(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **1 296 124**

(21) Número de solicitud: 202231137

(51) Int. CI.:

G06F 21/00 (2013.01)
G06F 21/30 (2013.01)
H04L 9/00 (2012.01)

(12) SOLICITUD DE MODELO DE UTILIDAD U

(22) Fecha de presentación:

06.07.2022

(43) Fecha de publicación de la solicitud:

30.12.2022

(71) Solicitantes:

PALACIO HOHENLEITER, Antonio (100.0%)
C/ CASCAIS Nº69 2ºA MONTEQUINTO
41089 DOS HERMANAS (Sevilla) ES

(72) Inventor/es:

PALACIO HOHENLEITER, Antonio

(74) Agente/Representante:

HERRERA DÁVILA, Álvaro

(54) Título: **DISPOSITIVO DE SEGURIDAD PARA ACCESO A REDES**

ES 1 296 124 U

DESCRIPCIÓN

DISPOSITIVO DE SEGURIDAD PARA ACCESO A REDES

OBJETO DE LA INVENCIÓN

La presente invención se refiere a un dispositivo electrónico que propone una plataforma de seguridad previa al acceso o entrada a la red (internet), actuando como antesala, y proporcionando un entorno seguro que protege, tanto al usuario, en cuanto a privacidad, anonimato y sus datos, como a sus dispositivos, antes y durante su conexión a la red.

El dispositivo alberga una aplicación contenedora de otras aplicaciones de forma que, cada vez que el usuario quiera abrir una aplicación, esta se tendrá que sincronizar con el dispositivo para dar acceso, no teniendo opción de hacerlo de manera remota, para impedir violaciones del sistema. Para mayor seguridad, por si existiese alguna vulneración, siempre solicitará confirmación de la apertura de cualquier aplicación.

Tendrá que hacerse a través de la sincronización de un elemento externo con conexión off-line, con un cifrado de alta seguridad que contiene caracteres especiales que son exclusivos y desconocidos, dando al usuario y a sus dispositivos, además de un nivel de seguridad extremo, privacidad y anonimato, dado que, además, la identificación de cada usuario será a través de un nick que el propio usuario elija, teniendo la opción de ocultar todos sus datos personales o que puedan comprometerle de algún modo.

Por otro lado, todas las conexiones a la red se harán a través de conexiones VPN o similares expresas para la aplicación del dispositivo objeto de la presente invención. Los datos irán cifrados, usándose, entre otras, la función HASH (función resumen), para asegurar que los datos que se reciben son exactamente los mismos que los originales. También se establecerá un control para evitar autorizar involuntariamente acceso a recursos protegidos, así como otras autorizaciones involuntarias provocadas por malware, ransomware u otros y que puedan provocar algún tipo de daño o perjuicio a los usuarios y/o dispositivos.

Viene a proponer una solución a la hora de poder acceder a internet de forma segura, proveyendo tanto a usuario como a dispositivos de un entorno de seguridad a modo de antesala, a través de una conexión segura, exclusiva y externa (off-line) a este dispositivo, que generará contraseñas aleatorias de alta seguridad cada cierto tiempo.

La aplicación del dispositivo de seguridad cuenta con una opción para instalarla en cualquier página web o aplicación, donde el usuario pueda elegir la opción de autenticar con la aplicación del dispositivo de seguridad objeto de la presente invención, eliminando así muchos de los riesgos que los usuarios tienen en internet como, por ejemplo:

- Robos de correo electrónico
- Bloqueo del buzón de correos
- Recepción de mensajes spam u ofensivos (ciberacoso)
- Phishing en todas sus modalidades
- Suplantación o robo de identidad

Así como las consecuencias asociadas a cada una de esas y de otras acciones maliciosas.

La aplicación industrial de esta invención se encuentra dentro de los equipos y sistemas de seguridad virtual y ciberseguridad, y más concretamente, dispositivos de seguridad para acceso a redes.

ANTECEDENTES DE LA INVENCIÓN

Aunque no se ha encontrado ninguna invención idéntica a la descrita, exponemos a continuación los documentos encontrados que reflejan el estado de la técnica relacionado con la misma.

Así el documento ES2739896T5 hace referencia a un procedimiento realizado en un dispositivo electrónico que está conectado comunicativamente a un servidor, comprendiendo el procedimiento: - autenticar al usuario del dispositivo electrónico y/o al dispositivo electrónico con el servidor, - proporcionar una primera clave procedente del servidor tras una autenticación satisfactoria; - descifrar datos cifrados almacenados en el dispositivo electrónico con la primera clave mediante un software almacenado en el dispositivo electrónico; - realizar una comunicación del dispositivo electrónico utilizando los datos descifrados, o - realizar una comunicación del dispositivo electrónico utilizando la primera clave junto con datos almacenados en el dispositivo electrónico.

EP3100446A1 propone un método para generar un registro de una llamada entre un primer dispositivo y un segundo dispositivo, incluyendo el registro datos de contenido de llamada recibidos, transmitidos o recibidos y transmitidos entre el primer y segundo dispositivos a través de un segundo canal de comunicaciones, siendo llevado a cabo el método por el primer dispositivo.

ES2895440T3 reivindica un método implementado por computadora para administrar derechos digitales basados en roles en un sistema informático, que comprende: la verificación de un estatus legal de un primer usuario que pretende actuar como autoridad de registro enviando una solicitud de verificación de estatus bajo un datagrama en un formato predefinido a un servidor de organismo expedidor de licencias que almacena información de estatus con respecto al estatus legal del primer usuario y en el que el servidor del organismo expedidor de licencias está programado para reconocer el formato predefinido y buscar y obtener automáticamente la información de estatus para asegurarse de que el primer usuario tiene licencia para actuar como autoridad de registro.

Conclusiones: Como se desprende de la investigación realizada, ninguno de los documentos encontrados soluciona los problemas planteados como lo hace la invención propuesta.

DESCRIPCIÓN DE LA INVENCIÓN

El dispositivo de seguridad para acceso a redes objeto de la presente invención se constituye a partir de un dispositivo que sirve de plataforma de seguridad previa a la entrada en la red (internet), que actúa como antesala y proporciona un entorno de seguridad que protege tanto al usuario (privacidad, anonimato e información) como a sus dispositivos electrónicos.

El dispositivo, que cuenta con medios de entrada y salida de datos al que se conecta el usuario a través de sus dispositivos, cuenta con una aplicación a la que se conecta, y que genera contraseñas aleatorias de alta seguridad cada cierto intervalo de tiempo programado.

Dicho dispositivo generador de claves seguras posee un número identificativo de serie único y exclusivo (número de serie de fabricación), además de una contraseña identificativa exclusiva, segura y secreta; contraseña también cambiante cada X segundos de manera aleatoria en donde se utilizarán caracteres especiales exclusivos creados expresamente para esta aplicación y que actualmente no existan, para dificultar aún más que alguien pueda descubrir dicha contraseña. Esta contraseña identificativa exclusiva también puede ser fija y ser cambiada a voluntad del usuario/empresa, en caso de pérdida o simplemente como refuerzo de la seguridad.

Además, dicha aplicación solo estará sincronizada con su dispositivo de seguridad correspondiente, y tanto la contraseña identificativa exclusiva y segura como la o las contraseñas aleatorias generadas cada cierto tiempo tendrán que estar sincronizadas y

conectadas por vía inalámbrica (Bluetooth, por ejemplo) que aporte el máximo de seguridad para dar acceso a la aplicación.

Solo el usuario específico del dispositivo de seguridad tendrá acceso a dichas claves y contraseñas, las cuales estarán almacenadas en un dispositivo externo fuera de red, para el caso en que un dispositivo de seguridad objeto de la presente invención se pierda o averíe, poder reemplazarlo con la contraseña exclusiva de un usuario concreto.

La aplicación de seguridad por su parte dispondrá de una carpeta contenedora de aplicaciones, donde cualquier aplicación que se compruebe que es confiable podrá estar dentro del entorno de seguridad que se proporciona.

Salvo que se indique lo contrario, todos los elementos técnicos y científicos usados en la presente memoria poseen el significado que habitualmente entiende un experto normal en la técnica a la que pertenece esta invención. En la práctica de la presente invención se pueden usar procedimientos y materiales similares o equivalentes a los descritos en la memoria.

A lo largo de la descripción y de las reivindicaciones la palabra “comprende” y sus variantes no pretenden excluir otras características técnicas, aditivos, componentes o pasos. Para los expertos en la materia, otros objetos, ventajas y características de la invención se desprenderán en parte de la descripción y en parte de la práctica de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para una mejor comprensión de la presente descripción se acompañan unos dibujos que representan una realización preferente no limitativa de la presente invención:

Figura 1: Vista esquemática del uso del dispositivo de seguridad para acceso a redes objeto de la presente invención.

Las referencias numéricas que aparecen en dichas figuras corresponden a los siguientes elementos constitutivos de la invención:

1. Dispositivo externo
2. Usuario
3. Dispositivos electrónicos
4. Medios de entrada y salida de datos
5. Aplicación
6. Número identificativo de serie
7. Contraseña identificativa exclusiva

DESCRIPCIÓN DE UNA REALIZACIÓN PREFERENTE

Una realización preferente del dispositivo de seguridad para acceso a redes objeto de la presente invención, con alusión a las referencias numéricas, puede basarse en un dispositivo externo (1) que actuará de plataforma de seguridad previa a la entrada en la red (internet), proporciona un entorno de seguridad que protege tanto al usuario (2) como a sus dispositivos electrónicos (3).

El dispositivo externo (1) comprende medios de entrada y salida de datos (4) al que se conecta el usuario (2) a través de sus dispositivos (3), y alberga una aplicación (5) que genera contraseñas aleatorias de alta seguridad cada cierto intervalo de tiempo programado, treinta segundos, por ejemplo.

Dicho dispositivo externo (1) posee un número identificativo de serie (6) único y exclusivo, además de una contraseña identificativa exclusiva (7), segura y secreta; contraseña también cambiante cada X segundos de manera aleatoria en donde se utilizarán caracteres especiales exclusivos creados expresamente para esta aplicación y que actualmente no existan, para dificultar aún más que alguien pueda descubrir dicha contraseña.

Además del número identificativo de serie (6) y la contraseña identificativa exclusiva (7), el dispositivo externo (1) será un generador de claves seguras, pudiendo generar una o varias claves aleatorias y cambiantes cada cierto tiempo, que irán sincronizadas con la aplicación que se instala en los dispositivos y que, además de que el dispositivo será reconocido por la aplicación por su contraseña identificativa exclusiva, la aplicación reconocerá las claves que se van generando haciendo una doble o triple autenticación y aportando mayor grado de seguridad. Las contraseñas generadas por el dispositivo externo (1) podrán estar o no a la vista, pero deberán ser reconocidas por la aplicación una vez instalada en cualquier dispositivo electrónico (3) del usuario (2).

La aplicación (5) comprende, entre otros elementos:

- Un nick de usuario, contraseña elegida por este, comprobación de huella dactilar y/o facial.
- Contraseña de entrada segura, con clave identificativa de usuario exclusiva y secreta y con claves cambiantes cada cierto tiempo.
- Soluciones antivirus. Donde se facilitarán accesos y enlaces que permitan revisar si algún elemento o dispositivo está infectado por algún malware. (no se permitirá la descarga de ningún malware, spyware, ransomware, etc. dentro de la aplicación de

seguridad, pues cualquier instalación solicitará comprobación y autorización; además, todas las descargas irán a una carpeta aislada del resto.

- Cifrado de datos
- Conexión VPN
- Sistema anti rastreo, en donde se podrá cambiar la información del dispositivo, pudiendo elegir para dicha información, entre otros navegadores y otros sistemas operativos y otros, sistema tipo User-Agent Switcher and Manager o similar.

La aplicación (5) del dispositivo externo (1) de seguridad cuenta con una opción para instalarla en cualquier página web o aplicación, donde el usuario pueda elegir la opción de autenticar con la aplicación del dispositivo de seguridad objeto de la presente invención. Dicha opción de autenticación podría sustituir o ser añadida como opción, a las autenticaciones que ciertas webs, redes sociales, etc., solicitan al usuario al darse de alta, dando el usuario en muchas ocasiones y sin saberlo, autorizaciones que pudieran perjudicarles y/o que entrañen riesgos para la privacidad de sus datos personales.

En una realización diferente, el dispositivo externo (1) se conecta a los dispositivos electrónicos (3) del usuario (2) a través de algún cable de conexión, con el requisito de que el dispositivo externo (1) deba desconectarse completamente de la red.

REIVINDICACIONES

1.- Dispositivo de seguridad para acceso a redes, constituido por un dispositivo externo (1) a modo de plataforma de seguridad previa a la entrada en la red (internet), caracterizado porque comprende unos medios de entrada y salida de datos (4) al que se conecta el usuario (2) a través de sus dispositivos (3), y alberga una aplicación (5) que genera contraseñas aleatorias de alta seguridad cada cierto intervalo de tiempo programado, y posee un número identificativo de serie (6) único y exclusivo, y una contraseña identificativa exclusiva (7), donde se utilizarán caracteres especiales para la conexión entre el dispositivo externo (1) y a los dispositivos electrónicos (3) del usuario (2).

2.- Dispositivo de seguridad para acceso a redes, según reivindicación 1, donde la conexión entre el dispositivo externo (1) y a los dispositivos electrónicos (3) del usuario (2) y los unos medios de entrada y salida de datos (4) son del tipo inalámbrico.

3.- Dispositivo de seguridad para acceso a redes, según reivindicación 1, donde la conexión entre el dispositivo externo (1) y a los dispositivos electrónicos (3) del usuario (2) y los unos medios de entrada y salida de datos (4) son por cable.

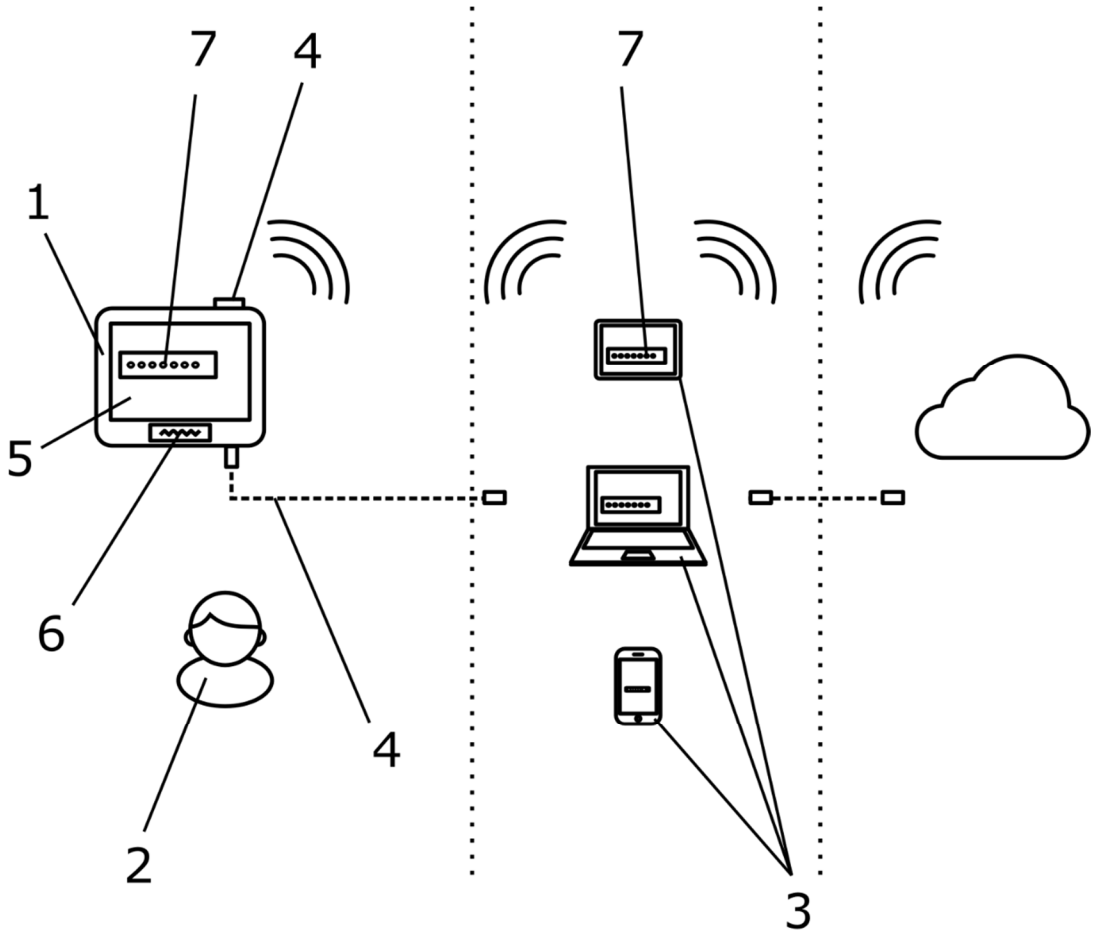


FIG 1