alojan cada una de dichas aplicaciones, así como las cuentas que permiten conectarse a estos servidores.

Cuando varios servidores alojan una misma aplicación, la pasarela realiza un balance de las cargas en función del número de conexiones ya abiertas hacia cada uno de los servidores, y selecciona para la nueva petición el servidor menos solicitado.

Asimismo, en ausencia de respuesta por un servidor que aloja una aplicación, la pasarela busca sucesivamente los otros servidores que alojan la misma aplicación, para seleccionar un destino disponible.

La etapa siguiente consiste en ejecutar un código informático (502) para:

- interrogar la pasarela (petición 402) para obtener las informaciones de autenticación que corresponden a la cuenta de la aplicación, a saber el identificador $ID_{proxy,aplicación}$ así como los datos de autenticación asociados a esta cuenta, por ejemplo una contraseña o un certificado criptográfico, o un ticket Kerberos. Estos datos se vuelven a enviar por la pasarela (respuesta 403). La petición y la respuesta se efectúan en un canal abierto para este propósito por el código informático.
- inyectar estos datos (503) en la aplicación (504) con el fin de abrir una sesión aplicativa y permitir al usuario usar dicha aplicación.

Este código puede:

- instalarse en el servidor (500) de manera permanente. En este caso, el camino de acceso a este código se define en la base de datos (302)
- o transmitirse transitoriamente, por un canal dedicado (401) previsto en el protocolo multicanal, para ejecutarse transitoriamente en el servidor (500).

El nombre de este código puede generarse de manera única, con el fin de dificultar la alteración de este código durante la ejecución de la aplicación, por un ataque informático.

Este código instalado transitoriamente puede incluir igualmente un testigo único con el fin de reducir los riesgos de acceso no autorizado a los datos registrados en la base (302), por medio de la sesión abierta, por un atacante que tenga acceso al servidor (500).

Acceso concurrente a aplicaciones en un mismo servidor por varios usuarios.

La figura 2 representa un esquema funcional de una solución que permite a varios usuarios el acceso a aplicaciones alojadas en un mismo servidor. El objetivo es evitar las interferencias entre las sesiones primarias (200 y 250), y hacerlas estancas en términos de seguridad.

Para este propósito, cuando un segundo usuario (150) trata de ejecutar una aplicación alojada en el mismo servidor (500) que una aplicación ejecutada para un primer usuario (100), la pasarela (300) inhibirá los datos de la base (302) relativos a la cuenta usada por el primer usuario (100), en el servidor (500). Solo autorizará la ejecución de una aplicación en este mismo servidor (500) si una cuenta permanece disponible para un segundo usuario (150).

Datos intercambiados entre los recursos informáticos

La figura 3 representa una vista esquemática de los datos intercambiados entre los diferentes recursos informáticos.

Durante la conexión por un usuario, el terminal (100) transmite a la pasarela intermediaria (300) los datos de autenticación digitales siguientes:

- $ID_{usuario}$
- Contraseña

Estos datos de autenticación pueden estar constituidos, en vez de la contraseña, por un ticket Kerberos o por un certificado X509).

Estos datos de autenticación se verifican por la pasarela (300), en función de las informaciones registradas en su base de datos (302).

En caso de validación, la pasarela (302) transmite la lista de los destinos autorizados.

Cada destino corresponde a un par:

- aplicación
- cuenta asociada a la aplicación.

La cuenta comprende:

- una información de identificación
- una información de autenticación, tal como una contraseña.

La pasarela transmite al usuario (100), para cada uno de los destinos autorizados, solamente la designación de la aplicación y la designación del identificador de la cuenta, pero no la información de autenticación, bajo la forma de cadenas de caracteres que designan los pares aplicación/cuenta.

El usuario (100) selecciona uno de los destinos propuestos y transmite de ello el identificador a la pasarela (300).

La pasarela (300) elige un servidor, y una cuenta para abrir una sesión en dicho servidor (500) según el proceso de selección del servidor y de la cuenta que se ha descrito anteriormente.

Abre de este modo una sesión secundaria, en el servidor, ejecutando el código informático que corresponde a la aplicación. Este código solicita a la pasarela el identificador de la cuenta de la aplicación así como los datos de autenticación asociados a esta cuenta.

El código informático transmite entonces estas informaciones a la aplicación para mandar la ejecución de la aplicación.

La invención permite al código informático interrogar la pasarela sin necesitar una nueva autenticación por el usuario, porque lo hace a través de una conexión ya autenticada.

REIVINDICACIONES

1. Procedimiento de conexión seguro a una aplicación (504) ejecutada en un servidor (500) desde un equipo informático cliente, por un usuario (100) que no dispone de los datos de autenticación de la cuenta declarada en dicha aplicación, comprendiendo dicha cuenta al menos una identidad $ID_{proxy,aplicación}$ y datos de autenticación asociados, implementando un proxy (300) que comprende una memoria para el registro, para cada usuario declarado por una cuenta primaria que comprende al menos una identidad $ID_{usuario,}$ de la lista de los destinos $D_{recursos, cuentas}$ a la que tiene acceso, comprendiendo el procedimiento las etapas siguientes:

- apertura por el usuario de una conexión (200) con el proxy por medio de un protocolo de administración nativo multicanal, con una primera identidad $ID_{usuario}$ para la apertura de una sesión multicanal primaria (301),
- definición simultánea o secuencial de la aplicación,
- conexión del proxy al servidor de alojamiento de dicha aplicación seleccionada por medio del mismo protocolo de administración nativo multicanal con una segunda identidad $ID_{proxy,servidor}$ para abrir una sesión multicanal secundaria (501),
- registro temporal de una información $I_{relé}$ correspondiente al enlace entre dicha sesión primaria y dicha sesión secundaria
- ejecución en el servidor de un código informático (502) que abre un canal entre dicho servidor y dicho proxy, en el marco de dicha sesión multicanal secundaria,
- envío por dicho código en dicho canal de una petición que solicita, para dicha aplicación y dicha cuenta, los datos de autenticación
- en respuesta a esta petición, transmisión por el proxy de estos datos de autenticación si el destino definido por dicha aplicación y dicha cuenta pertenece a la lista de los destinos $D_{recursos, cuentas,}$ asociados a un identificador $ID_{proxy,aplicación,}$ registrado por dicho usuario,
- y ejecución de dicha aplicación y transmisión (503) a dicha aplicación por dicho código de los datos usuarios o notificación de error si la cuenta no pertenece a dicha lista.

2. Procedimiento de conexión segura a una aplicación según la reivindicación anterior, que incluye además una etapa de selección de un servidor de aplicación de entre una pluralidad de servidor que aloja la misma aplicación.

3. Procedimiento de conexión segura a una aplicación según una cualquiera de las reivindicaciones anteriores, en el que el código informático se registra en el servidor de aplicación (500).

4. Procedimiento de conexión seguro a una aplicación según la reivindicación anterior, en el que el código informático se registra por el proxy (300) en el servidor de aplicación (500) con un nombre de uso único.

5. Procedimiento de conexión seguro a una aplicación según la reivindicación 3 o 4, en el que el código informático registrado en el servidor de aplicación (500) contiene un testigo de uso único transmitido con la petición.

6. Procedimiento de conexión seguro a una aplicación según la reivindicación 3 o 4, en el que la aplicación (504) se usa por dos usuarios (100, 150) diferentes que tienen como identidades $ID_{usuario\ A}$ e $ID_{usuario\ B}$, ejecutándose cada una de las sesiones secundarias con una identidad diferente ($ID_{proxy,/servidor\ A}$ e $ID_{proxy,servidor\ B}$), eligiéndose dichas identidades automáticamente por el proxy (300) de entre las identidades configuradas de modo que nunca haya al mismo tiempo dos sesiones secundarias con la misma identidad.

Fig. 1

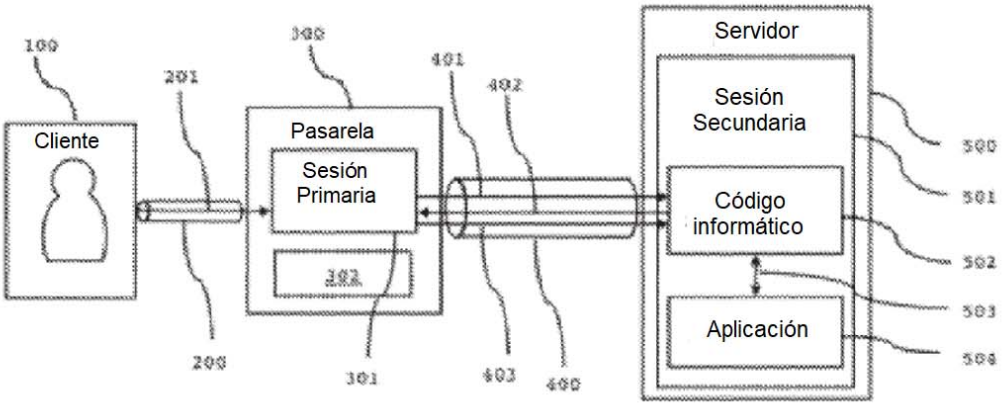

100
Cliente
201
200
300
Pasarela
Sesión
Primaria
302
301
401
402
403
400
Servidor
Sesión
Secundaria
Código
informático
Aplicación
500
501
502
503
504

Fig. 2

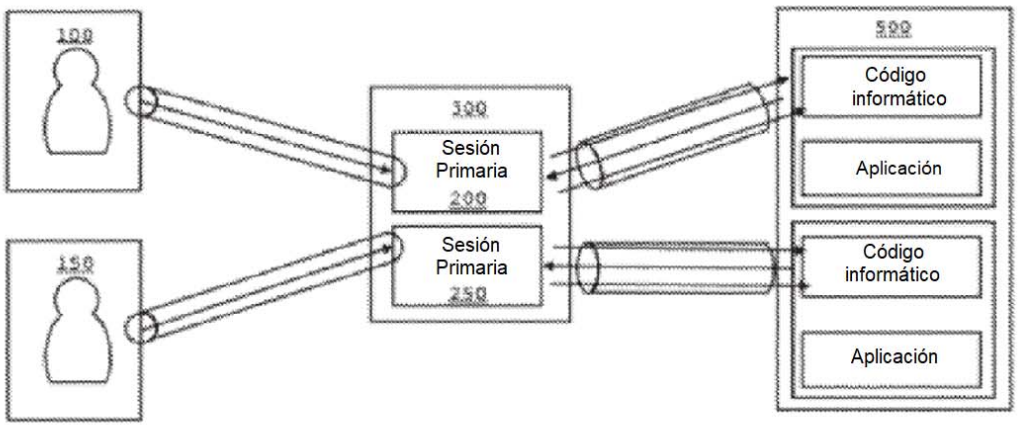
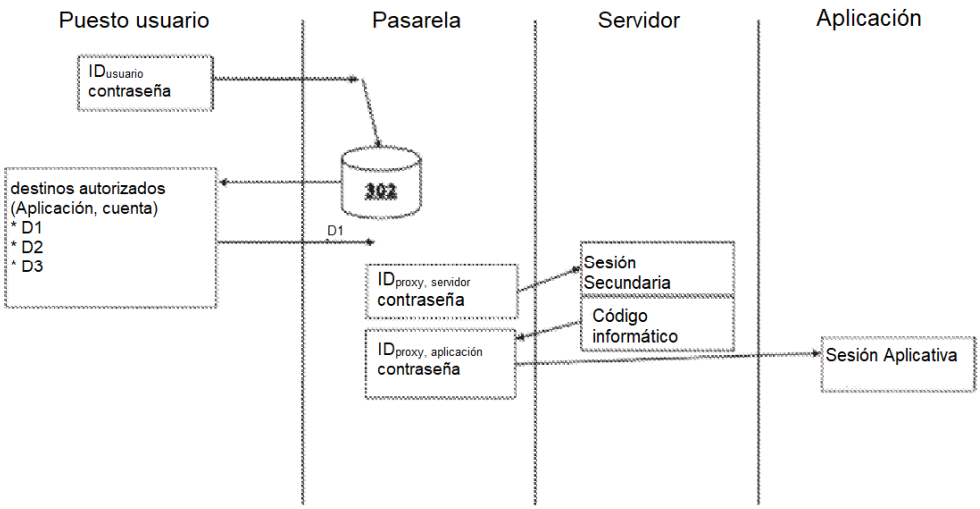

100
150
300
Sesión
Primaria
200
Sesión
Primaria
250
500
Código
informático
Aplicación
Código
informático
Aplicación

Fig. 3


Puesto usuario
Pasarela
Servidor
Aplicación
IDusuario
contraseña
302
destinos autorizados
(Aplicación, cuenta)
* D1
* D2
^ D3
D1
IDproxy, servidor
contraseña
IDproxy, aplicación
contraseña
Sesión
Secundaria
Código
informático
Sesión Aplicativa